IBM Cloud Application Performance Management
Junho de 2019

Guia do Usuário

Nota

Antes de utilizar estas informações e o produto suportado por elas, leia as informações em “Avisos” na página 1513.

Esta edição aplica-se à versão de junho de 2019 do IBM® Cloud Application Performance Management e a todas as liberações e modificações subsequentes, até que seja indicado de outra forma em novas edições.

Índice

Capítulo 1. O que há de novo

Novos recursos, capacidades e cobertura estão disponíveis na liberação mais recente.

- Para obter informações sobre a versão do agente em cada liberação ou atualização, consulte "Histórico de Mudanças" na página 50.

Dezembro de 2019

Novo agente

MariaDB agent

O Monitoring Agent for MariaDB oferece um ponto central de gerenciamento para seu ambiente ou aplicativo do MariaDB. O software fornece um meio abrangente de reunir as informações requeridas para detectar problemas antecipadamente e para preveni-los. As informações são padronizadas por meio do sistema. É possível monitorar diversos servidores de um único console. Ao usar o Monitoring Agent for MariaDB, é possível coletar e analisar facilmente informações específicas do MariaDB.
Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do MariaDB" na página 483

Expandido suporte da plataforma para agentes

Os agentes e plataformas a seguir são agora suportados:

Solaris X86-64

- Agente Oracle Database
- Agente WebLogic

Aprimoramentos do agente

Agente Cassandra

Foram incluídos dois novos atributos chamados `Agent Hostname` e `Agent Instance Name` nos grupos de atributos `Cluster Details`, `Node Statistics` e `Keyspace Details`.

Db2

Incluído o suporte para monitorar `Current Running SQL`.

IBM Integration Bus agent

Incluídos dois novos widgets de grupo, `TCPIP Client Connections` e `TCPIP Server Connections` na página `Integration Server Status - Detail`.

Monitoramento de Serviço da Internet

- Incluídas duas novas variáveis do painel de configuração:
  - *Active*: para selecionar um estado para elemento de perfil como ativo ou inativo.
  - *sniServerName*: indica o nome do host/servidor para o qual é necessário um certificado do servidor da web ativado por SNI.
- As **Configurações padrão** na guia **Validação de dados** para monitores HTTP, HTTPS e DNS são agora editáveis
- O agente agora suporta o caractere & no campo **página** para monitores HTTP e HTTPS
- O agente agora suporta caracteres dinamarqueses no campo **regex** de monitores HTTP e HTTPS

  Nota: Configure o código de idioma para a plataforma da_DK no Linux antes da instalação do agente para usar este recurso

Microsoft Active Directory agent

- Incluído um novo widget chamado `KCC details` na página `Status Overview`.
- Incluídos os novos grupos de atributos a seguir na guia Detalhes do atributo:

  - Serviços de Diretório
  - Kerberos Consistency Checker
  - Key Distribution Center do Kerberos
  - Name Service Provider
  - Serviço de Diretório de Troca

Microsoft .NET agent
Incluído um novo atributo chamado Request Name no grupo de atributos Database Call Details. Esse atributo exibe o nome da solicitação que dispara a consulta do banco de dados.

Microsoft Exchange Server agent

- Incluído um novo widget chamado Transport SMTP Recive na página Status Overview.
- Incluídos os novos grupos de atributos a seguir na guia Detalhes do atributo:
  - MS Exchange AB
  - Processos ADAccess do MS Exchange
  - Caches ADAccess do MS Exchange
  - Controladores de Domínio do MS Exchange ADAccess
  - MS Exchange ADAccess Forest Discovery

Microsoft Hyper-V Server agent
Incluído o suporte para o Windows Server 2019.

Microsoft IIS agent

- Incluídos novos widgets de grupo:
  - System-Main Memory Statistics
  - IIS Server- Assigned Memory Usage
  - IIS Server- Assigned CPU Usage
  - Worker Process Details
  - .Net Memory Management
- Em cada nome do conjunto de aplicativos no widget de grupo Worker Process Details é criada uma página que mostra a tendência histórica de Solicitações processadas por segundo, Tempo decorrido, Solicitações em fila, Utilização de memória e de CPU.
- Em cada nome do conjunto de aplicativos no widget de grupo .Net Memory Management, um pop-up é incluído, mostrando a tendência histórica de percentual de tempo em GC.

Microsoft SharePoint Server agent

- Incluído um novo grupo de atributos chamado Trace_Log que fornece as informações de logs de alta gravidade.
- Incluídos dois novos widgets de grupo chamados Trace Log Details e Last 1 Hour Trace Log Count na página Visão geral para exibir os detalhes de 100 eventos de log de rastreamento recentes e a contagem de 1 hora de logs de rastreamento inesperados e de alto nível.

Agente MySQL
O agente coleta dados de forma consistente após a reinicialização de servidor.

Agente NetApp Storage
O agente agora mostra a lista exata de Qtress que são mapeados para o Volume.

Agente PostgreSQL
Agora o agente suporta o PostgreSQL Server versão 12.

Agente Response Time Monitoring

- Um novo parâmetro de configuração KT5AARIPTOUSERID é incluído. Ele permite salvar o endereço IP do Cliente na propriedade Nome do usuário em dados brutos do AAR. Por padrão,

ele é configurado como NO. Para mudar a configuração, é necessário reiniciar o Agente Response Time Monitoring.

  - KT5AARIPTOUSERID=NO: se o valor for NO, o agente do Agente Response Time Monitoring salvará o nome de usuário de transação para a propriedade userID de AAR.
  - KT5AARIPTOUSERID=YES: se o valor for YES, o Agente Response Time Monitoring salvará o endereço IP de origem de transação para a propriedade userID de AAR.
- O Agente Response Time Monitoring agora suporta a especificação do valor KT5AARIPTOUSERID na configuração silenciosa.
- O título do widget de grupo existente `Worst By User - Top 5` é mudado para `Worst By User - Top 20`. O widget de grupo é mudado para exibir os 20 principais usuários com a maior porcentagem de falhas de transação durante o período selecionado.

VMware

- O agente agora suporta buscar o endereço IP ou o nome do Host do vCenter da chamada API do vSphere, em vez de mostrar `Endereço configurado` como é do painel de configuração. O usuário pode ativar esse recurso, configurando a sinalização no ambiente do agente para Y. Por exemplo, KVM_RETRIEVE_HOSTNAME_FROM_API=Y.
- Agora, a contagem de novas tentativas pode ter um limite para restringir as tentativas de conexão com a origem de dados. Por exemplo, KVM_DATA_PROVIDER_CONNECTION_RETRY_COUNT=1000, a inclusão desta variável no arquivo de ambiente do agente colocaria uma contagem de tentativas de bloqueio na contagem de tentativas de conexão em caso de falha de conexão com o vCenter. 1000 indica que o agente tentaria até 1000 tentativas de conexão malsucedidas subsequentes e, em seguida, interromperia o processo do provedor de dados com uma mensagem de log `NÃO MAIS TENTATIVAS DE CONEXÃO; PARANDO A COLETA DE DADOS, PARA RETOMAR O MONITORAMENTO, REINICIE O AGENTE. PARA TER MAIS TENTATIVA DE CONEXÕES, REAJUSTE O VALOR DA VARIÁVEL KVM_DATA_PROVIDER_CONNECTION_RETRY_COUNT`. O valor padrão para novas tentativas de conexão é 6, o usuário pode configurar o limite desejado conforme a necessidade.
- O agente suporta a configuração do tamanho de heap específico da instância para utilizar com eficiência a memória alocada no sistema. Por exemplo, KVM_CUSTOM_JVM_ARGS= -Xmx512m, configurar essa variável no arquivo de ambiente da instância significaria que a instância está configurada para usar 512 MB de memória heap. O tamanho pode ser mudado com base na contagem total de objetos de vCenter que uma instância está monitorando.

Setembro de 2019

Expandido suporte da plataforma para agentes

Os agentes e plataformas a seguir são agora suportados:

Solaris X86-64

- Db2
- Agente SAP
- Sybase agent
- agente de S.O. UNIX
- WebSphere Applications agent
- WebSphere MQ agent
- IBM Integration Bus agent

RHEL on x86-64 (64 bits)

- agente de Monitoramento de Serviço da Internet
- Microsoft SQL Server agent
- Sybase agent

RHEL on POWER Little Endian (ppc64le)

- Agente RabbitMQ

Aprimoramentos do agente

Db2

- Agora o agente suporta Db2 Server versão 11.5.

Agente do Hadoop

- Um novo parâmetro de configuração **`Unique Cluster Name`**, que é o nome exclusivo do cluster Hadoop, indicando que sua versão e seu tipo foram incluídos no painel de configuração.
- Agora o agente Hadoop mostra o item de exibição para os limites criados no Ambari Services.
- Agora o agente Hadoop suporta o monitoramento do serviço Streaming Analytics Manager no cluster Hadoop.
- Agora o agente Hadoop suporta o monitoramento do serviço Schema Registry no cluster Hadoop.

Agente do Servidor HTTP

- Agora o agente suporta o servidor HTTP Oracle no Solaris Sparc.

Monitoramento de Serviço da Internet

- Agora o agente suporta IBM Tivoli Netcool/OMNIbus.
- O agente foi aprimorado para excluir perfis de perfis existentes e renomear os existentes.

Agente MongoDB

- Agora o agente suporta o banco de dados MongoDB versão 4.x.

Agente MySQL

- O atributo FQDN está incluído para Disponibilidade do Aplicativo na seção Ajuda.
- Exibição da dica de ferramenta corrigida para o parâmetro IP Address Agent Configuration.
- Os novos atributos a seguir foram incluídos para monitoramento no IBM Cloud App Management.
  - Informações do tamanho do banco de dados
  - Informações de Erro
  - Contagem de bloqueios de instâncias do BD
  - Detalhes da conexão do usuário
  - Detalhes da lista de processos
  - Informações de Eventos

Agente PostgreSQL

- Duas novas situações chamadas `Deadlocks_Count_Crit` e `Deadlocks_Count_Warn` foram incluídas para monitorar o número de conflitos em um banco de dados, o que ajudará a abordar o problema exato do conflito.
- Um novo grupo de atributos chamado `Deadlocks_Info` foi incluído para verificar os detalhes do conflito.

Sybase agent

- O atributo FQDN está incluído para Disponibilidade do Aplicativo na seção Ajuda.

Synthetic Playback agent

- Agora o Firefox V68.0 ESR é suportado.
- Agora as configurações de proxy do sistema, proxy PAC e sem proxy são suportadas.

Agente Tomcat

- O agente foi aprimorado com métricas e visualizações de UI para monitorar o uso do conjunto de memórias de Heap/Não Heap para a JVM.
- O agente foi aprimorado com métricas e visualizações de UI para monitorar encadeamentos e informações de carregamento de classe para JVM.
- Agora a UI do agente exibe o FQDN na visualização Informações do Servidor.

agente de S.O. UNIX

- Agora o agente foi atualizado com o recurso de script customizado. Shell scripts, scripts PERL e outros tipos de scripts podem ser usados.

Agente VMware VI

- Um novo campo de configuração denominado **KEY_STORE_PASSWORD** foi incluído. Ele permite que um usuário configure o agente com a nova senha de armazenamento de chaves configurada para o JRE do agente.

Junho de 2019

Expandido suporte da plataforma para agentes

Os agentes e plataformas a seguir são agora suportados:

Red Hat Enterprise Linux (RHEL) 8

Os agentes e coletores de dados a seguir agora suportam o RHEL 8. Antes de instalar agentes no RHEL 8, certifique-se de ler a seção "Sistemas operacionais específicos" na página 126 do "Pré-instalação em sistemas Linux" na página 126.

RHEL 8 on x86-64 (64 bits)

- Agente Cassandra
- Cisco UCS agent
- DataPower agent
- DataStage agent
- Db2
- Agente do Hadoop
- Agente do Servidor HTTP
- Integration Agent for Netcool/OMNIbus
- Agente Monitoramento de Serviço da Internet
- Coletor de dados J2SE
- agente do Linux KVM
- agente do S.O. Linux
- Agente MongoDB
- Agente do MQ Appliance
- Agente MySQL
- Agente NetApp Storage
- Coletor de dados Node.js
- Agente PHP
- Coletor de dados do Python
- Agente PostgreSQL
- Agente RabbitMQ
- Response Time Monitoring Agent
- Agente Ruby

- Agente SAP
- SAP HANA Database agent
- SAP NetWeaver Java™ Stack
- Agente Sterling Connect Direct
- Agente Sterling File Gateway
- Sybase agent
- Agente Tomcat
- Agente VMware VI
- WebSphere Applications agent
- WebSphere MQ agent

RHEL 8 on System z

- Db2
- Agente do Hadoop
- agente do S.O. Linux
- Agente MySQL
- Coletor de dados Node.js
- Coletor de dados do Python
- Response Time Monitoring Agent
- WebSphere Applications agent
- WebSphere MQ agent

RHEL 8 on POWER Little Endian (ppc64le)

- Db2
- Agente do Hadoop
- Coletor de dados J2SE
- agente do S.O. Linux
- Agente MySQL
- Coletor de dados Node.js
- SAP NetWeaver Java Stack
- WebSphere Applications agent
- WebSphere MQ agent

Solaris Sparc 10 e 11

- agente JBoss
- Agente Oracle Database
- Agente WebLogic

Windows Server 2019

- WebSphere Applications agent

Aprimoramentos do agente

Agente do Hadoop

- Agora o Agente do Hadoop suporta o monitoramento do HDF 3.3 (com HDP 3.1.0) do serviço Ambari Big SQL 6.0.
- Agora o Agente do Hadoop suporta o SUSE Linux Enterprise Server (SLES) 15 na plataforma x86-64.

Agente HMC Base
O Agente HMC Base suporta HMC V9.1.

Integration Agent for Netcool/OMNIbus
O agente foi atualizado para suportar o Red Hat Enterprise Linux (RHEL) 8 e o SUSE Linux Enterprise Server (SLES) 15

Agente Monitoramento de Serviço da Internet
Agora o agente possui um monitor Service Assurance Agent, que monitora análises do Cisco Service Assurance Agent.

Microsoft IIS agent
O agente foi aprimorado com provisão de tolerância para o servidor Windows 2019. Esse aprimoramento exibe os dados do site FTP para o agente instalado no servidor Windows 2019.

Agente MongoDB
Agora o agente suporta Red Hat Enterprise Linux (RHEL) 8 na plataforma x86-64 (64 bits).

Coletor de dados do Python ifix02
Agora o coletor de dados suporta Django 1.10 e superior.

Agente SAP

Agora o Agente SAP suporta as seguintes plataformas:

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

SAP HANA Database agent

O SAP HANA Database agent foi aprimorado com os seguintes recursos:

- O nome do host é incluído no nó do subnó :HDB do SAP HANA Database agent para sua identificação exclusiva.
- Agora o agente suporta arquitetura de ampliação.
- Red Hat Enterprise Linux (RHEL) 8 em plataformas x86-64 (64 bits) e Linux ppc64le.
- SUSE Linux Enterprise Server (SLES) 15 em plataformas x86-64 (64 bits).
- Um novo atributo Trimmed Host é incluído no grupo de atributos Banco de Dados do Sistema.

SAP NetWeaver Java Stack

O SAP NetWeaver Java Stack suporta as seguintes plataformas:

- Red Hat Enterprise Linux (RHEL) 8 on x86-64 (64 bits)
- SUSE Linux Enterprise Server (SLES) 15 no x86-64 (64 bits)
- Windows Server 2019 DE e SE
- Windows Server 2016 DE e SE

Synthetic Playback agent

- Suporta script .side registrado por Selenium IDE 3.2.X, 3.3.X ou 3.5.X
- Suporta reprodução por Firefox ESR 60.5.1
- Suporta os comandos **`wait`**, **`flow control`** e **`linkText locator type`** do Selenium IDE

Agente Skype for Business Server

O Agente Skype for Business Server foi aprimorado com os seguintes recursos:

- Agora o agente suporta Skype for Business Server 2019.
- Dois novos widgets de grupo, como `Database-Throttled Requests(DBStore)` e `Database-Throttled Requests(SHAREDDBStore)` foram incluídos na página Visão Geral, que exibe o número de solicitações reguladas pelo Skype for Business Server devido à alta latência da fila do banco de dados para DBstore e DBstore compartilhado.

Scanner de Pré-requisitos

Agora, o comando **IGNORE_PRECHECK_WARNING** está disponível como uma alternativa para o comando **SKIP_PRECHECK**. Para obter mais informações, consulte “Efetuando bypass do scanner de pré-requisitos” na página 142.

Aprimoramento da documentação

Foi criada uma página para ajudar a descobrir rapidamente as informações de versão e o histórico de mudanças para cada agente e coletor de dados. Consulte “Histórico de Mudanças” na página 50.

Março de 2019

Expandido suporte da plataforma para agentes

Os agentes e plataformas a seguir são agora suportados:

Windows Server 2019

- Agente Cassandra
- DataStage agent
- Db2
- Agente do Hadoop
- Monitoramento de Serviço da Internet
- Microsoft Active Directory agent
- Microsoft Cluster Server agent
- Microsoft IIS agent
- Microsoft Exchange Server agent
- Microsoft SQL Server agent
- Agente MySQL
- Agente PostgreSQL
- Agente RabbitMQ
- Agente SAP
- SAP HANA Database agent
- Sybase agent
- Agente Tomcat
- Windows OS agent

Solaris SPARC 10 e 11

- Db2
- Servidor HTTP
- Agente MySQL
- Agente SAP
- Sybase agent
- agente de S.O. UNIX
- WebSphere Applications agent

Monitoring Agent for Cassandra

O Agente Cassandra foi aprimorado com os seguintes recursos:

- Incluído suporte para o sistema operacional Windows Server 2019.
- Incluída criação de log detalhada para resolução de problemas.

Monitoring Agent for Db2

O agente Db2 é aprimorado com os seguintes recursos:

- Agora o agente Db2 suporta Windows Server 2019.
- Agora o agente Db2 suporta plataformas Solaris SPARC 10/11.

Monitoring Agent for Hadoop

O Agente do Hadoop foi aprimorado com os seguintes recursos:

- Incluído suporte para monitorar os clusters Hadoop BigInsights, Hortonworks e Cloudera ativados por SSL.
- Incluído suporte para testar a conexão com o cluster Hadoop ativado por SSL.
- Incluído suporte do sistema operacional Windows Server 2019 (Datacenter e Standard Editions).
- Incluído suporte para monitoramento da oferta Hadoop: Cloudera 6.1.1 (CDH 6.1.1).
- Incluído suporte para monitoramento da oferta Hadoop: Hortonworks 3.1.0 (HDP 3.1.0).

Monitoring Agent for IBM Integration Bus

O IBM Integration Bus agent foi aprimorado com o seguinte recurso:

- Incluído suporte de tolerância para monitorar IBM App Connect Enterprise V11. Para obter mais informações, consulte "Configurando o IBM Integration Bus agent" na página 275.

Monitoring Agent for Microsoft Internet Information Services

Agora o Microsoft IIS agent suporta o sistema operacional Windows Server 2019.

Monitoring Agent for InfoSphere DataStage

O DataStage agent foi aprimorado com os seguintes recursos:

- Incluído suporte para o sistema operacional Windows Server 2019.
- Incluído tempo limite de consulta para consultas de coleta de dados para melhorar o desempenho do agente.

Monitoring Agent for Microsoft Active Directory

O Microsoft Active Directory agent foi aprimorado com os seguintes recursos:

- Incluído suporte para Windows Server 2019.
- Incluído novo grupo de atributos `AD_Services_Status` que fornece o estado de serviços relacionados ao Active Directory Server.
  Com base no estado do serviço, determina o Status do Active Directory Server.
- Incluída nova situação `AD_Server_Status` que monitora o Status do Active Directory Server.
- Incluído novo grupo de atributos `Root_Directory_server` que fornece uma versão ativa e um nome de S.O. monitorado.

Monitoring Agent for Microsoft Cluster Server

O Microsoft Cluster Server agent foi aprimorado com os seguintes recursos:

- Incluído suporte para o sistema operacional Windows Server 2019.
- Incluído atributo `CLUSTER_SERVICE_VERSION`.

Monitoring Agent for Microsoft Exchange Server

O Microsoft Exchange Server agent foi aprimorado com os seguintes recursos:

- Incluído suporte para MS Exchange Server 2019.
- Incluído novo grupo de atributos `MSExchange MAPIoverHTTP` que fornece informações sobre o MAPI sobre as estatísticas do protocolo HTTP.

Monitoring Agent for Internet Services

O agente Monitoramento de Serviço da Internet foi aprimorado com os seguintes recursos:

- Incluído suporte para os monitores LDAP, NTP, NNTP, SOAP, SNMP, SIP, RTSP, RPING, RADIUS e TFTP.
- Incluído suporte para o S.O. do servidor Windows 2008 R2 e Windows Server 2019.

Monitoring Agent for Microsoft SQL Server

Agora o Microsoft SQL Server agent suporta Windows Server 2019.

Monitoring Agent for MySQL

O Monitoring Agent for MySQL foi aprimorado com os seguintes recursos:

- Incluído suporte para Windows Server 2019.
- Incluído suporte para plataformas Solaris SPARC 10/11.
- Incluída capacidade de configurar propriedades adicionais para a conexão JDBC iniciada pelo agente com o servidor MySQL.

Monitoring Agent for PostgreSQL

Agora o Agente PostgreSQL suporta o sistema operacional Windows Server 2019.

Monitoring Agent for RabbitMQ

Agora o Agente RabbitMQ suporta o sistema operacional Windows Server 2019.

Monitoring Agent for Skype for Business Server

O Agente Skype for Business Server foi aprimorado com os seguintes recursos:

- Incluído suporte para o sistema operacional Windows Server 2019.
- Incluído novo grupo de atributos chamado `KQL_Server` para exibir informações relacionadas ao produto Skype for Business Server.
- Incluída nova situação chamada `Skype_Server_Down` para monitorar o status do Skype for Business Server com base nos status de serviços de conferência de mensagem instantânea e de front-end do servidor.

Monitoring Agent for SAP Applications

O Agente SAP foi aprimorado com os seguintes recursos:

- Incluído recurso de senha com distinção entre maiúsculas e minúsculas para o usuário do aplicativo sendo utilizado entre o agente SAP e o servidor SAP.
- Incluído suporte para sistema operacional Windows Server 2019 (Datacenter e Standard Editions).
- Incluído suporte para visualizar as Tarefas de Longa Execução presentes no Sistema SAP por mais de 24 horas.
- Melhora no desempenho do módulo de função /IBMMON/ITM_MAIALRT_INX.
- Incluído suporte para os sistemas operacionais Solaris v10 e v11 SPARC.
- Incluído recurso de corte para nome de host SAP para corresponder ao limite máximo de 32 caracteres no Nome do Sistema Gerenciado.

Monitoring Agent for SAP HANA Database

O SAP HANA Database agent foi aprimorado com os seguintes recursos:

- Incluído suporte para descobrir os bancos de dados do locatário quando o nome do BD do locatário e o SID do sistema HANA forem iguais.
- Incluído suporte para sistema operacional Windows Server 2019 (Datacenter e Standard Editions).

Monitoring Agent for Sybase Server

O Sybase agent foi aprimorado com os seguintes recursos:

- Incluído suporte para Windows Server 2019.
- Incluído suporte para plataformas Solaris SPARC 10/11.

- Consulta Sybase aprimorada para melhorar a simultaneidade e reduzir bloqueios.

Monitoring Agent for Tomcat

Agora o Agente Tomcat suporta o sistema operacional Windows Server 2019 (Datacenter e Standard Editions).

Monitoring Agent for UNIX OS

O agente de S.O. UNIX foi aprimorado com o seguinte recurso:

- Incluído suporte para Solaris SPARC 10 e 11.

Monitoring Agent for VMware VI

O Agente VMware VI foi atualizado para ignorar os valores indisponíveis (-1) durante a exibição da tendência de média no gráfico para todos os gráficos multilinhas.

Monitoring Agent for WebSphere Applications

O WebSphere Applications agent foi aprimorado com os seguintes recursos:

- Incluído suporte para Solaris SPARC 10 e 11.
- Incluído suporte para monitoramento do WebSphere® Extreme Scale. É possível configurar o monitoramento para uma zona ou várias zonas do Extreme Scale no nó, para qualquer servidor pertencente à zona ou às zonas. É possível fazer drill down para visualizar informações de diferentes servidores, conjuntos de mapas e partições na zona ou zonas. Para obter mais informações, consulte “Configurando o WebSphere Applications agent para monitorar o WebSphere Extreme Scale” na página 921.

Monitoring Agent for WebSphere MQ

O WebSphere MQ agent foi aprimorado com os seguintes recursos:

- Incluído suporte para SLES 15 xLinux.
- Incluído suporte para coletar estatísticas para o gerenciador de filas e exibir os dados coletados. Para obter mais informações, consulte “Ativando o monitoramento de estatísticas de fila para o gerenciador de filas do IBM MQ” na página 942.

Aprimoramentos do Coletor de Dados

Coletor de dados J2SE

O Coletor de dados J2SE foi aprimorado com os seguintes recursos:

- Incluído suporte para as versões 9, 10 e 11 do OpenJDK.
- Incluído suporte do sistema operacional Windows Server 2019 (Datacenter e Standard Editions).
- Incluído recurso para descoberta automática de classes e métodos específicos do aplicativo J2SE para monitoramento de Rastreamento de Transação e Dados de Diagnóstico.

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

Se sua assinatura incluir o complemento IBM Website Monitoring on Cloud, agora o Selenium IDE versões 3.2X e 3.3.X serão suportados; scripts e testes são salvos no formato `.side` em vez de no formato `.html` usado por versões mais antigas do Selenium IDE. Se você tiver os scripts `.html` existentes, ainda é possível usá-los. Em alguns casos, talvez você queira editar os scripts `.html` ou registrá-los novamente no novo formato `.side`.

Para obter mais informações, consulte esses subtópicos do “Gerenciando transações e eventos sintéticos com o Website Monitoring” na página 1026: “Registrando scripts sintéticos” na página 1027, “Estruturando scripts complexos” na página 1029 e “Atualizando scripts de versões anteriores do Selenium IDE” na página 1031.

Dezembro de 2018

Novo agente

Monitoring Agent for IBM Cloud

O Monitoring Agent for IBM Cloud coleta o inventário e as métricas da máquina virtual da conta do IBM Cloud (Softlayer). Use o IBM Cloud agent para rastrear quantos dispositivos virtuais você configurou e que estão em execução no IBM Cloud. É possível ver quais recursos são alocados para cada dispositivo virtual na página detalhada do painel, que também mostra informações como o data center em que um dispositivo está localizado, o sistema operacional e a largura da banda da rede pública projetada para o mês.

Aprimoramentos do agente

Monitoring Agent for Cassandra

O agente Cassandra foi aprimorado com os recursos a seguir:

- Incluído um novo limite denominado `Cassandra_Cluster_Down`, que monitora o estado da instância monitorada.
- Incluído suporte para o sistema operacional Ubuntu 18.04.
- Incluído suporte para plataforma SUSE Linux Enterprise Server 15.

Monitoring Agent for Db2

O agente Db2 é aprimorado com os seguintes recursos:

- Agora o agente Db2 suporta Capacidades de Monitoramento de HADR para múltiplas esperas.
- Agora o agente Db2 suporta o novo valor `Stopped` para o atributo Database Status. O status `Stopped` indica que o banco de dados não está ativo e que tem zero conexões ativas enquanto ele está funcionando e pronto para aceitar novas conexões.
- Incluído o novo widget `Db2 Server Information` para exibir detalhes do Db2 Server.
- Incluída a nova página `HADR Status – Local Databases` para exibir as informações sobre bancos de dados parceiros nos novos widgets a seguir:
  - `HADR Databases Details` é o widget da tabela que exibe valores de atributos importantes para o banco de dados do parceiro.
  - `Log Gap (History)` é o widget gráfico que exibe a tendência do intervalo de log vs. tempo.
  - `Standby Flag Status` é o widget da tabela que exibe os valores de status da sinalização de espera.
- Incluído o novo limite predefinido `UDB_HADR_Aux_Standby_Disconnect` para monitorar bancos de dados de espera secundários no ambiente HADR.
- O widget de uso de memória do banco de dados 5 Principais foi atualizado para mostrar o valor correto.
- Agora o agente Db2 suporta as seguintes plataformas:
  - Ubuntu zLinux 18.04
  - SUSE Linux Enterprise Server 15 no x86-64 (64 bits)
  - SUSE Linux Enterprise Server 15 for zLinux
  - SUSE Linux Enterprise Server 15 for Power Linux Little Endian

Monitoring Agent for InfoSphere DataStage

O agente InfoSphere DataStage foi aprimorado com os seguintes recursos:

- Incluído recurso para desativar a coleta de dados para grupos de atributos selecionados.
- Coleção de dados otimizada para grupo de atributos de Execuções de Tarefas.
- Incluído suporte para plataforma SUSE Linux Enterprise Server 15.

Monitoring Agent for Internet Services

Monitoramento de Serviço da Internet Agora o agente suporta plataformas Windows de 64 bits e Linux de 64 bits.

Monitoring Agent for Microsoft .NET

O agente .NET foi aprimorado com os recursos a seguir:

- O agente .NET agora rastreia as solicitações com falha. O status dessas solicitações é mostrado como `failed` no widget de grupo Solicitações Mais Recentes da página Detalhes da Transação de Middleware. Além disso, o widget do grupo Erros Mais Recentes lista as solicitações recentes com falha juntamente com o código de status e a descrição do erro.
- O agente .NET também monitora os dados do usuário disponíveis por meio das sessões Identidade do ASP.NET e ASP.NET. Os dados do usuário são exibidos no widget de grupo 5 Principais Usuários da página Detalhes da Transação de Middleware.

Monitoring Agent for MongoDB

Agora o Agente MongoDB suporta a plataforma SUSE Linux Enterprise Server 15.

Monitoring Agent for NetApp Storage

O agente NetApp Storage é aprimorado com os recursos a seguir:

- Uma nova caixa de Procura foi incluída na página Detalhes do evento que filtra os dados do evento com base nos critérios de procura.
- Uma nova página de Detalhes foi incluída para LUNs.
- O usuário agora está apto a verificar os detalhes do plano relacionado mapeado para cada objeto de armazenamento na página **Detalhes**.

Monitoring Agent for OpenStack

Foi incluído suporte para monitorar instâncias da máquina virtual, como o uso da CPU da instância da máquina virtual, memória, disco e controlador de interface de rede.

Monitoring Agent for PostgreSQL

- Incluído suporte para SUSE Linux Enterprise Server 15
- Coleção de dados otimizada para grupos de atributos CPU e Memória

Monitoring Agent for RabbitMQ

Incluído suporte para SUSE Linux Enterprise Server 15

Monitoring Agent for SAP Applications

O Agente SAP agora suporta as seguintes plataformas:

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

Monitoring Agent for Skype for Business Server

O Skype for Business Server foi aprimorado com os recursos a seguir:

- Os Comandos de Transação Sintética no Módulo de Transação Sintética agora são executáveis por Usuários de Teste já configurados. Para usar esse recurso, desative o painel de configuração `Usar valores de configuração do agente` no Agent e forneça o valor de `FQDN do conjunto` para o qual os Comandos Sintéticos devem ser executados. Certifique-se de que o Usuário de Teste esteja configurado por meio do comando NewCsHealthMonitoringConfiguration para a Identidade fornecida no campo FQDN do Conjunto do Painel Configuração do Agente.
- Os usuários agora podem desativar os Comandos Sintéticos. Para desativar qualquer comando específico da execução, forneça `false` com relação a esse nome de comando no arquivo `LyncSyntheticTrans.exe.config` presente no local `<CANDLE_HOME>\tmaitm6` para a versão de 32 bits e em `<CANDLE_HOME>\TMAITM6_x64` para a versão de 64 bits.

Monitoring Agent for Tomcat

- O novo grupo de atributos Cluster foi incluído. Ele contém informações de propriedades de um cluster.
- Um novo widget Informações do cluster foi incluído. Este widget exibe informações do grupo de atributos Cluster. Ele não exibirá nenhum dado se o agente estiver monitorando uma configuração do Tomcat sem cluster.

- A variável do painel de configuração *Tomcat Server Port* foi incluída. Essa variável representa a porta na qual o servidor Tomcat está em execução. O valor padrão da variável é 8080.

Monitoring Agent for VMware VI

- A página do componente foi aprimorada para mostrar o Endereço IP ou o Nome do Host do vCenter configurado e sua conectividade com o agente.

Agente WebSphere Infrastructure Manager
Agora o WebSphere Infrastructure Manager suporta AIX.

Agente do WebSphere MQ
Agora o agente WebSphere MQ é suportado no IBM WebSphere MQ 9.1.

Aprimoramentos do Coletor de Dados

Coletor de dados J2SE
O Coletor de dados J2SE foi aprimorado com os seguintes recursos:

- Incluído suporte para SUSE Linux Enterprise Server 11 for Power Linux Big Endian (64 bits).
- Incluído suporte para Power Linux Big Endian (pLinux BE) (64 bits).
- Incluído suporte para Power Linux Little Endian (pLinux LE) (64 bits).
- Incluído módulo de configuração e monitoramento do servidor Jetty.

Expandido suporte da plataforma para agentes
Os agentes e plataformas a seguir são agora suportados:

Plataforma SUSE Linux Enterprise Server 15

- Agente Cassandra
- DataPower agent
- DataStage agent
- Db2
- Servidor HTTP
- IBM Integration Bus agent
- agente do S.O. Linux
- Agente MongoDB
- OpenStack agent
- Agente PostgreSQL
- Monitoring Agent for RabbitMQ
- Agente SAP
- WebSphere MQ agent

Power Linux

- Coletor de dados J2SE

Ubuntu 18.04

- Agente Cassandra
- IBM Integration Bus agent
- OpenStack agent
- agente do S.O. Linux
- Agente RabbitMQ
- WebSphere MQ agent

Suporte ao Power 9
Agora o suporte ao Power 9 está incluído para todos os agentes.

O que há de novo para a atualização de outubro de 2018 da V8.1.4

Integração com o Gerenciamento de eventos de nuvem

O Gerenciamento de eventos de nuvem fornece o gerenciamento de incidente em tempo real em seus serviços, aplicativos e infraestrutura. Agora, com a integração entre o Gerenciamento de eventos de nuvem e o IBM Cloud Application Performance Management, todos os eventos que são gerados no Cloud APM são enviados para o Gerenciamento de eventos de nuvem.

Setembro de 2018

Novo agente disponível

Monitoring Agent for MQ Appliance

O agente do MQ Appliance fornece informações de monitoramento que são específicas para o nível do dispositivo do MQ em Dispositivos do MQ, por exemplo, informações de resumo de CPU, memória, armazenamento, sensores e gerenciadores de filas.

Aprimoramentos do agente

Monitoring Agent for Db2

Agora o agente Db2 suporta sistema operacional Power Linux Big Endian.

Monitoring Agent for Hadoop

- O agente Hadoop agora monitora o status de mais dois serviços: SmartSense e Druid.
- O agente Hadoop agora suporta o Hortonworks Data Platform (HDP) 3.0.0.

agente de Monitoramento de Serviço da InternetAgente

A funcionalidade editar para o agente agente de Monitoramento de Serviço da Internet foi aprimorada. Todos os monitores que possuem parâmetros configuráveis podem ser editados.

Monitoring Agent for MySQL

O agente MySQL agora suporta o monitoramento do MySQL v8.0.11.

Monitoring Agent for NetApp Storage

O agente NetApp Storage é aprimorado com os recursos a seguir:

- Um novo widget chamado Resumo de Eventos Gerais é incluído na página Instância de Armazenamento do NetApp. Ele exibe a contagem acumulativa de eventos. É possível visualizar todos os eventos que ocorreram em todo o ambiente, independentemente de gravidade ou do objeto, clicando na barra de status representada como Total de Eventos.

  Além disso, uma coluna Status do Evento é incluída em cada tabela de objetos, que mostra o status do evento priorizado com base no tempo e, em seguida, no nível de severidade.

  A página Instância de Armazenamento do NetApp agora exibe a tabela Resumo de Eventos em vez de um gráfico.
- A página Detalhes do Agregado é atualizada para exibir os dispositivos relacionados que estão associados ao agregado selecionado.

Monitoring Agent for SAP Applications

Incluído suporte para o SAP NW RFC SDK 750.

Monitoring Agent for SAP HANA Database

Dois novos recursos são incluídos:

- O SAP HANA Database pode ser monitorado no modo de espera.
- O SAP HANA Database agent suporta a plataforma Big Endian para Power System.

Monitoring Agent for VMware VI

- O monitoramento de **`HostVFlashManager`** agora é suportado
- O Painel do Servidor ESX agora mostra a contagem de máquinas virtuais que estão em seus status Crítico, Aviso e Normal com relação à utilização da CPU.

Nova plataforma: Linux on POWER Big Endian

Há uma nova plataforma disponível. Os agentes a seguir são agora suportados no Linux on POWER Big Endian:

- Db2
- IBM Integration Bus agent
- agente do S.O. Linux
- SAP HANA Database agent
- WebSphere MQ agent
- WebSphere Applications agent

julho de 2018

Novos agentes disponíveis

Monitoring Agent for Sybase Server

O Sybase agent oferece um ponto central de gerenciamento para bancos de dados distribuídos. Ela coleta as informações necessárias para administradores de bancos de dados e de sistemas examinarem o desempenho do sistema do servidor Sybase, detectar problemas antecipadamente e evitá-los.

Aprimoramentos do agente

Monitoring Agent for Hadoop

- Incluído suporte para o monitoramento de serviços Hadoop, como, Mahout, Atlas e Falcon.
- Incluído suporte para o monitoramento da oferta Hadoop: Cloudera CDH 5.13.
- Incluído suporte para o monitoramento da oferta Hadoop: Hortonworks HDP 2.6.4.

Monitoring Agent for HMC Base

O HMC V8 R8.7.0 agora é suportado.

Monitoring Agent for HTTP Server

O suporte para o Servidor HTTP Apache de 64 bits no Windows foi incluído.

Monitoring Agent for Microsoft .NET

O Monitoring Agent for Microsoft .NET foi aprimorado, conforme a seguir:

- Agora o módulo de Tempo de Resposta do IIS monitora a subtransação e o detalhamento do tempo de renderização através de injeção de JavaScript para formulários da web ASP.NET (páginas .aspx) e visualizações detalhadas MVC do ASP.NET, que satisfazem às seguintes condições:
  - A página atende às normas HTML do W3C.
  - Os cabeçalhos de resposta contêm `Content-Type: text/html, application/xml,application/json`.
  - O conteúdo de resposta inclui o elemento *<head>* .
- O agente .NET faz upload dos dados de detalhamento para o serviço Diagnostic Query Engine (DQE) no servidor APM. O painel de detalhamento do serviço DQE carrega e exibe rapidamente os dados.
- O novo limite **`NET_Slow_IIS_Request_Crit`** foi incluído que é acionado quando o widget Slow Top 10 tem solicitações com tempo de resposta maior que 500 milissegundos.
- A ferramenta de filtragem seletiva foi atualizada com a caixa de procura para procurar por um conjunto de aplicativos a partir da lista de conjuntos de aplicativos.
- O utilitário **`ProcListCaller`** foi incluído para fornecer a lista de processos que carregaram o gerenciador de perfis do .NET Agent CLR (`CorProfLog.dll`).

Monitoring Agent for Microsoft SQL Server

- O Microsoft SQL Server agent agora suporta múltiplas ordenações na análise sintática ERR0RL0G com base nas configurações de ordenação no arquivo koqErrConfig.ini. Quando o arquivo koqErrConfig.ini não contém nenhuma configuração de ordenação válida, é possível ver apenas a mensagem de erro padrão em inglês com nível de severidade mais alto que o nível de severidade padrão, se houver. O nível de severidade padrão é 17. Todas as ordenações existentes no arquivo koqErrConfig.ini serão consideradas ao analisar o arquivo ERR0RL0G. Portanto, somente as ordenações que estão em uso devem ser incluídas no arquivo koqErrConfig.ini. Como a análise sintática ERR0RL0G faz distinção entre maiúsculas e minúsculas, assegure-se de que os valores da palavra-chave de ordenação no arquivo koqErrConfig.ini sejam exatamente iguais aos valores de palavra-chave localizados no arquivo ERR0RL0G ou no arquivo koqErrConfigSample.ini de referência. Observe que as mudanças feitas no arquivo koqErrConfig.ini não são preservadas durante o upgrade do agente, portanto, deve-se fazer um backup antes do upgrade do agente.
- O agente também fornece a ferramenta do utilitário **koqVerifyPermissions.exe** para verificar se um usuário do SQL Server existente tem permissões suficientes para monitorar o Microsoft SQL Server. Se um usuário do SQL Server existente não tiver permissões suficientes, é possível usar a ferramenta de utilitário **permissions.cmd** como uma alternativa para conceder as permissões mínimas a um usuário do SQL Server existente para a coleta de dados.

Monitoring Agent for NetApp Storage

O Monitoring Agent for NetApp Storage foi aprimorado, conforme a seguir:

- A nova página Componente é incluída para exibir os detalhes do estado de conexão do agente, independentemente se o provedor de dados estar ativo ou inativo, juntamente com o endereço IP das origens de dados monitoradas. A barra de status individual representa o número de nós, agregações, volumes e discos que estão em estado crítico, normal, de aviso ou desconhecido.
- A nova página Instância de Armazenamento do NetApp foi incluída para destacar as propriedades-chave de clusters, agregações, volumes, discos e vServers. Ela também exibe o gráfico Resumo de eventos com a contagem de eventos que ocorreram em cada entidade de armazenamento ou objeto disponível no ambiente. Por exemplo, se houver 12 volumes configurados e cada volume tiver dois eventos com severidade Crítica, o gráfico Resumo do evento descreverá a contagem total de eventos que ocorreram em todos os volumes disponíveis em um ambiente. Nesse caso, o gráfico mostra uma barra com 24 eventos críticos com relação ao volume como uma entidade plotada no eixo X.
- A página de Detalhes do Nó foi atualizada para mostrar os detalhes de porta de rede.
- A página de Detalhes do Volume foi atualizada para exibir detalhes dos espelhos de snap associados e a contagem de LUNs para cada volume selecionado.
- A página de Detalhes de vServers foi atualizada para exibir informações sobre as interfaces lógicas de rede.

Monitoring Agent for Tomcat

O servidor Tomcat V9.0.5 agora é suportado.

Monitoring Agent for WebSphere MQ

O monitoramento remoto é suportado. Dois parâmetros de configuração são incluídos para o agente para que seja possível coletar dados de monitoramento para um gerenciador de filas remotas. No entanto, esses parâmetros de configuração não têm nenhum efeito em um gerenciador de filas locais. Se você deseja configurar o agente para monitorar um gerenciador de filas locais, é possível pressionar Enter para ignorar a especificação desses parâmetros.

Para obter mais informações sobre a configuração do agente, consulte "Configurando o WebSphere MQ agent" na página 935.

Aprimoramento de customização do slot EIF

Agora é possível incluir múltiplos valores de atributos e valores literais no slot do EIF. Por exemplo, em vez de uma mensagem `A porcentagem livre de disco é` **Disk_Free_Percent** para um

limite que testa um espaço em disco baixo disponível, é possível ter `A porcentagem livre de disco é` **`Disk_Free_Percent`** `e a porcentagem livre de inodes é` **`Inodes_Free_Percent`**. A mensagem encaminhada pode ser semelhante a esta: `A porcentagem livre de disco é 13 e a porcentagem livre de inodes é 9`. Para obter mais informações, consulte "Customizando um evento para encaminhar para um receptor EIF" na página 990.

Abril de 2018

Novo agente disponível

Monitoring Agent for AWS Elastic Load Balancer

O Agente Amazon ELB fornece um ponto central de monitoramento para o funcionamento, disponibilidade e desempenho de Balanceadores de Carga Elásticos AWS. O agente exibe um conjunto abrangente de métricas para cada aplicativo de tipo de balanceador de carga, de rede e clássico - para ajudá-lo a tomar decisões informadas sobre o ambiente do Balanceador de Carga Elástico AWS.

Aprimoramentos do agente

Response Time Monitoring Agent

Agora o Módulo de Tempo de Resposta do IBM HTTP Server suporta IBM HTTP Server versões 7, 8 e 9 no Windows.

Monitoring Agent for Node.js

Por padrão, as informações confidenciais do usuário, como cookies, contextos de solicitação de HTTP e contextos de solicitação do banco de dados não são mais coletadas pelo Coletor de dados Node.js. É possível mudar este comportamento padrão especificando a nova variável de ambiente, *SECURITY_OFF*.

Monitoring Agent for Amazon EC2

O nome do componente agora reflete o nome do agente.

Foi incluído o suporte de retenção de dados estendido.

Monitoring Agent for WebLogic

O rastreamento de transação e o diagnósticos detalhado são ativados no AIX. Anteriormente, esses recursos só eram ativados no Linux e Windows.

Foi aprimorado o drill down Resumo de solicitação para servlets que são implementados com anotações para diagnósticos de rastreamento de transação e de detalhamento.

Monitoring Agent for Skype for Business Server

Suporte para Windows Server 2016.

Monitoring Agent for Sterling File Gateway

O agente busca eventos para transferência de arquivos com falha como um comportamento padrão. É possível mudar este comportamento padrão especificando o valor apropriado para a nova variável de ambiente **KFG_ALL_FGEVENTS**.

Monitoring Agent for Sterling Connect Direct

O recurso de criação de log do agente foi melhorado. Para obter informações adicionais, consulte a seção Resolução de problemas.

Aprimoramentos do Coletor de Dados

Coletor de dados Node.js

Por padrão, as informações confidenciais do usuário, como cookies, contextos de solicitação de HTTP e contextos de solicitação de banco de dados não são mais coletadas pelo Coletor de dados Node.js. É possível mudar este comportamento padrão especificando a nova variável de ambiente, *SECURITY_OFF*.

Lembre-se: Para obter esse aprimoramento, você deve fazer download e aplicar a correção temporária 1 do IBM Cloud Application Performance Management Coletor de dados Node.js a partir do IBM Fix Central. Para obter mais informações, consulte Arquivo Leia-me da Correção Temporária 1.

Coletor de dados J2SE
O suporte foi incluído para autodescoberta da classe de ponto de entrada (classe principal) e nome do alias do aplicativo J2SE.

Os diagnósticos de rastreamento de transação e de detalhamento podem ser ativados e desativados localmente usando scripts de configuração.

Aprimoramentos da Documentação
Uma página da web é criada no Centro do Desenvolvedor de Gerenciamento de Desempenho do Aplicativo para ajudá-lo a encontrar o nível de agente em cada atualização ou liberação. Para obter mais informações, consulte a Versão do agente em liberações do Cloud APM.

O agente e os recursos do coletor de dados em cada tabela de oferta são simplificados para melhorar a capacidade de leitura. Para obter mais informações, consulte “Capacidades” na página 52.

Fevereiro de 2018

Novo agente disponível

Monitoring Agent for Azure Compute

O Agente Azure Compute fornece um ponto central para monitoramento do funcionamento, disponibilidade e desempenho de suas instâncias do Azure Compute. O agente exibe um conjunto abrangente de métricas para ajudá-lo a tomar decisões informadas sobre o ambiente do Azure Compute. Essas métricas incluem o uso da CPU, uso da rede e desempenho do disco.

Monitoring Agent for Sterling Connect Direct

É possível usar o Agente Sterling Connect Direct para monitorar o funcionamento e o desempenho do servidor Sterling Connect Direct. Ele monitora os recursos do servidor Sterling Connect Direct, como atividades de transferência de arquivos, processos planejados, processos de filas de suspensão e de espera. O agente suporta o monitoramento remoto e é multi-instância.

Monitoring Agent for Sterling File Gateway

O Agente Sterling File Gateway monitora o aplicativo Sterling File Gateway, que é usado para transferir arquivos entre parceiros internos e externos usando diferentes protocolos, diferentes convenções de nomenclatura de arquivo e diferentes formatos de arquivo. Ele também suporta o recurso de monitoramento remoto.

Aprimoramentos do agente

Monitoring Agent for DataPower
O rastreamento de transação entre o WebSphere MQ agent e o DataPower agent é suportado.

Monitoring Agent for Db2
O suporte foi incluído para monitoramento remoto.

Monitoring Agent for Hadoop
Foi incluído suporte para monitorar o status de serviços Hadoop, como HBase, MapReduce2, Tez e Ranger.

Foi incluído suporte para monitorar a oferta Hadoop: Cloudera CDH 5.12.

Monitoring Agent for InfoSphere DataStage
Foi incluído suporte para MS SQL como repositório de metadados.

Foi incluído suporte para o sistema operacional Windows.

Monitoring Agent for Tomcat
Rastreamento de transação e suporte de detalhamento para PLinux fazendo upgrade da estrutura do agente com a correção 8.1.4.0-IBM-APM-SERVER-IF0001.

Monitoring Agent for SAP Applications
Aprimoramento do recurso CCMS: automação de exclusão de arquivo `idx`. Essa automação funciona apenas quando o sistema SAP é reiniciado.

Monitoring Agent for Microsoft .NET
Foi incluído suporte para transações do usuário final usando o módulo Tempo de Resposta do IIS.

Monitoring Agent for Skype for Business Server
O nome do agente mudou de Monitoring Agent for Microsoft Lync Server para Monitoring Agent for Skype for Business Server.

Monitoring Agent for Linux KVM
Foi incluído suporte para RHEV-M 4.x.

Monitoring Agent for Linux OS
O intervalo de upload de memória mudou para 1 minuto.

O endereço IP associado à interface de rede é exibido no painel do Linux OS e no widget Informações do Sistema.

Monitoring Agent for UNIX OS
O intervalo de upload de memória mudou para 1 minuto.

Aprimoramentos do Coletor de Dados

Coletor de dados J2SE
Foi incluído suporte para o Spring Boot Applications.

Monitoramento de Disponibilidade Aprimoramentos do
Com o complemento do Monitoramento de Disponibilidade, agora é possível criar listas de desbloqueio e listas de bloqueio para especificar URLs que seus testes podem e não podem acessar. Sua lista de desbloqueio e a lista de bloqueio controlam quais dependências e recursos contribuem com os tempos de resposta do aplicativos da web testados, como métricas de terceiros. Filtre URLs por esquema, domínio ou tipo de arquivo usando caracteres curinga.

Dezembro de 2017

Novo agente disponível

Monitoring Agent for InfoSphere DataStage

É possível usar o DataStage agent para monitorar o funcionamento e o desempenho de recursos do servidor DataStage, como serviços de mecanismo, sistemas de mecanismo, atividade da tarefa, status de execução da tarefa e detalhes de execuções da tarefa. Esse agente suporta monitoramento remoto.

Aprimoramentos do agente

Monitoring Agent for Hadoop

Foi incluído suporte para monitorar um cluster Hadoop que é protegido com a autenticação baseada em Kerberos SPNEGO, que usa o Centro de Distribuição de Chaves (KDC) do Active Directory.

Foi incluído suporte para testar a conexão com hosts de um cluster Hadoop que é protegido com autenticação baseada no Kerberos SPENGO, que usa o MIT ou o Active Directory como o Centro de Distribuição de Chaves (KDC).

Foi incluído suporte para monitorar as seguintes ofertas Hadoop: Cloudera CDH 5.10 e CDH 5.11.

Foi incluído suporte para monitorar o status de serviços Hadoop, como Flume, Kafka, Titan, Spark, Knox, Pig, Slider e Solr.

Monitoring Agent for HTTP Server
O suporte para o Windows de 32 bits IBM HTTP Server e o Servidor HTTP Apache foi incluído.

O suporte para o Linux for System z foi incluído (o rastreamento de transação não é suportado).

Foi incluído suporte para o servidor HTTP Oracle no Linux for System x.

Monitoring Agent for IBM Integration Bus
O suporte para Linux for Power Systems (Little Endian) foi incluído.

Monitoring Agent for Microsoft .NET
Foi incluído suporte de monitoramento para ODP.NET.

Detalhes de rastreio de método foram incluídos para o método HttpWebRequest.GetResponse().

Monitoring Agent for Microsoft SQL Server

Foi incluído suporte de tolerância para SQL Server 2017.

Foi incluído suporte para o recurso Always On para a edição de desenvolvedores do SQL Server.

Monitoring Agent for MySQL

Foi incluído suporte de tolerância para as tabelas de esquema de informações que estão sendo migradas para o esquema de desempenho.

Foi incluído suporte para tabelas descontinuadas de esquema de informações por meio do esquema de desempenho.

Monitoring Agent for Microsoft Internet Information Services

Foi incluído suporte para monitoramento de websites de FTP.

Monitoring Agent for MongoDB

O suporte foi incluído para monitoramento remoto.

Foi incluído suporte para monitoramento do mecanismo de armazenamento de memória.

Monitoring Agent for OpenStack

Foi incluído suporte para a API de autenticação do OpenStack V3.

Monitoring Agent for Oracle Database

A versão do agente mudou para 8.0.

O parâmetro de configuração **Oracle JDBC jar file** foi incluído e os parâmetros de configuração **Oracle Home Directory** e **Oracle Instant Client Installation Directory** foram removidos.

Monitoring Agent for PostgreSQL

O suporte foi incluído para monitoramento remoto.

Monitoring Agent for SAP Applications

Foi incluído suporte para comunicação SNC.

O novo limite para o sistema SAP foi incluído.

Monitoring Agent for SAP NetWeaver Java Stack

Foi incluído o recurso para restaurar a instância do SAP NetWeaver Application Server.

Monitoring Agent for Tomcat

Foi incluído suporte para o Linux for Power Systems (Little Endian) (Apenas monitoramento de recursos).

Monitoring Agent for VMware VI

Foram incluídos Resumo de rede e Contagem de discos na página de visão geral do ESX Server.

Foi incluído o widget de grupo de eventos na página de resumo de Cluster.

Monitoring Agent for WebSphere Applications

Foi incluído suporte de rastreamento de transação para o Linux for Power Systems (Little Endian) e o Linux for System z.

Lembre-se: Para obter suporte de rastreamento de transação no Linux for Power Systems (Little Endian) e no Linux for System z, conclua as seguintes etapas:

1. Faça download da imagem de instalação do agente.
2. Instale o WebSphere Applications agent.
3. Faça download da correção temporária 2 do WebSphere Applications agent do Fix Central.
4. Siga o arquivo leia-me da correção temporária para aplicar a correção.

Monitoring Agent for WebSphere MQ

Foi incluído o widget de grupo Status de Serviço do MQ para fornecer os detalhes do serviço do MQ.

O suporte para Linux for Power Systems (Little Endian) foi incluído.

Aprimoramentos do Coletor de Dados

Coletor de dados Liberty

O nome do sistema gerenciado (MSN) registrado pelo Coletor de dados Liberty mudou para refletir o nome do host e o nome do servidor Liberty. O novo MSN para este coletor de dados é BI:*servername_hostname_md5*:BLP, em que *md5* é o GUID do aplicativo local baseado no MD5. O comprimento de *servername_hostname_md5* é 25 caracteres.

Lembre-se: Para obter esse aprimoramento, você deve fazer download e aplicar a Correção Temporária 1 do coletor de dados do IBM Cloud Application Performance Management Liberty do Fix Central.

Coletor de dados J2SE

Foi incluído suporte de rastreamento de transação para aplicativos J2SE.

Aprimoramentos da Documentação

As informações sobre portas padrão que são usadas por agentes e coletores de dados são fornecidas para facilitar a preparação do ambiente. Consulte "Portas padrão usadas pelos agentes e coletores de dados" na página 81.

São fornecidas informações sobre nomes de sistemas gerenciados (MSNs) de agentes do Cloud APM. Também são fornecidas instruções sobre como mudar a sequência de nomes do host no MSN. Consulte "Nomes de Sistemas Gerenciados" na página 165.

As informações sobre como executar o agente como um usuário não administrador ou as permissões que são necessárias para executar o agente por um usuário não administrador são fornecidas nos tópicos de configuração para os seguintes agentes:

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

Agosto de 2017

IBM Cloud Application Performance Management, Availability Monitoring

O complemento do Monitoramento de Disponibilidade fornece monitoramento sintético aprimorado de seus aplicativos da web a partir de vários pontos de presença ao redor do mundo. Crie testes sintéticos que imitam o comportamento do usuário em intervalos regulares. Execute seus testes a partir de pontos de presença públicos ou faça download e implemente seus próprios pontos de presença customizados em servidores locais ou privados. Use o painel do Monitoramento de Disponibilidade para monitorar a disponibilidade, o desempenho e os alertas do aplicativo usando gráficos, tabelas de detalhamento e visualizações de mapa. Use a análise em cascata para identificar quando ocorrem problemas de desempenho e disponibilidade e encontrar razões para esses problemas.

Monitoramento do IBM API Connect

Os agentes e coletores de dados do Cloud APM agora suportam o monitoramento do ambiente do IBM API Connect. É possível implementar os agentes e coletores de dados correspondentes para obter visibilidade do funcionamento e desempenho dos componentes em seu ambiente. Os dados de rastreamento de transação também estão disponíveis, além dos dados de monitoramento de recursos e de diagnósticos de detalhamento, o que permite visualizar informações de topologia sobre o ambiente do IBM API Connect. Para obter mais informações, consulte "Cenário: monitorando o IBM API Connect" na página 86.

Suporte ao S.O.

Linux for System z
Incluído suporte do Linux for System z para os seguintes agentes de monitoramento: Linux OS, WebSphere Application, Db2, WebSphere MQ, IBM Integration Bus, Tomcat e Monitoramento de Tempo de Resposta.

Linux for Power Systems (Little Endian)
Incluído suporte do Linux for Power Systems (Little Endian) para os seguintes agentes de monitoramento: Linux OS, WebSphere Application e Db2.

Linux for System x
Incluído Linux on System x para suportar o coletor de dados Liberty.

Suporte do agente de S.O. IBM i
Os dados para o agente de S.O. IBM i agora podem ser exibidos no Console do Cloud APM. Esse agente é um agente do IBM Tivoli Monitoring V6 e permanece como um agente V6 para a liberação da V8.1.4. É possível usar o Hybrid Gateway para recuperar os dados do agente e enviá-los para o Servidor Cloud APM. Como resultado, é possível visualizar dados e eventos de monitoramento para este agente no Console do Cloud APM. Para obter informações adicionais sobre o agente de S.O. IBM i, consulte o Agentes suportados pelo Hybrid Gateway (APM Developer Center).

Novos agentes disponíveis

Monitoring Agent for OpenStack

É possível usar o OpenStack agent para monitorar o funcionamento e desempenho de seus aplicativos OpenStack e visualizar informações, como informações sobre terminais da API, conexão do servidor SSH, processos e hypervisors.

Coletores de dados novos e aprimorados disponíveis
É possível usar os coletores de dados para monitorar o funcionamento e o desempenho dos seguintes aplicativos no IBM Cloud e/ou no local:

Coletor de dados J2SE
É possível usar o Coletor de dados J2SE para monitorar o funcionamento e desempenho de aplicativos Java e visualizar dados diagnósticos, como tempo de resposta, rendimento, contexto de solicitação e rastreio de método de solicitações.

Coletor de dados Liberty
O Coletor de dados Liberty monitora o perfil Liberty no ambiente do IBM Cloud e o perfil Liberty local no Linux for System x.

Coletor de dados Node.js
O Coletor de dados Node.js monitora os aplicativos IBM Cloud e no local. É possível visualizar dados de monitoramento de recursos e diagnósticos, como utilização de recurso, rendimento e informações detalhadas sobre solicitações e métodos.

Coletor de dados do Python
O Coletor de dados do Python monitora aplicativos IBM Cloud. É possível visualizar dados de monitoramento de recursos e diagnósticos, como utilização de recurso, rendimento e informações detalhadas sobre solicitações e métodos.

O Agente Python foi removido do pacote de instalação do agente no Cloud APM V8.1.4. É possível usar o Coletor de dados do Python para monitorar somente seus aplicativos Python.

Coletor de dados Ruby
O Coletor de dados Ruby monitora apenas os aplicativos IBM Cloud. É possível visualizar dados de monitoramento de recursos e diagnósticos, como utilização de recurso, rendimento e informações detalhadas sobre solicitações e métodos.

Aprimoramentos do agente

Monitoring Agent for Amazon EC2

- O agente pode manipular datas de encerramento nulas para eventos planejados corretamente.
- Foi incluído suporte para um proxy de encaminhamento entre o agente Amazon EC2 e o Amazon Web Services.

Monitoring Agent for Citrix Virtual Desktop Infrastructure

- Foi incluído monitoramento de eventos do Windows e métricas PowerShell mesmo quando o agente está instalado em um sistema Linux.
- Foi incluída a página **Sessões de VDA**, que é acessível através da página **Detalhes da máquina VDA**.
- O widget Métricas da Máquina foi incluído na página **Detalhes da máquina VDA**.
- A configuração do Desktop Delivery Controller (DDC) foi aprimorada para permitir que o agente manipule o failover de DDC em um ambiente distribuído.

Monitoring Agent for Db2

- O suporte para Linux for System z foi incluído.

Monitoring Agent for Hadoop

- Foi incluído o suporte para monitorar as seguintes ofertas de Hadoop: Hortonworks HDP 2.6 e Cloudera CDH 5.9, 5.10 e 5.11
- Foi incluído o suporte para monitorar o status de serviços Hadoop, como ZooKeeper, Sqoop, Hive, HDFS, YARN, Ambari Metrics e Oozie.
- Foi incluído suporte para monitorar um cluster Hadoop que é protegido com a autenticação baseada em Kerberos SPNEGO, que usa somente o MIT Kerberos V5 Key Distribution Center (KDC).

Monitoring Agent for IBM Integration Bus

Foi incluído suporte para o Linux for System z (O rastreamento de transação não é suportado).

Monitoring Agent for JBoss

- O processo de configuração de rastreamento de transação e de diagnósticos de detalhamento foi simplificado para o agente JBoss na oferta Agentes Avançados.
- Dois widgets do painel foram incluídos na página **Detalhes da coleta de lixo**. Um widget mostra a quantidade de memória heap que foi liberada desde a última coleta de lixo e o outro widget mostra o histórico dos tamanhos do conjunto de memórias heap Eden/Survivor/Tenured (Geração antiga).

Monitoring Agent for Linux OS

Foi incluído suporte para Linux for Power Systems (Little Endian).

Monitoring Agent for Skype for Business Server

- O widget de grupo Resumo de uso do Lync foi incluído no painel Visão geral do Lync Server para visualizar o status de registro front-end e a qualidade de chamadas insatisfatórias.
- Foi incluído um painel para exibir os detalhes de uso do Microsoft Lync Server.

Monitoring Agent for SAP NetWeaver Java Stack

Os seguintes aprimoramentos foram incluídos no painel do SAP NetWeaver Java Stack:

- Foram incluídos conjuntos de dados, widgets de grupo e páginas para coletar e visualizar os dados de rastreamento de transação e diagnósticos.
- Foi incluído suporte para instalar e configurar o agente nos sistemas Windows 2016.
- O widget de grupo 5 Principais solicitações mais lentas por tempo de resposta foi incluído no painel Instância de Java do SAP NW para fornecer informações sobre as 5 principais solicitações feitas pelo usuário para o aplicativo com o tempo de resposta alto.
- As informações de diagnóstico sobre as solicitações que são exibidas no widget de grupo 5 solicitações mais lentas por tempo de resposta podem ser vistas na página Instâncias de solicitação clicando na Solicitação. Foi incluído suporte para exibir as informações de diagnóstico sobre as solicitações no widget de grupo 5 solicitações mais lentas por tempo de resposta.

- O widget de grupo 5 principais sessões do usuário por tempo de resposta foi removido.

Monitoring Agent for MongoDB

Foi incluído o suporte para monitorar o cluster MongoDB ou a configuração de replicação quando o nó primário falha.

Monitoring Agent for MySQL

Foram incluídos conjuntos de dados e um parâmetro de configuração para monitorar remotamente os recursos do MySQL.

Monitoring Agent for NetApp Storage

- A página Componente foi atualizada para exibir as informações resumidas de clusters e Vservers.
- A página Instância de Armazenamento do NetApp foi atualizada para exibir informações sobre clusters.

Monitoring Agent for Node.js

Os seguintes aprimoramentos foram incluídos no Agente Node.js para alavancar Métricas de aplicativo do nó (Appmetrics):

- Novo painel e widgets de grupo para visualizar detalhes da coleta de lixo
- Novo painel e widgets de grupo para visualizar detalhes do loop de eventos

Monitoring Agent for PostgreSQL

- Suporte para instalar e configurar o agente nos sistemas Windows.
- Suporte para monitorar o PostgreSQL V9.6.
- A página **Visão geral de status** foi atualizada, portanto, o status não é crítico quando a taxa de ocorrência do buffer é zero.

Monitoring Agent for SAP HANA Database

O atributo Dias de Expiração da Licença e os limites HANA_License_Expiry_Crit_SYS e HANA_License_Expiry_Warn_SYS foram incluídos para monitorar o número de dias que restam antes da expiração da licença.

Monitoring Agent for Tomcat

- Foi incluído suporte para o Linux for System z
- Foram incluídos conjuntos de dados, painéis e widgets de grupo para rastreamento de transação e diagnósticos de detalhamento.

Monitoring Agent for VMware VI

O widget de grupo do Servidor ESX no painel Resumo do Servidor foi atualizado para mostrar o status do SSH.

Monitoring Agent for WebLogic

O rastreamento de transação e os diagnósticos de detalhamento foram incluídos no agente na oferta Agentes Avançados.

Monitoring Agent for WebSphere Applications

O suporte para o Linux for System z foi incluído (o rastreamento de transação não é suportado).

Monitoring Agent for WebSphere MQ

O suporte para o Linux for System z foi incluído (o rastreamento de transação não é suportado).

Os dados do histórico de longo prazo de canal e de fila são suportados. Após o gerenciador de filas ter sido configurado para coletar dados estatísticos de canal ou de fila, é possível configurar o agente para permitir a coleta de dados do histórico de longo prazo de canal ou de fila. Embora não haja painéis ou widgets predefinidos para exibir os dados do histórico de longo prazo coletados, é

possível usar a guia **Detalhes do atributo** para consultar os dados coletados em suas tabelas customizadas.

Response Time Monitoring Agent

- Foi incluído suporte para o Windows de 32 bits IBM HTTP Server e o Apache HTTP Server.
- Foi incluído suporte para configurar o rastreamento do usuário para aplicativos na página **Configuração do agente**.
- Foi incluído suporte para configurar o rastreamento de sessão para aplicativos na página **Configuração do agente**.

Visualização aprimorada

Visualizações customizadas

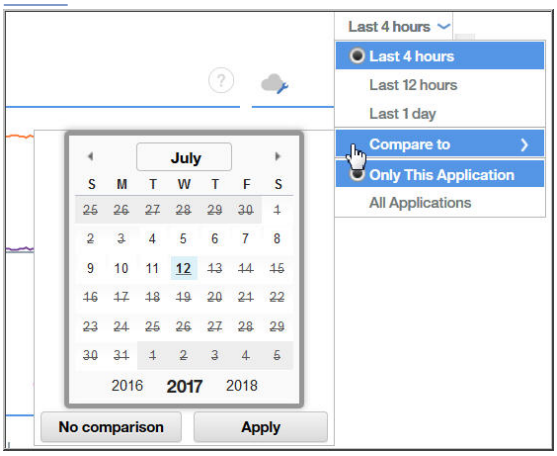
É possível usar o IBM Cloud Application Business Insights Universal View para criar páginas customizadas para os aplicativos que estão sendo monitorados. Na guia Visualizações customizadas, é possível usar um modelo existente ou criar modelos customizados para sua página. É possível escolher entre diferentes opções de gráfico e métrica para criar widgets para monitorar dados, de acordo com seu requisito.

Usando o Universal View, é possível criar painéis para monitorar dados de vários agentes. É possível exportar os dados da página customizada para um arquivo de Dados Brutos.

Para obter informações adicionais, consulte “Visualizações customizadas” na página 1112.

Calendário para comparar dados de um dia anterior

Quando estiver visualizando gráficos de linhas que mostram dados históricos, é aberto um calendário após você escolher a opção de seletor de tempo para comparar o intervalo de tempo de um dia anterior. Os dias que estão indisponíveis para comparação são riscados. Para obter mais informações, consulte “Ajustando e comparando métricas no decorrer do tempo” na página 1091.



Aprimoramentos do Agent Builder

Ao criar um agente para monitorar dados a partir de um banco de dados Java Database Connectivity (JDBC), é possível modificar os valores de enumeração que são configurados para Erro, Dados ausentes e Nenhum valor para evitar a sobreposição com valores legitimados no banco de dados.

É possível configurar o Time Stamping Authority para arquivos JAR na janela **Preferências** do Agent Builder. Se o certificado de assinatura padrão do Time Stamping Authority expirar, ao configurar uma nova autoridade, será possível continuar a verificar arquivos JAR.

Integração Aprimorada

Slots EIF Customizáveis para eventos

Quando tiver o encaminhamento de eventos configurado, será possível customizar a mensagem de slot EIF base e criar slots EIF customizados para eventos enviados para um receptor, como Netcool/OMNIbus. O Editor de Limite em um novo campo **Encaminhar evento EIF?** e um botão **Customização de slot EIF** para customizar como os eventos são mapeados para eventos

encaminhados. Para obter mais informações, consulte "Customizando um evento para encaminhar para um receptor EIF" na página 990.

Vários Hybrid Gateways

Na liberação anterior, era possível instalar o Hybrid Gateway em um único domínio do IBM Tivoli Monitoring, que tem um Tivoli Enterprise Monitoring Server central. Agora é possível instalar um Hybrid Gateway em vários domínios do Tivoli Monitoring. A categoria Hybrid Gateway na página Console do Cloud APM **Configuração Avançada** foi movida para sua própria página **Gerenciador de Gateway Híbrido**. Aqui é possível criar e editar perfis do Hybrid Gateway para monitorar sistemas gerenciados de vários domínios do Tivoli Monitoring, um perfil para cada domínio. Para obter mais informações, consulte "Hybrid Gateway" na página 953.

Escalabilidade Aprimorada

Um aumento no número máximo de caracteres gerenciados que podem ser monitorados no Cloud APM, que é de 4.000 a 10.000 sistemas gerenciados.

Liberações anteriores

Para obter informações sobre novos recursos, capacidades e cobertura em liberações anteriores, consulte os seguintes tópicos *O que há de novo*:

- "O que há de novo: abril de 2017" na página 27
- "O que há de novo: setembro de 2016" na página 34
- O que há de novo: abril de 2016

O que há de novo: abril de 2017

Novos recursos, capacidades e cobertura foram disponibilizados na liberação de abril de 2017 do Cloud APM.

Nova Application Performance Management Developer Center

O APM Developer Center é um local central do qual é possível acessar recursos para os produtos APM: blogs, vídeos, documentação, suporte, eventos, IBM Marketplace e outros recursos. O menu Console do Cloud APM **Ajuda** possui um link conveniente para o Application Performance Management Developer Center.

Renomeação e simplificação de produtos

A marca IBM Performance Management on Cloud foi redefinida para IBM Cloud Application Performance Management. A marca Os nomes de componentes também foram mudados. Por exemplo, Console do Cloud APM e Servidor Cloud APM eram chamados console do Performance Management e servidor Performance Management em liberações anteriores.

As ofertas de IBM Performance Management on Cloud foram consolidadas e renomeadas:

Nome da oferta Outubro de 2016liberação da e anterior	Nome da oferta Março de 2017 e mais recente
Monitoring on Cloud	Cloud APM, Base
Application Performance Management Advanced on Cloud	Cloud APM, Advanced

Algumas extensões de produtos foram consolidadas e renomeadas:

Nome da extensão Outubro de 2016liberação da e anterior	Nome da extensão Março de 2017 e mais recente
Base Extension Pack (Agente do Hadoop)	Base Extension Pack (inclui os novos Agente Cassandra e Microsoft Office 365 agent)

Nome da extensão Outubro de 2016liberação da e anterior	Nome da extensão Março de 2017 e mais recente
Advanced Extension Pack (SAP HANA Database agent e SAP NetWeaver Java Stack)	Pacote de Extensão Avançado (inclui o novo Agente RabbitMQ)

Suporte ao S.O.

Sistemas operacionais Windows 2016

Incluído suporte para sistemas operacionais Windows 2016. Para obter informações adicionais, consulte o Software Product Compatibility Report (SPCR) para todos os agentes: http://ibm.biz/agents-pm-systemreqs

Localize seu sistema operacional na seção Windows do relatório e clique no ícone do componente para obter uma lista de agentes suportados.

Novo pacote de extensão disponível

IBM Cloud Application Performance Management z Systems Extension Pack

O z Systems Extension Pack ativa o suporte para agentes IBM OMEGAMON em sua oferta Cloud APM. Os dados do agente OMEGAMON são enviados para o Servidor Cloud APM pelo Hybrid Gateway. O Hybrid Gateway recupera os dados do agente e eventos do OMEGAMON da infraestrutura do IBM Tivoli Monitoring à qual os agentes OMEGAMON estão conectados. Como resultado, é possível visualizar dados de monitoramento e eventos para seus agentes OMEGAMON no Console do Cloud APM.

O Cloud APM z Systems Extension Pack estará disponível se você tiver qualquer uma das ofertas do Cloud APM.

Para integrar esse pacote de extensão com o Cloud APM, conclua as etapas em "Integrando-se ao OMEGAMON" na página 964.

Novos agentes e coletores de dados disponíveis

Monitoring Agent for Cassandra

É possível usar o Agente Cassandra para monitorar o funcionamento e desempenho dos recursos de cluster do Cassandra, como os nós, keyspaces e famílias de colunas.

Monitoring Agent for Microsoft Office 365

É possível usar o Microsoft Office 365 agent para monitorar o funcionamento e desempenho dos recursos do Office 365, como serviços associados do Office 365, portal do Office 365, usuários da caixa de correio, sites do SharePoint e armazenamento no OneDrive.

Monitoring Agent for NetApp Storage

É possível usar o Agente NetApp Storage para monitorar o funcionamento, disponibilidade e desempenho dos sistemas de armazenamento NetApp usando o NetApp OnCommand Unified Manager (OCUM). O agente de monitoramento executa as seguintes tarefas:

- Identifica objetos do sistema de armazenamento com baixo desempenho
- Executa a descoberta e monitoramento usando o servidor OCUM no ponto focal

Monitoring Agent for RabbitMQ

É possível usar o Agente RabbitMQ para monitorar o funcionamento e desempenho de recursos de cluster do RabbitMQ, como nós, filas e canais do cluster.

Coletores de dados para aplicativos Bluemix

É possível usar os coletores de dados para aplicativos Bluemix para monitorar o funcionamento e o desempenho dos tipos de aplicativos a seguir no Bluemix:

- Aplicativos Liberty
- Aplicativos Node.js

- Aplicativos Python
- Aplicativos Ruby

É possível visualizar dados de monitoramento de recursos e diagnósticos, como utilização de recurso, rendimento e informações detalhadas sobre solicitações e métodos.

Monitoring Agent for Siebel

É possível usar o Agente Siebel para monitorar o funcionamento e desempenho de recursos do Siebel, incluindo estatísticas do Siebel, sessões do usuário, componentes, tarefas, servidor de aplicativos, Siebel Gateway Name Server, uso de CPU e memória do processo e monitoramento de eventos de log.

Aprimoramentos do agente

Monitoring Agent for Amazon EC2

Os seguintes aprimoramentos foram incluídos no Agente Amazon EC2:

- Substituir o ID da instância pelo nome de tag quando um nome de tag estiver disponível
- Permitir que os dados sejam filtrados e agrupados com base no nome de tag

Monitoring Agent for Db2

Foram incluídos os seguintes aprimoramentos no Agente do Hadoop:

- O Linux on Power Little Endian (pLinux LE) é suportado
- Incluído um arquivo de script para conceder privilégios a um usuário do Db2 para visualizar dados para todos os atributos do agente Db2 para uma instância monitorada

Monitoring Agent for Hadoop

Foram incluídos os seguintes aprimoramentos no Agente do Hadoop:

- Incluído suporte para instalar e configurar o agente em sistemas Windows 2016 e AIX 7.2
- Incluído suporte para monitorar as seguintes ofertas Hadoop: Hortonworks HDP 2.5, Cloudera CDH 5.6, 5.7 e 5.8 e IBM BigInsights 4.2
- Incluído o botão Testar conexão para verificar a conexão com os daemons Hadoop que são especificados durante a configuração do agente
- Melhorado o processo de configuração do agente para reduzir o tempo de configuração e a complexidade. A configuração foi simplificada porque as seguintes tarefas de pré-requisito e configuração não são necessárias:
  - Instalar o plug-in em cada nó do cluster Hadoop
  - Configurar e atualizar o arquivo `hadoop-metrics2.properties`
  - Reiniciar os daemons Hadoop depois de configurar o arquivo `hadoop-metrics2.properties`
  - Configurar todos os DataNodes e NodeManagers no cluster
  - Reiniciar o agente quando nós adicionais forem incluídos no cluster

Monitoring Agent for JBoss

Os seguintes aprimoramentos foram incluídos no agente JBoss:

- Incluído rastreamento de transação e monitoramento de detalhamento na oferta Agentes Avançados
- Incluída uma página de painel para monitorar métricas de origem de dados
- Incluído suporte para monitoramento das seguintes ofertas JBoss: WildFly 8.x/9.x/10.x, JBoss EAP 7.x, JBoss AS 7.x
- Incluído suporte para executar o agente no sistema operacional Windows

Monitoring Agent for Linux KVM

Foram incluídos os seguintes aprimoramentos no painel do agente do Linux KVM:

- Atualizado o widget de grupo Hosts na página Hosts, clusters e armazenamento para exibir o Máximo de memória de planejamento (GB) e os KPIs de captura instantânea ativos
- Incluída a página Detalhes de armazenamento para exibir detalhes sobre os discos e capturas instantâneas de discos no conjunto de armazenamentos
- Incluído o widget de grupo Dados transmitidos/recebidos pela rede (GB) na página Detalhes do host para exibir informações históricas do total de dados (em GB) que são transmitidos e recebidos pela rede

Monitoring Agent for Linux OS

O seguinte aprimoramento foi incluído no agente do S.O. Linux:

- O Linux on Power Little Endian (pLinux LE) é suportado

Monitoring Agent for Microsoft Exchange Server

Foram incluídos os seguintes aprimoramentos no painel do Microsoft Exchange Server agent:

- Incluídos os atributos de tempo de entrada e de tempo de saída no conjunto de dados Alcance
- Incluídas páginas e widgets de grupo para exibir detalhes de alcance
- Incluído um limite de acontecimentos para alcance
- Incluído suporte para instalar e configurar o agente no Exchange Server 2016 e no sistema Windows Server 2016

Monitoring Agent for Microsoft Internet Information Services

O seguinte aprimoramento foi incluído no Microsoft IIS agent:

- Incluído suporte para instalar e configurar o agente no sistema Microsoft Windows Server 2016

Monitoring Agent for Microsoft Active Directory

Foram incluídos os seguintes aprimoramentos no Microsoft Active Directory agent:

- Incluídos os widgets de grupo e páginas para exibir os detalhes do Objeto de política de grupo, Netlogon, Autoridade de segurança local e detalhes de LDAP
- Incluídos os seguintes conjuntos de dados que podem ser visualizados na guia **Detalhes do atributo**:
  - Conjunto de dados de serviços
  - Réplica
  - Serviço de Replicação de Arquivo
  - Unidade org. movida ou excluída
  - Atributos LDAP
  - Security Accounts Manager
  - DFS
  - Catálogo de Endereços
  - Log de Eventos
  - Objetos de Configuração de Senha
- Incluídos os conjuntos de dados para ADFS, Proxy ADFS e Fila de encadeamentos assíncronos
- Incluídos os widgets de grupo e páginas para exibir detalhes do ADFS e Proxy ADFS
- Incluído suporte para instalar e configurar o agente em sistemas Windows Server 2016

Monitoring Agent for Microsoft .NET

Foram incluídos os seguintes aprimoramentos no painel do Microsoft .NET agent:

- Atualizado o widget de grupo Status do MS .NET na página Componente para exibir os tempos de resposta de chamadas de banco de dados, status de processos .NET com alta contagem de encadeamentos e falhas de compilação Just in Time (JIT)
- Incluídos conjuntos de dados, páginas e widgets de grupo para mostrar detalhes de compilação JIT, detalhes de chamada do banco de dados, manipulações de GC e coleção de objetos fixados

para um processo .NET selecionado, taxa de contenção de encadeamento e e comprimento da fila de encadeamentos

- Incluídos limites de acontecimentos para falhas de JIT, falhas de solicitação de .NET, comandos lentos, coleta de lixo e os encadeamentos ativos em processos .NET

Monitoring Agent for Microsoft SQL Server

Foram incluídos os seguintes aprimoramentos no painel do Microsoft SQL Server agent:

- Incluído o widget de grupo Consultas dispendiosas na página Desempenho do servidor - Detalhes para visualizar os 10 principais planos de consulta em cache, de acordo com as estatísticas de desempenho do Microsoft SQL Server
- Incluído suporte para monitoramento do Microsoft SQL Server 2016
- Incluído suporte para instalar e configurar o Microsoft SQL Server agent no sistema Microsoft Windows Server 2016
- Incluída a nova variável de ambiente *COLL_ERRORLOG_RECYCLE_WAIT* para configurar o intervalo de tempo (em segundos) para o qual o agente espera antes de coletar dados do grupo de atributos Detalhe do Evento de Erro do MS SQL

Monitoring Agent for MongoDB

Foram incluídos os seguintes aprimoramentos no painel do Agente MongoDB:

- Atualizada a página Componente para exibir o número de instâncias MongoDB e seus status
- Incluídas páginas para exibir detalhes do MMAPv1 e dos mecanismos de armazenamento WiredTiger
- Incluída a página Informações de entrada e saída para exibir detalhes do cursor e dados históricos para as operações enfileiradas, conexões ativas, fluxo de dados e o acesso a dados do host selecionado
- Incluídas páginas para exibir detalhes dos bloqueios da versão 2.x e da versão 3.x ou mais recente
- Incluída a página Detalhes de replicação para exibir detalhes do número de replicação, de oplog e dos dados históricos do atraso de replicação e o espaço usado pelo oplog

Monitoring Agent for Node.js

Os seguintes aprimoramentos foram incluídos no Agente Node.js para alavancar o Node Application Metrics (Appmetrics):

- Incluídos novos painel e widgets de grupo para visualizar detalhes da coleta de lixo
- Incluídos novo painel e widgets de grupo para visualizar detalhes do loop de eventos

Monitoring Agent for PostgreSQL

Os seguintes aprimoramentos foram incluídos no Agente PostgreSQL:

- Incluído suporte para instalar e configurar o agente em sistemas Windows
- Incluído suporte para monitorar o PostgreSQL V9.6
- Atualizada a página Visão geral de status para que o status não seja crítico quando a taxa de ocorrência do buffer for zero

Monitoring Agent for SAP NetWeaver Java Stack

Os seguintes aprimoramentos foram incluídos no SAP NetWeaver Java Stack:

- Incluídos conjuntos de dados, widgets de grupo e páginas para coletar e visualizar os dados de rastreamento de transação e diagnósticos
- Incluído suporte para instalar e configurar o agente em sistemas Windows 2016

Monitoring Agent for Synthetic Playback

O seguinte aprimoramento foi incluído no Synthetic Playback agent:

- O Synthetic Playback agent inclui um novo recurso de filtragem para transações sintéticas. No Synthetic Script Manager, configure listas de bloqueio e listas de desbloqueio para suas transações sintéticas que excluem ou incluem solicitações para URLs e domínios especificados.

Use listas de bloqueio e listas de desbloqueio para filtrar ou incluir dependências que afetam os tempos de resposta para seu aplicativo, como métricas de terceiros.

Monitoring Agent for Tomcat

O seguinte aprimoramento foi incluído no Agente Tomcat:

- Incluído suporte para instalar e configurar o Agente Tomcat em sistemas Windows e SUSE Linux Enterprise 12

Monitoring Agent for WebSphere Applications

Os seguintes aprimoramentos foram incluídos no WebSphere Applications agent:

- O Linux on Power Little Endian (pLinux LE) é suportado. (O rastreamento de transação não é suportado em sistemas pLinux LE.)
- Incluído suporte para IBM WebSphere Application Server traditional V9.
- Incluído o painel Análise de memória para ajudar a diagnosticar possíveis fugas de memória, verificando as informações de uso do heap para cada dump do heap. O modo de diagnósticos deve ser ativado para que este painel contenha dados.
- Incluído suporte para usar o conjunto de dados Status de funcionamento do aplicativo para criar limites de eventos para monitoramento de status do aplicativo. A coleta de dados para esse uso é desativada por padrão. Deve-se modificar o arquivo de propriedades do coletor de dados para ativá-lo antes da criação de limites de eventos.
- Simplificada a configuração manual do coletor de dados. Para WebSphere Applications Server, é preciso somente incluir alguns argumentos e variáveis da JVM para o servidor de aplicativos no console administrativo do WebSphere. Para Liberty, é preciso somente modificar três arquivos para o servidor.

Response Time Monitoring Agent

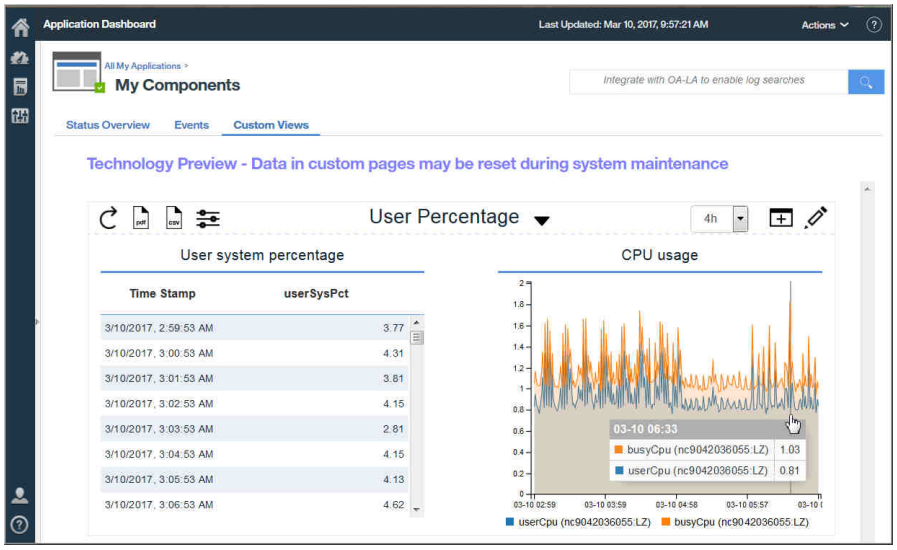
Os seguintes aprimoramentos foram incluídos no Agente Response Time Monitoring:

- Incluído suporte para configurar o rastreamento de usuário para aplicativos na página **Configuração do agente**.
- Incluído suporte para configurar o rastreamento de sessão para aplicativos na página **Configuração do agente**.

Console do Cloud APM Aprimoramentos do

Foram feitas várias melhorias nas interfaces de instalação e configuração do agente, além dos seguintes aprimoramentos do console:

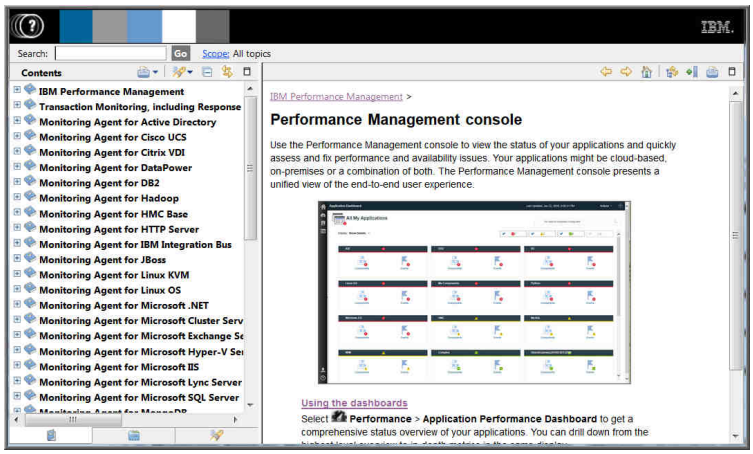
- Visualização de tecnologia: uma nova guia **Visualizações customizadas** está disponível para as páginas do Application Dashboard. É possível criar uma variedade de visualizações para métricas de relatório de um recurso gerenciado e aplicar funções, como média e contagem. Depois de abrir uma página salva, é possível atualizar a página com dados de um recurso diferente e fazer download das métricas da página como um arquivo PDF ou CSV. Para obter mais informações, consulte “Visualizações customizadas” na página 1112.



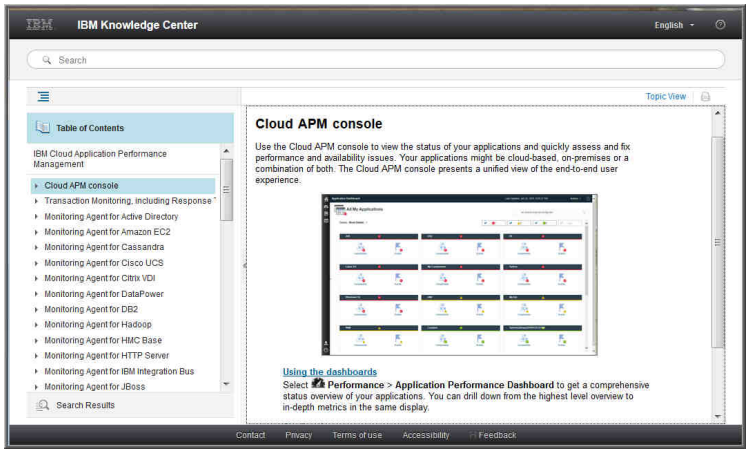
Se não aparecer **Visualizações customizadas** em sua assinatura do Cloud APM e se desejar tentar esse novo recurso, abra uma solicitação de serviço com o IBM Support para ativar a visualização de tecnologia **Visualizações customizadas**. Esteja ciente de que as páginas de painel customizado e os dados históricos que as preenchem não são salvos durante a manutenção do sistema.

- Quando abrir o sistema de ajuda do Console do Cloud APM, observe que ele é hospedado pelo IBM Knowledge Center. Você possui a ferramenta **Ocultar Índice**, recursos de procura e impressão e links para informações de suporte e opções de feedback.

Antes



Depois



Aprimoramentos do Agent Builder

O suporte foi melhorado para a construção de painéis de resumo do Cloud APM para agentes do Agent Builder. Deve-se usar conjuntos de dados de linha única para fornecer dados para painéis de

resumo. É possível fornecer esses conjuntos de dados de arquivos de log inteiros e de quaisquer conjuntos de dados que podem ser filtrados para uma única linha.

O que há de novo: setembro de 2016

Novos recursos, capacidades e cobertura foram disponibilizados na liberação de setembro de 2016 do Performance Management on Cloud.

Novos agentes disponíveis

Monitoring Agent for Amazon EC2

É possível usar o Agente Amazon EC2 para monitorar o funcionamento, a disponibilidade e o desempenho do seu Amazon Elastic Compute Cloud (EC2). Recursos de instância. Você pode monitorar os seguintes recursos:

- Utilização de CPU
- Utilização do Elastic Block Store (EBS)
- Utilização da rede
- Atualizações de manutenção do Amazon Web Services (AWS)
- Desempenho do Disco

Esse agente está no Infrastructure Extension Pack e está disponível para as seguintes ofertas: IBM Monitoring, IBM Application Performance Management e IBM Application Performance Management Advanced.

Monitoring Agent for SAP NetWeaver Java Stack

É possível usar o SAP NetWeaver Java Stack para monitorar o funcionamento, disponibilidade e desempenho do SAP NetWeaver Java Stack Cluster e de recursos da Instância. É possível usar o agente para monitorar os recursos de cluster, como dumps do heap, Instância da JVM, tempo de resposta das sessões do usuário, detalhes da transação, informações do sistema e detalhes da licença. É possível usar o agente para monitorar os recursos da instância, como utilização da CPU, utilização de disco, utilização de memória, coleta de banco de dados, coleta de lixo, dumps do heap, aplicativo com falha, contêiner da web e informações da sessão. Esse agente está no Advanced Extension Pack e ficará disponível se você tiver uma das seguintes ofertas: IBM Application Performance Management e IBM Application Performance Management Advanced.

Aprimoramentos do agente

Monitoring Agent for Citrix Virtual Desktop Infrastructure

Incluída a capacidade de recuperar eventos do Log de eventos do Windows para máquinas Virtual Delivery Agent (VDA) Desktop Delivery Controller (DDC).

Monitoring Agent for Linux KVM

Os painéis estão disponíveis para o agente monitorar a implementação de suas máquinas virtuais baseadas em Linux Kernel. Esses painéis fornecem as seguintes capacidades de monitoramento:

- O painel de resumo mostra o status geral dos hosts com base na utilização da CPU e da memória do ambiente ou aplicativo de máquinas virtuais baseadas em Linux Kernel.
- O painel Detalhe do Host mostra detalhes sobre o host selecionado.
- O painel Hosts, clusteres e armazenamento mostra detalhes sobre as máquinas virtuais monitoradas.
- O painel Detalhes da máquina virtual mostra detalhes sobre a máquina virtual selecionada na página Detalhe do host.

Monitoring Agent for Linux OS

O Docker V1.8.0 ou mais recente é suportado. Novos grupos de atributos e widgets foram incluídos para permitir que o Linux OS Agent entregue recursos de monitoramento do docker.

Monitoring Agent for Oracle Database

O painel do agente Oracle Database inclui os novos recursos a seguir na página Detalhes da Instância:

- Uma tabela que exibe informações sobre a contenção de bloqueio na instância selecionada.
- Uma tabela que exibe informações sobre o GCS e o GES do Oracle Real Application Clusters.
- Uma tabela que exibe detalhes dos grupos de disco Automatic Storage Management (ASM) que são conectados à instância selecionada.
- Uma visualização que mostra informações detalhadas por espaço de tabela, que estarão visíveis se clicar em **5 menores espaços de tabela livres**.
- Uma tabela que exibe os detalhes históricos dos processos de primeiro e segundo planos que são anexados à instância selecionada. É possível clicar na entidade na tabela e visualizar a tabela detalhada de todos os processos para essa instância.
- Uma tabela que exibe as 5 Piores Consultas SQL (por tempo de execução) na instância selecionada. É possível clicar na tabela e visualizar uma tabela detalhada das 50 piores consultas SQL para essa instância.

Monitoring Agent for Synthetic Playback

O Synthetic Playback agent inclui um novo recurso de segurança. É possível evitar que senhas que estão armazenadas em scripts sintéticos sejam exibidas no Synthetic Script Manager.

Monitoring Agent for VMware VI

Com a inclusão do recurso de desacoplamento do agente, é possível visualizar e selecionar o nó do agente e seus subnós na mesma visualização.

Ao selecionar o componente VMware Virtual Infrastructure na janela Selecionar componente, o Editor de componente exibe uma estrutura em árvore do nó do agente com todos os seus subnós.

- Se você expandir a árvore e selecionar o nó do agente, todos os subnós serão selecionados automaticamente. Também é possível expandir a árvore e selecionar individualmente os subnós que você deseja monitorar.
- Se você selecionar o nó do agente quando a árvore estiver reduzida, todos os subnós serão automaticamente excluídos.

Ao selecionar o componente ESX Server na janela Selecionar componente, junto de subnós, os ESX Servers independentes também serão exibidos no Editor de componente. Com os subnós, é possível selecionar Servidores ESX independentes para monitoramento.

Após a criação do aplicativo, o painel da UI do APM exibe uma estrutura em árvore da instância do agente como pai e seus nós como filhos.

Response Time Monitoring Agent

É possível customizar os locais que são aplicados a endereços IP ou variações de endereços específicas nos painéis Transação do usuário final para seu ambiente específico. Use a guia **Localização geográfica** na **Configuração do agente** para customizar valores de locais.

Console do Cloud APM Aprimoramentos do

- Vários aprimoramentos foram feitos nas interfaces de instalação e configuração do agente.
- Uma opção **Log do painel** foi incluída no menu **Ações** para revisar a lista de painéis do agente que foram atualizados desde a última reinicialização do servidor. Para obter mais informações, consulte “Todos os Meus Aplicativos - Application Performance Dashboard” na página 1079.
- A página Application Performance Dashboard para o aplicativo selecionado foi aperfeiçoada para melhorar a visualização. Uma contagem de eventos de severidade crítica e de aviso é exibida no título da guia Eventos e substitui o gráfico de barras **Resumo de severidade de** evento. Para aplicativos com as visualizações de topologia ativadas, a visualização **Topologia de aplicativo de agregado** possui um botão comutador para alternar para o gráfico de barras Status do componente atual. Para obter mais informações, consulte “Visão Geral de Status” na página 1082.

- Em liberações anteriores, a guia Application Performance Dashboard **Detalhes do Atributo** estava disponível somente para instâncias do componente. A guia **Detalhes do atributo** está disponível para criar tabelas históricas de instâncias de transação do Agente Response Time Monitoring e do Synthetic Playback agent. Para usuários com deficiências visuais, a capacidade de criar tabelas de históricos fornece uma alternativa aos gráficos de linhas, que não podem ser interpretados por tecnologias assistivas, como o software de leitor de tela. Para obter mais informações, consulte "Visualizando e gerenciando gráficos e tabelas customizados" na página 1092.

API

É possível usar APIs para criar scripts para automatizar a migração do ambiente do Performance Management. Para obter mais informações, consulte "Explorando as APIs" na página 1072.

O que há de novo: abril de 2016

Os novos recursos, capacidades e coberturas foram disponibilizados na liberação de abril de 2016 do Performance Management on Cloud.

IBM Marketplace

As ofertas IBM Performance Management on Cloud estão disponíveis no IBM Marketplace. Inscreva-se para uma avaliação grátis ou conta de assinatura. Para obter mais informações, consulte "Fazendo download de seus agentes e coletores de dados" na página 101.

Novos agentes disponíveis

Monitoring Agent for Citrix Virtual Desktop Infrastructure

É possível usar Citrix VDI agent para monitorar o funcionamento, a disponibilidade e o desempenho de recursos Citrix XenDesktop ou XenApp, como sites, máquinas, aplicativos, desktops, sessões e usuários. Esse agente está no Infrastructure Extension Pack e está disponível para as seguintes ofertas: IBM Monitoring, IBM Application Performance Management e IBM Application Performance Management Advanced.

Monitoring Agent for Skype for Business Server

É possível usar Agente Skype for Business Server para monitorar o funcionamento, a disponibilidade e o desempenho de recursos Microsoft Lync Server, como banco de dados, servidor de mediação, transações sintéticas, mensagem instantânea, operações de gravação de serviço CDR e peers SIP.

Monitoring Agent for WebLogic

É possível usar o Agente WebLogic para monitorar o funcionamento, a disponibilidade e o desempenho dos recursos do servidor WebLogic, como Java Virtual Machines (JVMs), Java Messaging Service (JMS) e Java Database Connectivity (JDBC).

Aprimoramentos de integração

Coexistência de agente

A coexistência do agente é suportada. É possível instalar agentes IBM Performance Management no mesmo computador em que os agentes IBM Tivoli Monitoring estão instalados. No entanto, os dois agentes não podem ser instalados no mesmo diretório. Consulte "Coexistência do agente Cloud APM e do agente Tivoli Monitoring" na página 950.

IBM Alert Notification

A Notificação de Alerta inclui um aplicativo móvel que oferece um subconjunto de funções de Notificação de Alerta em dispositivos iOS e Android.

Monitoramento do Pilha de integração IBM

É possível monitorar o Pilha de integração IBM para ver informações de rastreamento de transações para os produtos de middleware de dispositivo IBM MQ, IBM Integration Bus e DataPower e os serviços que eles expõem e resolver problemas, se surgirem problemas. Consulte "Cenário: monitorando o Pilha de integração IBM" na página 95.

Aprimoramentos do agente

Monitoring Agent for Db2
Comandos foram incluídos para conceder privilégios para o usuário padrão (para sistemas Windows) e usuário proprietário da instância (para sistemas Linux e AIX) para visualizar os dados de alguns dos atributos do Db2.

Monitoring Agent for Hadoop
O Agente do Hadoop é suportado em sistemas operacionais Linux, Windows e AIX.

Monitoring Agent for HMC Base
Recursos de monitoramento são fornecidos para E/S virtual e para eventos de hardware.

Monitoring Agent for IBM Integration Bus

O caminho da biblioteca da versão mais recente do IBM MQ (WebSphere MQ) pode ser descoberto automaticamente durante a configuração do agente em sistemas Linux e AIX.

Monitoring Agent for Microsoft Cluster Server
O Microsoft Cluster Server agent é configurado automaticamente após ser instalado.

Monitoring Agent for Microsoft Exchange Server
Alguns serviços adicionais foram incluídos na guia **Serviços do Exchange** da janela de configuração do agente para determinar o status do Exchange Server.

Monitoring Agent for Microsoft Hyper-V Server
Painel de configuração do agente removido. A configuração do agente não é necessária.

Monitoring Agent for SAP HANA Database
O widget do grupo Detalhes de informações de cache foi incluído no painel **Detalhes do banco de dados SAP HANA** para fornecer informações sobre a porcentagem de memória usada, a porcentagem de memória disponível e a taxa de acertos do cache para o banco de dados monitorado.

Monitoring Agent for Synthetic Playback
O Synthetic Playback agent inclui os seguintes recursos:

- É possível instalar e configurar o Synthetic Playback agent para monitorar o desempenho e a disponibilidade de aplicativos internos e privados no Application Performance Dashboard, além de aplicativos externos e públicos.
- Usar o Gerenciador de Script Sintético para gerar um script simples para testar a disponibilidade e o desempenho de seus aplicativos.
- Configurar a reprodução simultânea ou escalonada de transações sintéticas em diferentes locais.
- Monitorar seu uso de reprodução mensal no Gerenciador de Script Sintético.
- Visualizar métricas HTTP e taxas de disponibilidade em relatórios do Synthetic Playback agent.
- Visualizar dois novos relatórios: tendência de transações e tendência de subtransações.
- Organize suas transações sintéticas em um grupo de recursos e aplique limites a todas as transações desse grupo de recursos.
- Visualizar dados de transação sintéticos na janela **Minhas transações** no Application Performance Dashboard sem a necessidade de criar um aplicativo que contenha transações sintéticas associadas.
- Fazer download de scripts sintéticos do Synthetic Script Manager.

Monitoring Agent for VMware VI
O painel do Agente VMware VI foi aprimorado para incluir os novos recursos a seguir:

- O número de alarmes acionados no estado crítico ou de aviso também é exibido na página **Componente**.
- Uma nova tabela na página **Resumo do Cluster** fornece informações sobre alarmes proativos e de falha. É possível clicar na entidade acionada na tabela e visualizar a página de detalhes dessa entidade acionada.

- Uma nova tabela na página **Detalhes do Cluster** exibe detalhes dos servidores ESX que pertencem ao cluster selecionado. É possível clicar no servidor ESX e visualizar a página de detalhes desse servidor ESX.
- A tabela Armazenamento de dados na página **Detalhe do cluster** mostra a métrica de supercomprometimento do armazenamento de dados.
- A tabela Máquinas virtuais na página Detalhe da VM exibe mais métricas de desempenho, como tamanho da memória, NICs e discos. É possível clicar e visualizar suas páginas de detalhes.
- Novos widgets e páginas foram incluídos para exibir importantes métricas de desempenho da memória, dos discos e da rede para a máquina virtual selecionada.
- Uma nova tabela na página **Detalhe do ESX Server** exibe o desempenho da rede do servidor.
- A tabela Armazenamento de dados na página **Detalhe da VM** e na página **Detalhe do ESX Server** exibe a métrica de latência do armazenamento de dados.
- Uma nova tabela na página **Detalhe do armazenamento de dados** exibe informações sobre a máquina virtual que está associada ao armazenamento de dados. É possível clicar na máquina virtual na tabela e visualizar a página **Detalhes da Máquina Virtual**.
- O título do gráfico % de memória (Histórico) na página **Detalhe da VM** foi mudado para Memória guest (Histórico).

Monitoring Agent for WebSphere Applications

O painel Resumo de solicitações em andamento fornece recurso para identificar as instâncias de solicitação que estão atualmente lentas ou interrompidas. É possível executar uma operação de cancelamento simples em uma solicitação em andamento selecionando a solicitação e, em seguida, clicando em **Cancelar encadeamento** no widget Solicitação em Andamento nesse painel.

Todos os limites de acontecimento predefinidos foram refinados para fornecer uma melhor experiência de usuário. Os aprimoramentos e atualizações envolvem a condição que aciona um alerta, o intervalo de amostragem e a gravidade do limite.

A interface com o usuário do Monitoring Agent for WebSphere Applications está acessível aos usuários com deficiências físicas.

O processo de configuração foi refinado com base no feedback do cliente e revisão técnica para fornecer uma melhor experiência do usuário.

Monitoring Agent for WebSphere MQ

Algumas mudanças foram feitas para os limites de acontecimentos predefinidos:

- Todos os limites predefinidos têm um prefixo MQ_ em vez de MQSeries_ como nas versões anteriores.
- Dois limites, MQ_Channel_Initiator_Crit e MQ_Queue_Manager_Crit, foram incluídos para acionar alertas críticos para o status de servidor inicializador de canal e status do gerenciador de filas.
- A condição acionadora do evento MQ_Queue_Depth_High foi alterada de 80% estática para um alto valor de profundidade da fila.

O nome do widget **Fila não está sendo lida - 5 principais** foi mudada para **Fila em uso não sendo lida - 5 principais**. Esse widget fornece uma lista das cinco principais filas que possuem mensagens e estão conectadas por um ou mais aplicativos para inserir mensagens na fila, mas não estão sendo lidas por qualquer aplicativo.

O caminho da biblioteca da versão mais recente do IBM MQ (WebSphere MQ) pode ser descoberto automaticamente durante a configuração do agente. É possível manter o parâmetro **WMQLIBPATH** vazio no arquivo silencioso de resposta ou aceitar o valor padrão ao configurar o agente interativamente.

agentes de S.O.

Os agentes do sistema operacional contêm uma nova funcionalidade para monitorar arquivos de log do aplicativo. A funcionalidade inclui recurso para configurar o monitoramento do arquivo de log com base em expressões regulares.

Para compatibilidade, o agente do sistema operacional consome as seguintes informações e formatos:

- Informações de configuração e o arquivo de formato foram usados pelo IBM Tivoli Monitoring 6.x Log File Agent
- Informações de configuração e sequências de formatos que foram usadas pelo Tivoli Event Console Log File Adapter

Essas sequências de formato permitem que o agente filtre os dados de log de acordo com padrões no arquivo de formato e envie apenas os dados relevantes para um consumidor de evento. O OS Agent envia dados para o servidor Performance Management ou por meio de recurso de integração de evento (EIF) para qualquer receptor EIF, como análise OMNIbus EIF.

Response Time Monitoring Agent

Os painéis Transações de usuário final incluem informações do usuário e do dispositivo, que eram exibidas anteriormente nos painéis Usuários autenticados e Dispositivos móveis no grupo Usuários. As informações do usuário, da sessão e do dispositivo são classificadas por local (país, estado e cidade) com base no endereço IP do usuário. Use os painéis novos e atualizados para entender volumes do usuário e se problemas são isolados para conjuntos específicos de usuários.

Customize os locais que são aplicados a endereços IP ou intervalos de endereços específicos nos painéis Transação do usuário final para seu ambiente específico. Use a guia **Localização geográfica** na **Configuração do agente** para customizar valores de locais.

Rastreamento de Transações

A página Resumo de transação inclui uma topologia Dependências de serviço, que mostra o nó de recurso selecionado, como um IBM Integration Bus, e os serviços dos quais ele depende. A página Detalhes da transação inclui uma topologia Dependências de transação que mostra um nó de transação para cada instância do componente e um nó não instrumentado para cada serviço dependente no nível da transação, por exemplo, IBM Integration Bus e suas transações de serviço. A página Detalhes da transação também destaca os usuários do aplicativo selecionado que estão tendo os tempos de resposta mais lentos e os hosts com o volume mais alto de transações.

Aprimoramentos do agente geral

Os aprimoramentos de configuração e instalação gerais do agente a seguir foram feitos:

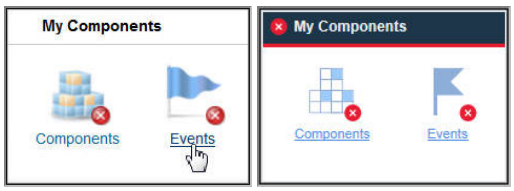
- O script de instalação do agente executa uma verificação de permissões antes do início da instalação. Se você não tiver permissão adequada, uma mensagem será exibida.
- O comando de status do agente verifica o status entre o agente e o console do Performance Management.
- Os agentes que são suportados em sistemas Windows possuem um utilitário de GUI que pode ser usado para executar a configuração do agente e verificar o status da conexão.
- É possível usar um novo comando para remover uma instância de agente sem desinstalar o agente.

Aprimoramentos do servidor Performance Management

A autenticação do usuário do Performance Management é gerenciada por meio de um IBMid do provedor OpenID Connect.

Aprimoramentos do console do Performance Management

- A aparência do console do Performance Management foi atualizada para se alinhar com a interface com o usuário do IBM Bluemix. Por exemplo, visualize as diferenças entre uma caixa de resumo no painel **Todos os Meus Aplicativos** da V8.1.2 e agora:



- Uma nova opção foi incluída na página Configuração Avançada, de modo que usuários avançados possam ativar ou desativar facilmente todos os limites predefinidos em todos os grupos do sistema. Consulte “Informações de histórico” na página 976.
- Uma nova opção foi incluída na página Configuração avançada para controlar a taxa de atualização automática do Application Performance Dashboard. Para obter mais informações, consulte “Integração de UI” na página 1073.
- Vários aprimoramentos foram feitos nas interfaces de instalação e configuração do agente.
- Melhorias na acessibilidade do console do Performance Management. Para obter informações sobre os recursos de acessibilidade da interface com o usuário, consulte “Recursos de Acessibilidade” na página 1511.

API

É possível usar APIs para criar scripts para automatizar a migração do ambiente do Performance Management. Para obter mais informações, consulte “Explorando as APIs” na página 1072.

Aprimoramento do Agent Builder

O Agent Builder inclui filtragem aprimorada do conjunto de dados. Você pode usar a filtragem para criar conjuntos de dados que retornam uma única linha com base nos conjuntos de dados com várias linhas, incluindo o conjunto de dados de disponibilidade. Use esse recurso para fornecer informações sobre painéis de resumo.

Capítulo 2. Documentação em PDF

Os documentos em PDF estão disponíveis para tópicos nesta coleção do IBM Knowledge Center e para referências de agente.

IBM Knowledge Center em formato PDF

Além deste Guia do Usuário, é possível fazer download do Guia do Usuário do IBM Agent Builder.

PDFs de referência do agente

Para fazer download da Referência para um agente, consulte Métricas do agente/PDFs de referência no Application Performance Management Developer Center. As Referências fornecem informações sobre painéis, limites de acontecimentos e conjuntos de dados. Os conjuntos de dados contêm atributos, que são as métricas relatadas pelo agente e que formam os principais indicadores de desempenho (KPIs). É possível localizar a versão do agente na página de título do arquivo PDF.

Capítulo 3. Visão geral do produto

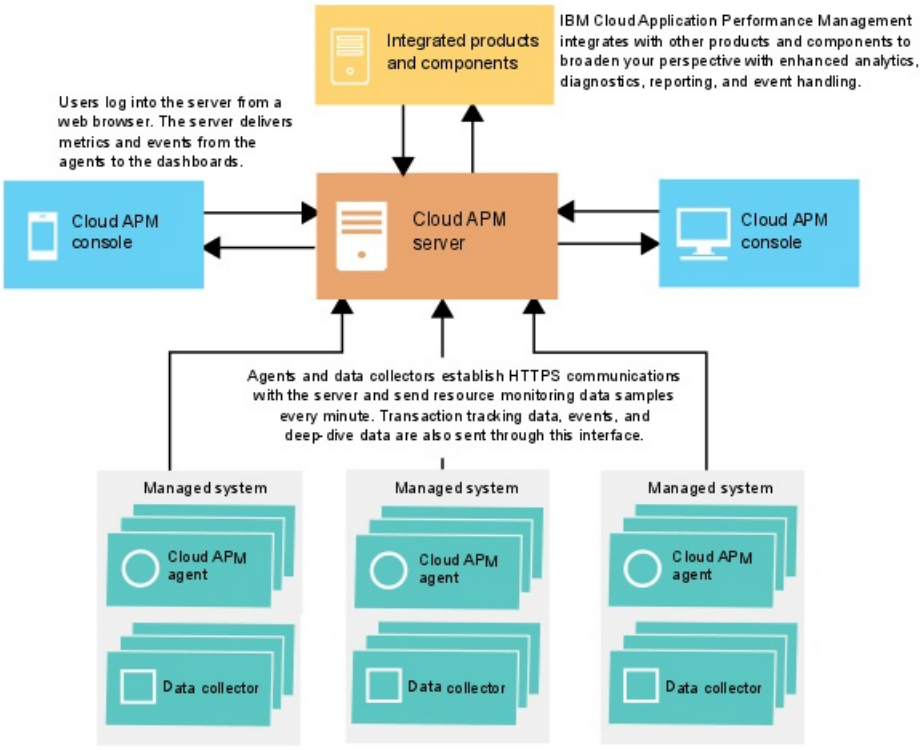
O IBM Cloud Application Performance Management (Cloud APM) é uma solução abrangente que ajuda a gerenciar o desempenho e a disponibilidade de aplicativos implementados no local (privado), em uma nuvem pública ou como uma combinação híbrida. Esta solução fornece visibilidade, controle e automação de seus aplicativos, assegurando desempenho ideal e uso eficiente de recursos.

Usando essa solução, você gerencia seu datacenter, infraestrutura em nuvem e cargas de trabalho com inteligência cognitiva. É possível reduzir e evitar indisponibilidades e redução de velocidade 24 horas por dia em um mundo de aplicativos híbridos, já que o Cloud APM lhe ajuda a ir da identificação de problemas de desempenho ao isolamento do local onde o problema está ocorrendo e ao diagnóstico de problemas antes que seus negócios sejam afetados.

Use os recursos-chave, que variam por oferta, para trabalhar com dados coletados pelos agentes e coletores de dados do Cloud APM. Mais recursos estão disponíveis por meio da integração com outros produtos e componentes.

Visão Geral de Arquitetura

O IBM Cloud Application Performance Management usa *agentes* e *coletores de dados* para coletar dados nos hosts monitorados. Os agentes e coletores de dados transmitem os dados para o Servidor Cloud APM, que os reduz no Console do Cloud APM. O Servidor Cloud APM é hospedado na nuvem IBM.



Coleção de dados

Os agentes e coletores de dados monitoram sistemas, subsistemas ou aplicativos e coletam dados. Um agente ou um coletor de dados interage com um único recurso (por exemplo, um sistema ou aplicativo) e, na maioria dos casos, está no mesmo computador ou máquina virtual na qual o sistema ou aplicativo está em execução. Por exemplo, o agente do S.O. Linux coleta indicadores de desempenho para o sistema operacional no host Linux e o WebSphere Applications agent monitora os indicadores de desempenho de

servidores de aplicativos WebSphere. Além disso, alguns agentes controlam transações entre diferentes recursos.

É possível configurar limites nos Principais indicadores de desempenho (KPIs). Se um indicador mudar para ficar acima ou abaixo do limite, o agente ou coletor de dados gerará um alerta, que o servidor processa. Também é possível configurar o encaminhamento de eventos para um destino, como o Netcool/OMNIbus Probe for Tivoli EIF ou um servidor SMTP e usar o Alert Notification para configurar notificações por e-mail para eventos.

Os agentes e coletores de dados são pré-configurados para se comunicarem com o Servidor Cloud APM.

Comunicação entre o servidor e agentes ou coletores de dados

Os agentes e coletores de dados em cada host monitorado estabelecem uma comunicação HTTPS com o Servidor Cloud APM, que está na nuvem IBM. O agente ou o coletor de dados é o lado do cliente da conexão.

Os agentes e coletores de dados requerem conectividade da Internet para enviar dados para o servidor e, se não puderem enviar dados diretamente pela Internet, um proxy de encaminhamento poderá ser necessário. Para obter mais informações, consulte “Conectividade de rede” na página 157.

Dados armazenados pelo servidor

Os agentes e coletores de dados enviam dados por push para o Servidor Cloud APM em intervalos que vão de 1 minuto a 8 minutos, dependendo do tipo de dados. O servidor armazena todos os valores que são enviados pelos agentes e coletores de dados por 8 dias Por padrão. Os dados da transação resumidos são armazenados por períodos mais longos.

Os dados de monitoramento salvos são chamados de dados *históricos*. O servidor usa dados históricos para exibir tabelas e gráficos que você pode usar para analisar as tendências em seu ambiente.

Os relatórios de histórico também estão disponíveis para determinados agentes. Para obter mais informações, consulte “Relatórios” na página 1124.

Escalabilidade

É possível monitorar até 10.000 sistemas gerenciados a partir do Cloud APM. Um sistema gerenciado é um único sistema operacional, subsistema ou aplicativo na sua empresa sendo monitorado por um agente.

O Cloud APM suporta entre 150 e 400 transações do usuário monitoradas por segundo.

Integração

O IBM Cloud Application Performance Management se integra com outros produtos e componentes quando eles são configurados para comunicação com o Servidor Cloud APM.

Os produtos que podem ser integrados incluem o IBM Control Desk, Netcool/OMNIbus, Tivoli Monitoring, OMEGAMON, Operations Analytics - Log Analysis, Operations Analytics - Predictive Insights, IBM Alert Notification e IBM Cloud.

O Agent Builder é um componente que pode ser usado para criar agentes customizados.

Interface com o Usuário

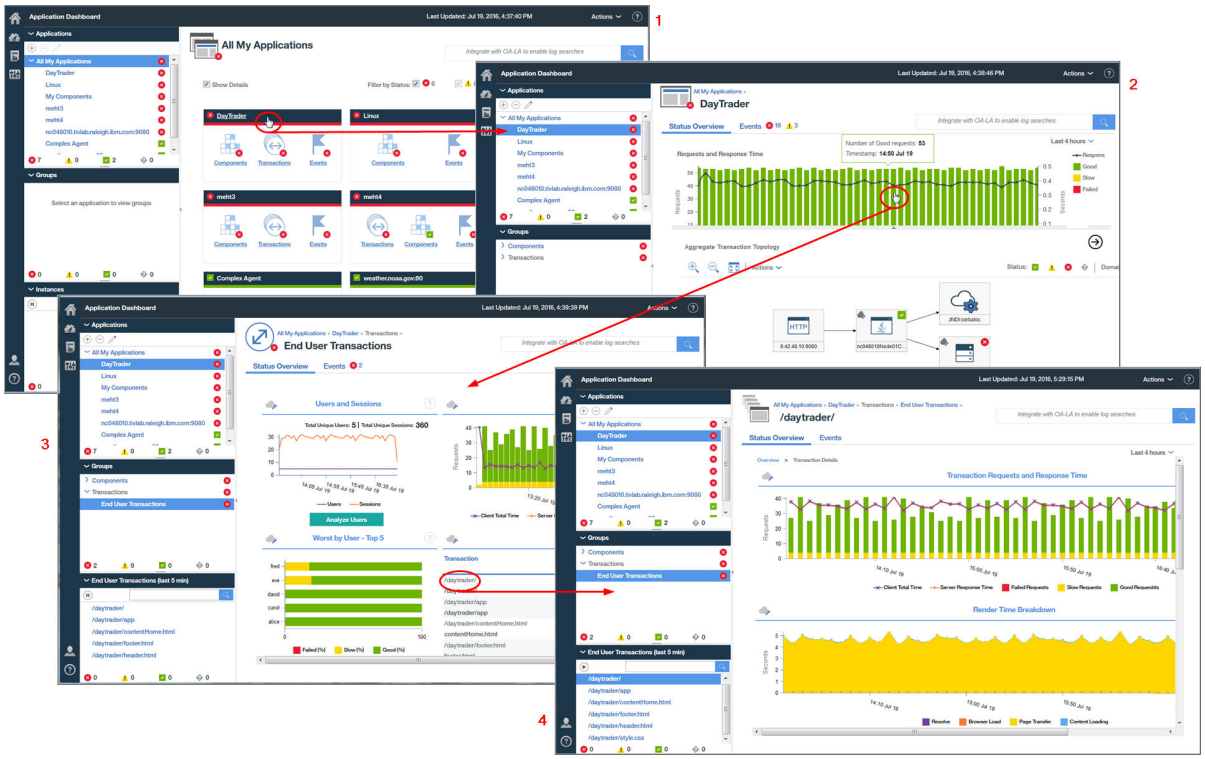
O Console do Cloud APM é a interface com o usuário para Cloud APM. Essa interface com o usuário unificada fornece uma visualização única em aplicativos híbridos. Você usa o console para visualizar o status de seus aplicativos e avaliar e corrigir rapidamente problemas de desempenho e disponibilidade.

Os painéis no console simplificam a identificação de problema, de modo que seja possível isolar gargalos que afetam o desempenho do aplicativo. Com navegação em painel simples, você se move de uma visualização de status do aplicativo para detalhes do nível de código. Você tem visibilidade dos problemas

de código-fonte no momento exato do problema. É possível procurar e diagnosticar problemas usando análise de dados de procura integrada.

O navegador do Application Performance Dashboard no console é hierárquico, fornecendo uma visão geral do status dos aplicativos, do funcionamento de seus componentes e da qualidade da experiência do usuário. Para obter mais detalhes sobre seu recurso monitorado, é possível clicar em um item do navegador ou em link nas visualizações de painel. Considere, por exemplo, que seu aplicativo tenha um tempo de resposta lento. O problema é revelado no painel. A partir do painel, é possível seguir o problema até a origem clicando nos links para descobrir a causa: alto uso de CPU em um sistema devido a um processo fora de coltrole.

Para obter mais informações sobre o uso de painéis no Console do Cloud APM, consulte Capítulo 10, “Usando os painéis”, na página 1079.



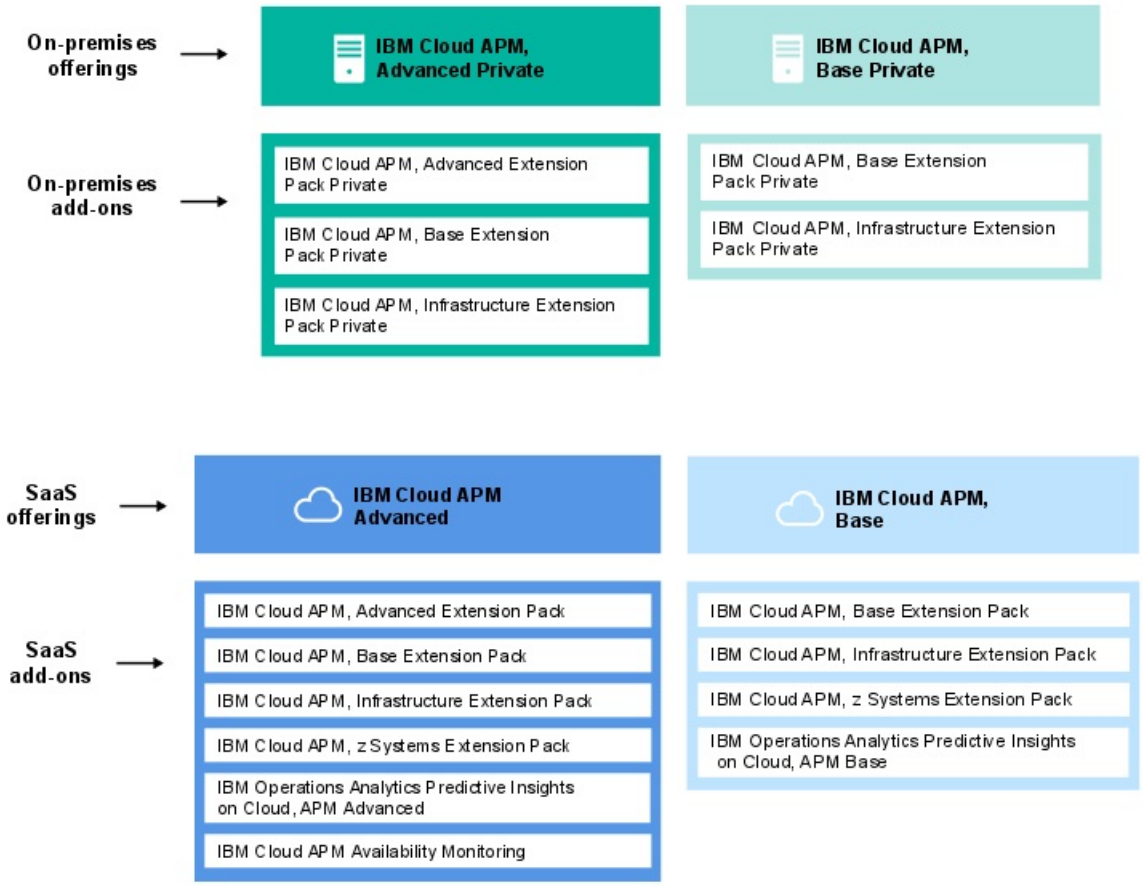
Ofertas e complementos

O IBM Cloud Application Performance Management contém duas ofertas e múltiplos complementos. As ofertas e complementos contêm agentes e coletores de dados. Os complementos específicos podem ser usados com cada oferta.

Para ver quais agentes estão incluídos em uma oferta ou complemento, o agente e os recursos do coletor de dados, consulte “Capacidades” na página 52.

Para cada oferta, os complementos estão disponíveis no IBM Marketplace. O IBM Cloud Application Performance Management, Advanced é a oferta mais abrangente, a que inclui todos os agentes, coletores de dados e páginas do painel. IBM Cloud Application Performance Management, Base é um subconjunto de Cloud APM, Advanced. É possível substituir o Cloud APM, Base pelo Cloud APM, Advanced a qualquer momento. A oferta final instalada após essa substituição é o Cloud APM, Advanced. O diagrama mostra quais complementos estão disponíveis para cada oferta.

Os complementos são os mesmos para todas as ofertas, exceto Monitoramento de Disponibilidade, que é um complemento somente para a oferta Cloud APM, Advanced.



Ofertas

IBM Cloud Application Performance Management, Advanced

Esta oferta é para a experiência do usuário final, rastreamento de transações e monitoramento de recursos de todos os seus componentes de aplicativo. Você tem visibilidade em nível de código de seus aplicativos e do funcionamento de seus servidores de aplicativos. Use os painéis de diagnósticos para localizar gargalos de desempenho no código do aplicativo e para gerenciar seus aplicativos críticos em produção.

A oferta inclui o IBM Cloud Application Performance Management, Base e contém agentes e coletores de dados que são usados para monitorar aplicativos, transações e outros recursos que estão instalados em sua empresa. Para obter uma lista de agentes e coletores de dados nesta oferta, consulte “Capacidades” na página 52.

Com esta oferta, o DevOps possui uma solução completa que fornece visibilidade completa e controle sobre seus aplicativos e infraestrutura. Os proprietários da linha de negócios podem gerenciar aplicativos críticos e a experiência do usuário final em produção. Os desenvolvedores de aplicativos podem visualizar detalhes da transação e diagnosticar problemas do aplicativo.

IBM Cloud Application Performance Management, Base

Esta oferta é para o monitoramento de recursos de infraestrutura, componentes de aplicativos e cargas de trabalho de nuvem. O monitoramento de recursos ajuda a identificar e resolver transações lentas, problemas de capacidade e indisponibilidades. A oferta contém agentes e coletores de dados que são usados para monitorar aplicativos e outros recursos que estão instalados em sua empresa. Para obter uma lista de agentes e coletores de dados nesta oferta, consulte “Capacidades” na página 52.

Com esta oferta, os operadores de TI podem lidar com transações lentas, problemas de capacidade e indisponibilidades.

Complementos

Pacote de Extensão Avançado

Esse pacote de extensão contém o Monitoring Agent for SAP HANA Database, o SAP NetWeaver Java Stack e o Monitoring Agent for RabbitMQ.

Use o SAP HANA Database agent para monitorar o banco de dados do SAP HANA. Use o SAP NetWeaver Java Stack para monitorar o SAP NetWeaver Java Stack. Use o Agente RabbitMQ para monitorar o sistema de mensagens RabbitMQ. Esse pacote de extensão estará disponível se você tiver a oferta IBM Cloud Application Performance Management, Advanced.

Base Extension Pack

Este pacote de extensão contém os seguintes agentes:

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

Use estes agentes para monitorar um banco de dados Cassandra, um cluster Hadoop, recursos do servidor DataStage, aplicativos Microsoft Office 365, servidores Connect Direct e o aplicativo Sterling File Gateway. Este pacote de extensão estará disponível se você tiver uma das ofertas do Cloud APM.

Infrastructure Extension Pack

Este pacote de extensão contém os seguintes agentes:

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

Use o Agente Amazon EC2 para monitorar as instâncias do Amazon EC2. Use o Agente Amazon ELB para monitorar os Balanceadores de Carga Elásticos AWS. Use o Agente Azure Compute para monitorar as máquinas virtuais Azure Compute. Use o Citrix VDI agent para monitorar a infraestrutura da área de trabalho virtual Citrix.

Este pacote de extensão estará disponível se você tiver uma das ofertas do Cloud APM.

z Systems Extension Pack

É possível usar o z Systems Extension Pack para visualizar dados e eventos de monitoramento para componentes de aplicativo do OMEGAMON no Console do Cloud APM. Este pacote de extensão estará disponível se você tiver uma das ofertas do Cloud APM.

Operations Analytics - Predictive Insights

Esse complemento serve para analisar os dados de métrica que são coletados pelo Cloud APM, e para gerar alarmes quando são detectadas anomalias. O complemento estará disponível se você tiver qualquer uma das ofertas Cloud APM.

Monitoramento de Disponibilidade

Este complemento é destinado ao monitoramento da disponibilidade e de desempenho de seus aplicativos da web a partir de vários pontos de presença distribuídos geograficamente. Esse complemento não funciona como uma oferta independente, mas estará disponível se você tiver a oferta IBM Cloud Application Performance Management, Advanced.

Para obter uma visão geral dos recursos em cada oferta, consulte “Detalhes da oferta” na página 48.

Para obter uma descrição de cada agente e coletor de dados e links para informações que são específicas para cada um deles, consulte “PDV” na página 56.

Detalhes da oferta

Alguns recursos estão disponíveis para todas as ofertas e outros estão disponíveis somente para ofertas específicas.

O Tabela 1 na página 48 mostra os principais recursos que estão disponíveis para cada oferta em uma visão rápida.

Tabela 1. Recursos em cada oferta

Recurso	Cloud APM, Advanced (Para DevOps, Desenvolvedores e Linha de negócios)	Cloud APM, Base (Para Operações)
Monitoramento de recursos de aplicativo: Idiomas, middleware (a cobertura varia por oferta).	✓	✓
Monitoramento do sistema operacional: sistemas Linux, UNIX, Windows	✓	✓
Monitoramento de arquivos de log: Use os Agentes de S.O. para monitorar arquivos de log do aplicativo.	✓	✓
Painéis: • Visualizar as KPIs do Tivoli Monitoring e do Cloud APM nos mesmos painéis • Métricas de histórico • Painéis customizáveis	✓	✓
APIs: Gerenciar seu ambiente usando APIs.	✓	✓
Controle de acesso baseado na função: Gerencie o acesso e privilégio de usuários do IBM Cloud Application Performance Management.	✓	✓
Relatório de histórico: Gere relatórios para o desempenho e o tempo de resposta de seus aplicativos que são divididos por transação, dispositivo, navegador e outros (varia por oferta).	✓	✓
IBM Agent Builder: Construa agentes customizados para monitorar qualquer plataforma ou tecnologia.	✓	✓
Monitoramento de recursos de banco de dados: (a cobertura varia por oferta).	✓	✓
Monitoramento de recursos de infraestrutura: Hypervisors, armazenamento e rede (a cobertura varia por oferta).	✓	✓
Monitoramento de recursos de aplicativos comerciais: Aplicativos de negócios e de colaboração (a cobertura varia por oferta).	✓	✓
Monitoramento de tempo de resposta: Veja como o desempenho do aplicativo está afetando seus usuários.	✓	✓

Tabela 1. Recursos em cada oferta (continuação)

Recurso	Cloud APM, Advanced (Para DevOps, Desenvolvedores e Linha de negócios)	Cloud APM, Base (Para Operações)
Integração com análises de dados de procura: Localize os insights para isolar, diagnosticar e resolver problemas rapidamente.	✓	✓
Operations Analytics - Predictive Insights (complemento): Determine anomalias de desempenho do aplicativo antes de afetarem seus usuários.	✓	✓
Monitoramento de experiência do usuário final real Veja a experiência de seus usuários com a infraestrutura para seu dispositivo.	✓	–
Rastreamento de transações: Rastreie transações de ponta a ponta por meio do ambiente de aplicativos. • Topologia do aplicativo: veja como todos os componentes estão conectados em seu ambiente de aplicativos. • Topologia de instância de transação: veja o caminho seguido por meio de seu ambiente para cada instância de uma transação.	✓	–
Diagnóstico detalhado: • Realize drill down de painéis de resumo para visualizar o nível de código, rastreio de pilha e detalhe da consulta SQL para agentes específicos. • Detecte, diagnostique e encerre transações interrompidas ou lentas que ainda estão em andamento.	✓	–
Limites: Detectar comportamentos e condições específicos do aplicativo com base em definições monitoradas ativamente.	✓	✓
Grupos de recursos: Categorize sistemas gerenciados em sua empresa monitorada por seu propósito.	✓	✓

Os seguintes recursos estão disponíveis para todas as ofertas por meio de integração com outros produtos e componentes. Consulte “Integração ” na página 77, e para obter mais detalhes, consulte Capítulo 8, “Integrando com outros produtos e componentes”, na página 949).

- Agentes Tivoli Monitoring e OMEGAMON: use o Hybrid Gateway para recuperar dados de monitoramento e eventos para que essas informações sejam exibidas no Console do Cloud APM.
- Coexistência de Agente: instalar o Cloud APM agentes no mesmo computador onde Tivoli Monitoring agentes estão Instalado .
- Netcool/OMNIbus e outros receptores EIF: encaminhar eventos para o IBM Tivoli Netcool/OMNIbus.
- Alert Notification: receba notificação quando o desempenho do aplicativo exceder os limites.

- IBM Control Desk: abra automaticamente chamados no Control Desk.
- IBM Cloud: Monitorar aplicativos IBM Cloud.

Agentes e coletores de dados

Os agentes e os coletores de dados do IBM Cloud Application Performance Management estão disponíveis nas ofertas e nos complementos.

Muitos recursos em seu ambiente podem ser monitorados pelos agentes. Alguns recursos no IBM Cloud e no local podem ser monitorados por coletores de dados. Os agentes correspondentes existem para todos os coletores de dados, exceto os coletores de dados do J2SE e Python. Para obter uma lista de agentes e coletores de dados e suas descrições, consulte "PDV" na página 56. Para saber os recursos que o agente ou o coletor de dados pode fornecer em cada oferta, consulte "Capacidades" na página 52. Para descobrir o histórico de mudanças de cada agente e coletor de dados, consulte "Histórico de Mudanças" na página 50.

É possível instalar esses agentes ou coletores de dados, dependendo de seu ambiente e requisitos. Os coletores de dados enviam dados diretamente para o Servidor Cloud APM. Quando um agente é configurado, os coletores de dados enviam dados para o agente, que os encaminha ao servidor. Os coletores de dados operam dentro do espaço de processo do aplicativo, enquanto os agentes são executados como um processo separado fora do espaço de processo do aplicativo.

Instale coletores de dados nas situações a seguir:

- Você deseja um processo de instalação mais simples.
- Você usa contêineres.

Instale agentes nas situações a seguir:

- Você deseja maior escalabilidade.
- Você deseja limitar soquetes dos terminais para o servidor.
- Ao incluir um limite no editor de limite, você desejar uma lista limpa que contém somente os atributos para o ambiente que você deseja monitorar. Se você usar um coletor de dados, deverá escolher entre os atributos de vários coletores de dados.
- Você deseja ativar ou desativar algumas das funções de coleta de dados na UI, como diagnósticos, rastreamento de transações ou rastreio de método.
- Você deseja visualizar dados diagnósticos on demand, como solicitações em andamento e dump do heap no horário atual.

Histórico de Mudanças

Localize as informações sobre versões e o histórico de mudanças para cada agente e coletor de dados.

A tabela a seguir lista os nomes de agente e coletor de dados com links de notas técnicas de histórico de mudanças. Clique nos links para visualizar detalhes do histórico de mudanças.

Tabela 2. Histórico de mudanças de agente e coletor de dados

Agentes e coletores de dados	**Links**
Agente Amazon EC2	Histórico de mudanças
Agente Amazon ELB	Histórico de mudanças
Agente Azure Compute	Histórico de mudanças
Agente Cassandra	Histórico de mudanças
Cisco UCS agent	Histórico de mudanças
Citrix VDI agent	Histórico de mudanças

Tabela 2. Histórico de mudanças de agente e coletor de dados (continuação)	
Agentes e coletores de dados	**Links**
DataPower agent	Histórico de mudanças
DataStage agent	Histórico de mudanças
Db2	Histórico de mudanças
Agente do Hadoop	Histórico de mudanças
Agente HMC Base	Histórico de mudanças
Agente do Servidor HTTP	Histórico de mudanças
IBM Cloud agent	Histórico de mudanças
IBM Integration Bus agent	Histórico de mudanças
Monitoramento de Serviço da Internet	Histórico de mudanças
Coletor de dados J2SE	Histórico de mudanças
agente JBoss	Histórico de mudanças
Coletor de dados Liberty	Histórico de mudanças
agente do Linux KVM	Histórico de mudanças
agente do S.O. Linux	Histórico de mudanças
MariaDB agent	Histórico de mudanças
Microsoft Active Directory agent	Histórico de mudanças
Microsoft Cluster Server agent	Histórico de mudanças
Microsoft Exchange Server agent	Histórico de mudanças
Microsoft Hyper-V Server agent	Histórico de mudanças
Microsoft IIS agent	Histórico de mudanças
Microsoft .NET agent	Histórico de mudanças
Microsoft Office 365 agent	Histórico de mudanças
Microsoft SharePoint Server agent	Histórico de mudanças
Microsoft SQL Server agent	Histórico de mudanças
Agente MongoDB	Histórico de mudanças
Agente do MQ Appliance	Histórico de mudanças
Agente MySQL	Histórico de mudanças
Agente NetApp Storage	Histórico de mudanças
Agente Node.js	Histórico de mudanças
Coletor de dados Node.js	Histórico de mudanças
OpenStack agent	Histórico de mudanças
Agente Oracle Database	Histórico de mudanças
Agente PHP	Histórico de mudanças
Agente PostgreSQL	Histórico de mudanças

Tabela 2. Histórico de mudanças de agente e coletor de dados (continuação)	
Agentes e coletores de dados	**Links**
Coletor de dados do Python	Histórico de mudanças
Agente RabbitMQ	Histórico de mudanças
Response Time Monitoring Agent	Histórico de mudanças
Agente Ruby	Histórico de mudanças
Coletor de dados Ruby	Histórico de mudanças
Agente SAP	Histórico de mudanças
SAP HANA Database agent	Histórico de mudanças
SAP NetWeaver Java Stack	Histórico de mudanças
Agente Siebel	Histórico de mudanças
Agente Skype for Business Server	Histórico de mudanças
Agente Sterling Connect Direct	Histórico de mudanças
Agente Sterling File Gateway	Histórico de mudanças
Sybase agent	Histórico de mudanças
Synthetic Playback agent	Histórico de mudanças
Agente Tomcat	Histórico de mudanças
agente de S.O. UNIX	Histórico de mudanças
Agente VMware VI	Histórico de mudanças
Agente WebLogic	Histórico de mudanças
WebSphere Applications agent	Histórico de mudanças
WebSphere Infrastructure Manager agent	Histórico de mudanças
WebSphere MQ agent	Histórico de mudanças
Windows OS agent	Histórico de mudanças

Capacidades

Os recursos do agente e do coletor de dados variam, dependendo de sua oferta. Os principais recursos do agente e do coletor de dados são monitoramento de recursos, rastreamento de transações e diagnósticos. É possível assinar qualquer uma das ofertas e complementos no IBM Cloud Application Performance Management. Ofertas específicas são necessárias para complementos.

Cada agente e coletor de dados monitora os recursos para os quais o agente ou o coletor de dados é nomeado, por exemplo, o Monitoring Agent for Cisco UCS monitora recursos do Cisco UCS.

Dependendo se você é um desenvolvedor, nas operações, ou um proprietário de linha de negócios, usa diferentes recursos do Cloud APM.

- O recurso de monitoramento de recurso inclui monitoramento do tempo de resposta, monitoramento de recurso de aplicativo e monitoramento de recurso de infraestrutura. Todos os agentes e coletores de dados podem fornecer capacidade de monitoramento de recursos.
- O recurso de rastreamento de transação fornece informações de instância de transação e de topologia.
- O recurso de diagnóstico inclui o rastreamento e a análise de solicitações individuais e, quando necessário, chamadas de métodos.

Lembre-se: A capacidade de monitoramento de recursos é comum a todas as ofertas e complementos. Os recursos de diagnósticos e de rastreamento de transação estão disponíveis apenas na oferta Cloud APM, Advanced e em complementos.

Os agentes e coletores de dados para os aplicativos que você deseja monitorar estão disponíveis para download do **Produtos e serviços**. Os agentes levam alguns minutos para instalar. Os coletores de dados não requerem instalação e é preciso somente configurá-los após a conclusão do download. Para obter instruções sobre a instalação de agentes, consulte Capítulo 6, “Instalando os agentes”, na página 117.

O Tabela 3 na página 53 fornece uma lista abrangente dos agentes e coletores de dados, mostra qual oferta ou complemento contém o agente ou coletor de dados e mostra os recursos do agente ou coletor de dados. Quando complementos (como o Infrastructure Extension Pack) são indicados para um agente ou um coletor de dados, eles são necessários. Os agentes e coletores de dados que suportam recursos de rastreamento de transação e/ou diagnósticos também são indicados na coluna do Cloud APM, Advanced.

✓ indica que o agente ou coletor de dados está disponível na oferta e pode fornecer a capacidade de monitoramento de recursos.

— indica que os dados ou o recurso não está disponível nesta oferta ou o complemento não é necessário para o agente ou coletor de dados.

TT indica rastreamento de transação.

DD indica diagnósticos.

Tabela 3. Recursos do agente e do coletor de dados em cada oferta

Agentes e coletores de dados	Cloud APM, BaseCloud APM, Base Private	Cloud APM, Advanced	Complemento (se necessário)
Agente Amazon EC2	✓	✓	Infrastructure Extension Pack
Agente Amazon ELB	✓	✓	Infrastructure Extension Pack
Agente Azure Compute	✓	✓	Infrastructure Extension Pack
Agente Cassandra	✓	✓	Base Extension Pack
Cisco UCS agent	✓	✓	—
Citrix VDI agent	✓	✓	Infrastructure Extension Pack
Db2	✓	✓	—
DataPower agent	✓	✓ TT	—
DataStage agent	✓	✓	Base Extension Pack
Agente do Hadoop	✓	✓	Base Extension Pack
Agente HMC Base	✓	✓	—

Tabela 3. Recursos do agente e do coletor de dados em cada oferta (continuação)			
Agentes e coletores de dados	**Cloud APM, BaseCloud APM, Base Private**	**Cloud APM, Advanced**	**Complemento (se necessário)**
Agente do Servidor HTTP	✓	✓ TT	—
IBM Cloud agent	✓	✓	Infrastructure Extension Pack
IBM Integration Bus agent	—	✓ TT	—
Monitoramento de Serviço da Internet	—	—	Base Extension Pack
Coletor de dados J2SE para aplicativos no local	—	✓ TT DD	—
agente JBoss	✓	✓ TT DD	—
Coletor de dados Liberty Para aplicativos IBM Cloud e no local	—	✓ TT DD	—
agente do Linux KVM	✓	✓	—
agente do S.O. Linux	✓	✓	—
Microsoft Active Directory agent	✓	✓	—
Microsoft Cluster Server agent	✓	✓	—
Microsoft Exchange Server agent	✓	✓	—
Microsoft Hyper-V Server agent	✓	✓	—
Microsoft IIS agent	✓	✓	—
Microsoft .NET agent	✓	✓ TT DD	—
Microsoft Office 365 agent	✓	✓	Base Extension Pack
Microsoft SharePoint Server agent	✓	✓	—
Microsoft SQL Server agent	✓	✓	—
Agente MongoDB	✓	✓	—
Agente do MQ Appliance	—	✓	—
Agente MySQL	✓	✓	—
Agente NetApp Storage	✓	✓	—
Agente Node.js	✓	✓ DD	—

Tabela 3. Recursos do agente e do coletor de dados em cada oferta (continuação)			
Agentes e coletores de dados	**Cloud APM, BaseCloud APM, Base Private**	**Cloud APM, Advanced**	**Complemento (se necessário)**
Coletor de dados Node.js Para aplicativos IBM Cloud e no local	—	✓ TT DD	—
OpenStack agent	✓	✓	—
Agente Oracle Database	✓	✓	—
Agente PHP	✓	✓	—
Agente PostgreSQL	✓	✓	—
Coletor de dados do Python Para aplicativos IBM Cloud e no local	✓	✓ DD	—
Agente RabbitMQ	—	✓	Pacote de Extensão Avançado
Response Time Monitoring Agent	✓	✓ TT	—
Agente Ruby	✓	✓ DD	—
Coletor de dados Ruby para aplicativos do IBM Cloud	—	✓ DD	—
Agente SAP	—	✓	—
SAP HANA Database agent	—	✓	Pacote de Extensão Avançado
SAP NetWeaver Java Stack	—	✓ TT DD	Pacote de Extensão Avançado
Agente Siebel	✓	✓	—
Agente Skype for Business Server (anteriormente conhecido como agente Microsoft Lync Server)	✓	✓	—
Agente Sterling Connect Direct	✓	✓	Base Extension Pack
Agente Sterling File Gateway	✓	✓	Base Extension Pack
Sybase agent	✓	✓	—
Agente Tomcat	✓	✓ TT	—
agente de S.O. UNIX	✓	✓	—
Agente VMware VI	✓	✓	—

Tabela 3. Recursos do agente e do coletor de dados em cada oferta (continuação)			
Agentes e coletores de dados	**Cloud APM, BaseCloud APM, Base Private**	**Cloud APM, Advanced**	**Complemento (se necessário)**
Agente WebLogic	✓	✓ TT DD	—
WebSphere Applications agent	✓	✓ TT DD	—
WebSphere Infrastructure Manager agent	✓	✓	—
WebSphere MQ agent	—	✓ TT	—
Windows OS agent	✓	✓	—

Para obter informações adicionais sobre se o rastreamento de transação ou diagnósticos são ativados por padrão para o agente ou coletor de dados, consulte Ativação de rastreamento de transação para a tabela de agentes e coletores de dados. Para obter informações sobre os painéis de diagnósticos predefinidos, consulte Painéis de diagnósticos de agentes e coletores de dados.

PDV

As descrições dos agentes e coletores de dados fornecem informações sobre o que cada um desses componentes monitora e links para mais informações sobre cada componente.

Cada agente e coletor de dados tem um número de versão, que muda cada vez que o agente ou o coletor de dados é atualizado. Em qualquer liberação, novos agentes e coletores de dados podem ser incluídos e os agentes e coletores de dados existentes podem ser atualizados. Se você não tiver a versão mais recente de um agente ou coletor de dados, considere atualizá-la. Para obter informações sobre como verificar a versão de um agente ou coletor de dados em seu ambiente, consulte Comando de versão do agente.

A descrição de cada agente e coletor de dados contém links para os seguintes tipos de detalhes sobre estes componentes:

- Configuração do agente ou coletor de dados e outras informações sobre recursos específicos do agente ou coletor de dados
- PDF de referência que contém descrições de painéis, widgets de grupo, limites, conjuntos de dados e atributos (métricas e KPIs) do agente ou coletor de dados do Cloud APM

Para links para a documentação de agentes do IBM Tivoli Monitoring V6 e V7 que podem coexistir com agentes e o coletor de dados do Cloud APM V8, consulte Tabela 236 na página 951.

Monitoramento do Amazon EC2

O Monitoring Agent for Amazon EC2 fornece um ponto central de monitoramento para o funcionamento, a disponibilidade e o desempenho do Amazon Elastic Compute Cloud (EC2) (EC2). O agente exibe um conjunto abrangente de métricas para ajudá-lo a tomar decisões informadas sobre seu ambiente EC2, incluindo utilização da CPU, utilização do Elastic Block Store (EBS), utilização de rede, atualizações de manutenção do Amazon Web Services (AWS) e desempenho do disco.

- Para obter informações sobre como configurar o agente após a instalação, consulte “Configurando o monitoramento do Amazon EC2 monitoring” na página 187.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente Amazon EC2 Reference.

Monitoramento do Balanceador de Carga Elástico AWS

O Agente Amazon ELB fornece um ponto central de monitoramento para o funcionamento, disponibilidade e desempenho de seus Balanceadores de Carga Elásticos AWS. O agente exibe um

conjunto abrangente de métricas para cada aplicativo de tipo de balanceador de carga, de rede e clássico - para ajudá-lo a tomar decisões informadas sobre o ambiente do Balanceador de Carga Elástico AWS.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Balanceador de Carga Elástico AWS" na página 195.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente Amazon ELB Reference.

Monitoramento do Azure Compute

O Agente Azure Compute fornece um ponto central de monitoramento para o funcionamento, disponibilidade e desempenho de instâncias do Azure Compute. O agente exibe um conjunto abrangente de métricas para ajudá-lo a tomar decisões informadas sobre o ambiente do Azure Compute. Essas métricas incluem o uso de CPU, uso de rede e desempenho do disco.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Azure Compute" na página 200.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente Azure Compute Reference.

Monitoramento do Cassandra

O Monitoring Agent for Cassandra oferece a capacidade para monitorar o cluster Cassandra. É possível coletar e analisar informações sobre os nós, keyspaces e famílias de colunas do cluster Cassandra.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Cassandra" na página 210.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente Cassandra Reference.

Monitoramento do Cisco UCS

O Monitoring Agent for Cisco UCS fornece um ambiente para monitorar o funcionamento, a rede e o desempenho do Cisco UCS. O agente Cisco UCS fornece uma maneira abrangente de coletar e analisar informações que são específicas para o Cisco UCS e necessárias para detectar problemas antecipadamente e evitá-los.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Cisco UCS" na página 213.
- Para obter informações sobre os painéis, limites e atributos, consulte o Cisco UCS agent Reference.

Monitoramento do Citrix Virtual Desktop Infrastructure

O Monitoring Agent for Citrix Virtual Desktop Infrastructure fornece um ponto central de monitoramento para o funcionamento, a disponibilidade e o desempenho do Citrix Virtual Desktop Infrastructure. O agente exibe um conjunto abrangente de métricas para ajudá-lo a tomar decisões informadas sobre seus recursos XenDesktop ou XenApp, incluindo sites, máquinas, aplicativos, desktops, sessões, usuários e mais.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Citrix Virtual Desktop Infrastructure" na página 220.
- Para obter informações sobre os painéis, limites e atributos, consulte o Citrix VDI agent Reference.

Monitoramento do DataPower

O Monitoring Agent for DataPower fornece um ponto central de monitoramento para o DataPower Appliances no seu ambiente corporativo. É possível identificar e receber as notificações sobre os problemas comuns com os dispositivos. O agente também fornece informações sobre desempenho, recurso e carga de trabalho para os dispositivos.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o DataPower agent" na página 238.
- Para obter informações sobre os painéis, limites e atributos, consulte o DataPower agent Reference.

- Para obter informações sobre monitoramento de dispositivos DataPower como parte de Pilha de integração IBM, consulte "monitorando a Pilha de integração IBM" na página 95.

Monitoramento do Db2

O Monitoring Agent for Db2 oferece um ponto central de monitoramento para o ambiente do Db2. É possível monitorar muitos servidores a partir de um único console do IBM Performance Management, com cada servidor monitorado por um agente Db2. É possível coletar e analisar informações em relação a aplicativos, bancos de dados e recursos do sistema.

- Para obter informações antes de fazer upgrade para uma nova versão do agente, consulte "Agentes em AIX: Parando o agente e executando slibclean antes de fazer upgrade" na página 1142
- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Db2 " na página 242.
- Para obter informações sobre os painéis, limites e atributos, consulte o Db2 Reference.
- Para obter informações sobre o monitoramento de transações do banco de dados como parte do IBM Pilha de aplicativos Java, consulte "Monitorando o IBM Pilha de aplicativos Java" na página 88.

Monitoramento do Hadoop

O Monitoring Agent for Hadoop fornece recursos para monitorar o cluster Hadoop em sua organização. É possível usar o agente para coletar e analisar informações sobre o cluster Hadoop, como status de nós de dados e Java Virtual Machine, informações de heap e não heap de memória e informações sobre nós Hadoop, sistemas de arquivo e filas.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Hadoop" na página 252.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente do Hadoop Reference.

Monitoramento do HMC Base

O Monitoring Agent for HMC Base fornece o recurso para monitorar o Hardware Management Console (HMC). O agente monitora a disponibilidade e o funcionamento dos recursos do HMC: cPU, memória, armazenamento e rede. O agente também relata no HMC o inventário e a configuração de servidores Power, conjuntos de CPUs e LPARs. A utilização da CPU do servidores Power, LPARs e conjuntos é monitorada usando os dados de amostra de desempenho do HMC.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do HMC Base" na página 261.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente HMC Base Reference.

Monitoramento do Servidor HTTP

O Monitoring Agent for HTTP Server coleta dados de desempenho sobre o IBM HTTP Server. Por exemplo, informações do servidor, como status e tipo de serviço, o número de erros do servidor e o número de logins bem-sucedidos e com falha para o servidor são mostrados. Um coletor de dados reúne dados que são enviados para o agente HTTP Server. O agente é executado no mesmo sistema que o IBM HTTP Server por ele monitorado. Cada servidor monitorado é registrado como um subnó. O módulo Tempo de Resposta do IBM HTTP Server é instalado com o agente HTTP Server. Quando você usa o agente HTTP Server com o agente Response Time Monitoring, o agente WebSphere Application e um agente de banco de dados, é possível ver informações de monitoramento de transação do navegador para o banco de dados para a pilha de aplicativos IBM Java.

- Antes de iniciar a instalação do agente, consulte Pré-instalação em sistemas AIX - Agente do Servidor HTTP e Pré-instalação em sistemas Linux - Agente do Servidor HTTP.
- Para obter instruções sobre como revisar as configurações do coletor de dados e ativar o coletor de dados após a instalação do agente, consulte "Configurando o monitoramento do Servidor HTTP" na página 266.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente do Servidor HTTP Reference.

- Para obter informações sobre o monitoramento de transações do HTTP Server como parte do IBM Pilha de aplicativos Java, consulte “Monitorando o IBM Pilha de aplicativos Java” na página 88.

Monitoramento do IBM Cloud

O Monitoring Agent for IBM Cloud coleta as métricas e o inventário de máquina virtual de sua conta do IBM Cloud (Softlayer). Use o agente IBM Cloud para rastrear quantos dispositivos virtuais você tem configurados e em execução no IBM Cloud. É possível ver quais recursos são alocados para cada dispositivo virtual na página de painel detalhada, que também mostra informações como o datacenter em que um dispositivo está localizado, o sistema operacional e a largura da banda da rede pública projetada para o mês.

- Para obter informações sobre como configurar o agente após a instalação, consulte Configurando o monitoramento do IBM Cloud.
- Para obter informações sobre os painéis, limites e atributos, consulte o IBM Cloud agent Reference.

Monitoramento do IBM Integration Bus

O Monitoring Agent for IBM Integration Bus é uma ferramenta de monitoramento e gerenciamento que fornece os meios para verificar, analisar e ajustar topologias do message broker que estão associadas aos produtos IBM WebSphere Message Broker e IBM Integration Bus.

- Para obter informações sobre como configurar o agente após a instalação, consulte “ Configurando o monitoramento do IBM Integration Bus ” na página 274.
- Para obter informações sobre os painéis, limites e atributos, consulte o IBM Integration Bus agent Reference.
- Para obter informações sobre o monitoramento de brokers IBM Integration Bus como parte do Pilha de integração IBM, consulte “monitorando a Pilha de integração IBM” na página 95.

Monitoramento do InfoSphere DataStage

O agente de monitoramento para InfoSphere DataStage monitora a disponibilidade, o uso de recursos e o desempenho do DataStage Server. O agente monitora o status de funcionamento dos nós e tarefas do mecanismo. É possível analisar as informações que o agente coleta e executar as ações apropriadas para resolver problemas no DataStage Server.

- Para obter informações sobre como configurar o agente após a instalação, consulte Configurando o monitoramento do InfoSphere DataStage.
- Para obter informações sobre os painéis, limites e atributos, consulte o DataStage agent Reference.

Monitoramento de Serviço da

As ofertas do Monitoramento de Serviço da Internet para determinar se um serviço específico está sendo executado adequadamente identificam áreas de problemas e relatam o desempenho do serviço medido com relação aos Acordos de Nível de Serviço. O agente de Monitoramento de Serviço da Internet funciona emulando as ações de um usuário real. Ele pesquisa ou testa regularmente serviços de Internet para verificar seu status e seu desempenho.

- Para obter informações sobre como configurar o agente após a instalação, consulte “Configurando o agente nos sistemas Windows” na página 446
- Para obter informações sobre os painéis, limites e atributos, consulte Referência do agente Monitoramento de Serviço da Internet

Monitoramento do coletor de dados J2SE

O coletor de dados J2SE coleta dados diagnósticos de monitoramento de recursos e de detalhamento para aplicativos Java. Os dados diagnósticos de detalhamento são mostrados nos painéis com base em solicitações e informações agregadas para suportar várias visualizações de drill-down. Ambos o monitoramento de recurso e os diagnósticos de detalhamento são suportados, o que ajuda a detectar, isolar e diagnosticar problemas com aplicativos Java. É possível configurar o coletor de dados para diagnosticar solicitações lentas.

- Para obter informações sobre como configurar o coletor de dados, consulte Configurando o coletor de dados do J2SE.

- Para obter informações sobre os painéis, limites e atributos, consulte Referência do coletor de dados J2SE.

Monitoramento do JBoss

O Monitoring Agent for JBoss monitora os recursos de servidores de aplicativos JBoss e a plataforma do JBoss Enterprise Application. Use os painéis fornecidos com o agente JBoss para identificar os aplicativos mais lentos, as solicitações mais lentas, gargalos do conjunto de encadeamentos, problemas de memória heap da JVM e de coleta de lixo, as sessões mais ocupadas e outros gargalos no servidor de aplicativos JBoss.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do JBoss" na página 456.
- Para obter informações sobre os painéis, limites e atributos, consulte o agente JBoss Reference.

Monitoramento do Linux KVM

O Monitoring Agent for Linux KVM é um agente de diversas instâncias e conexões e suporta conexões com o hypervisor KVM baseado no Linux Corporativo e nos ambientes do Red Hat Enterprise Virtualization Manager (RHEV-M). É possível criar múltiplas instâncias desse agente para monitorar múltiplos hypervisors em um ambiente do hypervisor RHEV-M ou KVM. É possível monitorar as cargas de trabalho virtualizadas e analisar a capacidade de recurso em diferentes máquinas virtuais. Para conectar o agente a uma máquina virtual no ambiente do hypervisor KVM, você deve instalar os pré-requisitos: `libvirt * .rpm` e Korn Shell Interpreter (pdksh). O agente coleta métricas conectando-se remotamente a um hypervisor libvirt que gerencia as máquinas virtuais.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Linux KVM" na página 472.
- Para obter informações sobre os painéis, limites e atributos, consulte o agente do Linux KVM Reference.

Monitoramento do Linux OS

O Monitoring Agent for Linux OS fornece recursos de monitoramento para a disponibilidade, desempenho e uso de recursos do ambiente do S.O. Linux. Esse agente suporta monitoramento contêiner Docker. Por exemplo, são mostradas informações detalhadas, como informações de uso da CPU, de uso de memória, rede e E/S que estão relacionadas ao contêiner do docker. Também são mostradas informações gerais sobre os contêineres do docker em execução no servidor, como o ID do docker e o nome da instância. Além disso, é possível configurar o monitoramento do arquivo de log para monitorar arquivos de log de aplicativo. É possível coletar e analisar informações específicas do servidor, como desempenho do sistema operacional e da CPU, informações de disco e análise de desempenho do Linux, análise do status do processo e desempenho de rede.

- Para obter informações sobre como configurar o monitoramento do arquivo de log após a instalação, consulte "Configurando monitoramento de arquivo de log do OS Agent" na página 633.
- Para obter informações sobre os painéis, limites e atributos, consulte o agente do S.O. Linux Reference.

Monitoramento do MariaDB

O Monitoring Agent for MariaDB oferece um ponto central de gerenciamento para seu ambiente ou aplicativo do MariaDB. O software fornece um meio abrangente de reunir as informações requeridas para detectar problemas antecipadamente e para preveni-los. As informações são padronizadas por meio do sistema. É possível monitorar diversos servidores de um único console. Ao usar o Monitoring Agent for MariaDB, é possível coletar e analisar facilmente informações específicas do MariaDB.
Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do MariaDB" na página 483

Monitoramento do Microsoft Active Directory

O Monitoring Agent for Microsoft Active Directory fornece recursos para monitorar o Active Directory em sua organização. É possível usar o agente para coletar e analisar as informações específicas para o Active Directory, como o status de rede, replicação Sysvol, desempenho da lista de endereços e uso do sistema de diretório.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Microsoft Active Directory" na página 486.
- Para obter informações sobre os painéis, limites e atributos, consulte o Microsoft Active Directory agent Reference.

Monitoramento do Microsoft Cluster Server

O Monitoring Agent for Microsoft Cluster Server fornece recursos para monitorar o Microsoft Cluster Server em sua organização. É possível usar o agente do Microsoft Cluster Server para coletar informações que estão relacionadas à disponibilidade de recursos do cluster, como nível do cluster, nós do cluster, grupos de recursos do cluster, recursos do cluster e redes do cluster. O agente também fornece estatísticas para uso de recursos de cluster, tais como o uso do processador, o uso de memória, o uso de disco e o uso de rede.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Microsoft Cluster Server" na página 493.
- Para obter informações sobre os painéis, limites e atributos, consulte o Microsoft Cluster Server agent Reference.

Monitoramento do Microsoft Exchange Server

O Monitoring Agent for Microsoft Exchange Server fornece recursos para monitorar o funcionamento, disponibilidade e desempenho do Exchange Servers em sua organização. É possível usar o agente do Microsoft Exchange Server para coletar informações específicas do servidor, como tráfego de correio, estado dos bancos de dados da caixa de correio e atividades dos clientes. Além disso, o agente fornece estatísticas sobre o uso do cache, uso do correio, uso do banco de dados e atividades do cliente que ajudam a analisar o desempenho dos Exchange Servers.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Microsoft Exchange" na página 495.
- Para obter informações sobre os painéis, limites e atributos, consulte o Microsoft Exchange Server agent Reference.

Monitoramento do Microsoft Hyper-V Server

O Monitoring Agent for Microsoft Hyper-V Server fornece o recurso para monitorar a disponibilidade e o desempenho de todos os sistemas Hyper-V em sua organização. O Microsoft Hyper-V Server agent fornece informações de configuração, como o número de máquinas virtuais, o estado das máquinas virtuais, o número de discos virtuais alocados, a memória virtual alocada e o número de processadores virtuais alocados. Além disso, o agente fornece estatísticas de uso do processador físico, uso de memória, uso de rede, uso do processador lógico e uso do processador virtual.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Microsoft Hyper-V" na página 508.
- Para obter informações sobre os painéis, limites e atributos, consulte o Microsoft Hyper-V Server agent Reference.

Monitoramento do Microsoft Internet Information Services

O Monitoring Agent for Microsoft Internet Information Services fornece o recurso para monitorar a disponibilidade e o desempenho do Microsoft Internet Information Server. É possível usar o agente do Microsoft Internet Information Server para monitorar detalhes do website, como taxa de solicitações, taxa de transferência de dados, estatísticas de erro e estatísticas de conexões.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Microsoft IIS" na página 512.
- Para obter informações sobre os painéis, limites e atributos, consulte o Microsoft IIS agent Reference.

Monitoramento do Microsoft .NET

O Monitoring Agent for Microsoft .NET monitora aplicativos do Microsoft .NET baseados em Internet Information Services (IIS) e recursos do Microsoft .NET Framework. O componente do coletor de dados coleta dados de solicitações HTTP recebidas. O coletor de dados coleta chamadas de métodos e constrói uma árvore de chamada e coleta o contexto de solicitações e os dados de rastreio da pilha.

Use os painéis fornecidos com o agente Microsoft .NET para identificar os problemas que estão associados ao Microsoft .NET Framework, e também para identificar as solicitações de HTTP mais lentas, de onde é possível realizar drill down para informações de rastreio de pilha para isolar problemas.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Registrando o coletor de dados" na página 522.
- Para obter informações sobre os painéis, limites e atributos, consulte o Microsoft .NET agent Reference.

Monitoramento do Microsoft Office 365

O Monitoring Agent for Microsoft Office 365 oferece a capacidade para monitorar o Microsoft Office 365. É possível coletar e analisar informações sobre o Microsoft Exchange Online, SharePoint Online, Skype for Business e OneDrive for Business.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Microsoft Office 365" na página 531.
- Para obter informações sobre os painéis, limites e atributos, consulte o Microsoft Office 365 agent Reference.

Monitoramento do Microsoft SharePoint Server

O Monitoring Agent para Microsoft SharePoint Server fornece o ambiente para monitorar a disponibilidade, eventos e desempenho do Microsoft SharePoint Server. Use esse agente para reunir dados do Microsoft SharePoint Server e gerenciar operações.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o Microsoft SharePoint Server de monitoramento " na página 536.
- Para obter informações sobre os painéis, limites e atributos, consulte o Microsoft SharePoint Server agent Reference.

Monitoramento do Microsoft SQL Server

O Monitoring Agent for Microsoft SQL Server fornece o recurso para monitorar o Microsoft SQL Server. O agente Microsoft SQL Server oferece um ponto central de gerenciamento para bancos de dados distribuídos. Use os painéis do agente Microsoft SQL Server para monitorar a disponibilidade, desempenho, uso de recursos e o status geral de todas as instâncias do SQL Server que estão sendo monitoradas.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Microsoft SQL Server " na página 539.
- Para obter informações sobre os painéis, limites e atributos, consulte o Microsoft SQL Server agent Reference.

Monitoramento do MongoDB

O Monitoring Agent for MongoDB fornece recursos de monitoramento para o uso, status e desempenho da implementação do ongoDB. É possível coletar e analisar informações como uso de capacidade do banco de dados, porcentagem de conexões abertas, uso de memória, status de instância e tempo de resposta em painéis virtualizados.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do MongoDB" na página 571.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente MongoDB Reference.

Monitoramento do MQ Appliances

O Monitoring Agent for MQ Appliance fornece informações de monitoramento que se concentram no nível do dispositivo do MQ em Dispositivos do MQ, por exemplo, informações de resumo de CPU, memória, armazenamento, sensores e gerenciadores de filas.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do IBM MQ Appliances" na página 289.

- Para obter informações sobre os painéis, limites e atributos, consulte Referência do agente MQ Appliance.

Monitoramento do MySQL

O Monitoring Agent for MySQL fornece recursos de monitoramento para o status, uso e desempenho da implementação do MySQL. É possível coletar e analisar informações, como Bytes recebidos versus enviados, Páginas do buffer pool InnoDB e Desempenho histórico.

- Antes de iniciar a instalação do agente, consulte Pré-instalação em sistemas Linux - Agente MySQL ou Pré-instalação em sistemas Windows - Agente MySQL.
- Para obter informações sobre como configurar o agente após a instalação, consulte “Configurando o monitoramento do MySQL” na página 577.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente MySQL Reference.

Monitoramento de armazenamento do NetApp

O Monitoring Agent for NetApp Storage fornece a capacidade para monitorar os sistemas de armazenamento NetApp usando o NetApp OnCommand Unified Manager (OCUM). É possível coletar e analisar informações sobre as agregações, nós, discos e volumes de sistemas de armazenamento NetApp.

- Para obter informações sobre como configurar o agente após a instalação, consulte “Configurando o monitoramento do NetApp Storage” na página 580.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente NetApp Storage Reference.

Monitoramento do Node.js

O Monitoring Agent for Node.js ou o coletor de dados Node.js independente pode ser usado para medir e coletar dados sobre o desempenho de aplicativos Node.js. Por exemplo, tempos de resposta e rendimento e outras medidas que se relacionam ao uso do recurso são monitoradas e armazenadas para exibição e análise. Para escolher entre o Agente Node.js e o Coletor de dados Node.js, consulte “Configurando o monitoramento do Node.js” na página 586 para obter instruções.

Agente Node.js

- Antes de iniciar a instalação, consulte Pré-instalação em sistemas Linux - Agente Node.js.
- Para obter informações sobre como configurar o agente após a instalação, consulte “Configurando o Agente Node.js” na página 587.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente Node.js Reference.

Coletor de dados Node.js (independente)

O Coletor de dados Node.js monitora os aplicativos IBM Cloud e no local. O monitoramento de recursos e diagnósticos de detalhamento são suportados, o que ajuda a detectar, isolar e diagnosticar problemas dos aplicativos. É possível configurar o coletor de dados para rastrear o desempenho de chamadas de solicitação e de método individuais e usar as informações para diagnosticar solicitações lentas e executar ações de forma apropriada.

IBM Cloud aplicativos

- Para obter informações sobre como configurar o coletor de dados, consulte “Configurando o Coletor de dados Node.js independente para aplicativos IBM Cloud(antigo Bluemix)” na página 593.
- Para obter informações sobre os painéis, limites e atributos, consulte a Referência de coletores de dados.

Aplicativos no local

- Para obter informações sobre como configurar o coletor de dados, consulte “Configurando o Coletor de dados Node.js para aplicativos no local” na página 598.
- Para obter informações sobre os painéis, limites e atributos, consulte a Referência de coletores de dados.

Monitoramento do OpenStack

O Monitoring Agent for OpenStack fornece os recursos para monitorar os aplicativos OpenStack. Use os painéis para visualizar o desempenho dos aplicativos OpenStack, como informações sobre terminais da API, conexão do servidor SSH, processos e hypervisors.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o OpenStack agent" na página 610.
- Para obter informações sobre os painéis, limites e atributos, consulte o OpenStack agent Reference.

Monitoramento do banco de dados Oracle

O Monitoring Agent for Oracle Database fornece capacidades de monitoramento para a disponibilidade, desempenho e uso de recursos do banco de dados Oracle. É possível configurar mais de uma instância do Agente Oracle Database para monitorar diferentes bancos de dados Oracle. A capacidade de monitoramento remoto também é fornecida por esse agente.

- Antes de iniciar a instalação do agente, consulte Pré-instalação em sistemas AIX - Agente Oracle Database, Pré-instalação em sistemas Linux - Agente Oracle Database, ou Pré-instalação em sistemas Windows - Agente Oracle Database (Windows).
- Para obter instruções sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Banco de Dados Oracle" na página 615.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente Oracle Database Reference.
- Para obter informações sobre o monitoramento de transações do banco de dados como parte do IBM Pilha de aplicativos Java, consulte "Monitorando o IBM Pilha de aplicativos Java" na página 88.

Monitoramento do PHP

O Monitoring Agent for PHP monitora aplicativos da web PHP coletando métricas de acesso à web por meio de um servidor da web Apache e de dados de estatísticas de desempenho do MySQL. O agente descobre todos os aplicativos WordPress em um servidor Apache e fornece informações de estatísticas de aplicativo WordPress. Use o agente PHP para monitorar a disponibilidade do servidor da Web, status do servidor Apache e solicitações GET/POST. O agente avalia apenas o desempenho de solicitações PHP em aplicativos WordPress. Carregamento CSS e JS não são avaliados. O agente não usa argumentos de URL para identificar URLs.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do PHP" na página 665.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente PHP Reference.

Monitoramento do PostgreSQL

O Monitoring Agent for PostgreSQL monitora o banco de dados PostgreSQL coletando métricas de PostgreSQL por meio de um driver JDBC. O agente fornece dados sobre o uso de recursos do sistema, a capacidade do banco de dados, as conexões que são usadas, status individual de instâncias em execução, estatísticas para operações, tempo de resposta para instruções de consulta SQL, detalhes de tamanho do banco de dados e informações de bloqueio.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do PostgreSQL" na página 667.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente PostgreSQL Reference.

Monitoramento do Python

O coletor de dados Python monitora os aplicativos IBM Cloud Python e no local. Ambos o monitoramento de recurso e os diagnósticos de detalhamento são suportados, o que fornece dados de monitoramento, como uso da CPU e de memória, coleta de lixo e encadeamentos. É possível configurar o coletor de dados para rastrear o desempenho de chamadas de solicitação e de método individuais e usar as informações para diagnosticar solicitações lentas e executar ações de forma apropriada.

IBM Cloud aplicativos

- Para obter informações sobre como configurar o coletor de dados, consulte "Configurando o coletor de dados Python para aplicativos IBM Cloud" na página 671.
- Para obter informações sobre os painéis, os limites e os atributos, consulte o Referência de coletores de dados.

Aplicativos no local

- Para obter informações sobre como configurar o coletor de dados, consulte "Configurando o Coletor de dados do Python para aplicativos no local" na página 677.
- Para obter informações sobre os painéis, limites e atributos, consulte a Referência do Coletor de Dados.

Monitoramento do RabbitMQ

O Monitoring Agent for RabbitMQ oferece a capacidade de monitorar o cluster RabbitMQ. É possível coletar e analisar informações sobre os nós, filas e canais do cluster RabbitMQ.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do RabbitMQ " na página 682.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente RabbitMQ Reference.

Monitoramento do Tempo de Resposta

O Response Time Monitoring Agent usa o monitoramento de rede para capturar dados de transação de HTTP e HTTPS, como tempos de resposta e códigos de status. Use o agente de Monitoramento do Tempo de Resposta para monitorar o desempenho e a disponibilidade dos aplicativos da web para os usuários, incluindo solicitações de transações, aplicativos e informações do servidor. Use também esse agente para monitorar dispositivos e informações de sessão.

- Antes de iniciar a instalação do Agente Response Time Monitoring, consulte Pré-instalação em sistemas AIX - Agente Response Time Monitoring, Pré-instalação em sistemas Linux - Agente Response Time Monitoring ou Pré-instalação em sistemas Windows - Agente Response Time Monitoring.
- Para obter informações sobre como configurar o agente após a instalação, consulte "JavaScript Injection" na página 689.
- Para obter informações sobre os painéis, limites e atributos, consulte o Transaction Monitoring Reference.
- Para obter informações sobre o uso do Response Time Monitoring como parte do IBM Pilha de aplicativos Java, consulte "Monitorando o IBM Pilha de aplicativos Java" na página 88.

Monitoramento do Ruby

O Monitoring Agent for Ruby ou os coletores de dados Ruby independentes monitoram o desempenho dos aplicativos Ruby on Rails, incluindo as estatísticas de configuração e de tráfego de solicitações. Também é possível usar a função de diagnóstico para obter uma visualização mais profunda em cada aplicativo.

O Coletor de dados Ruby monitora apenas os aplicativos IBM Cloud.

Agente Ruby

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Ruby" na página 718.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente Ruby Reference.

Coletor de dados Ruby (independente)

É possível usar o coletor de dados Ruby para monitorar os aplicativos do IBM Cloud. Ambos o monitoramento de recursos e os diagnósticos de detalhamento são suportados, o que ajuda a detectar, isolar e diagnosticar problemas dos aplicativos. É possível configurar o coletor de dados para rastrear o desempenho de chamadas de solicitação e de método individuais e usar as informações para diagnosticar solicitações lentas e executar ações de forma apropriada.

IBM Cloud aplicativos

- Para obter informações sobre como configurar o coletor de dados, consulte Configurando o coletor de dados Ruby.
- Para obter informações sobre os painéis, os limites e os atributos, consulte o Referência de coletores de dados.

Monitoramento de aplicativos SAP

O Monitoring Agent for SAP Applications fornece o recurso para monitorar os aplicativos SAP que são executados na pilha do Advanced Business Application Programming (ABAP). O agente também monitora o SAP Solution Manager, que é uma ferramenta de gerenciamento de ciclo de vida SAP, e o SAP NetWeaver Process Integration (SAP PI), que é um software de integração corporativo para SAP. Ele oferece um ponto central de gerenciamento para reunir informações que você precisa para detectar problemas antecipadamente e efetuar etapas para impedir que eles ocorram novamente. Ele permite o gerenciamento efetivo de sistemas em liberações, aplicativos e componentes do SAP; e em bancos de dados subjacentes, sistemas operacionais e interfaces externas.

- Para obter informações sobre como configurar o agente após a instalação, consulte “Configurando o monitoramento do SAP” na página 729.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente SAP Reference.

Monitoramento do SAP HANA Database

O Monitoring Agent for SAP HANA Database monitora a disponibilidade, o uso de recursos e o desempenho do banco de dados SAP HANA. O agente pode monitorar cenários de implementação HANA como um único host - único banco de dados, único host - diversos bancos de dados locatários, diversos hosts - único banco de dados e diversos hosts - diversos bancos de dados locatários. É possível analisar as informações que o agente coleta e executar as ações apropriadas para resolver problemas no banco de dados SAP HANA.

- Antes de iniciar a instalação do agente, consulte Pré-instalação nos sistemas AIX - SAP HANA Database agent ou Pré-instalação nos sistemas Linux - SAP HANA Database agent ou Pré-instalação nos sistemas Windows - SAP HANA Database agent.
- Para obter informações sobre como configurar o agente após a instalação, consulte “Configurando o monitoramento do SAP HANA Database” na página 763.
- Para obter informações sobre os painéis, limites e atributos, consulte o SAP HANA Database agent Reference.

Monitoramento do SAP NetWeaver Java Stack

O Monitoring Agent for SAP NetWeaver Java Stack monitora a disponibilidade, o uso de recursos e o desempenho do SAP NetWeaver Java Stack. O agente pode monitorar cenários de implementação do SAP NetWeaver Java Stack, como único host - única instância, único host - várias instâncias, vários hosts - únicas instâncias e vários hosts - várias instâncias. É possível analisar as informações que o agente coleta e executar as ações apropriadas para resolver problemas no SAP NetWeaver Java Stack.

- Para obter informações sobre como configurar o agente após a instalação, consulte “Configurando o monitoramento do SAP NetWeaver Java Stack” na página 765.
- Para obter informações sobre os painéis, limites e atributos, consulte o SAP NetWeaver Java Stack Reference.

Monitoramento do Siebel

O Monitoring Agent for Siebel fornece um ponto central de monitoramento para recursos do Siebel, que inclui estatísticas do Siebel, sessões do usuário, componentes, tarefas, servidor de aplicativos, Siebel Gateway Name Server, uso da CPU e da memória do processo e monitoramento de evento de log.

- Para obter informações sobre como configurar o agente após a instalação, consulte “Configurando o monitoramento do Siebel” na página 772.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente Siebel Reference.

Monitoramento do Skype for Business Server (anteriormente conhecido como Microsoft Lync Server)

O Monitoring Agent for Skype for Business Server fornece o recurso para monitorar o funcionamento, disponibilidade e desempenho do Skype for Business Server. É possível usar o agente Skype for Business Server para coletar informações específicas do servidor, como latência, transações sintéticas, operações de gravação de serviço de gravação de detalhes de chamada (CDR), estado de solicitações reguladas e peers de protocolo de inicialização de sessão (SIP). Além disso, o agente fornece estatísticas de uso históricas de mensagem instantânea e do servidor de mediação para ajudar a analisar o desempenho do Lync ou do Skype for Business Servers.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Skype for Business Server (anteriormente conhecido como Microsoft Lync Server)" na página 515.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente Skype for Business Server Reference.

Monitoramento do Sterling Connect Direct

O Monitoring Agent for Sterling Connect Direct fornece monitoramento de servidores Connect Direct. Ele fornece o funcionamento e desempenho dos servidores. Além disso, fornece a análise da atividade de transferência de arquivos.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Sterling Connect Direct" na página 784.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente Sterling Connect Direct Reference.

Monitoramento do Sterling File Gateway

O Monitoring Agent for Sterling File Gateway monitora o aplicativo Sterling File Gateway, que é usado para transferir arquivos entre parceiros internos e externos usando diferentes protocolos, diferentes convenções de nomenclatura de arquivo e diferentes formatos de arquivos. Ele também suporta o recurso de monitoramento remoto.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Sterling File Gateway" na página 786.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente Sterling File Gateway Reference.

Monitoramento do Sybase Server

O Monitoring Agent for Sybase Server oferece um ponto central de gerenciamento para bancos de dados distribuídos. Ele coleta as informações necessárias para que os administradores do banco de dados e do sistema examinem o desempenho do sistema do servidor Sybase, detectem problemas antecipadamente e os evitem.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Sybase Server" na página 793.
- Para obter informações sobre os painéis, limites e atributos, consulte a Sybase agentReferência.

Monitoramento do Tomcat

O Monitoring Agent for Tomcat monitora os recursos de servidores de aplicativos Tomcat. Use os painéis fornecidos com o agente Tomcat para identificar os aplicativos mais lentos, as solicitações mais lentas, gargalos do conjunto de encadeamentos, problemas de memória heap de JVM e de coleta de lixo, as sessões mais ocupadas e outros gargalos no servidor de aplicativos Tomcat.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do Tomcat" na página 801.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente Tomcat Reference.

Monitoramento do S.O. UNIX

O Monitoring Agent for UNIX OS fornece recursos de monitoramento para a disponibilidade, desempenho e uso de recursos do ambiente do S.O. UNIX. (Somente sistemas operacionais AIX e Solaris. Consulte Requisitos do sistema no APM Developer Center). Além disso, você pode configurar o monitoramento do arquivo de log para monitorar arquivos do log de aplicativo. É possível coletar e

analisar informações específicas do servidor, como desempenho do sistema operacional e da CPU, informações do disco do UNIX e análise de desempenho, análise de status do processo e desempenho de rede.

- Para obter informações sobre como configurar o monitoramento do arquivo de log após a instalação, consulte "Configurando monitoramento de arquivo de log do OS Agent" na página 633.
- Para obter informações sobre os painéis, limites e atributos, consulte o agente de S.O. UNIX Reference.

Monitoramento do VMware VI

O Monitoring Agent for VMware VI monitora o VMware Virtual Infrastructure conectando-se ao VMware Virtual Center. É possível usar o agente VMware VI para visualizar o resumo de status para clusters e monitorar vários componentes, como clusters, máquinas virtuais, armazenamentos de dados e servidores ESX a partir de um único console.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do VMware VI" na página 809.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente VMware VI Reference.

Monitoramento do WebLogic

O Monitoring Agent for WebLogic fornece um ponto central de monitoramento para o funcionamento, a disponibilidade e o desempenho do ambiente do servidor WebLogic. O agente exibe um conjunto abrangente de métricas para ajudá-lo a tomar decisões informadas sobre seus recursos WebLogic, incluindo Java virtual machines (JVMs), serviço de sistema de mensagens Java (JMS), Java Database Connectivity (JDBC).

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do WebLogic" na página 817.
- Para obter informações sobre os painéis, limites e atributos, consulte o Agente WebLogic Reference.

Monitoramento de Aplicativos WebSphere

O Monitoring Agent for WebSphere Applications com o coletor de dados integrado ou o coletor de dados Liberty independente monitora os recursos dos Servidores de Aplicativos WebSphere. Esses componentes de monitoramento podem ser configurados para fazer o seguinte:

- Reunir as métricas PMI para o monitoramento de recursos por meio de uma interface JMX no servidor de aplicativos.
- Reunir as métricas de desempenho de solicitação agregada.
- Controlar o desempenho de solicitação individual e de chamadas de método.

Os dados de monitoramento são exibidos nos painéis. É possível usar os painéis fornecidos para isolar áreas específicas de problemas do servidor de aplicativos. Realize drill down para determinar se um problema está em um recurso subjacente ou se está relacionado ao código do aplicativo.

Para obter informações sobre se deve usar o agente ou um dos coletores de dados, consulte "Configurando o monitoramento de aplicativos WebSphere" na página 833.

Agente de Aplicativos WebSphere e coletor de dados integrado

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o coletor de dados para WebSphere Applications agent" na página 833.
- Para obter informações sobre os painéis, limites e atributos, consulte o WebSphere Applications agent Reference.
- Para obter informações sobre o monitoramento de transações do WebSphere Application Server como parte do IBM Pilha de aplicativos Java, consulte "Monitorando o IBM Pilha de aplicativos Java" na página 88.

Coletor de dados Liberty (independente)

É possível usar o coletor de dados Liberty para monitorar o perfil do WebSphere Liberty no IBM Cloud ou para monitorar o WebSphere Application Server Liberty no Linux for System x. Monitoramento de recursos, diagnósticos e rastreamento de transações são todos suportados, o que ajuda a detectar, isolar e diagnosticar problemas dos aplicativos. É possível configurar o coletor de dados independente para rastrear o desempenho de solicitação individual e de chamadas de método e usar as informações para diagnosticar solicitações lentas e executar ações de forma correspondente.

IBM Cloud aplicativos

- Para obter informações sobre como configurar o coletor de dados, consulte "Configurando o coletor de dados Liberty para aplicativos IBM Cloud" na página 884.
- Para obter informações sobre os painéis, os limites e os atributos, consulte o Referência de coletores de dados.

Aplicativos no local (somente Linux for System x)

- Para obter informações sobre como configurar o coletor de dados, consulte "Configurando o coletor de dados Liberty para aplicativos no local" na página 880.
- Para obter informações sobre os painéis, os limites e os atributos, consulte o Referência de coletores de dados.

Monitoramento do WebSphere Infrastructure Manager

O Monitoring Agent for WebSphere Infrastructure Manager fornece os recursos de monitoramento para o WebSphere Application Server Deployment Manager and Node Agent, incluindo o status do servidor, recursos e transações. É possível usar os dados coletados pelo agente WebSphere Infrastructure Manager para analisar o desempenho do Deployment Manager e do Node Agent, e se ocorreu um problema.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento do WebSphere Infrastructure Manager" na página 930.
- Para obter informações sobre os painéis, limites e atributos, consulte o WebSphere Infrastructure Manager agent Reference.

Monitoramento do WebSphere MQ

Com o Monitoring Agent for WebSphere MQ, é possível coletar e analisar facilmente os dados que são específicos para o WebSphere MQ para os gerenciadores de filas a partir de um único ponto de vantagem. É possível então rastrear tendências nos dados que são coletados e resolver problemas do sistema usando os painéis predefinidos.

- Para obter informações sobre como configurar o agente após a instalação, consulte "Configurando o monitoramento WebSphere MQ" na página 930.
- Para obter informações sobre os painéis, limites e atributos, consulte o WebSphere MQ agent Reference.
- Para obter informações sobre o monitoramento de filas de mensagens como parte do Pilha de integração IBM, consulte "monitorando a Pilha de integração IBM" na página 95.

Monitoramento do S.O. Windows

O Monitoring Agent for Windows OS fornece recursos de monitoramento para a disponibilidade, desempenho e uso de recursos do ambiente do S.O. Windows. Além disso, é possível configurar o monitoramento do arquivo de log para monitorar arquivos de log de aplicativo. É possível coletar e analisar informações específicas de servidor, como sistema operacional e desempenho de CPU, informações de disco e análise de desempenho, análise de status do processo, dados de sessão da Internet, informações de logs monitorados, estatísticas do servidor de Internet, estatísticas de enfileiramento de mensagem, dados de status da impressora e de tarefas, estatísticas de Serviços de acesso remoto e informações de serviços. O serviço KNTCMA_FCProvider é instalado com o agente.

- Para obter informações sobre como configurar o monitoramento do arquivo de log após a instalação, consulte "Configurando monitoramento de arquivo de log do OS Agent" na página 633.

- Para obter informações sobre os painéis, limites e atributos, consulte o Windows OS agent Reference.

Recursos

Os recursos-chave variam por oferta. Alguns recursos estão disponíveis em uma ou ambas as ofertas, em um complemento, ou por meio da integração com outros produtos e componentes.

Monitoramento de recursos de aplicativo
Use agentes de monitoramento de recursos para monitorar idiomas e middleware. A cobertura varia por oferta. Consulte “Capacidades” na página 52.

Monitoramento do sistema operacional
Use agentes de monitoramento de recursos para monitorar os sistemas operacionais Linux, UNIX e Windows. Consulte “Capacidades” na página 52.

Monitoramento de arquivo de log
Os agentes do sistema operacional contêm um recurso para monitorar arquivos de log de aplicativo. Esse recurso inclui a capacidade de configurar o monitoramento de arquivo de log com base em expressões regulares.

Para compatibilidade, o agente do sistema operacional consome as seguintes informações e formatos:

- Informações de configuração e o arquivo de formato que foi usado pelo IBM Tivoli Monitoring Log File Agent V6.x.
- Informações de configuração e sequências de formatos que foram usadas pelo Tivoli Event Console Log File Adapter

Essas sequências de formato permitem que o agente filtre os dados do log de acordo com padrões no arquivo de formato e envie somente os dados relevantes para um consumidor de evento. O agente de S.O. envia dados para o Servidor Cloud APM ou pelo Event Integration Facility (EIF) para qualquer receptor EIF, como o Netcool/OMNIbus Probe for Tivoli EIF.

Painéis
O **Application Performance Dashboard** fornece um status de alto nível dos aplicativos em seu ambiente. Visualize áreas de interesse, selecionando no navegador ou clicando em uma caixa de resumo para fazer drill down para o nível seguinte.

Para saber sobre os recursos disponíveis em cada nível de painel, consulte “Todos os Meus Aplicativos - Application Performance Dashboard” na página 1079, “Aplicativo - Application Performance Dashboard” na página 1082 e “Grupo e instância - Application Performance Dashboard” na página 1087.

Visualize KPIs dos domínios do Tivoli Monitoring e do Cloud APM nos mesmos painéis
Em um ambiente que inclui produtos IBM Tivoli Monitoring e IBM Cloud Application Performance Management, é possível instalar o IBM Cloud Application Performance Management Hybrid Gateway para fornecer uma visualização consolidada dos sistemas gerenciados de ambos os domínios. Para visualizar o ambiente híbrido no Console do Cloud APM, é necessário criar um grupo de sistemas gerenciados, instalar o Hybrid Gateway no ambiente do Tivoli Monitoring e configurar comunicações com o Hybrid Gateway.

Para obter mais informações, consulte “Integrando com o IBM Tivoli Monitoring V6.3 ” na página 949.

Métricas de histórico
Obtenha visualizações de até 24 horas de dados históricos no Application Performance Dashboard. Quando um seletor de horários é exibido em uma guia do painel **Visão Geral de Status**, é possível ajustar o intervalo de tempo para os gráficos e tabelas, cujos valores são derivados de amostras de dados históricos. Para gráficos de linha, também é possível comparar os dados atuais, até as últimas 24 horas, com até 8 dias de dados históricos para identificar anormalidades.

Para obter mais informações, consulte “Ajustando e comparando métricas no decorrer do tempo” na página 1091.

IBM Cloud Application Business Insights Universal View

É possível usar o Universal View para criar páginas customizadas para os aplicativos que estão sendo monitorados. Escolha entre diferentes opções de gráfico e métrica para criar widgets para monitorar dados de acordo com seus requisitos. Com o Universal View, é possível customizar um painel para visualizar dados consolidados de vários agentes.

Quando estiver visualizando dados no painel, é possível mudar o tipo de gráfico dinamicamente. No widget de grade, é possível filtrar dados dinamicamente.

É possível exportar os dados da página customizada para um arquivo de Dados Brutos.

Para obter mais informações, consulte “Visualizações customizadas” na página 1112.

Detalhes do aplicativo

Depois de realizar drill down do painel **Todos os meus aplicativos** para um painel detalhado para uma instância do sistema gerenciado, a guia Detalhes do atributo é exibida para você criar e gerenciar gráficos de linha históricos customizados e as tabelas que podem ser salvas. É possível salvar mais gráficos e páginas de tabela somente para visualização ou para serem compartilhados com todos os usuários no mesmo ambiente.

Para obter mais informações, consulte “Criando uma página de gráfico ou tabela customizada” na página 1093.

APIs

APIs do Cloud APM estão disponíveis para gerenciamento do seu ambiente, como designar funções de usuários e criar limites. Para obter mais informações, consulte “Explorando as APIs” na página 1072.

Controle de acesso baseado na função

No Cloud APM, uma função é um grupo de permissões que controlam as ações que podem ser tomadas. Use o recurso Controle de Acesso Baseado na Função para criar funções customizadas, que são a base da segurança. Estão disponíveis estas quatro funções predefinidas: Administrador de Função, Administrador de Monitoramento, Administrador do Sistema e Usuário de Monitoramento. É possível designar usuários para funções customizadas ou funções predefinidas, e os usuários podem ser designados para várias funções. É possível designar permissões para funções customizadas ou designar mais permissões para as funções padrão existentes. As permissões são acumulativas. Um usuário tem permissões para todas as funções para as quais está designado.

Você pode designar as permissões Visualizar e Modificar para aplicativos individuais, grupos de recursos do sistema e grupos de recursos customizados. Por exemplo, se você for membro de uma função que tenha a permissão Visualizar para um aplicativo, poderá visualizar todos os componentes de suporte nesse aplicativo.

É possível designar as permissões Visualizar e Modificar a tarefas de administração do sistema. Por exemplo, se você for membro de uma função que tenha a permissão Visualizar para Configuração avançada, poderá fazer e salvar mudanças na janela **Configuração avançada**.

Para obter mais informações, consulte “Funções e permissões” na página 1002.

Relatório de Histórico

Relatórios estão disponíveis para dados que são coletados pelo WebSphere Applications agent, Response Time Monitoring Agent e Synthetic Playback agent. O rastreamento de transação é obrigatório para relatórios do Agente Response Time Monitoring (Não disponível com Cloud APM, Base) Para obter descrições de relatórios, consulte “Relatórios” na página 1124.

Agent Builder

Construa agentes customizados para monitorar qualquer plataforma ou tecnologia. Consulte https://www.ibm.com/support/knowledgecenter/SSMKFH/com.ibm.apmaas.doc/install/agent_builder_guide.htm.

Monitoramento de recursos de banco de dados
A cobertura varia por oferta. Consulte “Capacidades” na página 52 para obter os nomes dos bancos de dados que podem ser monitorados.

Monitoramento de recursos de infraestrutura
Use agentes de monitoramento de recursos para monitorar hypervisors, armazenamento e redes. A cobertura varia por oferta. Consulte “Capacidades” na página 52.

Monitoramento de recursos de aplicativos comerciais
Use agentes de monitoramento de recursos para monitorar aplicativos de negócios e de colaboração. A cobertura varia por oferta. Consulte “Capacidades” na página 52.

Monitoramento de tempo de resposta e da experiência do usuário final
Veja a experiência de seus usuários com a infraestrutura de seus dispositivos. Use o monitoramento de tempo de resposta para monitorar o desempenho e a disponibilidade de websites e aplicativos da web do navegador para o banco de dados e para monitorar dispositivos móveis. Depois de instalar o Agente Response Time Monitoring em quaisquer servidores da web que você deseja monitorar, os dados coletados por esses agentes são exibidos no Application Performance Dashboard com pouca ou nenhuma configuração adicional necessária. Os dados do Agente Response Time Monitoring são usados para os painéis **Transações do usuário final**. No Cloud APM, Advanced, é possível medir o tempo de resposta do Navegador e os dados do Agente Response Time Monitoring também são usados na **Topologia de transação de agregação**. Para obter mais informações, consulte “Cenário: Monitorando o IBM Pilha de aplicativos Java ” na página 87.

Rastreamento de transação
Esse recurso está disponível com o Cloud APM, Advanced. O recurso de rastreamento da transação permite visualizações de topologia e monitoramento de transação em nível da instância. O rastreamento da transação é instalado como parte do Servidor Cloud APM. O rastreamento da transação é automaticamente ativado para alguns agentes, mas precisa ser manualmente ativado para outros. Tabela 4 na página 72 fornece mais informações sobre agentes que suportam rastreamento de transação.

Tabela 4. Ativação de rastreamento de transação para agentes e coletores de dados

Implementação do agente ou coletor de dados	Ativado por padrão	Como ativar
DataPower agent	✓	“Configurando o rastreamento de transações para o DataPower agent” na página 241
IBM Integration Bus agent	—	“Configurando o rastreamento de transações para o IBM Integration Bus agent” na página 286 **Nota:** O TT não será suportado se você implementar esse agente no Solaris X86.
Coletor de dados J2SE	✓	“Configurando o monitoramento do J2SE” na página 450
agente JBoss	—	“Configure o coletor de dados de rastreamento de transações do agente JBoss” na página 468
Coletor de dados Liberty	✓	“Configurando o coletor de dados Liberty para aplicativos no local” na página 880“Configurando o coletor de dados Liberty para aplicativos IBM Cloud” na página 884
Microsoft .NET agent	—	“Ativando a coleta de dados de rastreamento de transações e diagnósticos” na página 525

Tabela 4. Ativação de rastreamento de transação para agentes e coletores de dados (continuação)		
Implementação do agente ou coletor de dados	**Ativado por padrão**	**Como ativar**
Coletor de dados Node.js	—	"Customizando o coletor de dados Node.js independente para aplicativos IBM Cloud" na página 595 "Customizando o Coletor de dados Node.js para aplicativos no local" na página 600
Agente Response Time Monitoring + Agente do Servidor HTTP	—	"Planejando a Instalação " na página 687
SAP NetWeaver Java Stack	—	"Ativando a coleta de dados de rastreamento de transações e diagnósticos" na página 770
Agente Tomcat	—	"Ativando a coleta de dados de rastreamento de transações e diagnósticos" na página 807
Agente WebLogic	—	"Configurando o monitoramento do WebLogic" na página 817
WebSphere Applications agent	—	"Configurando o coletor de dados interativamente" na página 840 **Nota:** O TT não será suportado se você implementar esse agente no Solaris X86.
WebSphere MQ agent	—	"Configurando o rastreamento de transações para o WebSphere MQ agent" na página 940 **Nota:** O TT não será suportado se você implementar esse agente no Solaris X86.

Os dados são mostrados nas visualizações **Topologia de transação de agregação** e **Topologia de instância de transação** para todos os agentes que suportam o rastreamento de transação.

Topologia de Aplicativo
Veja como todos os componentes estão conectados em seu ambiente de aplicativos. Para obter mais informações, consulte "Aplicativo - Application Performance Dashboard" na página 1082.

Topologia da instância de transação
Visualize o caminho seguido através de seu ambiente para cada instância de uma transação. Para obter mais informações, consulte "Topologia da Instância de Transação " na página 93

Monitoramento de Disponibilidade
O IBM Cloud Availability Monitoring fornece monitoramento sintético aprimorado de seus aplicativos da web de vários pontos de presença ao redor do mundo. Crie testes sintéticos que imitam o comportamento do usuário em intervalos regulares. Execute seus testes a partir de pontos de presença públicos ou faça download e implemente seus próprios pontos de presença customizados em servidores locais ou privados. Use o painel do Monitoramento de Disponibilidade para monitorar a disponibilidade, o desempenho e os alertas do aplicativo usando gráficos, tabelas de detalhamento e visualizações de mapa. Use a análise em cascata para identificar quando ocorrem problemas de desempenho e disponibilidade e encontrar as razões para esses problemas.

Para obter informações adicionais sobre como usar testes sintéticos, consulte "Monitoramento de Disponibilidade" na página 1045.

Diagnósticos detalhados
Para agentes específicos, é possível realizar drill down de painéis de resumo para painéis de diagnósticos de detalhamento e visualizar informações sobre solicitações individuais. Realize drill down de painéis de resumo para visualizar o nível de código, rastreio de pilha e detalhe da consulta SQL. Use os painéis de diagnósticos para identificar quais solicitações têm um problema e depurar a

transação problemática. Também é possível detectar, diagnosticar e encerrar transações interrompidas ou lentas que ainda estão em andamento (consulte o WebSphere Applications agent Reference). A Tabela 5 na página 74 fornece informações adicionais sobre os agentes de diagnósticos.

Tabela 5. Painéis de diagnósticos de agentes e coletores de dados

Agente ou coletor de dados	**Dados diagnósticos configurados por padrão**	**Painéis de diagnósticos disponíveis**	**Como acessar painéis de diagnósticos**	**Como configurar o agente ou coletor de dados para coletar dados diagnósticos**
Coletor de dados J2SE	✓	Detalhe, Módulos da web, Instâncias de solicitação, Resumo de solicitação, Rastreios de solicitação	Clique em **Diagnosticar** no painel **Visão Geral** ou no painel **Módulos da web**.	"Configurando o monitoramento do J2SE" na página 450
agente JBoss	–	Painel de Diagnóstico, Resumo de solicitações em andamento, Painel de rastreio de pilha de solicitação em andamento, Coleta de lixo da JVM, Dump do heap, Comparação de dump do heap	Clique em **Diagnosticar**, **Solicitações em andamento**, **Detalhes** ou **Dump do heap** no painel **Visão Geral**.	"Configure o coletor de dados de rastreamento de transações do agente JBoss" na página 468
Coletor de dados Liberty	✓	Detalhe, Dump do heap, Comparação de dump do heap, Análise de memória	Clique em **Diagnosticar**, **Visualizar dump do heap** ou **Visualizar análise de memória** no painel **Visão Geral**.	• "Configurando o coletor de dados Liberty para aplicativos IBM Cloud" na página 884 • "Configurando o coletor de dados Liberty para aplicativos no local" na página 880
Microsoft .NET agent	–	Instâncias de solicitação, Resumo de solicitação, Rastreios de solicitação	Clique em **Diagnosticar** no painel **Visão Geral**.	"Ativando a coleta de dados diagnósticos usando o comando configdc" na página 526
Agente Node.js	✓	Detalhes de GC, Instâncias de solicitação, Resumo de solicitação, Rastreios de solicitação	Clique em **Diagnosticar** no painel **Visão Geral**.	"Configurando o Agente Node.js" na página 587

Tabela 5. Painéis de diagnósticos de agentes e coletores de dados (continuação)

Agente ou coletor de dados	Dados diagnósticos configurados por padrão	Painéis de diagnósticos disponíveis	Como acessar painéis de diagnósticos	Como configurar o agente ou coletor de dados para coletar dados diagnósticos
Coletor de dados Node.js	✓	Detalhes de GC, Detalhe de solicitações mais lentas, Instâncias de solicitação, Rastreios de solicitação	Clique em **Diagnosticar** ou **Detalhes de GC** no painel Visão Geral.	• "Configurando o Coletor de dados Node.js independente para aplicativos IBM Cloud(antigo Bluemix)" na página 593 • "Configurando o Coletor de dados Node.js para aplicativos no local" na página 598
Coletor de dados do Python	✓	Detalhes de solicitações mais lentas, Detalhe de instâncias de solicitação, Detalhe de rastreios de solicitação, Detalhes de encadeamento do Python, Coleta de lixo do Python, Detalhes de heap do Python	Clique em **Diagnosticar**, **Detalhe de encadeamentos** ou **Detalhe da memória** no painel **Visão Geral**.	• "Configurando o coletor de dados Python para aplicativos IBM Cloud" na página 671 • "Configurando o Coletor de dados do Python para aplicativos no local" na página 677
Agente Ruby	—	Detalhe de resumo de solicitação, Instâncias de solicitação de amostra, Rastreios de solicitação	Clique em **Diagnosticar** no painel **Visão Geral**.	"Configurando o monitoramento do Ruby" na página 718
Coletor de dados Ruby	✓	Instâncias de solicitação, Resumo de solicitação, Rastreios de solicitação	Clique em **Diagnosticar** no painel **Visão Geral**.	"Configurando o Coletor de dados Ruby para aplicativos IBM Cloud" na página 726
SAP NetWeaver Java Stack	✓	Instâncias de solicitação, Resumo de solicitação, Rastreios de solicitação	Clique em **Diagnosticar** no painel **Visão Geral**.	"Ativando a coleta de dados de rastreamento de transações e diagnósticos" na página 770

Tabela 5. Painéis de diagnósticos de agentes e coletores de dados (continuação)

Agente ou coletor de dados	Dados diagnósticos configurados por padrão	Painéis de diagnósticos disponíveis	Como acessar painéis de diagnósticos	Como configurar o agente ou coletor de dados para coletar dados diagnósticos
Agente Tomcat	—	Instâncias de solicitação, Resumo de solicitação, Rastreios de solicitação	Clique em **Diagnosticar** no painel **Visão Geral**.	"Ativando a coleta de dados de rastreamento de transações e diagnósticos" na página 807
Agente WebLogic	—	Painel de Diagnóstico, Resumo de solicitações em andamento, Painel de rastreio de pilha de solicitação em andamento, Detalhe de GC da JVM, Dump do heap, Comparação de dump do heap	Clique em **Diagnosticar**, **Visualizar solicitações**, **Detalhes** ou **Dump do heap** no painel **Visão Geral**.	"Configurando o monitoramento do WebLogic" na página 817
WebSphere Applications agent	—	Diagnósticos, Instância de solicitação, Sequência de solicitação, Resumo de solicitações em andamento, Rastreio de pilha de solicitação em andamento, Dump do heap, Comparação de dump do heap, Análise de memória	Clique em **Diagnosticar**, **Visualizar solicitações**, **Visualizar dump do heap** ou **Visualizar análise de memória** no painel **Visão Geral**. O botão **Visualizar análise de memória** funciona apenas depois que o monitoramento de fuga de memória é ativado.	• "Configurando o coletor de dados com o utilitário de configuração simples" na página 837 • "Ativando o monitoramento de fuga de memória" na página 877

O botão **Diagnosticar** é ativado somente quando os diagnósticos de detalhamento estão configurados para seu agente e você é um membro da função de Administrador de Função, da função de Administrador de Monitoramento ou alguma outra função customizada que tem permissão de visualização para Painéis de diagnósticos.

Limites

Com limites, é possível detectar comportamentos de aplicativo e condições específicos com base em definições monitoradas ativamente. Há limites predefinidos disponíveis para cada agente e é possível definir novos limites para monitoramento. Para obter mais informações, consulte "Gerenciador de Limites" na página 985.

Quando tiver o encaminhamento de eventos configurado, os eventos serão enviados para o receptor EIF. É possível usar o mapeamento padrão entre limites e eventos encaminhados para o servidor de

eventos ou customizar como os limites são mapeados. Para obter mais informações, consulte “Customizando um evento para encaminhar para um receptor EIF” na página 990.

No **Application Performance Dashboard**, após selecionar um aplicativo, a guia **Eventos** é exibida. A guia **Eventos** mostra os eventos abertos para o aplicativo atual. É possível realizar drill down para painéis detalhados, que contêm métricas de desempenho que o ajudam a determinar a causa do evento. Para obter mais informações, consulte “Status da Ocorrência” na página 1109.

Grupos de recursos

Os sistemas gerenciados existentes no ambiente corporativo monitorado podem ser categorizados por suas finalidades. Muitas vezes, esses sistemas possuem os mesmos requisitos de limite. Use o Gerenciador de Grupo de Recursos para organizar os sistemas monitorados em grupos, aos quais é possível designar limites de criação de eventos. Para obter mais informações, consulte “Gerenciador de Grupos de Recursos” na página 980.

Página Introdução

Após você efetuar login no Console do Cloud APM, será apresentada a página Introdução. Clique em qualquer uma das **Tarefas do Usuário** ou **Tarefas do Administrador** para obter um link para um tour baseado no cenário ou uma demonstração de vídeo. Os links "Comece agora" o levam diretamente para o recurso, como o Gerenciador de Limite. **Recursos da comunidade** o levam para **Perguntas mais frequentes**, para o fórum do Cloud APM etc.

Recursos extras estão disponíveis por meio da integração com outros produtos e componentes. Para obter mais informações, consulte o “Integração ” na página 77 e mais detalhes em Capítulo 8, “Integrando com outros produtos e componentes”, na página 949.

Integração

Recursos extra são fornecidos através da integração com outros produtos e componentes: Tivoli Monitoring, OMEGAMON, Netcool/OMNIbus, Operations Analytics - Log Analysis, Operations Analytics - Predictive Insights, Alert Notification, Control Desk, IBM Cloud e Agent Builder.

IBM Tivoli Monitoring

A coexistência de agente é suportada. É possível instalar agentes do IBM Cloud Application Performance Management no mesmo computador no qual agentes do IBM Tivoli Monitoring estão instalados. Entretanto, os dois tipos de agentes não podem ser instalados no mesmo diretório.Para obter mais informações, consulte “Coexistência do agente Cloud APM e do agente Tivoli Monitoring” na página 950.

Se seu ambiente tiver os produtos IBM Tivoli Monitoring e Cloud APM (nuvem, no local ou ambos), será possível instalar o IBM Cloud Application Performance Management Hybrid Gateway para fornecer uma visualização consolidada de sistemas gerenciados para ambos os ambientes. Para obter mais informações, consulte “Hybrid Gateway” na página 953. Para obter a lista atual de agentes do Tivoli Monitoring suportados, consulte Agentes suportados pelo Hybrid Gateway (APM Developer Center).

IBM OMEGAMON

O z Systems Extension Pack conecta um ou mais agentes OMEGAMON que estão em execução no mainframe z Systems ao Cloud APM. Usando o z Systems Extension Pack e o Hybrid Gateway para conectar agentes implementados OMEGAMON com o Cloud APM, é possível visualizar dados e eventos de monitoramento para componentes de aplicativo OMEGAMON no Console do Cloud APM.

Para obter mais informações, consulte “Integrando-se ao OMEGAMON” na página 964.

IBM Netcool/OMNIbus

É possível encaminhar seus eventos a partir do Cloud APM em seu gerenciador de eventos do Netcool/OMNIbus nas instalações. Para obter mais informações, consulte “Integrando-se ao Netcool/OMNIbus” na página 965.

IBM Operations Analytics - Log Analysis

Quando seu ambiente inclui o IBM Operations Analytics - Log Analysis, é possível reunir dados do log do aplicativo e dados de desempenho para ajudar a localizar a causa raiz dos problemas que são

enfrentados pelos seus aplicativos. É possível procurar por dados de log que estão associados aos seus aplicativos para localizar a causa de um problema, como lentidão ou uma falha. Para obter mais informações, consulte “Integrando-se ao Operations Analytics - Log Analysis” na página 970.

IBM Operations Analytics - Predictive Insights

O Operations Analytics - Predictive Insights analisa os dados e aprende o comportamento normal de um sistema. Ele cria um modelo de desempenho e o utiliza para detectar ou prever o comportamento fora do intervalo modelado, gerando alarmes quando ocorrer comportamentos irregulares. É possível incluir Operations Analytics - Predictive Insights na assinatura do Cloud APM. É possível, então, visualizar anomalias no Application Performance Dashboard e realizar drill down na interface com o usuário do Operations Analytics - Predictive Insights para visualizar mais detalhes. Para obter mais informações, consulte “Integração com Operations Analytics - Predictive Insights” na página 970.

IBM Cloud

É possível visualizar informações de monitoramento para seus aplicativos no ambiente do IBM Cloud usando os coletores de dados independentes. Os coletores de dados permitem a integração de recursos de monitoramento com o IBM Cloud transferindo dados de monitoramento de diagnósticos de recursos e de detalhamento sobre seus aplicativos IBM Cloud para o Servidor Cloud APM. O Servidor Cloud APM recebe e processa informações de monitoramento que são reunidas pelos coletores de dados. Os seguintes tipos de aplicativos IBM Cloud podem ser monitorados:

- Aplicativos Liberty
- Aplicativos Node.js
- Aplicativos Python
- Aplicativos Ruby

Após configurar um coletor de dados, será possível visualizar dados de monitoramento no Console do Cloud APM. Para obter mais informações, consulte “Procedimento geral para configurar coletores de dados” na página 183.

IBM Alert Notification

Se estiver usando o IBM Cloud Application Performance Management, o IBM Alert Notification é automaticamente integrado para você. O Alert Notification é um sistema de notificação fácil de usar e simples, que fornece à equipe de TI notificação instantânea de alertas para problemas em seu ambiente de operações de TI. Dados recebidos de agentes fornecem a origem dos alertas. Após você ativar o Alert Notification, conecte-o a uma instância do Cloud APM. Como um pacote independente, é possível integrar o Alert Notification com qualquer ferramenta de monitoramento no local que possa implementar e iniciar uma API REST. As ferramentas suportadas incluem o IBM Tivoli Netcool/OMNIbus. Para obter mais informações, consulte Integrando-se com a Notificação de alerta.

IBM Control Desk

A integração com o IBM Control Desk estará disponível mediante o envio de um chamado de suporte para o Suporte IBM. É possível configurar eventos Cloud APM para abrir automaticamente os chamados em IBM Control Desk. Acesse Suporte IBM e selecione **Assinatura**. Para obter informações adicionais sobre os detalhes que são necessários para o suporte para permitir que eles configurem esta integração, consulte “Integrando-se ao Control Desk” na página 972.

IBM Agent Builder

É possível usar Agent Builder para construir agentes customizados para qualquer tecnologia. Para obter mais informações, consulte https://www.ibm.com/support/knowledgecenter/SSMKFH/com.ibm.apmaas.doc/install/agent_builder_guide.htm.

Documentação

É possível localizar informações para o IBM Cloud Application Performance Management no IBM Knowledge Center, Console do Cloud APM e Application Performance Management Developer Center.

IBM Knowledge Center

O Cloud APM no IBM Knowledge Center é a fonte oficial de informações técnicas para o produto.

Ajuda da interface com o usuário
Quando você estiver com login efetuado no Console do Cloud APM ou explorando o Demo Guiada, poderá acessar o sistema de arquivos:

- Clique em **Conteúdos de ajuda** na barra de navegação. menu Ajuda.
- Clique em no banner do Painel de Desempenho do Aplicativo.
- Clique no link **Saiba mais** nas páginas Configuração do sistema.
- Clique em em um widget do painel.

IBM Application Performance Management Developer Center
O Application Performance Management Developer Center é um local central para uma variedade de conteúdo do APM que é aplicável a uma ampla faixa de usuários do APM. O conteúdo inclui documentação, blogs, vídeos e links para recursos adicionais.

IBM Cloud Application Performance Management Forum and dwAnswers
O Fórum do Cloud Application Performance Management e dwAnswers contêm discussões técnicas sobre problemas de produtos, incluindo a resolução de problemas e soluções.

As informações também estão disponíveis nos seguintes websites:

Ferramenta Software Product Compatibility Reports (SPCR)
É possível usar a ferramenta SPCR para gerar vários tipos de relatórios que estão relacionados à oferta e requisitos do componente. Procure um dos nomes da oferta Cloud Application Performance Management ou para IBM Cloud Application Performance Management - Agentes.

IBM Marketplace
Recursos como demonstrações de vídeo e perguntas mais frequentes estão disponíveis em IBM Marketplace.

IBM API Explorer
Para obter a documentação sobre as APIs do Cloud APM, consulte “Explorando as APIs” na página 1072.

IBM Terminology
O website do IBM Terminology contém terminologia que é relevante para produtos IBM e consolidada em um local conveniente.

IBM Redbooks
O website do IBM Redbooks contém publicações Redbooks, Redpapers e notas técnicas de Redbooks que fornecem informações sobre produtos das perspectivas de plataforma e solução.

Convenções usadas na documentação

Diversas convenções são usadas na documentação para termos especiais, ações, comandos, caminhos que dependem do sistema operacional e para informações específicas da plataforma e específicas do produto.

Convenções de fontes

As seguintes convenções de fontes são usadas na documentação:

Negrito

- Comandos compostos por letras minúsculas, comandos compostos por letras maiúsculas e minúsculas, parâmetros e variáveis de ambiente que, de outra forma, são difíceis de distinguir do texto circundante
- Controles de interface (caixas de seleção, botões de comando, botões de opções, botões de rotação, campos, pastas, ícones, caixas de listagem, itens dentro das caixas de listagem, listas multicolunas, contêineres, opções de menu, nomes de menu, guias, folhas de propriedade), rótulos (como **Dica:**)
- Palavras-chave e parâmetros em um texto

Itálico

- Citações (exemplos: títulos de publicações, disquetes e CDs)
- Palavras e frases definidas no texto (exemplo: uma linha não comutada é chamada de *linha de ponto a ponto*)
- Ênfase de palavras e letras (exemplo: O endereço LUN deve iniciar com a letra *L*).
- Novos termos no texto, exceto em uma lista de definição (exemplo: uma *visualização* é uma estrutura em uma área de trabalho contendo dados.)
- Variáveis e valores que você deve fornecer (exemplo: em que *myname* representa...)

`Espaço Simples`

- Exemplos e exemplos de código
- Nomes de arquivo, nomes de diretório, nomes de caminho, palavras-chave de programação, propriedades e outros elementos que são difíceis de distinguir do texto circundante
- Texto e prompts de mensagem
- Texto que você deve digitar
- Valores para argumentos ou opções de comandos

`Espaço simples em negrito`

- Nomes de comandos e nomes de macros e utilitários que podem ser digitados como comandos
- Nomes de variáveis de ambiente no texto
- Palavras-Chave
- Nomes de parâmetros no texto: parâmetros da estrutura da API, parâmetros e argumentos de comando e parâmetros de configuração
- Nomes de processos
- Nomes de variáveis de registro no texto
- Nomes de scripts

Variáveis e caminhos dependentes de sistema operacional

A direção da barra para os caminhos de diretório pode variar na documentação. Independente do que é visto na documentação, siga essas diretrizes:

- Linux AIX Use uma barra (**/**).
- Windows Use uma barra invertida (****).

Os nomes de variáveis de ambiente nem sempre são os mesmos no Windows e no AIX. Por exemplo, %TEMP% no Windows é equivalente a $TMPDIR no AIX ou Linux.

Para as variáveis de ambiente, siga essas diretrizes:

- Linux AIX Use **$***variável*.
- Windows Use **%***variável***%**.

Windows Se você estiver usando o shell bash em um sistema Windows, será possível usar as convenções do AIX.

Variável e caminhos do diretório de instalação para os agentes

install_dir é o diretório de instalação para os agentes. O local padrão depende do sistema operacional:

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

Capítulo 4. Planejando a implementação

Para assegurar que a implementação do IBM Cloud Application Performance Management seja bem-sucedida, o planejamento é fundamental.

Requisitos do sistema

Para os agentes e coletores de dados do IBM Cloud Application Performance Management, vários sistemas operacionais são suportados e cada um desses componentes possui requisitos específicos.

Fuso Horário

Use o Network Time Protocol (NTP) nos sistemas gerenciados para assegurar que o horário esteja exato. Configurar o tempo para correspondência com o local físico dos servidores (como Hora Universal Coordenada - 03:00 para Brasília e Hora Universal Coordenada +06:30 para Yangon) ajuda a garantir registros de data e hora precisos para eventos e transações. Os agentes relatam dados na IU do APM no horário local do usuário.

Requisitos do agente e do coletor de dados do Cloud APM
Obtenha informações sobre os requisitos para cada agente de monitoramento e coletor de dados independente que você planeja instalar.

O agente e o coletor de dados do Cloud APM em geral são transparentes ao hypervisor, o que significa que eles podem ser instalados e implementados em qualquer sistema operacional suportado, independentemente dos hypervisors nos quais os sistemas operacionais estão hospedados, como Hyper-V, IBM PowerVM, KVM, VMWare ESX, etc.

Para requisitos para os agentes e coletores de dados, use os links na seção Relatórios do componente do Requisitos do sistema (APM Developer Center).

Para obter informações atualizadas sobre navegadores suportados, consulte o Relatório Requisitos detalhados do sistema do IBM Cloud Application Performance Management.

Também é possível procurar IBM Cloud Application Performance Management na ferramenta Relatórios de compatibilidade do produto de software.

O sistema de computador local onde o agente está instalado deve suportar codificação UTF-8, se o agente enviar dados globalizados para o Servidor Cloud APM.

Portas padrão usadas pelos agentes e coletores de dados

Várias portas são usadas para comunicação entre o componente do Cloud APM e o aplicativo ou sistema (local ou remoto) que esteja sendo monitorado. Na maioria dos casos, portas padrão são fornecidas para facilitar a configuração. A maioria dos padrões pode ser customizada usando parâmetros de configuração.

O Tabela 6 na página 82 lista as portas padrão que são usadas pelos agentes e pelos coletores de dados do Cloud APM para comunicação com os aplicativos ou os sistemas que eles estejam monitorando. N/A na tabela indica uma das seguintes situações:

- O agente ou o coletor de dados não usa nenhuma porta para comunicar-se com o aplicativo ou o sistema monitorado.
- A porta usada para comunicação é determinada pela configuração do aplicativo monitorado.
- Portas usadas pelo agente ou coletor de dados são designadas dinamicamente e nenhum padrão estático é fornecido.
- Todas as portas a serem usadas devem ser especificadas pelo usuário e nenhum padrão é fornecido.

Tabela 6. Portas padrão usadas pelos agentes e coletores de dados

Agentes e coletores de dados	Portas Padrão	Configurável	Cópias	Remoto
Agente Amazon EC2	• Porta TCP 80 (para HTTP) • Porta TCP 443 (para HTTPS)	N/A	Sim	Não
Agente Amazon ELB	• Porta TCP 80 (para HTTP) • Porta TCP 443 (para HTTPS)	N/A	Não	Não
Agente Azure Compute	• Porta TCP 80 (para HTTP) • Porta TCP 443 (para HTTPS)	Não	Não	Não
Agente Cassandra	7199 (para servidor JMX, local e remoto)	Sim	Sim	Sim
Cisco UCS agent	• Porta TCP 80 (para HTTP) • Porta TCP 443 (para HTTPS)	Não	Sim	Não
Citrix VDI agent	Para chamadas do PowerShell: • 5985 (para HTTP) • 5986 (para HTTPS)	Sim	Sim	Sim
Db2	• 50000 (porta padrão do Db2 Server) • Monitoramento remoto suportado: usa o número de porta fornecido pelo usuário ao catalogar a instância de servidor remoto.	Sim	Sim	Sim
DataPower agent	5550 (para conexão com o dispositivo DataPower remoto)	Sim	Não	Sim
Agente do Hadoop	• Monitoramento local: valor da variável de ambiente **CP_PORT** • Monitoramento remoto: – 50070 (Standby Namenode) – 50090 (Secundário Namenode) – 8088 (ResourceManager) – 19888 (JobHistoryServer) – 8080 (Ambari)	Sim	Sim	Sim
Agente HMC Base	12443 (para fazer download do SDK do HMC)	Não	Sim	Não
Agente do Servidor HTTP	O servidor HTTP pode ser configurado para uma porta diferente, mas o agente em si não possui porta padrão.	N/A	Sim	Não
IBM Cloud agent	Conexão de saída para a porta api.softlayer.com 443.	N/A	Não	Sim
IBM Integration Bus agent	N/A	N/A	Sim	Não

Tabela 6. Portas padrão usadas pelos agentes e coletores de dados (continuação)

Agentes e coletores de dados	Portas Padrão	Configurável	Cópias	Remoto
Monitoramento de Serviço da Internet	Para a ponte de dados: • 9510 • 9520	Sim	Não	Sim
DataStage agent	• 9443 (porta HTTPS do WAS) • 50000 (porta JDBC do Banco de dados) • 1433 (Microsoft SQL) • 1521 (Oracle)	Sim	Sim	Sim
Coletor de dados J2SE	N/A	N/A	Não	Não
agente JBoss	Varia de acordo com a versão do servidor JBoss: • 9990 • 9994 • 9999	Não	Sim	Não
Coletor de dados Liberty	N/A	N/A	Não	Não
agente do Linux KVM	• 8080 (para HTTP) • 8443 (para HTTPS)	Sim	Sim	Não
agente do S.O. Linux	22 (para monitoramento remoto de log com SSH)	Sim	Sim	Não
MariaDB agent	3306	Sim	Sim	Sim
Microsoft Active Directory agent	O número da porta depende da configuração do listener para uso de monitoramento.	N/A	Sim	Sim
Microsoft Cluster Server agent	N/A	N/A	Não	Não
Microsoft Exchange Server agent	N/A	N/A	Não	Não
Microsoft Hyper-V Server agent	N/A	N/A	Não	Não
Microsoft IIS agent	N/A	N/A	Não	Não
Microsoft .NET agent	Para enviar dados de rastreamento de transação, a porta 5456 é usada por padrão.	Sim	Sim	Não
Microsoft Office 365 agent	7799 (por transação sintética do Skype)	Sim	Sim	Não
Microsoft SharePoint Server agent	1433 (para SQL server)	Não	Sim	Sim
Microsoft SQL Server agent	1433 (padrão de servidor SQL)	Sim (por **COLL_PORT**)	Sim	Não

Tabela 6. Portas padrão usadas pelos agentes e coletores de dados (continuação)

Agentes e coletores de dados	Portas Padrão	Configurável	Cópias	Remoto
Agente do MQ Appliance	• 162 (para receber eventos SNMP) • 5554 (para conexão com o MQ Appliances)	Sim	Sim	Sim
Agente MongoDB	• 27017 (para única instância) • 27019 (para o cluster)	Sim	Sim	Não
Agente MySQL	3306 (para conexão JDBC)	Sim	Sim	Sim
Agente NetApp Storage	Para monitoramento remoto: • 8088 • 8488 • 443 • 8443	Não	Não	Sim
Agente Node.js	63336	Sim	Sim	Não
Coletor de dados Node.js	N/A	N/A	Não	Não
OpenStack agent	5000 (para conectar serviço de identidade OpenStack)	Sim	Não	Sim
Agente Oracle Database	1521 (para conexão SQL)	Sim	Sim	Não
Agente PHP	• Conexão do Apache • O número da porta é baseado na configuração do Apache	Sim	Sim	Não
Agente PostgreSQL	5432 (para conexão JDBC)	Sim	Sim	Sim
Coletor de dados do Python	N/A	N/A	Não	Não
Agente RabbitMQ	O número da porta na qual o plug-in de gerenciamento RabbitMQ está ativado (local e remota): 15672	Sim	Sim	Sim
Response Time Monitoring Agent	• O modelo de analisador de pacote monitora transações HTTP na porta 80. • O modelo de servidor HTTP monitora todas as portas.	Sim	Sim	Não
Agente Ruby	Gerado dinamicamente	N/A	Sim	Não
Coletor de dados Ruby	N/A	N/A	Não	Não
Agente SAP	33*nn* (em que *nn* é o número da instância SAP)	Não	Sim	Não
SAP HANA Database agent	Padrão: 30013. Intervalo: 30013-39913.	Sim	Sim	Não
SAP NetWeaver Java Stack	Padrão: 50004. Intervalo: 50004-59904.	Sim	Sim	Não

Tabela 6. Portas padrão usadas pelos agentes e coletores de dados (continuação)

Agentes e coletores de dados	Portas Padrão	Configurável	Cópias	Remoto
Agente Siebel	N/A	N/A	Sim	Não
Agente Skype for Business Server (anteriormente conhecido como agente Microsoft Lync Server)	• Porta padrão do servidor de negócios 5061 • Porta do SQL server 1433 (local ou remota, dependendo do ambiente).	Não	Sim	Não
Agente Sterling Connect Direct	1363	Sim	Não	Sim
Agente Sterling File Gateway	50000 O número da porta API de REST do IBM B2B Integrator e o número da porta do banco de dados são obrigatórios e configuráveis.	Sim	Sim	Sim
Sybase agent	5000	N/A	Sim	Não
Synthetic Playback agent	• 4444 (para conectar o servidor Selenium interno) • Portas remotas são especificadas na URL http de websites monitorados, normalmente HTTP 80 e HTTPS 443	Não	Sim	Não
Agente Tomcat	8686 (para servidor MBean Tomcat)	Sim (por porta JMX)	Sim	Não
agente de S.O. UNIX	22 (para monitoramento remoto de log com SSH)	Sim	Sim	Não
Agente VMware VI	• 443 (para monitoramento remoto) • 80 (para monitoramento local)	Não	Sim	Sim
Agente WebLogic	7003 (tráfego HTTP de gerenciamento do JMX)	Sim	Sim	Não
WebSphere Applications agent	• 63335 (para V8 agente de monitoramento) • 63336 (para V6 agente de monitoramento) • 63355 (para monitoramento de recursos) • 5457 (para Transaction Framework Extension)	Sim	Sim	Não
WebSphere Infrastructure Manager agent	N/A	N/A	Sim	Não
WebSphere MQ agent	O número da porta depende da configuração do listener para uso de monitoramento.	N/A	Não	Sim

Tabela 6. Portas padrão usadas pelos agentes e coletores de dados (continuação)				
Agentes e coletores de dados	**Portas Padrão**	**Configurável**	**Cópias**	**Remoto**
Windows OS agent	22 (para monitoramento remoto de log com SSH)	Sim	Sim	Não

Cenários

Dependendo da complexidade de seu ambiente, deve-se instalar diferentes agentes para monitorar diferentes componentes. Use esses cenários de implementação para ajudá-lo a entender o que você deve instalar onde para obter os melhores resultados a partir do IBM Cloud Application Performance Management.

Cenário: monitorando o IBM API Connect

É possível monitorar e solucionar problemas do ambiente do IBM API Connect usando agentes do APM e coletores de dados.

O produto Cloud APM ajuda a gerenciar o desempenho e a disponibilidade do ambiente do API Connect. Usando agentes e coletores de dados do Cloud APM, você terá visibilidade e controle tanto da infraestrutura do API Connect quanto das APIs de aplicativos, assegurando desempenho ideal e uso eficiente de recursos. Ao encontrar problemas de desempenho no ambiente do API Connect, o produto Cloud APM poderá ajudá-lo a detectar, diagnosticar e isolá-los.

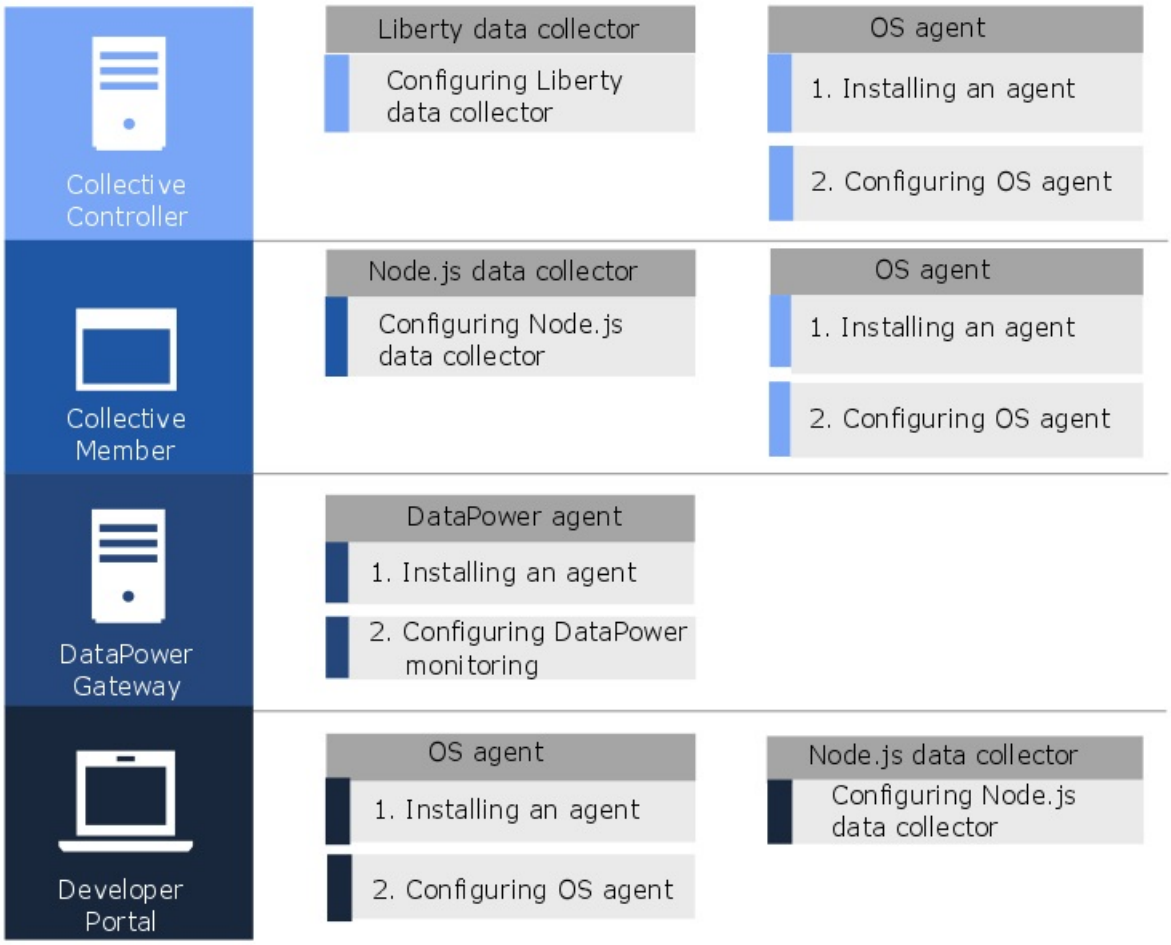
Por exemplo, é possível instalar os agentes de S.O. em todos os sistemas aplicáveis. Use os agentes de S.O. para coletar a analisar o desempenho específico do servidor, incluindo o desempenho da CPU, E/S e utilização de disco, disponibilidade e desempenho do processo e desempenho de rede. Além disso, os agentes de S.O. podem ser configurados para monitorar os principais logs e os logs do sistema do API Connect.

Se você tiver outros produtos de middleware implementados, o recurso de rastreamento de transação, que é instalado como parte do Servidor Cloud APM, poderá fornecer visualizações de topologia para ver informações de rastreamento de transação dos produtos de middleware e dos serviços que eles expõem e solucionar problemas quando eles surgem.

A figura a seguir mostra os componentes do API Connect e os agentes e coletores de dados correspondentes do Cloud APM que podem monitorá-los. Para ativar esses agentes e coletores de dados, conclua as tarefas de instalação e de configuração que são listadas sob o nome do agente e do coletor de dados. Clique nas caixas retangulares na figura que contém o nome da tarefa para acessar as tarefas de instalação ou configuração.

Nota:

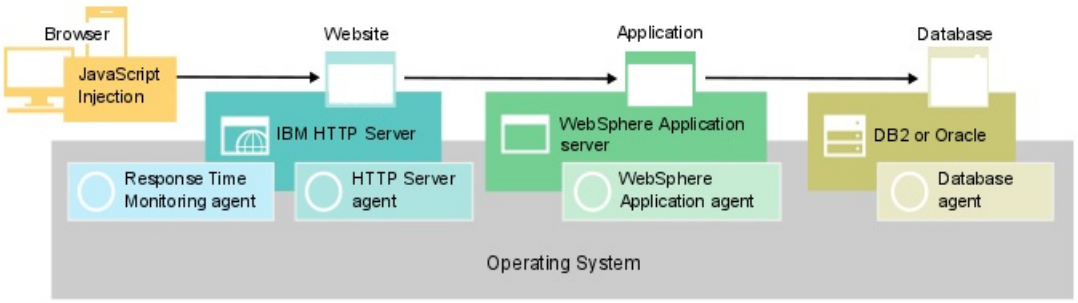
- Instale um Coletor de dados Node.js para cada aplicativo IBM API Connect publicado no membro coletivo.
- Ao monitorar o DataPower Gateway, o DataPower agent é executado remotamente a partir do dispositivo DataPower.



1. “Configurando o coletor de dados Liberty para aplicativos no local” na página 880
2. Capítulo 6, “Instalando os agentes”, na página 117
3. “Configurando o monitoramento do S.O.” na página 631
4. “Configurando o Coletor de dados Node.js para aplicativos no local” na página 598
5. Capítulo 6, “Instalando os agentes”, na página 117
6. “Configurando o monitoramento do S.O.” na página 631
7. Capítulo 6, “Instalando os agentes”, na página 117
8. “Configurando o monitoramento do DataPower” na página 230
9. Capítulo 6, “Instalando os agentes”, na página 117
10. “Configurando o monitoramento do S.O.” na página 631
11. “Configurando o Coletor de dados Node.js para aplicativos no local” na página 598

Cenário: Monitorando o IBM Pilha de aplicativos Java

É possível monitorar e solucionar problemas do IBM Pilha de aplicativos Java para ver informações de monitoramento de transação a partir do navegador através do banco de dados, incluindo monitoramento de recurso a partir de componentes individuais. O IBM Pilha de aplicativos Java inclui o banco de dados IBM HTTP Server, o WebSphere Application Server e o IBM Db2 ou Oracle.



Monitorando o IBM Pilha de aplicativos Java
Para monitorar o IBM Pilha de aplicativos Java, instale os agentes que estão listados para cada componente na ordem especificada.

Opcionalmente, se você também deseja monitorar o sistema, instale agentes do S.O. em todos os componentes.

Para o servidor da web, conclua as etapas a seguir:

1. Instale o Agente do HTTP Server.

   Atalho: Essa instalação também instala o Módulo de Tempo de Resposta do IBM HTTP Server e configura automaticamente a injeção do JavaScript.
2. Configure a instalação do Agente do HTTP Server.
3. Instale o agente do Response Time Monitoring.

Para o servidor de aplicativos, instale o agente de aplicativos WebSphere.

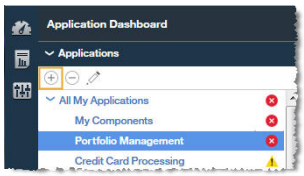
Para o banco de dados, instale o agente Oracle Database ou o agente Db2, dependendo de seu banco de dados.

Incluindo aplicativos da web no Painel de Desempenho do Aplicativo
Inclua os aplicativos da web que você deseja monitorar no Painel de Desempenho do Aplicativo .

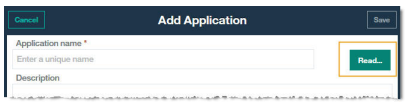
Procedimento

Para incluir aplicativos da web, conclua as etapas a seguir:

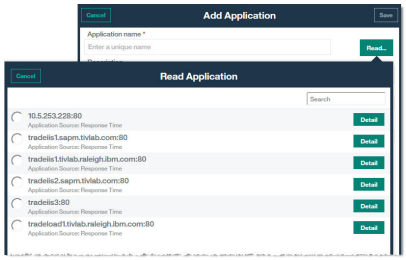
1. No Painel de Desempenho do Aplicativo , clique em **Incluir Aplicativo**.



2. Clique em **Ler** para abrir uma lista de aplicativos descobertos.



3. Selecione o aplicativo da web que você deseja monitorar.



4. Clique em **Salvar**.

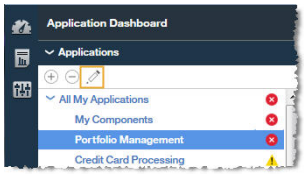
Associando o IBM Pilha de aplicativos Java com o aplicativo da web

Edite o aplicativo da web para associar o WebSphere Application Server e componentes do banco de dados que você deseja monitorar com ele.

Procedimento

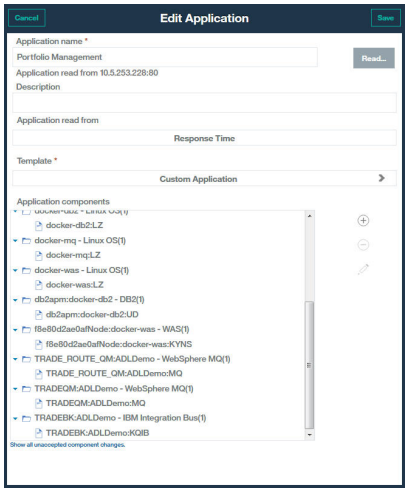
Para exibir os componentes no Pilha de aplicativos Java, conclua as seguintes etapas no Painel de Desempenho do Aplicativo :

1. Selecione o servidor da web e clique em **Editar Aplicativo**.



2. Na janela **Editar Aplicativo**, clique em **Incluir componentes** +.
3. Na janela **Selecionar Componente**, selecione WebSphere Application Server.
4. No **Editor de Componente**, selecione as instâncias do componente necessárias e clique em **Incluir**.

   Qualquer instância do WebSphere Application Server detectada é automaticamente incluída na lista.
5. Clique em **Voltar** e repita as etapas “3” na página 89 - “4” na página 89 para o seu banco de dados. Continue incluindo o WebSphere Application Server e instâncias de banco de dados até que a Pilha de aplicativos Java esteja completa.



6. Clique em **Fechar** e, em seguida, em **Salvar** para retornar para o Painel de Desempenho do Aplicativo .

Resultados

Dica: Se a Topologia de Transação de Agregado não mostrar inicialmente a topologia que você espera, espere que ela seja atualizada e verifique novamente em alguns minutos. Se a topologia ainda não for o que você espera, seu aplicativo pode não estar se comunicando com os componentes esperados. Verifique o seu ambiente.

Visualizando resultados de monitoramento do IBM Pilha de aplicativos Java

É possível visualizar os resultados de monitoramento do IBM Pilha de aplicativos Java nas topologias.

Sobre Esta Tarefa

Nas topologias, você verá informações de monitoramento de transação a partir do navegador até o banco de dados, incluindo monitoramento de recurso a partir de componentes individuais. Os seguintes nós são exibidos na Topologia de Transação de Agregado e na Topologia de Instância de Transação:

- Navegador, exibido somente quando o JavaScript Injection estiver ativado
- Servidor HTTP
- WebSphere Application Server
- Banco de Dados

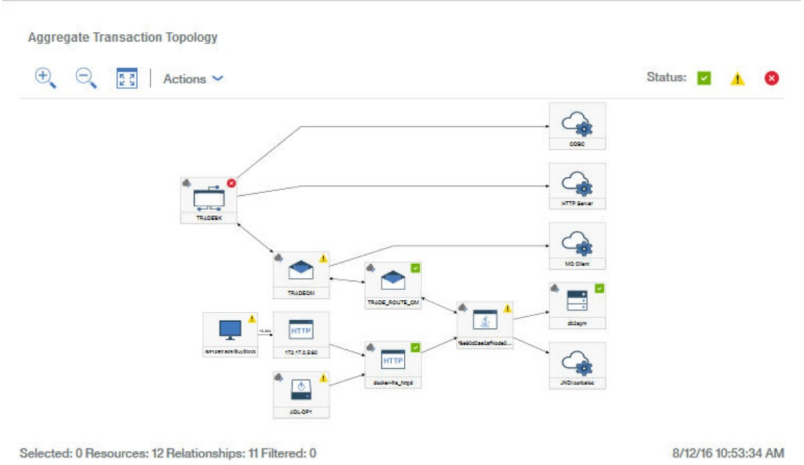
Procedimento

É possível vincular a partir de nós na topologia a mais detalhes sobre esse nó:

1. Passe o mouse sobre um nó para exibir uma janela com informações adicionais.
2. Para fazer drill down para um painel mais detalhado para o nó, clique com o botão direito do mouse no nó e selecione o link.

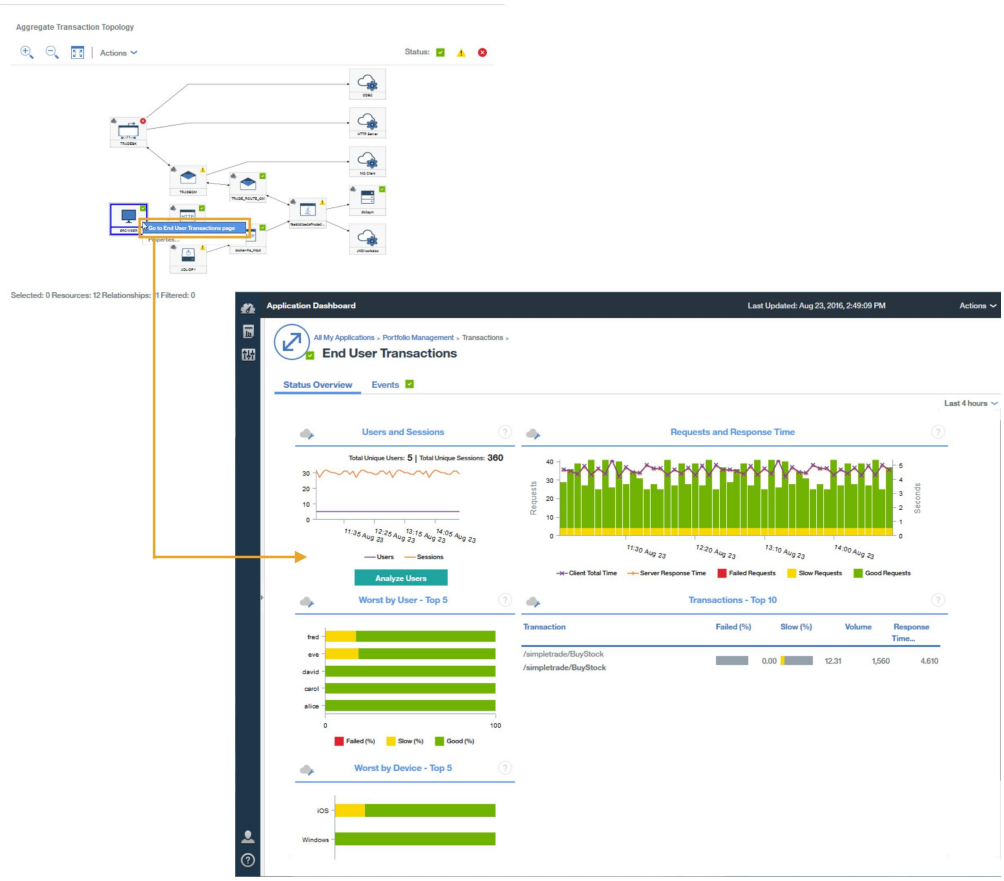
Topologia de Transação de Agregado

A Topologia de Transação de Agregado é exibida no painel Resumo do aplicativo.



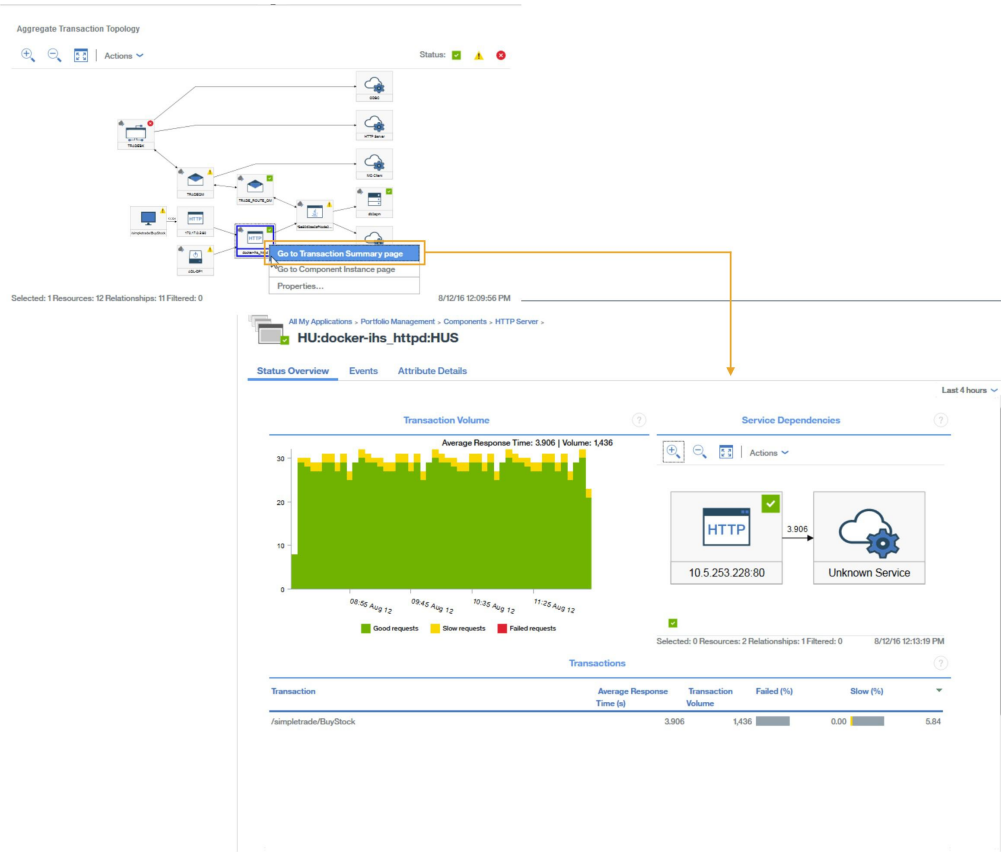
Topologias de Transação de Agregado exibem as seguintes informações:

- Nó para clientes baseados em navegador, pesquisar detalhadamente a experiência do usuário final



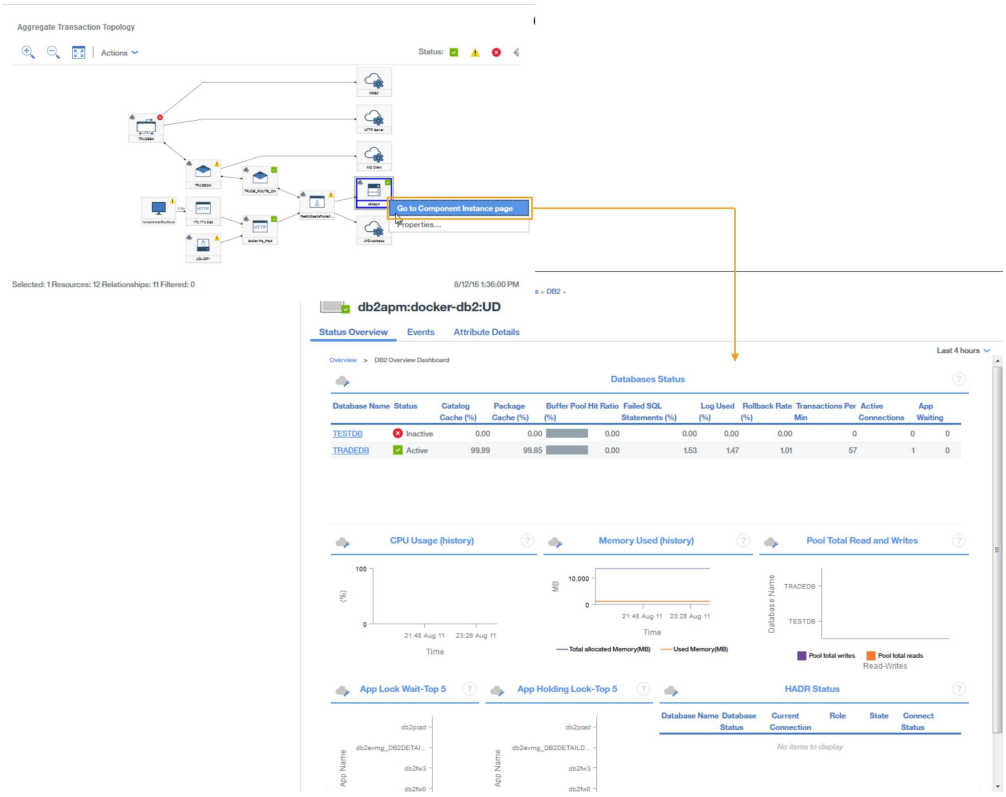
Lembre-se: Esse nó é exibido somente quando a injeção do JavaScript automática estiver medindo dados a partir do navegador.

- Nós para aplicativos baseados em HTTP, realizar drill down para a página de recursos do servidor da web ou uma página



- Nós para WebSphere Application Server baseado em aplicativos, realizar drill down para uma página de recursos de aplicativos, ou uma página de resumo da transação

- Nós para os servidores de banco de dados específicos, realizar drill down para uma página de recursos de banco de dados se disponíveis

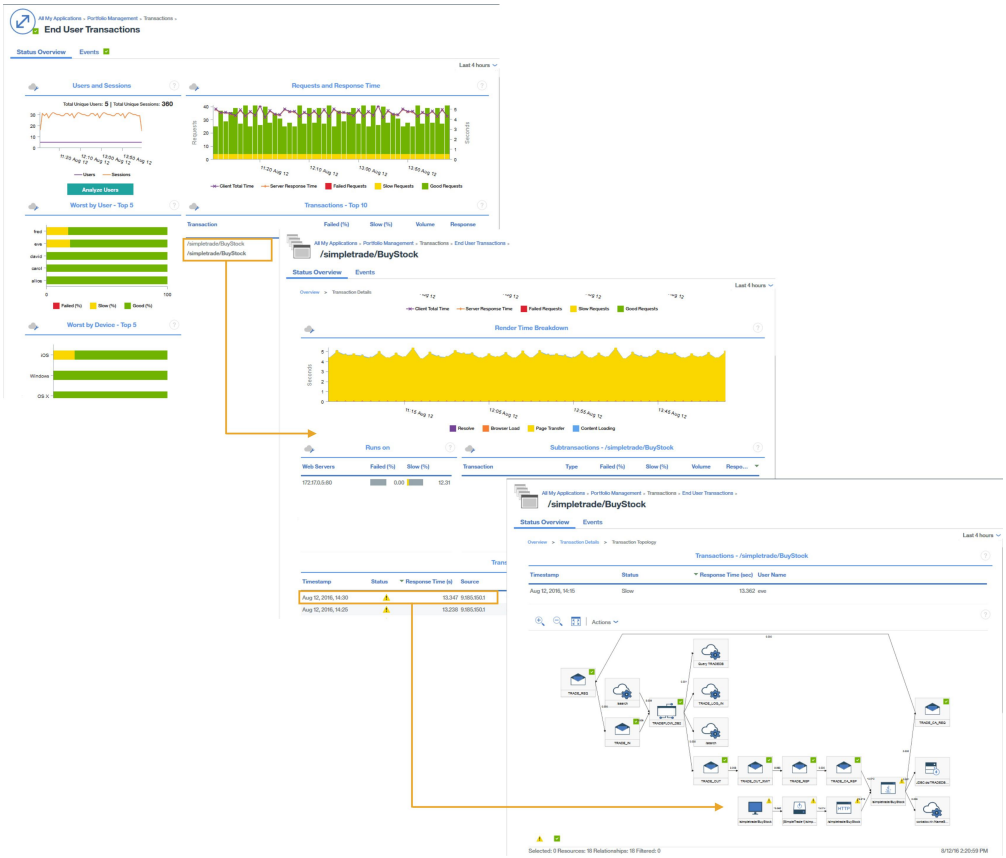


Topologia da Instância de Transação

Topologias de instância de transação são exibidas para transações reais do usuário final.

Realize drill down a partir do resumo de **Transações do Usuário Final** por meio dos seguintes widgets:

1. Selecione uma transação na tabela Transações - 10 Principais
2. Selecione uma instância na tabela Instâncias de Transações



As topologias de instância de transação para a pilha de aplicativos Java exibem os seguintes nós. Clique no nó para exibir informações sobre ele.

- Nó para clientes baseados no navegador

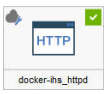
  Lembre-se: Esse nó é exibido somente quando a injeção do JavaScript automática estiver medindo dados a partir do navegador.
- Nós de HTTP, incluindo tempos de resposta a partir do navegador
- Nós do DataPower, se instrumentado
- WebSphere Application Server , a partir da qual é possível realizar drill down para uma página de recursos de aplicativos
- Os nós do servidor do banco de dados, a partir da qual é possível realizar drill down para um status de recurso de banco de dados, e informações de diagnóstico instrução SQL para pedidos JDBC

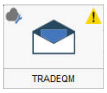
  Dica: Quando a topologia indica que a maioria do tempo de resposta é gasto no banco de dados, informações de instrução SQL é aberta diretamente quando você clica em **Diagnosticar**.

Também são exibidos gráficos de Gantt, que resumem os tempos da instância.

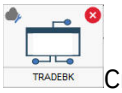
Diagnosticando problemas em seu ambiente
Se as instâncias de transação para um dos componentes em seu ambiente estiverem lentas ou falhando, o componente afetado é designado com um status apropriado.

Um nó pode ter um dos status a seguir:

- 

Bom, o nó tem um carrapato cercado por um quadrado verde no canto superior direito
- 

Aviso, o nó possui um ponto de exclamação cercado por um triângulo amarelo na Superior direito Ram R

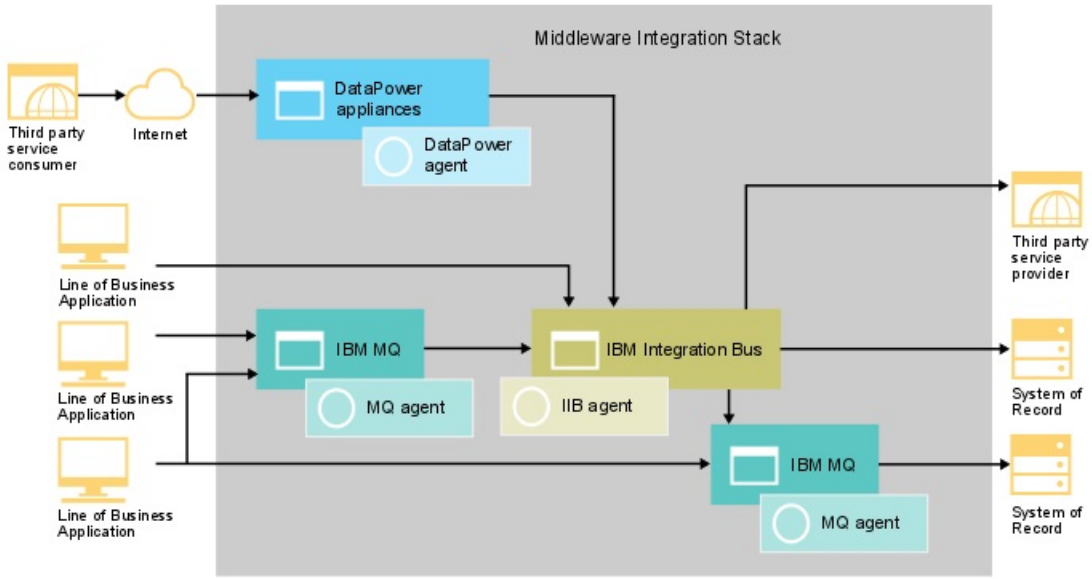
- 

Crítico, o nó tem um plano de fundo vermelho e uma cruz que está circundada em vermelho no canto superior direito

Para identificar a causa dos problemas para esses componentes com um status de aviso ou crítico, clique com o botão direito do mouse no nó e realizar drill down para ver mais informações sobre o que pode estar causando as falhas.

Cenário: monitorando o Pilha de integração IBM

É possível monitorar o Pilha de integração IBM para ver informações de rastreamento de transação para os produtos de middleware e os serviços que elas expõem e solucionar problemas se quaisquer problemas surgirem. O Pilha de integração IBM inclui IBM MQ, IBM Integration Bus e dispositivo DataPower.



monitorando a Pilha de integração IBM

Para monitorar o Pilha de integração IBM, instale os agentes que estão listados para cada componente na ordem especificada.

Opcionalmente, se você também deseja monitorar um sistema, instale agentes do S.O nesse sistema.

Para IBM MQ, conclua as etapas a seguir:

1. Instale o Monitoring Agent for WebSphere MQ.
2. Configure o WebSphere MQ agent para se conectar ao gerenciador de filas.
3. Ative **Rastreio de Atividade do Aplicativo MQ** no gerenciador de filas.

Para IBM Integration Bus, conclua as etapas a seguir:

1. Instale o Monitoring Agent para IBM Integration Bus.
2. Ative o IBM Integration Bus para rastreamento de transações.
3. Configure o rastreamento de transação para as instâncias necessárias do IBM Integration Bus agent.

Para dispositivo DataPower, conclua as etapas a seguir:

1. Instale o Monitoring Agent for DataPower.
2. Configure o DataPower agent para se conectar ao dispositivo DataPower.
3. Assegure-se de que o rastreamento de transação esteja ativado para as instâncias necessárias do DataPower agent.
4. Configure o dispositivo DataPower.

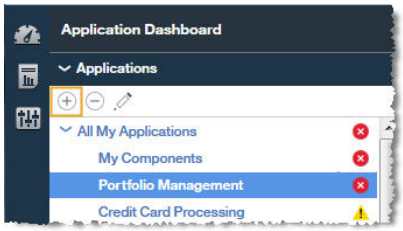
Incluindo aplicativos middleware no Painel de Desempenho do Aplicativo

Crie um aplicativo Pilha de integração IBM e inclua as instâncias IBM MQ, IBM Integration Bus e dispositivo DataPower que deseja para monitorá-lo.

Procedimento

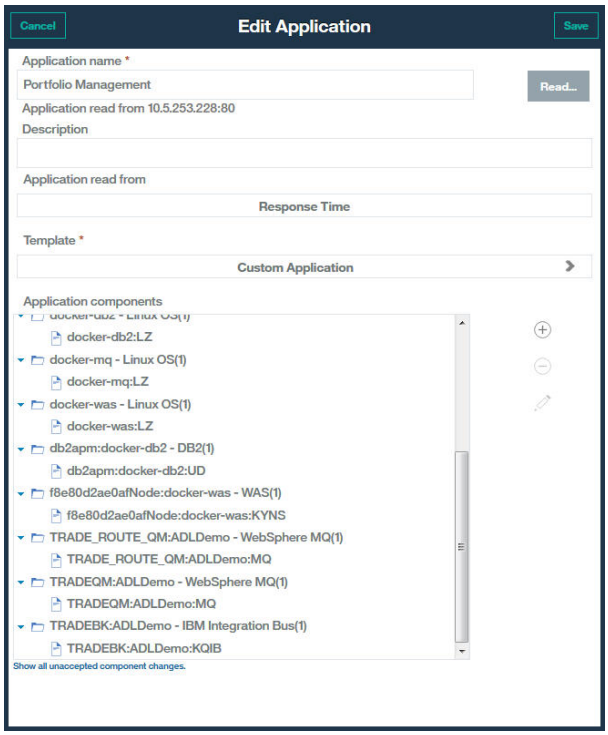
Para exibir os componentes no Pilha de integração IBM, conclua as seguintes etapas no Painel de Desempenho do Aplicativo :

1. No Painel de Desempenho do Aplicativo , clique em **Incluir Aplicativo**.



2. Na janela **Editar Aplicativo**, inclua um nome de aplicativo e clique em **Incluir componentes** +.
3. Na janela **Selecionar componente**, selecione **IBM Integration Bus**.
4. No **Editor de Componente**, selecione as instâncias do componente necessárias e clique em **Incluir**.

   Todas as instâncias detectadas do IBM Integration Bus são automaticamente incluídas nessa lista.
5. Clique em **Voltar** e repita as etapas 3 - 4 para **WebSphere MQ** e **DataPower Appliance**. Continue incluindo instâncias do IBM Integration Bus, IBM MQ e dispositivo DataPower até que o Pilha de integração IBM esteja concluído.



6. Clique em **Fechar** e, em seguida, em **Salvar** para retornar para o Painel de Desempenho do Aplicativo .

Resultados

Dica: Se a Topologia de Transação de Agregado não mostrar inicialmente a topologia que você espera, espere que ela seja atualizada e verifique novamente em alguns minutos. Se a topologia ainda for o que não é esperado, pode haver um problema com o seu aplicativo não se comunicando com os componentes esperados. Verifique o seu ambiente.

Visualizando resultados de monitoramento do Pilha de integração IBM

É possível visualizar os resultados de monitoramento do Pilha de integração IBM nas topologias e páginas de middleware. Também é possível visualizar eventos gerados quando uma transação viola um limite definido.

Sobre Esta Tarefa

Nas topologias, é possível ver as interações entre os componentes de middleware. Os nós de middleware a seguir são exibidos na Topologia de Transação de Agregado e na Topologia de Instância de Transação:

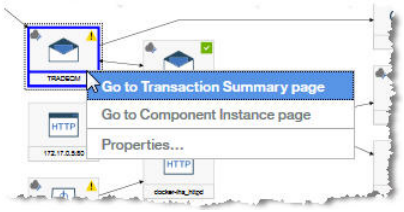
- IBM Integration Bus
- IBM MQ
- dispositivo DataPower

Passe o mouse sobre um nó para exibir a janela Propriedades que mostra informações que explicam porque ele tem um status específico. O status é determinado por situações; as situações com um status inválido são exibidas.

Procedimento

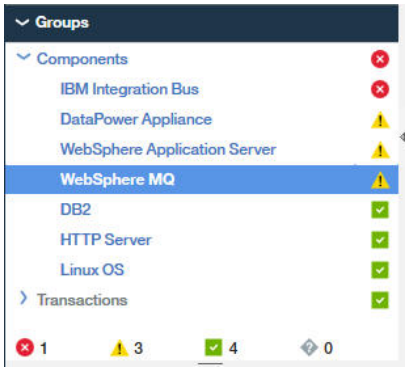
É possível vincular-se de nós na topologia para mais detalhes sobre esse nó:

1. Clique com o botão direito em um nó.



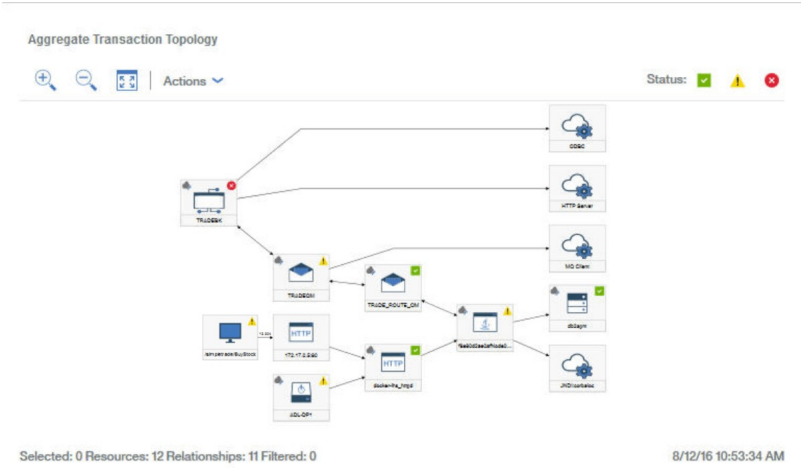
2. Selecione **Acessar a página Componente** para exibir informações sobre o componente.
3. Selecione **Acessar a página Resumo de Transações** para exibir informações sobre as transações de middleware.

   Dica: Selecione **Grupos** > **Componentes** > ***componente de middleware*** no navegador e selecione um período de solicitação no widget de volume para acessar o mesmo painel.



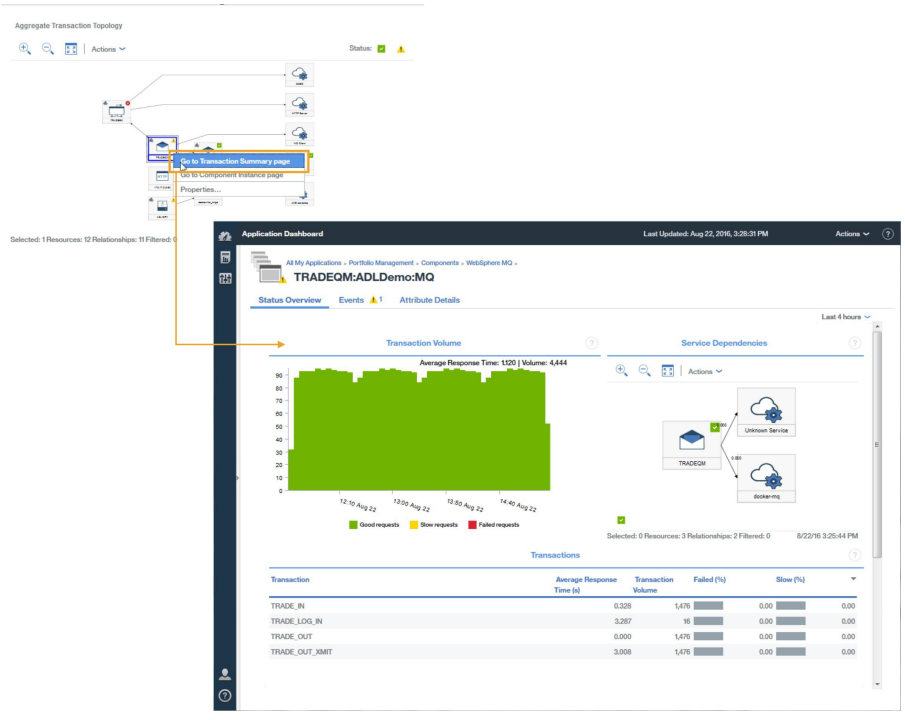
Topologia de Transação de Agregado

A Topologia de Transação de Agregado é exibida no painel Resumo do aplicativo.



As topologias Transação de Agregado podem exibir nós IBM MQ, IBM Integration Bus e dispositivo DataPower. Realize drill down a partir destes nós para obter mais informações sobre a pilha de integração de middleware.

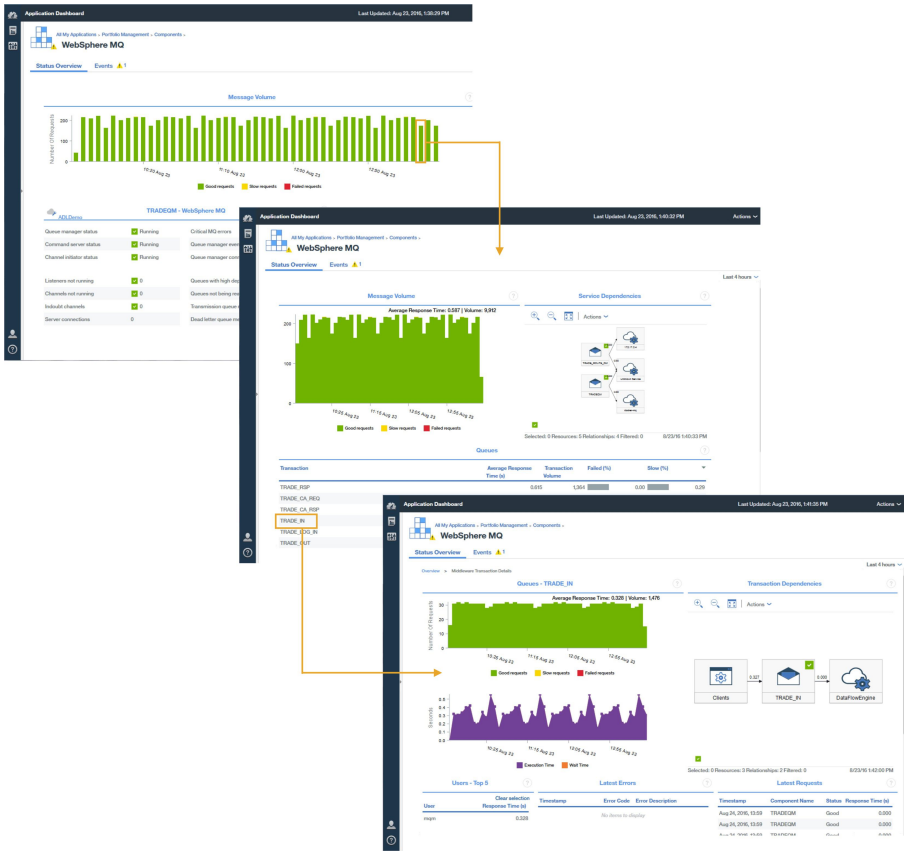
Para realizar drill down, clique com o botão direito em um nó middleware na Topologia de Transação de Agregado e selecione **Acessar página de Resumo da Transação**. Como alternativa, selecione **Grupos** > **Componentes** > ***componente de middleware*** no navegador e selecione um período de solicitação no widget de volume para acessar as mesmas informações.



Detalhes da transação de middleware

Na página Resumo de Transações de Middleware, é possível realizar drill down para detalhes da transação de middleware.

Para realizar drill down para detalhes da transação de middleware para o componente, conclua as seguintes etapas:



1. Na página Resumo de transações de middleware do componente, selecione um intervalo de monitoramento no diagrama **Mensagem ou** volume.
2. No **Resumo da Transação do Middleware**, no **Filas**, **Brokers**, ou **Dispositivos** widget, selecione uma fila, intermediário, OU Dispositivo .

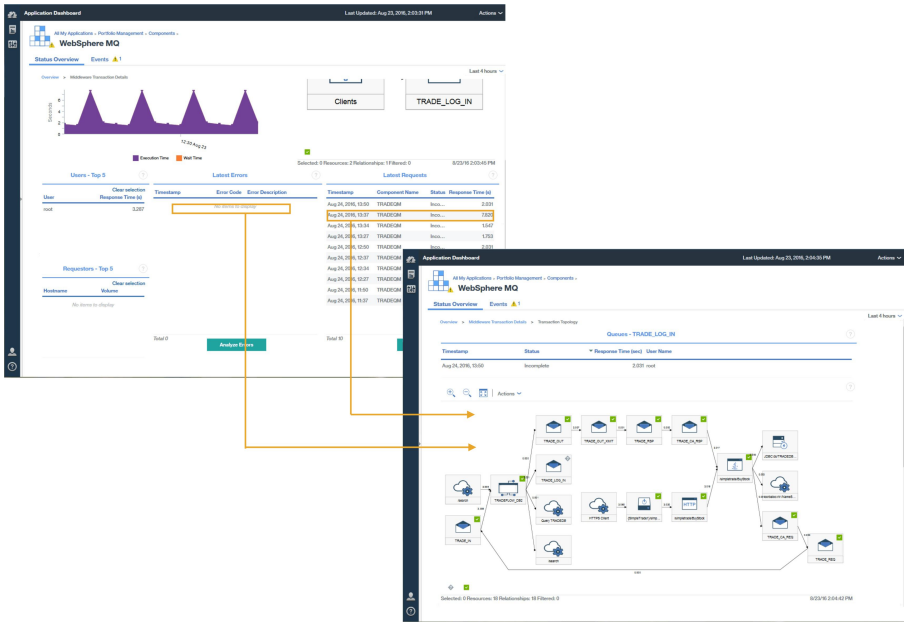
Analisando erros e instâncias

Na página Detalhes de Transações do middleware, é possível fazer drill down adicional das informações, o que ajuda a analisar erros e instâncias e a acessar a topologia Instância de Transação.

Para realizar drill down para erros e instâncias para os componentes de middleware e, em seguida, para a Topologia de Instância de Transação, na página **Detalhes da Transação**, conclua uma das etapas a seguir:

- Clique em **Analisar Erros** para exibir a **Análise de Erro** página, selecione um erro.
- Clique em **Analisar Solicitações** para exibir a **Análise de Instância** página, selecione uma instância.

Como alternativa, na página **Detalhes da Transação**, selecione um erro ou uma instância para ir diretamente para a Topologia de Instância de Transação.



Topologias de instância de transação exibem os nós middleware a seguir:

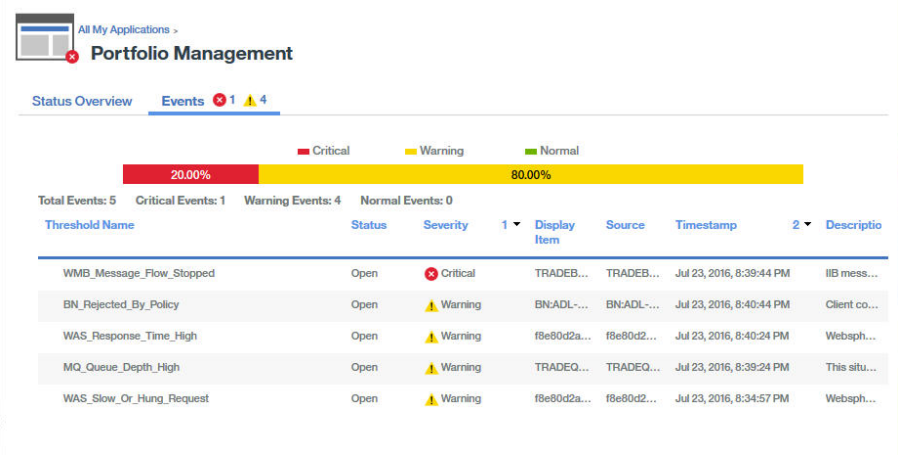
- Gerenciadores de filas de mensagens
- Brokers do IBM Integration Bus
- Dispositivos DataPower

Selecione um nó para exibir suas propriedades que expliquem porque ele tem um status específico.

Um Gráfico de Gantt de Transação é exibido para a fila ou broker selecionado. O gráfico de Gantt ajuda a isolar os contribuidores mais significativos para o tempo de resposta geral da transação.

Eventos

Os eventos são gerados para o Pilha de integração IBM pelo padrão de Rastreamento de Transação limites além dos outros agentes.



Para obter mais informações sobre os eventos padrão de Rastreamento de transações, consulte “Limites de evento para Monitoramento de transação ” na página 1013.

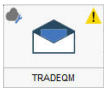
Você pode incluir limites para criar mais eventos, por exemplo para taxas de transação que estão lentos ou cair abaixo de um determinado limite.

Para obter mais informações sobre a inclusão de eventos, consulte “Criando limites para gerar eventos para o monitoramento de transações” na página 1016.

Diagnosticando problemas em seu ambiente
Se as instâncias de transação para um dos componentes em seu ambiente estiverem lentas ou falhando, o componente afetado é designado com um status apropriado.

Um nó pode ter um dos status a seguir:

- 

Bom, o nó tem um carrapato cercado por um quadrado verde no canto superior direito
- 

Aviso, o nó possui um ponto de exclamação cercado por um triângulo amarelo na Superior direito Ram R
- 

Crítico, o nó tem um plano de fundo vermelho e uma cruz que está circundada em vermelho no canto superior direito

Para identificar a causa dos problemas para esses componentes com um status de aviso ou crítico, clique com o botão direito do mouse no nó e realizar drill down para ver mais informações sobre o que pode estar causando as falhas.

Fazendo download de seus agentes e coletores de dados

É possível acessar a assinatura do Cloud APM a partir do website do IBM Marketplace. Conecte-se à sua conta e faça download dos archives de instalação. Os archives de instalação incluem arquivos de instalação e de configuração para os agentes e coletores de dados.

Você pode aprender mais sobre como fazer download de agentes e de coletores de dados concluindo as etapas nos tutoriais a seguir:

- “Tutorial: fazendo download e instalando um agente” na página 102
- “Tutorial: fazendo download e configurando um coletor de dados” na página 106

É possível inscrever-se para uma avaliação ativa ou comprar uma assinatura para uma das ofertas do IBM Cloud Application Performance Management a partir do IBM Marketplace.

IBM Marketplace

Inscreva-se para uma avaliação em IBM Marketplace > Cloud APM > Free Trial. Compre uma assinatura em IBM Marketplace > Cloud APM > Purchase . Conecte-se à página Produtos e serviços para fazer download de seus agentes e coletores de dados.

A página **Produtos e serviços** está disponível para assinantes ativos. Se você tiver problemas, acesse Marketplace support.

Testar conectividade

Para obter informações sobre como verificar a conectividade com o Servidor Cloud APM, que é usado para fazer download de pacotes, consulte Conectividade de rede.

Tutorial: fazendo download e instalando um agente

Use esse tutorial para adquirir uma experiência prática com o download e instalação de um Cloud APM Windows OS agent a partir do IBM Marketplace. É possível, então, iniciar o Console do Cloud APM e verificar o funcionamento de seu recurso monitorado visualizando os principais indicadores de desempenho (KPIs) nos painéis.

Sobre Esta Tarefa

Esse tutorial envolve o download do pacote de instalação do Windows da página **Produtos e serviços** no IBM Marketplace, a extração dos arquivos de instalação e a instalação do Windows OS agent. Você retorna ao **Produtos e serviços** para ativar o Console do Cloud APM e abrir o Application Performance Dashboard para verificar o funcionamento do sistema Windows.

Procedimento

1. Se não estiver conectado ao IBM Marketplace, conecte-se com seu IBMid e senha e acesse **Produtos e serviços**.

   A página **Produtos e serviços** está disponível para assinantes ativos. Se você tiver algum problema, acesse o Fórum do Cloud Application Performance Management ou o Marketplace support.
2. Faça download do arquivo de instalação do Windows:
   a) Na caixa de assinatura do Cloud APM, clique em **Gerenciar** > **Downloads**.
   b) Selecione o sistema operacional Windows.

      Selecione o pacote de 64 bits dos agentes do IBM Cloud Application Performance Management. Se estiver usando a versão de 32 bits do Windows, selecione o pacote do agente de 32 bits.
   c) Clique em **Download** e salve o archive de instalação do agente para seu sistema.
   Por exemplo:

   ```
   C:\Users\MY_ADMIN\Downloads\IAPM_Agent_Install.zip
   ```
3. No sistema Windows local, navegue para o diretório no qual você salvou o arquivo transferido por download e extraia-o.
   Por exemplo, no Windows Explorer, abra o diretório **Downloads**, clique com o botão direito em `IAPM_Agent_Install.zip` e selecione **Extrair todos**.
4. Abra um prompt de comandos como um administrador:
   a) No menu **Iniciar** do Windows, digite `command` na caixa de procura.
   b) Clique com o botão direito em **Prompt de Comandos** na lista que é exibida e selecione **Executar como administrador**.
5. Mude para o diretório no qual os arquivos de instalação foram extraídos.
   Por exemplo:

   ```
   cd C:\Users\MY_ADMIN\Downloads\IAPM_Agent_Install\IAPM_Agent_Install_8.1.4
   ```
6. Execute o script de instalação para instalar o Windows OS agent:

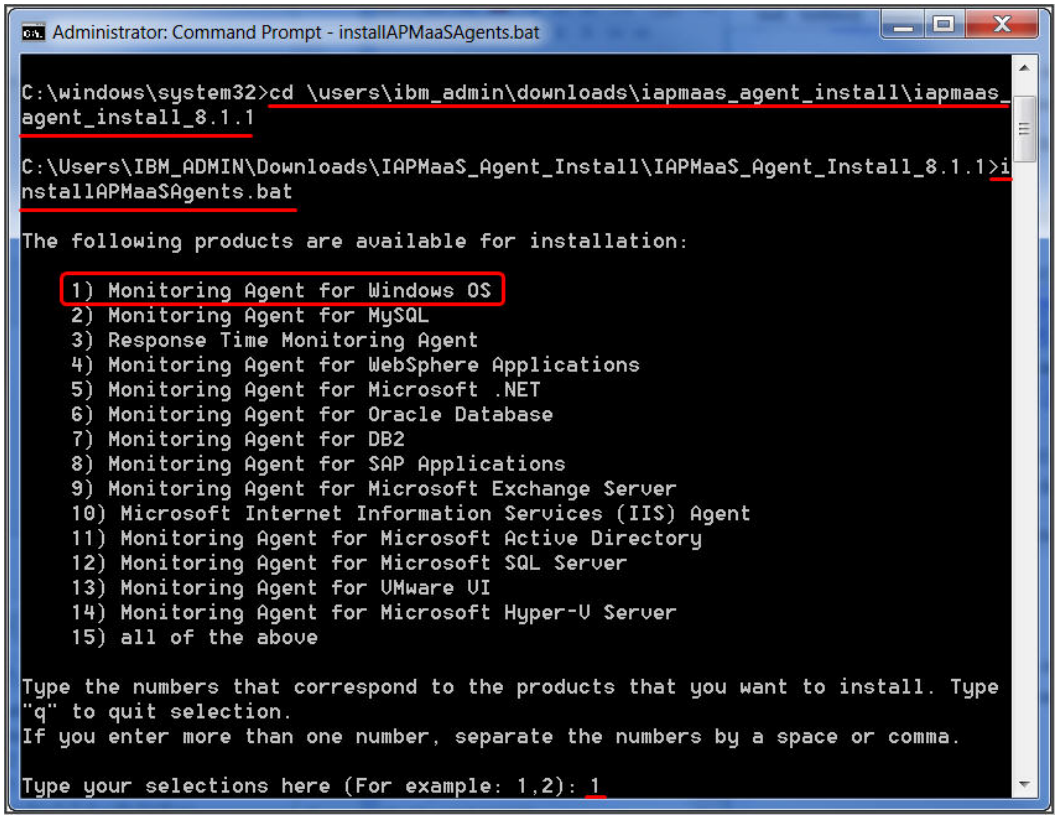
a) Insira o comando a seguir:

```
installAPMAgents.bat
```

b) Na lista de agentes disponíveis, insira o número que corresponde ao Windows OS agent.

c) Responda aos prompts para confirmar que você deseja instalar o Windows OS agent e para aceitar o contrato de licença.

Uma varredura de pré-requisito de seu ambiente é iniciada e demora alguns minutos para ser concluída. Para quaisquer requisitos ausentes, você recebe uma mensagem que o direciona para um arquivo de log com a razão da falha. Um pré-requisito como espaço em disco insuficiente parará a instalação. Deve-se resolver a falha e iniciar o script de instalação novamente. Se tiver algum problema, acesse o Fórum do Cloud Application Performance Management ou envie um e-mail para `info@ibmserviceengage.com`.



Para visualizar o relatório de requisitos do sistema operacional Windows, consulte Requisitos do sistema (APM Developer Center).

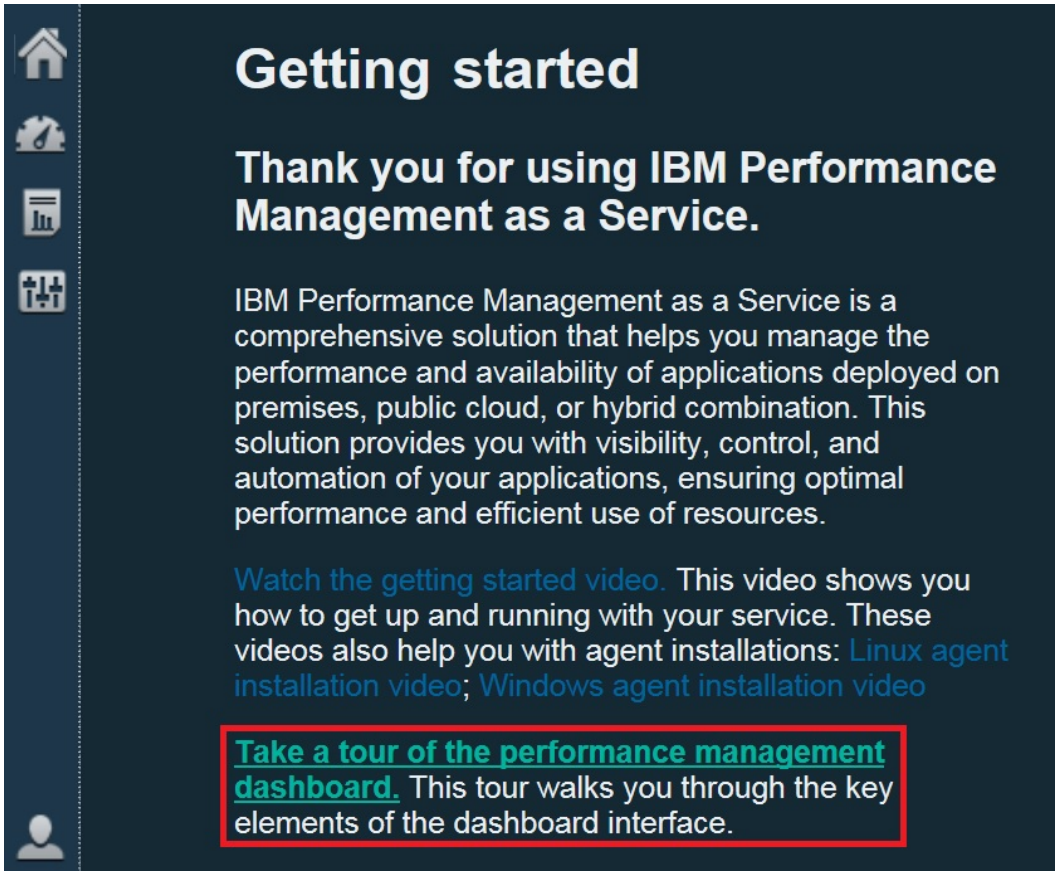
Após a instalação bem-sucedida, o Windows OS agent é iniciado automaticamente e é possível iniciar o Console do Cloud APM para começar a monitorar o sistema Windows.

Nota: Se o seu ambiente incluir um firewall que não permita conexões HTTPS de saída transparentes para um host externo, você deverá configurar um proxy de encaminhamento para comunicações entre o agente e o Servidor Cloud APM. Ao configurar um proxy de encaminhamento, é possível encaminhar todo o tráfego para um ponto específico na rede e, em seguida, permitir somente uma única conexão por meio do firewall. Para obter mais informações, consulte “Configurando agentes para se comunicar através de um proxy de encaminhamento” na página 157.

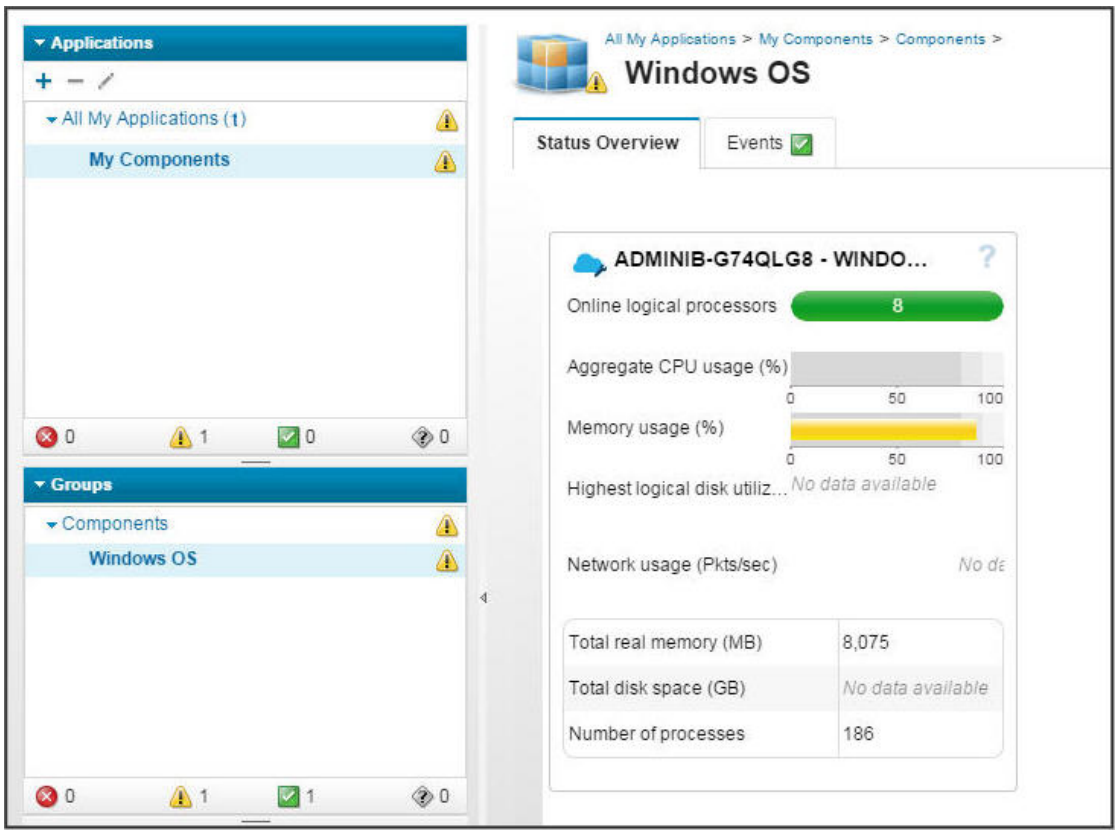
7. Volte para **Produtos e serviços** no IBM Marketplace e clique em **Ativar** a partir da caixa de assinatura do Cloud APM.

   O Console do Cloud APM é aberto na página **Introdução**, na qual é possível aprender sobre os recursos, assistir vídeos para cenários de usuário diferentes e abrir as páginas do console associado.

8. Na página **Introdução**, clique em "Fazer um tour do painel de gerenciamento de desempenho" para um tour rápido dos elementos de navegação.



9. Abra o painel de resumo do sistema operacional Windows:
   a) Na barra de navegação, clique em **Desempenho** > **Application Performance Dashboard**.
      - O painel **Todos os Meus Aplicativos** é exibido com uma caixa de status do resumo para cada aplicativo definido em seu ambiente. Inicialmente, somente o aplicativo predefinido **Meus Componentes** é exibido.
      - Se você vir uma janela **Incluir Aplicativo** em vez de **Meus Componentes**, crie um aplicativo para ver o recurso monitorado:
        1) Insira um nome para o aplicativo, tal como "Meus Aplicativos".
        2) Clique em +.
        3) Vá para o fim da lista **Selecionar Componente** e clique em **S.O. Windows**.
        4) No Editor de Componente, clique em *Host_Name*:NT primário, clique em **Incluir** e clique em **Voltar** para incluir seu agente no aplicativo.
        5) Clique em **Salvar** para fechar a janela e visualizar uma caixa de status do resumo para seu novo aplicativo no painel.
   b) Na caixa de resumo, clique em **Componentes**.
      - O painel de resumo do sistema gerenciado pelo sistema operacional Windows é exibido. A partir daqui, é possível clicar em qualquer lugar no widget de grupo de resumo do status para realizar drill down nos painéis detalhados com KPIs relatados a partir do Windows OS agent.
      - Pode demorar alguns minutos para um agente recém-iniciado se comunicar com a infraestrutura de monitoramento e enviar os KPIs para o console.



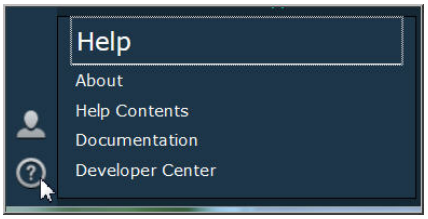
Se o agente não estiver se comunicando com o Servidor Cloud APM ou não for iniciado, o painel de resumo não mostra KPIs e o status é mostrado como desconhecido. É possível usar o comando **os-agent** para verificar o status e iniciar o agente, se necessário. Abra um prompt de comandos como um administrador e insira o comandos **os-agent status** a partir da pasta `C:\\IBM\APM\bin`. Se o agente não for iniciado, insira o comando **os-agent start**.

Resultados

Você instalou um agente do Cloud APM e observou dados de monitoramento que são enviados para o Application Performance Dashboard.

O que Fazer Depois

- Explorar o console: enquanto você estiver usando o Console do Cloud APM, explore os recursos. É possível aprender sobre o painel atual clicando em no banner da janela. É possível abrir o sistema de ajuda ou a coleção de tópico Cloud APM no IBM Knowledge Center a partir do menu **Ajuda** na barra de navegação.



- Instalação de outros agentes: você tem todos os arquivos de instalação que são necessários para instalar outros tipos de agentes do Windows para monitorar o ambiente. Você também pode instalar agentes em outros sistemas em seu ambiente. Em caso de sistemas AIX ou Linux, faça download do arquivo de instalação associado. Alguns tipos de agente precisam que pré-requisitos sejam concluídos antes de você instalá-los, e a maioria dos tipos de agente requer alguma configuração após a instalação. Para obter mais informações, consulte “Pré-instalação em sistemas AIX” na página 119,

"Pré-instalação em sistemas Linux" na página 126, "Pré-instalação em sistemas Windows" na página 134 e Capítulo 7, "Configurando seu Ambiente", na página 157.

Tutorial: fazendo download e configurando um coletor de dados

Use esse tutorial para obter uma experiência prática com o download e configuração de um coletor de dados Cloud APM Bluemix Ruby do IBM Marketplace. É possível, então, iniciar o Console do Cloud APM e verificar o funcionamento de seu recurso monitorado visualizando os principais indicadores de desempenho (KPIs) nos painéis.

Sobre Esta Tarefa

Esse tutorial envolve o download do pacote coletor de dados para aplicativos Bluemix por meio da página do **Produtos e serviços** no IBM Marketplace, extraindo os arquivos de instalação e configurando o coletor de dados do Bluemix Ruby em um sistema Linux. Retorne ao **Produtos e serviços** para ativar o Console do Cloud APM e abrir o Application Performance Dashboard para verificar o funcionamento de seu aplicativo Bluemix Ruby.

Procedimento

1. Se não estiver conectado ao IBM Marketplace, conecte-se com seu IBMid e senha e acesse **Produtos e serviços**.

   A página **Produtos e serviços** está disponível para assinantes ativos. Se você tiver algum problema, acesse o Fórum do Cloud Application Performance Management ou o Marketplace support.
2. Faça download do pacote de Coletores de dados para aplicativos Bluemix `IBM_Bluemix_Data_Collectors_Install.tgz`.
3. No sistema local, navegue para o diretório onde foi salvo o archive transferido por download e extraia-o executando o seguinte comando:

   ```
   tar -zxvf IBM_Bluemix_Data_Collectors_Install.tgz
   ```

   Você obtém seus arquivos compactados, cada um representando um coletor de dados para um tipo de aplicativo Bluemix. O pacote do coletor de dados para aplicativos Ruby Bluemix é `ruby_datacollector.tgz`.
4. Extraia os arquivos em `ruby_datacollector.tgz` executando o seguinte comando, por exemplo:

   ```
   tar -zxvf ruby_datacollector.tgz
   ```

   Você obtém uma pasta `ibm_ruby_dc`.
5. Copie toda a pasta `etc` em `ibm_ruby_dc` para a pasta raiz de seu aplicativo Ruby executando o seguinte comando, por exemplo:

   ```
   cp –r directory to the etc folder  home directory of your Ruby application
   ```

   Se você extrair o coletor de dados no diretório `/opt/ibm/ccm/ibm_ruby_dc/etc` e o diretório inicial do seu aplicativo Ruby for `/root/ruby_app/`, o comando será como a seguir:

   ```
   cp –r /opt/ibm/ccm/ibm_ruby_dc/etc /root/ruby_app/
   ```
6. Inclua a seção a seguir no `Gemfile` na pasta inicial de seu aplicativo Bluemix Ruby:

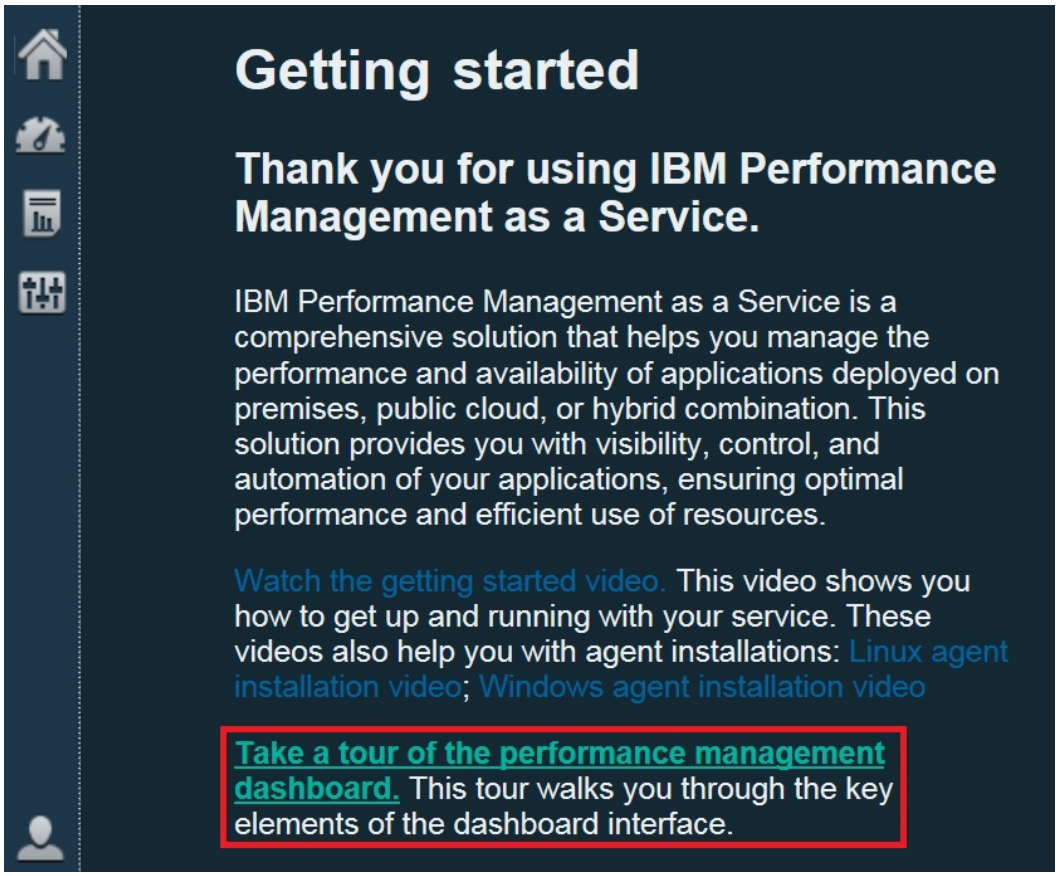
   ```
   gem 'logger',  '>= 1.2.8'
   source 'https://managemserver.ng.bluemix.net' do
     gem 'ibm_resource_monitor'
     gem 'stacktracer'
   end
   ```
7. Execute o comando `bundle lock` para gerar novamente o arquivo `Gemfile.lock`.
8. No diretório inicial de seu aplicativo Ruby, execute o seguinte comando:

   ```
   cf push
   ```

9. Volte para **Produtos e serviços** no IBM Marketplace e clique em **Ativar** a partir da caixa de assinatura do Cloud APM.

   O Console do Cloud APM é aberto na página **Introdução**, na qual é possível aprender sobre os recursos, assistir vídeos para cenários de usuário diferentes e abrir as páginas do console associado.

10. Na página **Introdução**, clique em "Fazer um tour do painel de gerenciamento de desempenho" para um tour rápido dos elementos de navegação.



11. Abra o painel de resumo de aplicativos Bluemix Ruby:

    a) Na barra de navegação, clique em **Desempenho** > **Application Performance Dashboard**.

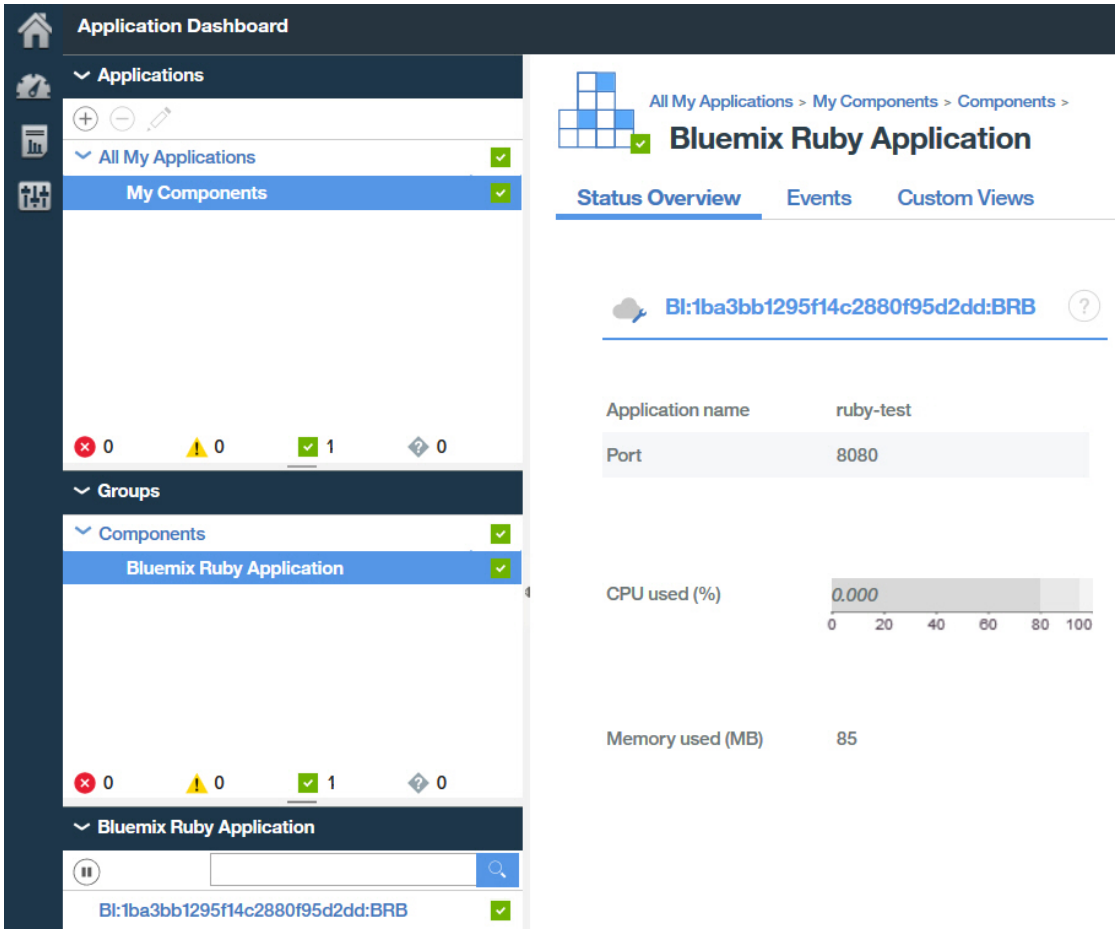
    - O painel **Todos os Meus Aplicativos** é exibido com uma caixa de status do resumo para cada aplicativo definido em seu ambiente. Inicialmente, somente o aplicativo predefinido **Meus Componentes** é exibido.
    - Se você vir uma janela **Incluir Aplicativo** em vez de **Meus Componentes**, crie um aplicativo para ver o recurso monitorado:

      1) Insira um nome para o aplicativo, tal como "Meus Aplicativos".
      2) Clique em +.
      3) Clique em **Aplicativo Ruby Bluemix**.
      4) No Editor de componente, selecione uma instância, clique em **Incluir** e clique em **Voltar** para incluir seu coletor dados no aplicativo.
      5) Clique em **Salvar** para fechar a janela e visualizar uma caixa de status do resumo para seu novo aplicativo no painel.

    b) Na caixa de resumo, clique em **Componentes**.

    - O painel de resumo para seu aplicativo Ruby Bluemix é exibido. Daqui, é possível clicar em qualquer lugar no widget de grupo de resumo de status para realizar drill down para os painéis detalhados com KPIs relatados de seu coletor de dados Ruby Bluemix.

- Pode levar alguns minutos para que um coletor de dados recém-iniciado se comunique com a infraestrutura de monitoramento e envie KPIs para o console.

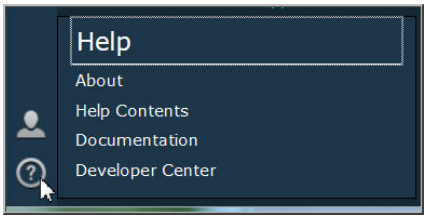


Resultados

Você instalou um coletor de dados do Cloud APM e observou dados de monitoramento que são enviados para o Application Performance Dashboard.

O que Fazer Depois

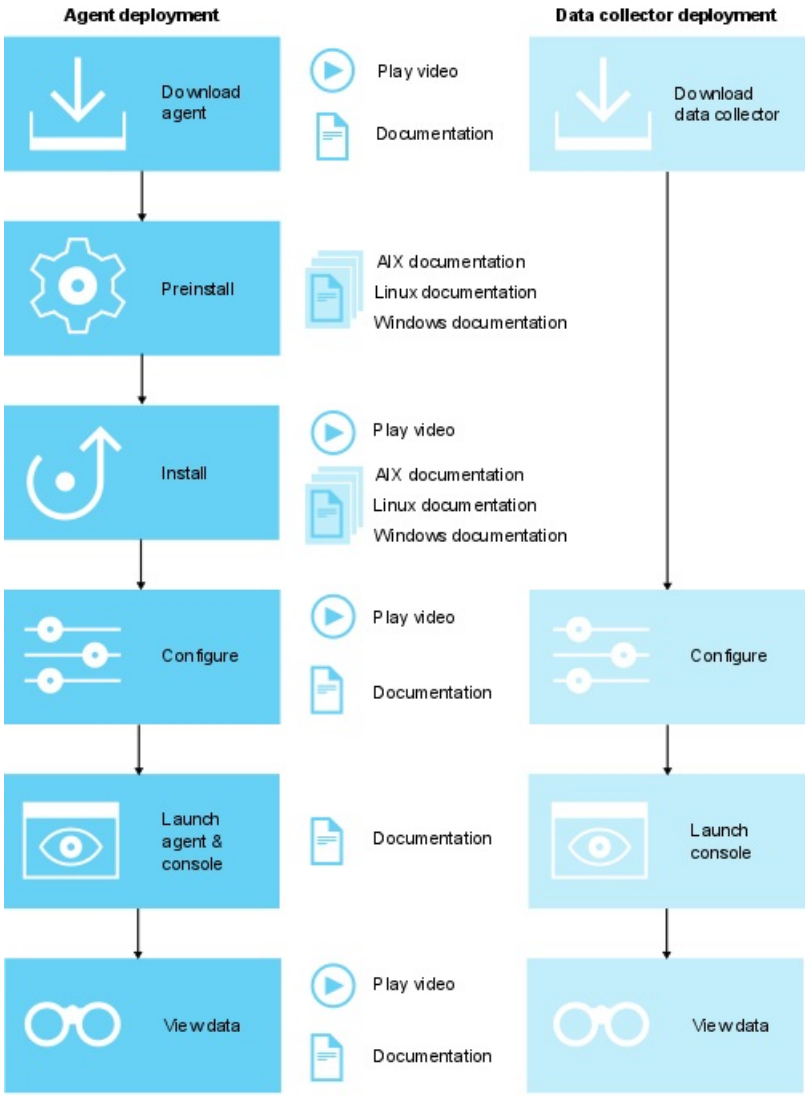
- Explorar o console: enquanto você estiver usando o Console do Cloud APM, explore os recursos. É possível aprender sobre o painel atual clicando em ⓘ no banner da janela. É possível abrir o sistema de ajuda ou a coleção de tópico Cloud APM no IBM Knowledge Center a partir do menu ⓘ **Ajuda** na barra de navegação.



- Instale outros coletores de dados: você tem todos os arquivos de instalação necessários para instalar outros tipos de coletores de dados para monitorar seu ambiente. Também é possível instalar coletores de dados em outros sistemas em seu ambiente. Para obter mais informações, consulte Capítulo 7, “Configurando seu Ambiente”, na página 157.

Capítulo 5. Implementação do agente e do coletor de dados

Os agentes variam nas tarefas que são necessárias entre a instalação e visualização dos dados que eles coletam. Algumas tarefas são tarefas automáticas e outras são manuais. Depois de fazer download de seus coletores de dados, você deve configurar manualmente cada coletor de dados.



1. Reproduzir vídeo de download
2. Fazer download da documentação
3. Documentação de pré-instalação do AIX
4. Documentação de pré-instalação do Linux
5. Documentação de pré-instalação do Windows
6. Reproduzir vídeo de instalação
7. Documentação de instalação do AIX
8. Documentação de instalação do Linux

9. Documentação de instalação do Windows
10. Reproduzir vídeos de configuração
11. Documentação de configuração
12. Ativar documentação
13. Reproduzir vídeo de dados da visualização
14. Documentação de recursos

1. Reproduzir vídeo de download
2. Fazer download da documentação
3. Documentação de pré-instalação do AIX
4. Documentação de pré-instalação do Linux
5. Documentação de pré-instalação do Windows
6. Reproduzir vídeo de instalação
7. Documentação de instalação do AIX
8. Documentação de instalação do Linux
9. Documentação de instalação do Windows
10. Reproduzir vídeos de configuração
11. Documentação de configuração
12. Ativar documentação
13. Reproduzir vídeo de dados da visualização
14. Documentação de recursos

Após a instalação, alguns agentes são configurados e iniciados automaticamente
Para qualquer agente que é iniciado, o agente é definido com as configurações padrão. Para determinar quais agentes são configurados e iniciados manualmente, consulte Tabela 7 na página 111.

Após a instalação, alguns agentes requerem configuração manual, mas iniciam automaticamente
Para obter informações sobre como configurar seus agentes, consulte Capítulo 7, “Configurando seu Ambiente”, na página 157. Para determinar quais agentes são configurados manualmente e iniciados automaticamente, consulte Tabela 7 na página 111.

Após a instalação, alguns agentes devem ser configurados e iniciados manualmente
Para qualquer agente que não seja iniciado automaticamente, você deve configurar o agente antes que ele possa ser iniciado. Para determinar quais agentes são configurados e iniciados manualmente, consulte Tabela 7 na página 111.

Agentes de múltiplas instâncias requererem a criação de uma primeira instância e o início manual.
Você deve criar a primeira instância e iniciar o agente manualmente. Um agente de várias instâncias significa que uma única instalação do agente cria uma instância de monitoramento exclusivo para cada instância exclusiva do aplicativo. Essas instâncias são visualizadas no Console do Cloud APM como resultado. Para determinar quais agentes são agentes com várias instâncias, consulte Tabela 7 na página 111.

Monitoramento de agentes de sistema operacional e de arquivo de log.
O agente do S.O. Linux, o agente de S.O. UNIX e o Windows OS agent são configurados e iniciados automaticamente. No entanto, é possível configurar o monitoramento de arquivos de log para os agentes de S.O., para que seja possível monitorar arquivos de log do aplicativo. Para obter mais informações, consulte “Configurando monitoramento de arquivo de log do OS Agent” na página 633.

Implementação do agente inicialização e características da instância do agente e do coletor de dados

Tabela 7. Lista de verificação pós-instalação

Implementação do agente ou coletor de dados	Configurado e iniciado automaticamente	Configurado manualmente e iniciado automaticamente	Configurado e iniciado manualmente	Instância múltipla (iniciado manualmente)
Agente Amazon EC2	—	—	—	✓
Agente Amazon ELB	—	—	—	✓
Agente Azure Compute	—	—	—	✓
Agente Cassandra	—	—	✓	✓
Cisco UCS agent	—	—	✓	✓
Citrix VDI agent	—	—	—	✓
DataPower agent	—	—	—	✓
DataStage agent	—	—	✓	✓
Db2	—	—	—	✓
Agente do Hadoop	—	—	✓	—
Agente HMC Base	—	—	—	✓
Agente do Servidor HTTP	✓ Deve-se revisar o arquivo de configuração que o agente cria para o HTTP Server. Em seguida, inclua a configuração do coletor de dados manualmente no arquivo de configuração do servidor.	—	—	—
IBM Cloud agent	—	—	—	✓
IBM Integration Bus agent	—	—	—	✓
Coletor de dados J2SE	—	✓	—	—
agente JBoss	—	—	—	✓
Coletor de dados Liberty	—	✓	—	—
agente do Linux KVM	—	—	✓	✓
agente do S.O. Linux	✓	—	—	—

Tabela 7. Lista de verificação pós-instalação (continuação)

Implementação do agente ou coletor de dados	Configurado e iniciado automaticamente	Configurado manualmente e iniciado automaticamente	Configurado e iniciado manualmente	Instância múltipla (iniciado manualmente)
Microsoft Active Directory agent	–	✓ Este agente é iniciado automaticamente. No entanto, você deve configurar o agente para visualizar dados para alguns atributos.	–	–
Microsoft Cluster Server agent	–	–	✓	–
Microsoft Exchange Server agent	–	✓ Este agente é iniciado automaticamente. No entanto, você deve configurar o agente para visualizar os dados para todos os atributos.	–	–
Microsoft Hyper-V Server agent	✓	–	–	–
Microsoft IIS agent	✓	–	–	–
Agente Skype for Business Server (anteriormente conhecido como agente Microsoft Lync Server)	✓	✓ Este agente é iniciado automaticamente. No entanto, você deve configurar o agente para visualizar dados para alguns atributos.	–	–
Microsoft Office 365 agent	–	–	✓	–

Tabela 7. Lista de verificação pós-instalação (continuação)

Implementação do agente ou coletor de dados	Configurado e iniciado automaticamente	Configurado manualmente e iniciado automaticamente	Configurado e iniciado manualmente	Instância múltipla (iniciado manualmente)
Microsoft .NET agent	—	✓ O coletor de dados deve ser configurado antes que os dados sejam relatados.	—	—
Microsoft SharePoint Server agent	✓	—	—	—
Microsoft SQL Server agent	—	—	—	✓ Cada instância do agente deve ser configurada e iniciada manualmente.
Agente do MQ Appliance	—	—	—	✓
Agente MongoDB	—	—	—	✓
Agente MySQL	—	—	—	✓
Agente NetApp Storage	—	—	✓	✓
Agente Node.js	—	✓ O agente deve ser configurado antes que os dados sejam relatados. Inclua um plug-in de monitoramento no aplicativo Node.js.	—	—
Coletor de dados Node.js	—	✓	—	—
OpenStack agent	—	—	✓	✓
Agente Oracle Database	—	—	—	✓
Agente PHP	—	—	—	✓
Agente PostgreSQL	—	—	—	✓
Coletor de dados do Python	—	✓	—	—
Agente RabbitMQ	—	—	✓	✓
Response Time Monitoring Agent	✓	—	—	—

Tabela 7. Lista de verificação pós-instalação (continuação)

Implementação do agente ou coletor de dados	Configurado e iniciado automaticamente	Configurado manualmente e iniciado automaticamente	Configurado e iniciado manualmente	Instância múltipla (iniciado manualmente)
Agente Ruby	—	—	—	✓ Para diagnósticos detalhados, o agente deve ser configurado antes que os dados sejam relatados. Para ativar os painéis de diagnósticos, deve-se instalar e configurar o coletor de dados diagnósticos.
Coletor de dados Ruby	—	✓	—	—
Agente SAP	—	—	✓	✓
SAP HANA Database agent	—	—	✓	✓
SAP NetWeaver Java Stack	—	—	✓	✓
Agente Siebel	—	—	—	✓
Agente Sterling Connect Direct	—	—	—	✓
Agente Sterling File Gateway	—	—	✓	✓
Sybase agent	—	—	✓	✓

Tabela 7. Lista de verificação pós-instalação (continuação)

Implementação do agente ou coletor de dados	Configurado e iniciado automaticamente	Configurado manualmente e iniciado automaticamente	Configurado e iniciado manualmente	Instância múltipla (iniciado manualmente)
Synthetic Playback agent	✓ O agente é configurado e iniciado automaticamente para aplicativos externos públicos, mas transações devem ser criadas no Gerenciador de Script Sintético antes de os dados serem relatados.	✓ O agente é iniciado automaticamente, mas deve ser configurado para aplicativos internos privados. Transações devem ser criadas no Gerenciador de Script Sintético antes de os dados serem relatados.	—	✓
Agente Tomcat	—	—	—	✓
agente de S.O. UNIX	✓	—	—	—
Agente VMware VI	—	—	✓	✓
Agente WebLogic	—	—	—	✓
WebSphere Applications agent	—	✓ O agente é iniciado automaticamente, mas o coletor de dados deve ser configurado antes que os dados sejam relatados.	—	—
WebSphere Infrastructure Manager agent	—	—	—	✓
WebSphere MQ agent	—	—	—	✓
Windows OS agent	✓	—	—	—

Capítulo 6. Instalando os agentes

A infraestrutura do IBM Cloud Application Performance Management é instalada e gerenciada pela IBM. Para monitorar seus aplicativos, selecione e instale os agentes de monitoramento para os aplicativos que você deseja monitorar. É possível instalar os agentes em sistemas operacionais Linux, AIX ou Windows. Os coletores de dados independentes não requerem instalação.

Se você escolher coletores de dados independentes para monitorar seus aplicativos, será possível ignorar o procedimento de instalação. Continue para Capítulo 7, “Configurando seu Ambiente”, na página 157 para obter instruções sobre como implementar coletores de dados para monitoramento de seus aplicativos.

Monitoramento Remoto

Alguns agentes podem ser instalados remotamente a partir do recurso que eles estão monitorando. Os seguintes agentes suportam o monitoramento remoto:

- Monitoring Agent for Amazon EC2
- Monitoring Agent for AWS Elastic Load Balancer
- Monitoring Agent for Azure Compute
- Monitoring Agent for Cassandra
- Monitoring Agent for Cisco UCS
- Monitoring Agent for Citrix Virtual Desktop Infrastructure
- Monitoring Agent for DataPower - Esse agente pode ser instalado apenas em uma máquina remota.
- Monitoring Agent for Db2
- Monitoring Agent for Hadoop
- Monitoring Agent for HMC Base
- Monitoring Agent for IBM Cloud
- Monitoring Agent for InfoSphere DataStage
- Monitoring Agent for JBoss - Se desejar usar esse agente para monitoramento de recursos, instale-o remotamente ou localmente. Se quiser usar o agente para rastreamento de transações e diagnósticos detalhados, instale-o localmente.
- Monitoring Agent for Linux KVM
- Monitoring Agent for MariaDB
- Monitoring Agent for Microsoft Cluster Server
- Monitoring Agent for Microsoft Exchange Server
- Monitoring Agent for Microsoft Office 365
- Monitoring Agent para Microsoft SharePoint Server
- Monitoring Agent for MongoDB
- Monitoring Agent for MySQL
- Monitoring Agent for NetApp Storage
- Monitoring Agent for OpenStack
- Monitoring Agent for Oracle Database
- Monitoring Agent for PostgreSQL
- Monitoring Agent for RabbitMQ
- Monitoring Agent for SAP Applications
- Monitoring Agent for SAP HANA Database

- Monitoring Agent for SAP NetWeaver Java Stack - Se desejar usar esse agente para monitoramento de recursos, instale-o remotamente ou localmente. Se quiser usar o agente para rastreamento de transações e diagnósticos detalhados, instale-o localmente.
- Monitoring Agent for Sterling Connect Direct
- Monitoring Agent for Sterling File Gateway
- Monitoring Agent for VMware VI
- Monitoring Agent for WebLogic - Se desejar usar esse agente para monitoramento de recursos, instale-o remotamente ou localmente. Se quiser usar o agente para rastreamento de transações e diagnósticos detalhados, instale-o localmente.
- Response Time Monitoring Agent - Se estiver usando o componente analisador de pacotes, o agente pode ser instalado remotamente ou localmente. Se estiver usando o módulo Tempo de Resposta do IBM HTTP Server, o agente deve ser instalado na mesma máquina que o servidor HTTP.

Instalando agentes em sistemas UNIX

Instale os agentes de monitoramento em sistemas AIX ou Solaris para os recursos que deseja gerenciar.

Lista de agentes que podem ser instalados no AIX

- Monitoring Agent for DataPower
- Monitoring Agent for Cassandra
- Monitoring Agent for Db2
- Monitoring Agent for Hadoop
- Monitoring Agent for HMC Base
- Monitoring Agent for HTTP Server
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for MQ Appliance
- Monitoring Agent for Oracle Database
- Monitoring Agent for SAP Applications
- Monitoring Agent for SAP HANA Database
- Monitoring Agent for SAP NetWeaver Java Stack
- Monitoring Agent for Siebel
- Monitoring Agent for Sybase Server
- Monitoring Agent for UNIX OS
- Monitoring Agent for WebLogic
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ
- Response Time Monitoring Agent

Lista de agentes que podem ser instalados no Solaris Sparc

- Monitoring Agent for Db2
- Monitoring Agent for HTTP Server
- Monitoring Agent for JBoss
- Monitoring Agent for MySQL
- Monitoring Agent for Oracle Database
- Monitoring Agent for SAP Applications

- Monitoring Agent for Sybase Server
- Monitoring Agent for UNIX OS
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebLogic

Lista de agentes que podem ser instalados no Solaris X86

- Monitoring Agent for Db2
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for SAP Applications
- Monitoring Agent for Sybase Server
- Monitoring Agent for UNIX OS
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ

Pré-instalação em sistemas AIX

Deve-se concluir as tarefas de pré-instalação necessárias antes de instalar agentes nos sistemas AIX. Algumas tarefas de pré-instalação são específicas do agente e outras tarefas se aplicam a vários agentes.

Nota: Estes requisitos são além dos requisitos identificados nos Software Product Compatibility Reports.

Para obter os requisitos e as dependências da versão atual para seu agente, consulte Requisitos do sistema (APM Developer Center) para obter um link para os Relatórios de compatibilidade de produto de software.

Todos os agentes

As tarefas de pré-instalação a seguir são aplicáveis a todos os agentes:

Testar conectividade
Antes de instalar os agentes, assegure-se de que seu sistema possa se comunicar com o Servidor Cloud APM. Para obter informações sobre a verificação de conectividade com o Servidor Cloud APM, consulte Conectividade de rede.

Instalação do usuário não raiz
Deve-se ter permissões de leitura, gravação e execução para o diretório de instalação. Caso contrário, a instalação será cancelada. Para obter mais informações sobre a instalação do usuário não raiz, consulte “Instalando agentes como um usuário não raiz” na página 138.

limitação de 70 caracteres para o caminho de instalação
O diretório de instalação e o caminho para ele devem ter, no máximo, 70 caracteres.

Limitação de 100 caracteres para nomes de arquivos `.tar`
O comando **`tar`** padrão nos sistemas AIX não pode manipular nomes de arquivos com mais de 100 caracteres. Para evitar problemas de instalação, execute as seguintes etapas:

1. Faça o download e instale a versão GNU do comando **`tar`**, a partir do website AIX Toolbox for Linux Applications.
2. Torne a versão GNU o comando **`tar`** padrão. Execute uma das seguintes etapas:
   - Inclua `/opt/freeware/bin` no início da variável de ambiente *PATH* atual. Por exemplo:

     ```
     export PATH=/opt/freeware/bin:$PATH
     ```

     em que /opt/freeware/bin é o diretório do bin GUN.
   - Substitua `/bin/tar` por um link simbólico para `/opt/freeware/bin/tar`, como abaixo:

     ```
     ln -s /opt/freeware/bin/tar /bin/tar
     ```

Como alternativa, faça upgrade para a versão mais recente do AIX para receber a correção de código que permite manipular nomes de arquivos com mais de 100 caracteres. Para obter detalhes, consulte o Nota técnica do comando TAR para AIX V6.1 ou o Nota técnica do comando TAR para AIX V7.1.

Configurando a variável de ambiente *CANDLEHOME*

Se você usou anteriormente o ITM Agent Converter para instalar e configurar um agente no mesmo sistema gerenciado, a variável de ambiente *CANDLEHOME* foi mudada para o diretório onde o agente foi instalado com o \Agent Converter. Antes de instalar e configurar um agente nativo Cloud APM, deve-se configurar a variável de ambiente *CANDLEHOME* para um diretório diferente, caso contrário, o agente nativo Cloud APM não poderá ser iniciado.

Agentes específicos

As seguintes tarefas de pré-instalação são aplicáveis nos agentes especificados:

DataPower agent

Antes de o agente ser instalado, o verificador de pré-requisitos verifica se *ulimit* está configurado como **unlimited** no AIX. Deve-se executar o comando **ulimit -d unlimited** para assegurar que a variável de ambiente do sistema *max data segment size* seja configurada como **unlimited**. Esse agente não pode ser instalado na mesma máquina que o dispositivo DataPower que você deseja monitorar.

Agente HMC Base

Se você planeja instalar o agente como um usuário raiz, deve assegurar que o TL07 do sistema esteja instalado. Se planeja instalar o agente como um usuário não raiz, deve assegurar que o TL08 do sistema esteja instalado somente para o AIX versão 6.

Agente do Servidor HTTP

Instale e execute esse agente como um usuário raiz. Use o mesmo ID de usuário para instalar e executar o agente. Se você instalar e executar o agente como um usuário não raiz, o usuário não raiz deve ter o mesmo ID de usuário que o usuário que iniciou o IBM HTTP Server. Caso contrário, o agente tem problemas com a descoberta do IBM HTTP Server.

A instalação falha no AIX porque no sistema AIX o comando **.tar** padrão truncou um caminho longo. Para obter mais informações, consulte a seção "Limitação de 100 caracteres para nomes de arquivos `.tar`" neste tópico.

Somente AIX: Instale o utilitário lynx ou o aplicativo curl.

Agente Oracle Database

No Red Hat Enterprise Linux versão 5 e versão 6 e no SUSE Linux Enterprise Server versão 11 e versão 12 x64, se o Agente Oracle Database monitora o banco de dados Oracle remotamente, deve-se instalar os clientes instantâneos do Oracle primeiro. Instale os clientes instantâneos Oracle a partir do Oracle Technology Network - Instant Client Downloads.

Os clientes instantâneos v10.x ,v11.x e v12.x são suportados pelo Agente Oracle Database.

Response Time Monitoring Agent

Antes de instalar o Agente Response Time Monitoring, revise a seção de planejamento de instalação aqui: “Planejando a Instalação ” na página 687.

SAP HANA Database agent

1. Instale o cliente de banco de dados SAP HANA HDBSQL versão 1.00.102.06 ou mais recente no sistema AIX.
2. Execute o comando a seguir para incluir o caminho do diretório de instalação na variável de ambiente **LIBPATH**:

   `export LIBPATH=$LIBPATH:`*`install_directory_path`*

   Exemplo: `export LIBPATH=$LIBPATH:/usr/sap/hdbclient`, onde `/usr/sap/hdbclient` indica o caminho de instalação do cliente de banco de dados do SAP HANA.

Importante:

Se o caminho de instalação do cliente de banco de dados do SAP HANA não for incluído na variável de ambiente **LIBPATH**, o scanner de pré-requisitos retornará o resultado FAIL.

A variável de ambiente incluída usando o comando de exportação persistirá somente para uma determinada sessão do terminal. Portanto, certifique-se de executar o script de instalação do agente a partir do mesmo terminal usado para incluir a variável de ambiente.

WebSphere Applications agent
Antes de instalar o agente, o verificador de pré-requisitos verifica se *ulimit* está configurado como **524000** no sistema AIX. Você deve executar o comando **ulimit -d 524000** para assegurar que a variável de ambiente do sistema *max data segment size* esteja configurada como **524000**.

Pré-instalação em sistemas Solaris

Deve-se concluir as tarefas de pré-instalação necessárias antes de instalar agentes em sistemas Solaris. Algumas tarefas de pré-instalação são específicas do agente e outras se aplicam a diversos agentes.

Nota: Estes requisitos são além dos requisitos identificados nos Software Product Compatibility Reports.

Para obter os requisitos e as dependências da versão atual para seu agente, consulte Requisitos do sistema (APM Developer Center) para obter um link para os Relatórios de compatibilidade de produto de software.

Todos os agentes

As seguintes tarefas de pré-instalação são aplicáveis a todos os agentes:

Testar conectividade
Antes de instalar os agentes, assegure-se de que seu sistema possa se comunicar com o Servidor Cloud APM. Para obter informações sobre a verificação de conectividade com o Servidor Cloud APM, consulte Conectividade de rede.

Instalação do usuário não raiz
Deve-se ter permissões de leitura, gravação e execução para o diretório de instalação. Caso contrário, a instalação será cancelada. Para obter mais informações sobre a instalação do usuário não raiz, consulte “Instalando agentes como um usuário não raiz” na página 138.

limitação de 70 caracteres para o caminho de instalação
O diretório de instalação e o caminho para ele devem ter, no máximo, 70 caracteres.

Limitação de 100 caracteres para nomes de arquivos `.tar`
O comando padrão **tar** em sistemas Solaris não pode manipular nomes de arquivos com mais de 100 caracteres. Para evitar problemas de erro @LongLink, conclua as seguintes etapas:

1. Faça o download e instale a versão GNU do comando **tar**, a partir do website http://www.gnu.org.
2. Torne a versão GNU o comando **tar** padrão. Execute uma das seguintes etapas:
   - Na variável de ambiente *PATH*, coloque a variável a seguir primeiro:

     ```
     export PATH=/opt/freeware/bin:$PATH
     ```

   - Substitua `/bin/tar` com um link simbólico para `/opt/freeware/bin/tar`

Configurando a variável de ambiente *CANDLEHOME*
Se você usou anteriormente o ITM Agent Converter para instalar e configurar um agente no mesmo sistema gerenciado, a variável de ambiente *CANDLEHOME* foi mudada para o diretório onde o agente foi instalado com o \Agent Converter. Antes de instalar e configurar um agente nativo Cloud APM, deve-se configurar a variável de ambiente *CANDLEHOME* para um diretório diferente, caso contrário, o agente nativo Cloud APM não poderá ser iniciado.

Agentes específicos

As tarefas de pré-instalação a seguir são aplicáveis aos agentes especificados:

Agente do Servidor HTTP

Instale e execute esse agente como um usuário raiz. Use o mesmo ID de usuário para instalar e executar o agente. Se você instalar e executar o agente como um usuário não raiz, o usuário não raiz deve ter o mesmo ID de usuário que o usuário que iniciou o IBM HTTP Server. Caso contrário, o agente tem problemas com a descoberta do IBM HTTP Server.

Instalando agentes

É possível instalar qualquer combinação de agentes de monitoramento em um sistema gerenciado. Por exemplo, se você instalar o Agente Ruby para monitorar aplicativos Ruby On Rails, poderá desejar também instalar o Response Time Monitoring Agent, o agente do S.O. Linux, ou ambos os agentes. Com o Agente Response Time Monitoring, é possível reunir mais informações de tempo de resposta para seus aplicativos Ruby. Com o agente do S.O. Linux, é possível monitorar outros aspectos do sistema, tal como o total de CPU, memória e disco.

A oferta determina quais agentes de monitoramento estão disponíveis para instalação. Para obter uma lista dos agentes incluídos em cada oferta, consulte “Capacidades” na página 52.

Para obter uma lista dos agentes executados em sistemas AIX e Solaris, consulte “Instalando agentes em sistemas UNIX” na página 118.

Antes de Iniciar

Faça download dos agentes. Consulte “Fazendo download de seus agentes e coletores de dados” na página 101.

Revise as informações em “Requisitos do sistema” na página 81 para ter certeza de que você atendeu os requisitos para os agentes que pretende instalar.

Revise as tarefas de pré-instalação do agente antes de instalar os agentes.

- Para sistemas AIX, consulte o “Pré-instalação em sistemas AIX” na página 119.
- Para sistemas Solaris, consulte o “Pré-instalação em sistemas Solaris” na página 121.

Importante: O Java Runtime é instalado somente quando o agente o requer e nem sempre está disponível. Além disso, o ksh não é mais necessário para instalação do agente e o SELinux no modo de aplicação é suportado.

Sobre Esta Tarefa

É possível instalar agentes de monitoramento como um usuário raiz ou usuário não raiz. Se você não tiver privilégios de administrador e desejar instalar um agente de monitoramento, será possível instalar o agente como um usuário não raiz, consulte “Instalando agentes como um usuário não raiz” na página 138. Além disso, é possível instalar o agente como um usuário não raiz, se você for um administrador do host e não desejar executar o agente de monitoramento como um usuário raiz. O fluxo de instalação é o mesmo que para um usuário raiz.

A coexistência de agente é suportada. É possível instalar agentes do IBM Cloud Application Performance Management no mesmo computador no qual agentes do IBM Tivoli Monitoring estão instalados. Entretanto, os dois tipos de agentes não podem ser instalados no mesmo diretório. Para obter mais informações sobre coexistência de agente, consulte “Coexistência do agente Cloud APM e do agente Tivoli Monitoring” na página 950.

Procedimento

1. Abra uma sessão de shell do terminal no sistema AIX ou sistema Solaris.
2. Em seu sistema, navegue para o diretório no qual você transferiu o arquivo .tar por download.

   Os agentes devem ser instalados no sistema no qual o aplicativo que você deseja monitorar está instalado. Se necessário, transfira o archive de instalação para o sistema a ser monitorado. O archive contém os agentes e o script de instalação.

   Lembre-se: Certifique-se de que o diretório não contenha uma versão mais antiga do archive.

3. Extraia os arquivos de instalação do usando o seguinte comando:

   ```
   tar -xf./installation files
   ```

   em que *installation files* é o nome do arquivo de instalação para sua oferta.

   O script de instalação é extraído para um diretório nomeado para o archive e a versão. Por exemplo: *offering*_Agent_Install_8.1.4.0. Os arquivos binários e relacionados à configuração do agente são extraídos em subdiretórios dentro desse diretório.
4. Opcional: Esta etapa é obrigatória SOMENTE para o Solaris 10. Deve-se criar um soft link para o ksh antes da execução do script de instalação no Solaris 10.
   a) Faça backup do comando /bin/sh:

      ```
      mv /bin/sh /bin/sh.bkup_origin
      ```

   b) Crie um soft link para o comando ksh:

      ```
      ln -s /bin/ksh /bin/sh
      ```

   c) Confirme se o resultado aponta para ksh:

      ```
      ls -l /bin/sh
      ```
5. Execute o script de instalação a partir do diretório nomeado para o archive e a versão:

   ```
   ./installAPMAgents.sh
   ```

   Para instalar os agentes no modo silencioso, consulte “Instalando agentes silenciosamente” na página 141.
6. Especifique se deseja instalar agentes individuais, uma combinação dos agentes ou todos os agentes.
7. Dependendo de se você está instalando ou atualizando os agentes, execute uma das etapas a seguir:
   - Se você estiver instalando os agentes, especifique um diretório inicial de instalação do agente diferente ou use o diretório padrão aplicável:
     – /opt/ibm/apm/agent
   - Se você estiver atualizando os agentes, depois de ser solicitado o diretório inicial de instalação do agente, insira o diretório de instalação da versão anterior dos agentes.
8. Quando questionado se você aceita o contrato de licença, insira 1 para aceitar o contrato e continuar ou insira 2 para recusar.

   Após inserir 1 (aceitar), uma varredura de pré-requisito de seu ambiente é iniciada e demora alguns minutos para ser concluída. Se algum dos requisitos estiver ausente, uma mensagem direcionará você para um arquivo de log com a razão da falha. Um pré-requisito, como uma biblioteca ausente ou espaço em disco suficiente, para a instalação. Deve-se abordar a falha e iniciar o script de instalação novamente.
9. Caso tenha instalado os agentes usando um ID do usuário não raiz, você deverá atualizar os scripts de inicialização do sistema (consulte “Instalando agentes como um usuário não raiz” na página 138).
10. Após a instalação ser concluída e a linha de comandos estar disponível, será possível repetir as etapas neste procedimento para instalar mais agentes de monitoramento no sistema gerenciado.

O que Fazer Depois

Configure o agente conforme necessário. Se seu agente de monitoramento requerer configuração conforme descrito em Capítulo 5, “Implementação do agente e do coletor de dados”, na página 109 ou se você desejar revisar configurações padrão, consulte Capítulo 7, “Configurando seu Ambiente”, na página 157.

- Se você estiver usando um proxy de encaminhamento porque seu firewall não permite conexões HTTPS de saída transparentes para hosts externos, deverá editar o arquivo de configuração do ambiente do

agente. Para obter instruções, veja “Configurando agentes para se comunicar através de um proxy de encaminhamento” na página 157.

- Se você fez upgrade de um agente a partir de uma versão anterior, identifique qualquer tarefa de reconfiguração ou migração que você deve concluir antes de efetuar login no Console do Cloud APM. Para obter informações sobre essas tarefas, consulte “Fazendo upgrade de agentes” na página 1139. Após um upgrade, é necessário reiniciar qualquer agente que não seja configurado e iniciado automaticamente pelo instalador.

Para iniciar um agente, execute o comando a seguir:

```
./name-agent.sh start
```

Para obter informações sobre os comandos do agente de monitoramento, incluindo o *name* a ser usado, consulte “Utilizando comandos do agente” na página 175. Para obter informações sobre quais os agentes são iniciados automaticamente e manualmente, consulte Capítulo 5, “Implementação do agente e do coletor de dados”, na página 109.

Após um upgrade, é necessário reiniciar qualquer agente que não seja configurado e iniciado automaticamente pelo instalador.

Depois de configurar e iniciar o agente, visualize os dados que o agente está coletando.

- Se você não estiver com login efetuado, siga as instruções em “Iniciando o Console do Cloud APM” na página 975.
- Se você deseja visualizar sistemas gerenciados de seu domínio do IBM Tivoli Monitoring no Application Performance Dashboard, conclua as tarefas descritas em “Integrando com o IBM Tivoli Monitoring V6.3 ” na página 949.

Instalando agentes nos sistemas Linux

Instale agentes de monitoramento em seus sistemas Linux para os recursos que você deseja gerenciar.

- Monitoring Agent for Amazon EC2
- Monitoring Agent for AWS Elastic Load Balancer
- Monitoring Agent for Azure Compute
- Monitoring Agent for Cassandra
- Monitoring Agent for Cisco UCS
- Monitoring Agent for Citrix Virtual Desktop Infrastructure
- Monitoring Agent for DataPower
- Monitoring Agent for Db2
- Monitoring Agent for Hadoop
- Monitoring Agent for HTTP Server
- Monitoring Agent for IBM Cloud
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for Internet Services
- Monitoring Agent for MQ Appliance
- Monitoring Agent for InfoSphere DataStage
- Monitoring Agent for JBoss
- Monitoring Agent for Linux OS
- Monitoring Agent for Linux KVM
- Monitoring Agent for MariaDB
- Monitoring Agent for Microsoft SQL Server

- Monitoring Agent for MongoDB
- Monitoring Agent for MySQL
- Monitoring Agent for NetApp Storage
- Monitoring Agent for Node.js
- Monitoring Agent for OpenStack
- Monitoring Agent for Oracle Database
- Monitoring Agent for PHP
- Monitoring Agent for PostgreSQL
- Monitoring Agent for RabbitMQ
- Monitoring Agent for Ruby
- Monitoring Agent for SAP Applications
- Monitoring Agent for SAP HANA Database
- Monitoring Agent for SAP NetWeaver Java Stack
- Monitoring Agent for Siebel
- Monitoring Agent for Sterling Connect Direct
- Monitoring Agent for Sterling File Gateway
- Monitoring Agent for Sybase Server
- Monitoring Agent for Synthetic Playback
- Monitoring Agent for Tomcat
- Monitoring Agent for VMware VI
- Monitoring Agent for WebLogic
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere Infrastructure Manager
- Monitoring Agent for WebSphere MQ
- Response Time Monitoring Agent

Os seguintes agentes são suportados nos sistemas Linux on Power Little Endian (pLinux LE):

- Monitoring Agent for Db2
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for Linux OS
- Monitoring Agent for Tomcat - Suporte disponível para monitoramento de recursos.
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ

Os agentes a seguir são suportados nos sistemas Linux for System z:

- Monitoring Agent for Db2
- Monitoring Agent for HTTP Server - O rastreamento de transação não é suportado.
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for Linux OS
- Response Time Monitoring Agent
- Monitoring Agent for Tomcat
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ

O seguinte agente é suportado em sistemas Linux for System x:

- Monitoring Agent for HTTP Server - O rastreamento de transação não é suportado.

Pré-instalação em sistemas Linux

Deve-se concluir as tarefas de pré-instalação necessárias antes de instalar agentes nos sistemas Linux. Algumas tarefas de pré-instalação são específicas do agente e outras se aplicam a diversos agentes.

Nota: Estes requisitos são além dos requisitos identificados nos Software Product Compatibility Reports.

Para obter os requisitos e as dependências da versão atual para seu agente, consulte Requisitos do sistema (APM Developer Center) para obter um link para os Relatórios de compatibilidade de produto de software.

Todos os agentes

As tarefas de pré-instalação a seguir são aplicáveis a todos os agentes:

Testar conectividade
Antes de instalar os agentes, assegure-se de que seu sistema possa se comunicar com o Servidor Cloud APM. Para obter informações sobre a verificação de conectividade com o Servidor Cloud APM, consulte Conectividade de rede.

Instalação do usuário não raiz
Deve-se ter permissões de leitura, gravação e execução para o diretório de instalação. Caso contrário, a instalação será cancelada. Para obter mais informações sobre a instalação do usuário não raiz, consulte "Instalando agentes como um usuário não raiz" na página 138.

limitação de 70 caracteres para o caminho de instalação
O diretório de instalação e o caminho para ele devem ter, no máximo, 70 caracteres.

Configurando a variável de ambiente *CANDLEHOME*
Se você usou anteriormente o ITM Agent Converter para instalar e configurar um agente no mesmo sistema gerenciado, a variável de ambiente *CANDLEHOME* foi mudada para o diretório onde o agente foi instalado com o \Agent Converter. Antes de instalar e configurar um agente nativo Cloud APM, deve-se configurar a variável de ambiente *CANDLEHOME* para um diretório diferente, caso contrário, o agente nativo Cloud APM não poderá ser iniciado.

Sistemas operacionais específicos

Red Hat Enterprise Linux (RHEL) 8

O pacote libnsl.so.1 é necessário no RHEL 8

Por padrão, o `libnsl.so.1` não é instalado no Red Hat Enterprise Linux liberação 8.0. Sem esse pacote, nenhum agente pode ser instalado com sucesso. Deixe seu administrador configurar um repositório yum para você e, em seguida, execute este comando:

```
yum install libnsl
```

Após a instalação bem-sucedida, é possível ver `/usr/lib64/libnsl.so.1`.

Nota: O pacote `libnsl.so.1` é necessário somente para agentes. Não é preciso executar esta etapa para coletores de dados.

Ignorando o scanner de pré-requisitos para alguns agentes

Antes de o scanner de pré-requisitos ser atualizado para se tornar compatível com os requisitos mais recentes, para alguns agentes, é possível ignorar o scanner de pré-requisitos. Para obter cenários adequados e instruções, consulte "Efetuando bypass do scanner de pré-requisitos" na página 142.

Nota: Não é preciso executar esta etapa para coletores de dados.

Agentes específicos

As tarefas de pré-instalação a seguir são aplicáveis aos agentes especificados:

DataPower agent

Deve-se executar o comando **ulimit -d unlimited** para assegurar que a variável de ambiente do sistema *max data segment size* seja configurada como **unlimited**. Esse agente não pode ser instalado na mesma máquina que o dispositivo DataPower que você deseja monitorar.

DataStage agent

1. Ative parâmetros no arquivo DSODBConfig.cfg. Conclua as etapas a seguir:
   a. Abra o arquivo DSODBConfig.cfg no seguinte local em um editor:

      infosphere_information_server_install_dir/Server/DSODB

   b. Remova o comentário dos seguintes parâmetros removendo o símbolo #:

      MonitorLinks=1
      JobRunUsage=1
      ResourceMonitor=1
      DSODBON=1

   c. Edite valores desses parâmetros iguais a 1.
2. Copie o driver JDBC do banco de dados usado para configuração de repositório de metadados no computador agente.
   a. Tipo 4 JDBC 4 ou mais recente. Exemplo: db2jcc4.jar
   b. Driver JDBC Tipo 4 para Oracle. Exemplo: ojdbc6.jar
   c. Driver JDBC para MS SQL:
      - Sqljdbc41.jar requer um JRE de 7 e suporta a API JDBC 4.1.
      - Sqljdbc42.jar requer um JRE de 8 e suporta a API JDBC 4.2.

Agente do Servidor HTTP

Se instalar esse agente como um usuário raiz, deverá usar o mesmo ID do usuário para executar e configurar o agente.

Ao instalar e executar o agente como um usuário não raiz, é necessário que o usuário não raiz tenha o mesmo ID de usuário que o usuário que iniciou o IBM HTTP Server. Caso contrário, o agente tem problemas com a descoberta do IBM HTTP Server. É possível usar o mesmo ID do usuário para executar e configurar o agente.

agente do Linux KVM

O Monitoring Agent for Linux KVM é um agente de diversas instâncias e conexões e suporta conexões com o hypervisor KVM baseado no Linux Corporativo e nos ambientes do Red Hat Enterprise Virtualization Manager (RHEV-M). É possível criar múltiplas instâncias desse agente para monitorar múltiplos hypervisors em um ambiente do hypervisor RHEV-M ou KVM. É possível monitorar as cargas de trabalho virtualizadas e analisar a capacidade de recurso em diferentes máquinas virtuais. Para conectar o agente a uma máquina virtual no ambiente do hypervisor KVM, você deve instalar os pré-requisitos: libvirt * .rpm e Korn Shell Interpreter (pdksh). O agente coleta métricas conectando-se remotamente a um hypervisor libvirt que gerencia as máquinas virtuais.

Microsoft SQL Server agent

Para monitorar um ambiente Microsoft SQL, o driver Microsoft SQL Server e Microsoft SQL ODBC deve ser instalado antes de instalar o Monitoring Agent for Microsoft SQL Server. Por exemplo, para instalar o driver ODBC no Red Hat Enterprise Linux, use o comando a seguir:

```
sudo yum install unixODBC
sudo yum install msodbcsql17
```

Para concluir a execução do verificador de pré-requisitos, o agente precisa ser configurado na Correção provisória de servidor 15 do Cloud Application Performance Management Versão 8.1.4.0 (8.1.4.0-IBM-APM-SERVER-IF0015. tar) ou mais recente.

Agente MongoDB

Deve-se instalar e configurar o Agente MongoDB no sistema em que o servidor de banco de dados MongoDB está instalado.

Agente MySQL

Para monitorar um ambiente MySQL, o servidor MySQL e o driver JDBC MySQL deverão ser instalados antes de você instalar o Monitoring Agent for MySQL. Por exemplo, para instalar o driver JDBC no Red Hat Enterprise Linux, use o comando a seguir:

```
yum install mysql-connector-java
```

Após iniciar a instalação do agente e durante a verificação de pré-requisito para o nome do pacote MySQL, você pode receber um aviso se um provedor diferente de RedHat é usado, tal como Oracle. Se o MySQL Server e o driver JDBC estiverem disponíveis, o aviso não fará com que a instalação falhe e será possível desconsiderar a mensagem. Saída de amostra:

```
Scenario: Prerequisite Scan
KSE - Monitoring Agent for MySQL Prerequisite Checker [version 01000005]:
Property                                Result   Found
Expected
========                          ====== =====       ========
os.package.mysql-server         WARN  Unavailable  mysql-server-5.1.12+
os.package.mysql-connector-java WARN Unavailable mysql-connector-java-5.
1.12+
```

Agente Node.js

A versão de Node.js usada para executar seu aplicativo monitorado deve ser a mesma que a versão padrão instalada.

Atualmente, Node.js v5 não é suportado.

OpenStack agent

Antes de poder usar o agente OpenStack agent, deve-se ter o software a seguir no servidor em que o agente é instalado:

- Python 2.6.0 ou mais recente ou Python 2.7.0 ou mais recente
- Clientes do OpenStack mais recente:
  - OpenStack
  - Pedra angular
  - Neutron
  - Swift

  Para instalar os clientes da linha de comandos do OpenStack, consulte Instalar os clientes da linha de comandos do OpenStack.
- Biblioteca Paramiko para acesso remoto em Python.

  Nota: Se você deseja instalar o OpenStack agent em um servidor RedHat Linux limpo, antes de instalar a biblioteca Paramiko, execute o seguinte comando para instalar o software necessário:

  ```
  Wget https://ftp.dlitz.net/pub/dlitz/crypto/pycrypto/pycrypto-2.6.1.tar.gz
  Yum install gcc/openssl-devel/libffi-devel
  ```
- ShellKorn

Agente Oracle Database

No Red Hat Enterprise Linux versão 5 e versão 6 e no SUSE Linux Enterprise Server versão 11 e versão 12 x64, se o Agente Oracle Database monitora o banco de dados Oracle remotamente, deve-se instalar os clientes instantâneos do Oracle primeiro. Instale os clientes instantâneos Oracle a partir do Oracle Technology Network - Instant Client Downloads.

Os clientes instantâneos v10.x ,v11.x e v12.x são suportados pelo Agente Oracle Database.

Agente PHP

Se o aplicativo PHP for implementado usando o usuário raiz, deve-se usar o usuário raiz para instalar, configurar, iniciar ou parar o agente. Se o aplicativo PHP for implementado usando um usuário não raiz, é possível usar o usuário raiz ou o mesmo usuário não raiz para instalar, configurar, iniciar ou parar o agente.

Você deve ter um aplicativo WordPress existente instalado. O Agente PHP monitora o WordPress V3.7.1 ou posterior.

O agente avalia somente o desempenho de solicitações PHP em aplicativos WordPress. Carregamento CSS e JS não são avaliados.

O agente não usa argumentos de URL para identificar URLs.

Coletor de dados do Python

O Coletor de dados do Python monitora aplicativos Django.

Response Time Monitoring Agent

Antes de instalar o Agente Response Time Monitoring, revise a seção de planejamento de instalação aqui: “Planejando a Instalação ” na página 687.

SAP HANA Database agent

1. Instale o cliente de banco de dados SAP HANA HDBSQL versão 1.00.102.06 ou mais recente no sistema Linux.

   Importante: Para o sistema operacional RHEL 5.x de 64 bits, instale o Linux SUSE 9 no cliente de banco de dados x86_64 64bit SAP HANA em vez do Linux on x86_64 64bit. Para os sistemas operacionais RHEL 6.x, ou mais recente de 64 bits, instale o Linux no cliente de banco de dados x86_64 64bit SAP HANA.

2. Execute o comando a seguir para incluir o caminho do diretório de instalação na variável de ambiente **LD_LIBRARY_PATH**:

   `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:`*`install_directory_path`*

   Exemplo: `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/sap/hdbclient`, onde `/usr/sap/hdbclient` indica o caminho de instalação do cliente de banco de dados do SAP HANA.

Importante:

Se o caminho de instalação do cliente de banco de dados do SAP HANA não for incluído na variável de ambiente **LD_LIBRARY_PATH**, o scanner de pré-requisitos retornará o resultado FAIL.

A variável de ambiente incluída usando o comando de exportação persistirá somente para uma determinada sessão do terminal. Portanto, certifique-se de executar o script de instalação do agente a partir do mesmo terminal usado para incluir a variável de ambiente.

Synthetic Playback agent

Para instalar o Synthetic Playback agent, o usuário do sistema operacional requer as seguintes permissões:

- Ativar permissão de leitura e execução para a imagem de instalação
- Ativar permissão de gravação para o início do agente

Para executar o Synthetic Playback agent, o usuário do sistema operacional requer as seguintes permissões:

- Ativar permissão de leitura, gravação e execução para o local de instalação do agente e seus subdiretórios e arquivos.
- Ativar permissão para executar o Mozilla Firefox.
- Certifique-se de que o binário de execução do Mozilla Firefox esteja na variável de ambiente PATH do perfil do usuário.

Antes de instalar Synthetic Playback agent, deve-se concluir as etapas a seguir:

1. Sincronize os locais de instalação do agente com o Console do Cloud APM.
2. Instale o Mozilla Firefox e o servidor de exibição Xvfb.
3. Verifique se o servidor de exibição Xvfb está funcionando. Execute o comando:

```
# Xvfb -ac
```

Não deve haver nenhuma saída de erro.

4. Verifique se o processo Xvfb está em execução. Execute o seguinte comando:

```
# ps -ef|grep Xvfb
```

Saída de amostra:

```
root 7192 1 0 Jan14 ? 00:00:14 Xvfb -ac
root 20393 17900 0 02:05 pts/0 00:00:00 grep -i xvfb
```

5. Pare o processo Xvfb. Execute o seguinte comando:

```
# kill -9 7192
```

6. Navegue para *install_dir*/etc/hosts e edite o início dos arquivos host para incluir os parâmetros a seguir:

```
127.0.0.1 localhost
```

Em seguida, salve e feche os arquivos host.

WebSphere Applications agent

Antes de instalar o agente, o verificador de pré-requisitos verifica se *ulimit* está configurado como **524000** no sistema Linux. Você deve executar o comando **ulimit -d 524000** para assegurar que a variável de ambiente do sistema *max data segment size* esteja configurada como **524000**.

Instalando agentes

É possível instalar qualquer combinação de agentes de monitoramento em um sistema gerenciado. Por exemplo, se você instalar o Agente Ruby para monitorar aplicativos Ruby On Rails, poderá desejar também instalar o Response Time Monitoring Agent, o agente do S.O. Linux, ou ambos os agentes. Com o Agente Response Time Monitoring, é possível reunir mais informações de tempo de resposta para seus aplicativos Ruby. Com o agente do S.O. Linux, é possível monitorar outros aspectos do sistema, tal como o total de CPU, memória e disco.

A oferta determina quais agentes de monitoramento estão disponíveis para instalação. Para obter uma lista dos agentes incluídos em cada oferta, consulte “Capacidades” na página 52.

Para obter uma lista dos agentes que são executados em sistemas Linux, consulte “Instalando agentes nos sistemas Linux” na página 124.

Antes de Iniciar

Faça download dos agentes. Consulte “Fazendo download de seus agentes e coletores de dados” na página 101.

Revise as informações em “Requisitos do sistema” na página 81 para ter certeza de que você atendeu os requisitos para os agentes que pretende instalar.

Revise as tarefas de pré-instalação do agente antes de instalar os agentes. Para obter detalhes, consulte “Pré-instalação em sistemas Linux” na página 126.

Nota: O Java Runtime é instalado somente quando o agente o requer e nem sempre está disponível. Além disso, o ksh não é mais necessário para instalação do agente, exceto para instalação do Summarization and Pruning Agent, que é instalado durante a instalação do Servidor Cloud APM. O SELinux no modo forçado é suportado.

Sobre Esta Tarefa

É possível instalar agentes de monitoramento como um usuário raiz ou usuário não raiz. Se você não tiver privilégios de administrador e desejar instalar um agente de monitoramento, será possível instalar o

agente como um usuário não raiz, consulte "Instalando agentes como um usuário não raiz" na página 138. Além disso, é possível instalar o agente como um usuário não raiz, se você for um administrador do host e não desejar executar o agente de monitoramento como um usuário raiz. O fluxo de instalação é o mesmo que para um usuário raiz.

A coexistência de agente é suportada. É possível instalar agentes do IBM Cloud Application Performance Management no mesmo computador no qual agentes do IBM Tivoli Monitoring estão instalados. Entretanto, os dois tipos de agentes não podem ser instalados no mesmo diretório. Para obter mais informações sobre coexistência de agente, consulte "Coexistência do agente Cloud APM e do agente Tivoli Monitoring" na página 950.

Procedimento

1. Abra uma sessão de shell do terminal no sistema Red Hat Enterprise Linux.
2. Em seu sistema, navegue para o diretório no qual você transferiu por download o arquivo .tar

   Os agentes devem ser instalados no sistema no qual o aplicativo que você deseja monitorar está instalado. Se necessário, transfira o archive de instalação para o sistema a ser monitorado. O archive contém os agentes e o script de instalação.

   Lembre-se: Certifique-se de que o diretório não contenha uma versão mais antiga do archive.
3. Extraia os arquivos de instalação do usando os comandos a seguir, que dependem de sua oferta:

   ```
   tar -xf ./installation files.tar
   ```

   em que *installation files* é o nome do arquivo de instalação para sua oferta.

   O script de instalação é extraído para um diretório nomeado para o archive e a versão. Por exemplo: *offering*_Agent_Install_8.1.4.0. Os arquivos binários e relacionados à configuração do agente são extraídos em subdiretórios dentro desse diretório.
4. Execute o script de instalação a partir do diretório nomeado para o archive e a versão:

   ```
   ./installAPMAgents.sh
   ```

   Para instalar os agentes no modo silencioso, consulte "Instalando agentes silenciosamente" na página 141.
5. Especifique se deseja instalar agentes individuais, uma combinação dos agentes ou todos os agentes.
6. Dependendo de se você está instalando ou atualizando os agentes, execute uma das etapas a seguir:
   - Se você estiver instalando os agentes, especifique um diretório inicial de instalação do agente diferente ou use o diretório padrão aplicável:
     - /opt/ibm/apm/agent
   - Se você estiver atualizando os agentes, depois de ser solicitado o diretório inicial de instalação do agente, insira o diretório de instalação da versão anterior dos agentes.
     a. Caso haja uma versão mais antiga dos agentes no diretório /opt/ibm/apm/agent, você deverá especificar um novo diretório de instalação. Na próxima etapa, você será questionado se deseja migrar a configuração do agente a partir do diretório /opt/ibm/apm/agent.
     b. Se você confirmar que deseja migrar a configuração do agente do diretório de instalação antigo (/opt/ibm/ccm/agent) para o novo diretório de instalação, por exemplo, /opt/ibm/apm/agent, será necessário iniciar o agente no novo local de instalação.

        Restrição: A versão mais antiga do agente é interrompida automaticamente no local de instalação antigo, mas ela não é iniciada automaticamente no novo local de instalação.
     c. Após a instalação ser concluída e você verificar se o agente funciona no novo diretório de instalação, deve-se desinstalar a versão mais antiga do agente do diretório /opt/ibm/ccm/agent. Caso deseje remover todos os agentes, execute o comando **/opt/ibm/ccm/agent/bin/smai-agent.sh uninstall_all**.

7. Quando questionado se você aceita o contrato de licença, insira 1 para aceitar o contrato e continuar ou insira 2 para recusar.

   Após inserir 1 (aceitar), uma varredura de pré-requisito de seu ambiente é iniciada e demora alguns minutos para ser concluída. Se algum dos requisitos estiver ausente, uma mensagem direcionará você para um arquivo de log com a razão da falha. A ausência de um pré-requisito, como uma biblioteca ausente ou espaço em disco insuficiente, para a instalação. Deve-se abordar a falha e iniciar o script de instalação novamente.

   Nota: Se a instalação sair com a seguinte mensagem, verifique se o serviço do servidor foi iniciado (Iniciar -> Ferramentas Administrativas -> Serviços). Se não, inicie o serviço do Servidor e execute `installAPMAgents.bat` novamente.

   ```
   This script [installAPMAgents.bat] must be run as Administrator.
   ```

8. Caso tenha instalado os agentes usando um ID do usuário não raiz, você deverá atualizar os scripts de inicialização do sistema (consulte "Instalando agentes como um usuário não raiz" na página 138).
9. Após a instalação ser concluída e a linha de comandos estar disponível, será possível repetir as etapas neste procedimento para instalar mais agentes de monitoramento no sistema gerenciado.

O que Fazer Depois

Configure o agente conforme necessário. Se seu agente de monitoramento requerer configuração conforme descrito em Capítulo 5, "Implementação do agente e do coletor de dados", na página 109 ou se você desejar revisar configurações padrão, consulte Capítulo 7, "Configurando seu Ambiente", na página 157.

- Se você estiver usando um proxy de encaminhamento porque seu firewall não permite conexões HTTPS de saída transparentes para hosts externos, deverá editar o arquivo de configuração do ambiente do agente. Para obter instruções, veja "Configurando agentes para se comunicar através de um proxy de encaminhamento" na página 157.
- Se você fez upgrade de um agente a partir de uma versão anterior, identifique qualquer tarefa de reconfiguração ou migração que você deve concluir antes de efetuar login no Console do Cloud APM. Para obter informações sobre essas tarefas, consulte "Fazendo upgrade de agentes" na página 1139. Após um upgrade, é necessário reiniciar qualquer agente que não seja configurado e iniciado automaticamente pelo instalador.

Para iniciar um agente, execute o comando a seguir:

```
./name-agent.sh start
```

Para obter informações sobre os comandos do agente de monitoramento, incluindo o nome a ser utilizado, consulte "Utilizando comandos do agente" na página 175. Para obter informações sobre quais os agentes são iniciados automaticamente e manualmente, consulte Capítulo 5, "Implementação do agente e do coletor de dados", na página 109.

Após um upgrade, é necessário reiniciar qualquer agente que não seja configurado e iniciado automaticamente pelo instalador.

Depois de configurar e iniciar o agente, visualize os dados que o agente está coletando.

- Se você não estiver com login efetuado, siga as instruções em "Iniciando o Console do Cloud APM" na página 975.
- Se você deseja visualizar sistemas gerenciados de seu domínio do IBM Tivoli Monitoring no Application Performance Dashboard, conclua as tarefas descritas em "Integrando com o IBM Tivoli Monitoring V6.3 " na página 949.

Instalando agentes nos sistemas Windows

É possível instalar alguns dos agentes de monitoramento do Cloud APM em sistemas Windows.

Os seguintes agentes de monitoramento são suportados em sistemas Windows de 64 bits. No local indicado, os agentes também são suportados em sistemas Windows de 32 bits.

- Monitoring Agent for Amazon EC2
- Monitoring Agent for AWS Elastic Load Balancer
- Monitoring Agent for Azure Compute
- Monitoring Agent for Cassandra
- Monitoring Agent for Cisco UCS
- Monitoring Agent for Citrix Virtual Desktop Infrastructure
- Monitoring Agent for Db2
- Monitoring Agent for Hadoop
- Monitoring Agent for HTTP Server*
- Monitoring Agent for IBM Cloud
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for Internet Services*
- Monitoring Agent for MQ Appliance
- Monitoring Agent for JBoss
- Monitoring Agent for MariaDB
- Monitoring Agent for Microsoft Active Directory*
- Monitoring Agent for Microsoft Cluster Server*
- Monitoring Agent for Microsoft Exchange Server
- Monitoring Agent for Microsoft Hyper-V Server
- Monitoring Agent for Microsoft Internet Information Services
- Monitoring Agent for Skype for Business Server (anteriormente conhecido como Microsoft Lync Server)*
- Monitoring Agent for Microsoft .NET
- Monitoring Agent for Microsoft Office 365
- Monitoring Agent para Microsoft SharePoint Server
- Monitoring Agent for Microsoft SQL Server*
- Monitoring Agent for MySQL
- Monitoring Agent for NetApp Storage
- Monitoring Agent for Oracle Database
- Monitoring Agent for PostgreSQL
- Monitoring Agent for RabbitMQ
- Monitoring Agent for SAP Applications
- Monitoring Agent for SAP HANA Database
- Monitoring Agent for SAP NetWeaver Java Stack
- Monitoring Agent for Siebel
- Monitoring Agent for Sterling Connect Direct
- Monitoring Agent for Sterling File Gateway
- Monitoring Agent for Sybase Server
- Monitoring Agent for Tomcat
- Monitoring Agent for VMware VI
- Monitoring Agent for WebLogic
- Monitoring Agent for WebSphere Applications

- Monitoring Agent for WebSphere MQ
- Monitoring Agent for Windows OS*
- Response Time Monitoring Agent*

* Suportados em sistemas Windows de 64 bits e de 32 bits.

Pré-instalação em sistemas Windows

Deve-se concluir as tarefas de pré-instalação necessárias antes de instalar agentes nos sistemas Windows. Algumas tarefas de pré-instalação são específicas do agente e outras tarefas se aplicam a vários agentes.

Nota: Estes requisitos são além dos requisitos identificados nos Software Product Compatibility Reports.

Para obter os requisitos e as dependências da versão atual para seu agente, consulte Requisitos do sistema (APM Developer Center) para obter um link para os Relatórios de compatibilidade de produto de software.

Todos os agentes

As seguintes tarefas de pré-instalação são aplicáveis a todos os agentes:

Testar conectividade
Antes de instalar os agentes, assegure-se de que seu sistema possa se comunicar com o Servidor Cloud APM. Para obter informações sobre a verificação de conectividade com o Servidor Cloud APM, consulte Conectividade de rede.

Instalação a partir do prompt de comandos em uma unidade local
Use o prompt de comandos do Windows para iniciar o script de instalação. Não use o Windows PowerShell para iniciar o script de instalação.

Copie os arquivos de instalação para um disco local ou para uma unidade de rede mapeada e, em seguida, inicie o script de instalação. Não inicie o script de instalação a partir de um local de rede.

Inicie o script de instalação a partir de um novo prompt de comandos. Não inicie o script de instalação a partir de um prompt de comandos existente porque é possível que esse prompt de comandos tenha variáveis de ambiente obsoletas.

Configurando a variável de ambiente *CANDLEHOME*
Se você usou anteriormente o ITM Agent Converter para instalar e configurar um agente no mesmo sistema gerenciado, a variável de ambiente *CANDLEHOME* foi mudada para o diretório onde o agente foi instalado com o \Agent Converter. Antes de instalar e configurar um agente nativo Cloud APM, deve-se configurar a variável de ambiente *CANDLEHOME* para um diretório diferente, caso contrário, o agente nativo Cloud APM não poderá ser iniciado.

Agentes específicos

As tarefas de pré-instalação a seguir são aplicáveis aos agentes especificados:

DataStage agent

1. Ative parâmetros no arquivo `DSODBConfig.cfg`. Conclua as etapas a seguir:
   a. Abra o arquivo `DSODBConfig.cfg` no seguinte local em um editor:

      ```
      infosphere_information_server_install_dir\Server\DSODB
      ```

   b. Remova o comentário dos seguintes parâmetros removendo o símbolo *#*:

      ```
      MonitorLinks=1
      JobRunUsage=1
      ResourceMonitor=1
      DSODBON=1
      ```

   c. Edite valores desses parâmetros iguais a 1.

2. Copie o driver JDBC do banco de dados usado para configuração de repositório de metadados no computador agente.
   a. Tipo 4 JDBC 4 ou mais recente. Exemplo: `db2jcc4.jar`
   b. Driver JDBC Tipo 4 para Oracle. Exemplo: `ojdbc6.jar`
   c. Driver JDBC para MS SQL:
      - `Sqljdbc41.jar` requer um JRE de 7 e suporta a API JDBC 4.1.
      - `Sqljdbc42.jar` requer um JRE de 8 e suporta a API JDBC 4.2.

IBM Integration Bus agent

Certifique-se de que o ID do usuário para instalar o IBM Integration Bus agent esteja no grupo de usuários `mqbrkrs`.

Monitoramento de Serviço da Internet

Para o Monitoramento de Serviço da Internet, deve-se aplicar a Correção Temporária 3 da estrutura principal do IBM Cloud Application Performance Management 8.1.4.0 no APM Server a partir daqui e, em seguida, pré-configurar o agente. O Agente e o módulo de ponte usam as portas 9510 e 9520. Se essas portas já estiverem em uso, a instalação não avançará.

Nota:

- Para usuários existentes, é recomendável instalar o agente do Monitoramento de Serviço da Internet em plataformas de 64 bits, seja Windows ou Linux, em vez de fazer upgrade do agente na plataforma Windows de 32 bits para uma versão mais recente.
- O Monitoramento de Serviço da Internet Agent não suporta o Windows 2008 R2 em plataforma Windows de 64 bits.

Agente MySQL

Para Monitoring Agent for MySQL, deve-se instalar o servidor MySQL e o driver JDBC MySQL antes de instalar o Agente MySQL no sistema. Para instalar o driver JDBC, veja MySQL Connector/Driver JDBC J.

Agente Oracle Database

Se o Agente Oracle Database monitora o banco de dados Oracle remotamente, é necessário primeiro instalar os clientes instantâneos Oracle a partir do Oracle Technology Network - Instant Client Downloads nos seguintes sistemas:

- Windows Server 2012 de 64 bits
- Windows Server 2012 R2 de 64 bits
- Windows Server 2008 R2 Datacenter de 64 bits
- Windows Server 2008 R2 Enterprise de 64 bits
- Windows Server 2008 R2 Standard de 64 bits

Os clientes instantâneos v10.x, v11.x e v12.x são suportados pelo Agente Oracle Database.

Response Time Monitoring Agent

Antes de instalar o Agente Response Time Monitoring, revise a seção de planejamento de instalação aqui: “Planejando a Instalação ” na página 687.

SAP HANA Database agent

1. Instale o cliente de banco de dados SAP HANA HDBSQL versão 1.00.102.06 ou mais recente no sistema Windows.
2. Inclua o caminho de instalação do cliente do SAP HANA na variável de ambiente **PATH**.

   Exemplo: Inclua `C:\Program Files\sap\hdbclient` na variável de ambiente **PATH**, onde `C:\Program Files\sap\hdbclient` indica o caminho de instalação do cliente de banco de dados do SAP HANA.

Agente Tomcat

1. O Java SDK está instalado no servidor Tomcat no qual o agente está instalado.

2. O caminho SDK é incluído na variável *PATH* diretamente ou usando o comando **set path** antes de instalar o agente.
3. O comando **JAR** está funcionando.

Instalando agentes

É possível instalar qualquer combinação de agentes de monitoramento em um sistema gerenciado. Por exemplo, se você instalar o Monitoring Agent for MySQL para o monitoramento de servidores MySQL, talvez também queira instalar o Response Time Monitoring Agent para reunir mais informações de tempo de resposta para seus aplicativos Ruby. Você também pode desejar instalar o Monitoring Agent for Windows OS para monitorar outros aspectos do sistema, tais como o total de CPU, memória e disco.

Sua oferta determina quais agentes de monitoramento estão disponíveis para instalação. Para obter uma lista dos agentes incluídos em cada oferta, consulte "Capacidades" na página 52.

Para obter uma lista dos agentes que são executados em um sistema Windows, consulte "Pré-instalação em sistemas Windows" na página 134.

Antes de Iniciar

Faça download dos agentes. Consulte "Fazendo download de seus agentes e coletores de dados" na página 101.

Revise as informações em "Requisitos do sistema" na página 81 para ter certeza de que você atendeu os requisitos para os agentes que pretende instalar.

Revise as tarefas de pré-requisito do agente antes de instalar os agentes. Para obter detalhes, consulte "Pré-instalação em sistemas Windows" na página 134.

Sobre Esta Tarefa

Assegure-se de ter permissão adequada para executar o script de instalação do agente e comandos do agente. Deve-se ter efetuado login usando um dos seguintes tipos de conta do usuário:

- conta do usuário administrador padrão do Windows
- conta do usuário administrador
- conta do usuário, que seja membro do grupo de administradores
- conta do usuário, que seja registrada como um administrador nos serviços do Active Directory

A coexistência de agente é suportada. É possível instalar agentes do IBM Cloud Application Performance Management no mesmo computador no qual agentes do IBM Tivoli Monitoring estão instalados. Entretanto, os dois tipos de agentes não podem ser instalados no mesmo diretório. Para obter mais informações sobre a coexistência de agentes, consulte "Coexistência do agente Cloud APM e do agente Tivoli Monitoring" na página 950.

Procedimento

Conclua estas etapas para instalar agentes de monitoramento em VMs e sistemas nos quais o sistema operacional Windows está instalado:

1. Em seu sistema, navegue para o diretório no qual você transferiu o arquivo compactado por download.
2. Extraia os arquivos de instalação do agente para sua oferta (ou ofertas) para o local onde deseja instalar o software do agente de monitoramento.
   O script de instalação .bat é extraído para um diretório nomeado para o archive e a versão. Por exemplo: *offering*_Agent_Install_8.1.4.0. Os arquivos binários e relacionados à configuração do agente são extraídos em subdiretórios dentro desse diretório.
3. Abra um prompt de comandos como administrador.
   a) A partir do menu **Iniciar**, digite comando na caixa de procura.
   b) Clique com o botão direito em **Prompt de Comandos** na lista que é exibida e selecione **Executar como administrador**.

4. No prompt de comandos, execute o script de instalação com privilégios de Administrador no diretório que é nomeado para o archive e a versão:

   ```
   cd offering_Agent_Install_version
   installAPMAgents.bat
   ```

   Restrição: Para o WebSphere Applications agent, os privilégios de administrador devem ser os mesmos privilégios que foram usados para instalar o WebSphere Application Server.

   Para instalar os agentes no modo silencioso, consulte “Instalando agentes silenciosamente” na página 141.
5. Se você estiver instalando os agentes, forneça o nome do diretório de instalação.

   O caminho da instalação padrão é `C:\IBM\APM`. O nome do diretório de instalação não pode exceder 80 caracteres e nem conter caracteres não ASCII, especiais ou caracteres de byte duplo. Os nomes de diretórios no caminho podem conter somente os seguintes caracteres: `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ _\:0123456789()~-./`.

   Nota: Quando a criação de nome curto de arquivo (*8dot3Name*) estiver desativada, se os nomes de diretório no caminho contiverem espaços, a instalação não será suportada.

   Se estiver fazendo upgrade do agente, essa etapa será ignorada e o agente será instalado no diretório de instalação anterior.
6. Quando questionado se você aceita o contrato de licença, insira 1 para aceitar o contrato e continuar ou insira 2 para recusar.

   Após inserir 1 (aceitar), uma varredura de pré-requisito de seu ambiente é iniciada e demora alguns minutos para ser concluída. Se algum dos requisitos estiver ausente, uma mensagem direcionará você para um arquivo de log com a razão da falha. A ausência de um pré-requisito, como uma biblioteca ausente ou espaço em disco insuficiente, para a instalação. Deve-se abordar a falha e iniciar o script de instalação novamente.

   Nota: Se a instalação sair com a seguinte mensagem, verifique se o serviço do servidor foi iniciado (Iniciar -> Ferramentas Administrativas -> Serviços). Se não, inicie o serviço do Servidor e execute `installAPMAgents.bat` novamente.

   ```
   This script [installAPMAgents.bat] must be run as Administrator.
   ```
7. Após a instalação ser concluída e o prompt de comandos estar disponível, repita estas etapas para instalar mais agentes de monitoramento.

O que Fazer Depois

Configure seus agentes conforme necessário. Para verificar se seu agente de monitoramento requer configuração manual, consulte Capítulo 5, “Implementação do agente e do coletor de dados”, na página 109. Para obter instruções de configuração ou se desejar revisar as definições de configuração padrão, consulte Capítulo 7, “Configurando seu Ambiente”, na página 157.

Antes de instalar os novos agentes, o Windows Installer para temporariamente todos os agentes atualmente em execução no local do produto instalado. Após a conclusão da instalação, o instalador reinicia quaisquer agentes interrompidos. Deve-se reiniciar manualmente qualquer agente de monitoramento que não tiver sido iniciado automaticamente pelo instalador.

- Se você estiver usando um proxy de encaminhamento porque seu firewall não permite conexões HTTPS de saída transparentes para hosts externos, deverá editar o arquivo de configuração do ambiente do agente. Para obter instruções, veja “Configurando agentes para se comunicar através de um proxy de encaminhamento” na página 157.
- Se você fez upgrade de um agente a partir de uma versão anterior, identifique qualquer tarefa de reconfiguração ou migração que precise concluir antes de efetuar login no Console do Cloud APM. Para obter informações sobre essas tarefas, consulte “Fazendo upgrade de agentes” na página 1139.

Use um dos métodos a seguir para iniciar o agente:

- Clique em **Iniciar** > **Todos os programas** > **Agentes IBM Monitoring** > **IBM Cloud Application Performance Management**. Clique com o botão direito em um agente e clique em **Iniciar**.
- Execute o seguinte comando

```
name-agent.bat start
```

Para obter informações sobre os comandos do agente de monitoramento, incluindo o nome a ser utilizado, consulte "Utilizando comandos do agente" na página 175. Para obter informações sobre quais agentes são iniciados automaticamente e manualmente, consulte Capítulo 5, "Implementação do agente e do coletor de dados", na página 109

Após um upgrade, é necessário reiniciar qualquer agente que não seja configurado e iniciado automaticamente pelo instalador.

Depois de configurar e iniciar o agente, visualize os dados que o agente está coletando.

- Se você não estiver com login efetuado, siga as instruções em "Iniciando o Console do Cloud APM" na página 975.
- Se você deseja visualizar sistemas gerenciados de seu domínio do IBM Tivoli Monitoring no Application Performance Dashboard, conclua as tarefas descritas em "Integrando com o IBM Tivoli Monitoring V6.3 " na página 949.

Instalando agentes como um usuário não raiz

Se você não tiver privilégios de administrador e deseja instalar um agente de monitoramento, é possível instalar o agente como um usuário não raiz. Além disso, é possível instalar o agente como um usuário não raiz, se você for um administrador do host e não desejar executar o agente de monitoramento como um usuário raiz. O fluxo de instalação é o mesmo que para um usuário raiz. Após uma instalação não raiz, execute o script **UpdateAutoRun.sh** com acesso de usuário raiz ou de usuário sudo.

Antes de Iniciar
Para identificar exclusivamente o sistema de computador, o agente do S.O. Linux deve identificar o identificador exclusivo universal (UUID), fabricante, modelo e número de série da placa-mãe do computador. Essas informações são necessárias antes da inclusão do agente em um aplicativo no console do Cloud APM .

Obtenha as informações do sistema de computador verificando se as seguintes entidades existem no sistema de computador:

1. Verifique se o comando **/usr/bin/hal-get-property** está instalado no sistema de computador e se o processo hald (HAL daemon) está em execução. Se o comando não estiver instalado, continue na etapa 2. Se o comando estiver instalado, pule para a etapa 2 e etapa 3. Nota: se a versão do S.O. for Red Hat 7, o processo hald não estará disponível.
2. Se o comando **/usr/bin/hal-get-property** não estiver instalado no sistema de computador, confirme se o arquivo `/sys/class/dmi/id/product_uuid` existe e contém o UUID do sistema de computador e se o usuário que instala o agente de S.O. Linux possui acesso de leitura a esse arquivo. Se esse arquivo não existir, continue na etapa 3. Se o arquivo existir, ignore a etapa 3.
3. Se o comando **/usr/bin/hal-get-property** não estiver instalado e o arquivo `/sys/class/dmi/id/product_uuid` não existir, será necessário assegurar que os comandos **hostname** ou **hostnamectl** retornem o nome completo do host. Se esses comandos retornarem o nome do host abreviado sem o domínio, será necessário configurar o nome completo do host inserindo os comandos **"hostname <fqhn>"** ou **"hostnamectl set-hostname <fqhn>"**, em que *<fqhn>* deve ser substituído pelo nome completo do host.

Nota: O agente do S.O. Linux recupera essas informações periodicamente, portanto, os comandos ou arquivos nas etapas anteriores devem permanecer no local, mesmo após a instalação.

Nota: O Linux OS Agent não suporta o monitoramento do Docker durante a execução como não raiz.

Procedimento

1. Instale seus agentes de monitoramento no Linux ou UNIX conforme descrito em "Instalando agentes nos sistemas Linux" na página 124 e "Instalando agentes em sistemas UNIX" na página 118.
2. Opcional: Se você instalou o seu agente como um usuário selecionado e deseja configurar o agente como um usuário diferente, execute o script `./secure.sh`.

   Para obter mais informações sobre o script **`./secure.sh`**, consulte "Configurando agentes como um usuário não raiz" na página 181 e Protegendo os arquivos de instalação do agente.

   Por exemplo: **`./secure.sh -g db2iadm1`**
3. Opcional: Configure seus agentes de monitoramento no Linux ou UNIX conforme necessário; consulte Capítulo 7, "Configurando seu Ambiente", na página 157.
4. Para atualizar os scripts de inicialização do sistema, execute o script a seguir com acesso de usuário raiz ou de usuário sudo: *`install_dir`*`/bin/UpdateAutoRun.sh`

O que Fazer Depois

Se você instalou seu agente como um usuário não raiz e deseja configurar o agente como o mesmo usuário, nenhuma ação especial será necessária. Se você instalou o seu agente como um usuário selecionado e deseja configurar o agente como um usuário diferente, consulte "Configurando agentes como um usuário não raiz" na página 181.

Se você instalou e configurou seu agente como um usuário não raiz e deseja iniciar o agente como o mesmo usuário, nenhuma ação especial será necessária. Se você instalou e configurou seu agente como um usuário selecionado e deseja iniciar o agente como um usuário diferente, consulte "Iniciando agentes como um usuário não raiz" na página 1012.

Use o mesmo ID de usuário para a instalação e os upgrades do agente.

Se você executar o script **`UpdateAutoRun.sh`** como usuário raiz, o agente será configurado para iniciar automaticamente após a reinicialização do sistema operacional. Se você não deseja este comportamento do agente, é possível desativar o início automático do agente. Para obter mais informações, consulte "Desativando o início automático do agente em sistemas UNIX e Linux" na página 182.

Protegendo os arquivos de instalação do agente

Após instalar agentes de monitoramento como um usuário não raiz em sistemas Linux ou UNIX, é possível executar o script `secure.sh` para proteger a instalação do agente removendo permissões de gravação mundiais e configurando a propriedade correta do arquivo.

Antes de Iniciar

- Deve-se ter permissões de leitura, gravação e execução para o diretório de instalação.
- A instalação dos agentes de monitoramento e qualquer configuração de agente devem ser concluídas no sistema e os agentes devem ser iniciados com êxito.
- Se você estiver executando os agentes como diferentes contas de usuário, eles devem ser membros do mesmo grupo. (Consulte a opção `-g`.)

Sobre Esta Tarefa

Conclua esta etapa para bloquear as permissões de arquivo em sua instalação. As opções estão disponíveis para não solicitarem senha raiz, para especificarem um nome de grupo e para visualizar ajuda para o comando.

Procedimento

- Execute o seguinte comando a partir do diretório *`install_dir`*`/bin`. Uso:

```
secure.sh [-g common_group] [-n] [-h]
```

- No modo mais simples, execute o script **./secure.sh**, que remove as permissões de gravação global e configura o usuário atual e o grupo do usuário como os proprietários do arquivo. Se o script for executado por um usuário não raiz, será solicitada ao usuário a senha raiz.
- Se um usuário não raiz executar o script **./secure.sh** com a opção -n, não será solicitada a esse usuário uma senha raiz. Nesse caso, a mudança de permissões de arquivo e a mudança de propriedade são feitas usando privilégios deste usuário. Se o diretório de instalação contiver arquivos que pertencem a diferentes usuários e o usuário atual não tiver privilégios para modificar as permissões e a propriedade dos arquivos de outro usuário, esse modo poderá falhar.
- Se você deseja configurar um determinado grupo como o proprietário do grupo, o proprietário deve fornecer a opção -g com um nome de grupo válido como um argumento para essa opção. (Consulte Exemplo.)
  Execute `secure.sh -g common_group`.
  O comando altera a propriedade dos arquivos e diretórios recursivamente.

  Se o grupo *common_group* não for o grupo primário do usuário, será possível configurar o grupo *common_group* para ser o proprietário do grupo de novos arquivos criados em um diretório, executando o seguinte comando:

  ```
  chmod g+s install_dir/bin/sub_dir
  ```

  em que *sub_dir* é qualquer subdiretório, por exemplo, /opt/ibm/ccm/agent.
- Execute o script **./secure.sh** com a opção –h para obter informações de ajuda para o script.

Resultados
O diretório de instalação permite acesso somente ao usuário que executou o script ou somente para os usuários no grupo especificado.

Exemplo

Se a usuária Alice for membro do grupo de sistemas que é denominado "apmgroup", ela poderá usar o grupo para configurar a propriedade do grupo de arquivos com o comando a seguir:

```
./secure.sh -g apmgroup
```

Após o script ser executado, o grupo será configurado como "apmgroup" para todos os arquivos em *install_dir* para o grupo.

O que Fazer Depois

A execução do script **./secure.sh** deve resultar nas seguintes permissões sendo configuradas para os agentes.

```
rwx rwx ---
```

Após executar o script, verifique as permissões para os arquivos do agente. Por exemplo, para Monitoramento de Tempo de Resposta, verifique os arquivos em *install_dir*/*arch*/hu/lib/mod_wrt.so. Se as permissões para esses arquivos não estiverem configuradas corretamente, atualize as permissões manualmente. Por exemplo, para o agente Monitoramento de Tempo de Resposta:

1. Configure as permissões, execute:

   ```
   chmod g+rx
   $AGENT_HOME/bin/rt-agent.sh
   ```

2. Configure o usuário e grupo, execute:

   ```
   chown
   newuser:newgroup
   $AGENT_HOME/bin/rt-agent.sh
   ```

Instalando agentes silenciosamente

Instalar agentes silenciosamente reduz o tempo de instalação. Para instalar um agente de monitoramento no modo silencioso, deve-se fazer download de um archive da imagem de instalação do agente do site de download da IBM Marketplace do agente, extrair os arquivos de instalação do agente, preparar um arquivo de resposta silencioso e executar o script de instalação no modo silencioso.

Antes de Iniciar

1. Revise os pré-requisitos para instalação dos agentes de monitoramento e faça download e extraia os arquivos de instalação do agente. Para obter detalhes, consulte Instalando agentes em sistemas UNIX, Instalando agentes em sistemas Linux ou Instalando agentes em sistemas Windows.
2. Conclua as etapas a seguir para preparar um arquivo de resposta silencioso para instalar agentes:
   a. Localize o arquivo de instalação silenciosa para sua oferta (ou ofertas) *offering*`_silent_install.txt`, faça uma cópia desse arquivo e abra-o em um editor de texto.
   b. Remova o comentário do contrato de licença.
   c. Conclua uma das etapas a seguir para especificar os agentes que você deseja instalar:
      - Remova o comentário dos agentes individuais a serem instalados. Por exemplo:

        ```
        INSTALL_AGENT=os
        ```

        ```
        INSTALL_AGENT=ruby
        ```

      - Remova o comentário de `INSTALL_AGENT=all` para instalar todos os agentes.
   d. Remova o comentário `AGENT_HOME` e especifique o diretório no qual deseja instalar os agentes.

      Lembre-se: Linux Se estiver fazendo upgrade de agentes em um sistema Linux, você não deverá especificar o diretório `/opt/ibm/apm/agent`.
   e. Linux Se você estiver fazendo upgrade dos agentes em um sistema Linux, remova o comentário de `MIGRATE_CONF=yes`.
   f. Salve o arquivo.

Procedimento

1. Na linha de comandos, mude para o diretório no qual você extraiu o script de instalação e execute o comando a seguir:

   ```
   cd offering_Agent_Install_version
   ```

2. Opcional: Esta etapa é obrigatória SOMENTE para o Solaris 10. Deve-se criar um soft link para o ksh antes da execução do script de instalação no Solaris 10.
   a) Faça backup do comando `/bin/sh`:

   ```
   mv /bin/sh /bin/sh.bkup_origin
   ```

   b) Crie um soft link para o comando ksh:

   ```
   ln -s /bin/ksh /bin/sh
   ```

   c) Confirme se o resultado aponta para ksh:

   ```
   ls -l /bin/sh
   ```

3. Execute o comando de instalação:
   - Linux AIX

```
./installAPMAgents.sh -p path_to_silent_response_file
```

- Windows

```
installAPMAgents.bat -p path_to_silent_response_file
```

A instalação do agente falhará no Windows se o scanner de pré-requisitos não puder obter o tipo de disco no qual o agente deve ser instalado. Se isso ocorrer, você verá um resultado de falha para a propriedade validDestLocation no arquivo de log de instalação. Nesse caso, é possível ignorar o scanner de pré-requisitos incluindo SKIP_PRECHECK=1 no comando de instalação. Por exemplo:

```
installAPMAgents.bat -p path_to_silent_response_file SKIP_PRECHECK=1
```

Nota: Windows Quando a criação de nome curto de arquivo (*8dot3Name*) estiver desativada, se os nomes de diretório no caminho contiverem espaços, a instalação não será suportada.

Resultados
Os agentes são instalados.

O que Fazer Depois

Configure os agentes. Consulte o procedimento e a tabela de comandos para sistemas Linux e UNIX e para sistemas Windows.

Efetuando bypass do scanner de pré-requisitos

Ao instalar agentes de monitoramento, inicia-se uma varredura de pré-requisito do ambiente e ela pode demorar alguns minutos para ser concluída. Se algum dos requisitos estiver ausente, uma mensagem direcionará você para um arquivo de log com a razão da falha. Em alguns cenários de instalação, você talvez queira ignorar mensagens de aviso ou efetuar bypass completamente da verificação de pré-requisito.

Sobre Esta Tarefa

Há dois níveis de mensagens de falha, WARN e FAIL, e há dois níveis de bypass:

- A configuração da variável **IGNORE_PRECHECK_WARNING** faz com que o instalador ignore as mensagens de aviso (WARN).
- A configuração da variável **SKIP_PRECHECK** faz com que o instalador ignore todas as mensagens de falha.

Caso a instalação do agente tenha falhado e você tenha recebido um aviso (WARN) do verificador de pré-requisitos, revise o aviso. Se quiser continuar com a instalação, configure **IGNORE_PRECHECK_WARNING** e instale novamente.

Em um ambiente no qual você tem imagens de máquina virtual que servem como modelos, a varredura de pré-requisito que é executada antes que a instalação comece pode ser feita somente na primeira imagem do modelo. Se uma imagem de VM passar a varredura, as outras VMs criadas a partir dessa imagem também passarão. É possível economizar tempo efetuando bypass da verificação de pré-requisito para outras VMs que foram criadas a partir da mesma imagem. Configure a variável **SKIP_PRECHECK** e instale novamente.

A configuração **SKIP_PRECHECK** também é adequada para um cenário no qual há um novo sistema operacional que o Suporte IBM ou os Relatórios de compatibilidade de produto de software indicam que é suportado, mas o verificador de pré-requisitos ainda não foi atualizado. Primeiro, certifique-se de tentar instalar o agente, verifique o log e assegure-se de que esse novo S.O. seja o único item com falha – e o único item do qual se está efetuando bypass – porque **SKIP_PRECHECK** faz com que o instalador efetue bypass de cada item na lista de verificação de pré-requisito.

Após o download e a extração dos arquivos de instalação, conclua este procedimento para ignorar as mensagens de aviso ou para efetuar bypass da varredura de pré-requisito.

Procedimento

No sistema no qual os agentes de monitoramento serão instalados, insira um dos seguintes comandos:

- Ignorar as mensagens de aviso (WARN) durante a verificação de pré-requisito:
  - Linux AIX `export IGNORE_PRECHECK_WARNING=1`
  - Windows `set IGNORE_PRECHECK_WARNING=1`
- Efetuar bypass da varredura de pré-requisito:
  - Linux AIX `export SKIP_PRECHECK=1`
  - Windows `set SKIP_PRECHECK=1`

O que Fazer Depois

Para restaurar a configuração padrão na próxima vez em que desejar instalar o agente com o scanner de pré-requisitos, desative a variável **IGNORE_PRECHECK_WARNING** ou **SKIP_PRECHECK**:

- Linux AIX `unset IGNORE_PRECHECK_WARNING`
- Windows `set IGNORE_PRECHECK_WARNING=`

ou

- Linux AIX `unset SKIP_PRECHECK`
- Windows `set SKIP_PRECHECK=`

Desinstalando os agentes

Desinstale um único agente ou todos os agentes de um sistema gerenciado.

Antes de Iniciar

Para agentes de várias instâncias, você deve remover todas as instâncias de agente antes de desinstalar o agente. Caso contrário, as entradas do agente não serão limpas do registro. Para remover instâncias, execute o seguinte comando:

- Windows *name*`-agent.bat remove` *instance_name*
- Linux AIX `./`*name*`-agent.sh remove` *instance_name*

em que *name* é o nome do agente e *instance_name* é o nome da instância. Para obter mais informações, consulte “Utilizando comandos do agente” na página 175. Para obter uma lista de agentes de várias instâncias, consulte Tabela 7 na página 111.

Para os agentes a seguir, uma tarefa específica do agente deve ser concluída antes de concluir o procedimento de desinstalação:

- Para o Monitoring Agent for HTTP Server, você deve excluir a instrução `Include` no arquivo `http.conf`, por exemplo, `"Include "/opt/ibm/apm/agent/tmp/khu/kvm65s2_8044.conf"`, antes de reiniciar o IBM HTTP Server.
- Para o Monitoring Agent for Python, execute *install_dir*`/lx8266/pg/bin/uninstall.sh` para remover os códigos de injeção antes de desinstalar o agente.
- Para o Monitoring Agent for PHP, execute *install_dir*`/bin/lx8266/pj/lib/uninstall.`*instance_name*`.sh` para mover os códigos de injeção antes de desinstalar o agente.

- Para o Monitoring Agent for WebSphere Applications, é necessário desconfigurar o coletor de dados para todas as instâncias do servidor monitorado antes de desinstalar o agente. Siga as instruções em "WebSphere Applications agent: desconfigurando o coletor de dados" na página 145.

  Para o WebSphere Applications agent, certifique-se de que o ID do usuário, que é usado para desinstalar o agente, tenha permissões completas de leitura e gravação para os diretórios `logs` e `runtime` e todos os seus subdiretórios e arquivos contidos no diretório inicial do coletor de dados. O diretório inicial do coletor de dados é o seguinte:

  – Windows *install_dir*\dchome\7.3.0.14.08

  – Linux AIX *install_dir*/yndchome/7.3.0.14.08
- Para o Agente Node.js, você deve remover o plug-in de monitoramento a partir do seu aplicativo Node.js antes de desinstalar o agente. Siga as instruções em "Agente Node.js: Removendo o plug-in de monitoramento" na página 154.
- Para o Microsoft .NET agent, é necessário remover o coletor de dados dos aplicativos Node.NET antes de desinstalar o agente. Siga as instruções em "Microsoft .NET agent: Removendo o coletor de dados .NET" na página 155.
- Para o IBM Integration Bus agent, se você configurou o rastreamento de transação para intermediários com a saída de usuário fornecida pelo agente, deverá remover a saída de usuário antes de desinstalar o agente. Siga as instruções em "Removendo a saída de usuário KQIUserExit" na página 288.
- Para o Monitoramento de Serviço da Internet, acesse `<candle_home>\BIN` e execute o arquivo ism-agent.bat com `uninstall` como um argumento. Caso você deseja desinstalar todos os agentes de monitoramento no servidor usando smai-agent.bat, primeiramente execute o ism-agent.bat com `uninstall` como um argumento e, em seguida, execute o smai-agent.bat
- Para o Monitoring Agent for SAP NetWeaver Java Stack, antes de desinstalar o agente, pare todas as instâncias do agente SAP NetWeaver Java Stack usando o seguinte comando:

  – Windows `sap_netweaver_java_stack-agent.bat stop instance_name`

Sobre Esta Tarefa

Nos sistemas Windows, o agente Oracle pode ser desinstalado somente usando o prompt de comandos.

Procedimento

1. Na VM ou no sistema em que o agente de monitoramento (ou agentes) está instalado, inicie uma linha de comandos e mude para o diretório binário:
   - Linux AIX *install_dir*/bin
   - Windows *install_dir*\BIN

   em que *install_dir* é o diretório de instalação do(s) agente(s) de monitoramento.
2. Para desinstalar um agente de monitoramento específico, insira o nome do script do agente e a opção de desinstalação, em que *name* é o nome do script do agente:
   - Linux AIX `./`*name*`-agent.sh uninstall`
   - Windows *name*`-agent.bat uninstall`

   Para obter uma lista dos nomes do script do agente, consulte "Utilizando comandos do agente" na página 175.

   Lembre-se: Para o Monitoring Agent for Microsoft .NET, você deve executar o comando com privilégios de Administrador.

   O agente de monitoramento é desinstalado do sistema gerenciado.

   Se você tiver desinstalado todos os agentes de monitoramento individualmente, continue removendo os arquivos de estrutura. Consulte O que fazer depois.

3. Para desinstalar todos os agentes de monitoramento do sistema gerenciado com um prompt de confirmação, insira o nome do script e desinstale todas as opções:
   - Linux AIX `./smai-agent.sh uninstall_all`
   - Windows `smai-agent.bat uninstall_all`

   Um prompt de confirmação é exibido. Digite 1 para continuar ou 2 para cancelar.

   Todos os agentes de monitoramento são desinstalados do sistema ou da VM.
4. Linux AIX

   No Linux e no UNIX, para forçar a desinstalação de todos os agentes de monitoramento sem um prompt de confirmação, insira o nome do script e a opção forçar desinstalação de todos:

   `./smai-agent.sh uninstall_all force`

O que Fazer Depois

Para o Monitoring Agent for HTTP Server, depois de desinstalar o agente, remova os seguintes arquivos manualmente:

- `/tmp/khu_cps.properties`
- `/tmp/httpserver-disc.error`

Para o Monitoring Agent for Python:

1. Exclua o arquivo de configuração `pyc` do Django para assegurar que o arquivo `pyc` Django restaurado gere seu binário.
2. Reinicie o servidor Apache para remover o middleware carregado nos processos do Apache.

Para o Monitoring Agent for Ruby, para desinstalar o coletor de dados diagnósticos:

1. Navegue para o diretório inicial do seu aplicativo, abra o `Gemfile` e remova a linha a seguir do arquivo: `gem 'stacktracer'`
2. Reinicie o seu aplicativo Ruby on Rails.
3. Desinstale o coletor de dados diagnósticos. Insira: `gem uninstall` *`Gemfile`*
4. Remova o diretório de tempo de execução do coletor de dados. O local padrão desse diretório é *`install_dir`*`/install-images/kkm/dchome`

Para o Monitoring Agent for Microsoft .NET, execute estas etapas:

1. Remova os arquivos `dll` do coletor de dados usando uma das opções a seguir:
   - Reinicialize o seu sistema operacional.
   - Tente excluir o arquivo *`install_dir`*`\qe\bin64\CorProfLog.dll`.

     Uma caixa de diálogo `Arquivo em uso` é exibida. Ela identifica os processos .NET que estão atualmente em execução.
   - Reinicie cada um dos processos .NET.
2. Reinicie seus aplicativos .NET.

WebSphere Applications agent: desconfigurando o coletor de dados

Se você desinstalar o WebSphere Applications agent antes de desconfigurar o coletor de dados, a desinstalação do agente falhará. É possível remover o coletor de dados de uma instância do servidor de aplicativos manualmente ou usando o utilitário interativo ou o processo de desconfiguração silencioso.

Para instâncias monitoradas com o monitoramento de recurso de PMI, a desconfiguração não está disponível. O monitoramento de dados de PMI continua enquanto o servidor está disponível.

Desconfigurando o coletor de dados interativamente

Se você não quiser mais que o coletor de dados para monitore um ou mais instâncias do servidor de aplicativos, é possível desconfigurar o coletor de dados para elas.

Antes de Iniciar

Use o ID do usuário para configurar o coletor de dados para desconfigurar o coletor de dados, que também é o ID do usuário para instalar o servidor de aplicativos. Verifique se esse ID do usuário tem permissões de leitura e gravação para o diretório inicial do coletor de dados e todos os seus subdiretórios. O diretório inicial do coletor de dados é o seguinte, em que *install_dir* é o diretório de instalação do WebSphere Applications agent.

- Windows *install_dir*\dchome\7.3.0.14.08
- Linux AIX *install_dir*/yndchome/7.3.0.14.08

Sobre Esta Tarefa

O utilitário de desconfiguração (`unconfig.sh` ou `unconfig.bat`) é um utilitário de linha de comandos orientado a menu para desconfigurar o coletor de dados.

Procedimento

1. Efetue login no sistema como o ID do usuário que é usado para configurar o coletor de dados.
2. Navegue para o seguinte diretório `bin`:
   - Windows *install_dir*\dchome\7.3.0.14.08\bin
   - Linux AIX *install_dir*/yndchome/7.3.0.14.08/bin
3. Opcional: Configure o local do diretório inicial Java antes de iniciar o utilitário.

   Por exemplo:

   Linux AIX
   ```
   export JAVA_HOME=/opt/IBM/AppServer80/java
   ```

   Windows
   ```
   set JAVA_HOME=C:\Progra~1\IBM\WebSphere\AppServer80\java
   ```
4. Inicie o utilitário de desconfiguração emitindo o seguinte comando:

   Linux AIX
   ```
   ./unconfig.sh
   ```

   Windows
   ```
   unconfig.bat
   ```
5. O utilitário procura por todas as instâncias do servidor monitoradas pelo coletor de dados. Insira o número que corresponde à instância do servidor de aplicativos para desconfigurar para coleta de dados ou insira um asterisco (`*`) para desconfigurar a coleta de dados para todas as instâncias do servidor de aplicativos. Para especificar um subconjunto de servidores, insira os números, separados por vírgulas, que representam os servidores. Por exemplo: `1,2,3`.

   Lembre-se:

   - Para um ambiente independente, as instâncias do servidor de aplicativos devem estar em execução durante a configuração. (Uma instância do WebSphere Application Server Liberty não precisa estar em execução).
   - Para um ambiente de implementação de rede, o Agente do nó e o Deployment Manager devem estar em execução.
6. O utilitário solicita que você especifique se deseja criar um backup de sua configuração atual do WebSphere Application Server. Insira 1 para criar um backup da configuração atual. Caso contrário, insira 2 e ignore a etapa 8.
7. O utilitário solicita que você especifique o diretório no qual armazenar o backup da configuração. Especifique um diretório no qual armazenar o backup da configuração ou aceite o diretório padrão.

   O utilitário exibe o nome do diretório inicial do WebSphere e o perfil do WebSphere para o qual um backup é criado.
8. O utilitário indica se o WebSphere Global Security está ativado para o perfil do aplicativo WebSphere que você especificou. Se a segurança global não estiver ativada, vá para a etapa 10.

9. O utilitário solicita que você especifique se deseja recuperar configurações de segurança de um arquivo de propriedades do cliente. Insira 1 para permitir que o utilitário recupere o nome de usuário e a senha do arquivo de propriedades do cliente adequado e vá para a etapa “10” na página 147. Caso contrário, insira 2 para inserir o nome de usuário e a senha.

   O coletor de dados se comunica com o WebSphere Administrative Services usando o RMI ou o protocolo SOAP. Se a segurança global estiver ativada para um perfil, é necessário especificar o ID do usuário e a senha de um usuário que está autorizado a efetuar login no console administrativo do IBM WebSphere Application Server para o perfil. Alternativamente, é possível criptografar o nome de usuário e a senha e armazená-los nos arquivos de propriedades do cliente antes de configurar o coletor de dados. Você deve usar o arquivo `sas.client.props` para uma conexão RMI ou o arquivo `soap.client.props` para uma conexão SOAP.

   Se você selecionou a opção para fazer backup da configuração atual do WebSphere, o utilitário iniciará o backup da configuração.
10. O utilitário desconfigura o coletor de dados para as instâncias do servidor de aplicativos especificado. Uma mensagem de status é exibida para indicar que o coletor de dados foi desconfigurado com sucesso.
11. Após a conclusão da desconfiguração do coletor de dados, reinicie as instâncias do servidor de aplicativos.

    A configuração do coletor de dados entra em vigor quando as instâncias do servidor de aplicativos são reiniciadas. O monitoramento de recurso PMI para a instância do servidor ainda está disponível.
12. Opcional: Se você deseja usar o monitoramento de recurso para uma instância de servidor depois de desconfigurar o coletor de dados, reinicie o agente de monitoramento, executando os comandos a seguir:
    - Windows

      ```
      cd install_dir\bin
      was-agent.bat stop
      was-agent.bat start
      ```
    - Linux AIX

      ```
      cd install_dir/bin
      ./was-agent.sh stop
      ./was-agent.sh start
      ```

Resultados
O coletor de dados é desconfigurado para as instâncias do servidor de aplicativos especificadas.

Removendo a Configuração do Coletor de Dados no Modo Silencioso
É possível desconfigurar o coletor de dados usando o utilitário de desconfiguração no modo silencioso.

Antes de Iniciar

Use o ID do usuário para configurar o coletor de dados para desconfigurar o coletor de dados, que também é o ID do usuário para instalar o servidor de aplicativos. Verifique se esse ID do usuário tem permissões de leitura e gravação para o diretório inicial do coletor de dados e todos os seus subdiretórios. O diretório inicial do coletor de dados é o seguinte, em que *install_dir* é o diretório de instalação do WebSphere Applications agent.

- Windows *install_dir*\dchome\7.3.0.14.08
- Linux AIX *install_dir*/yndchome/7.3.0.14.08

Sobre Esta Tarefa

Ao desconfigurar o coletor de dados no modo silencioso, primeiro você especifica opções de configuração em um arquivo de propriedades. Um arquivo de propriedades de amostra,

`sample_silent_unconfig.txt`, é empacotado com o utilitário de desconfiguração. O arquivo está disponível no diretório `bin` no diretório inicial do coletor de dados.

Procedimento

1. Efetue login no sistema com o ID do usuário que é usado para configurar o coletor de dados.
2. Especifique as opções de configuração no arquivo `properties.txt`.

   As seguintes propriedades estão disponíveis para desconfigurar o coletor de dados no modo silencioso:

   Configurações de conexão do WebSphere Application Server

   was.wsadmin.connection.host
   Especifica o nome do host ao qual a ferramenta wsadmin está se conectando.

   WebSphere Configurações de Segurança Global do Servidor de Aplicativos

   was.wsadmin.username
   Especifica o ID de um usuário que está autorizado a efetuar logon no console administrativo do IBM WebSphere Application Server. Esse usuário deve ter a função de agente no servidor de aplicativos.

   was.wsadmin.password
   Especifica a senha que corresponde ao usuário especificado na propriedade `was.wsadmin.username`.

   Configurações do WebSphere Application Server

   was.appserver.profile.name
   Especifica o nome do perfil do servidor de aplicativos que você deseja desconfigurar.

   was.appserver.home
   Especifica o diretório inicial do WebSphere Application Server.

   was.appserver.cell.name
   Especifica o nome da célula do WebSphere Application Server.

   was.appserver.node.name
   Especifica o nome do nó do WebSphere Application Server.

   Faça backup da configuração do WebSphere Application Server

   was.backup.configuration
   Especifica se deve-se fazer backup da atual configuração do coletor de dados do WebSphere Application Server antes de desconfigurar o coletor de dados. Os valores válidos são `True` e `False`.

   was.backup.configuration.dir
   Especifica o local do diretório de backup.

   WebSphere Configurações da instância de tempo de execução do servidor

   was.appserver.server.name
   Especifica uma instância do servidor de aplicativos no perfil do servidor de aplicativos para o qual deseja desconfigurar o coletor de dados.

   Dica: O arquivo silencioso de resposta pode ter diversas instâncias desta propriedade.
3. Navegue até o seguinte diretório:
   - Windows *install_dir*\dchome\7.3.0.14.08\bin
   - Linux AIX *install_dir*/yndchome/7.3.0.14.08/bin
4. Execute o seguinte comando:
   - Windows

   ```
   unconfig.bat -silent path_to_silent_file
   ```

- Linux AIX

```
unconfig.sh -silent path_to_silent_file
```

5. Após a conclusão da desconfiguração do coletor de dados, reinicie as instâncias do servidor de aplicativos.

   A configuração do coletor de dados entra em vigor quando as instâncias do servidor de aplicativos são reiniciadas. O monitoramento de recurso PMI para a instância do servidor ainda está disponível.
6. Opcional: Se você deseja usar o monitoramento de recurso para uma instância de servidor depois de desconfigurar o coletor de dados, reinicie o agente de monitoramento, executando os comandos a seguir:

   - Windows

   ```
   cd install_dir\bin
   was-agent.bat stop
   was-agent.bat start
   ```

   - Linux AIX

   ```
   cd install_dir/bin
   ./was-agent.sh stop
   ./was-agent.sh start
   ```

Removendo Manualmente a Configuração do Coletor de Dados de uma Instância do Servidor de Aplicativos

Para remover manualmente a configuração do coletor de dados de uma instância do servidor de aplicativos, você deve ser capaz de se conectar ao servidor de aplicativos usando a ferramenta wsadmin. Isso será possível somente se você estiver usando o WebSphere Application Server Network Deployment e o Deployment Manager estiver em execução. Se o servidor de aplicativos WebSphere não puder ser iniciado, você deverá restaurar o servidor de aplicativos WebSphere a partir do backup feito quando executar o utilitário de configuração.

Sobre Esta Tarefa

É possível remover manualmente a configuração do coletor de dados a partir de uma instância do servidor de aplicativos, se qualquer uma das seguintes condições se aplicar:

- Em um ambiente não de implementação de rede, você incluiu manualmente a configuração do coletor de dados na instância do servidor de aplicativos e deseja desconfigurar a coleta de dados. A instância do servidor de aplicativos deve estar em execução.
- Em um ambiente Network Deployment, você incluiu manualmente a configuração do coletor de dados na instância do servidor de aplicativos e deseja desconfigurar a coleta de dados. O Agente do Nó e o Deployment Manager no servidor de aplicativos devem estar em execução.
- Em um ambiente de Implementação de Rede, você configurou a instância do servidor de aplicativos para coleta de dados manualmente e o servidor de aplicativos falha em iniciar. O Agente do Nó e o Deployment Manager no servidor de aplicativos devem estar em execução.

Se você configurou uma instância de servidor de aplicativos independente para coleta de dados manualmente ou com o utilitário de configuração ou migração e o servidor de aplicativos falhou ao ser iniciado, você deverá restaurar a configuração do WebSphere Application Server com sua configuração de backup. Para obter mais informações, consulte “Restaurando a Configuração do Servidor de Aplicativos a Partir de um Backup” na página 879.

Lembre-se:

- Deve-se fazer mudanças manuais na configuração do WebSphere Application Server para coletores de dados como o usuário administrativo do WebSphere.

- As mudanças manuais no WebSphere Application Server para coleta de dados devem ser feitas somente por um administrador experiente do WebSphere. Qualquer erro na alteração de configuração manual pode resultar no servidor de aplicativos não iniciado.
- Se você configurar manualmente o coletor de dados para monitorar instâncias do servidor de aplicativos, não será possível usar o utilitário de desconfiguração para desconfigurar o coletor de dados.

Procedimento

Para remover manualmente a configuração do coletor de dados, conclua o seguinte procedimento:

1. Efetue login no WebSphere Administration Server Console.
2. Clique em **Servidores**.
3. Expanda **Servidor Tipo** e selecione **servidores de aplicativos WebSphere**.
4. Clique no nome do servidor.
5. Na guia Configuração, acesse **Infraestrutura do servidor** > **Gerenciamento de Java e processos** > **Definição de processo** > **Java Virtual Machine** > **Propriedades adicionais: Propriedades customizadas**.
6. Remova todas as seguintes Propriedades Customizadas JVM, se estiverem presentes:
   - `am.home`
   - `ITCAM.DC.ENABLED`
   - `TEMAGCCollector.gclog.path`
   - `com.ibm.tivoli.itcam.toolkit.ai.runtimebuilder.enable.rebuild`
   - `com.ibm.tivoli.jiti.injector.ProbeInjectorManagerChain.primaryInjectorFile`
7. Identifique os argumentos da JVM que foram incluídos no coletor de dados.
   a) Na área de janela de navegação, clique em **Ambiente** > **Variáveis do WebSphere**.
   b) Se você configurou manualmente o servidor de aplicativos para coleta de dados, localize os argumentos da JVM que foram incluídos manualmente.
      Se você configurou o servidor de aplicativos para coleta de dados com os utilitários de configuração, compare os valores dos argumentos **AM_OLD_ARGS** e **AM_CONFIG_JVM_ARGS** para determinar quais argumentos foram incluídos pelo utilitário de configuração.
8. Clique em **Servidor** > **Servidor de aplicativos** e selecione o nome do servidor apropriado.
9. Na guia Configuração, acesse **Infraestrutura do servidor** > **Gerenciamento de Java e processos** > **Definição de processo** > **Java Virtual Machine**.
10. No campo **Argumentos genéricos de JVM**, remova os argumentos da JVM identificados na Etapa 7 para o coletor de dados.
11. Clique em **Aplicar** ou **OK**.
12. Na caixa de diálogo **Mensagens**, clique em **Salvar**.
13. Na caixa de diálogo **Salvar na Configuração Principal**, conclua uma das seguintes etapas:
    - Se você estiver em um ambiente do Network Deployment, certifique-se de que a caixa de seleção **Sincronizar com nós** esteja selecionada e, em seguida, clique em **Salvar**.
    - Se você não estiver em um ambiente de Implementação de Rede, clique em **Salvar**.
14. Remova as entradas de ambiente que foram incluídas para o coletor de dados.
    a) Na guia Configuração, acesse **Infraestrutura do servidor** > **Gerenciamento de Java e processos** > **Definição de processo** > **Entradas de ambiente**.
    b) Dependendo do sistema operacional, exclua a seguinte entrada de ambiente:
       - UNIX **LIBPATH**
       - Linux **LD_LIBRARY_PATH**
       - Windows **PATH**
    c) Remova a entrada do ambiente **NLSPATH**.

15. Clique em **Aplicar** ou **OK**.
16. Na caixa de diálogo **Mensagens**, clique em **Salvar**.
17. Na caixa de diálogo **Salvar na Configuração Principal**, conclua uma das seguintes etapas:
    - Se você estiver em um ambiente do Network Deployment, certifique-se de que a caixa de seleção **Sincronizar mudanças com nós** esteja selecionada e, em seguida, clique em **Salvar**.
    - Se você não estiver em um ambiente de Implementação de Rede, clique em **Salvar**.
18. Na área de janela de navegação, clique em **Ambiente** > **Variáveis do WebSphere**.
19. Exclua as seguintes variáveis:
    - **AM_CONFIG_JVM_ARGS**
    - **AM_OLD_JVM_ARGS**
    - **ITCAMDCHOME**
    - **ITCAMDCVERSION**
20. Na caixa de diálogo **Mensagens**, clique em **Salvar**.
21. Na caixa de diálogo **Salvar na Configuração Principal**, conclua uma das seguintes etapas:
    - Se você estiver em um ambiente do Network Deployment, certifique-se de que a caixa de seleção **Sincronizar mudanças com nós** esteja selecionada e, em seguida, clique em **Salvar**.
    - Se você não estiver em um ambiente de Implementação de Rede, clique em **Salvar**.
22. Se você configurou a instância do servidor para coleta de dados com a ferramenta de configuração do coletor de dados, em vez de fazê-lo manualmente, conclua as seguintes etapas:
    a) Navegue para o diretório *dc_home*/runtime.
    b) Renomeie o arquivo $profile.$cell.$node.$server.input.properties para $profile.$cell.$node.$server.input.properties.bak.
23. Se você estiver removendo manualmente a configuração do coletor de dados de todas as instâncias do servidor de aplicativos em um perfil, execute as seguintes etapas:
    a) Navegue para o diretório $appserverhome/bin.
    b) Execute o comando **osgiCfgInit.sh/bat -all** em sistemas Windows ou o comando **osgiCfgInit.sh -all** em sistemas UNIX e Linux.
24. Reinicie a instância do servidor de aplicativos que foi monitorada pelo coletor de dados.

Desconfigurar manualmente o coletor de dados
Depois de configurar manualmente o coletor de dados para o WebSphere Applications agent, para remover a coleta de dados no servidor de aplicativos configurado, é preciso desconfigurar manualmente o coletor de dados.

Sobre Esta Tarefa

O procedimento a seguir se aplica somente após a configuração manual do coletor de dados seguindo as instruções em "Configurar manualmente o coletor de dados se os utilitários de configuração falharem" na página 855. Se você usou os utilitários de configuração para configurar o coletor de dados, também deverá usar o utilitário de desconfiguração para desconfigurar o coletor de dados. Para obter instruções, consulte "Desconfigurando o coletor de dados interativamente" na página 145 ou "Removendo a Configuração do Coletor de Dados no Modo Silencioso" na página 147.

Procedimento

- Para desconfigurar manualmente o coletor de dados para WebSphere Application Server, consulte "Desconfigurando manualmente o coletor de dados para o WebSphere Application Server tradicional" na página 152.
- Para desconfigurar manualmente o coletor de dados para o servidor Liberty, consulte "Desconfigurando manualmente o coletor de dados para o WebSphere Application Server Liberty" na página 153.

Desconfigurando manualmente o coletor de dados para o WebSphere Application Server tradicional

Procedimento

1. Efetue login no Console Administrativo do WebSphere como o administrador.
2. Na área de janela de navegação, clique em **Servidores**, expanda **Tipo de servidor** e selecione **Servidores de aplicativos WebSphere**.
3. Clique no nome do servidor de aplicativos.
4. Na seção **Infraestrutura do servidor** na guia Configuração, expanda **Java Virtual Machine** e clique em **Definição de processo**.
5. Na seção **Propriedades Adicionais**, clique em **Java Virtual Machine**.
6. No campo **Argumentos de JVM genéricos**, remova as seguintes entradas do conteúdo.

```
-agentlib:am_ibm_16=${WAS_SERVER_NAME} -Xbootclasspath/p:${ITCAMDCHOME}/
toolkit/lib/bcm-bootstrap.jar -Djava.security.policy=${ITCAMDCHOME}/itcamdc/
etc/datacollector.policy -verbosegc
```

7. Clique em **Aplicar** e clique em **Salvar**. Na caixa de diálogo Salvar na Configuração Principal, conclua as seguintes etapas:
   - Se você estiver em um ambiente de implementação de rede, assegure-se de que **Sincronizar Mudanças com Nós** esteja selecionado e, em seguida, clique em **Salvar**.
   - Se você não estiver em um ambiente de Implementação de Rede, clique em **Salvar**.
8. Na área de janela de navegação, clique em **Servidores**, expanda **Tipos de servidor**, clique em **Servidores de aplicativos WebSphere** e, em seguida, clique no nome do servidor.
9. Na guia Configuração, acesse **Infraestrutura do servidor** > **Gerenciamento de Java e processos** > **Definição de processo** > **Entradas de ambiente**.
10. Dependendo do sistema operacional, da plataforma de hardware e da JVM do servidor de aplicativos, remova a seguinte entrada de ambiente.
    - UNIX LIBPATH
    - Linux LD_LIBRARY_PATH
    - Windows PATH
11. Na área de janela de navegação, clique em **Ambiente** > **Variáveis do WebSphere**.
12. Remova a variável *ITCAMDCHOME*, se ela existir.
13. Clique em **Aplicar** e clique em **Salvar**. Na caixa de diálogo Salvar na Configuração Principal, conclua as seguintes etapas:
    - Se você estiver em um ambiente de implementação de rede, assegure-se de que **Sincronizar Mudanças com Nós** esteja selecionado e, em seguida, clique em **Salvar**.
    - Se você não estiver em um ambiente de Implementação de Rede, clique em **Salvar**.
14. Reinicie a instância do servidor de aplicativos.
15. Acesse o diretório `runtime` no diretório de instalação do agente e remova o arquivo *`profile_name.cell_name.node_name.server_name`*`.manual.input.properties`.
    - Linux AIX *`install_dir`*`/yndchome/7.3.0.14.08/runtime/`*`profile_name.cell_name.node_name.server_name`*`.manual.input.properties`
    - Windows *`install_dir`*`\dchome\7.3.0.14.08\runtime\`*`profile_name.cell_name.node_name.server_name`*`.manual.input.properties`

Desconfigurando manualmente o coletor de dados para o WebSphere Application Server Liberty

Procedimento

1. Navegue para o diretório do servidor Liberty e abra o arquivo `jvm.options` no diretório *`server_name`* no diretório de instalação do servidor Liberty. Por exemplo, `/opt/ibm/wlp/usr/servers/defaultServer`.
2. Remova os seguintes parâmetros do arquivo `jvm.options`.

```
-agentlib:am_ibm_16=server_name
–Xbootclasspath/p:dc_home/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=dc_home/itcamdc/etc/datacollector.policy
-verbosegc
```

   em que, *server_name* é o nome do servidor Liberty; *dc_home* é o diretório inicial do coletor de dados.
3. Abra o arquivo `server.xml` e remova as seguintes linhas:

```
<feature>webProfile-7.0</feature>
<feature>monitor-1.0</feature>
<feature>usr:itcam-730.140</feature>
```

4. Abra o arquivo `server.env` e remova o seguinte valor de entrada da entrada de ambiente pelo sistema operacional:

Tabela 8. Entrada de ambiente

Plataforma	Nome da entrada de ambiente	Valor da entrada de ambiente
AIX R6.1 (JVM de 64 bits)	LIBPATH	`/lib:`*`dc_home`*`/toolkit/lib/aix536`
AIX R7.1 (64 bit JVM)	LIBPATH	`/lib:`*`dc_home`*`/toolkit/lib/aix536`
Solaris 10 (JVM de 64 bits)	LIBPATH	`/lib:`*`dc_home`*`/toolkit/lib/sol296`
Solaris 11 (JVM de 64 bits)	LIBPATH	`/lib:`*`dc_home`*`/toolkit/lib/sol296`
Linux x86_64 R2.6 (JVM de 64 bits)	LD_LIBRARY_PATH	`/lib:`*`dc_home`*`/toolkit/lib/lx8266`
Linux Intel R2.6 (JVM de 32 bits)	LD_LIBRARY_PATH	`/lib:`*`dc_home`*`/toolkit/lib/li6263`
Windows (JVM de 32 bits)	PATH	`/lib;`*`dc_home`*`/toolkit/lib/win32`
Windows (JVM de 64 bits)	PATH	`/lib;`*`dc_home`*`/toolkit/lib/win64`

5. Reinicie o servidor Liberty.
6. Acesse o diretório `runtime` no diretório de instalação do WebSphere Applications agent e remova o arquivo *`cell_name.node_name.server_name`*`.manual.input.properties`.
   - Linux AIX *`install_dir`*`/yndchome/7.3.0.14.08/runtime/`*`cell_name.node_name.server_name`*`.manual.input.properties`
   - Windows *`install_dir`*`\dchome\7.3.0.14.08\runtime\`*`cell_name.node_name.server_name`*`.manual.input.properties`

Agente Node.js: Removendo o plug-in de monitoramento

Antes de desinstalar o Agente Node.js, deve-se remover o plug-in de monitoramento de seu aplicativo Node.js.

Procedimento

1. Remova os plug-ins do coletor de dados do começo do arquivo de aplicativos Node.js.
   - Se você fizer upgrade do Agente Node.js do da V01.00.12.00 para a V01.00.13.00, conclua o seguinte procedimento:
     - Caso você tenha ativado a coleta de dados, remova a linha a seguir do começo do arquivo de aplicativos Node.js:

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_index.js');
       ```

       em que *KNJ_NPM_LIB_LOCATION* é o diretório para a pasta `lib` de seu diretório de instalação global do pacote do npm. O diretório padrão é `/usr/local/lib`.
     - Se você ativou a coleta de dados de recurso e a coleta de dados diagnósticos de detalhamento, remova a linha a seguir do início do arquivo de aplicativo Node.js:

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_deepdive.js');
       ```

     - Se você ativou a coleta de dados de recurso, a coleta de dados diagnósticos de detalhamento e a coleta de rastreios de método, remova a linha a seguir do início do arquivo de aplicativo Node.js:

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_methodtrace.js');
       ```

   - Se você fizer upgrade do Agente Node.js do da V01.00.10.00 para a V01.00.13.00, conclua o seguinte procedimento:
     - Caso você tenha ativado a coleta de dados de recurso, remova a linha a seguir do começo do arquivo de aplicativos Node.js.

       ```
       require('install_dir/lx8266/nj/bin/plugin/knj_index.js');
       ```

       , em que *install_dir* é o diretório de instalação do Agente Node.js.
     - Se você ativou a coleta de dados de recurso e a coleta de dados diagnósticos de detalhamento, remova a linha a seguir do início do arquivo de aplicativo Node.js.

       ```
       require('install_dir/lx8266/nj/bin/plugin/knj_deepdive.js');
       ```

     - Se você ativou a coleta de dados de recurso, a coleta de dados diagnósticos de detalhamento e a coleta de rastreios de método, remova a linha a seguir do início do arquivo de aplicativo Node.js.

       ```
       require('install_dir/lx8266/nj/bin/plugin/knj_methodtrace.js');
       ```

2. Reinicie o aplicativo Node.js para desativar os plug-ins do coletor de dados.
   - Se a versão de seu Agente Node.js atual for V01.00.10.00, até o momento os plug-ins do coletor de dados foram removidos com sucesso.
   - Se a versão de seu Agente Node.js atual for V01.00.12.00, continue com a próxima etapa.
3. Execute o comando `./uninstall.sh` a partir do diretório *install_dir*`/lx8266/nj/bin` para remover suas configurações de agente anteriores.

O que Fazer Depois

Para obter mais informações sobre como desinstalar o Agente Node.js, consulte "Desinstalando os agentes" na página 143.

Microsoft .NET agent: Removendo o coletor de dados .NET

Antes de desinstalar o Microsoft .NET agent, é necessário remover o coletor de dados .NET de seus aplicativos .NET.

Procedimento

1. Cancele o registro do coletor de dados.

   Como um administrador, digite:

   ```
   cd install_dir\qe\bin configdc unregisterdc
   ```

   Em que *install_dir* é o diretório de instalação do Microsoft .NET agent.
2. Pare todos os aplicativos .NET para desativar o coletor de dados.

   Insira `net stop was /y`
3. Para assegurar a limpeza completa do .NET Data Collector após a desinstalação, siga estas etapas:
   a) No prompt de comandos, acesse o diretório `<APM_HOME>\qe\bin`.
   b) Execute o arquivo `ProcListCaller.bat` .
   c) Verifique o arquivo de log `CorProfAttach.Log` no diretório `<APM_HOME>\qe\logs`. O arquivo de log lista os processos aos quais o componente do gerenciador de perfis .NET DC está anexado.
   d) Antes de desinstalar o agente, pare os processos a partir do arquivo `CorProfAttach.Log`.
   e) Se nenhum processo estiver listado, continue com a desinstalação do agente.

O que Fazer Depois

Desinstale o Microsoft .NET agent. Consulte “Desinstalando os agentes” na página 143.

Capítulo 7. Configurando seu Ambiente

Se o seu agente de monitoramento requerer configuração ou você desejar revisar as configurações padrão para um agente, siga as etapas fornecidas para seu agente.

Tópicos comuns

Alguns tópicos são comuns quando você configura agentes e coletores de dados.

Conectividade de rede

Para assegurar que as comunicações do servidor de agente sejam estabelecidas, teste a conectividade de seu sistema com o Servidor Cloud APM.

Para validar comunicações, teste sua conectividade com o datacenter do Cloud APM. Para assegurar que suas regras de firewall permitam retornar o tráfego de três endereços IP específicos e da porta 443, localize os três endereços IP do datacenter necessários para verificar a conexão. Para obter mais informações, consulte Endereços IP do datacenter (somente SaaS) no Application Performance Management Developer Center. Verifique se seus agentes podem se conectar a esses três endereços IP usando o comando **openssl**. Para obter mais informações sobre como usar o comando **openssl**, consulte Configurando agentes para comunicação por meio de um proxy de encaminhamento. Se seu agente não puder se conectar, entre em contato com a equipe de TI local. Eles podem ajustar as regras de firewall, ativar a porta 443 e ativar o tráfego TLS 1.2 de seus servidores, ou configurar um servidor proxy para se conectar ao Servidor Cloud APM.

Se suas regras de firewall não permitirem conexões HTTPS de saída transparentes com hosts externos, é possível configurar seus agentes para enviar tráfego para um proxy de encaminhamento. Para obter mais informações, consulte “Configurando agentes para se comunicar através de um proxy de encaminhamento” na página 157.

Conectividade do navegador

Para verificar a conectividade do navegador com o Console do Cloud APM, localize a URL **Ativar**, que foi fornecida pela IBM quando sua assinatura foi fornecida. Você também pode conectar-se à sua conta e iniciar o console. Conecte-se à página **Produtos e Serviços** (http://ibm.biz/my-prodsvcs) com seus detalhes de assinatura do IBM Marketplace. Clique em **Ativar** para iniciar o console e visualizar a URL, por exemplo: `8b68ba1b9.agents.na.apm.ibmserviceengage.com`. Verifique se é possível usar a URL para efetuar login no console.

Comunicação Segura

A comunicação segura entre os agentes e o Servidor Cloud APM requer o TLS 1.2.

Comunicação entre os agentes e o Servidor Cloud APM no IBM Cloud usa HTTPS com TLS 1.2 e conjuntos de cifras FIPS Suite-B. As seguintes cifras são usadas:

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
```

As comunicações entre o navegador e o Servidor Cloud APM também requerem o TLS 1.2. Em alguns navegadores, o TLS 1.2 não é ativado por padrão e deve ser ativado manualmente.

Configurando agentes para se comunicar através de um proxy de encaminhamento

Se suas regras de firewall não permitirem conexões HTTPS de saída transparente para hosts externos, é possível configurar agentes de monitoramento IBM para enviar tráfego para um proxy de encaminhamento. Edite a variável de ambiente KDH_FORWARDPROXY para configurar agentes para comunicação por meio do proxy de encaminhamento.

Antes de Iniciar

Para determinar o endereço IP do datacenter do Cloud APM ao qual seus agentes se conectam, consulte Endereços IP do Data Center (APM Developer Center). Depois, ajuste suas regras de firewall para permitir que solicitações sejam enviadas a esses endereços IP de seu proxy de encaminhamento.

É possível usar o comando **openssl** para verificar se o sistema de computador no qual seus agentes estão instalados tem conectividade aos servidores de datacenter do Cloud APM. Também é possível usar o comando **openssl** para verificar se sua rede suporta os conjuntos de criptografia que são usados pelo Cloud APM. Se os resultados do comando **openssl** indicam que o sistema de computador não pode se conectar, pode ser necessário configurar um proxy de encaminhamento. Se os resultados do comando indicam que o certificado do Servidor Cloud APM não pôde ser obtido, então, trabalhe com sua equipe de rede para determinar porque os conjuntos de cifras não são suportados. Para obter a lista de conjuntos de cifras que são usados pelo Cloud APM, consulte "Comunicação Segura" na página 157.

Execute o comando **openssl**, conforme mostrado no exemplo a seguir:

```
echo quit | openssl s_client
-state -connect <domain-name>:443
-tls1_2 -cipher
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384
```

em que *domain-name* é o nome de domínio para sua assinatura do Cloud APM (por exemplo: `8b68ba1b9.agents.na.apm.ibmserviceengage.com`).

Para determinar o nome de domínio para sua assinatura, conclua as seguintes etapas:

1. Abra o arquivo de configuração do ambiente de agente em um editor de texto:

   Linux AIX `/opt/ibm/apm/agent/config/global.environment`

   Windows `install_dir\TMAITM6_x64\K`*pc*`ENV` para sistemas Windows de 64 bits e `install_dir\TMAITM6\K`*pc*`ENV` para sistemas Windows de 32 bits, em que *pc* é o código de produto do agente.

   Para obter uma lista de códigos de produtos, consulte o "Utilizando comandos do agente" na página 175.
2. Localize a variável *IRA_ASF_SERVER_URL*. O valor está no formulário: `https://domain-name/ccm/asf/request`. Use a parte de nome de domínio do valor com o comando **openssl**.

Se a conexão for bem-sucedida, serão exibidas mensagens semelhantes ao exemplo a seguir:

```
CONNECTED(00000003)
SSL_connect:before/connect initialization
SSL_connect:SSLv3 write client hello A
SSL_connect:SSLv3 read server hello A
depth=2 C = US, O = IBM Service Engage,
CN = ca_ec_384.ibmserviceengage.com
verify error:num=19:self signed certificate in certificate chain
verify return:0
SSL_connect:SSLv3 read server certificate A
SSL_connect:SSLv3 read server key exchange A
SSL_connect:SSLv3 read server certificate request A
SSL_connect:SSLv3 read server done A
SSL_connect:SSLv3 write client certificate A
SSL_connect:SSLv3 write client key exchange A
SSL_connect:SSLv3 write change cipher spec A
SSL_connect:SSLv3 write finished A
SSL_connect:SSLv3 flush data
SSL_connect:SSLv3 read finished A
---
Cadeia de Certificados
0 s:/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/OU=Application Performance
```

```
Management/CN =ca_ec_384.apm.ibmserviceengage.com
1 s:/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
2 s:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
---
Certificado do Servidor
-----BEGIN CERTIFICATE-----
MIICkjCCAhegAwIBAgIIXlr284nLPaMwDAYIKoZIzj0EAwMFADCBhDELMAkGA1UE
BgwCVVMxGzAZBgNVBAoMEklCTSBTZXJ2aWNlIEVuZ2FnZTErMCkGA1UECwwiQXBw
bGljYXRpb24gUGVyZm9ybWFuY2UgTWFuYWdlbWVudDErMCkGA1UEAwwiY2FfZWNf
Mzg0LmFwbS5pYm1zZXJ2aWNlZW5nYWdlLmNvbTAeFw0xMzEyMDIxNjM2MDlaFw0y
MzEyMDExNjM2MDlaMIGGMQswCQYDVQQGDAJVUzEbMBkGA1UECgwSSUJNIFNlcnZp
Y2UgRW5nYWdlMSswKQYDVQQLDCJBcHBsaWNhdGlvbiBQZXJmb3JtYW5jZSBNYW5h
Z2VtZW50MS0wKwYDVQQDDCQqLmFnZW50cy5uYS5hcG0uaWJtc2VydmljZWVuZ2Fn
ZS5jb20wdjAQBgcqhkjOPQIBBgUrgQQAIgNiAAQmrGoCkAMoNAC3F6MIo1zR8fcO
mczYXtUux2bhlOibn3jQdxamhDR91nr2RBerGjMIITKNXd2MaOr3b6m8euk1BAL3
KsbN9lqvw94kXg0BTO1IHAcdsZQB+AuEVVhmDVGjUDBOMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAU/zpE5TOnQ8LSuvbSWRfpbiGea08wHQYDVR0OBBYEFHL0At4O
GUdcOHVGg4Tfo4hl7LLGMAwGCCqGSM49BAMDBQADZwAwZAIwDWPHo5I04ZFVrkfk
St6gwH2UNF37jBscRN1lOE4SIwezZAqVs42BNMkWRjJBgiHzAjBm4m3zOjsXzNL8
+u8ALjQQCpBDT6dUHujzY5CRxG0xEHi5IXsXf4QwbctnjjvTeYA=
-----FIM DO CERTIFICADO-----
subject=/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
issuer=/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
---
Nomes da autoridade de certificação do certificado de cliente aceitável
/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert
Global Root CA/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
Chave temporária do servidor: ECDH, prime256v1, 256 bits
---
O handshake SSL leu 2659 bytes e gravou 261 bytes
---
Novo, TLSv1/SSLv3, a cifra é ECDHE-ECDSA-AES128-GCM-SHA256
A chave pública do servidor é de 384 bits
Secure Renegotiation IS suportado
Compactação: NENHUMA
Expansão: NENHUMA
SSL-Session:
Protocolo: TLSv1.2
Cifra: ECDHE-ECDSA-AES128-GCM-SHA256
Session-ID:
A18C31D0B45A1166357C917E1CFCD86A9FBEDB4A0EB768EF5390AC28C95CB7EF
Session-ID-ctx:
Chave mestra:
252B8FE2731E51AC0B79A27C7BED33CA8B15AF4CFD015C98DBACA46EA01DC40B
9E6B56E62E0F332FF6B56266B5ADD7B0
Key-Arg: Nenhum
Krb5 Principal: nenhuma
Identidade do PSK: nenhum
Sugestão de identidade do PSK: nenhum
```

```
Horário de início: 1510772474
Tempo limite: 7200 (seg)
Verify return code: 19 (self signed certificate in certificate chain)
---
FEITO
SSL3 alert write:warning:close notify
```

Se o sistema de computador não tiver conectividade com o Servidor Cloud APM, mensagens semelhantes ao exemplo a seguir serão exibidas:

```
getaddrinfo: Name or service not known
connect:errno=2
```

Se o sistema de computador não puder obter o certificado do servidor, porque os conjuntos de cifras estão sendo bloqueados em algum lugar da rede, serão exibidas mensagens como a seguinte:

```
SSL_connect:failed
---
nenhum certificado do peer disponível
---
No client certificate CA names sent
```

Sobre Esta Tarefa

Ao utilizar um proxy de encaminhamento, o agente primeiro abre uma conexão TCP com o proxy. O agente envia uma solicitação HTTP CONNECT e a URL do terminal de destino (Servidor Cloud APM) para o proxy de encaminhamento. Em seguida, o proxy de encaminhamento estabelece uma conexão TCP com o terminal de destino e configura uma sessão de tunelamento de HTTPS entre o agente e o Servidor Cloud APM.

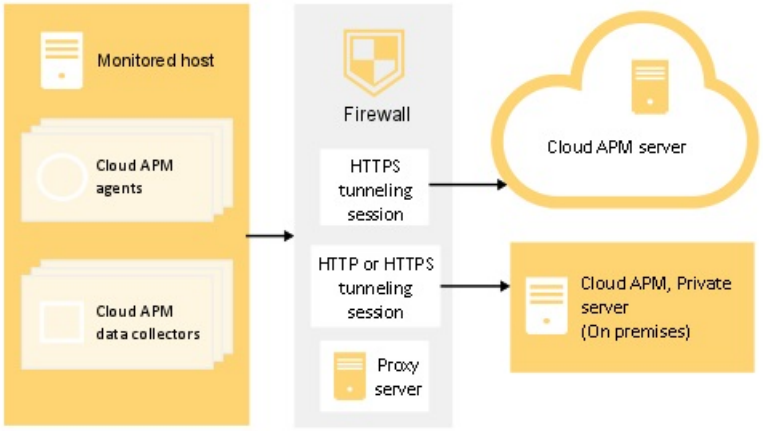


Figura 1. Diagrama de conexão para usar um proxy de encaminhamento

O agente de monitoramento não suporta a autenticação de proxies, o que significa que o agente não suporta que seja feito login em um proxy de encaminhamento usando o ID de usuário e a senha de um usuário do proxy configurado.

Procedimento

1. Abra o arquivo de configuração do ambiente de agente em um editor de texto:

   Linux AIX O arquivo *install_dir*`/config/global.environment`, em que *install_dir* é o diretório inicial de instalação dos agentes. O arquivo `global.environment` configura todos os agentes no diretório de instalação.

   As configurações customizadas no arquivo `.global.environment` são perdidas depois do upgrade do agente. Para preservar suas configurações, faça mudanças na customização nos arquivos `global.environment`. As configurações neste arquivo não são sobrescritas pelo upgrade de agente.

Windows O arquivo *install_dir*\TMAITM6_x64\K*pc*ENV para agentes de 64 bits e *install_dir*\TMAITM6\K*pc*ENV para agentes 32 bits, em que *pc* é o código do produto do agente. Configure o arquivo K*pc*ENV para cada agente.

Para obter uma lista de códigos de produtos, consulte o "Utilizando comandos do agente" na página 175.

2. Edite a variável de ambiente KDH_FORWARDPROXY para especificar o endereço e porta do proxy:

```
KDH_FORWARDPROXY=http://proxy-address:proxy-port-number
```

Por exemplo:

```
KDH_FORWARDPROXY=http://HostA:8085
```

3. Reinicie o agente para implementar suas mudanças. Consulte "Utilizando comandos do agente" na página 175.

Configurando coletores de dados para se comunicarem através de um proxy de encaminhamento

Se suas regras de firewall não permitem conexões transparentes de HTTPS de saída com hosts externos, é possível configurar os coletores de dados para enviar o tráfego para um proxy de encaminhamento. Edite a variável de ambiente APM_GW_PROXY_CONNECTION para configurar coletores de dados para se comunicarem através do proxy de encaminhamento.

Antes de Iniciar

Para determinar o endereço IP do data center do Cloud APM ao qual seus coletores de dados se conectam, consulte Endereços IP do Data Center (APM Developer Center). Depois, ajuste suas regras de firewall para permitir que solicitações sejam enviadas a esses endereços IP de seu proxy de encaminhamento.

É possível usar o comando **openssl** para verificar se o sistema de computador em que seus coletores de dados estão instalados tem conectividade com os servidores do data center do Cloud APM. Também é possível verificar se sua rede suporta conjuntos de criptografia que são usados pelo Cloud APM. Se os resultados do comando **openssl** indicam que o sistema de computador não pode se conectar, pode ser necessário configurar um proxy de encaminhamento. Se os resultados do comando indicam que o certificado do Servidor Cloud APM não pôde ser obtido, então, trabalhe com sua equipe de rede para determinar porque os conjuntos de cifras não são suportados. Para obter a lista de conjuntos de cifras que são usados pelo Cloud APM, consulte "Comunicação Segura" na página 157.

Execute **openssl**, conforme mostrado no exemplo a seguir:

```
echo quit | openssl s_client
-state -connect <domain-name>:443
-tls1_2 -cipher
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384
```

em que *domain-name* é o nome de domínio para a assinatura do Cloud APM.

Para determinar o nome de domínio para sua assinatura, consulte "Configurando agentes para se comunicar através de um proxy de encaminhamento" na página 157.

Se a conexão for bem-sucedida, serão exibidas mensagens semelhantes ao exemplo a seguir:

```
CONNECTED(00000003)
SSL_connect:before/connect initialization
SSL_connect:SSLv3 write client hello A
SSL_connect:SSLv3 read server hello A
depth=2 C = US, O = IBM Service Engage,
CN = ca_ec_384.ibmserviceengage.com
verify error:num=19:self signed certificate in certificate chain
verify return:0
SSL_connect:SSLv3 read server certificate A
SSL_connect:SSLv3 read server key exchange A
SSL_connect:SSLv3 read server certificate request A
```

```
SSL_connect:SSLv3 read server done A
SSL_connect:SSLv3 write client certificate A
SSL_connect:SSLv3 write client key exchange A
SSL_connect:SSLv3 write change cipher spec A
SSL_connect:SSLv3 write finished A
SSL_connect:SSLv3 flush data
SSL_connect:SSLv3 read finished A
---
Cadeia de Certificados
0 s:/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN =ca_ec_384.apm.ibmserviceengage.com
1 s:/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
2 s:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
i:/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
---
Certificado do Servidor
-----BEGIN CERTIFICATE-----
MIICkjCCAhegAwIBAgIIXlr284nLPaMwDAYIKoZIzj0EAwMFADCBhDELMAkGA1UE
BgwCVVMxGzAZBgNVBAoMEklCTSBTZXJ2aWNlIEVuZ2FnZTErMCkGA1UECwwiQXBw
bGljYXRpb24gUGVyZm9ybWFuY2UgTWFuYWdlbWVudDErMCkGA1UEAwwiY2FfZWNf
Mzg0LmFwbS5pYm1zZXJ2aWNlZW5nYWdlLmNvbTAeFw0xMzEyMDIxNjM2MDlaFw0y
MzEyMDExNjM2MDlaMIGGMQswCQYDVQQGDAJVUzEbMBkGA1UECgwSSUJNIFNlcnZp
Y2UgRW5nYWdlMSswKQYDVQQLDCJBcHBsaWNhdGlvbiBQZXJmb3JtYW5jZSBNYW5h
Z2VtZW50MS0wKwYDVQQDDCQqLmFnZW50cy5uYS5hcG0uaWJtc2VydmljZWVuZ2Fn
ZS5jb20wdjAQBgcqhkjOPQIBBgUrgQQAIgNiAAQmrGoCkAMoNAC3F6MIo1zR8fcO
mczYXtUux2bhlOibn3jQdxamhDR91nr2RBerGjMIITKNXd2MaOr3b6m8euk1BAL3
KsbN9lqvw94kXg0BTO1IHAcdsZQB+AuEVVhmDVGjUDBOMAwGA1UdEwEB/wQCMAAw
HwYDVR0jBBgwFoAU/zpE5TOnQ8LSuvbSWRfpbiGea08wHQYDVR0OBBYEFHL0At4O
GUdcOHVGg4Tfo4hl7LLGMAwGCCqGSM49BAMDBQADZwAwZAIwDWPHo5I04ZFVrkfk
St6gwH2UNF37jBscRN1lOE4SIwezZAqVs42BNMkWRjJBgiHzAjBm4m3zOjsXzNL8
+u8ALjQQCpBDT6dUHujzY5CRxG0xEHi5IXsXf4QwbctnjjvTeYA=
-----FIM DO CERTIFICADO-----
subject=/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
issuer=/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
---
Nomes da autoridade de certificação do certificado de cliente aceitável
/C=US/O=IBM Service Engage/CN=ca_ec_384.ibmserviceengage.com
/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=ca_ec_384.apm.ibmserviceengage.com
/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert
Global Root CA/C=US/O=IBM Service Engage/OU=Application Performance
Management/CN=*.agents.na.apm.ibmserviceengage.com
Chave temporária do servidor: ECDH, prime256v1, 256 bits
---
O handshake SSL leu 2659 bytes e gravou 261 bytes
---
Novo, TLSv1/SSLv3, a cifra é ECDHE-ECDSA-AES128-GCM-SHA256
A chave pública do servidor é de 384 bits
Secure Renegotiation IS suportado
Compactação: NENHUMA
Expansão: NENHUMA
SSL-Session:
```

```
Protocolo: TLSv1.2
Cifra: ECDHE-ECDSA-AES128-GCM-SHA256
Session-ID:
A18C31D0B45A1166357C917E1CFCD86A9FBEDB4A0EB768EF5390AC28C95CB7EF
Session-ID-ctx:
Chave mestra:
252B8FE2731E51AC0B79A27C7BED33CA8B15AF4CFD015C98DBACA46EA01DC40B
9E6B56E62E0F332FF6B56266B5ADD7B0
Key-Arg: Nenhum
Krb5 Principal: nenhuma
Identidade do PSK: nenhum
Sugestão de identidade do PSK: nenhum
Horário de início: 1510772474
Tempo limite: 7200 (seg)
Verify return code: 19 (self signed certificate in certificate chain)
---
FEITO
SSL3 alert write:warning:close notify
```

Se o sistema de computador não tiver conectividade com o Servidor Cloud APM, mensagens semelhantes ao exemplo a seguir serão exibidas:

```
getaddrinfo: Name or service not known
connect:errno=2
```

Se o sistema de computador não puder obter o certificado do servidor, porque os conjuntos de cifras estão sendo bloqueados em algum lugar da rede, serão exibidas mensagens como a seguinte:

```
SSL_connect:failed
---
nenhum certificado do peer disponível
---
No client certificate CA names sent
```

Sobre Esta Tarefa

Quando um proxy de encaminhamento é usado, o coletor de dados primeiro abre uma conexão TCP com o proxy. O coletor de dados envia uma solicitação de conexão e a URL do terminal de destino (servidor Servidor Cloud APM) para o proxy de encaminhamento. Em seguida, o proxy de encaminhamento estabelece uma conexão TCP com o terminal de destino e configura uma sessão de tunelamento HTTPS entre o coletor de dados e o servidor Servidor Cloud APM.

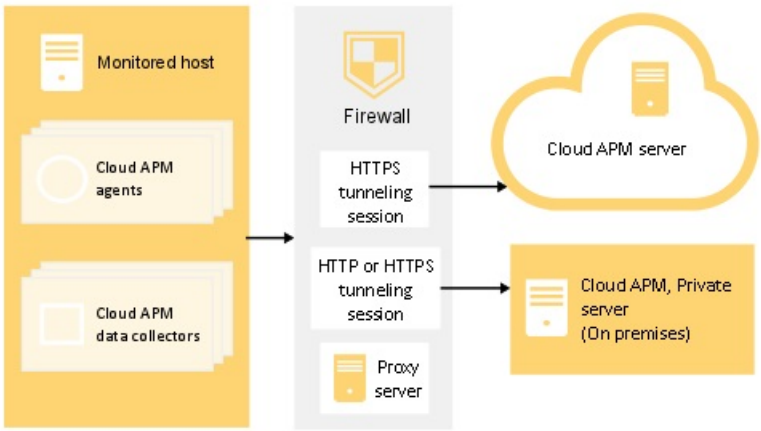


Figura 2. Diagrama de conexão para usar um proxy de encaminhamento

Alguns coletores de dados suportam proxies de autenticação, por exemplo, Node.js e coletores de dados Liberty. Esses coletores de dados suportam logon em um proxy de encaminhamento usando um ID do usuário e senha de proxy configurado.

Procedimento

1. Para configurar a comunicação do proxy de encaminhamento para coletores de dados Python, conclua uma das seguintes etapas:
   - Abra o arquivo de propriedades do coletor de dados *<dc home>*/config.properties em um editor de texto, em que *<dc home>* é o diretório inicial de instalação dos coletores de dados, por exemplo, /usr/lib/python2.7/site-packages/ibm_python_dc. Atualize a variável com o host do proxy e o número da porta, por exemplo, APM_GW_PROXY_CONNECTION =http://9.181.138.247:8085. A edição da variável neste arquivo afeta todos os aplicativos com o coletor de dados Python ativado.

     Nota: Para configurar a comunicação do proxy de encaminhamento para um único aplicativo, copie o arquivo *<dc home>*/config.properties no diretório do aplicativo único. Atualize a variável no diretório do aplicativo.
   - Execute o comando a seguir nos Sistemas Linux:

     ```
     export APM_GW_PROXY_CONNECTION =http://<http proxy host>:<http proxy port>
     ```

     por exemplo,

     ```
     export APM_GW_PROXY_CONNECTION =http://9.181.138.247:8085
     ```
2. Para configurar a comunicação do proxy de encaminhamento para coletores de dados Node.js, conclua uma das seguintes etapas:
   - Execute o comando a seguir nos Sistemas Linux:

     ```
     export APM_GW_PROXY_CONNECTION =http://<http proxy host>:<http proxy port>
     ```

     por exemplo,

     ```
     export APM_GW_PROXY_CONNECTION =http://9.181.138.247:8085
     ```
   - Se um nome do usuário e senha forem necessários para acessar o servidor proxy de encaminhamento para coletores de dados Node.js, execute o seguinte comando em sistemas Linux:

     ```
     export APM_GW_PROXY_CONNECTION =http://<http proxy user>:
     <http proxy password>@<http proxy host>:<http proxy port>
     ```

     por exemplo,

     ```
     Export APM_GW_PROXY_CONNECTION =http://Joe:passw0rd@9.181.138.247:8085
     ```
3. Para configurar a comunicação do proxy de encaminhamento para coletores de dados Liberty, edite o arquivo *<Liberty server home>*/jvm.options, em que *<Liberty server home>* é o diretório inicial do servidor Liberty, por exemplo: /opt/ibm/wlp/usr/servers/defaultServer/jvm.options. Execute uma das seguintes etapas:
   - Se a autenticação não for necessária, inclua o seguinte código no arquivo jvm.options:

     ```
     -Dhttp.proxyHost=<http proxy host>
     -Dhttp.proxyPort=<http proxy port>
     -Dhttps.proxyHost=<https proxy host>
     -Dhttps.proxyPort=<https proxy port>
     -Djava.net.useSystemProxies=true
     ```

- Se um nome do usuário e senha forem necessários para acessar o servidor proxy de encaminhamento, inclua o seguinte código no arquivo `jvm.options`:

```
-Dhttp.proxyHost=<http proxy host>
-Dhttp.proxyPort=<http proxy port>
-Dhttp.proxyUser=<http proxy user>
-Dhttp.proxyPassword=<http proxy password>
-Dhttps.proxyHost=<https proxy host>
-Dhttps.proxyPort=<https proxy port>
-Dhttps.proxyUser=<https proxy user>
-Dhttps.proxyPassword=<https proxy password>
-Djava.net.useSystemProxies=true
```

4. Reinicie o aplicativo local para implementar suas mudanças.

Resultados
Você configurou seus coletores de dados para se comunicarem através de um proxy de encaminhamento.

Nomes de Sistemas Gerenciados

O nome do sistema gerenciado (MSN) é usado para identificar exclusivamente cada agente do Cloud APM em seu ambiente. Ele também é o nome da instância vista no Application Performance Dashboard durante a seleção de um grupo para cada sistema gerenciado da seção **Grupos** do navegador. Para evitar conflitos em seu ambiente, designe MSNs exclusivos a seus agentes.

O formato do MSN do agente difere, dependendo de seu tipo de agente. Ele está em uma das seguintes categorias:

- “Formato comum do MSN para agentes de instância única” na página 165
- “Formato comum do MSN para agentes de multi-instâncias” na página 165
- “Formato de MSN especial” na página 166

Formato comum do MSN para agentes de instância única

Para a maioria dos agentes de instância única, a forma comum do MSN segue este formato:

```
hostname:pc
```

em que:

- *hostname* é o nome do computador em que o agente está instalado. Essa parte pode ser mudada, se necessário.
- *pc* é o código do agente de dois caracteres maiúsculos, que não pode ser mudado. Para obter mais informações sobre os códigos do agente, consulte “Utilizando comandos do agente” na página 175.
- `:` é o separador, que não pode ser mudado.

Exemplo: `linuxhost01:LZ` é o MSN do agente do S.O. Linux.

Alguns agentes de instância única que não seguem esse formato de MSN são listados em Tabela 9 na página 166.

O MSN é limitado a 32 caracteres. Para esta categoria de MSN, 29 caracteres estão disponíveis para o nome do host porque o código do agente e o separador não podem ser mudados.

Importante: Se o comprimento do MSN exceder 32 caracteres, parte do MSN é truncado e não é exibido corretamente no Console do Cloud APM. Por exemplo, se seu nome do host for `VeryLongSalesDivisionServerName03`, o nome do sistema gerenciado deverá ser `VeryLongSalesDivisionServerName03:PC`. No entanto, ele é truncado para `VeryLongSalesDivisionServerName0`.

Formato comum do MSN para agentes de multi-instâncias

Para a maioria dos agentes de multi-instâncias, o formato comum do MSN segue este formato:

```
instancename:hostname:pc
```

em que:

- *instancename* é o nome da instância de agente especificado durante a configuração do agente. Use esta variável para assegurar um MSN exclusivo para cada instância de cada tipo de agente em cada computador host do agente.

  Lembre-se:

  – Letras do alfabeto latino (a-z, A-Z), numerais arábicos (0-9), e o caractere hífen ou sinal de menos (-) podem ser usados para criar nomes de instâncias do agente.

  – O caractere de sublinhado (_) não é permitido em nomes de instâncias do agente.

  – O nome da instância especificado é limitado da seguinte forma:

  - Linux AIX 28 caracteres, menos o comprimento do nome do host em sistemas Linux ou AIX.
  - Windows 28 caracteres, menos o comprimento do nome do host ao usar o arquivo de resposta silencioso para configuração em sistemas Windows. Exemplo, `Server-Name` tem 11 caracteres. Portanto, as instâncias de agente no host `Server-Name` devem ter 17 caracteres ou menos.
  - Windows 20 caracteres menos o comprimento pelo qual seu nome do host excede 8 caracteres ao usar a configuração do Console do Cloud APM em sistemas Windows. Exemplo, `TestServer` tem 10 caracteres, que excede 8 em 2. Portanto, as instâncias de agente no host `TestServer` devem ter 18 caracteres ou menos.

- *hostname* é o nome do computador em que o agente está instalado. O componente do nome do host do MSN pode ser mudado se necessário.
- *pc* é o código do agente de dois caracteres maiúsculos, que não pode ser mudado. Para obter mais informações sobre os códigos do agente, consulte “Utilizando comandos do agente” na página 175.
- `:` é o separador, que não pode ser mudado.

Exemplo: `jboss1:win2016:JE` é o MSN para o agente JBoss.

Alguns agentes de multi-instâncias que não seguem este formato de MSN são listados em Tabela 9 na página 166.

O MSN é limitado a 32 caracteres. Para esta categoria de MSN, 28 caracteres estão disponíveis entre o nome da instância e o nome do host, porque o código do agente e os separadores não podem mudar.

Importante: Se o comprimento do MSN exceder 32 caracteres, parte do MSN é truncado e não é exibido corretamente no Console do Cloud APM. Por exemplo, se você especificar `VeryLongInstanceName` como o nome da instância, e o nome de seu servidor for `Production09`, o nome do sistema gerenciado deverá ser `VeryLongInstanceName:Production09:`*PC*. No entanto, ele é truncado para `VeryLongInstanceName:Production0`.

Formato de MSN especial

O formato de MSN especial se aplica aos agentes cujos MSNs não seguem os dois formatos comuns de MSN acima. Esses agentes estão listados em Tabela 9 na página 166.

O MSN especial é limitado a 32 caracteres. No Tabela 9 na página 166, apenas as sequências em itálico na coluna de formato do MSN podem mudar.

Tabela 9. Formato de MSN especial

Agentes	Formato de MSN	Exemplo de MSN
Agente Amazon EC2	`B5:`*ec2subnodename*`:INS`	`B5:sales:INS`

Tabela 9. Formato de MSN especial (continuação)

Agentes	Formato de MSN	Exemplo de MSN
Agente Amazon ELB	• AL:*instancename*A:APP • AL:*instancename*C:CLA • AL:*instancename*N:NET	• AL:elb-inst3A:APP • AL:elb-inst3C:CLA • AL:elb-inst3N:NET
Agente Azure Compute	AK:*azure_compute_subnode_name*:AVM	AK:azc-inst3:AVM
Citrix VDI agent	VD:*citrixsitename*:XDS	VD:xds1:XDS
DataPower agent	BN:*datapowersystemname*:DPS	BN:datapower23:DPS
Agente do Servidor HTTP	HU:*hostname_alias*:HUS	HU:docker-ihs_httpd:HUS
IBM Integration Bus agent	*monitoredbrokername*:*agentID*:KQIB	TRADEBRK:AGT1:KQIB
Agente do MQ Appliance	MK:*hostname_sectionname*:ARM	MK:bvtmin_linux150:ARM
Agente Node.js	NJ:*hostname_port*:NJA	NJ:KVM-014179_3000:NJA
Agente Oracle Database	• RZ:*dbconnection-instancename-hostname*:ASM • RZ:*dbconnection-instancename-hostname*:DG • RZ:*dbconnection-instancename-hostname*:RDB	RZ:11g-oracledbdemo-GVT-1BL:RDB
Agente Ruby	KM:*hostname_appname*:RAP	KM:nc9098036112_Blog:RAP
Agente SAP	• Instância SAP: *instancename-hostname_sid_instancenumber*:Ins • Integração de processos SAP: *instancename-hostname*:PI • SAP Solution Manager: *instancename-hostname*:Slm • Sistema SAP: *instancename-hostname*:Sys	• PS5-IBMSAP3V1_PS5_11:Ins • PS5-IBMSAP3V1:PI • PS8-IBMSAP3V3:Slm • PS5-IBMSAP3V1:Sys
SAP HANA Database agent	• SAP Hana Database: S7:*dbname-systemsid*:HDB • Sistema SAP Hana: *instancename*:*hostname*:S7	• S7:HNA-HNA:HDB • HNA:PS8760:S7
SAP NetWeaver Java Stack	• Cluster SAP NW Java AS: *instancename*:*hostname*:SV • Instância do SAP NW Java AS: SV:*systemsid-jvmid*:NWJ	• J01:VPT02F17:SV • SV:J01-83309750:NWJ
agente de S.O. UNIX	*hostname*:KUX	worklight17:KUX

Tabela 9. Formato de MSN especial (continuação)		
Agentes	**Formato de MSN**	**Exemplo de MSN**
Agente WebLogic	`WB:`*`instancename`*`:WLS`	`WB:Server1:WLS`
WebSphere Applications agent	• WebSphere Application Server: *`serveralias`*`:`*`hostname`*`:KYNS` • WebSphere Portal Server: *`serveralias`*`:`*`hostname`*`:KYNR` • WebSphere Process Server: *`serveralias`*`:`*`hostname`*`:KYNP`	`simpletrade:worklight 17:KYNS`
WebSphere MQ agent	*`monitoredqmgrname`*`:`*`agentnam e`*`:MQ`	`TRADEQM:PoC:MQ`
Windows OS agent	`Primary:`*`hostname`*`:NT`	`Primary:TRADEIIS1:NT`

Mudando o nome do sistema gerenciado do agente

Diferentes procedimentos se aplicam para mudar o nome do sistema gerenciado para diferentes agentes do Cloud APM. Para alguns agentes, a mudança do nome do sistema gerenciado significa a mudança do nome do host ou do nome da instância do agente (ou ambos) no nome do sistema gerenciado. Para outros agentes, procedimentos específicos são necessários para mudar o nome do sistema gerenciado.

Antes de Iniciar

Familiarize-se com os formatos de nome do sistema gerenciado e com as restrições de nomenclatura, conforme descrito em “Nomes de Sistemas Gerenciados” na página 165.

Sobre Esta Tarefa

Para a maioria dos agentes do Cloud APM, é possível usar o parâmetro **CTIRA_HOSTNAME** para mudar o nome do host usado no nome do sistema gerenciado. Para mudar o nome da instância de agente no nome do sistema gerenciado para agentes de múltiplas instâncias, é possível usar o parâmetro de configuração do agente. Se você configurou o agente, deverá reconfigurá-lo para designar um nome de instância de agente diferente. Depois de reconfigurar o agente, não será possível recuperar os dados coletados pela instância de agente anterior.

Talvez não seja possível mudar o nome do sistema gerenciado em um único procedimento, dependendo de qual parte do nome do sistema gerenciado você deseja mudar.

Para descobrir o método de mudança de nome do sistema gerenciado para o agente de seu interesse, consulte Tabela 10 na página 168.

Exception: A mudança do nome do sistema gerenciado não é suportada pelo Agente do Servidor HTTP, pelo Agente Node.js ou pelo Synthetic Playback agent

Tabela 10. Mudando os métodos de nome do sistema gerenciado para agentes do Cloud APM	
Agente	**método de mudança de nome do sistema gerenciado**
Agente Amazon EC2	Use o parâmetro de configuração do agente para mudar o nome do subnó do EC2 no nome do sistema gerenciado, consulte “Parâmetros de Configuração para o Agente Amazon EC2” na página 193.
Agente Amazon ELB	Crie uma nova instância do agente com um novo nome de instância para mudar o nome do sistema gerenciado.

Tabela 10. Mudando os métodos de nome do sistema gerenciado para agentes do Cloud APM (continuação)

Agente	**método de mudança de nome do sistema gerenciado**
Agente Azure Compute	Use o parâmetro de configuração do agente para mudar o nome do subnó no nome do sistema gerenciado, consulte “Parâmetros de Configuração para o Agente Azure Compute” na página 208.
Agente Cassandra	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte “Mudando o nome do host no nome do sistema gerenciado” na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
Cisco UCS agent	Use o parâmetro de configuração do agente para mudar o nome da instância de agente; consulte “Parâmetros de configuração para o agente” na página 217.
Citrix VDI agent	Use o parâmetro de configuração do agente para mudar o nome do site do Citrix; consulte “Parâmetros de Configuração para o Citrix VDI agent” na página 227.
Db2	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte “Mudando o nome do host no nome do sistema gerenciado” na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
DataPower agent	Use o parâmetro de configuração do agente para mudar o nome do sistema gerenciado; consulte “Configurando o DataPower agent” na página 238.
DataStage agent	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte “Mudando o nome do host no nome do sistema gerenciado” na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
Agente do Hadoop	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte “Mudando o nome do host no nome do sistema gerenciado” na página 173.
Agente HMC Base	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte “Mudando o nome do host no nome do sistema gerenciado” na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
IBM Cloud agent	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte “Mudando o nome do host no nome do sistema gerenciado” na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.

Tabela 10. Mudando os métodos de nome do sistema gerenciado para agentes do Cloud APM (continuação)

Agente	método de mudança de nome do sistema gerenciado
IBM Integration Bus agent	"Especificando um nome do sistema gerenciado exclusivo para o IBM Integration Bus agent" na página 287
agente JBoss	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
agente do Linux KVM	Use parâmetros de configuração do agente; consulte "Configurando o monitoramento do Linux KVM" na página 472.
agente do S.O. Linux	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173.
Microsoft .NET agent	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173.
Microsoft Active Directory agent	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173.
Microsoft Exchange Server agent	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173.
Microsoft Hyper-V Server agent	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173.
Microsoft IIS agent	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173.
Microsoft Office 365 agent	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173.
Microsoft SQL Server agent	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
Microsoft SharePoint Server agent	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173.

Tabela 10. Mudando os métodos de nome do sistema gerenciado para agentes do Cloud APM (continuação)

Agente	**método de mudança de nome do sistema gerenciado**
Agente MongoDB	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
Agente MySQL	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
Agente NetApp Storage	Use parâmetros de configuração do agente; consulte "Configurando o monitoramento do NetApp Storage" na página 580.
OpenStack agent	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
Agente Oracle Database	Use parâmetros de configuração do agente; consulte "Configurando o monitoramento do Banco de Dados Oracle" na página 615.
Agente PHP	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
Agente PostgreSQL	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
Agente RabbitMQ	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
Agente Response Time Monitoring	"Especificando um nome do sistema gerenciado exclusivo para o Agente Response Time Monitoring" na página 717
Agente Ruby	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173.

Tabela 10. Mudando os métodos de nome do sistema gerenciado para agentes do Cloud APM (continuação)

Agente	método de mudança de nome do sistema gerenciado
Agente SAP	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
SAP HANA Database agent	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
SAP NetWeaver Java Stack	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
Agente Siebel	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
Agente Skype for Business Server (anteriormente conhecido como agente Microsoft Lync Server)	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173.
Agente Sterling File Gateway	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
Agente Sterling Connect Direct	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
Agente Tomcat	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.

Tabela 10. Mudando os métodos de nome do sistema gerenciado para agentes do Cloud APM (continuação)	
Agente	**método de mudança de nome do sistema gerenciado**
agente de S.O. UNIX	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173.
WebSphere Applications agent	Para mudar o nome do host no nome do sistema gerenciado, consulte Como mudar o nome do host usado no nome do sistema gerenciado para a instância do agente do WAS?. Para mudar o nome do alias do servidor no nome do sistema gerenciado, reconfigure o agente, consulte "Reconfigurando o coletor de dados interativamente" na página 845.
WebSphere Infrastructure Manager agent	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173. Use o parâmetro de configuração do agente para mudar o nome da instância no nome do sistema gerenciado.
WebSphere MQ agent	"Especificando nomes de sistemas gerenciados exclusivos para vários gerenciadores de filas" na página 938
Windows OS agent	Use o parâmetro **CTIRA_HOSTNAME** para mudar o nome de host no nome do sistema gerenciado. Consulte "Mudando o nome do host no nome do sistema gerenciado" na página 173.

Mudando o nome do host no nome do sistema gerenciado

Sobre Esta Tarefa

Não é uma prática comum mudar o nome do host no nome do sistema gerenciado. O nome do host é automaticamente detectado e configurado durante a configuração do agente. Mude o nome do host no nome do sistema gerenciado apenas quando necessário e certifique-se de que o valor especificado não cause truncamentos devido às restrições de nomenclatura do nome do sistema gerenciado.

Procedimento

1. Pare todas as instâncias existentes do agente e aguarde até que o Console do Cloud APM mostre que o agente ou seus subnós estão off-line. Se você não tiver nenhuma instância de agente existente, avance para a próxima etapa.

   Para obter mais informações sobre como parar as instâncias de agente, consulte "Utilizando comandos do agente" na página 175.
2. Se o agente for um agente de instância única, conclua as seguintes etapas para mudar o parâmetro **CTIRA_HOSTNAME**. O valor especificado para o parâmetro **CTIRA_HOSTNAME** é o valor que é aplicado a todas as novas instâncias de agente.
   a) Faça uma cópia de backup do seguinte arquivo:
   - Linux AIX *install_dir*/config/*pc*.environment
   - Windows *install_dir*/TMAITM6_x64/k*pc*cma.ini

   em que:
   - *install_dir* é o diretório de instalação do agente.

- *pc* é o código do agente de dois caracteres. Consulte Nomes de agentes e tabela de códigos do agente.

b) Edite o arquivo mudando o valor de parâmetro **CTIRA_HOSTNAME** da seguinte forma, em que *newhostname* é a sequência customizada que é usada, em vez do nome real do host do computador onde o agente está instalado.

- Linux AIX **CTIRA_HOSTNAME**=*newhostname*
- Windows **CTIRA_HOSTNAME**=*newhostname* .TYPE=REG_EXPAND_SZ

c) Salve suas mudanças.

3. Se o agente for um agente de multi-instâncias, conclua as seguintes etapas para mudar o parâmetro **CTIRA_HOSTNAME**. Normalmente, todas as instâncias do agente em um computador usam o mesmo valor de nome do host. Se for preciso que as instâncias do agente usem valores diferentes, varie o valor designado a **CTIRA_HOSTNAME** ao executar esta etapa.

a) Faça uma cópia de backup dos seguintes arquivos:

- Linux AIX *install_dir*/config/*pc_instance*.environment
- Windows *install_dir*/TMAITM6_x64/kpccma_*instance*.ini

b) Edite o arquivo e mude o valor de parâmetro **CTIRA_HOSTNAME** conforme a seguir:

- Linux AIX **CTIRA_HOSTNAME**=*newhostname*
- Windows **CTIRA_HOSTNAME**=*newhostname* .TYPE=REG_EXPAND_SZ

c) Salve suas mudanças.

4. Windows
Reconfigure as instâncias do agente existentes.
5. Inicie todas as instâncias do agente.

O que Fazer Depois
Depois de mudar o nome do sistema gerenciado do agente, inicie o Console do Cloud APM e modifique seus aplicativos removendo o antigo nome do sistema gerenciado dos aplicativos e incluindo o novo no lugar.

Configurando Agentes

Após a instalação, alguns agentes são configurados e iniciados automaticamente, enquanto alguns agentes requerem configuração manual, mas são iniciados automaticamente. Alguns agentes devem ser configurados e iniciados manualmente. Agentes de várias instâncias requererem a criação de uma primeira instância e o início manual.

Antes de Iniciar

Ao instalar um agente, um arquivo de configuração silenciosa de amostra é colocado no diretório `/opt/ibm/apm/agent/samples`, por exemplo, `ynv_silent_config_agent.txt` e `datapower_silent_config.txt`.

Nota: Alguns agentes, por exemplo, Monitoring Agent for WebSphere Applications, têm vários arquivos de configuração silenciosa para diferentes tarefas, como configurar o coletor de dados.

Sobre Esta Tarefa
Para obter detalhes da implementação específicos para agentes, consulte Capítulo 5, “Implementação do agente e do coletor de dados”, na página 109.

Para configurar um agente, é possível usar a linha de comandos ou um arquivo silencioso de resposta, conforme descrito neste procedimento.

Os métodos de configuração variam entre os agentes; use o procedimento fornecido para seu agente.

Procedimento

- Execute o comando *agent-name*.sh config.
  Para mais comandos, consulte a Tabela 12 na página 178 e a Tabela 13 na página 179.
- Edite o arquivo de resposta silencioso e execute um dos comandos a seguir:
  - Para agentes de instância única, execute o seguinte comando:

    ```
    agent-name.sh config response_file
    ```

  - Para agentes de várias instâncias, execute o seguinte comando:

    ```
    agent-name.sh config instance_name response_file
    ```

  - em que *instance_name* é o nome da instância, que pode ser designado para indicar o que está sendo monitorado.
- Windows
  Para agentes que são suportados em sistemas Windows, é possível executar algumas tarefas de configuração usando o IBM Cloud Application Performance Management. Clique em **Iniciar** > **Todos os Programas** > **Agentes de Monitoramento IBM** > **IBM Cloud Application Performance Management**. Para obter mais informações, consulte "Usando a janela IBM Cloud Application Performance Management em sistemas Windows" na página 180.
- Para executar configuração avançada para alguns agentes, como configurar rastreamento de transações ou coleta de dados e ativar dados diagnósticos, use a janela **Configuração do agente**. Para obter mais informações, consulte "Página Configuração do Agente" na página 180.

Utilizando comandos do agente
Os mesmos scripts que você usa para instalar agentes de monitoramento também são usados para verificar o status de um agente instalado, pará-lo ou iniciá-lo ou desinstalar o agente.

Sobre Esta Tarefa
O nome do agente e os códigos do agente são fornecidos para sua referência.

Use o nome do agente nos comandos a seguir:

Linux AIX *name*-agent.sh
Windows *name*-agent.bat

Em que *name* é o nome do agente que é especificado em Tabela 11 na página 175.

Tabela 11. Nomes do agente e códigos do agente

Agente de monitoramento	***name***	**Código do agente de duas letras**
Monitoring Agent for Amazon EC2	amazon_ec2	b5
Monitoring Agent for Azure Compute	azure_compute	ak
Monitoring Agent for Cassandra	cassandra	zc
Monitoring Agent for Cisco UCS	cisco_ucs	v6
Monitoring Agent for Citrix Virtual Desktop Infrastructure	citrix_vdi	vd
Monitoring Agent for DataPower	datapower	bn
Monitoring Agent for Db2	db2	ud
Monitoring Agent for Hadoop	hadoop	h8
Monitoring Agent for HMC Base	hmc_base	ph

Tabela 11. Nomes do agente e códigos do agente (continuação)		
Agente de monitoramento	***name***	**Código do agente de duas letras**
Monitoring Agent for HTTP Server	`http_server`	`hu`
Monitoring Agent for IBM Cloud	`ibm_cloud`	`sistema de arquivos`
Monitoring Agent for IBM Integration Bus	`iib`	`qi`
Monitoring Agent for MQ Appliance	`ibm_mq_appliances`	`mk`
Monitoring Agent for InfoSphere DataStage	`DataStage`	`dt`
Monitoring Agent for JBoss	`jboss`	`je`
Monitoring Agent for Linux KVM	`linux_kvm`	`v1`
Monitoring Agent for Linux OS	`os`	`lz`
Monitoring Agent for MariaDB	`mariadb`	`mj`
Monitoring Agent for Microsoft Active Directory	`msad`	`3z`
Monitoring Agent for Microsoft Cluster Server	`mscs`	`q5`
Monitoring Agent for Microsoft Exchange Server	`msexch`	`ex`
Monitoring Agent for Microsoft Hyper-V Server	`microsoft_hyper-v_server`	`hv`
Monitoring Agent for Microsoft Internet Information Services	`msiis`	`q7`
Monitoring Agent for Skype for Business Server (anteriormente conhecido como Microsoft Lync Server)	`skype_for_business_server`	`ql`
Monitoring Agent for Microsoft .NET	`dotnet`	`qe`
Monitoring Agent for Microsoft Office 365	`microsoft_office365`	`mês`
Monitoring Agent para Microsoft SharePoint Server	`ms_sharepoint_server`	`qp`
Monitoring Agent for Microsoft SQL Server	`mssql`	`oq`
Monitoring Agent for MongoDB	`mongodb`	`kj`
Monitoring Agent for MySQL	`mysql`	`se`
Monitoring Agent for NetApp Storage	`netapp_storage`	`ni`
Monitoring Agent for Node.js	`nodejs`	`nj`
Monitoring Agent for OpenStack	`openstack`	`sg`
Monitoring Agent for Oracle Database	`oracle_database`	`rz`
Monitoring Agent for PHP	`php`	`pj`
Monitoring Agent for PostgreSQL	`postgresql`	`pn`
Monitoring Agent for Python	`python`	`pg`
Monitoring Agent for RabbitMQ	`rabbitMQ`	`zr`
Monitoring Agent for Ruby	`ruby`	`km`

Tabela 11. Nomes do agente e códigos do agente (continuação)		
Agente de monitoramento	***name***	**Código do agente de duas letras**
Monitoring Agent for SAP Applications	`sap`	`sa`
Monitoring Agent for SAP HANA Database	`sap_hana_database`	`s7`
Monitoring Agent for SAP NetWeaver Java Stack	`sap_netweaver_java_stack`	`sv`
Monitoring Agent for Siebel	`siebel`	`uy`
Monitoring Agent for Sterling Connect Direct	`sterling_connect_direct-agent`	`FC`
Monitoring Agent for Sterling File Gateway	file_gateway	fg
Monitoring Agent for Sybase Server	sybase	oy
Monitoring Agent for Synthetic Playback	`synthetic_transactions`	`sn`
Monitoring Agent for Tomcat	`tomcat`	`ot`
Monitoring Agent for UNIX OS	`os`	`ux`
Monitoring Agent for VMware VI	`vmware_vi`	`vm`
Monitoring Agent for WebLogic	`oracle_weblogic`	`wb`
Monitoring Agent for WebSphere Applications	`was`	`yn`
Monitoring Agent for WebSphere Infrastructure Manager	`wim`	`d0`
Monitoring Agent for WebSphere MQ	`mq`	`mq`
Monitoring Agent for Windows OS	`os`	`nt`
Response Time Monitoring Agent	`rt`	`t5`

Procedimento

- Linux AIX
  No sistema em que você deseja enviar um comando para o agente de monitoramento, mude para o diretório *`install_dir`*`/bin`. Insira qualquer um dos comandos em Tabela 12 na página 178 em que *name* é o nome do agente especificado em Tabela 11 na página 175.

Tabela 12. Comandos para sistemas UNIX e Linux	
Comando	**Descrição**
`./`*name*`-agent.sh status`	Verifica o status do agente. Os status podem ser em execução ou não em execução. Quando o agente estiver em execução, o status da conexão entre o agente e o Servidor Cloud APM também será verificado. Os possíveis status de conexão negativa são: falha na Conexão, Erro Detectado, Desconectado-Erro. O status positivo é Conectado, que é o status esperado. O status transitório é Conectando. Um status de Desconhecido significa que o status do agente não pode ser reconhecido possivelmente devido a erros no sistema de arquivos ou no arquivo de log do agente.
`./`*name*`-agent.sh start`	Inicia o agente de monitoramento. Se o agente possuir instâncias, insira um nome de instância após o comando.
`./`*name*`-agent.sh stop`	Para o agente. Se o agente possuir instâncias, insira um nome de instância após o comando.
`./`*name*`-agent.sh prereqcheck`	Executa uma varredura de pré-requisito. Esta opção de comando está disponível pra a maioria dos agentes.
`./`*name*`-agent.sh install`	Instala o agente de monitoramento. Para obter mais informações, consulte “Instalando agentes em sistemas UNIX” na página 118 e “Instalando agentes nos sistemas Linux” na página 124.
`./`*name*`-agent.sh config` *instance_name path_to_silent_config_file*	Configura o agente de monitoramento. Execute o comando a partir do diretório *install_dir*`/bin` e inclua o caminho do arquivo de resposta, se necessário. Se o agente possuir instâncias, insira um nome de instância. Para obter mais informações sobre quais agentes são agentes de múltiplas instâncias, consulte a Tabela 7 na página 111 . O *silent_config_file* é opcional. Se não especificar um arquivo para configuração silenciosa, poderá configurar o agente de monitoramento interativamente seguindo os prompts.
`./`*name*`-agent.sh uninstall`	Desinstala o agente de monitoramento. Para obter mais informações, consulte “Desinstalando os agentes” na página 143.
`./smai-agent.sh uninstall_all`	Desinstala todos os agentes de monitoramento no sistema gerenciado.
`./`*name*`-agent.sh remove` *instance_name*	Remove uma instância de um agente de instâncias múltiplas.
`./`*name*`-agent.sh`	Visualizar uma descrição das funções que estão disponíveis com o script.

- Windows

No sistema em que você deseja enviar um comando para o agente de monitoramento, vá para o diretório *install_dir*\BIN no prompt de comandos, por exemplo: C:\IBM\APM\bin. Insira qualquer um dos comandos em Tabela 13 na página 179 em que *name* é o nome do agente especificado em Tabela 11 na página 175.

Tabela 13. Comandos para sistemas Windows

Comando	Descrição
name-agent.bat status	Verifica o status do agente. Verifica o status da conexão entre o agente e o Servidor Cloud APM. Os possíveis status de conexão negativa são: falha na Conexão, Erro Detectado, Desconectado-Erro. O status positivo é Conectado, que é o status esperado. O status transitório é Conectando. Um status de Desconhecido significa que o status do agente não pode ser reconhecido possivelmente devido a erros no sistema de arquivos ou no arquivo de log do agente.
name-agent.bat start	Inicia o agente de monitoramento. Se o agente possuir instâncias, insira um nome de instância após o comando.
name-agent.bat stop	Para o agente. Se o agente possuir instâncias, insira um nome de instância após o comando.
name-agent.bat prereqcheck	Executa uma varredura de pré-requisito. Esta opção de comando está disponível pra a maioria dos agentes.
name-agent.bat install	Instala o agente de monitoramento. Para obter mais informações, consulte “Instalando agentes” na página 136.
name-agent.bat config *instance_name path_to_silent_config_file*	Configura o agente de monitoramento. Execute o comando a partir do diretório *install_dir* \bin e inclua o caminho do arquivo de resposta, se necessário. Se o agente possuir instâncias, insira um nome de instância. Para obter mais informações sobre quais agentes são agentes de múltiplas instâncias, consulte a Tabela 7 na página 111 . O *silent_config_file* é opcional. Se não especificar um arquivo para configuração silenciosa, poderá configurar o agente de monitoramento interativamente seguindo os prompts.
name-agent.bat uninstall	Desinstala o agente de monitoramento. Para obter mais informações, consulte “Desinstalando os agentes” na página 143.
smai-agent.bat uninstall_all	Desinstala todos os agentes de monitoramento no sistema gerenciado.
name-agent.bat remove *instance_name*	Remove uma instância de um agente de instâncias múltiplas.

Tabela 13. Comandos para sistemas Windows (continuação)	
Comando	**Descrição**
name-agent.bat	Visualizar uma descrição das funções que estão disponíveis com o script.

Comando de versão do agente

- Para ver a versão de um agente em seu ambiente, execute os comandos a seguir:
  - Linux AIX

    ```
    install_dir/bin/cinfo
    ```

    Insira 1 para mostrar as versões.
  - Windows

    ```
    install_dir/InstallITM/kincinfo
    ```

Tarefas relacionadas

"Usando a janela IBM Cloud Application Performance Management em sistemas Windows" na página 180

Usando a janela IBM Cloud Application Performance Management em sistemas Windows

Agentes suportados do Windows têm um utilitário de GUI que pode ser usado para executar a configuração do agente e verificar o status da conexão.

O utilitário de configuração de GUI não está disponível para Monitoring Agent for WebSphere MQ ou Monitoring Agent for IBM Integration Bus.

Procedimento

- Clique em **Iniciar** > **Todos os Programas** > **Agentes de Monitoramento IBM** > **IBM Cloud Application Performance Management**.

Resultados

A janela IBM Cloud Application Performance Management é exibida. Cada componente de agente instalado é listado com seu status de configuração, seja ele iniciado ou interrompido, o status da conexão, o número da versão e outras informações.

O que Fazer Depois

Inicie ou pare o agente ou configure os parâmetros clicando com o botão direito no agente e selecionando uma opção.

Página Configuração do Agente

Use a página **Configuração do agente** para configurar definições centralmente para esses agentes como Response Time Monitoring Agent e WebSphere Applications agent.

Uso geral

Após clicar em **Configuração do Sistema** > **Configuração do Agente** na barra de navegação, um painel tabulado é exibido com uma guia para cada agente de monitoramento configurável. A tabela mostra colunas de informações de configuração tais como, o nome e o endereço IP para cada sistema gerenciado, uma linha para cada sistema gerenciado.

Ações

Use as opções Ações para ativar ou desativar essas funções como rastreamento de transação ou coleta de dados.

Redimensionamento da coluna

Arraste a borda do título da coluna para ajustar a largura da coluna.

Classificação da Coluna

Clique dentro de um título da coluna para classificar por essa coluna. Clique no mesmo título da coluna novamente para alternar entre a ordem de classificação crescente e decrescente.

Filtro da Tabela

Clique dentro da caixa de texto de filtro  e digite o início do valor pelo qual filtrar a tabela. Conforme você digita, as linhas da tabela que não se encaixam nos critérios são filtradas e a linha ***Total*** é atualizada para o número de linhas encontradas.

Clique no "x" na caixa de filtragem  ou pressione a tecla BACKSPACE para limpar o filtro.

Configuração do Agent

Para obter informações adicionais sobre as configurações para os agentes específicos, consulte os seguintes tópicos:

- DataPower agent: “Configurando o monitoramento do DataPower” na página 230
- IBM Integration Bus agent: “Configurando o rastreamento de transações para o IBM Integration Bus agent” na página 286
- Monitoramento de Serviço da Internet“Configurando o agente nos sistemas Windows” na página 446
- agente JBoss: “Configure o coletor de dados de rastreamento de transações do agente JBoss” na página 468
- Microsoft .NET agent: “Ativando a coleta de dados de rastreamento de transações e diagnósticos” na página 525
- Monitoramento de arquivo de log do OS Agent: “Incluindo ou removendo a configuração de monitoramento do arquivo de log para os agentes de S.O.” na página 633
- Response Time Monitoring Agent: “Configurando usando a página Configuração do agente” na página 692
- Localização geográfica: “Customizando valores de locais de Transações do Usuário Final” na página 713
- Agente Ruby: “Desativando ou ativando dados diagnósticos para aplicativos Ruby” na página 725
- SAP NetWeaver Java Stack: “Ativando a coleta de dados de rastreamento de transações e diagnósticos” na página 770
- Agente Tomcat: “Ativando a coleta de dados de rastreamento de transações e diagnósticos” na página 807
- Agente WebLogic: “Configurando o rastreamento de transações para o Agente WebLogic” na página 826
- WebSphere Applications agent: “Configuração dinâmica da coleta de dados na página Configuração do Agente” na página 876
- WebSphere MQ agent: “Configurando o rastreamento de transações para o WebSphere MQ agent” na página 940

Configurando agentes como um usuário não raiz

Se você deseja configurar o agente como um usuário não raiz, crie um grupo comum no sistema e torne cada usuário um membro desse grupo.

Antes de Iniciar

Se você instalou seu agente como um usuário raiz ou não raiz e deseja configurar o agente como o mesmo usuário, nenhuma ação especial será necessária.

Se você instalou seu agente como um usuário selecionado e deseja configurar o agente como um usuário diferente, crie um grupo comum no sistema. Torne todos os usuários do gerenciamento de agente membros deste grupo comum. Transfira a propriedade de todos os arquivos e diretórios do agente para esse grupo.

Nota:

- Para o Agente do Servidor HTTP, se você configurar o agente como um usuário não raiz, o usuário não raiz deverá ter o mesmo ID do usuário que aquele que iniciou o IBM HTTP Server. Caso contrário, o agente tem problemas com a descoberta do IBM HTTP Server.
- Para o IBM Integration Bus agent, se a instalação do IBM Integration Bus for uma implementação de um único usuário, use o mesmo ID do usuário que o usuário que instalou o IBM Integration Bus para configurar o agente. Antes de configurar o agente, conclua as seguintes etapas para esse ID do usuário.

Procedimento

1. Instale seus agentes de monitoramento no Linux ou UNIX, conforme descrito em "Instalando agentes nos sistemas Linux" na página 124 e "Instalando agentes em sistemas UNIX" na página 118.
2. Execute o script `./secure.sh` com o nome do grupo do usuário não raiz para proteger os arquivos e configure a propriedade do grupo de arquivos para os arquivos.
   Por exemplo: **`./secure.sh -g db2iadm1`**
3. Configure seus agentes de monitoramento no Linux ou AIX conforme necessário, consulte Capítulo 7, "Configurando seu Ambiente", na página 157.
4. Para atualizar os scripts de inicialização do sistema, execute o script a seguir com acesso de usuário raiz ou de usuário sudo: *`install_dir`*`/bin/UpdateAutoRun.sh`

O que Fazer Depois

Para obter mais informações sobre o script **`./secure.sh`**, consulte Protegendo os arquivos de instalação do agente.

Use o mesmo ID de usuário para a instalação e os upgrades do agente.

Desativando o início automático do agente em sistemas UNIX e Linux
No sistema UNIX ou Linux, um agente pode ser iniciado automaticamente após a reinicialização do sistema operacional. Se você não deseja que o agente seja iniciado automaticamente após a reinicialização do sistema, é possível desativar o início automático do agente.

Sobre Esta Tarefa

Se você instalar um agente como usuário raiz no sistema UNIX ou Linux, o agente poderá iniciar automaticamente após a reinicialização do sistema. Ou, se você instalar um agente como um usuário não raiz, mas executar o script **`UpdateAutoRun.sh`** como raiz após a instalação, o agente poderá iniciar automaticamente após a reinicialização do sistema.

Procedimento

1. Conclua as etapas a seguir para desativar o início automático em alguns agentes:
   a. Para o agente do S.O. Linux e o agente WebSphere® Applications, inclua o código a seguir no arquivo `agent_install_dir/registry/kcirunas.cfg`:

```
<productCode>lz</productCode>
 <default>
   <autoStart>no</autoStart>
 </default>
 <productCode>yn</productCode>
 <default>
   <autoStart>no</autoStart>
 </default>
```

   b. Execute o comando **`agent_install_dir/bin/UpdateAutoRun.sh`**.
2. Conclua as etapas a seguir para ativar o início automático em alguns agentes:
   a. Para o agente do S.O. Linux e o agente WebSphere® Applications, no arquivo `agent_install_dir/registry/kcirunas.cfg`, altere o valor da tag *<autoStart>* para **yes**.
   b. Abra o arquivo `agent_install_dir/registry/AutoStart` e verifique o conteúdo.

c. Exclua o arquivo `/etc/init.d/ITMAgents{$Num}`, em que *{$Num}* é um número positivo no arquivo `agent_install_dir/registry/AutoStart`. Se o valor for 1, o arquivo `/etc/init.d/ITMAgents1` deverá ser excluído.

d. Execute o comando **`agent_install_dir/bin/UpdateAutoRun.sh`**.

Resultados

Após a reinicialização do sistema, um script do agente não será executado automaticamente para iniciar o agente.

Procedimento geral para configurar coletores de dados

Para usar um coletor de dados para visualizar dados de monitoramento no Console do Cloud APM para seus aplicativos, deve-se concluir várias tarefas de configuração.

Sobre Esta Tarefa

Este procedimento é um roteiro para configurar o monitoramento para seus aplicativos, que inclui etapas necessárias, condicionais e opcionais. Conclua as etapas necessárias de acordo com suas necessidades.

Procedimento

1. Faça download e extraia o pacote coletor de dados. Para obter instruções, veja "Fazendo download de seus agentes e coletores de dados" na página 101.
2. Configure o coletor de dados para coletar dados de monitoramento sobre os aplicativos IBM Cloud e no local e enviá-los para o Servidor Cloud APM. Conclua uma ou mais das seguintes tarefas, de acordo com o tipo de seu aplicativo:

   Aplicativos Liberty

   - "Configurando o coletor de dados Liberty para aplicativos no local" na página 880
   - "Configurando o coletor de dados Liberty para aplicativos IBM Cloud" na página 884

   Aplicativos Node.js

   - "Configurando o Coletor de dados Node.js independente para aplicativos IBM Cloud(antigo Bluemix)" na página 593
   - "Configurando o Coletor de dados Node.js para aplicativos no local" na página 598

   Aplicativos Python

   - "Configurando o coletor de dados Python para aplicativos IBM Cloud" na página 671
   - "Configurando o Coletor de dados do Python para aplicativos no local" na página 677

   Aplicativos Ruby

   - "Configurando o Coletor de dados Ruby para aplicativos IBM Cloud" na página 726

   Aplicativos Java

   - "Configurando o monitoramento do J2SE" na página 450
3. Se o arquivo-chave ou o Servidor Cloud APM mudar, reconecte o coletor de dados ao Servidor Cloud APM. Para obter instruções, veja "Reconectando o coletor de dados ao Servidor Cloud APM" na página 183.

O que Fazer Depois

Depois de concluir todas as tarefas de configuração necessárias, será possível verificar se os dados de monitoramento de seu aplicativo IBM Cloud são exibidos no console do Cloud APM.

Reconectando o coletor de dados ao Servidor Cloud APM

Se o Servidor Cloud APM, o arquivo-chave ou a senha do arquivo-chave mudar, você deve configurar diversas variáveis de ambiente para reconectar o coletor de dados ao Servidor Cloud APM.

Antes de Iniciar

Se o arquivo-chave mudar, criptografe a senha de texto simples de seu arquivo-chave usando Base64 primeiro. Se você for um usuário do Linux, execute o comando a seguir:

```
Echo -n keyfile_password | base64
```

A saída de comando é sua senha criptografada. Por exemplo, se a sua senha de texto simples for `password`, a saída de comando `cGFzc3dvcmQ=` será sua senha criptografada. Em seguida, use a senha criptografada para configurar `APM_KEYFILE_PSWD: encrypted_keyfile_password` e `APM_KEYFILE_PSWD=encrypted_keyfile_password` nas seguintes configurações.

Procedimento

- Para reconectar os coletores de dados ao Servidor Cloud APM para aplicativos IBM Cloud, consulte "Reconectando os coletores de dados para aplicativos IBM Cloud" na página 184.
- Para reconectar os coletores de dados no Servidor Cloud APM no local, consulte "Reconectando o coletor de dados para aplicativos no local" na página 185.

Reconectando os coletores de dados para aplicativos IBM Cloud

Sobre Esta Tarefa

Você tem as duas seguintes opções para reconectar o coletor de dados ao Servidor Cloud APM:

- Edite o `manifest.yml` de seu aplicativo para configurar as variáveis.
- Configure as variáveis na IU do IBM Cloud.

Procedimento

- Para usar o arquivo `manifest.yml` de seu aplicativo IBM Cloud para reconectar o coletor de dados, conclua as seguintes etapas:
  a) Edite as variáveis no arquivo `manifest.yml` de seu aplicativo IBM Cloud de acordo com as mudanças.
     – Para configurar o Gateway para usar *HTTP*, configure a variável a seguir:

       ```
       APM_BM_GATEWAY_URL: http://server_ip_or_hostname:80
       ```

     – Para configurar o Gateway para usar *HTTPS*, configure as três variáveis a seguir:

       ```
       APM_BM_GATEWAY_URL: https://server_ip_or_hostname:443
       APM_KEYFILE_PSWD: encrypted_keyfile_password
       APM_KEYFILE_URL: http://hosted_http_server:port/keyfile_name
       ```

       Dica: O arquivo-chave para o coletor de dados Liberty é um arquivo `.jks`. Para os coletores de dados Python, Node.js e Liberty, os arquivos-chave são arquivos `.p12`.
  b) Mude para o diretório de seu aplicativo IBM Cloud e execute o comando a seguir:

     ```
     cf push
     ```

- Para usar a IU do IBM Cloud para reconectar o coletor de dados, conclua as seguintes etapas:
  a) Efetue login na UI do IBM Cloud.
  b) Clique no aplicativo IBM Cloud.
  c) Clique em **Tempo de execução** no painel esquerdo.
  d) Alterne para a guia **Variável de ambiente**.
  e) Na seção **definido pelo usuário**, use um dos seguintes métodos para definir as variáveis de acordo com suas necessidades:

– Para configurar o Gateway para usar *HTTP*, configure a variável a seguir:

```
APM_BM_GATEWAY_URL: http://server_ip_or_hostname:80
```

– Para configurar o Gateway para usar *HTTPS*, configure as três variáveis a seguir:

```
APM_BM_GATEWAY_URL: https://server_ip_or_hostname:443
APM_KEYFILE_PSWD: encrypted_keyfile_password
APM_KEYFILE_URL: http://hosted_http_server:port/keyfile_name
```

Dica: O arquivo-chave para o coletor de dados Liberty é um arquivo `.jks`. Para os coletores de dados Python, Node.js e Liberty, os arquivos-chave são arquivos `.p12`.

f) No diretório onde é executado o comando **`cf push`** para enviar seu aplicativo por push, execute o seguinte comando para que suas mudanças entrem em vigor:

```
cf restage <app_name>
```

Resultados

Os valores das variáveis são configurados corretamente para conectar o coletor de dados ao Servidor Cloud APM.

Reconectando o coletor de dados para aplicativos no local

Sobre Esta Tarefa

Ao modificar o arquivo `global.environment` ou `dc.java.properties`, é possível customizar a conexão entre o coletor de dados e o servidor Cloud APM.

Procedimento

1. Localize o arquivo correspondente que contém as variáveis de conexão.
   a) Para o Coletor de dados Liberty, o Coletor de dados Node.js e o Coletor de dados do Python, localize o arquivo `global.environment` de acordo com as informações na tabela a seguir:

O nome do coletor de dados	**Diretório para o `global.environment` arquivo**
Coletor de dados Liberty	A pasta `itcamdc/etc/global.environment` na qual o Coletor de dados Liberty está instalado.
Coletor de dados Node.js	A pasta `ibmapm/etc` na qual o Coletor de dados Node.js está instalado.
Coletor de dados do Python	A pasta `etc` na qual o Coletor de dados do Python está instalado.

   b) Para o Coletor de dados J2SE, localize o arquivo `dc.java.properties` na pasta *DC_HOME*`/itcamdc/etc`. *DC_HOME* é o diretório no qual o Coletor de dados J2SE está instalado.
2. Edite as variáveis no arquivo correspondente de acordo com as mudanças.
   a) Para o Coletor de dados Liberty, Coletor de dados Node.js e o Coletor de dados do Python, edite o arquivo `global.environment` de acordo com a seguinte instrução:
      • Para configurar o Gateway para usar *HTTP*, configure a variável a seguir:

```
APM_BM_GATEWAY_URL=http://server_ip_or_hostname:80
```

- Para configurar o Gateway para usar *HTTPS*, configure as seguintes variáveis:

```
APM_BM_GATEWAY_URL=https://server_ip_or_hostname: 443
APM_KEYFILE_PSWD=encrypted_keyfile_password
APM_KEYFILE_URL=http://hosted_http_server_:port/keyfile_name
```

Dica: O arquivo-chave para o Coletor de dados Liberty é um arquivo `.jks`. Para os coletores de dados Python, Node.js e Liberty, os arquivos-chave são arquivos `.p12`.

b) Para o Coletor de dados J2SE, edite o arquivo `dc.java.properties` de acordo com a seguinte instrução:

- Para configurar o Gateway para usar *HTTP*, configure a variável a seguir:

```
Apm.http.type=http
```

Se o valor dessa variável for deixado vazio, `http` será o valor padrão

- Para configurar o Gateway para usar *HTTPS*, configure as seguintes variáveis:

```
apm.ssl.password=encrypted_keyfile_password
Apm.http.type=https
```

Importante: Se a senha for mudada, substitua o arquivo *DC_HOME*`/itcamdc/etc/keyfile.jks` pelo arquivo `/opt/ibm/ccm/keyfiles/default.agent/keyfiles/keyfile.jks` do servidor Cloud APM, em que *DC_HOME* é o diretório inicial de seu Coletor de dados J2SE.

3. Opcional: Se você não usar o arquivo-chave padrão para seu Coletor de dados Node.js, configure a variável a seguir:

```
APM_SNI=owner_host_in_the_key_file
```

Dica: Para descobrir o valor da variável *owner host*, abra o arquivo-chave que você usa e procure por `owner`. Em seguida, configure a variável *APM_SNI* para o mesmo valor de *owner*.

4. Reinicie o aplicativo para que a mudança entre em vigor.

Resultados
Os valores das variáveis são configurados corretamente para conectar o coletor de dados ao Servidor Cloud APM.

Arquivo `manifest.yml` de amostra
Consulte as seguintes linhas para o conteúdo do arquivo `manifest.yml` de um aplicativo IBM Cloud:

```
applications:

- disk_quota: 1024M
  host: myBluemixApp
  name: myBluemixApp
  path: .
  domain: mybluemix.net

  instances: 1
  memory: 512M

  env:
    KNJ_ENABLE_TT: "true"
    KNJ_SAMPLING: 1
```

Removendo coletores de dados do Console do Cloud APM
Depois de desconfigurar um coletor de dados, também é necessário remover o coletor de dados dos aplicativos e dos grupos de recursos nos quais ele foi incluído. Caso contrário, o Console do Cloud APM mostrará que nenhum dado está disponível para o aplicativo e não indicará que o coletor de dados está off-line.

Procedimento

1. Remova o coletor de dados de quaisquer aplicativos que você tenha incluído editando manualmente os aplicativos.

   Isso é semelhante à remoção de agentes off-line de seu aplicativo, consulte "Visualizando e removendo agentes off-line" na página 1104.
2. Remova o coletor de dados de todos os grupos de recursos customizados nos quais você incluiu.

   Para obter mais informações, consulte "Gerenciador de Grupos de Recursos" na página 980.
3. Abra um chamado para a equipe de Operações do Cloud APM para executar as seguintes etapas no Servidor Cloud APM:
   a) Edite o arquivo *install_dir*/serveragents/config/hostname_bi.cfg para remover as linhas para o coletor de dados que foi desconfigurado.
   b) Reinicie o componente do servidor para coletores de dados executando o comando a seguir como usuário raiz:

```
apm restart biagent
```

Resultados

Após alguns minutos, o Console do Cloud APM indicará que o coletor de dados está off-line no aplicativo **Meus componentes** e na IU do **Gerenciador de grupo de recursos** ao selecionar o grupo de recursos do sistema para o coletor de dados.

Após o intervalo especificado pela propriedade de configuração **Remover atraso do sistema off-line** na página **Configuração avançada**, o coletor de dados será removido automaticamente de **Meus componentes** e de seu grupo de recursos do sistema.

Dica: É possível ajustar a configuração **Remover atraso do sistema off-line** na página **Configuração Avançada** para aumentar ou diminuir o tempo de espera antes de o agente off-line ser removido da visualização. Para obter mais informações, consulte "Agent Subscription Facility" na página 1074.

Lembre-se: Se o coletor de dados forneceu dados de rastreamento de transação para o Servidor Cloud APM, o Console do Cloud APM poderá continuar a exibir o coletor de dados no aplicativo **Meus componentes** e exibirá a mensagem de `The agent is invalid` para o coletor de dados após o período de tempo especificado pela configuração **Remover atraso do sistema off-line** ter expirado. Se você instalou a Correção Temporária 3 do Cloud APM 8.1.4.0 Server ou mais recente, um coletor de dados inválido será removido eventualmente do aplicativo **Meus componentes** 8 dias após os dados de rastreamento de transação pararem de ser recebidos do coletor de dados.

Configurando o monitoramento do Amazon EC2 monitoring

O Agente Amazon EC2 fornece um ponto central de monitoramento para o funcionamento, disponibilidade e desempenho de Instâncias do Amazon Elastic Compute Cloud (EC2). O agente exibe um conjunto abrangente de métricas para ajudá-lo a tomar decisões informadas sobre seu ambiente do EC2. Essas métricas incluem o uso de CPU, o uso do Elastic Block Store (EBS), uso de rede, as atualizações de manutenção do Amazon Web Services (AWS), e o desempenho do disco.

Antes de Iniciar

- Leia o tópico "Configurando o monitoramento do Amazon EC2 monitoring" na página 187 inteiro para determinar o que é necessário para concluir a configuração.
- Estas instruções são para a liberação mais atual do agente, exceto conforme indicado.
- Certifique-se de que os requisitos do sistema para o Agente Amazon EC2 sejam atendidos em seu ambiente. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Agente Amazon EC2.
- Assegure-se de que as seguintes informações estejam disponíveis:

  - Uma lista de nomes da região AWS que contêm instâncias do EC2 a monitorar.
  - As credenciais de segurança do AWS (ID da chave de acesso e chave de acesso secreta) com permissão para acessar cada região do AWS.
- Assegure-se de que as credenciais de segurança do AWS que são usadas para cada região do AWS sejam membros de um grupo que inclua pelo menos a política *AmazonEC2ReadOnlyAccess*.

Sobre Esta Tarefa

O Agente Amazon EC2 é um agente de múltiplas instâncias e também um agente do subnó. É possível criar uma instância de agente com múltiplos subnós, um para cada região do Amazon EC2, ou é possível criar uma instância do agente para cada região do Amazon EC2 com um subnó para essa região. Ou é possível criar uma combinação de cada tipo de configuração. Depois de configurar instâncias de agente, você deve iniciar cada instância de agente manualmente. Se você tiver mais de 50 recursos por região do Amazon EC2, sugere-se criar uma instância do agente por região ou usar identificação em suas instâncias do EC2 e filtrar as instâncias do agente pelas tags que você cria usando o parâmetro de condição de filtragem do agente.

Procedimento

1. Configure o agente nos sistemas Windows com a janela **IBM Performance Management** ou o arquivo de resposta silencioso.
   - "Configurando o agente nos sistemas Windows" na página 188.
   - "Configurando o agente usando o arquivo silencioso de resposta" na página 192.
2. Configure o agente nos sistemas Linux com o script que solicita respostas ou com o arquivo de resposta silencioso.
   - "Configurando o agente respondendo aos prompts" na página 191.
   - "Configurando o agente usando o arquivo silencioso de resposta" na página 192.

O que Fazer Depois

No Console do Cloud APM, acesse seu Application Performance Dashboard para visualizar os dados que foram coletados. Para obter informações adicionais sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Se você não conseguir visualizar os dados nos painéis do agente, primeiro verifique os logs de conexão do servidor e, em seguida, os logs do provedor de dados. Os caminhos padrão para esses logs são listados aqui:

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Para obter ajuda com a resolução de problemas, consulte o Fórum do Cloud Application Performance Management.

Configurando o agente nos sistemas Windows

É possível configurar o Agente Amazon EC2 em sistemas operacionais Windows usando a janela IBM Cloud Application Performance Management. Após fazer a atualização dos valores de configuração, deve-se iniciar o agente para salvar os valores atualizados.

Procedimento

1. Clique em **Iniciar** > **Todos os programas** > **Agentes do IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito no modelo **Monitoring Agent for Amazon EC2** e, em seguida, clique em **Configurar agente**.

Lembre-se: Depois de configurar uma instância de agente pela primeira vez, a opção **Configurar agente** é desativada. Para configurar a instância de agente novamente, clique nela com o botão direito e clique em **Reconfigurar**.

3. Insira um nome de instância exclusivo e, em seguida, clique em **OK**. Use apenas letras latinas, numerais arábicos e o caractere de hífen ou de menos no nome da instância. Exemplo, `ec2-inst3`.

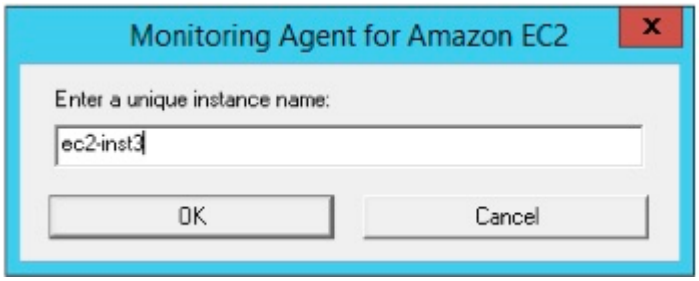


Figura 3. A janela para inserir um nome exclusivo da instância.

4. Clique em **Avançar** na janela de nome da instância de agente.

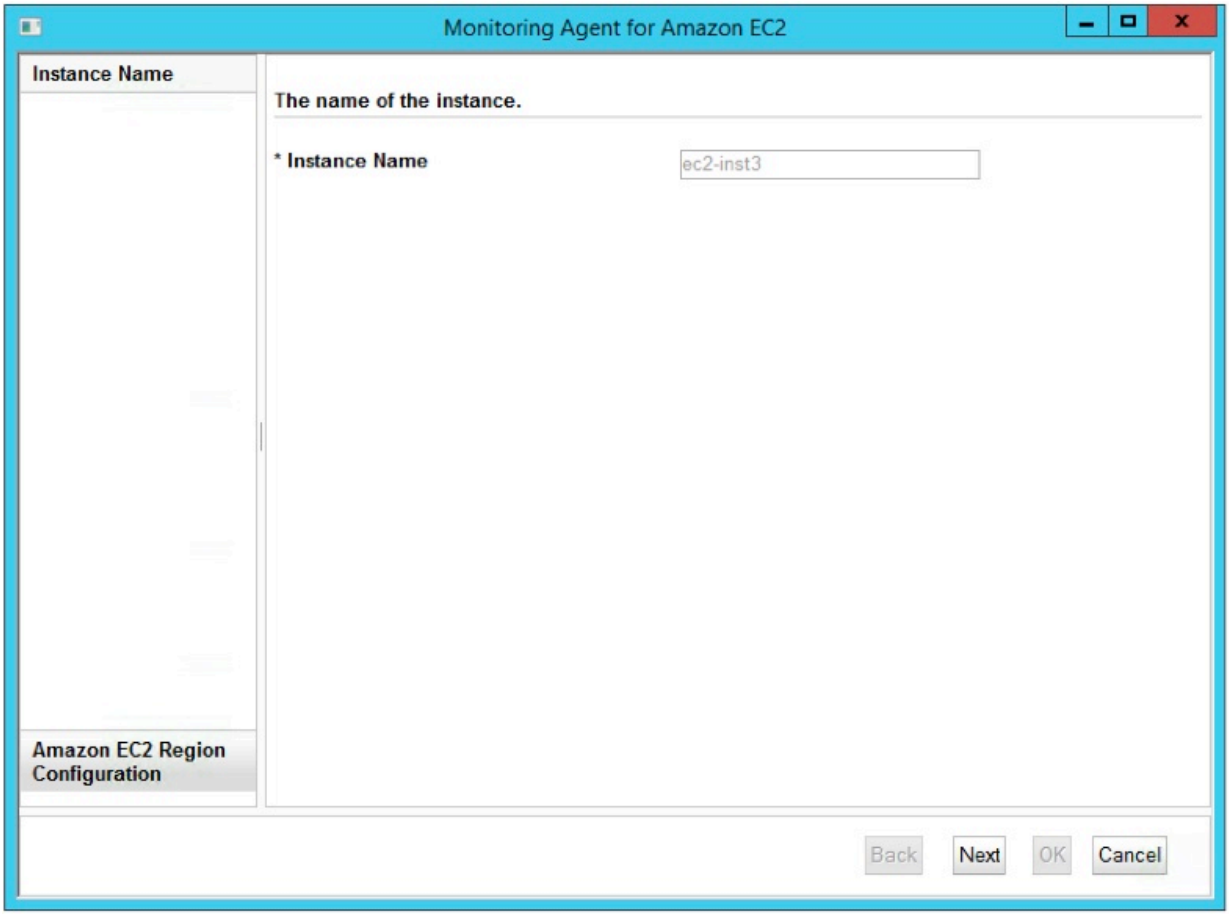


Figura 4. A janela de nome da instância de agente.

5. Insira as configurações de modelo de instância de **Configuração de região do Amazon EC2**.

   Nota: Esta seção não é a configuração da instância da região do Amazon EC2. É uma seção modelo para configurações que são usadas como valores padrão quando você inclui as configurações da instância da região real do Amazon EC2 na etapa 6.

   Consulte Tabela 14 na página 193 para obter uma explicação de cada um dos parâmetros de configuração.

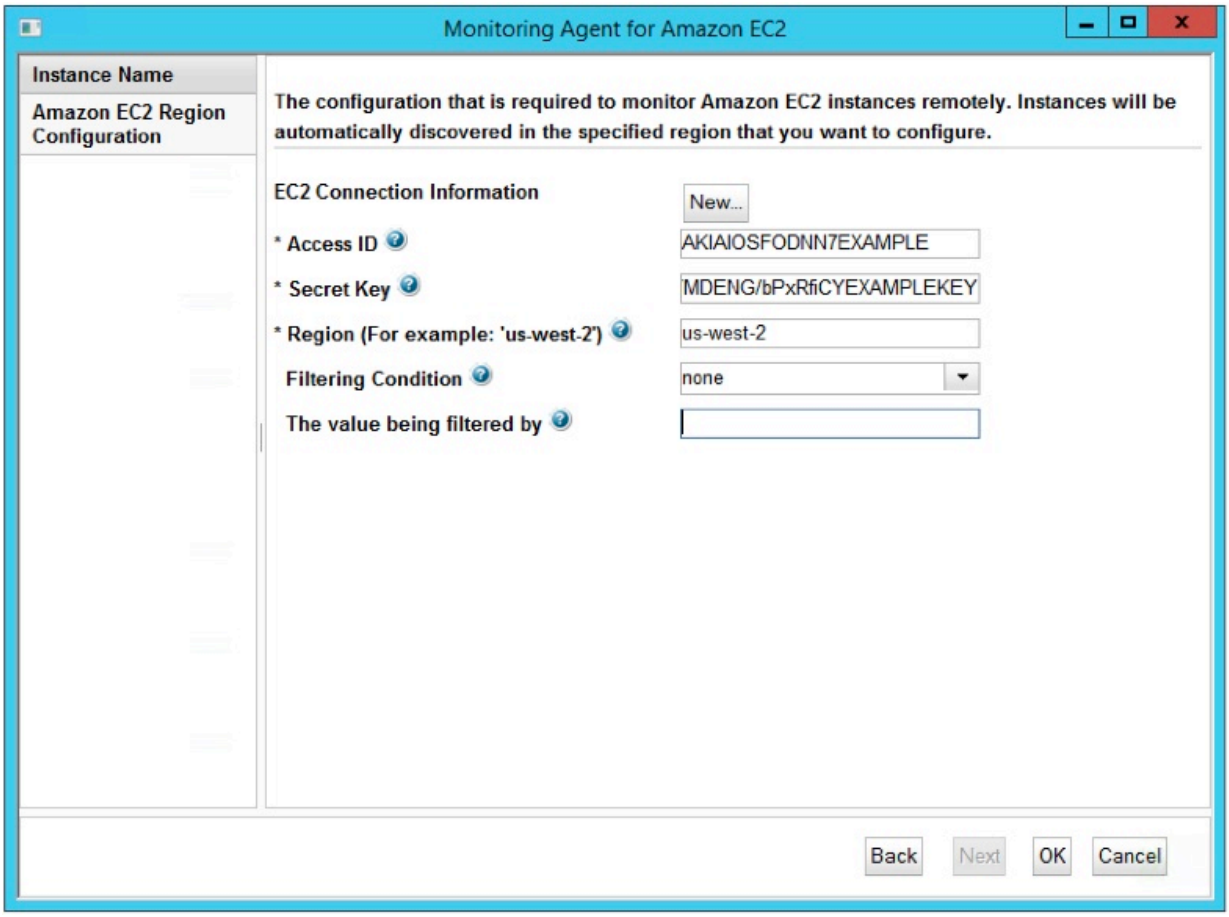


Figura 5. A janela para especificar as configurações de modelo de instância da região do Amazon EC2 .

6. Pressione **Novo** e insira as configurações de instância da região do Amazon EC2 e, em seguida, clique em **Avançar**.

   Consulte a seção Tabela 14 na página 193 para obter uma explicação de cada um dos parâmetros de configuração.

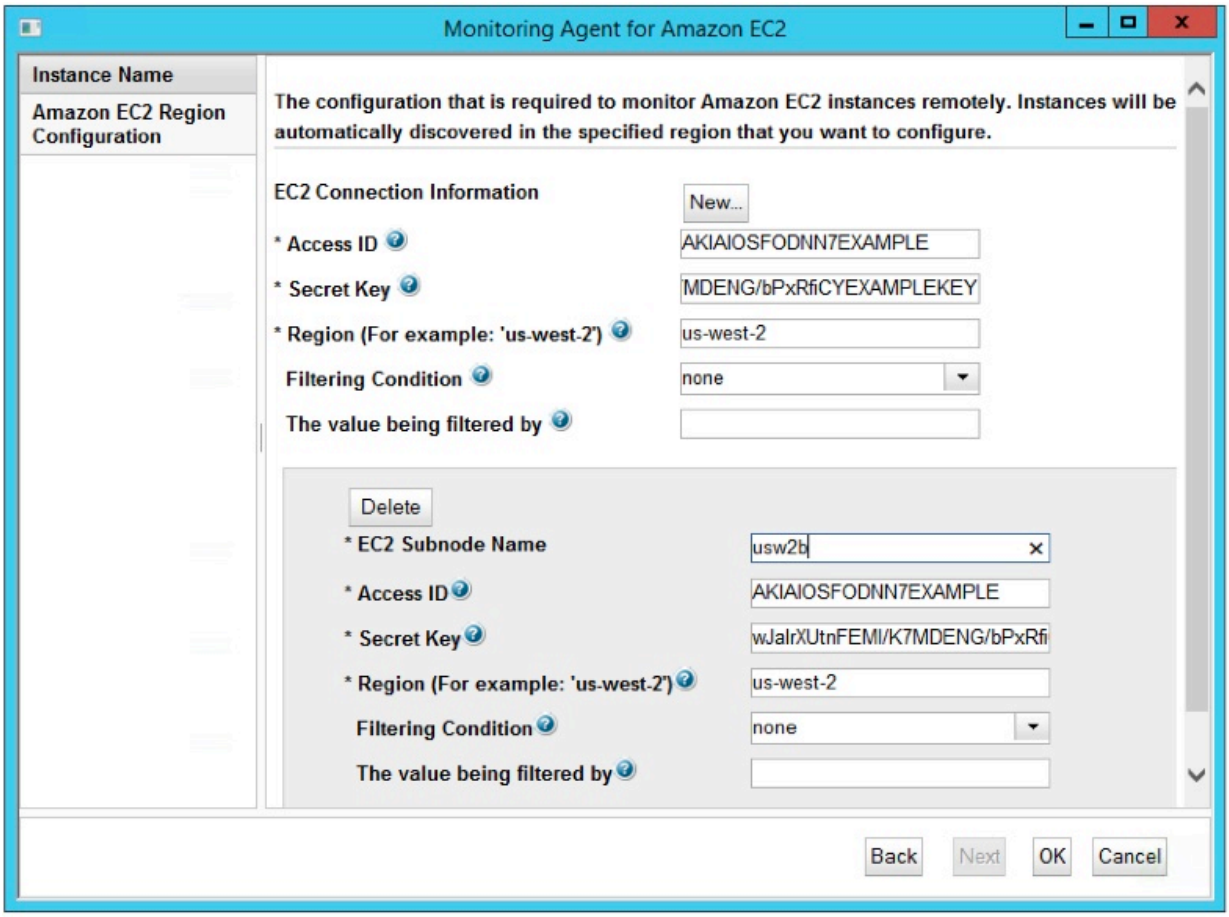


Figura 6. A janela para especificar as configurações de instância da região do Amazon EC2.

7. Clique em **OK** para concluir a configuração.
8. Na janela IBM Cloud Application Performance Management, clique com o botão direito na instância configurada e, em seguida, clique em **Iniciar**.

Configurando o agente respondendo aos prompts

Após a instalação do Agente Amazon EC2, deve-se configurá-lo antes de iniciar o agente. Se o Agente Amazon EC2 estiver instalado em um computador Linux local, será possível seguir essas instruções para configurá-lo interativamente por meio de prompts da linha de comandos.

Sobre Esta Tarefa

Lembre-se: Se estiver reconfigurando uma instância do agente configurada, o valor que é definido na última configuração será exibido para cada configuração. Se desejar limpar um valor existente, pressione a tecla Espaço quando a configuração for exibida.

Procedimento

Siga essas etapas para configurar o Agente Amazon EC2 executando um script e respondendo aos prompts.

1. Execute o seguinte comando:

```
install_dir/bin/amazonec2-agent.sh config instance_name
```

em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome que você deseja fornecer para a instância de agente.

Exemplo

```
/opt/ibm/apm/agent/bin/amazonec2-agent.sh config ec2-inst3
```

2. Responda aos prompts para configurar valores de configuração para o agente.

   Consulte "Parâmetros de Configuração para o Agente Amazon EC2" na página 193 para obter uma explicação de cada um dos parâmetros de configuração.

3. Execute o comando a seguir para iniciar o agente:

   ```
   install_dir/bin/amazonec2-agent.sh start instance_name
   ```

   em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome da instância de agente.

   Exemplo

   ```
   /opt/ibm/apm/agent/bin/amazonec2-agent.sh start ec2-inst3
   ```

Configurando o agente usando o arquivo silencioso de resposta

O arquivo silencioso de resposta contém os parâmetros de configuração do agente. É possível editar o arquivo silencioso de resposta para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

O arquivo silencioso de resposta contém os parâmetros de configuração do agente com valores padrão que são definidos para alguns parâmetros. É possível editar o arquivo silencioso de resposta para especificar os valores diferentes para os parâmetros de configuração.

Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

- Configure o Agente Amazon EC2 no modo silencioso:
  a) Abra o arquivo `amazonec2_silent_config.txt` em um dos seguintes caminhos em um editor de texto.
     – Linux *install_dir*`/samples/amazonec2_silent_config.txt`

       Exemplo, `/opt/ibm/apm/agent/samples/amazonec2_silent_config.txt`
     – Windows *install_dir*`\samples\amazonec2_silent_config.txt`

       Exemplo, `C:\IBM\APM\samples\amazonec2_silent_config.txt`

     em que *install_dir* é o caminho no qual o agente está instalado.
  b) No arquivo `amazonec2_silent_config.txt`, especifique valores para todos os parâmetros obrigatórios e modifique os valores padrão de outros parâmetros, conforme necessário.

     Consulte a seção "Parâmetros de Configuração para o Agente Amazon EC2" na página 193 para obter uma explicação de cada um dos parâmetros de configuração.
  c) Salve e feche o arquivo `amazonec2_silent_config.txt` e execute o seguinte comando:
     – Linux *install_dir*`/bin/amazonec2-agent.sh config` **instance_name** *install_dir*`/samples/amazonec2_silent_config.txt`

       Exemplo, **/opt/ibm/apm/agent/bin/amazonec2-agent.sh config ec2-inst3 /opt/ibm/apm/agent/samples/amazonec2_silent_config.txt**
     – Windows *install_dir*`\bin\amazonec2-agent.bat config` **instance_name** *install_dir*`\samples\amazonec2_silent_config.txt`

Exemplo, **C:\IBM\APM\bin\amazonec2-agent.bat config ec2-inst3 C:\IBM\APM \samples\amazonec2_silent_config.txt**

em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome que você deseja fornecer para a instância de agente.

Importante: Assegure que você inclua o caminho absoluto no arquivo silencioso de resposta. Caso contrário, os dados do agente não serão mostrados nos painéis.

d) Execute o comando a seguir para iniciar o agente:

– Linux *install_dir*/bin/amazonec2-agent.sh start **instance_name**

Exemplo, **/opt/ibm/apm/agent/bin/amazonec2-agent.sh start ec2-inst3**

– Windows *install_dir*\bin\amazonec2-agent.bat start **instance_name**

Exemplo, **C:\IBM\APM\bin\amazonec2-agent.bat start ec2-inst3**

em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome da instância de agente.

Parâmetros de Configuração para o Agente Amazon EC2

Os parâmetros de configuração para o Agente Amazon EC2 são exibidos em uma tabela.

1. Configuração de região do Amazon EC2 - Configurações para monitorar instâncias do Amazon EC2 remotamente. As instâncias são descobertas automaticamente na região especificada que você deseja configurar.

Tabela 14. Configuração de região do Amazon EC2

Nome do parâmetro	Descrição	Nome do parâmetro do arquivo de configuração silenciosa
Nome do subnó do EC2	Nome do subnó do EC2 para coleta de dados. Exemplo, *usw2a*. Este alias faz parte do nome do sistema gerenciado (MSN) e é usado para identificar visualmente o ambiente monitorado no Console do Cloud APM. **Nota:** Este alias pode ser qualquer coisa que você escolher para representar a instância do subnó do Amazon EC2 com as seguintes restrições. Letras do alfabeto latino (a-z, A-Z), numerais arábicos (0-9), o caractere de hífen ou de menos (-) e o caractere sublinhado (_) podem ser usados para criar nomes de instância do subnó do agente. O comprimento máximo de um nome de subnó do EC2 é de 25 caracteres.	Cada um dos seguintes parâmetros deve ter um sufixo de nome de subnó do agente que é o mesmo para cada parâmetro de uma instância do subnó do agente. Novas instâncias de subnó do agente devem usar um nome exclusivo para seu conjunto de parâmetros. Por exemplo, uma instância do subnó do agente pode usar *.usw2a* e outra instância do subnó do agente pode usar *.usw2b* em vez de *.subnode_name* nos nomes de parâmetro que seguem.
ID de Acesso	ID da chave de acesso de credenciais de segurança do AWS que é usado para autenticar-se com a região do Amazon especificada. Por exemplo, 'AKIAxxxxxxxxxxxxxx'.	**KB5_INS_ACCESS_ID.subnode_name**
Chave Secreta	Chave de acesso de segredo de credenciais de segurança do AWS que é usada para autenticar-se com a região do Amazon especificada. Por exemplo, 'kK7txxxxxxxxxxxxxxxxxxxxxxxx'.	**KB5_INS_SECRET_KEY.subnode_name**

Tabela 14. Configuração de região do Amazon EC2 (continuação)		
Nome do parâmetro	**Descrição**	**Nome do parâmetro do arquivo de configuração silenciosa**
Região	Região do AWS a monitorar. Por exemplo, 'us-west-2'.	**KB5_INS_REGION.subnode_name**
Condição de filtragem	O tipo de filtragem que está sendo feita. É possível usar tags customizadas em instâncias do EC2 para limitar quais instâncias do EC2 são monitoradas pelo agente. Para obter mais informações, consulte Marcando seus recursos do Amazon EC2. Opções de filtragem. **nenhum** Todas as instâncias do EC2 na região são monitoradas. **Filter Value** é ignorado. **tagName** As instâncias do EC2 com a chave de tag que é especificada em **Filter Value** são monitoradas, independentemente do valor real no valor de tag da instância do EC2 correspondente. Por exemplo, para monitorar todas as instâncias do EC2 que possuam a chave de tag *Stack*, independentemente do valor em seu valor de tag, especifique `Stack` em **Filter Value**. **tagName|tagValue** As instâncias do EC2 com o par de chave de tag e de valores de tag que é separado com uma barra vertical (|) e que é especificado em **Filter Value** são monitoradas. Por exemplo, para monitorar todas as instâncias do EC2 que tenham a chave de tag *Stack* e o valor de tag *Production*, especifique `Stack|Production` em **Filter Value**. **monitoring-tag** As instâncias do EC2 que possuem pelo menos uma tag são monitoradas. **Filter Value** é ignorado.	**FILTER_CONDITION.subnode_name** Valores válidos, **nenhum** nenhum **tagName** tagName **tagName|tagValue** tagName|tagValue **monitoring-tag** monitoring-tag
Valor de filtro	O valor da tag pelo qual as instâncias do EC2 são filtradas quando o `tagName` ou `tagName|tagValue` é selecionado para **Filtering Condition**.	**FILTER_VALUE.subnode_name**

Configurando o monitoramento do Balanceador de Carga Elástico AWS

O Agente Amazon ELB fornece um ponto central de monitoramento para o funcionamento, disponibilidade e desempenho de seus Balanceadores de Carga Elásticos AWS. O agente exibe um conjunto abrangente de métricas para cada aplicativo de tipo de balanceador de carga, de rede e clássico - para ajudá-lo a tomar decisões informadas sobre o ambiente do Balanceador de Carga Elástico AWS.

Antes de Iniciar

- Leia o tópico "Configurando o monitoramento do Balanceador de Carga Elástico AWS" na página 195 inteiro para determinar o que é necessário para concluir a configuração.
- Estas instruções são para a liberação mais atual do agente, exceto conforme indicado.
- Certifique-se de que os requisitos do sistema para o Agente Amazon ELB sejam atendidos em seu ambiente. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Agente Amazon ELB.
- Assegure-se de que as seguintes informações estejam disponíveis:
  - As credenciais de segurança de AWS (ID da chave de acesso e Chave de acesso secreta) com permissão para acessar cada região AWS com Balanceadores de Carga Elásticos.

Sobre Esta Tarefa

O Agente Amazon ELB é um agente de múltiplas instâncias e também um agente do subnó. Os subnós são criados automaticamente para cada tipo de Balanceador de Carga Elástico que está disponível em seu ambiente AWS.

Procedimento

1. Configure o agente nos sistemas Windows com a janela **IBM Performance Management** ou o arquivo de resposta silencioso.
   - "Configurando o agente nos sistemas Windows" na página 196.
   - "Configurando o agente usando o arquivo silencioso de resposta" na página 198.
2. Configure o agente nos sistemas Linux com o script que solicita respostas ou com o arquivo de resposta silencioso.
   - "Configurando o agente respondendo aos prompts" na página 197.
   - "Configurando o agente usando o arquivo silencioso de resposta" na página 198.

O que Fazer Depois

No Console do Cloud APM, acesse seu Application Performance Dashboard para visualizar os dados que foram coletados. Para obter informações adicionais sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Se você não conseguir visualizar os dados nos painéis do agente, primeiro verifique os logs de conexão do servidor e, em seguida, os logs do provedor de dados. Os caminhos padrão para esses logs são listados aqui:

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Para obter ajuda com a resolução de problemas, consulte o Fórum do Cloud Application Performance Management.

Configurando o agente nos sistemas Windows

É possível configurar o Agente Amazon ELB em sistemas operacionais Windows usando a janela IBM Cloud Application Performance Management. Após fazer a atualização dos valores de configuração, deve-se iniciar o agente para salvar os valores atualizados.

Procedimento

1. Clique em **Iniciar** > **Todos os programas** > **Agentes do IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito no modelo **Monitoring Agent for AWS Elastic Load Balancer** e, em seguida, clique em **Configurar agente**.

   Lembre-se: Depois de configurar uma instância de agente pela primeira vez, a opção **Configurar agente** é desativada. Para configurar a instância de agente novamente, clique nela com o botão direito e clique em **Reconfigurar**.
3. Insira um nome de instância exclusivo e, em seguida, clique em **OK**. Use apenas letras latinas, numerais arábicos e o caractere de hífen ou de menos no nome da instância. Exemplo, `elb-inst3`. Para obter mais informações, consulte *instancename* em "Formato comum do MSN para agentes de multi-instâncias" na página 165.

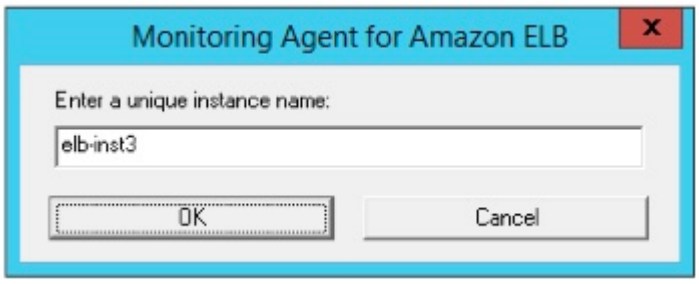


Figura 7. A janela para inserir um nome da instância de agente exclusivo.

4. Insira as **Credenciais de assinatura do Amazon ELB**, em seguida, clique em **Avançar**.

   Consulte a seção "Parâmetros de Configuração para o Agente Amazon ELB" na página 199 para obter uma explicação de cada um dos parâmetros de configuração.

   Importante: Windows Se seu **`Secret Key/Password`** contiver um sinal de igual (=), você deve reinseri-lo sempre que reconfigurar o agente.

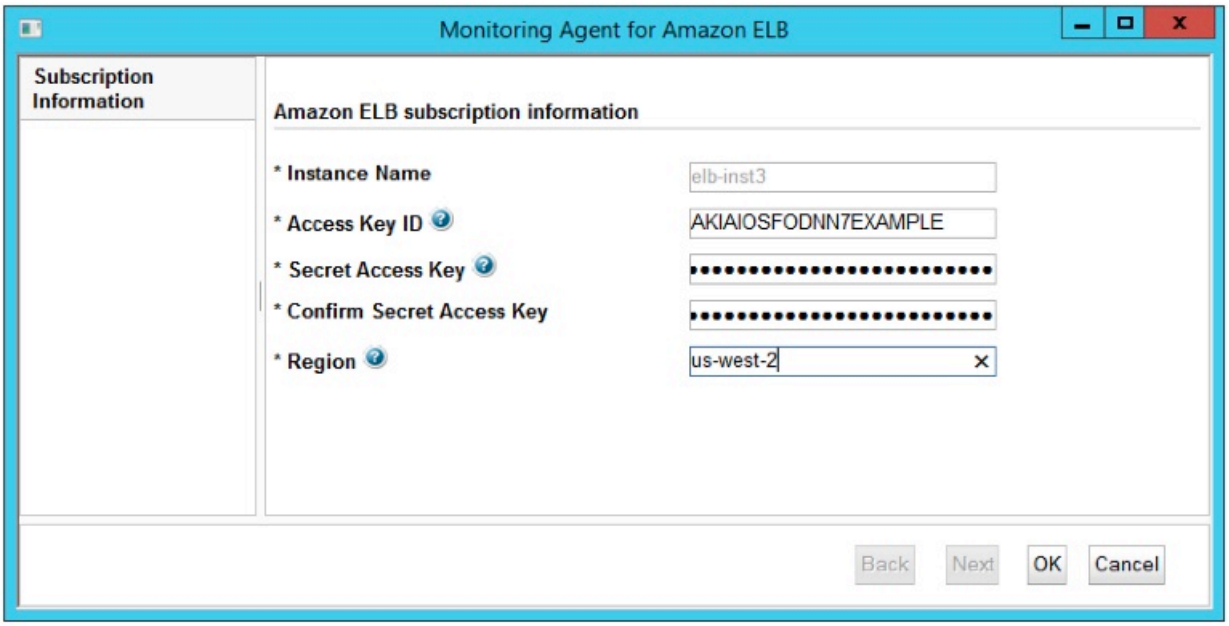


Figura 8. A janela de credenciais de assinatura do Amazon ELB.

5. Clique em **OK** para concluir a configuração.
6. Na janela IBM Cloud Application Performance Management, clique com o botão direito na instância configurada e, em seguida, clique em **Iniciar**.

Configurando o agente respondendo aos prompts

Após a instalação do Agente Amazon ELB, deve-se configurá-lo antes de iniciar o agente. Se o Agente Amazon ELB estiver instalado em um computador Linux local, será possível seguir essas instruções para configurá-lo interativamente por meio de prompts da linha de comandos.

Sobre Esta Tarefa

Lembre-se: Se estiver reconfigurando uma instância do agente configurada, o valor que é definido na última configuração será exibido para cada configuração. Se desejar limpar um valor existente, pressione a tecla Espaço quando a configuração for exibida.

Procedimento

Siga essas etapas para configurar o Agente Amazon ELB executando um script e respondendo aos prompts.

1. Execute o seguinte comando:

   ```
   install_dir/bin/amazon_elb-agent.sh config instance-name
   ```

   Em que *install_dir* é o caminho onde o agente está instalado e *instance-name* é o nome que você deseja dar à instância de agente. Use apenas letras latinas, numerais arábicos e o caractere hífen ou sinal de menos no *instance-name*. Para obter mais informações, consulte *instancename* em “Formato comum do MSN para agentes de multi-instâncias” na página 165.

   Exemplo

   ```
   /opt/ibm/apm/agent/bin/amazon_elb-agent.sh config elb-inst3
   ```

2. Responda aos prompts para configurar valores de configuração para o agente.

   Consulte “Parâmetros de Configuração para o Agente Amazon ELB” na página 199 para obter uma explicação de cada um dos parâmetros de configuração.

3. Execute o comando a seguir para iniciar o agente:

   ```
   install_dir/bin/amazon_elb-agent.sh start instance-name
   ```

   Em que *install_dir* é o caminho onde o agente está instalado e *instance-name* é o nome da instância de agente.

   Exemplo

   ```
   /opt/ibm/apm/agent/bin/amazon_elb-agent.sh start elb-inst3
   ```

Exemplo

Criando uma instância de agente chamada `elb-inst3`.

```
# ./amazon_elb-agent.sh config elb-inst3
Configurando o Monitoring Agent for Amazon ELB

Editar configurações de 'Monitoring Agent for Amazon ELB'? [1=Sim,2=Não](o padrão é: 1): 1

Informações de assinatura:
Informações de assinatura do Amazon ELB

O ID de acesso que é usado para autenticação com a Região Amazon especificada.
Por exemplo, 'AKIAxxxxxxxxxxxxxx'.
O ID da chave de acesso (o padrão é: ): AKIAIOSFODNN7EXAMPLE

A chave de acesso secreta que é usada para autenticação com a Região Amazon
```

```
especificada. Por exemplo, 'kK7txxxxxxxxxxxxxxxxxxxxxxxx'.
Insira a chave de acesso secreta (o padrão é: ): hidden

Digitar novamente: Chave de acesso secreta (o padrão é: ): hidden

A região Amazon onde os balanceadores de carga estão localizados. Por exemplo, 'us-west-2'.
Região (o padrão é: ): us-west-2

Configuração concluída com sucesso.
O início automático na inicialização do sistema foi configurada.
A parada automática no encerramento do sistema foi configurada.
```

Configurando o agente usando o arquivo silencioso de resposta

O arquivo de resposta silencioso contém os parâmetros de configuração do agente. É possível editar o arquivo de resposta silencioso para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

O arquivo silencioso de resposta contém os parâmetros de configuração do agente com valores padrão que são definidos para alguns parâmetros. É possível editar o arquivo de resposta silencioso para especificar os valores diferentes para os parâmetros de configuração.

Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

Siga essas etapas para configurar o Agente Amazon ELB no modo silencioso.

1. Abra o arquivo `amazon_elb_silent_config.txt` em um dos seguintes caminhos em um editor de texto.
   - Linux *install_dir*`/samples/amazon_elb_silent_config.txt`

     Exemplo, `/opt/ibm/apm/agent/samples/amazon_elb_silent_config.txt`
   - Windows *install_dir*`\samples\amazon_elb_silent_config.txt`

     Exemplo, `C:\IBM\APM\samples\amazon_elb_silent_config.txt`

   Em que *install_dir* é o caminho onde o agente está instalado.
2. No arquivo `amazon_elb_silent_config.txt`, especifique valores para todos os parâmetros obrigatórios e modifique os valores padrão de outros parâmetros, conforme necessário.

   Consulte a seção "Parâmetros de Configuração para o Agente Amazon ELB" na página 199 para obter uma explicação de cada um dos parâmetros de configuração.
3. Salve e feche o arquivo `amazon_elb_silent_config.txt` e execute o seguinte comando:
   - Linux *install_dir*`/bin/amazon_elb-agent.sh config` **instance-name** *install_dir*`/samples/amazon_elb_silent_config.txt`

     Exemplo, **/opt/ibm/apm/agent/bin/amazon_elb-agent.sh config elb-inst3 /opt/ibm/apm/agent/samples/amazon_elb_silent_config.txt**
   - Windows *install_dir*`\bin\amazon_elb-agent.bat config` **instance-name** *install_dir*`\samples\amazon_elb_silent_config.txt`

     Exemplo, **C:\IBM\APM\bin\amazon_elb-agent.bat config elb-inst3 C:\IBM\APM\samples\amazon_elb_silent_config.txt**

   Em que *install_dir* é o caminho onde o agente está instalado e *instance-name* é o nome que você deseja dar à instância de agente. Use apenas letras latinas, numerais arábicos e o caractere hífen ou sinal de menos no *instance-name*. Para obter mais informações, consulte *instancename* em "Formato comum do MSN para agentes de multi-instâncias" na página 165.

Importante: Assegure que você inclua o caminho absoluto no arquivo de resposta silencioso. Caso contrário, os dados do agente não serão mostrados nos painéis.

4. Execute o comando a seguir para iniciar o agente:
   - Linux *install_dir*/bin/amazon_elb-agent.sh start **instance-name**

     Exemplo, **/opt/ibm/apm/agent/bin/amazon_elb-agent.sh start elb-inst3**
   - Windows *install_dir*\bin\amazon_elb-agent.bat start **instance-name**

     Exemplo, **C:\IBM\APM\bin\amazon_elb-agent.bat start elb-inst3**

   Em que *install_dir* é o caminho onde o agente está instalado e *instance-name* é o nome da instância de agente.

Exemplo

amazon_elb_silent_config.txt editado.

```
#
# This is a sample configuration response file for agent Amazon ELB.
#
# It contains an entry for every configuration property.
# Entries for optional properties that have no default value are included
# in comments.
# Ensure that all uncommented properties have a value before configuring
# the agent.
#

# Access Key ID: The access ID that is used to authenticate with the
# specified Amazon Region. Por exemplo, 'AKIAxxxxxxxxxxxxxx'.
KAL_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

# Secret Access Key: The secret access key that is used to authenticate with
# the specified Amazon Region. Por exemplo, 'kK7txxxxxxxxxxxxxxxxxxxxxxxx'.
KAL_SECRET_ACCESS_KEY_PASSWORD=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

# Region: The Amazon region where the load balancers are located. For
# example, 'us-west-2'.
KAL_REGION=us-west-2
```

Parâmetros de Configuração para o Agente Amazon ELB

Os parâmetros de configuração para o Agente Amazon ELB são exibidos em uma tabela.

1. Tabela 15 na página 199 - Credenciais que são necessárias para acesso à Assinatura do Amazon que contém os Balanceadores de Carga Elásticos AWS a serem monitorados.

Tabela 15. Informações de assinatura

Nome de parâmetro	Descrição	Nome do parâmetro do arquivo de configuração silenciosa
Acessar ID da Chave	O ID de acesso que é usado para autenticação com a Região Amazon especificada. Por exemplo, 'AKIAxxxxxxxxxxxxxx'.	**KAL_ACCESS_KEY_ID**
Tecla de Acesso Secreta	A chave de acesso secreta que é usada para autenticação com a Região Amazon especificada. Por exemplo, 'kK7txxxxxxxxxxxxxxxxxxxxxxxx'.	**KAL_SECRET_ACCESS_KEY_PASSWORD**
Região	A região Amazon onde os balanceadores de carga estão localizados. Por exemplo, 'us-west-2'.	**KAL_REGION**

Configurando o monitoramento do Azure Compute

O Agente Azure Compute fornece um ponto central para monitoramento do funcionamento, disponibilidade e desempenho de suas instâncias do Azure Compute. O agente exibe um conjunto abrangente de métricas para ajudá-lo a tomar decisões informadas sobre o ambiente do Azure Compute. Essas métricas incluem o uso da CPU, uso da rede e desempenho do disco.

Antes de Iniciar

- Leia o tópico "Configurando o monitoramento do Azure Compute" na página 200 inteiro para determinar o que é necessário para concluir a configuração.
- Estas instruções são para a liberação mais atual do agente, exceto conforme indicado.
- Certifique-se de que os requisitos do sistema para o Agente Azure Compute sejam atendidos em seu ambiente. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Agente Azure Compute.
- Assegure-se de que as seguintes informações estejam disponíveis:
  - As Credenciais de assinatura Azure com permissão para acessar as instâncias do Azure Compute para monitorar. Consulte o "Informações de configuração do Azure Compute" na página 201 para obter mais detalhes.

Sobre Esta Tarefa

O Agente Azure Compute é um agente de múltiplas instâncias e também um agente do subnó. Cada subnó do Agente Azure Compute monitora um agrupamento de máquinas virtuais Azure Compute de acordo com um filtro definido. É possível criar uma instância de agente com vários subnós – um para cada agrupamento de máquinas virtuais, ou é possível criar uma instância de agente para cada agrupamento de máquinas virtuais com um subnó para esse agrupamento. Ou é possível criar uma combinação de cada tipo de configuração. Depois de configurar instâncias de agente, você deve iniciar cada instância de agente manualmente. É sugerido ter um máximo de 50 recursos por agrupamento de máquinas virtuais Azure Compute. Cada nome do subnó do agente Azure Compute deve ser exclusivo em seu ambiente.

Procedimento

1. Configure o agente nos sistemas Windows com a janela **IBM Performance Management** ou o arquivo de resposta silencioso.
   - "Configurando o agente nos sistemas Windows" na página 201.
   - "Configurando o agente usando o arquivo silencioso de resposta" na página 206.
2. Configure o agente nos sistemas Linux com o script que solicita respostas ou com o arquivo de resposta silencioso.
   - "Configurando o agente respondendo aos prompts" na página 204.
   - "Configurando o agente usando o arquivo silencioso de resposta" na página 206.

O que Fazer Depois

No Console do Cloud APM, acesse seu Application Performance Dashboard para visualizar os dados que foram coletados. Para obter informações adicionais sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Se você não conseguir visualizar os dados nos painéis do agente, primeiro verifique os logs de conexão do servidor e, em seguida, os logs do provedor de dados. Os caminhos padrão para esses logs são listados aqui:

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Para obter ajuda com a resolução de problemas, consulte o Fórum do Cloud Application Performance Management.

Informações de configuração do Azure Compute

O Agente Azure Compute requer a configuração adicional no ambiente do Azure Compute.

Sobre Esta Tarefa

Para executar essas etapas, você deve efetuar login no console do Microsoft Azure.

Procedimento

1. ID da assinatura
   - Na área de janela esquerda, selecione "Assinaturas" e escolha a assinatura que você deseja usar para este agente.
   - Selecione "Visão Geral", em seguida, copie o ID da Assinatura. Isso será usado como um dos parâmetros de configuração do Agente.
2. ID do Locatário
   - Navegue para "Azure Active Directory".
   - Selecione "Propriedades", em seguida, copie o ID do Locatário.
3. Registrar um Aplicativo
   - Vá para "Todos os Serviços" e procure "Registros de Aplicativos".
   - Clique em "Novo Registro de Aplicativo".
   - Preencha um nome, selecione Tipo de Aplicativo "Web App/API" e uma URL de conexão (essa URL não será usada, portanto, escolha qualquer coisa que você desejar).
   - Clique em "Criar"
   - Copie o ID do Aplicativo - Ele será utilizado no campo "ID do Cliente" do Agente.
4. Crie a Chave do Aplicativo
   - Clique no aplicativo que você acabou de criar e, em seguida, vá para "Configurações" seguido por "Chaves".
   - Insira uma descrição (por exemplo, "Chave IBM") e a duração (por exemplo, "Nunca Expira"); em seguida, clique em "Salvar".
   - Copie a chave secreta e armazene-a em algum lugar seguro - você verá essa chave apenas uma vez e precisará gerar uma nova se perdê-la.
5. Conceda Permissões ao Aplicativo
   - Vá para "Assinaturas" e selecione a assinatura a ser monitorada.
   - Acesse "Controle de Acesso (IAM)" e clique em "Incluir".
   - Selecione a função "Leitor" ou superior para monitoramento.
   - Em "Selecionar", localize o aplicativo que você acabou de registrar e selecione-o; em seguida, clique em "Salvar".

Configurando o agente nos sistemas Windows

É possível configurar o Agente Azure Compute em sistemas operacionais Windows usando a janela IBM Cloud Application Performance Management. Após fazer a atualização dos valores de configuração, deve-se iniciar o agente para salvar os valores atualizados.

Procedimento

1. Clique em **Iniciar** > **Todos os programas** > **Agentes do IBM Monitoring** > **IBM Cloud Application Performance Management**.

2. Na janela **IBM Performance Management**, clique com o botão direito no modelo **Monitoring Agent for Azure Compute** e, em seguida, clique em **Configurar agente**.

   Lembre-se: Depois de configurar uma instância de agente pela primeira vez, a opção **Configurar agente** é desativada. Para configurar a instância de agente novamente, clique nela com o botão direito e clique em **Reconfigurar**.
3. Insira um nome de instância exclusivo e, em seguida, clique em **OK**. Use apenas letras latinas, numerais arábicos e o caractere de hífen ou de menos no nome da instância. Exemplo, `azc-inst3`. Para obter mais informações, consulte *instancename* em "Formato comum do MSN para agentes de multi-instâncias" na página 165.

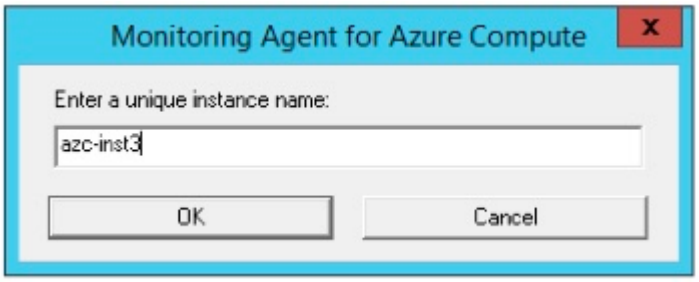


Figura 9. A janela para inserir um nome da instância de agente exclusivo.

4. Insira as **Credenciais de Assinatura Azure**, em seguida, clique em **Avançar**.

   Consulte Tabela 16 na página 208 para obter uma explicação de cada um dos parâmetros de configuração.

   Importante: Windows Se seu **`Secret Key/Password`** contiver um sinal de igual (=), você deve reinseri-lo sempre que reconfigurar o agente.

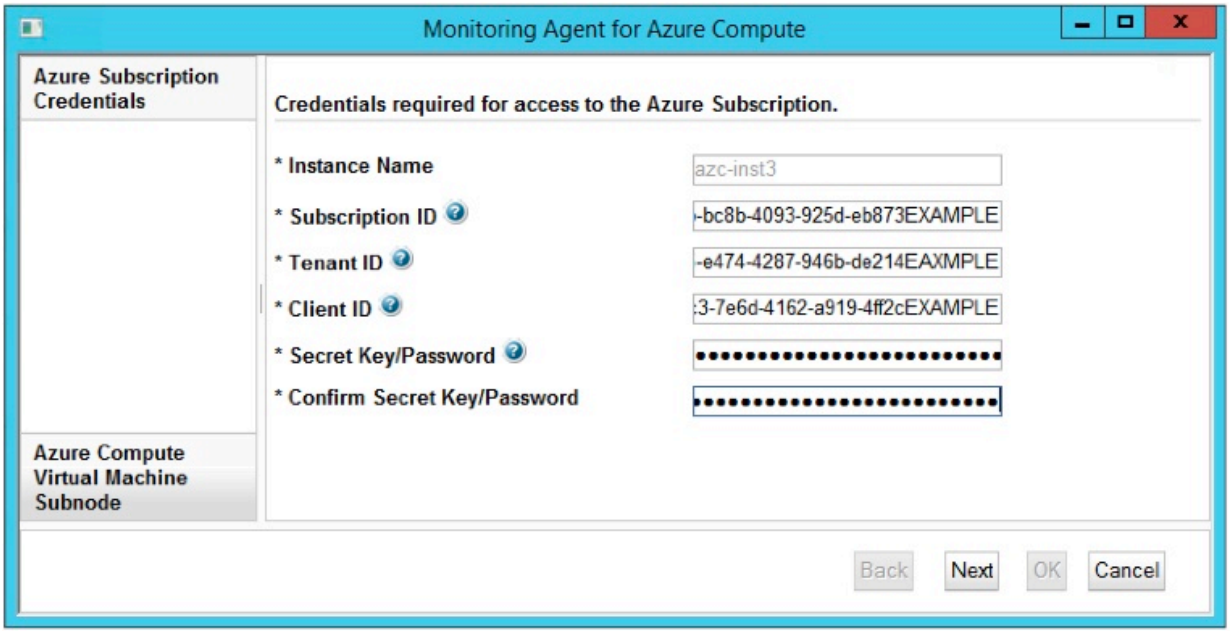


Figura 10. A janela Credenciais de assinatura Azure.

5. Insira as configurações do modelo **Subnó de máquina virtual Azure Compute**.

   Consulte Tabela 17 na página 209 para obter uma explicação de cada um dos parâmetros de configuração.

   Nota: Esta seção não é a configuração da instância do Subnó de máquina virtual Azure Compute. É uma seção de modelo para configurar o que é usado como os valores padrão ao incluir as configurações reais da instância do subnó de máquina virtual Azure Compute na etapa 6.

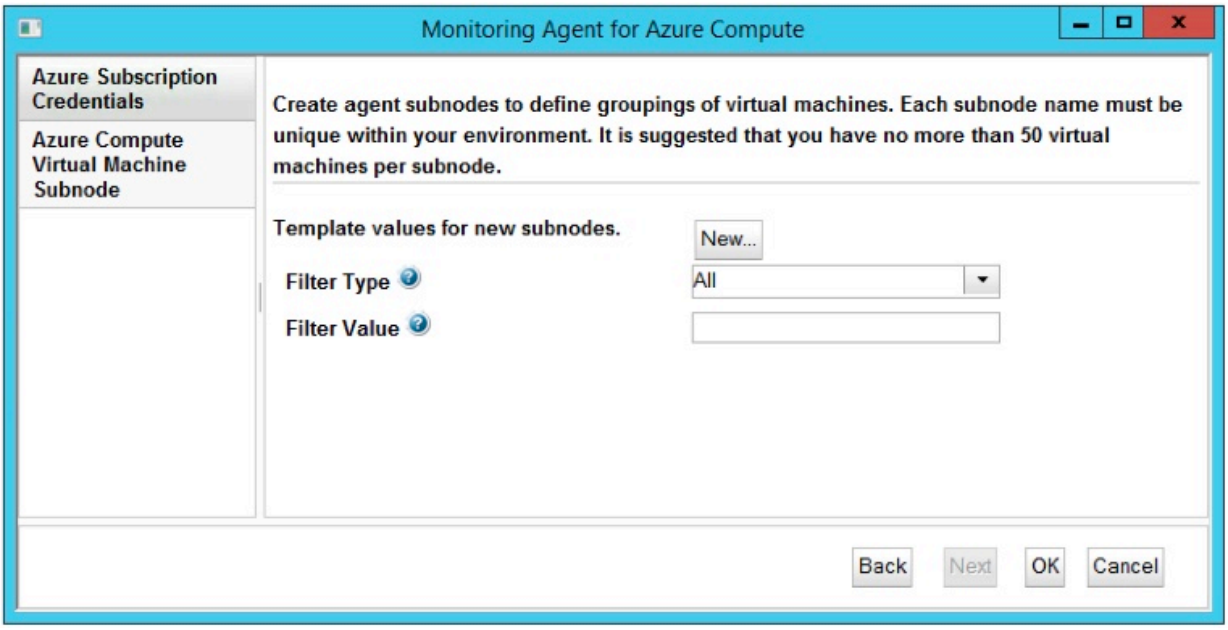


Figura 11. A janela para especificar configurações de modelo do subnó de máquina virtual Azure Compute.

6. Pressione **Novo** e insira configurações da instância do **Subnó de máquina virtual Azure Compute** , em seguida, clique em **Avançar**.

   Consulte Tabela 17 na página 209 para obter uma explicação de cada um dos parâmetros de configuração.

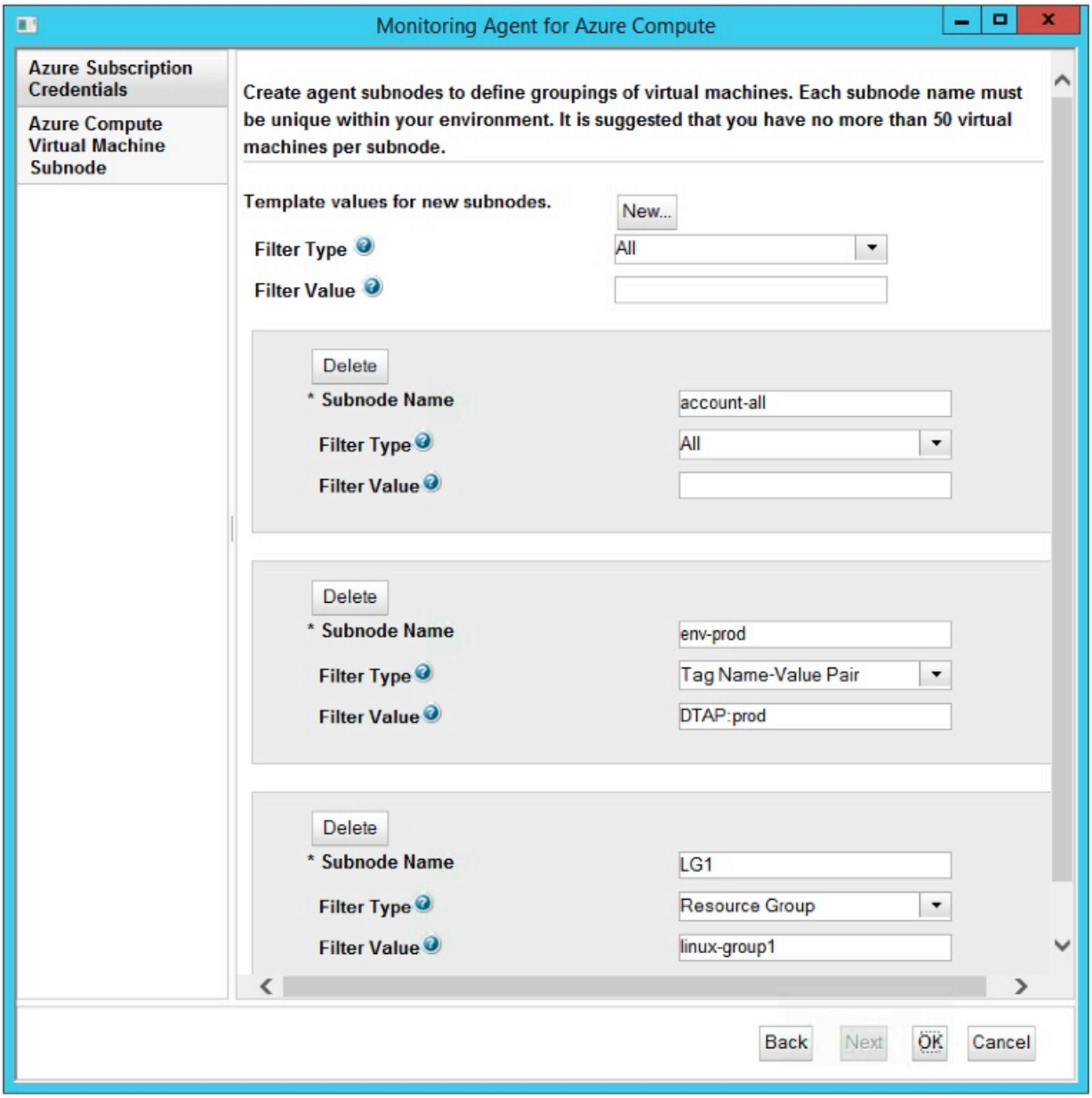


Figura 12. A janela para especificar configurações da instância do subnó de máquina virtual Azure Compute.

7. Clique em **OK** para concluir a configuração.
8. Na janela IBM Cloud Application Performance Management, clique com o botão direito na instância configurada e, em seguida, clique em **Iniciar**.

Configurando o agente respondendo aos prompts

Após a instalação do Agente Azure Compute, deve-se configurá-lo antes de iniciar o agente. Se o Agente Azure Compute estiver instalado em um computador Linux local, será possível seguir essas instruções para configurá-lo interativamente por meio de prompts da linha de comandos.

Sobre Esta Tarefa

Lembre-se: Se estiver reconfigurando uma instância do agente configurada, o valor que é definido na última configuração será exibido para cada configuração. Se desejar limpar um valor existente, pressione a tecla Espaço quando a configuração for exibida.

Procedimento

Siga essas etapas para configurar o Agente Azure Compute executando um script e respondendo aos prompts.

1. Execute o seguinte comando:

   ```
   install_dir/bin/azure_compute-agent.sh config instance-name
   ```

   Em que *install_dir* é o caminho onde o agente está instalado e *instance-name* é o nome que você deseja dar à instância de agente. Use apenas letras latinas, numerais arábicos e o caractere hífen ou sinal de menos no *instance-name*. Para obter mais informações, consulte *instancename* em "Formato comum do MSN para agentes de multi-instâncias" na página 165.

   Exemplo

   ```
   /opt/ibm/apm/agent/bin/azure_compute-agent.sh config azc-inst3
   ```

2. Responda aos prompts para configurar valores de configuração para o agente.

   Consulte "Parâmetros de Configuração para o Agente Azure Compute" na página 208 para obter uma explicação de cada um dos parâmetros de configuração.

   Lembre-se: Ao configurar uma instância de agente pela primeira vez, você deve incluir pelo menos um subnó quando solicitado a **Editar configurações do 'Subnó da máquina virtual do Azure Compute'**.

3. Execute o comando a seguir para iniciar o agente:

   ```
   install_dir/bin/azure_compute-agent.sh start instance-name
   ```

   Em que *install_dir* é o caminho onde o agente está instalado e *instance-name* é o nome da instância de agente.

   Exemplo

   ```
   /opt/ibm/apm/agent/bin/azure_compute-agent.sh start azc-inst3
   ```

Exemplo

Criando uma instância de agente chamada `azc-inst3` e que tem uma instância do subnó chamada `azc1`.

```
# ./azure_compute-agent.sh config azc-inst3
Configurando o Monitoring Agent for Azure Compute

Editar configurações do 'Monitoring Agent for Azure Compute'? [1=Sim,2=Não](o padrão é: 1): 1

Credenciais de Assinatura do Azure:
As credenciais necessárias para acesso à Assinatura do Azure.

O ID designado pelo Azure para a Assinatura que é monitorada.
ID da assinatura (o padrão é: ): 09x73b6b-bcxb-40x3-92xd-ebx7-EXAMPLE

O ID do locatário que é designado pelo Azure. Usado para efetuar login na API de serviço do
Azure.
ID do locatário (o padrão é: ): 75x2e745-e4x4-42x7-94xb-dex1-EXAMPLE

O ID do cliente que é designado pelo Azure para identificar este agente como um aplicativo
externo que monitora os serviços de cálculo do Azure.
ID do cliente (o padrão é: ): 79x2e6c3-7exd-41x2-a9x9-4fx2-EXAMPLE

A chave secreta de acesso ou senha que é criada pelo Azure para o aplicativo cliente.
Inserir Chave secreta/Senha (o padrão é:): oculto

Digitar novamente : Chave secreta/Senha (o padrão é:): oculto

Subnó de máquina virtual Azure Compute:

Crie subnós de agente para definir agrupamentos de máquinas virtuais. Cada nome de subnó deve
ser exclusivo em seu ambiente. Não são recomendadas mais de 50 máquinas virtuais por subnó.

Não há configurações de 'Subnó de máquina virtual Azure Compute' disponíveis.
```

```
Editar configurações de 'Subnó de máquina virtual Azure Compute, [1=Add, 2=Edit, 3=Del,
4=Next, 5=Exit] (default is: 5): 1
Nome do subnó (o padrão é:): azc1
O tipo de filtro a ser aplicado.
Tipo de filtro [ 1=Todos, 2=Par nome-valor de tag, 3=Grupo de recursos] (o padrão é: 1): 2
O valor do filtro correspondente ao Tipo de filtro selecionado. Este valor pode ser um
Grupo de recursos ou Par nome-valor de tag, por exemplo, Environment\:Production.
Pode aparecer uma barra invertida no exemplo, não insira uma barra invertida no valor
fornecido.
Valor de filtro (o padrão e:): Environment:Production



Configurações do subnó de máquina virtual Azure Compute: Nome do subnó=azc1
Editar configurações de 'Subnó de máquina virtual Azure Compute, [1=Add, 2=Edit, 3=Del,
4=Next, 5=Exit] (o padrão é: 5): 5
Configuração concluída com sucesso.
O início automático na inicialização do sistema foi configurada.
A parada automática no encerramento do sistema foi configurada.
Você tem um novo e-mail em /var/spool/mail/root
```

Configurando o agente usando o arquivo silencioso de resposta

O arquivo de resposta silencioso contém os parâmetros de configuração do agente. É possível editar o arquivo de resposta silencioso para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

O arquivo silencioso de resposta contém os parâmetros de configuração do agente com valores padrão que são definidos para alguns parâmetros. É possível editar o arquivo de resposta silencioso para especificar os valores diferentes para os parâmetros de configuração.

Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

Siga essas etapas para configurar o Agente Azure Compute no modo silencioso.

1. Abra o arquivo `azure_compute_silent_config.txt` em um dos seguintes caminhos em um editor de texto.
   - Linux *install_dir*`/samples/azure_compute_silent_config.txt`

     Exemplo, `/opt/ibm/apm/agent/samples/azure_compute_silent_config.txt`
   - Windows *install_dir*`\samples\azure_compute_silent_config.txt`

     Exemplo, `C:\IBM\APM\samples\azure_compute_silent_config.txt`

   Em que *install_dir* é o caminho onde o agente está instalado.
2. No arquivo `azure_compute_silent_config.txt`, especifique valores para todos os parâmetros obrigatórios e modifique os valores padrão dos outros parâmetros, conforme necessário.

   Consulte “Parâmetros de Configuração para o Agente Azure Compute” na página 208 para obter uma explicação de cada um dos parâmetros de configuração.

   Importante: Você deve ativar e especificar os parâmetros de Tipo de filtro e Valor de filtro para pelo menos um nome de subnó.
3. Salve e feche o arquivo `azure_compute_silent_config.txt` e execute o seguinte comando:
   - Linux *install_dir*`/bin/azure_compute-agent.sh config` **instance-name** *install_dir*`/samples/azure_compute_silent_config.txt`

     Exemplo, **/opt/ibm/apm/agent/bin/azure_compute-agent.sh config azc-inst3 /opt/ibm/apm/agent/samples/azure_compute_silent_config.txt**

- Windows *install_dir*\bin\azure_compute-agent.bat config **instance-name** *install_dir*\samples\azure_compute_silent_config.txt

  Exemplo, **C:\IBM\APM\bin\azure_compute-agent.bat config azc-inst3 C:\IBM\APM\samples\azure_compute_silent_config.txt**

Em que *install_dir* é o caminho onde o agente está instalado e *instance-name* é o nome que você deseja dar à instância de agente. Use apenas letras latinas, numerais arábicos e o caractere hífen ou sinal de menos no *instance-name*. Para obter mais informações, consulte *instancename* em "Formato comum do MSN para agentes de multi-instâncias" na página 165.

Importante: Assegure que você inclua o caminho absoluto no arquivo de resposta silencioso. Caso contrário, os dados do agente não serão mostrados nos painéis.

4. Execute o comando a seguir para iniciar o agente:
   - Linux *install_dir*/bin/azure_compute-agent.sh start **instance-name**

     Exemplo, **/opt/ibm/apm/agent/bin/azure_compute-agent.sh start azc-inst3**
   - Windows *install_dir*\bin\azure_compute-agent.bat start **instance-name**

     Exemplo, **C:\IBM\APM\bin\azure_compute-agent.bat start azc-inst3**

   Em que *install_dir* é o caminho onde o agente está instalado e *instance-name* é o nome da instância de agente.

Exemplo

Edite azure_compute_silent_config.txt com três subnós chamados account-all, env-prod e LG1.

```
#
# This is a sample configuration response file for agent Azure Compute.
#
# It contains an entry for every configuration property.
# Entries for optional properties that have no default value are included in
# comments.
# Entries for subnode AVM are given a sample subnode instance name of avm1.
# Ensure that all uncommented properties have a value before configuring the
# agent.
#

# Subscription ID: The ID assigned by Azure for the Subscription that is
# monitored.
KAK_SUBSCRIPTION_ID=09x73b6b-bcxb-40x3-92xd-ebx7-EXAMPLE
# Tenant ID: The tenant ID that is assigned by Azure. Used to log in to the
# Azure service API.
KAK_TENANT_ID=75x2e745-e4x4-42x7-94xb-dex1-EXAMPLE
# Client ID: The client ID that is assigned by Azure to identify this agent
# as an external
# application that monitors the Azure compute services.
KAK_CLIENT_ID=79x2e6c3-7exd-41x2-a9x9-4fx2-EXAMPLE
# Secret Key/Password: The secret access key or password that is created by
# Azure for the client application.
KAK_SECRET_PASSWORD=hZxWPq/IOxlnvg/wdxLwTf2Fs3x2sWQV/sCE-EXAMPLE

# Filter Type: The type of filter to be applied.
# Valid values: ALL (All), TAG_NAME_VALUE (Tag Name-Value Pair),
# RESOURCE_GROUP (Resource Group)
#KAK_FILTER_TYPE.avm1=ALL
# Filter Value: The filter value corresponding to the selected Filter Type.
# This value can be a Resource Group or Tag Name-Value Pair, for example
# Environment:Production. A backslash might appear in the example, do not
# enter a backslash in the value you provide.
#KAK_FILTER_VALUE.avm1=

# Filter Type: The type of filter to be applied.
# Valid values: ALL (All), TAG_NAME_VALUE (Tag Name-Value Pair),
# RESOURCE_GROUP (Resource Group)
KAK_FILTER_TYPE.account-all=ALL
# Filter Value: The filter value corresponding to the selected Filter Type.
# This value can be a Resource Group or Tag Name-Value Pair, for example
# Environment:Production. A backslash might appear in the example, do not
# enter a backslash in the value you provide.
```

```
KAK_FILTER_VALUE.account-all=

# Filter Type: The type of filter to be applied.
# Valid values: ALL (All), TAG_NAME_VALUE (Tag Name-Value Pair),
# RESOURCE_GROUP (Resource Group)
KAK_FILTER_TYPE.env-prod=TAG_NAME_VALUE
# Filter Value: The filter value corresponding to the selected Filter Type.
# This value can be a Resource Group or Tag Name-Value Pair, for example
# Environment:Production. A backslash might appear in the example, do not
# enter a backslash in the value you provide.
KAK_FILTER_VALUE.env-prod=DTAP:prod

# Filter Type: The type of filter to be applied.
# Valid values: ALL (All), TAG_NAME_VALUE (Tag Name-Value Pair),
# RESOURCE_GROUP (Resource Group)
KAK_FILTER_TYPE.LG1=RESOURCE_GROUP
# Filter Value: The filter value corresponding to the selected Filter Type.
# This value can be a Resource Group or Tag Name-Value Pair, for example
# Environment:Production. A backslash might appear in the example, do not
# enter a backslash in the value you provide.
KAK_FILTER_VALUE.LG1=linux-group1
```

Parâmetros de Configuração para o Agente Azure Compute

Os parâmetros de configuração para o Agente Azure Compute são exibidos em tabelas que os agrupam de acordo com as seções.

1. Tabela 16 na página 208 - Credenciais que são necessárias para acesso à Assinatura do Azure que contém os recursos do Azure Compute para monitorar.
2. Tabela 17 na página 209 - Crie subnós do agente para definir agrupamentos de máquinas virtuais. Cada nome de subnó deve ser exclusivo em seu ambiente. Não são recomendadas mais de 50 máquinas virtuais por subnó.

Tabela 16. Credenciais de Assinatura do Azure

Nome de parâmetro	Descrição	Nome do parâmetro do arquivo de configuração silenciosa
ID da assinatura	O ID designado pelo Azure para a Assinatura que é monitorada.	**KAK_SUBSCRIPTION_ID**
ID do Locatário	O ID do locatário que é designado pelo Azure. Usado para efetuar login na API de serviço do Azure.	**KAK_TENANT_ID**
ID do cliente	O ID do cliente que é designado pelo Azure para identificar este agente como um aplicativo externo que monitora os serviços de cálculo do Azure.	**KAK_CLIENT_ID**
Chave secreta/ Senha	A chave secreta de acesso ou senha que é criada pelo Azure para o aplicativo cliente. **Importante:** Windows Se seu **Secret Key/Password** contiver um sinal de igual (=), você deve reinseri-lo sempre que reconfigurar o agente.	**KAK_SECRET_PASSWORD**

Tabela 17. Subnó de Máquina Virtual do Azure Compute

Nome de parâmetro	**Descrição**	**Nome do parâmetro do arquivo de configuração silenciosa**
Nome do Subnó	Nome do subnó do Azure Compute para coleta de dados. Exemplo, *azc1*. O nome do subnó deve ser exclusivo em seu ambiente. Este alias faz parte do nome do sistema gerenciado (MSN) e é usado para identificar visualmente o ambiente monitorado no Console do Cloud APM. **Nota:** Este alias pode ser qualquer coisa escolhida para representar a instância do subnó do Azure Compute com as seguintes restrições. Letras do alfabeto latino (a-z, A-Z), numerais arábicos (0-9), o caractere de hífen ou de menos (-) e o caractere sublinhado (_) podem ser usados para criar nomes de instância do subnó do agente. O comprimento máximo de um nome de subnó do Azure Compute é de 25 caracteres.	Cada um dos seguintes parâmetros deve usar um ponto (.) seguido por um **Subnode Name** do agente como um sufixo. O **Subnode Name** deve ser o mesmo para cada parâmetro de subnó. As novas instâncias do subnó do agente devem usar um **Subnode Name** exclusivo para seu conjunto de parâmetros. Por exemplo, uma instância do subnó do agente pode usar *.azc1* e outra instância do subnó do agente pode usar *.azc2* no lugar de *.subnode_name* nos nomes de parâmetros a seguir.
Tipo de Filtro	O tipo de filtro a ser aplicado.	**KAK_FILTER_TYPE.subnode_name** Valores válidos, **TODOS** Tudo **TAG_NAME_VALUE** Par nome-valor de Tag **RESOURCE_GROUP** Grupo de Recursos

Tabela 17. Subnó de Máquina Virtual do Azure Compute (continuação)		
Nome de parâmetro	**Descrição**	**Nome do parâmetro do arquivo de configuração silenciosa**
Valor de filtro	O valor de filtro correspondente ao **`Filter Type`** selecionado. Este valor pode ser um **Grupo de recursos** ou **Par nome-valor de tag**. Deixe-o vazio para **`Filter Type`** **Todos**. Para a configuração da linha de comandos, pode aparecer uma barra invertida no exemplo exibido. Não insira uma barra invertida no valor fornecido. Exemplos de pares de tipo de filtro e valor de filtro: • Subnó do Azure Compute para monitorar todas as máquinas virtuais. Deixe o valor de filtro vazio. O valor de filtro não é necessário e é ignorado para o tipo de filtro **Todos**. – Tipo de filtro: **Todos** – Valor do Filtro: • Subnó do Azure Compute para monitorar todas as máquinas virtuais com um nome de tag de DTAP e um valor de tag que corresponde à sequência `prod`. – Tipo de filtro: **Par nome-valor de tag** – Valor de filtro: `DTAP:prod` • Subnó do Azure Compute para monitorar todas as máquinas virtuais com uma propriedade do grupo de recursos que corresponde à sequência `linux-group1`. – Tipo de filtro: **Grupo de recursos** – Valor de filtro: `linux-group1`	**`KAK_FILTER_VALUE.subnode_name`**

Configurando o monitoramento do Cassandra

Você deve configurar o Agente Cassandra para que o agente possa coletar dados dos nós no cluster para monitorar o funcionamento do Banco de dados Cassandra.

Antes de Iniciar

Revise os pré-requisitos de hardware e de software, consulte Agente do Software Product Compatibility Reports for Cassandra

Sobre Esta Tarefa

O Agente Cassandra é um agente de múltiplas instâncias. Você deve criar a primeira instância e iniciar o agente manualmente.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de

versões do agente e o que há de novo para cada versão, consulte o "Histórico de Mudanças" na página 50.

- Para configurar o agente em sistemas Windows, é possível usar a janela IBM Cloud Application Performance Management ou o arquivo silencioso de resposta.
- Para configurar o agente em sistemas Linux, é possível executar o script e responder aos prompts, ou usar o arquivo silencioso de resposta.

Configurando o agente nos sistemas Windows

Você pode utilizar o Use a janela do IBM Cloud Application Performance Management para configurar o agente nos sistemas Windows.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito em **Modelo** na coluna **Tarefa/Subsistema** e clique em **Configurar usando padrões**.

   A janela **Monitoring Agent for Cassandra** é aberta.
3. No campo **Inserir um nome de instância exclusivo**, digite um nome de instância do agente e clique em **OK**.
4. Na janela **Monitoring Agent for Cassandra**, especifique valores para os parâmetros de configuração e clique em **OK**.

   Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração do agente" na página 212.
5. Na janela **IBM Performance Management**, clique com o botão direito na instância do agente criada e clique em **Iniciar**.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o console, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Configurando o agente nos sistemas Linux

Para configurar o agente em sistemas operacionais Linux, você deve executar o script e responder aos prompts.

Procedimento

1. Na linha de comandos, mude o caminho para o diretório de instalação do agente.
   Exemplo: `/opt/ibm/apm/agent/bin`
2. Execute o comando a seguir em que instance_name é o nome que deseja dar à instância:

   `./cassandra-agent.sh config instance_name`
3. Quando a linha de comandos exibir a seguinte mensagem, digite 1 e insira:

   `Editar configuração do 'Monitoring Agent for Cassandra'? [1=Yes, 2=No]`
4. Especifique valores para os parâmetros de configuração quando solicitado.

   Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração do agente" na página 212.
5. Execute o comando a seguir para iniciar o agente:

   `./cassandra-agent.sh start instance_name`

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Configurando o agente usando o arquivo silencioso de resposta

O arquivo silencioso de resposta contém os parâmetros de configuração do agente. É possível editar o arquivo silencioso de resposta para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa
É possível usar o arquivo silencioso de resposta para configurar o Agente Cassandra em sistemas Linux e Windows. Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

1. Em um editor de texto, abra o arquivo de configuração silencioso que está disponível no seguinte local e especifique valores para todos os parâmetros:

   Windows `install_dir\samples\cassandra_silent_config_windows.txt`
   Linux `install_dir\samples\cassandra_silent_config_UNIX.txt`

   Windows `C:\IBM\APM\samples`

   Linux `/opt/ibm/apm/agent/samples`

   Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração do agente" na página 212.
2. Na linha de comandos, mude o caminho para `install_dir\bin`.
3. Execute o seguinte comando:

   Windows `cassandra-agent.bat config instance_name install_dir\samples \cassandra_silent_config_windows.txt`
   Linux `cassandra-agent.sh config instance_name install_dir\samples \cassandra_silent_config_UNIX.txt`
4. Inicie o agente.

   Windows Na janela **IBM Performance Management**, clique com o botão direito na instância do agente criada e clique em **Iniciar**.
   Linux Execute o seguinte comando: `./cassandra-agent.sh start instance_name`

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Parâmetros de configuração do agente

Ao configurar o Agente Cassandra, é possível mudar o valor padrão dos parâmetros, como endereço IP e JMX_PORT.

A tabela a seguir contém descrições detalhadas dos parâmetros de configuração do Agente Cassandra.

Tabela 18. Nomes e descrições dos parâmetros de configuração		
Nome do parâmetro	**Descrição**	**Campo obrigatório**
Nome da instância	O valor padrão para esse campo é idêntico ao valor especificado no campo **Inserir um nome da instância exclusivo**.	Sim
Endereço IP	O endereço IP de qualquer nó no cluster.	Sim
JMX_PORT	O número da porta JMX para ativar o monitoramento. **Importante:** Certifique-se de especificar a Porta JMX, o Nome do usuário JMX e a Senha JMX em todo o cluster. Se o nó através do qual o agente é conectado ao cluster não estiver funcionando, o agente poderá coletar dados por meio de um nó diferente no cluster usando os mesmos parâmetros.	Sim
JMX_Username	O nome do usuário para acessar JMX.	Não
JMX_Password	A senha para acessar o JMX.	Não

Configurando o monitoramento do Cisco UCS

O Monitoring Agent for Cisco UCS monitora o Cisco UCS Virtual Infrastructure conectando-se ao Cisco UCSM. Você deve configurar o Cisco UCS agent para que o agente possa coletar os dados do Cisco UCS.

Antes de Iniciar

- Revise os pré-requisitos de hardware e software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Cisco UCS agent.
- Certifique-se de que o usuário que se conecta à infraestrutura do Cisco UCSM tenha privilégios aaa ou de administrador. Use um ID do usuário existente, que tenha privilégios aaa ou de administrador, ou crie um novo ID do usuário.
- Se Cisco UCS agent estiver configurado para se comunicar com suas origens de dados Cisco UCS que usam o agente SSL, inclua o certificado SSL de cada origem de dados no armazenamento confiável de certificado do agente. Para obter mais informações sobre como ativar a comunicação de SSL com as origens de dados do Cisco UCS, consulte “Ativando a comunicação de SSL com origens de dados Cisco UCS” na página 218.

Sobre Esta Tarefa

O Cisco UCS agent é um agente de múltiplas instâncias. Deve-se criar a primeira instância e iniciar o agente manualmente.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Versão do Agente. Para acessar a documentação para liberações anteriores do agente, consulte a tabela a seguir:

Tabela 19. Documentação e versões do agente	
Versão do Cisco UCS agent	**Documentação**
7.2.0.4, 7.2.0.3	IBM Cloud Application Performance Management **Nota:** O link abre um tópico do Knowledge Center no local.

Tabela 19. Documentação e versões do agente (continuação)	
Versão do Cisco UCS agent	**Documentação**
7.2.0.2	IBM Performance Management 8.1.3 **Nota:** O link abre um tópico do Knowledge Center no local.
7.2.0.1	IBM Performance Management 8.1.2 **Nota:** O link abre um tópico do Knowledge Center no local.

Os atributos de configuração definem qual infraestrutura Cisco UCS é monitorada. Os atributos definem uma conexão com o Cisco UCSM 1.4 ou posterior. É possível configurar mais de uma instância do agente de monitoramento em um sistema host de monitoramento remoto. Também é possível criar instâncias separadas para monitorar a infraestrutura Cisco UCS específica.

Após o Cisco UCS agent ser instalado, é possível iniciar o agente. No entanto, deve-se configurar manualmente o agente para visualizar dados para todos os atributos de agente.

- Para configurar o agente em sistemas Windows, é possível usar a janela **IBM Performance Management** ou o arquivo de resposta silencioso.
- Para configurar o agente em sistemas Linux, é possível executar o script e responder aos prompts, ou usar o arquivo de resposta silencioso.

Configurando o Agente em Sistemas Windows

É possível configurar o agente em sistemas operacionais Windows usando a janela **IBM Performance Management**. Após fazer a atualização dos valores de configuração, deve-se iniciar o agente para salvar os valores atualizados.

Sobre Esta Tarefa

O Cisco UCS agent fornece valores padrão para alguns parâmetros. É possível especificar diferentes valores para esses parâmetros.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **Agentes de Monitoramento IBM** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito em **Monitoring Agent for Cisco UCS** e, em seguida, clique em **Configurar agente**.

   Lembre-se: Após você configurar o agente pela primeira vez, a opção **Configurar Agente** é desativada. Para configurar o agente novamente, clique em **Reconfigurar**.
3. Na janela Monitoring Agent for Cisco UCS, conclua as seguintes etapas:
   a) Insira um nome exclusivo para a instância do Cisco UCS agent e clique em **OK**.
   b) Na guia **CONFIG**, especifique valores para os parâmetros de configuração e clique em **Avançar**.
   c) Na guia **LOG_CONFIG**, especifique valores para os parâmetros de configuração e clique em **Avançar**.

   Para obter informações sobre os parâmetros de configuração em cada guia da janela Monitoring Agent for Cisco UCS, consulte os seguintes tópicos:

   - “Parâmetros de configuração para o agente” na página 217
   - “Parâmetros de configuração para o provedor de dados” na página 218
4. Na janela **IBM Performance Management**, clique com o botão direito em **Monitoring Agent for Cisco UCS** e, em seguida, clique em **Iniciar**.

O que Fazer Depois

- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

  Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.
- Se você estiver monitorando um ambiente Cisco UCS grande, pode ser necessário aumentar o tamanho de heap para o provedor de dados Java™. Para obter mais informações, consulte "Aumentando o tamanho de heap Java" na página 219.

Configurando o agente usando o arquivo de resposta silencioso

O arquivo de resposta silencioso contém os parâmetros de configuração do agente. É possível editar o arquivo de resposta silencioso para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

O arquivo silencioso de resposta contém os parâmetros de configuração do agente com valores padrão que são definidos para alguns parâmetros. É possível editar o arquivo de resposta silencioso para especificar os valores diferentes para os parâmetros de configuração.

Após você atualizar os valores de configuração no arquivo de resposta silencioso, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

- Para configurar o Cisco UCS agent no modo silencioso, conclua as seguintes etapas:
  a) Em um editor de texto, abra o arquivo `cisco_ucs_silent_config.txt` disponível no caminho a seguir:
     – Linux *install_dir*`/samples/cisco_ucs_silent_config.txt`

       Exemplo `/opt/ibm/apm/agent/samples/cisco_ucs_silent_config.txt`
     – Windows *install_dir*`\samples\cisco_ucs_silent_config.txt`

       Exemplo `C:\IBM\APM\samples\cisco_ucs_silent_config.txt`
  b) No arquivo `cisco_ucs_silent_config.txt`, especifique valores para todos os parâmetros obrigatórios. Também é possível modificar os valores padrão de outros parâmetros.

     Para obter informações sobre os parâmetros de configuração, consulte os tópicos a seguir:
     – "Parâmetros de configuração para o agente" na página 217
     – "Parâmetros de configuração para o provedor de dados" na página 218
  c) Salve e feche o arquivo `cisco_ucs_silent_config.txt` e execute o comando a seguir:
     – Linux *install_dir*`/bin/cisco_ucs-agent.sh config` *instance_name* *install_dir*`/samples/cisco_ucs_silent_config.txt`

       Exemplo **`/opt/ibm/apm/agent/bin/cisco_ucs-agent.sh config instance_name /opt/ibm/apm/agent/samples/cisco_ucs_silent_config.txt`**
     – Windows *install_dir*`\bin\cisco_ucs-agent.bat config` *instance_name* *install_dir*`\samples\cisco_ucs_silent_config.txt`

       Exemplo **`C:\IBM\APM\bin\cisco_ucs-agent.bat config instance_name C:\IBM\APM\samples\cisco_ucs_silent_config.txt`**

       Em que

instance_name
O nome que você deseja fornecer para a instância.

install_dir
Caminho onde o agente está instalado.

Importante: Assegure que você inclua o caminho absoluto no arquivo de resposta silencioso. Caso contrário, os dados do agente não serão mostrados nos painéis.

d) Execute o comando a seguir para iniciar o agente:

– Linux *install_dir*/bin/cisco_ucs-agent.sh start *instance_name*

Exemplo: **/opt/ibm/apm/agent/bin/cisco_ucs-agent.sh start instance_name**

– Windows *install_dir*start *instance_name*

Exemplo **C:\IBM\APM\bin\cisco_ucs-agent.bat start instance_name**

O que Fazer Depois

- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

  Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.
- Se você estiver monitorando um ambiente Cisco UCS grande, pode ser necessário aumentar o tamanho de heap para o provedor de dados Java™. Para obter mais informações, consulte "Aumentando o tamanho de heap Java" na página 219.

Configurando o agente respondendo aos prompts

Para configurar o agente em sistemas operacionais Linux, você deve executar o script e responder aos prompts.

Procedimento

- Para configurar o agente executando o script e respondendo aos prompts, conclua as seguintes etapas:

  a) Na linha de comandos, digite o seguinte comando:

  install_dir/bin/cisco_ucs-agent.sh config *instance_name*

  Exemplo **/opt/ibm/apm/agent/bin/cisco_ucs-agent.sh config instance_name**

  Em que

  instance_name
  O nome que você deseja fornecer para a instância.

  install_dir
  Caminho onde o agente está instalado.

  b) Responda aos prompts consultando os seguintes tópicos:

  – "Parâmetros de configuração para o agente" na página 217
  – "Parâmetros de configuração para o provedor de dados" na página 218

  c) Execute o comando a seguir para iniciar o agente:

  install_dir/bin/cisco_ucs-agent.sh start *instance_name*

  Exemplo: **/opt/ibm/apm/agent/bin/cisco_ucs-agent.sh start instance_name**

O que Fazer Depois

- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

  Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.
- Se estiver monitorando um ambiente Cisco UCS grande, pode ser necessário aumentar o tamanho de heap para o provedor de dados Java™. Para obter mais informações, consulte "Aumentando o tamanho de heap Java" na página 219.

Parâmetros de configuração para o agente

Quando você configura o Cisco UCS agent, é possível mudar os valores padrão dos parâmetros, como o nome da instância e os certificados de validação SSL.

A tabela a seguir contém descrições detalhadas dos parâmetros de configuração para o Cisco UCS agent.

Tabela 20. Nomes e descrições dos parâmetros de configuração para o Cisco UCS agent

Nome do parâmetro	Descrição	Campo obrigatório
Nome da instância	O nome da instância. **Restrição:** O campo **Nome da Instância** exibe o nome da instância que você especifica ao configurar o agente pela primeira vez. Ao configurar o agente novamente, não é possível mudar o nome da instância do agente.	Sim
URL	A URL do Cisco UCS Manager. Para configurar a URL do Cisco UCS Manager, insira a URL no formato http://ip_address/nuova.	Sim
Nome de Usuário	O nome do usuário administrador do Cisco UCS Manager.	Sim
Senha	A senha do administrador do Cisco UCS Manager.	Sim
Confirmar Senha	A mesma senha inserida no campo **Senha**.	Sim
Caminho do Arquivo do Armazenamento Confiável SSL	O caminho do arquivo de armazenamento confiável Secure Sockets Layer (SSL). Se quiser que o agente valide certificados SSL ao usar SSL para se comunicar por meio da rede, especifique o local onde o arquivo de armazenamento confiável Secure Sockets Layer (SSL) está localizado.	Sim
Validar Certificados SSL	Um valor booleano que indica se o agente valida certificados SSL ao usar SSL para se comunicar por meio da rede. Configure o valor para `Sim` se desejar que o agente valide certificados SSL ao usar SSL para se comunicar pela rede. Configure o valor para `Não` para evitar que o agente valide certificados SSL. **Dica:** Para obter mais informações sobre como ativar a comunicação de SSL com as origens de dados do Cisco UCS, consulte "Ativando a comunicação de SSL com origens de dados Cisco UCS" na página 218.	Sim

Parâmetros de configuração para o provedor de dados

Quando você configura o Cisco UCS agent, pode mudar os valores padrão dos parâmetros para o provedor de dados, como o número máximo de arquivos de log do provedor de dados, o tamanho máximo do arquivo de log e o nível de detalhes incluídos no arquivo de log.

A tabela a seguir contém descrições detalhadas dos parâmetros de configuração para o provedor de dados.

Tabela 21. Nomes e descrições dos parâmetros de configuração para o provedor de dados

Nome de parâmetro	Descrição	Campo obrigatório
Número Máximo de Arquivos de Log do Provedor de Dados	O número máximo de arquivos de log que o provedor de dados cria antes de sobrescrever os arquivos de log anteriores. O valor padrão é 10.	Sim
Tamanho Máximo em KB de Cada Log do Provedor de Dados	O tamanho máximo em KB que um provedor de dados deve atingir antes de o provedor de dados criar um novo arquivo de log. O valor padrão são 5190 KB.	Sim
Nível de Detalhe no Log do Provedor de Dados	O nível de detalhes que pode ser incluído no arquivo de log criado pelo provedor de dados. O valor padrão é INFO. Os valores a seguir são válidos: OFF, SEVERE, WARNING, INFO, FINE, FINER, FINEST e ALL.	Sim

Ativando a comunicação de SSL com origens de dados Cisco UCS

O Cisco UCS agent pode ser configurado para se comunicar com segurança com suas origens de dados Cisco UCS usando SSL. Nessa configuração, é necessário incluir um certificado SSL de origem de dados no armazenamento confiável de certificados do agente.

Sobre Esta Tarefa

Importante: As informações a seguir aplicam-se somente se o agente estiver configurado para validar certificados SSL.

Se a validação de certificados SSL estiver desativada, o Cisco UCS agent se conectará às origens de dados do Cisco UCS mesmo se seus certificados SSL estiverem expirados, não forem confiáveis ou forem inválidos. No entanto, é preciso ter cuidado ao desligar a validação de certificados SSL, pois isso não é seguro.

Se uma origem de dados do Cisco UCS usar um certificado SSL que é assinado por uma Autoridade de Certificação comum (por exemplo, Verisign, Entrust ou Thawte), não será necessário incluir certificados no armazenamento confiável de certificados do Cisco UCS agent. No entanto, se a origem de dados usar um certificado que não é assinado por uma Autoridade de Certificação comum, como é o caso por padrão, o certificado deve ser incluído no armazenamento confiável, para permitir que o agente tenha êxito ao se conectar e coletar dados.

Procedimento

1. Copie o arquivo de certificado da origem de dados para o computador do agente.
2. No computador agente, substitua o arquivo de certificado em um diretório de sua escolha. Não sobrescreva os arquivos de certificado. Use um nome e rótulo de arquivo exclusivo para cada certificado que você incluir.
3. Use o comando `keytool` para incluir o certificado de origem de dados no armazenamento confiável de certificados do agente:

   ```
   keytool -import -noprompt -trustcacerts -alias CertificateAlias -file
   CertificateFile -keystore Truststore -storepass TruststorePassword
   ```

   Em que

CertificateAlias

Referência exclusiva para cada certificado incluído no armazenamento confiável de certificados do agente, por exemplo, um alias apropriado para o certificado de *datasource.example.com* é *datasource*.

CertificateFile
O nome completo do caminho e do arquivo para o certificado de origem de dados do Cisco UCS para incluir no armazenamento confiável.

Armazenamento Confiável

O nome completo do caminho e arquivo para o banco de dados de certificados do Cisco UCS agent. Use o seguinte nome de caminho e arquivo:

- Windows (64 bit) *install_dir*\tmaitm6_x64\kv6.truststore
- Linux (64 bits) install_dir/lx8266/vm/etc/kv6.truststore

TruststorePassword

ITMFORVE é a senha padrão para o armazenamento confiável do Cisco UCS agent. Para alterar essa senha, consulte a documentação do Java Runtime para obter informações sobre as ferramentas a serem usadas.

Importante: Para usar o comando keytool, o diretório bin do Java Runtime deve estar em seu caminho. Use os seguintes comandos:

- Windows (64 bits) set PATH=%PATH%;install_dir\java\java70_x64\jre\bin
- Linux (64 bits) PATH="$PATH":/opt/ibm/apm/agent/JRE/lx8266/bin

4. Após incluir todos os certificados de origem de dados, inicie o agente de monitoramento.

Aumentando o tamanho de heap Java

Após configurar o Cisco UCS agent, se você estiver monitorando um grande ambiente Cisco UCS, talvez seja necessário aumentar o tamanho do heap para o provedor de dados Java™.

Sobre Esta Tarefa

O tamanho de heap padrão para o provedor de dados Java é 256 megabytes. Em grandes ambientes Cisco UCS, se os seguintes problemas surgirem, talvez seja necessário aumentar o tamanho do heap:

- O provedor de dados Java parar devido a um problema de javacore e criar um arquivo chamado javacore.*date.time.number*.txt no diretório CANDLEHOME\tmaitm6_x64.
- O arquivo javacore.*date.time.number*.txt contém a sequência java/lang/OutOfMemoryError.

Procedimento

- Windows
  Execute as etapas a seguir para configurar um valor de 1 GB como tamanho de heap:
  1. Abra o arquivo %CANDLE_HOME%\TMAITM6_x64\kv6_data_provider.bat.
  2. Inclua a linha a seguir antes da linha que inicia com KV6_JVM_ARGS="$KV6_CUSTOM_JVM_ARGS...:

     ```
     SET KV6_CUSTOM_JVM_ARGS=-Xmx1024m
     ```

  3. Reinicie o agente.
- Linux
  Execute as etapas a seguir para configurar um valor de 1 GB como tamanho de heap:
  1. Abra o arquivo $CANDLEHOME/lx8266/vm/bin/kv6_data_provider.sh.

2. Inclua a linha a seguir antes da linha que inicia com `KV6_JVM_ARGS="$KV6_CUSTOM_JVM_ARGS...`:

```
KV6_CUSTOM_JVM_ARGS=-Xmx1024m
```

3. Reinicie o agente.

Configurando o monitoramento do Citrix Virtual Desktop Infrastructure

O Citrix VDI agent fornece um ponto central de monitoramento para seus recursos do Citrix XenDesktop ou XenApp, incluindo grupos de entrega, catálogos, aplicativos, áreas de trabalho, usuários e sessões. Para que o agente possa ser usado, deve-se configurá-lo para coletar dados por meio do controlador de entrega.

Antes de Iniciar

- Estas instruções são para a liberação mais atual do agente, exceto conforme indicado.
- Certifique-se de que os requisitos do sistema para o Citrix VDI agent sejam atendidos em seu ambiente. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Citrix VDI agent.
- Assegure-se de que as seguintes informações estejam disponíveis:
  - Nome do host do controlador de entrega ao qual você planeja se conectar.
  - Nome do usuário, senha e domínio do OData.
  - O nome do usuário do PowerShell, senha, domínio, porta do PowerShell, tipo de verificação SSL e mecanismo de autenticação, se você ativar o Windows Event Log Event e a recuperação de métrica PowerShell.
- Certifique-se de que uma conta do usuário operador do agente tenha pelo menos privilégios de administrador somente leitura do Citrix. Consulte Ativando privilégios de administrador somente leitura do Citrix.
- A partir do Citrix VDI agent versão 8.1.3.1, a capacidade de recuperar eventos do Log de eventos do Windows ficou disponível. Para recuperar Eventos do Windows Event Log de todas as máquinas de Desktop Delivery Controller (DDC) e Virtual Delivery Agent (VDA), o acesso remoto ao PowerShell precisa ser ativado para a conta do usuário que é especificada durante a configuração da instância de agente. Siga estas etapas para assegurar que o agente possa desempenhar essa função:
  1. Efetue login em um computador Windows como o usuário especificado na configuração da instância de agente.
  2. Execute o seguinte comando PowerShell, em que *vda_system* é o nome de uma máquina VDA que está ligada:
     ```
     Get-WinEvent -FilterHashtable
     @{ProviderName='Citrix*';LogName='Citrix*';StartTime=((Get-
     Date).AddDays(-10))} -ComputerName vda_system
     ```
- Certifique-se de que as seguintes políticas de balanceamento de carga estejam ativadas para o ambiente monitorado:
  - Uso de CPU
  - Uso de Disco
  - Uso de Memória

  Essas políticas podem ser configuradas por meio do aplicativo Citrix Studio.

Sobre Esta Tarefa

O Citrix VDI agent é um agente de múltiplas instâncias. Você deve criar pelo menos uma instância, e iniciar a instância do agente manualmente.

A configuração para servidores XenApp é a mesma para servidores XenDesktop. Se um nome ou uma descrição do parâmetro de configuração mencionar somente "XenDesktop", será também para XenApp.

Procedimento

1. Configure o agente nos sistemas Windows com a janela **IBM Performance Management** ou o arquivo de resposta silencioso.
   - "Configurando o agente nos sistemas Windows" na página 222.
   - "Configurando o agente usando o arquivo silencioso de resposta" na página 226.
2. Configure o agente nos sistemas Linux com o script que solicita respostas ou com o arquivo de resposta silencioso.
   - "Configurando o agente respondendo aos prompts" na página 225.
   - "Configurando o agente usando o arquivo silencioso de resposta" na página 226.

O que Fazer Depois

No Console do Cloud APM, acesse seu Application Performance Dashboard para visualizar os dados que foram coletados. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Se você não conseguir visualizar os dados nos painéis do agente, primeiro verifique os logs de conexão do servidor e, em seguida, os logs do provedor de dados. Os caminhos padrão para esses logs são listados aqui:

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Para obter ajuda com a resolução de problemas, consulte o Fórum do Cloud Application Performance Management.

Ativando privilégios de administrador somente leitura do Citrix

O Citrix VDI agent requer que a conta do usuário operador do agente tenha pelo menos privilégios de administrador somente leitura do Citrix.

Sobre Esta Tarefa

Para executar essas etapas remotamente a partir de um computador que possui o Citrix Delegated Admin PowerShell Snap-in instalado, use o parâmetro `AdminAddress`. Por exemplo, o comando na etapa 2 será `New-AdminAdministrator -Name "YOURDOMAIN\NewAdmin" -AdminAddress "controller1.YOURDOMAIN.com"`. Em que *YOURDOMAIN* é o nome do domínio de rede, *NewAdmin* é a conta do usuário que está recebendo privilégios administrativos do Citrix e *controller1.YOURDOMAIN.com* é o nome completo do domínio do servidor de site do Citrix.

Procedimento

1. Inicie uma sessão do PowerShell com uma conta do administrador Citrix existente.
2. Carregue o Delegated Admin PowerShell Snap-in para gerenciar o site do Citrix XenApp ou XenDesktop.

   ```
   (Add-PSSnapin Citrix.DelegatedAdmin.Admin.V1)
   ```
3. Inclua a conta do usuário operador do agente como um administrador do site do Citrix.

   ```
   New-AdminAdministrator -Name "YOURDOMAIN\NewAdmin"
   ```

   Em que *YOURDOMAIN* é o nome do domínio de rede e *NewAdmin* é a conta do usuário que está recebendo privilégios administrativos do Citrix.
4. Consulte as funções e escopos disponíveis para designar a *NewAdmin*.

```
Get-AdminRole
Get-AdminScope
```

5. Designe funções para a conta do usuário do operador do agente, incluindo permissões de administrador somente leitura.

   ```
   Add-AdminRight -Administrator "YOURDOMAIN\NewAdmin" -Role "Read Only
   Administrator" -Scope "All"
   ```

   Em que

   - *YOURDOMAIN* é o nome do domínio de rede.
   - *NewAdmin* é a conta do usuário que está recebendo privilégios de administração do Citrix.
   - *Read Only Administrator* é a função de administrador do site do Citrix que você está designando.
   - *All* é o escopo do administrador do site do Citrix que você está designando.

6. Confirme a inclusão e mudanças do administrador.

   ```
   Get-AdminAdministrator -Name "YOURDOMAIN\NewAdmin"
   ```

   Em que *YOURDOMAIN* é o nome do domínio de rede e *NewAdmin* é a conta do usuário que está recebendo privilégios administrativos do Citrix.

Configurando o agente nos sistemas Windows

É possível configurar o Citrix VDI agent em sistemas operacionais Windows usando a janela IBM Cloud Application Performance Management. Após fazer a atualização dos valores de configuração, deve-se iniciar o agente para salvar os valores atualizados.

Procedimento

1. Clique em **Iniciar** > **Todos os programas** > **Agentes do IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito no modelo **Monitoring Agent for Citrix Virtual Desktop Infrastructure** e, em seguida, clique em **Configurar agente**.

   Lembre-se: Depois de configurar uma instância de agente pela primeira vez, a opção **Configurar agente** é desativada. Para configurar a instância de agente novamente, clique nela com o botão direito e clique em **Reconfigurar**.
3. Insira um nome de instância exclusivo e, em seguida, clique em **OK**. Use apenas letras, numerais Arábicos, o caractere sublinhado e o caractere de menos no nome da instância. Exemplo, `vdi_inst2`.

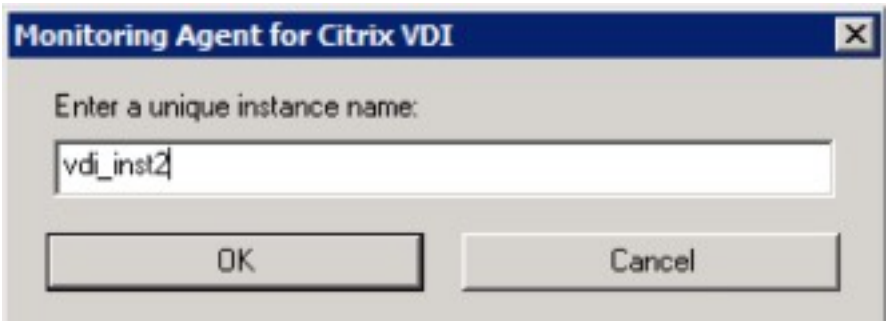


Figura 13. A janela para inserir um nome exclusivo da instância.

4. Clique em **Avançar** na janela de nome da instância de agente.

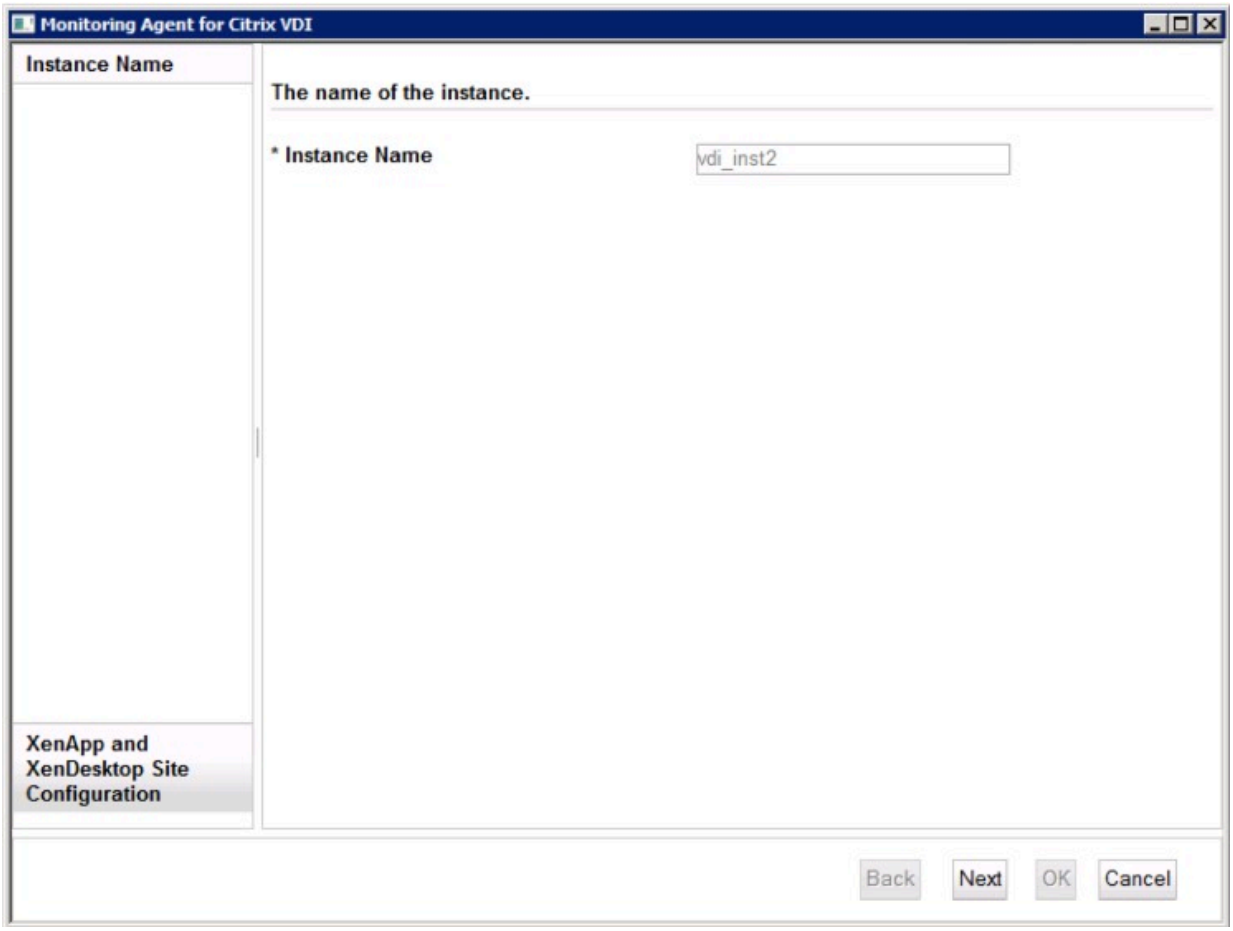


Figura 14. A janela de nome da instância de agente.

5. Insira as configurações de modelo da instância **Configuração do Site do XenApp e XenDesktop**.

   Nota: Esta seção não é a configuração da instância do site do XenApp ou XenDesktop. É uma seção de modelo para configurar o que é usado como os valores padrão ao incluir as configurações reais da instância do site do XenApp ou XenDesktop na etapa 6.

   Consulte Tabela 22 na página 227 para obter uma explicação de cada um dos parâmetros de configuração.

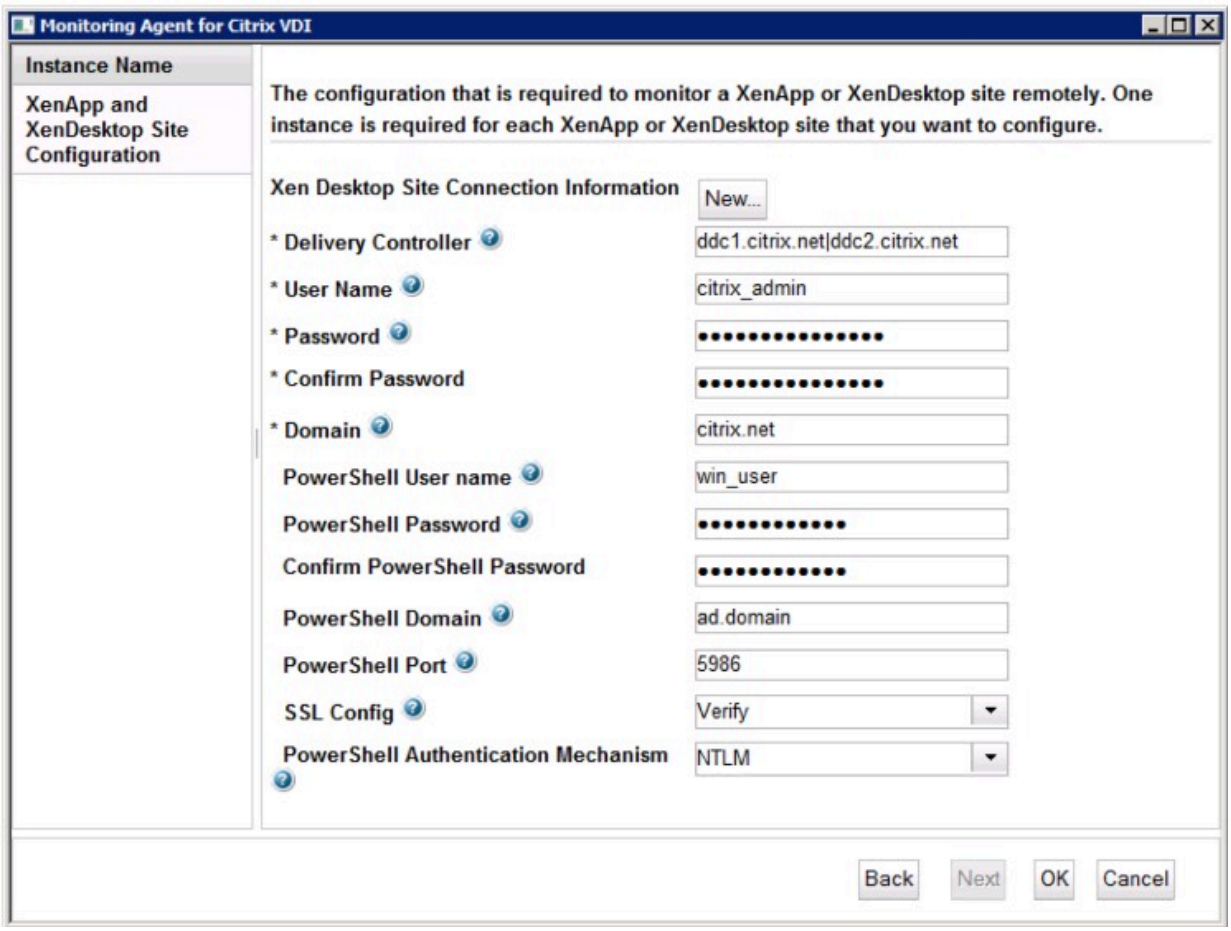


Figura 15. A janela para especificar configurações de modelo da instância do site do XenApp ou XenDesktop.

6. Pressione **Novo** e insira configurações da instância do site do XenApp ou XenDesktop, em seguida, clique em **Avançar**.

   Consulte Tabela 22 na página 227 para obter uma explicação de cada um dos parâmetros de configuração.

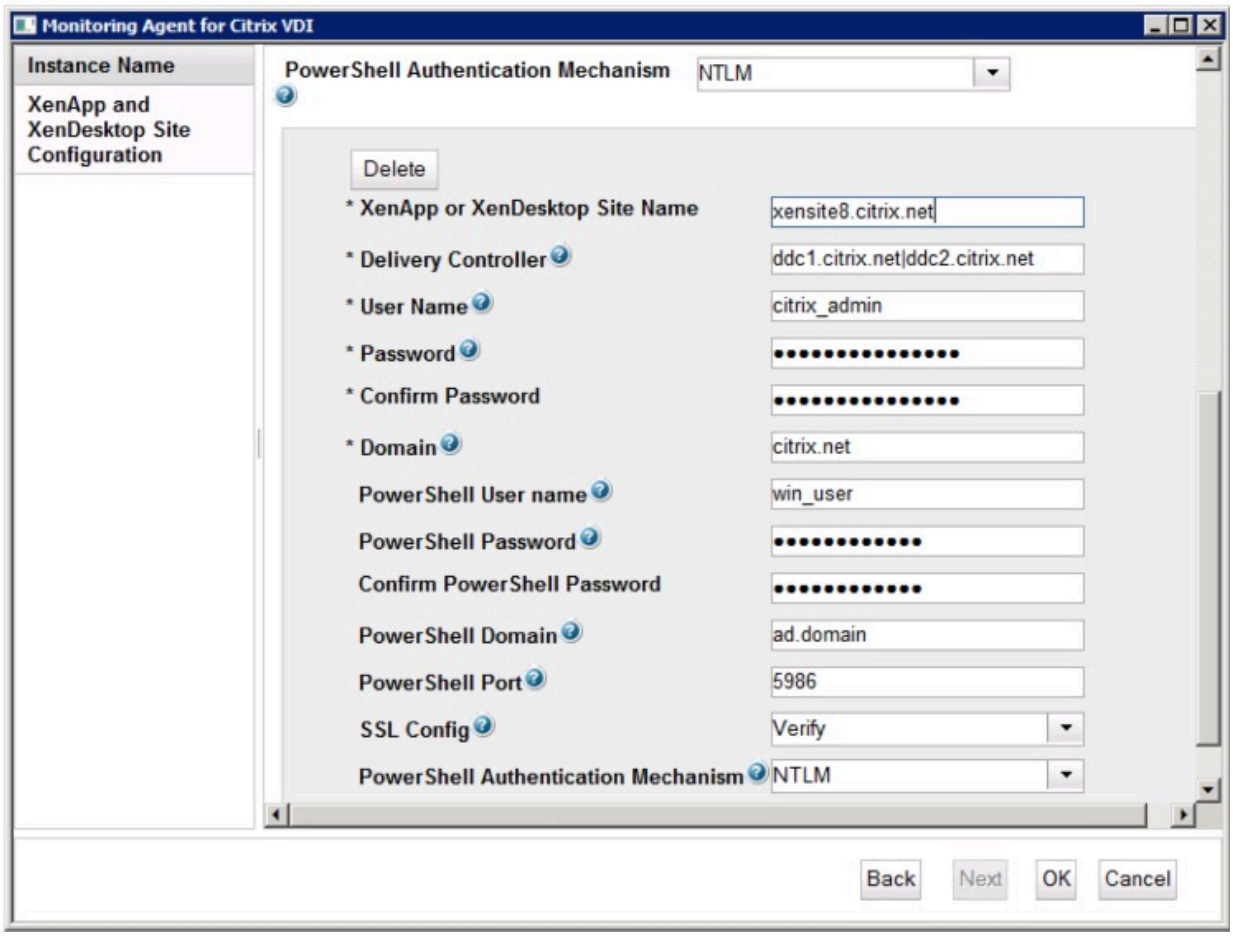


Figura 16. A janela para especificar configurações da instância do site do XenApp ou XenDesktop.

Nota: O parâmetro **`PowerShell User name`** e todos os parâmetros PowerShell a seguir são necessários somente quando "Ativando o monitoramento de eventos do Windows e as métricas do PowerShell" na página 229. Por padrão, essas variáveis de ambiente avançadas estão fora devido à carga significativa que colocam no sistema monitorado.

Nota: Assegure que os parâmetros **`SSL Config`** e **`PowerShell Authentication Mechanism`** sejam configurados corretamente para cada instância nova do site do XenApp ou XenDesktop. Um defeito faz com que os valores padrão sejam configurados, em vez dos valores modelo.

7. Clique em **OK** para concluir a configuração.
8. Na janela IBM Cloud Application Performance Management, clique com o botão direito na instância configurada e, em seguida, clique em **Iniciar**.

Configurando o agente respondendo aos prompts

Após a instalação do Citrix VDI agent, deve-se configurá-lo antes de iniciar o agente. Se o Citrix VDI agent estiver instalado em uma máquina Linux local, será possível seguir estas instruções para configurá-lo interativamente por meio de prompts da linha de comandos.

Sobre Esta Tarefa

Lembre-se: Se estiver reconfigurando uma instância do agente configurada, o valor que é definido na última configuração será exibido para cada configuração. Se desejar limpar um valor existente, pressione a tecla Espaço quando a configuração for exibida.

Procedimento

Siga essas etapas para configurar o Citrix VDI agent executando um script e respondendo aos prompts.

1. Execute o seguinte comando:

   ```
   install_dir/bin/citrixvdi-agent.sh
   config instance_name
   ```

   em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome que você deseja fornecer para a instância de agente.

   Exemplo

   ```
   /opt/ibm/apm/agent/bin/citrixvdi-agent.sh config vdi_inst01
   ```

2. Responda aos prompts para configurar valores de configuração para o agente.

   Consulte "Parâmetros de Configuração para o Citrix VDI agent" na página 227 para obter uma explicação de cada um dos parâmetros de configuração.

   Nota: O parâmetro **PowerShell User name** e todos os parâmetros PowerShell a seguir são necessários somente quando "Ativando o monitoramento de eventos do Windows e as métricas do PowerShell" na página 229. Por padrão, essas variáveis de ambiente avançadas estão fora devido à carga significativa que colocam no sistema monitorado.

3. Execute o comando a seguir para iniciar o agente:

   ```
   install_dir/bin/citrixvdi-agent.sh
   start instance_name
   ```

   em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome da instância de agente.

   Exemplo

   ```
   Vdi_inst01 start
   ```

Configurando o agente usando o arquivo silencioso de resposta

O arquivo silencioso de resposta contém os parâmetros de configuração do agente. É possível editar o arquivo silencioso de resposta para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

O arquivo silencioso de resposta contém os parâmetros de configuração do agente com valores padrão que são definidos para alguns parâmetros. É possível editar o arquivo silencioso de resposta para especificar os valores diferentes para os parâmetros de configuração.

Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

- Configure o Citrix VDI agent no modo silencioso:
  a) Abra o arquivo `citrixvdi_silent_config.txt` em um dos seguintes caminhos em um editor de texto.
  - Linux *install_dir*`/samples/citrixvdi_silent_config.txt`

    Exemplo, `/opt/ibm/apm/agent/samples/citrixvdi_silent_config.txt`
  - Windows *install_dir*`\samples\citrixvdi_silent_config.txt`

    Exemplo, `C:\IBM\APM\samples\citrixvdi_silent_config.txt`

  em que *install_dir* é o caminho no qual o agente está instalado.

b) No arquivo `citrixvdi_silent_config.txt`, especifique valores para todos os parâmetros obrigatórios e modifique os valores padrão de outros parâmetros, conforme necessário.

Consulte "Parâmetros de Configuração para o Citrix VDI agent" na página 227 para obter uma explicação de cada um dos parâmetros de configuração.

Nota: O parâmetro **PowerShell User name** e todos os parâmetros PowerShell a seguir são necessários somente quando "Ativando o monitoramento de eventos do Windows e as métricas do PowerShell" na página 229. Por padrão, essas variáveis de ambiente avançadas estão fora devido à carga significativa que colocam no sistema monitorado.

c) Salve e feche o arquivo `citrixvdi_silent_config.txt`, e execute o comando a seguir:

- Linux `install_dir/bin/citrixvdi-agent.sh config` **instance_name** `install_dir/samples/citrixvdi_silent_config.txt`

  Exemplo, **/opt/ibm/apm/agent/bin/citrixvdi-agent.sh config vdi_inst01 /opt/ibm/apm/agent/samples/citrixvdi_silent_config.txt**

- Windows `install_dir\bin\citrixvdi-agent.bat config` **instance_name** `install_dir\samples\citrixvdi_silent_config.txt`

  Exemplo, **C:\IBM\APM\bin\citrixvdi-agent.bat config vdi_inst01 C:\IBM\APM\samples\citrixvdi_silent_config.txt**

em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome que você deseja fornecer para a instância de agente.

Importante: Assegure que você inclua o caminho absoluto no arquivo silencioso de resposta. Caso contrário, os dados do agente não serão mostrados nos painéis.

d) Execute o comando a seguir para iniciar o agente:

- Linux `install_dir/bin/citrixvdi-agent.sh start` **instance_name**

  Exemplo, **/opt/ibm/apm/agent/bin/citrixvdi-agent.sh start vdi_inst01**

- Windows `install_dir\bin\citrixvdi-agent.bat start` **instance_name**

  Exemplo, **C:\IBM\APM\bin\citrixvdi-agent.bat start vdi_inst01**

em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome da instância de agente.

Parâmetros de Configuração para o Citrix VDI agent

Os parâmetros de configuração para o Citrix VDI agent são exibidos em uma tabela.

1. Configurações do Agente Citrix VDI - Configurações do ambiente do agente Citrix VDI.

Tabela 22. Configurações do agente Citrix VDI

Nome de parâmetro	Descrição	Nome do parâmetro do arquivo de configuração silenciosa
Nome do Site do XenApp ou XenDesktop	Forneça um nome para identificar a instância de agente do site do XenApp ou XenDesktop. Exemplo, *vdi_inst2* **Nota:** Esse alias pode ser qualquer coisa que é possível escolher para representar a instância de agente do servidor WebLogic com as restrições a seguir. Somente letras, numerais arábicos, o caractere sublinhado e o caractere menos podem ser usados no nome da conexão. O comprimento máximo do nome de uma conexão é 25 caracteres.	Cada um dos seguintes parâmetros deve ter um sufixo de nome da instância que é o mesmo para cada parâmetro de uma instância de agente. As novas instâncias de agente devem usar um nome de instância exclusivo para seu conjunto de parâmetros. Por exemplo, uma instância de agente pode usar *.vdi1* e outra instância de agente pode usar *.vdi2* no lugar de *.instance_name* nos nomes de parâmetros que seguem.

Tabela 22. Configurações do agente Citrix VDI (continuação)		
Nome de parâmetro	**Descrição**	**Nome do parâmetro do arquivo de configuração silenciosa**
Delivery Controller	Nome do host ou endereço IP do controlador de entrega. Se múltiplos DDCs forem configurados em um cluster, uma lista separada por '|' de controladores de entrega poderá ser fornecida.	**KVD_XDS_DELIVERY_CONTROLLER.instance_name**
Nome do Usuário	O nome do usuário que é usado para se autenticar com a API OData no controlador de entrega especificado do XenApp ou XenDesktop.	**KVD_XDS_ODATA_USERNAME.instance_name**
Senha	A senha que é usada para se autenticar com a API OData no controlador de entrega especificado do XenApp ou XenDesktop.	**KVD_XDS_ODATA_PASSWORD.instance_name**
Domínio	O domínio que é usado para se autenticar com a API OData no controlador de entrega especificado do XenApp ou XenDesktop.	**KVD_XDS_ODATA_DOMAIN.instance_name**
Nome do Usuário do PowerShell	O nome do usuário usado para se autenticar para chamadas do PowerShell para máquinas remotas VDA e DDC. **Nota:** Este e todos os parâmetros do PowerShell a seguir são necessários somente quando "Ativando o monitoramento de eventos do Windows e as métricas do PowerShell" na página 229. Por padrão, essas variáveis de ambiente avançadas estão fora devido à carga significativa que colocam no sistema monitorado.	**KVD_XDS_POWERSHELL_USERNAME.instance_name**
Senha do PowerShell	A senha associada ao nome do usuário do PowerShell fornecido.	**KVD_XDS_POWERSHELL_PASSWORD.instance_name**
Domínio do PowerShell	O domínio associado ao nome do usuário do PowerShell fornecido.	**KVD_XDS_POWERSHELL_DOMAIN.instance_name**
Porta do PowerShell	A porta SSL que é aberta para uso pelo WinRm. As portas de conexão remota padrão do PowerShell são 5985 para HTTP e 5986 para HTTPS.	**KVD_XDS_POWERSHELL_PORT.instance_name**
Requisito de SSL	Escolha a opção de SSL necessária para seu ambiente.	**KVD_XDS_SSL_CONFIG.instance_name** Valores válidos, **KVD_XDS_SSL_CONFIG_VERIFY** Verificar **KVD_XDS_SSL_CONFIG_NOVERIFY** Sem Verificação **KVD_XDS_SSL_CONFIG_NOSSL** Sem SSL

Tabela 22. Configurações do agente Citrix VDI (continuação)		
Nome de parâmetro	**Descrição**	**Nome do parâmetro do arquivo de configuração silenciosa**
Mecanismo de Autenticação do PowerShell	Define o tipo de autenticação usado para criar uma credencial para recuperar informações a partir de sistemas remotos com PowerShell.	**KVD_XDS_POWERSHELL_AUTH_MECH.instance_name** Valores válidos, **KVD_XDS_POWERSHELL_BASIC** Basic **KVD_XDS_POWERSHELL_CREDSSP** CredSSP **KVD_XDS_POWERSHELL_NTLM** NTLM **KVD_XDS_POWERSHELL_DEFAULT** Padrão **KVD_XDS_POWERSHELL_DIGEST** Sumário **KVD_XDS_POWERSHELL_KERBEROS** Kerberos **KVD_XDS_POWERSHELL_NEGOTIATE** Negociar

Ativando o monitoramento de eventos do Windows e as métricas do PowerShell

Ative o monitoramento de eventos do Windows e as métricas do PowerShell com este procedimento. O monitoramento desses dados pode ter um impacto significativo no desempenho para o sistema monitorado.

Antes de Iniciar

Assegure-se de que os parâmetros de configuração do PowerShell do agente estejam configurados.

Sobre Esta Tarefa

Uma ou mais das seguintes variáveis de ambiente avançadas devem ser ativadas para o agente para monitorar eventos do Windows e métricas do PowerShell.

GET_SESSION_LATENCY
Se a latência da sessão e o tempo de roundtrip forem recuperados remotamente a partir do VDA conectado do PowerShell.

GET_VDA_MACHINE_METRICS_REMOTELY
Se as métricas da máquina VDA forem recuperadas remotamente a partir do PowerShell.

RETRIEVE_WINDOWS_EVENTS
Se os Eventos do Windows Event Log forem recuperados do PowerShell a partir dos VDAs e DDCs do Windows.

Procedimento

1. Acesse o diretório de instalação do agente do Citrix VDI agent:
   - Linux *install_dir*/config
   - Windows *install_dir*\TMAITM6_x64

   em que *install_dir* é o caminho no qual o agente está instalado.

2. Edite o arquivo de configuração do Citrix VDI agent para configurar uma ou mais das variáveis *GET_SESSION_LATENCY*, *GET_VDA_MACHINE_METRICS_REMOTELY* e *RETRIEVE_WINDOWS_EVENTS* para `true`.
   - Linux `vd.environment`
   - Windows KVDENV_*instance_name*

   em que *instance_name* é o nome da instância de agente.
3. Reinicie o agente.

   Importante: Para tornar essas configurações padrão para todas as novas instâncias do agente, configure-as para `true` nos arquivos de modelo de configuração:
   - Linux Essa configuração já se tornou padrão para novas instâncias de agentes editando `vd.environment` na Etapa 2.
   - Windows KVDENV

Exemplo

```
GET_SESSION_LATENCY=true
GET_VDA_MACHINE_METRICS_REMOTELY=true
RETRIEVE_WINDOWS_EVENTS=true
```

Configurando o monitoramento do DataPower

Para monitorar dispositivos DataPower, é necessário primeiro concluir algumas tarefas de configuração nos dispositivos e, em seguida, configurar o Monitoring Agent for DataPower.

Dica: Clique em APM v8: Configurando o monitoramento do DataPower no IBM APM para assistir a um vídeo que cobre o processo de configuração básica de monitoramento do DataPower.

Configurando DataPower Appliances

Antes de configurar o Monitoring Agent for DataPower, deve-se concluir algumas tarefas de configuração nos dispositivos.

Dica: Para obter informações sobre os DataPower Appliances suportados, consulte a guia Pré-requisitos em Software Product Compatibility Reports.

É possível monitorar dispositivos DataPower em três níveis diferentes. Configure os três níveis, de acordo com suas necessidades, em cada dispositivo DataPower que você deseja monitorar para exibir dados do dispositivo DataPower no Console do Cloud APM.

1. Monitoramento de Recursos

   Para ver dados de monitoramento, como utilização de recurso, rendimento e estatísticas de conexão, ative o monitoramento de recursos. Para obter instruções, veja “Monitoramento de Recursos” na página 231.
2. Rastreamento de transação de middleware

   Para ver dados de monitoramento para transações, como informações detalhadas de transação, volume e dependências, ative o rastreamento de transações de middleware. Para obter instruções, veja “Rastreamento de transação de middleware” na página 232.
3. Rastreamento de transações em nível de instância do dispositivo DataPower

   Para exibir dados de monitoramento para transações em topologias de instância, configure o rastreamento de exibição em nível de instância do dispositivo DataPower. Para obter instruções, veja “Rastreamento de transação em nível de instância de dispositivo DataPower” na página 233.

Importante: Certifique-se de que o ID do usuário tenha as permissões adequadas para configurar o dispositivo DataPower. É possível inserir `*/*/*?Access=r` no campo **Perfil de acesso** para o ID do

usuário usado para configurar o dispositivo DataPower. Em seguida, use esse ID do usuário para configurar o dispositivo DataPower.

Exportando o certificado público
Se a Interface de Gerenciamento XML do DataPower Appliance possuir o Perfil Proxy SSL ativado, você deverá exportar o certificado público usado pela Interface de Gerenciamento XML do DataPower Appliance para a máquina que executa o DataPower agent.

Procedimento

1. Para fazer download do certificado crypto que é usado pela Interface de Gerenciamento XML do dispositivo DataPower, por exemplo, `pubcert:///mycert.pem`, clique em **Administração** > **Principal** > **Gerenciamento de arquivo** e salve o certificado na máquina que executa o DataPower agent.
2. Ao configurar o DataPower agent, há uma opção para especificar o campo **Perfil Proxy SSL**. Digite o caminho absoluto do certificado público.

   Nota: Quando mais gateways multiprotocolo forem incluídos, será preciso repetir essas etapas.

Monitoramento de Recursos
O primeiro nível de monitoramento disponível para um dispositivo DataPower é ativar o monitoramento de recurso, como gerenciamento SOAP, estatísticas e taxas de transação.

A operação na interface com o usuário (UI) do DataPower Gateway nas seguintes tarefas de configuração se aplica ao DataPower Gateway Versão 7.5.1 e versões anteriores. Se a versão do DataPower Gateway usada for mais recente que a V 7.5.1, será possível clicar no ponto de interrogação, no canto superior direito na UI e escolher **WebGUI** para retornar à UI da versão anterior. E depois, siga as instruções para concluir as tarefas de configuração do dispositivo DataPower.

Ativando o gerenciamento SOAP
Se você desejar que o DataPower agent colete dados de DataPower Appliances, deverá configurar a interface de gerenciamento XML e ativar o gerenciamento SOAP.

Procedimento

Para ativar o SOAP:

1. Efetue logon na WebGUI para o DataPower Appliance que você deseja monitorar.
2. Clique em **Objetos** > **Gerenciamento de Dispositivos** > **Interface de Gerenciamento XML**.

   Nota: Assegure-se de que o estado Administrativo esteja ativado.
3. Para o **Número da Porta**, digite o número da porta na qual o DataPower agent atende relatórios de notificação. Por padrão, o número da porta é 5550.
4. Para **Serviços Ativados**, assegure-se de que o **Gerenciamento SOAP** seja selecionado.

Ativando estatísticas
Se desejar que o DataPower agent colete dados de dispositivos DataPower, a opção Estatísticas deve ser ativada.

Procedimento

Para ativar Estatísticas, conclua as etapas a seguir:

1. Efetue logon na WebGUI para o DataPower Appliance que você deseja monitorar.
2. Clique em **Administração** > **Dispositivo** > **Configurações de Estatísticas**.
3. Ative **Configurações de Estatísticas** e clique em **Aplicar**.

Ativando a taxa de transação
Se você desejar que o DataPower agent colete dados de dispositivos DataPower, a Taxa de Transação deve estar ativada.

Procedimento

Para ativar a Taxa de Transação, conclua as etapas a seguir:

1. Efetue logon na WebGUI para o DataPower Appliance que você deseja monitorar.
2. Selecione o domínio `default`.
3. Clique em **Status** > **Conexão** > **Taxa de Transação**.
4. Se **Estatísticas Estão Atualmente Desativadas** for exibido, clique em **desativado**; em Configurações de Estatísticas, configure **Estado Administrativo** para **ativado**.
5. Se você tiver vários domínios, clique em **Mostrar Todos os Domínios** e repita as etapas 3 e 4 para ativar a Taxa de Transação para todos os domínios aplicáveis.
6. Clique em **Aplicar**.

Rastreamento de transação de middleware
O segundo nível de monitoramento disponível para um dispositivo DataPower é exibir rastreamento de transação de middleware em áreas de trabalho.

A operação na interface com o usuário (UI) do DataPower Gateway nas seguintes tarefas de configuração se aplica ao DataPower Gateway Versão 7.5.1 e versões anteriores. Se a versão do DataPower Gateway usada for mais recente que a V 7.5.1, será possível clicar no ponto de interrogação, no canto superior direito na UI e escolher **WebGUI** para retornar à UI da versão anterior. E depois, siga as instruções para concluir as tarefas de configuração do dispositivo DataPower.

O rastreamento de transação de tráfego SOAP e de tráfego REST por meio do dispositivo DataPower é suportado. O rastreamento de transação do DataPower suporta SOAP usando arquivos `store:///soapreq.xsl`, `store:///soaprsp.xsl` e `store:///soaperror.xsl`. Esses arquivos XSL instrumentam o Web Service Proxy para incluir e relatar `kd4:KD4SoapHeaderV2` no Envelope do SOAP.

Além dos arquivos `soap*.xsl`, o rastreamento de transações do DataPower também inclui `apm_req.xsl`, `apm_rsp.xsl` e `apm_error.xsl`, que suportam solicitações de HTTP recebidas contendo um `Cabeçalho de HTTP ARM_CORRELATOR:` ou um Envelope SOAP contendo `ITCAMCorrelator` ou `kd4:KD4SoapHeaderV2`. O Web Service Proxy atualiza ou configura a solicitação realizada para conter um `ARM_CORRELATOR: HTTP Header` e remove os correlacionadores de SOAP.

Nota: Se dispositivos DataPower forem incluídos em um aplicativo de negócios, e o dispositivo levar o tráfego para diversos aplicativos, depois que o rastreamento de transação for ativado, a topologia de aplicativo exibida para esses aplicativos de negócios incluirá caminhos para nós de todos os aplicativos.

Configurando o Web Service Management
Conclua estas etapas para cada dispositivo DataPower para os quais deseja exibir dados de rastreamento.

1. Efetue logon na WebGUI para o DataPower Appliance que você deseja monitorar.
2. Selecione o domínio `default`.
3. Procure `Interface de Gerenciamento XML`. Configure os valores a seguir e clique em **Aplicar**.
   - Na guia **Principal**, na seção **Serviços Ativados**, ative **Terminal WS-Management**
4. Procure por `Web Services Management Agent`. Configure os valores a seguir e clique em **Aplicar**.
   - Configure **Estado Administrativo** para **ativado**
   - Configure **Modo de Captura** para **Nenhum**
   - Configure **Modo de Armazenamento em Buffer (descontinuado)** para **Descartar**
5. Configure o Web Service Proxy ou o gateway multiprotocolo conforme descrito nos seguintes tópicos.

Configurando o Web Service Proxy
Conclua estas etapas para cada Web Service Proxy do qual deseja exibir dados de rastreamento.

Procedimento

1. Selecione o domínio do qual o Web Service Proxy faz parte.

2. Na guia **Configurações de proxy**, configure os seguintes valores e clique em **Aplicar**:
   - Configure **Monitorar via Web Services Management Agent** para **ativado**
3. Para relatar falhas de SOAP, desative o processamento de erro e ative o relatório de erro no Console do Cloud APM: na guia **Configurações avançadas de proxy**, configure **Processar erros de HTTP** como `off` e clique em **Aplicar**.

Configurando o gateway multiprotocolo
Conclua essas etapas para cada Multi-Protocol Gateway para o qual você deseja exibir dados de rastreamento de transação.

Procedimento

1. Selecione o domínio do qual o gateway multiprotocolo faz parte.
2. Na guia **Avançado** do gateway multiprotocolo, configure os seguintes valores e clique em **Aplicar**:
   - Configure **Monitorar via Web Services Management Agent** para **ativado**
   - Se o servidor da web usar redirecionamentos, configure **Seguir redirecionamentos** como **off**. Depois configure **Regravar URL de local** para **on**.
3. Se você estiver monitorando um gateway multiprotocolo com Tipo de resposta ou Tipo de solicitação de `Não XML`, deverá definir uma Política de gateway multiprotocolo com regras abrangendo as direções de cliente para servidor e servidor para cliente. Se um Gateway Multiprotocolo Não XML não tiver regras em sua política, nenhum tráfego será capturado pelo Web Services Management Agent ou Análise de Depuração do DataPower (se ativada).
4. Para propagar o código de resposta HTTP do servidor de backend e para relatar falhas de SOAP, na guia **Configurações avançadas**, configure **Processar erros de backend** como `off` e clique em **Aplicar**.

Rastreamento de transação em nível de instância de dispositivo DataPower
O terceiro nível de monitoramento disponível para um dispositivo DataPower é exibir seus dados em topologias de instância.

A operação na interface com o usuário (UI) do DataPower Gateway nas seguintes tarefas de configuração se aplica ao DataPower Gateway Versão 7.5.1 e versões anteriores. Se a versão do DataPower Gateway usada for mais recente que a V 7.5.1, será possível clicar no ponto de interrogação, no canto superior direito na UI e escolher **WebGUI** para retornar à UI da versão anterior. E depois, siga as instruções para concluir as tarefas de configuração do dispositivo DataPower.

Configurando transformações
Conclua estas etapas em cada dispositivo DataPower que deseja exibir em topologias de instância.

Sobre Esta Tarefa

Para IBM Performance Management V8.1.2 Fix Pack 1, o rastreamento de transação de tráfego SOAP por meio do dispositivo DataPower é suportado. O rastreamento de transação DataPower suporta SOAP usando arquivos `store:///soapreq.xsl`, `store:///soaprsp.xsl` e `store:///soaperror.xsl`. Esses arquivos XSL instrumentam o Web Service Proxy para incluir e relatar `kd4:KD4SoapHeaderV2` no Envelope do SOAP.

Para IBM Performance Management V8.1.3 e posterior, o rastreamento de transação de tráfego REST por meio do dispositivo DataPower também é suportado. Além de arquivos `soap*.xsl`, o rastreamento de transação DataPower também inclui `apm_req.xsl`, `apm_rsp.xsl` e `apm_error.xsl`, que suportam solicitações de HTTP recebidas contendo `ARM_CORRELATOR: HTTP Header` ou um Envelope SOAP contendo `ITCAMCorrelator` ou `kd4:KD4SoapHeaderV2`. O Web Service Proxy atualiza ou configura a solicitação realizada para conter um `ARM_CORRELATOR: HTTP Header` e remove os correlacionadores de SOAP.

O DataPower agent suporta o rastreamento de transação para tráfego SOAP por meio do dispositivo DataPower, tráfego REST por meio do dispositivo DataPower e o tráfego entre o DataPower e o WebSphere MQ.

- Se desejar ativar o rastreamento de transação para tráfego SOAP e REST por meio do dispositivo DataPower, aplique `apm_req.xsl`, `apm_rsp.xsl` e `apm_error.xsl`, que suportam solicitações de HTTP recebidas contendo um `ARM_CORRELATOR: HTTP Header`, ou um Envelope SOAP contendo `ITCAMCorrelator` ou `kd4:KD4SoapHeaderV2`. O Web Service Proxy atualiza ou configura a solicitação realizada para conter um `ARM_CORRELATOR: HTTP Header` e remove os correlacionadores de SOAP.
- Além do tráfego SOAP e REST por meio do dispositivo DataPower, se você desejar ativar o rastreamento de transação entre o DataPower e o WebSphere MQ, aplique os arquivos `apm_req_MQ.xsl`, `apm_rsp_MQ.xsl` e `apm_error_MQ.xsl`. O rastreamento de transação para tráfego SOAP e REST também é ativado automaticamente após a aplicação desses arquivos.

Procedimento

Para rastrear o tráfego REST e ativar o rastreamento de transação entre o DataPower e o WebSphere MQ, conclua as seguintes etapas:

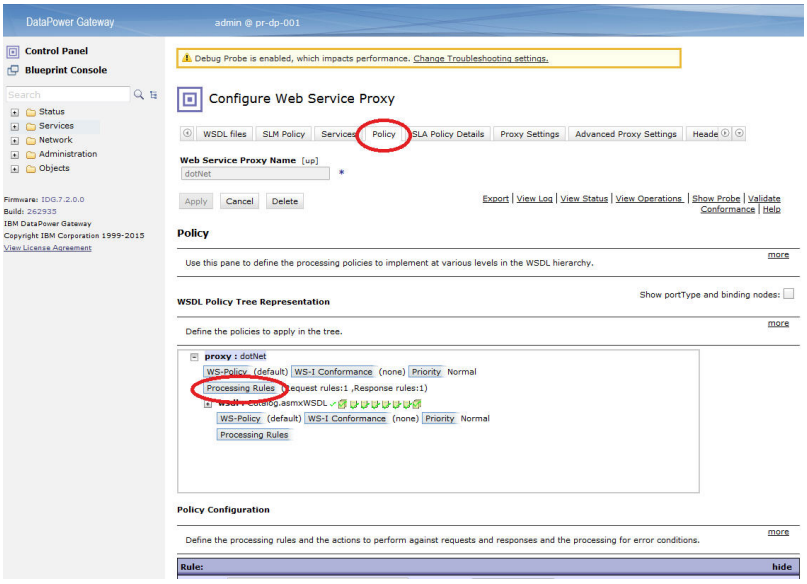
1. Faça download dos arquivos a partir do seguinte local:
   - Para sistemas Linux, `/opt/ibm/apm/agent/`*`lx8266`*`/bn/bin`
   - Para sistemas AIX, `/opt/ibm/apm/agent/`*`aix536`*`/bn/bin`
2. Faça upload de arquivos XSL em cada dispositivo DataPower que deseja monitorar como parte do Pilha de integração IBM.
3. Configure o Web Service Proxy ou o gateway multiprotocolo conforme descrito nos seguintes tópicos.
4. Para cada Domínio que deseja monitorar, configure-os com as etapas a seguir:
   a) Selecione o Domínio da lista suspensa no cabeçalho do DataPower Gateway.
   b) No navegador Painel de Controle, selecione **Objetos** > **Gerenciamento de Dispositivo** > **Web Services Management Agent**.
   c) Configure **Modo de Armazenamento em Buffer (descontinuado)** para `Descartar`.
   d) Clique em **Aplicar**.

Configurando o Web Service Proxy
Conclua estas etapas em cada Web Service Proxy que deseja exibir em topologias de instância.

Procedimento

Na WebGUI, conclua as seguintes etapas para cada Web Service Proxy que deseja monitorar:

1. Na página **Configurar Web Service Proxy**, selecione o nome do Web Service Proxy para configurar.
2. Na guia **Política**, expanda **proxy : *domain*** e clique em **Regras de Processamento**.



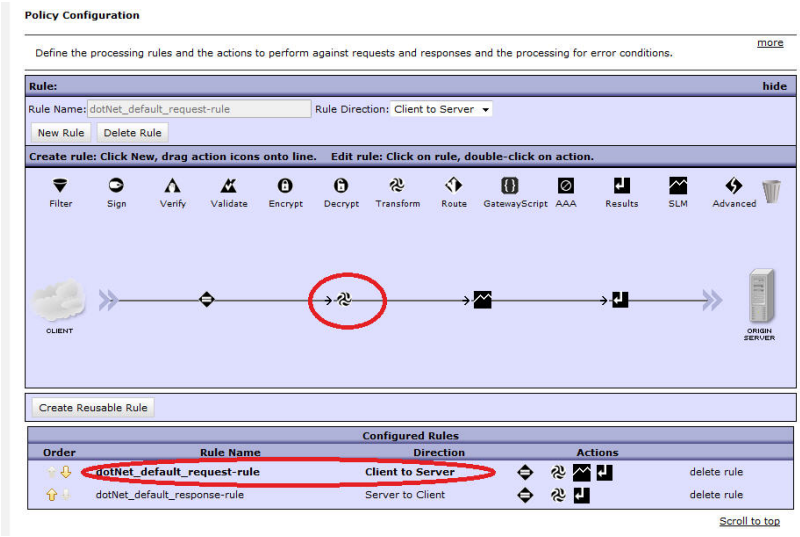
3. Na seção **Configuração de Política**, selecione uma regra `Cliente para Servidor` existente ou clique em **Nova Regra** para criar uma.

   a. Arraste uma Transformação para a linha de tempo.

      Nota:

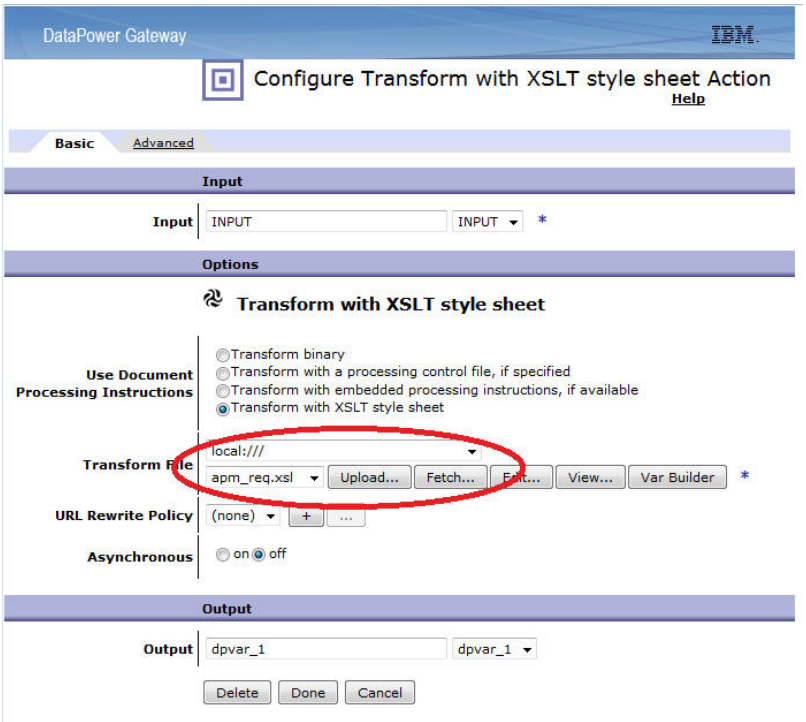
      1) Se uma regra `Cliente para servidor` já existir, inclua o nó de transformação nele.
      2) Se a regra `Cliente para Servidor` tiver um nó de Autenticação, Autorização e Auditoria (AAA), certifique-se de que o nó de transformação que inclui o arquivo xslt do agente DataPower preceda o nó AAA.

   b. Dê um clique duplo em Transformação para editá-la.



   c. Na janela **Configurar Transformação com Ação da Folha de Estilo XSLT**, próxima de Arquivo de Transformação, selecione `apm_req.xsl` a partir do armazenamento de dados para o qual você o transferiu por upload. Por exemplo, `local:///`

      Se o arquivo não existir, clique em **Upload** para obtê-lo do local instalado



Dica: Além do tráfego SOAP e REST por meio do dispositivo DataPower, se desejar configurar uma regra `Cliente para Servidor` para monitorar o tráfego entre o DataPower e o WebSphere MQ, aplique o arquivo `apm_req_MQ.xsl` em vez do arquivo `apm_req.xsl` nesta etapa.

d. Clique em **Concluído**.

4. Novamente na seção **Configuração de política**, repita a etapa 3 para configurar uma regra `Servidor para cliente` ou clique em **Nova regra** para criar uma.

   a. Arraste uma Transformação para a linha de tempo.

   b. Dê um clique duplo na Transformação para editá-la.

   c. Na janela **Configurar Transformação com Ação da Folha de Estilo XSLT**, próxima de Arquivo de Transformação, selecione `apm_rsp.xsl` a partir do armazenamento de dados para o qual você o transferiu por upload. Por exemplo, `local:///`

   Se o arquivo não existir, clique em **Upload** para obtê-lo do local instalado

   Dica: Além do tráfego SOAP e REST por meio do dispositivo DataPower, se desejar configurar uma regra `Servidor para Cliente` para monitorar o tráfego entre o DataPower e o WebSphere MQ, aplique o arquivo `apm_rsp_MQ.xsl` em vez do arquivo `apm_rsp.xsl` nesta etapa.

   d. Clique em **Concluído**.

5. Novamente na seção **Configuração de política**, repita a etapa 3 para configurar uma regra `Erro` ou clique em **Nova regra** para criar uma.

   a. Arraste uma Transformação para a linha de tempo.

   b. Dê um clique duplo na regra Transformação para editá-la.

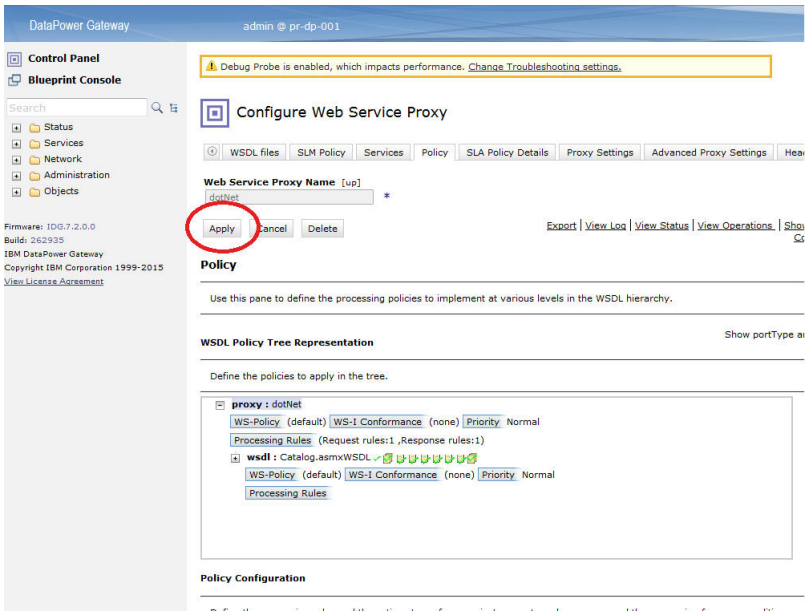
   c. Na janela **Configurar Transformação com Ação da Folha de Estilo XSLT**, próxima de Arquivo de Transformação, selecione `apm_error.xsl` a partir do armazenamento de dados para o qual você o transferiu por upload. Por exemplo, `local:///`

   Se o arquivo não existir, clique em **Upload** para obtê-lo do local instalado

   Dica: Além do tráfego SOAP e REST por meio do dispositivo DataPower, se desejar configurar uma regra de `erro` para monitorar o tráfego entre o DataPower e o WebSphere MQ, aplique o arquivo `apm_error_mq.xsl` em vez do arquivo `apm_error.xsl` nesta etapa.

   d. Clique em **Concluído**.

6. De volta à página **Configurar Web Service Proxy**, clique em **Aplicar**.



Configurando o gateway multiprotocolo

Conclua estas etapas em cada gateway multiprotocolo que deseja exibir em topologias de instância.

Procedimento

Na WebGUI, conclua as seguintes etapas para cada gateway multiprotocolo que você deseja monitorar.

1. Na página **Configurar Gateway Multiprotocolo**, clique no nome do Gateway Multiprotocolo que deseja configurar.
2. Na página **Política de Gateway Multiprotocolo**, configure a política. Clique em **...**.
3. Na página **Configurar Política de Estilo de Gateway Multiprotocolo**, selecione uma regra `Cliente para Servidor` existente ou clique em **Nova Regra** para criar uma.
   a. Arraste uma Transformação para a linha de tempo.

      Nota:

      1) Se uma regra `Cliente para servidor` já existir, inclua o nó de transformação nele.
      2) Se a regra `Cliente para servidor` tiver um nó Autenticação, Autorização e Auditoria (AAA), verifique se o nó de transformação que inclui o arquivo xslt do agente DataPower precede o nó AAA.

   b. Dê um clique duplo na regra Transformação para editá-la.
   c. Na janela **Configurar Transformação com Ação da Folha de Estilo XSLT**, próxima de Arquivo de Transformação, selecione `apm_req.xsl` a partir do armazenamento de dados para o qual você o transferiu por upload. Por exemplo, `local:///`

      Se o arquivo não existir, clique em **Upload** para obtê-lo do local instalado

      Dica: Além do tráfego SOAP e REST por meio do dispositivo DataPower, se desejar configurar uma regra `Cliente para Servidor` para monitorar o tráfego entre o DataPower e o WebSphere MQ, aplique o arquivo `apm_req_MQ.xsl` em vez do arquivo `apm_req.xsl` nesta etapa.
   d. Clique em **Concluído**.
4. De volta à página **Configurar Política de Estilo de Gateway Multiprotocolo**, selecione uma regra `Servidor para Cliente` existente ou clique em **Nova Regra** para criar uma.
   a. Arraste uma Transformação para a linha de tempo.
   b. Dê um clique duplo na regra Transformação para editá-la.
   c. Na janela **Configurar Transformação com Ação da Folha de Estilo XSLT**, próxima de Arquivo de Transformação, selecione `apm_rsp.xsl` a partir do armazenamento de dados para o qual você o transferiu por upload. Por exemplo, `local:///`

      Se o arquivo não existir, clique em **Upload** para obtê-lo do local instalado

      Dica: Além do tráfego SOAP e REST por meio do dispositivo DataPower, se desejar configurar uma regra `Servidor para Cliente` para monitorar o tráfego entre o DataPower e o WebSphere MQ, aplique o arquivo `apm_rsp_MQ.xsl` em vez do arquivo `apm_rsp.xsl` nesta etapa.
   d. Clique em **Concluído**.
5. De volta à página **Configurar Política de Estilo de Gateway Multiprotocolo**, selecione uma regra `Erro` existente ou clique em **Nova Regra** para criar uma.
   a. Arraste uma Transformação para a linha de tempo.
   b. Dê um clique duplo na regra Transformação para editá-la.
   c. Na janela **Configurar Transformação com Ação da Folha de Estilo XSLT**, próxima de Arquivo de Transformação, selecione `apm_error.xsl` a partir do armazenamento de dados para o qual você o transferiu por upload. Por exemplo, `local:///`

      Se o arquivo não existir, clique em **Upload** para obtê-lo do local instalado

      Dica: Além do tráfego SOAP e REST por meio do dispositivo DataPower, se desejar configurar uma regra de `erro` para monitorar o tráfego entre o DataPower e o WebSphere MQ, aplique o arquivo `apm_error_mq.xsl` em vez do arquivo `apm_error.xsl` nesta etapa.
   d. Clique em **Concluído**.

6. De volta à página **Configurar Política de Estilo de Gateway Multiprotocolo**, na guia **Avançado**, configure **Monitorar via Web Services Management Agent** para **ativado** e clique em **Aplicar**.
7. Clique em **Aplicar**.

O que Fazer Depois

Em alguns casos, incluir transformações para Rastreamento de Transações poderá resultar na mudança pelo DataPower do valor de cabeçalhos de Tipo de Conteúdo de HTTP. Você pode ver páginas da web com imagens que não são carregadas ou arquivos binários sendo renderizados como texto de HTML truncado.

O comportamento do DataPower muda ao comparar uma regra com não transformações de XSL com uma regra com uma ou mais transformações de XSL. Se o serviço manipular MIME, MTOM, XOP ou outras mensagens codificadas, esse comportamento pode ser desejado; caso contrário, modifique a sua configuração do DataPower para evitar o comportamento.

Para evitar que o DataPower modifique o cabeçalho de Tipo de Conteúdo de HTTP, configure a variável var://service/mpgw/proxy-content-type em cada regra afetada:

1. Arraste um objeto Avançado para a regra.
2. Clique duas vezes no objeto Avançado para editá-lo.
3. Selecione **Configurar Variável** e clique em **Avançar**.
4. Insira o Nome de Variável `service/mpgw/proxy-content-type` e o Valor da Variável `1` e clique em **Pronto**.
5. Aplique as mudanças na configuração de política e de serviço.
6. Repita as etapas 1-5 para cada regra afetada.

Configurando o DataPower agent

O Monitoring Agent for DataPower fornece um ponto central de monitoramento para o DataPower Appliances no seu ambiente corporativo. É possível identificar e receber as notificações sobre os problemas comuns com os dispositivos. O agente também fornece informações sobre desempenho, recurso e carga de trabalho para os dispositivos.

Sobre Esta Tarefa

O agente DataPower é um agente de múltiplas instâncias; você deve criar a primeira instância e iniciar o agente manualmente. O Nome do sistema gerenciado inclui o nome da instância que você especifica, por exemplo, *instance_name*:*host_name*:*pc*, em que *pc* é seu código de produto de dois caracteres. O Nome do sistema gerenciado é limitado a 32 caracteres.

O nome da instância que você especifica é limitado a 28 caracteres, menos o comprimento do nome do host. Por exemplo, se você especificar `DataPower` como o nome da instância, o nome do sistema gerenciado será `DataPower:hostname:BN`.

Importante: Se você especificar um longo nome de instância, o nome do Sistema gerenciado é truncado e o código do agente não é exibido corretamente.

Nota: O XSLT do agente DataPower não analisa caracteres BLOB usados para aplicativos mainframe.

Para cada dispositivo DataPower de produção, configure uma instância. Se os dispositivos DataPower forem aqueles pequenos ou de não produção, será possível configurar somente uma instância de agente para monitorar todos eles. Várias instâncias podem ser executadas na mesma máquina. É possível executar o script de configuração para criar uma instância e alterar quaisquer definições de configuração. É possível editar o arquivo de resposta silencioso do agente antes de executar o script para ignorar os prompts e as respostas necessárias.

Procedimento

- Para configurar o agente DataPower, execute um dos seguintes procedimentos:

- Linux AIX Para configurar o agente respondendo aos prompts, execute as seguintes etapas:

  1. Acesse o diretório *install_dir*/bin, em que *install_dir* é o diretório de instalação do agente DataPower.
  2. Execute o comando `./datapower-agent.sh config` *instance_name*.

     Escolha um *instance_name* que seja exclusivo no servidor.
  3. Quando solicitado que edite as configurações do agente DataPower, insira 1 para continuar.
  4. Quando solicitado que edite os **Detalhes do sistema gerenciado**, insira uma das seguintes opções:

     - 1=Add
     - 2=Edit
     - 3=Del
     - 4=Next
     - 5=Exit

     Se essa for a primeira vez que você configura uma instância de agente DataPower em seu sistema, a mensagem `No 'DataPower Appliances' settings available` será exibida. Insira 1 para incluir a configuração de dispositivos DataPower. O padrão é a opção `5=Exit`.
  5. Insira as propriedades para o dispositivo DataPower:

     Nome do sistema gerenciado
     Para **Nome do sistema gerenciado**, insira o nome do sistema gerenciado do agente.

     Escolha um **Nome do sistema gerenciado** que seja exclusivo entre todas as instâncias do agente e que podem ser usadas para identificar facilmente um dispositivo. O nome deve conter somente caracteres alfanuméricos, por exemplo, o nome do host do dispositivo DataPower.

     Host do Dispositivo
     Para **Host do dispositivo**, insira o endereço IP do DataPower Appliance monitorado. O endereço IP padrão é *9.123.109.139*.

     Porta da Interface de Gerenciamento de XML
     Para **Porta da Interface de Gerenciamento de XML**, digite o número da porta para a Interface de Gerenciamento de XML. O número padrão é 5550.

     ID do usuário
     Para **ID do Usuário**, digite o ID do usuário usado para efetuar login no Dispositivo DataPower monitorado. O valor padrão é admin.

     Senha
     Para **Senha**, digite a senha usada para efetuar login no Dispositivo DataPower monitorado e, em seguida, confirme a senha.

     Perfil Proxy SSL
     Para **Perfil Proxy SSL**, insira o caminho absoluto do certificado público de seu perfil proxy SSL, se a interface de gerenciamento de XML do dispositivo estiver configurada para usar o perfil. Por exemplo,

     ```
     the location of the .pem file exported from datapower appliances/mycert.pem
     ```

     em que *the location of the .pem file exported from datapower appliances* é o caminho absoluto do certificado público. Para exportar o certificado público, consulte Exportando certificado público.

     Opção de proxy SSL
     Para **Opção de proxy SSL**, configure como `Yes` se a interface de gerenciamento XML do dispositivo monitorado for configurada para usar um perfil de proxy SSL customizado. Caso contrário, selecione `Não`.

6. Para monitorar vários dispositivos DataPower, repita “4” na página 239 e “5” na página 239 para configurar uma instância de agente para cada dispositivo DataPower. Caso contrário, digite 5 e pressione **Enter** para concluir a configuração.
7. Execute o comando a seguir para iniciar o agente:

```
./datapower-agent.sh start instance_name
```

- Configuração silenciosa

1. Para configurar o agente ao editar o arquivo de resposta silenciosa e executar o script sem nenhuma interação, conclua as seguintes etapas:
   - Linux AIX Abra *install_dir*/samples/datapower_silent_config.txt em um editor de texto.
   - Windows Abra *install_dir*/samples/datapower_silent_config.txt em um editor de texto.
2. Para configurar o agente DataPower para monitorar um dispositivo, digite as seguintes propriedades:

   Host do Dispositivo
   Digite o nome do host ou o endereço IP do dispositivo. Por exemplo, **SOAP_HOST.ManageSystemName=** *datapower01*.

   Porta da Interface de Gerenciamento de XML
   Digite o número da porta para a Interface de Gerenciamento de XML. O valor padrão é 5550. Por exemplo, **DP_PORT.ManageSystemName=** *5550*.

   ID do usuário
   Digite o ID do Usuário usado para conexão com o dispositivo. O valor padrão é admin. Por exemplo, **DP_UID.ManageSystemName=** *admin*.

   Senha
   Digite a senha do ID do Usuário. Por exemplo, **DP_PASSWORD.ManageSystemName=** *password*.

   Perfil Proxy SSL
   Digite o caminho absoluto do certificado público de seu perfil proxy SSL, se a interface de gerenciamento de XML do dispositivo estiver configurada para usar o perfil. Por exemplo,

   ```
   the location of the .pem file exported from datapower appliances/mycert.pem
   ```

   em que *the location of the .pem file exported from datapower appliances* é o caminho absoluto do certificado público. Para exportar o certificado público, consulte Exportando certificado público.

   Opção de proxy SSL
   Para **Opção de proxy SSL**, configure como Yes se a interface de gerenciamento XML do dispositivo monitorado for configurada para usar um perfil de proxy SSL customizado. Caso contrário, configure-o para No. Por exemplo, **DP_SSL_OPTION.ManageSystemName1=** Yes.

   Importante: ManageSystemName é exclusivo. Substitua-o por seu próprio nome de sistema em todas as entradas. Se desejar monitorar vários dispositivos, copie e repita as etapas mostradas para monitorar um aplicativo. Lembre-se de configurar os parâmetros ManageSystemName e DataPower Appliance apropriados.
3. Acesse o diretório de instalação do agente e execute o seguinte comando para iniciar o agente:

```
./datapower-agent.sh start instance_name
```

O que Fazer Depois

- Para verificar os nomes e as configurações das instâncias do agente configuradas, execute o comando **`./cinfo -s bn`**.
- É possível verificar se os dados do DataPower agent são exibidos no console do Cloud APM. Para obter instruções sobre como iniciar o console do Cloud APM, consulte Iniciando o console do Cloud APM. Para obter informações sobre o uso do Editor de aplicativos, consulte Gerenciando aplicativos.
- Para exibir dados de rastreamento de transação no Console do Cloud APM, configure o rastreamento de transação para o DataPower agent. Para obter instruções, consulte Configurando o rastreamento de transação para o agente DataPower.
- Para exibir o monitoramento em níveis diferentes, configure o dispositivo DataPower de forma apropriada. Para obter instruções, consulte Monitoramento de recursos, Rastreamento de transações de middleware e Rastreamento de transações em nível de instância de dispositivos DataPower.

Configurando o rastreamento de transações para o DataPower agent
Para exibir dados de rastreamento de transação para dispositivos DataPower nos painéis de topologia e middleware, deve-se ativar o rastreamento de transação para DataPower agent.

Antes de Iniciar

- Instale o DataPower agent e configure-o para conectar-se ao dispositivo DataPower.
- Ative o monitoramento para SOAP ou ARM no dispositivo DataPower.

Procedimento

Para ativar o rastreamento de transação para o DataPower agent, conclua as seguintes etapas:

1. Na barra de navegação, clique em **Configuração do Sistema** > **Configuração do Agente**.
2. Na guia **DataPower**, selecione as instâncias de agente para as quais deseja ativar o rastreamento de transação.
3. Selecione **Ações** > **Configurar Rastreamento de Transação** > **Ativado** para ativar o rastreamento de transação. O status do agente na coluna de **Rastreamento de Transações** é atualizado para **Ativado**.

Resultados
Você ativou o rastreamento de transação para as instâncias de agente selecionadas.

O que Fazer Depois
Para ver dados para um dispositivo DataPower nos painéis de topologia e de middleware, agora deve-se incluir os dispositivos que você deseja monitorar no Painel de Desempenho de Aplicativo. Para obter informações adicionais sobre como incluir um dispositivo DataPower no Painel de Desempenho do Aplicativo , consulte “Incluindo aplicativos middleware no Painel de Desempenho do Aplicativo ” na página 96.

Nota: Se você estiver usando os Serviços de Integração e desejar monitorar os dados que são transmitidos entre o IBM Integration Bus e o DataPower, é necessária uma configuração adicional para mostrar uma Topologia de Transação de Agregação precisa. O IBM Integration Bus agent não pode incluir suporte de correlação para mensagens SOAP sem um envelope SOAP. Nós `SOAPRequest`, nós `SOAPAsyncRequest` e nós `SOAPReply` podem aceitar mensagens sem Envelopes SOAP como mensagens de entrada. Para esses nós, não há relacionamentos exibidos na visualização de topologia da mediação para a mediação de recebimento de dados ou servidor de aplicativos. Para evitar esse problema, insira o nó `SOAPEnvelope` imediatamente antes dos nós `SOAPRequest`, `SOAPAsyncRequest` ou `SOAPReply` no fluxo de mensagens do IBM Integration Bus e selecione a opção **Criar Novo Envelope** para o nó `SOAPEnvelope` para incluir um envelope SOAP para a mensagem SOAP.

Configurando o monitoramento do Db2

O Monitoring Agent for Db2 monitora a disponibilidade e o desempenho do Db2 Server. É possível monitorar vários servidores a partir do Console do Cloud APM; cada servidor é monitorado por uma instância do Db2. O monitoramento remoto também é suportado pelo Db2.

Antes de Iniciar

Revise os pré-requisitos de hardware e de software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Db2.

Sobre Esta Tarefa

O Db2 é um agente de várias instâncias, primeiro você deve criar a instância e, em seguida, iniciar o agente manualmente.

O nome do sistema gerenciado inclui o nome da instância do agente especificado, por exemplo, *instance_name*:*host_name*:*pc*.

Em que:

- O *pc* é o código do produto de dois caracteres.
- O *instance_name* é o nome da instância do agente e deve ser igual ao nome da instância do Db2 a ser monitorada.

O nome do sistema gerenciado pode conter até 32 caracteres. O nome da instância do agente especificado pode conter até 8 caracteres, excluindo o comprimento do nome do host. Por exemplo, se você especificar `DB2inst1` como o nome da instância de agente, o nome do sistema gerenciado será `DB2inst1:hostname:ud`.

Importante: Se você especificar um nome da instância de agente longo, o nome do sistema gerenciado será truncado e o código do agente não será exibido completamente.

Para evitar problemas de permissão ao configurar o agente, certifique-se de usar o mesmo ID do usuário raiz ou do usuário não raiz que foi usado para instalar o agente. Se você instalou o seu agente como um usuário selecionado e deseja configurar o agente como um usuário diferente, consulte “Configurando agentes como um usuário não raiz” na página 181. Se você instalou e configurou seu agente como um usuário selecionado e deseja iniciar o agente como um usuário diferente, consulte “Iniciando agentes como um usuário não raiz” na página 1012.

Execute o script de configuração para criar uma instância e altere as configurações. É possível editar o arquivo de resposta silencioso do Db2 antes de executar o script de configuração para ignorar os prompts e respostas que, de outra forma, são necessários.

Depois de configurar o Db2, certifique-se de iniciar o agente com um ID do usuário que tenha a autoridade SYSADM do Db2 para a instância monitorada. O agente requer a autoridade SYSADM para ativar todos os comutadores do monitor e coletar os dados de monitoramento. Portanto, um usuário com a autoridade SYSADM deve iniciar o agente. Use o usuário proprietário da instância, que tem a autoridade SYSADM, para iniciar o agente.

As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte “Histórico de Mudanças” na página 50.

Procedimento

Para configurar o agente com as configurações padrão, conclua as seguintes etapas:

1. Execute o comando a seguir em que *instance_name* é o nome que você deseja fornecer à instância:

```
install_dir/bin/db2-agent.sh config instance_name
 install_dir /samples/db2_silent_config.txt
```

O nome da instância do agente *instance_name* é sempre igual ao nome da instância do Db2 que está sendo monitorada. Para obter mais detalhes sobre as instâncias de agente existentes, consulte "Página Configuração do Agente" na página 180

2. Execute o seguinte comando para iniciar o Db2:

```
install_dir/bin/db2-agent.sh start instance_name
```

O que Fazer Depois

- Conceda privilégios ao usuário do Db2 para visualizar dados para alguns atributos do Db2. Para obter informações sobre a concessão desses privilégios, consulte "Concedendo privilégios para visualizar métricas do Db2" na página 247.
- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o agente nos sistemas Windows

Você pode utilizar o Use a janela do IBM Cloud Application Performance Management para configurar o agente nos sistemas Windows.

Antes de Iniciar

Antes de iniciar a configuração do Db2 para monitoramento local e remoto, certifique-se de que a seguinte tarefa esteja concluída para monitoramento remoto.

- Configure o ambiente do cliente/servidor para monitoramento remoto; consulte "Pré-requisitos para monitoramento remoto" na página 251.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **Agentes de Monitoramento IBM** > **IBM Cloud Application Performance Management**.
2. Na janela IBM Cloud Application Performance Management, clique com o botão direito em **Monitoring Agent for DB2** e, em seguida, clique em **Configurar agente**.
3. No campo **Inserir um nome de instância exclusivo**, digite o nome de instância do agente e clique em **OK**.

   Importante: Para monitoramento local, o nome da instância de agente deve corresponder ao nome da instância do Db2 que está sendo monitorada.

   Para monitoramento remoto, o nome da instância de agente deve ser o nome do nó do catálogo exclusivo.
4. Na janela **Monitoring Agent for DB2**, conclua estas etapas:
   a) Em **Nome do usuário**, insira o nome do usuário da instância do Db2.

      Para Db2 local, insira o nome do proprietário da instância do Db2.

      Para Db2 remoto, insira o nome do proprietário da instância real do Db2 da máquina remota do Db2.

      Importante: Este parâmetro é obrigatório para monitoramento remoto da instância do Db2.
   b) Em **Senha**, insira a senha da instância do Db2.

      Para Db2 local, insira a senha do proprietário da instância do Db2.

      Para Db2 remoto, insira a senha do proprietário da instância real do Db2 da máquina remota do Db2.

      Importante: Este parâmetro é obrigatório para monitoramento remoto da instância do Db2.

c) No campo **Arquivo de definição SQL DB2Customized**, insira o nome do caminho do arquivo completo para o arquivo de definição SQL. Se o arquivo de definição SQL estiver no diretório padrão, deixe esse campo em branco. Caso contrário, insira o nome do caminho do arquivo completo do arquivo. O nome do arquivo padrão com o caminho é o seguinte:

Linux AIX `CANDLEHOME/config/kudcussql.properties`

Windows `CANDLEHOME\TMAITM6_x64\kudcussql.properties`

d) No campo **Caminho do arquivo de log db2diag**, insira o caminho de diretório para o arquivo de log db2diag. Se o arquivo de log db2diag estiver no diretório padrão, deixe esse campo em branco. Caso contrário, insira o caminho do diretório. O caminho do diretório padrão é o seguinte:

Linux AIX `/home/`*`DB2owner_home_dir`*`/sqllib/db2dump`

Windows `C:\ProgramData\IBM\DB2\DB2COPY\`*`DB2INSTANCENAME`*

Nota: Este parâmetro não é aplicável para monitoramento remoto.

e) No campo **Filtro MSGID na expressão regular**, insira o *MSGID* para filtrar o log de diagnóstico. O MSGID é uma combinação do tipo de mensagem, número da mensagem e nível de gravidade. Use uma expressão regular para filtrar o log com base no tipo de mensagem, número da mensagem ou nível de severidade, por exemplo, `ADM1\d*1E|ADM222\d2W`.

f) Na lista **Ativar monitoramento para partições em hosts remotos**, selecione `Sim` para especificar que o Db2 pode monitorar partições em hosts remotos.

g) Na lista **Ativar monitoramento de todos os bancos de dados**, selecione `Sim` para especificar que o Db2 pode monitorar todos os bancos de dados.

h) Clique em **OK**.

A instância de agente é exibida na janela IBM Cloud Application Performance Management.

5. Execute as seguintes etapas para configurar o monitoramento remoto.
   a) Abra *`install_dir`*`\TMAITM6_x64\KUDENV_<instanceName>`.
   b) Configure *KUD_DB2_CLIENT_INST* para o nome da instância do cliente do Db2 com o qual a instância de servidor Db2 remoto está catalogada.
6. Clique com o botão direito na instância **Monitoring Agent for DB2** e clique em **Iniciar**.

O que Fazer Depois

- Conceda privilégios ao usuário do Db2 para visualizar dados para alguns atributos do Db2. Para obter informações sobre a concessão desses privilégios, consulte "Concedendo privilégios para visualizar métricas do Db2" na página 247.
- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o agente em sistemas Linux ou UNIX

Configure o script de configuração para configurar o agente em sistemas Linux.

Antes de Iniciar

Antes de iniciar a configuração do Db2 para monitoramento local e remoto, certifique-se de que a seguinte tarefa esteja concluída para monitoramento remoto.

- Configure o ambiente do cliente/servidor para monitoramento remoto; consulte "Pré-requisitos para monitoramento remoto" na página 251.

Procedimento

1. Execute o comando *`install_dir`*`/bin/db2-agent.sh config `*`instance_name`*

   Em que *instance_name* é o nome que você deseja dar à instância:

Importante: Para monitoramento local, o nome da instância de agente deve corresponder ao nome da instância do Db2 que está sendo monitorada.

Para monitoramento remoto, o nó local catalogado da instância remota do Db2 Server que será monitorada.

2. Quando for solicitado para fornecer um valor para os parâmetros a seguir, pressione Enter para aceitar o valor padrão, ou especifique um valor e, em seguida, pressione Enter:
   - Nome de Usuário
   - Senha
   - Caminho SQL do DB2
   - Caminho de diaglog
   - Filtro do ID de mensagem diaglog
   - Partições remotas do monitor
   - Monitorar todos os bancos de dados
3. Execute o comando a seguir para iniciar o agente:

   Para monitoramento local, execute *install_dir*/bin/db2-agent.sh start *instance_name* pelo usuário proprietário da instância do Db2.

   Para monitoramento remoto, execute *install_dir*/bin/db2-agent.sh start *node_name* com o proprietário da instância da instância do cliente do Db2 na qual a instância remota do Db2 Server está catalogada.

O que Fazer Depois

- Conceda privilégios ao usuário do Db2 para visualizar dados para alguns atributos do Db2. Para obter informações sobre a concessão desses privilégios, consulte "Concedendo privilégios para visualizar métricas do Db2" na página 247.
- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o agente usando o arquivo de resposta silencioso

Use o arquivo de resposta silencioso para configurar o agente sem responder aos prompts ao executar o script de configuração. É possível usar o arquivo de resposta silencioso para configurar o agente em sistemas Windows e Linux.

Antes de Iniciar

Antes de iniciar a configuração do Db2 para monitoramento local e remoto, certifique-se de que a seguinte tarefa esteja concluída para monitoramento remoto.

- Configure o ambiente do cliente/servidor para monitoramento remoto; consulte "Pré-requisitos para monitoramento remoto" na página 251.

Sobre Esta Tarefa

O arquivo de resposta silencioso contém os parâmetros de configuração. É possível editar os valores de parâmetros no arquivo de resposta e executar o script de configuração para criar uma instância do agente e atualizar os valores de configuração.

Procedimento

1. Em um editor de texto, abra o arquivo db2_silent_config.txt que está disponível no caminho a seguir:

   Linux AIX *install_dir* /samples/db2_silent_config.txt

Windows *install_dir*\tmaitm6_x64\samples\db2_silent_config.txt

2. No arquivo de resposta, especifique um valor para os parâmetros a seguir:
   - Em **Nome do usuário**, insira o nome do usuário da instância do Db2.

     Para Db2 local, insira o nome do proprietário da instância do Db2.

     Para Db2 remoto, insira o nome do proprietário da instância real do Db2 da máquina remota do Db2.

     Importante: Este parâmetro é obrigatório para monitoramento remoto da instância do Db2.
   - Em **Senha**, insira a senha da instância do Db2.

     Para Db2 local, insira a senha do proprietário da instância do Db2.

     Para Db2 remoto, insira a senha do proprietário da instância real do Db2 da máquina remota do Db2.

     Importante: Este parâmetro é obrigatório para monitoramento remoto da instância do Db2.
   - Para o parâmetro **DB2 SQL path**, deixe este campo em branco se o arquivo de definição SQL estiver disponível no diretório padrão. Caso contrário, insira o caminho de diretório correto. O arquivo de definição de SQL está disponível no caminho padrão a seguir:

     Linux AIX CANDLEHOME/config/kudcussql.properties Por exemplo, **KUD_DB2_SQL_PATH=** /opt/ibm/apm/agent/config/kudcussql.properties

     Windows CANDLEHOME\TMAITM6_x64\kudcussql.properties Por exemplo, **KUD_DB2_SQL_PATH=** C:\IBM\ITM\TMAITM6_x64\kudcussql.properties
   - Para o parâmetro **dialog path**, deixe este campo em branco se o arquivo de log db2diag estiver disponível no diretório padrão. Caso contrário, insira o caminho de diretório correto. O arquivo de log está disponível no caminho padrão a seguir:

     Linux AIX /home/DB2owner_home_dir/sqllib/db2dump
     Por exemplo, **KUD_DIAGLOG_PATH=** /home/db2inst1/sqllib/db2dump.

     Windows Windows Install_Driver:\ProgramData\IBM\DB2\DB2COPY \DB2INSTANCENAME
     Por exemplo, **KUD_DIAGLOG_PATH=** C:\ProgramData\IBM\DB2\DB2COPY1\DB2

     Nota: Este parâmetro não é aplicável para monitoramento remoto.
   - No campo **Filtro de ID da mensagem de diálogo** especifique o *MSGID* para filtrar o log de diagnóstico. O MSGID é uma combinação do tipo de mensagem, número da mensagem e nível de gravidade. Também é possível usar uma expressão regular, por exemplo, **KUD_DIAGLOG_MSGID_FILTER=** ADM1\d*1E|ADM222\d2W.
   - Para o parâmetro **monitor remote partitions**, insira Yes para especificar que o Db2 monitora partições em hosts remotos. Por exemplo, **KUD_MONITOR_REMOTE_PARTITIONS=** *Yes*.
   - Para o parâmetro **monitor all databases**, insira Yes para especificar se deseja que o Db2 monitore todos os bancos de dados. Por exemplo, **KUD_MONITOR_ALL_DATABASES=** *Yes*.
3. Salve e feche o arquivo db2_silent_config.txt e execute o comando a seguir

   Linux AIX *install_dir*/bin/db2-agent.sh config *instance_name* *install_dir*/samples/
   db2_silent_config.txt

   Windows *install_dir*\bin\db2-agent.bat config*instance_name* \tmaitm6_x64\samples\db2_silent_config.txt

   <instance_name> is
   - Para Db2 Server de monitoramento local: O nome da instância do Db2 Server que você deseja monitorar.
   - Para Db2 Server de monitoramento remoto: O nome do nó do catálogo da instância remota do Db2 Server.

Importante: Assegure que você inclua o caminho absoluto no arquivo de resposta silencioso. Caso contrário, os dados do agente não serão mostrados nos painéis.

4. Para Windows, abra o arquivo CANDLEHOME\TMAITM6_x64\KUDENV_<instance_name>. E edite a linha KUD_DB2_CLIENT_INST como KUD_DB2_CLIENT_INST=<client instance name under which remote Db2 server instance is cataloged>
5. Execute o comando a seguir para iniciar o agente:

   Linux AIX *install_dir*/bin/db2-agent.sh start *instance_name*

   Windows *install_dir*\bin\db2-agent.bat start instance_name

   Lembre-se: Ao monitorar a instância remota do Db2 Server a partir do UNIX ou Linux, o comando deve ser executado com o proprietário da instância do cliente com o qual cada instância do servidor remoto está catalogada.

O que Fazer Depois

- Conceda privilégios ao usuário do Db2 para visualizar dados para alguns atributos do Db2. Para obter informações sobre a concessão desses privilégios, consulte "Concedendo privilégios para visualizar métricas do Db2" na página 247.
- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Concedendo privilégios para visualizar métricas do Db2

Para monitorar recursos do Db2, um usuário do Db2 deve ter as autoridades do Db2 SYSADM, SYSCTRL, SYSMAINT e SYSMON para a instância monitorada para visualizar dados para alguns atributos do Db2.

Sobre Esta Tarefa

Para visualizar os dados de monitoramento que o agente coleta para todos os atributos no painel, o usuário do Db2 deve ter privilégios específicos. Para designar esses privilégios ao usuário do Db2, execute o arquivo de script que está presente no seguinte local:

Linux AIX *install_dir*/config/KudGrantUserPermissions.sh

Windows *install_dir*\TMAITM6_x64\KudGrantUserPermissions.bat

Um usuário do Db2 com a autoridade SYSADM pode executar o script para conceder privilégios a si mesmo ou a qualquer outro usuário do Db2. Para uma instância do Db2, use o proprietário da instância, que já tem a autoridade SYSADM para executar o script para conceder outras permissões a si mesmo ou para conceder todas as permissões a qualquer outro usuário do Db2.

Procedimento

1. Para monitoramento local, consulte as seguintes etapas.
   a) No sistema em que o Db2 está instalado, abra a interface da linha de comandos do Db2.
   b) Execute o seguinte comando, em que *instance_name* é o nome da instância do Db2 e *username* é o nome do usuário do Db2:

      Linux AIX *install_dir*/config/KudGrantUserPermissions.sh *instance_name username*

      Windows *install_dir*\TMAITM6_x64\KudGrantUserPermissions.bat *instance_name username*

      Nota: Para sistemas Windows, *username* é opcional no comando. Se um nome do usuário não for especificado no comando, os privilégios serão designados ao usuário padrão (sistema).
2. Para monitoramento remoto, consulte as seguintes etapas.

a) Copie KudGrantUserPermissions.sh para Unix ou Linux e KudGrantUserPermissions.bat para Windows de *install_dir*/TMAITM6_x64/ da estação de trabalho do agente para a máquina do Db2 Server.

b) Execute o seguinte comando a partir do usuário proprietário da instância do Db2, em que *instance_name* é o nome da instância do Db2 e *username* é o nome do usuário do Db2:

Linux AIX `./KudGrantUserPermissions.sh instance_name username`

Windows `KudGrantUserPermissions.bat instance_name username`

Lembre-se: Para monitoramento do Db2 remoto no Windows, o *username* deve ser o nome do usuário fornecido durante a configuração do Db2 na estação de trabalho do cliente.

Configurando as variáveis de ambiente local

É possível configurar as variáveis de ambiente local para alterar o comportamento do Db2.

Procedimento

1. Em sistemas Windows, clique em **Iniciar** > **Todos os Programas** > **Agentes de Monitoramento IBM** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, no menu **Ações**, clique em **Avançado > Editar Arquivo ENV**.
3. Em sistemas Linux ou AIX, acesse a linha de comandos e edite o arquivo ud.environment no diretório install_dir/config. Em que install_dir é o diretório de instalação do agente.

   Nota: O arquivo ud.environment é um arquivo oculto.
4. No arquivo de variável de ambiente, insira valores para as variáveis de ambiente.

   Para obter informações sobre as variáveis de ambiente que podem ser configuradas, consulte "variáveis de ambiente local" na página 248.

variáveis de ambiente local

É possível alterar o comportamento do Db2, configurando as variáveis de ambiente local.

Variáveis para definir o método de coleta de dados para o conjunto de dados do espaço de tabela

Para configurar o método para coleta de dados do conjunto de dados de espaço de tabela, use as seguintes variáveis de ambiente:

- **KUD_T1_BY_SQL**: use esta variável para configurar o método de coleta de dados para o conjunto de dados de espaço de tabela usando consultas SQL. Para ativar a coleta de dados usando consultas SQL, configure o valor desta variável como Y. Para coletar dados para o conjunto de dados de espaço de tabela usando o método de captura instantânea, configure o valor desta variável como N. O valor padrão desta variável é N.

  Importante: Para coletar dados usando consultas SQL, a versão do Db2 deve ser 9.7 ou mais recente. Além disso, o usuário que inicia o Db2 deve ter a autoridade SYSADM para todos os bancos de dados.
- **KUD_T1_DISABLE**: use esta variável para desativar a coleta de dados para o conjunto de dados de espaço de tabela. Para ativar a coleta de dados para o conjunto de dados de espaço de tabela, configure o valor desta variável como N. Para desativar a coleta de dados para o conjunto de dados de espaço de tabela, configure o valor desta variável como Y. O valor padrão desta variável é N.

Variável para a exclusão dos nós do recurso de armazenamento em cache (CF) da coleta de dados

Para excluir nós do recurso de armazenamento em cache (CF) a partir do algoritmo de coleta de dados no ambiente do pureScale, use a variável **DB2_CF_PARTITION_NUMS**. No arquivo de ambiente do agente, configure a variável **DB2_CF_PARTITION_NUMS** como DB2_CF_PARTITION_NUMS=<CF node number>. Por exemplo, DB2_CF_PARTITION_NUMS=1. Para mais de um nó CF, configure o valor da variável **DB2_CF_PARTITION_NUMS** como uma lista que usa qualquer símbolo especial de #. :,; | @

como delimitador. Por exemplo, DB2_CF_PARTITION_NUMS=12,13,23,34. Nenhum valor padrão é configurado para essa variável.

Variável para a limitação da coleção de dados para o conjunto de dados da tabela Db2

Para configurar o número máximo de linhas que o Db2 deve retornar, ao coletar dados para o conjunto de dados da tabela Db2, use a variável de ambiente **KUD_TABLE_NUMBER**. O valor padrão é 10000.

Variável para configurar o intervalo de recarregamento do arquivo de propriedades SQL customizado

Para configurar o intervalo de tempo de recarregamento (em segundos) para o arquivo de propriedades SQL customizado, use a variável **KUD_CUS_SQL_INTERVAL**. O valor padrão é 20 segundos.

Variável para limitar as linhas na coleta de dados para o conjunto de dados de Evento de agente

Para configurar o número de linhas para coleta de dados do conjunto de dados de Evento de agente, use a variável **KUD_AGENT_EVENT_CACHE**. O conjunto de dados de Evento de agente fornece informações detalhadas sobre eventos predefinidos e acionados e determina problemas com o funcionamento do banco de dados monitorado. O valor padrão é 50.

Variável para a limitação das linhas na coleta de dados para o conjunto de dados de Registro de log do Db2

Para configurar o número de linhas para a coleta de dados do conjunto de dados de Registro de log do Db2, use a variável **KUD_DBHISTORY_MAXROW**. O conjunto de dados de Registro de log do Db2 fornece informações históricas sobre o log de archive do Db2. O valor padrão é 500.

Variáveis para definir a coleta de dados para o conjunto de dados de Log de diagnóstico do Db2

Para configurar o método para a coleta de dados do conjunto de dados de Log de diagnóstico do Db2, use as variáveis de ambiente a seguir:

- **KUD_DIAGLOG_BY_TABLE**: use essa variável para configurar o método de coleta de dados para o conjunto de dados de Log de diagnóstico do Db2. Se o valor dessa variável for configurado como Y, os dados para o conjunto de dados de Log de diagnóstico do Db2 serão coletados usando consultas SQL. Se o valor dessa variável for configurado como N, os dados para o conjunto de dados de Log de diagnóstico do Db2 serão coletados analisando o db2diag.log. O valor padrão dessa variável é Y.

  Importante: Para coletar dados usando consultas SQL, a versão do Db2 deve ser 10 ou mais recente.
- **KUD_DIAGLOG_TAILCOUNT**: Use esta variável para definir o número de linhas do arquivo db2diag.log que o Db2 analisa para coletar dados para o conjunto de dados de Log de diagnósticos do DB2. Esta variável limita o Db2 para processar o arquivo de log do Db2 para que apenas as mensagens e eventos mais recentes sejam monitorados. O valor padrão dessa variável é 1000.
- **KUD_DIAGLOG_CACHE**: use essa variável para limitar o número de registros de log que são exibidos no painel para o conjunto de dados de Log de diagnóstico do Db2. O valor padrão dessa variável é 20.
- **KUD_DIAGLOG_INTERVAL**: use essa variável para definir o intervalo de tempo de recarregamento (em segundos) para o arquivo db2diag.log para a coleta de dados para o conjunto de dados de Log de diagnóstico do Db2. O valor padrão desta variável é 30 segundos.
- **KUD_DISABLE_DIAGLOG**: use essa variável para desativar a coleta de dados para o conjunto de dados de Log de diagnóstico do Db2. Para ativar a coleta de dados para o conjunto de dados de Log de diagnóstico do Db2, configure o valor dessa variável como N. Para desativar a coleta de dados para o conjunto de dados de Log de diagnóstico do Db2, configure o valor dessa variável como Y. O valor padrão dessa variável é N.

Variável para configuração do intervalo de tempo limite de consulta

Se uma consulta SQL demorar muito para concluir, isso afeta o desempenho do Db2. Para configurar o intervalo de tempo limite de consulta para o Db2, use a variável **KUD_QUERY_TIMEOUT**. Use esta variável para definir a quantidade máxima de tempo (em segundos) que o Db2 espera para receber uma resposta

de uma consulta enviada para o Db2 Server. O valor para esta variável deve ser menor que 300 segundos. O valor padrão dessa variável é 45 segundos.

Variável para definir a coleta de dados para o conjunto de dados DB2 Database01 (Substituído)

O agente não deve ativar consultas ASN para coletar dados para o conjunto de dados DB2 Database01 (Substituído) quando esquemas ASN não estão presentes. Para ativar a execução das consultas ASN, use a variável **KUD_REPLICATION_ON**. Se o valor desta variável estiver configurado como Y, o Db2 executará consultas ASN mesmo quando os esquemas ASN não estiverem presentes. Se o valor dessa variável for configurado como N, o Db2 não executará as consultas ASN. O valor padrão dessa variável é Y.

Variável para configurar os comutadores do monitor ao coletar dados usando o método de captura instantânea

Se você desejar coletar os dados de monitoramento do Db2 usando o método de captura instantânea, ative o comutador do monitor do Db2 para o conjunto de dados. Para ativar o comutador do monitor do Db2, use a variável **KUD_MON_SWITCH_OVERRIDE**. A lista de comutadores do monitor do Db2 é a seguinte:

BLOQUEIO
Informações de Bloqueio

SORT
Classificando Informações

STATEMENT
Informações sobre a Instrução ISQL

TABELA
Informações de atividade da tabela

TIMESTAMP
Obter informações de registro de data e hora

UOW
Informações da Unidade de trabalho

Se o valor dessa variável for configurado como Y, o Db2 reterá a definição de configuração dos comutadores do monitor do Db2. Se o valor dessa variável for configurado como N, o Db2 ativará todos os comutadores do monitor para coletar dados. O valor padrão dessa variável é N.

Variável para rastrear os dados em buffer de captura instantânea do Db2 de um conjunto de dados

Para visualizar os dados coletados para um conjunto de dados usando o método de captura instantânea, use a variável **KUD_SNAPSHOT_DUMPOUT**. Se o valor dessa variável for configurado como Y, o Db2 fará dump dos dados em buffer de captura instantânea para grupos de atributos no arquivo de log do agente. Se o valor dessa variável for configurado como N, o Db2 não fará dump dos dados em buffer de captura instantânea no arquivo de log do agente. O valor padrão dessa variável é N.

Variável para rastrear o Db2 usando os dados em buffer de captura instantânea de um conjunto de dados

Para rastrear o Db2 usando os dados em buffer de captura instantânea que são coletados para um conjunto de dados, use a variável **KUD_SNAPSHOT_READIN**. Para ativar o rastreio do Db2, configure o valor dessa variável como Y. Para desativar o rastreio do Db2, configure o valor dessa variável como N.

Variável para definir o método de coleta de dados para o conjunto de dados de Conflito de bloqueio

Para configurar o método de coleta de dados para o conjunto de dados de Conflito de bloqueio, use a variável **KUD_LOCKCONFLICT_BY_SQL**. Para coletar dados para o conjunto de dados de Conflito de bloqueio usando consultas SQL, configure o valor dessa variável como Y. Para coletar dados para o conjunto de dados de Conflito de bloqueio usando o método de captura instantânea, configure o valor dessa variável como N. O valor padrão dessa variável é Y.

Importante: Para coletar dados usando consultas SQL, a versão do Db2 deve ser 9.7 FP1 ou mais recente. Além disso, o usuário que inicia o Db2 deve ter autoridade SYSADM para todos os bancos de dados.

Variável para monitorar o Db2 Server remoto no Windows

KUD_DB2_CLIENT_INST: Configure esta variável como o nome da instância do cliente Db2 com o qual a instância do Db2 Server remoto é catalogada. É preciso configurar esta variável apenas se você estiver usando o monitoramento remoto em que o agente está no Windows.

Pré-requisitos para monitoramento remoto

É possível usar o Monitoring Agent for Db2 para monitoramento remoto. Consulte o tópico para pré-requisitos de monitoramento remoto do Db2.

Sobre Esta Tarefa

Para monitoramento remoto do Db2, primeiro você deve fazer a configuração básica do ambiente do cliente/servidor do Db2. Faça essa configuração para Windows e UNIX ou Linux.

Para esta configuração, um usuário deve ter autoridade SYSADM ou SYSCTRL do Db2.

Lembre-se: Execute todas as etapas na estação de trabalho do agente, exceto a etapa 2.

Procedimento

1. Na estação de trabalho do Db2, instale o cliente Db2. A versão desse cliente deve ser maior ou igual à versão da instância do Db2 Server que será monitorada.
2. Verifique se o protocolo de comunicação da instância do Db2 é TCPIP.
   a) Para verificar, execute o comando **db2set** na `linha de comandos` do Db2.
   b) Se ele não for configurado para TCPIP, execute **db2set DB2COMM=tcpip** na `linha de comandos` do Db2.

   Importante: Esta etapa é executada no lado do servidor.
3. Catalogue a instância do servidor remoto na estação de trabalho do agente do Db2 com o seguinte comando.

   Importante: A instância do servidor deve ser catalogada na instância do cliente. Portanto, execute o seguinte comando na instância do cliente.

   db2=>CATALOG TCPIP NODE<node_name> REMOTE <hostname/ip_address> SERVER <service_name/port_number>

   no Db2, em que

   a. *<node_name>* representa um apelido local da instância do Db2 no componente do cliente.

      Nota: Para UNIX ou Linux, *<node_name>* não deve ser igual a nenhum nome da instância do cliente Db2 ou do servidor Db2 disponível na mesma estação de trabalho.

   b. <hostname/ip_address> representa o nome ou endereço IP da estação de trabalho do Db2 Server.

   c. <service_name/port_number> em que o TCPIP do Db2 foi configurado.

   Para catalogar a instância do servidor Db2 em execução no número da porta 50000 no servidor remoto "**myserver**" como o nó "db2node", insira o seguinte comando a partir da linha de comandos do Db2

   db2 => CATALOG TCPIP NODE db2node REMOTE myserver SERVER 50000

   Para obter mais detalhes sobre o nó do catálogo, consulte https://www.ibm.com/support/knowledgecenter/SSEPGG_11.1.0/com.ibm.db2.luw.qb.client.doc/doc/t0005621.html
4. Se a estação de trabalho do Db2 for UNIX/Linux,
   - Crie um usuário com o nome do nó, que é usado no comando de catálogo

Emita o comando

useradd -g <group> -m -d <home_dir> <user> -p <password>

em que

- **<group>** representa um grupo de proprietários de instância do DB2 UDB.
- **<user>** representa um **username** local na estação de trabalho do cliente. **Userame** deve ser igual ao nome do nó pelo qual a instância do servidor foi catalogada na máquina do agente

- Marque o nome da instância do cliente do Db2 com o qual a instância remota do Db2 Server é catalogada e designe as permissões de leitura, gravação e execução do diretório inicial do usuário recém-criado ao proprietário dessa instância. Esta etapa é necessária para disponibilizar o ambiente do Db2 do cliente para operações no nó remoto
- Emita o comando

  chmod -R 775 /home/<nodename>

  em que

  - **<nodename>** representa um nome do usuário local da instância do Db2 no componente do cliente

5. Catalogue todos os bancos de dados que você deseja monitorar na instância do cliente presente na estação de trabalho do Db2.

   Emita o comando no CLP do Db2 para catalogar o banco de dados.

   CATALOG DATABASE <db_name> AS <db_alias> AT NODE <node_name>authentication server

   a. <db_name> representa o nome do banco de dados do servidor.

   b. <db_alias> representa o apelido local para o banco de dados no cliente Db2.

   c. <node_name> representa um apelido local da instância do Db2 no componente do cliente no qual o banco de dados está catalogado.

   Para catalogar um banco de dados chamado "sample" no nó do catálogo "db2node" com o alias como "dbAlias1", insira o seguinte comando a partir de um prompt do Db2.

   db2 => CATALOG DATABASE sample AS dbAlias1 AT NODE db2node authentication server

Configurando o monitoramento do Hadoop

Você deve configurar o Monitoring Agent for Hadoop para que o agente possa coletar dados de um cluster Hadoop que ele monitora. O agente pode monitorar um cluster Hadoop de único nó e um cluster Hadoop multinós.

Antes de Iniciar

Revise os pré-requisitos de hardware e software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Agente do Hadoop.

Certifique-se de que os seguintes hosts possam ser resolvidos no computador em que o Agente do Hadoop está instalado:

- Todos os hosts Hadoop que você deseja configurar, como NameNode, ResourceManager e outros
- Hosts Hadoop somente com a função NodeManager

Por exemplo, é possível concluir essas etapas para resolver hosts:

- Inclua o endereço IP, nome do host e nome completo do domínio de todos os hosts Hadoop no arquivo `hosts` que está disponível no seguinte caminho:
  - Windows `C:\Windows\System32\drivers\etc\hosts`

– Linux AIX `/etc/hosts`

- Inclua o computador no qual o Agente do Hadoop está instalado no mesmo domínio que o dos hosts Hadoop.

Lembre-se: Para monitorar um cluster Hadoop que é protegido com autenticação baseada em Kerberos SPNEGO, certifique-se de que todos os hosts possam ser resolvidos no computador onde o Agente do Hadoop está instalado.

Sobre Esta Tarefa

O Agente do Hadoop é um agente de instância única. Deve-se configurar o agente manualmente após sua instalação. O Agente do Hadoop pode ser configurado em sistemas Windows, Linux e AIX.

Lembre-se:

- Para um cluster Hadoop de um único nó, o mesmo nó executa todas as funções, como NameNode, ResourceManager e secondary NameNode, de acordo com a configuração do cluster Hadoop. No entanto, para um cluster Hadoop multinós, diferentes nós Hadoop desempenham essas funções.
- Quando o agente é configurado, ele detecta automaticamente DataNodes e NodeManagers no cluster Hadoop que está sendo monitorado.

Quando fizer upgrade do agente baseado em soquete (8.1.2 Fix Pack 2 ou anterior) para o agente baseado em API REST (8.1.3 ou mais recente), conclua as etapas de configuração especificadas nos tópicos subsequentes. No entanto, certifique-se de especificar os nomes do host de acordo com as seguintes diretrizes quando configurar o agente.

- O nome do host de vários processos daemon (NameNode, ResourceManger e outros) que você especifica deve ser igual (maiúsculas e minúsculas e formato) aos nomes do host que estão configurados para o agente baseado em soquete.
- O nome completo do domínio (FQDN) deve ser usado ao especificar um nome do host. Por exemplo, `hos1.ibm.com`. Se o comprimento do FQDN exceder 25 caracteres, especifique somente o nome abreviado do host sem o nome de domínio. Por exemplo, se o FQDN de um host for *myhadoopclustersetupnode.ibm.com*, o nome abreviado do host será `myhadoopclustersetupnode`.

Depois de configurar o agente atualizado e de visualizar dados no Console do Cloud APM, reverta as mudanças que foram feitas no arquivo `hadoop-metrics2.properties` para o Agente do Hadoop. Para obter detalhes, consulte “Fazendo upgrade de agentes” na página 1139.

Em sistemas Windows, é possível executar o Agente do Hadoop com um usuário não administrador. No entanto, esse usuário requer uma permissão específica para visualizar dados nos painéis. Para obter informações sobre como conceder esta permissão, consulte “Concedendo permissão a usuários não administrativos” na página 261.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte o “Histórico de Mudanças” na página 50.

Configurando o agente nos sistemas Windows

É possível configurar o agente em sistemas Windows usando a janela **IBM Performance Management**.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito em **Monitoring Agent for Hadoop**.
3. Clique em **Configurar Agente**.

Atenção: Se **Configurar agente** estiver desativado, clique em **Reconfigurar**.

A janela **Configurar Monitoring Agent for Hadoop** é aberta.

4. Para monitorar o cluster Hadoop com a autenticação baseada em Kerberos SPNEGO ativada, conclua estas etapas:
   a) Em **É autenticação baseada em Kerberos SPNEGO para serviços do Hadoop baseados em HTTP no cluster Hadoop ativado**, clique em **Sim**.

      Se você não tiver a autenticação baseada em Kerberos SPNEGO para proteger terminais REST de serviços Hadoop baseados em HTTP no cluster Hadoop, clique em **Não** e os valores para os campos **Nome da região** , **Nome do host KDC**, **Nome do principal SPNEGO** e **Arquivo keytab SPNEGO** poderão ser mantidos em branco.

   b) No campo **Nome da região**, insira o nome da região do Kerberos que é usada para criar principais de serviço.
      Geralmente, um nome da região é igual ao nome de domínio. Por exemplo, se seu computador estiver no domínio `tivoli.ibm.com`, o nome da região do Kerberos será `TIVOLI.IBM.COM`. Este nome faz distinção entre maiúsculas e minúsculas.

   c) No campo **Nome do host do KDC**, insira o nome completo do domínio (FQDN) do host do centro de distribuição de chaves (KDC) para a região especificada.

      Também é possível especificar o endereço IP do host do KDC em vez do FQDN. No caso de Active Directory KDC, o controlador de domínio é o host do KDC.

   d) No campo **Nome do principal SPNEGO**, insira o nome do Kerberos principal que é usado para acessar terminais REST autenticados por SPNEGO de serviços baseados em HTTP.

      O nome faz distinção entre maiúsculas e minúsculas e o formato do nome é HTTP/*fully_qualified_host_name*@*kerberos_realm*

   e) No campo **Arquivo keytab do SPNEGO**, insira o nome do arquivo keytab para o serviço do SPNEGO com seu caminho completo ou clique em **Procurar** e selecione-o.

      O arquivo keytab contém os nomes de principais de serviço e chaves do Kerberos. Esse arquivo fornece acesso direto aos serviços do Hadoop sem requerer uma senha para cada serviço. O arquivo pode estar localizado no caminho a seguir: `etc/security/keytabs/`
      Assegure que o nome do principal e o arquivo keytab do SPNEGO pertençam ao mesmo host. Por exemplo, se o nome do principal é *HTTP/abc.ibm.com@IBM.COM*, o arquivo keytab que é usado deve pertencer ao host *abc.ibm.com*.
      Se o agente for instalado em um computador remoto, copie o arquivo keytab do principal para o computador remoto em qualquer caminho e, em seguida, especifique este caminho no campo **Arquivo keytab SPNEGO**.

   f) Clique em **Avançar**.
5. Para monitorar o cluster Hadoop com HTTPS/SSL ativado, conclua estas etapas:
   a) Em **O SSL do Hadoop Cluster está ativado?**, clique em **Sim**

      Se você não quiser que o cluster do Hadoop seja ativado por SSL selecione **Não** e, em seguida, os valores para o **TrustStore file path**, os campos **TrustStore Password** podem ser mantidos como em branco.

   b) No **Caminho de arquivo do trustStore**, selecione o arquivo TrustStore armazenado em sua máquina local.

      Esse arquivo pode ser copiado do cluster do Hadoop para a sua máquina local e, em seguida, usado para configuração.

   c) Em **TrustStore Password**, insira a senha criada ao configurar o arquivo TrustStore.
6. Para especificar valores para os parâmetros do cluster Hadoop, conclua estas etapas:
   a) No campo **Nome do Cluster Hadoop Exclusivo**, insira o nome exclusivo do cluster Hadoop indicando a versão e o tipo do Hadoop. O limite máximo de caracteres para este campo é 12.

   b) No campo **NameNode Hostname**, insira o nome do host do nó onde o processo daemon para NameNode é executado.

c) No campo **NameNode Port**, insira o número da porta que está associado ao processo daemon para NameNode. O número padrão da porta é 50070.

d) No campo **ResourceManager Hostname**, insira o nome do host do nó onde o processo daemon para ResourceManager é executado.

e) No campo **ResourceManager Port**, insira o número da porta que está associado ao processo daemon para ResourceManager. O número padrão da porta é 8088.

f) Opcional: No campo **JobHistoryServer Hostname**, insira o nome do host do nó onde o processo daemon para JobHistoryServer é executado.

g) Opcional: No campo **JobHistoryServer Port**, insira o número da porta que está associado ao processo daemon para JobHistoryServer. O número padrão da porta é 19888.

h) Opcional: No campo **Additional NameNode Hostname**, insira o nome do host onde o processo daemon para um Standby NameNode ou um Secondary NameNode é executado.

i) Opcional: No campo **Additional NameNode Port**, insira o número da porta que está associado ao processo daemon para um Standby NameNode ou um Secondary NameNode.

Lembre-se: Se o NameNode adicional for um Standby NameNode, o número padrão da porta associado ao processo daemon do Standby NameNode será 50070. Se o NameNode adicional for um Secondary NameNode, o número padrão da porta associado ao processo daemon do Secondary NameNode será 50090.

j) Clique em **Testar conexão** para verificar a conexão com os nomes de hosts e portas especificados.

Após clicar em **Conexão de teste**, uma mensagem de validação apropriada será exibida quando:

- A conexão com os nomes de host e com as portas especificados foi concluída ou falhou.
- Um valor para um nome do host é mantido como blank.
- Um valor para uma porta é mantido em branco.
- Um valor de número não inteiro é especificado para um número de porta.

Atualize os valores de configuração conforme sugerido nas mensagens de validação e verifique a conexão novamente.

k) Opcional: Para incluir ResourceManagers de espera no cluster Hadoop, clique em **Sim** em **ResourceManager(s) de espera no cluster Hadoop**.

É solicitado que inclua os detalhes de ResourceManagers de espera posteriormente.

l) Opcional: Para monitorar serviços Hadoop no cluster Hadoop que é gerenciado pelo Apache Ambari, clique em **Sim** em **Monitoramento de serviços Hadoop para instalações de Hadoop baseadas em Ambari** e, em seguida, clique em **Avançar**.

7. Opcional: Para especificar os detalhes do servidor Ambari para monitorar serviços Hadoop, conclua as seguintes etapas:

a) No campo **Nome do host do servidor Ambari**, insira o nome do host onde o servidor Ambari é executado.

b) No campo **Porta do servidor Ambari**, insira o número da porta que está associado ao servidor Ambari.
O número da porta padrão é 8080.

c) No campo **Nome do Usuário do Ambari**, insira o nome do usuário do Ambari.

d) No campo **Senha do usuário do Ambari**, insira a senha do usuário do Ambari.

e) Clique em **Avançar**.

8. Para especificar valores para os parâmetros Java, conclua estas etapas:

a) Na lista **Nível de rastreio Java**, selecione um valor para o nível de rastreio que é usado por provedores Java.

b) Opcional: No campo **Argumentos da JVM**, especifique uma lista de argumentos para a Java virtual machine.

A lista de argumentos deve ser compatível com a versão de Java que está instalada junto com o agente.

c) Clique em **Avançar**.

9. Opcional: Para incluir o Standby ResourceManagers, conclua as etapas a seguir:
   a) Clique em **Novo**.
   b) No campo **Standby ResourceManager Hostname**, insira o nome do host do nó onde o processo daemon para Standby ResourceManager é executado.
   c) No campo **Standby ResourceManager Port**, insira o número da porta que está associado ao processo daemon para Standby ResourceManager. O número padrão da porta é 8088.
   d) Clique em **Testar conexão** para validar a conexão com o nome do host e o número da porta especificados.

      Após clicar em **Conexão de teste**, uma mensagem de validação apropriada será exibida quando:

      - A conexão com os nomes de host e com as portas especificados foi concluída ou falhou.
      - Um valor para um nome do host é mantido como blank.
      - Um valor para uma porta é mantido em branco.
      - Um valor de número não inteiro é especificado para um número de porta.

      Atualize os valores de configuração conforme sugerido nas mensagens de validação e verifique a conexão novamente.
   e) Repita as etapas a, b e c para incluir mais Standby ResourceManagers.

      Se desejar remover qualquer um dos Standby ResourceManagers, clique em **Excluir** correspondente ao Standby ResourceManager que você deseja remover.
   f) Clique em **Avançar**.
10. No campo **Caminho da classe para jars externos**, especifique o caminho da classe para arquivos JAR.

    Esse caminho da classe é incluído no caminho da classe que é gerado pelo agente. É possível manter esse campo em branco.
11. Clique em **OK**.

    As definições de configuração especificadas são salvas.
12. Clique com o botão direito em **Monitoring Agent for Hadoop** e clique em **Iniciar**.

O que Fazer Depois

1. Ative os eventos de subnó para visualizar os limites de acontecimentos do Agente do Hadoop. Para obter informações sobre como ativar eventos do subnó, consulte "Configurando o painel para visualizar eventos Hadoop" na página 261.
2. Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o agente nos sistemas Linux e AIX

Execute o script de configuração e responda aos prompts para configurar o agente nos sistemas Linux e AIX.

Procedimento

1. Na linha de comandos, execute o seguinte comando: *install_dir*/bin/hadoop-agent.sh config
   Em que *install_dir* é o diretório de instalação do agente Hadoop.

   O agente é instalado no seguinte diretório de instalação padrão: /opt/ibm/apm/agent

2. Quando a linha de comandos exibe a mensagem a seguir, digite 1 para continuar com as etapas de configuração e pressione Enter.
   `Edit "Monitoring Agent for Hadoop" setting? [1= yes, 2= No]`
3. Quando a linha de comandos exibir a seguinte mensagem, digite 1 para especificar valores para monitorar o cluster Hadoop com a autenticação baseada em Kerberos SPNEGO ativada e pressione Enter. Caso contrário, digite 2 e pressione Enter, e é possível manter um valor em branco para os campos **Nome da região**, **Nome do host KDC**, **Nome do principal SPNEGO** e **Arquivo keytab SPNEGO**:
   `Is Kerberos SPNEGO-based authentication for HTTP based Hadoop services in Hadoop cluster enabled\: [ 1=Yes, 2=No (default is: 2)`
   a) Para o parâmetro **Nome da região**, insira o nome da região do Kerberos que é usada para criar principais de serviço.
   Geralmente, um nome da região é igual ao nome de domínio. Por exemplo, se o seu computador estiver no domínio `tivoli.ibm.com`, o nome da região do Kerberos será `TIVOLI.IBM.COM`. Este nome faz distinção entre maiúsculas e minúsculas.
   b) No campo **Nome do host do KDC**, insira o nome completo do domínio (FQDN) do host do centro de distribuição de chaves (KDC) para a região especificada. Também é possível especificar o endereço IP do host do KDC em vez do FQDN. No caso do KDC do Active Directory, o Controlador de domínio é o host do KDC
   c) Para o parâmetro **Nome do principal SPNEGO**, insira o nome do Kerberos principal que é usado para acessar terminais REST autenticados por SPNEGO de serviços baseados em HTTP.
   O nome faz distinção entre maiúsculas e minúsculas e o formato do nome é HTTP/*fully_qualified_host_name*@*kerberos_realm*
   d) Para o parâmetro de **Arquivo keytab do SPNEGO**, insira o nome do arquivo keytab para o serviço do SPNEGO com seu caminho completo.
   O arquivo keytab contém os nomes de principais de serviço e chaves do Kerberos. Esse arquivo fornece acesso direto aos serviços do Hadoop sem requerer uma senha para cada serviço. O arquivo pode estar localizado no caminho a seguir: `etc/security/keytabs/`
   Assegure que o nome do principal e o arquivo keytab do SPNEGO pertençam ao mesmo host. Por exemplo, se o nome do principal é *HTTP/abc.ibm.com@IBM.COM*, o arquivo keytab que é usado deve pertencer ao host *abc.ibm.com*.
   Se o agente for instalado em um computador remoto, copie o arquivo keytab do principal para o computador remoto em qualquer caminho e, em seguida, especifique este caminho para o parâmetro **Arquivo keytab SPNEGO**.
4. Quando a linha de comandos exibe a seguinte mensagem, digite 1 para especificar valores para monitoramento do cluster Hadoop com o SSL ativado e pressione **Enter**. Caso contrário, digite 2 e pressione **Enter** e será possível manter um valor em branco para os campos **TrustStore file path** e **TrustStore Password**:
   `Is Hadoop Cluster SSL enabled [ 1=Yes, 2=No (default is: 2)`
   a) No **`TrustStore file path`**, especifique o caminho do arquivo TrustStore em sua máquina local.
   Esse arquivo pode ser copiado do cluster do Hadoop para a sua máquina local e, em seguida, usado para configuração.
   b) Em **`TrustStore Password`**, especifique a senha criada durante a configuração do arquivo TrustStore.
5. Quando for solicitado que insira os detalhes do cluster Hadoop, especifique um valor apropriado para cada um dos seguintes parâmetros e pressione Enter.
   a) No **Unique Hadoop Cluster Name**, especifique o nome exclusivo para o cluster Hadoop indicando a versão e o tipo do Hadoop. O limite máximo de caracteres para este campo é 12.
   b) Para o parâmetro **`NameNode Hostname`**, especifique o nome do host do nó onde o processo daemon para NameNode é executado e pressione Enter.

Atenção: Se você pressionar Enter sem especificar um nome do host, será solicitado a inserir o nome do host.

c) Para o parâmetro **NameNode Port**, especifique o número da porta que está associado ao processo daemon para NameNode e pressione Enter. O número padrão da porta é 50070.

d) Para o parâmetro **ResourceManager Hostname**, especifique o nome do host do nó onde o processo daemon para ResourceManager é executado e pressione Enter.

Atenção: Se você pressionar Enter sem especificar um nome do host, será solicitado a inserir o nome do host.

e) Para o parâmetro **ResourceManager Port**, insira o número da porta que está associado ao processo daemon para ResourceManager. O número padrão da porta é 8088.

6. Opcional: Quando for solicitado a incluir os detalhes dos seguintes parâmetros do cluster Hadoop, aceite o valor padrão ou especifique um valor apropriado para cada um dos seguintes parâmetros e pressione Enter:

   a) Para o parâmetro **JobHistoryServer Hostname**, insira o nome do host do nó onde o processo daemon para JobHistoryServer é executado.

   b) Para o parâmetro **JobHistoryServer Port**, insira o número da porta que está associado ao processo daemon para JobHistoryServer. O número padrão da porta é 19888.

   c) Para o parâmetro **Additional NameNode Hostname**, insira o nome do host do nó onde o processo daemon para um Secondary ou Standby NameNode é executado.

   d) Para o parâmetro **Additional NameNode Port**, insira o número da porta que está associado ao processo daemon para um Secondary ou Standby NameNode. O número da porta padrão para um Secondary NameNode é 50090. Para um Standby NameNode, o número da porta padrão é 50070.

7. Opcional: Quando a linha de comandos exibir a seguinte mensagem, insira 1 para incluir detalhes de Standby ResourceMangers para um cluster de alta disponibilidade e pressione Enter.
   `Standby ResourceManager(s) in Hadoop Cluster [ 1=Yes, 2=No ] (default is: 2):`

8. Quando a linha de comandos exibir a seguinte mensagem, especifique 1 e pressione Enter para monitorar serviços Hadoop no cluster Hadoop que é gerenciado pelo Ambari:
   `Monitoring of Hadoop services for Ambari based Hadoop installations [ 1=Yes, 2=No ] (default is: 2):`
   Caso contrário, retenha o valor padrão 2 e pressione Enter. Se você ativar o monitoramento de serviços Hadoop, especifique um valor para cada um dos seguintes parâmetros do servidor Ambari e pressione Enter:

   a) Para o parâmetro **Nome do host do servidor Ambari**, insira o nome do host onde o servidor Ambari é executado.

   b) Para o parâmetro de **Porta do servidor Ambari**, insira o número da porta que está associado ao servidor Ambari.
   O número da porta padrão é 8080.

   c) Para o parâmetro de **Nome do usuário do Ambari**, insira o nome do usuário do Ambari.

   d) Para o parâmetro de **Senha do usuário do Ambari**, insira a senha do usuário do Ambari.

9. Quando a linha de comandos exibir a seguinte mensagem, selecione o nível de rastreio Java apropriado e pressione Enter:
   `This parameter allows you to specify the trace level used by the Java providers Java trace level [ 1=Off, 2=Error, 3=Warning, 4=Information, 5=Minimum Debug, 6=Medium Debug, 7=Maximum Debug, 8=All ] (default is: 2)`

10. Opcional: Quando a linha de comandos exibir a seguinte mensagem, especifique os argumentos para a Java virtual machine e pressione Enter. A lista de argumentos deve ser compatível com a versão de Java que está instalada com o agente.
    `Este parâmetro permite que você especifique uma lista opcional de argumentos para os argumentos da java virtual machine JVM (o padrão é:)`

11. Opcional: Quando a linha de comandos exibir a seguinte mensagem, insira 1 para incluir os seguintes detalhes de Standby ResourceManagers e pressione Enter:
`Edit "Hadoop High Availability(HA) Cluster with Standby ResourceManagers" settings, [1=Add, 2=Edit, 3=Del, 4=Next, 5=Exit] (default is: 5): 1`
    a) Para o parâmetro **`Standby ResourceManager Hostname`**, insira o nome do host do nó onde o processo daemon para Standby ResourceManger é executado.
    b) Para **`Standby ResourceManager Port`**, insira o número da porta que está associado ao processo daemon para Standby ResourceManager. O número padrão da porta é 8088.
    c) Quando solicitado, insira 1 para incluir mais Standby ResourceManagers e repita as etapas a e b, ou insira 5 para acessar a próxima etapa.

    - Para editar as definições de configuração de um Standby ResourceManager específico, digite 4 e pressione Enter até aparecer o nome do host do Standby ResourceManager necessário.
    - Para remover um Standby ResourceManager, digite 3 e pressione Enter depois de ver o nome do host do Standby ResourceManger que você deseja remover.
12. Quando solicitado, insira o caminho da classe para os arquivos JAR requeridos pelo provedor de dados da API Java e pressione Enter.
    Os valores de configuração especificados são salvos e uma mensagem de confirmação é exibida.
13. Execute o comando a seguir para iniciar o agente: *`install_dir`*`/bin/hadoop-agent.sh start`

O que Fazer Depois

1. Ative os eventos de subnó para visualizar os limites de acontecimentos do Agente do Hadoop. Para obter informações sobre como ativar eventos do subnó, consulte "Configurando o painel para visualizar eventos Hadoop" na página 261.
2. Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o agente usando o arquivo de resposta silencioso

O arquivo de resposta silencioso contém os parâmetros de configuração do agente. Para alguns parâmetros, os valores padrão são fornecidos nos comentários. É possível especificar valores diferentes para esses parâmetros, e remover as tags de comentário que são colocadas no início dos parâmetros.

Sobre Esta Tarefa

É possível usar o arquivo de resposta silencioso para configurar o Agente do Hadoop nos sistemas Linux, AIX e Windows.

Procedimento

1. Abra o arquivo silencioso de resposta que está disponível nesse caminho: *`install_dir`*`\samples\hadoop_silent_config.txt`
2. No arquivo de resposta, conclua as seguintes etapas:
    a) Quando desejar monitorar o Cluster Hadoop que é ativado para autenticação baseada em Kerberos SPNEGO, especifique `yes` e insira valores para os seguintes parâmetros:

    ```
    HADOOP_REALM_NAME
    HADOOP_KDC_HOSTNAME
    HADOOP_PRINCIPAL_NAME
    HADOOP_SPNEGO_KEYTAB
    ```

    b) Quando você deseja monitorar o Cluster Hadoop que é ativado por SSL, digite `yes` e insira valores para os seguintes parâmetros:

    ```
    HADOOP_TRUSTSTORE_PATH
    HADOOP_TRUSTSTORE_PASSWORD
    ```

c) Insira valores para os seguintes parâmetros de Cluster, NameNode (NN), ResourceManager (RM) e Job History Server (JHS):

```
HADOOP_CLUSTER_NAME (optional)
HADOOP_NN_HOSTNAME
HADOOP_NN_PORT
HADOOP_RM_HOSTNAME
HADOOP_RM_PORT
HADOOP_JHS_HOSTNAME (optional)
HADOOP_JHS_PORT (optional)
```

d) Opcional: Para o parâmetro **HADOOP_ADDITIONAL_NN_HOSTNAME**, especifique o nome do host do Standby ou Secondary NameNode.

e) Opcional: Para o parâmetro **HADOOP_ADDITIONAL_NN_PORT**, especifique o número da porta do Standby ou Secondary NameNode.

Lembre-se: Se o NameNode adicional for um Standby NameNode, o número padrão da porta associado ao processo daemon do Standby NameNode será 50070. Se o NameNode adicional for um Secondary NameNode, o número padrão da porta associado ao processo daemon do Secondary NameNode será 50090.

f) Opcional: Para o parâmetro **Hadoop_SRM**, especifique `Sim` para incluir Standby ResourceManagers para um cluster de alta disponibilidade e acesse a etapa g.

g) Opcional: Para monitorar serviços do Hadoop no cluster Hadoop que é gerenciado pelo Ambari, insira valores para cada um dos parâmetros a seguir, e pressione Enter:

```
AMBARI_SERVER_HOSTNAME
AMBARI_SERVER_PORT
USERNAME_OF_AMBARI_USER
PASSWORD_OF_AMBARI_USER
```

h) Para o parâmetro **JAVA_TRACE_LEVEL**, especifique o nível de rastreio adequado.

i) Opcional: Para o parâmetro **JAVA_JVM_ARGS**, especifique argumentos para a Java™ virtual machine.

j) Opcional: Inclua o nome do host e o número da porta de um Standby ResourceManager no seguinte formato: HADOOP_SRM_PORT.*hadoop_srm_config_sec_1*=8088

Em que *hadoop_srm_config_sec_1* é o nome do host do nó em que o processo daemon para Standby ResourceManager é executado, e 8088 é o número da porta padrão. Para incluir mais Standby ResourceManagers, inclua o nome do host e o número da porta de outros Standby ResourceManagers nas novas linhas no mesmo formato.

3. Salve o arquivo de resposta e execute o comando a seguir:

Linux AIX *install_dir*/bin/hadoop-agent.sh config *install_dir*/samples/hadoop_silent_config.txt

Windows *install_dir*/bin/hadoop-agent.bat config *install_dir*/samples/hadoop_silent_config.txt

4. Inicie o agente:

Linux AIX Execute o comando a seguir: *install_dir*\bin\hadoop-agent.sh start

Windows Clique com o botão direito em **Monitoring Agent for Hadoop** e clique em **Iniciar**.

O que Fazer Depois

1. Ative os eventos de subnó para visualizar os limites de acontecimentos do Agente do Hadoop. Para obter informações sobre como ativar eventos do subnó, consulte "Configurando o painel para visualizar eventos Hadoop" na página 261.
2. Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o painel para visualizar eventos Hadoop

Deve-se configurar o painel para ativar os eventos de subnó para que a guia **Eventos** possa exibir eventos Hadoop.

Sobre Esta Tarefa

O valor padrão para **Ativar eventos de subnó** é false. Mude esse valor para true para visualizar eventos Hadoop.

Procedimento

1. Abra o Console do Cloud APM e acesse **Configuração do sistema**.
2. Na página **Configuração avançada**, clique em **Integração da UI** em **Categorias de configuração**.
3. Na lista **Ativar eventos do subnó**, selecione **True**.
4. Clique em **Salvar**.

Concedendo permissão a usuários não administrativos

Em sistemas Windows, conceda a permissão *Depurar programa* a um usuário não administrativo para executar o Agente do Hadoop. Essa permissão é necessária para visualizar dados nos painéis do Agente do Hadoop.

Procedimento

Conclua as seguintes etapas no computador onde o agente Hadoop está instalado:

1. Clique em **Iniciar > Painel de Controle > Ferramentas Administrativas**.
2. Dê um clique duplo em **Política de Segurança Local**.
3. Na área de janela Configurações de segurança, expanda **Políticas locais** e clique em **Designação de direitos do usuário**.
4. Clique com o botão direito em **Depurar programas** e clique em **Propriedades**.
5. Clique em **Incluir usuário ou grupo** e inclua o nome do usuário não administrativo ao qual você deseja conceder essa permissão.
6. Clique em **OK**.

O que Fazer Depois

Configure e execute o Agente do Hadoop com o usuário não administrativo.

Configurando o monitoramento do HMC Base

O Monitoring Agent for HMC Base fornece o recurso para monitorar o Hardware Management Console (HMC). O agente monitora a disponibilidade e o funcionamento dos recursos do HMC: cPU, memória, armazenamento e rede. O agente também relata no HMC o inventário e a configuração de servidores Power, conjuntos de CPUs e LPARs. A utilização da CPU do servidores Power, LPARs e conjuntos é monitorada usando os dados de amostra de desempenho do HMC.

Antes de Iniciar

Antes de configurar o Agente HMC Base, você deve concluir as seguintes tarefas:

- Configure a conexão SSH entre o sistema que está executando o agente e o HMC. Para obter mais informações, consulte “Configurando a conexão SSH” na página 263.
- Prepare o HMC SDK antes de iniciar a primeira instância de agente. Para obter mais informações, consulte “Preparando SDK para HMC” na página 264.

Procedimento

- Para configurar o agente ao editar o arquivo de resposta silenciosa e executar o script sem nenhuma interação, conclua as seguintes etapas:

  1. Abra o arquivo `hmc_base_silent_config.txt` em um editor de texto:
     - AIX *install_dir*`/samples/hmc_base_silent_config.txt`.
  2. Para **Nome do host do HMC**, é possível especificar o endereço IP ou o nome do host.
  3. Para **Nome do usuário do HMC**, insira o nome do usuário de login do HMC, por exemplo, **HMC_USERNAME=** *hscroot*.

     Nota: O nome do usuário de login designado para o HMC requer, no mínimo, a autoridade hscviewer.
  4. Para **HMC Password**, deve-se inserir a senha do usuário.
  5. Para o **Número Máximo de Arquivos de Log do Provedor de Dados:**, especifique o número máximo de arquivos de log do provedor de dados criados. Por exemplo, **KPH_LOG_FILE_MAX_COUNT=***10*.
  6. Para o **Tamanho Máximo em KB de Cada Log do Provedor de Dados**, insira o tamanho máximo em KB que um arquivo de log do provedor de dados pode atingir antes da criação de um novo arquivo de log, por exemplo, **KPH_LOG_FILE_MAX_SIZE=** *5190*.
  7. Para o **Nível de Detalhes no Log do Provedor de Dados**, insira a quantidade de detalhes que o provedor de dados incluirá nos arquivos de log do provedor de dados, por exemplo, **KPH_LOG_LEVEL=***Fine*. Especifique um dos seguintes valores:
     - 1= Off
     - 2=Severe
     - 3=Warning
     - 4=Info
     - 5=Fine
     - 6=Finer
     - 7=Finest
     - 8=All

     Importante: O valor padrão é 4.
  8. Salve e feche o arquivo `hmc_base_silent_config.txt` e, em seguida, insira: `./hmc_base-agent.sh config` *instance_name install_dir*`/samples/hmc_base_silent_config.txt` em que *instance_name* é o nome a ser fornecido à instância e *install_dir* é o diretório de instalação do Agente HMC Base. O diretório de instalação padrão é `/opt/ibm/apm/agent`.

- AIX Para configurar o agente respondendo aos prompts, execute as seguintes etapas:

  1. Abra o diretório *install_dir*`/bin`, em que *install_dir* é o diretório de instalação do Agente HMC Base.
  2. Para configurar o Agente HMC Base, execute o seguinte comando: **./hmc_base-agent.sh config instance_name**.
  3. Quando solicitado a **editar as configurações do Monitoring Agent for HMC Base**, pressione **Enter**. O valor padrão é Yes.
  4. Para inserir as informações de configuração do HMC, execute as etapas a seguir.
     a. Quando o **Nome do host do HMC** for solicitado, digite o nome do host ou endereço IP e pressione **Enter**.
     b. Quando o **Nome do usuário do HMC** for solicitado, digite o nome do usuário de logon que está associado ao HMC e pressione **Enter**.
  5. Quando for solicitada a **Senha do HMC**, digite a senha do usuário.

6. Para inserir as informações do provedor de dados, execute as etapas a seguir:
   a. Quando for solicitado o **número máximo de arquivos de log do provedor de dados**, digite a quantidade de arquivos de log e pressione **Enter**.

      O número máximo padrão de arquivos de log do provedor de dados é 10.
   b. Quando for solicitado o **tamanho máximo em KB de cada log do provedor de dados**, digite o tamanho e pressione **Enter**.

      O tamanho máximo padrão em KB é 5190.
   c. Quando for solicitado o **Nível de detalhes no log do provedor de dados**, digite um dos níveis a seguir e pressione **Enter**:
      - 1= Off
      - 2=Severe
      - 3=Warning
      - 4=Info
      - 5=Fine
      - 6=Finer
      - 7=Finest
      - 8=All

O que Fazer Depois

- Para iniciar o agente, insira: `./hmc_base-agent.sh start` *InstanceName*.
- Configure o HMC Console Server de acordo com as instruções em "Configurando o HMC Console Server para monitorar Virtual I/O" na página 265 para monitorar a E/S virtual.
- Ative o monitoramento de utilização da CPU e memória de acordo com as instruções em "Ativando o monitoramento de utilização de memória e CPU" na página 266.

Configurando a conexão SSH

Você deve configurar a conexão SSH entre o sistema que está executando o agente e o HMC para o agente coletar dados.

Sobre Esta Tarefa

O provedor de dados do agente coleta os dados do console de gerenciamento, executando os comandos CLI sobre SSH. Por padrão, o provedor de dados aguarda até 1 minuto para que um comando CLI conclua a execução. Após esse tempo, o provedor de dados fecha a sessão SSH na qual o comando CLI está em execução, e nenhum dos dados para esse comando está disponível em conjuntos de dados do agente até que o comando seja executado com êxito. O caminho padrão para o comando SSH é `/usr/bin/ssh`. Se você instalou SSH em um local diferente, deverá indicar o caminho usando a variável de ambiente **KPH_SSH_PATH**.

Procedimento

Use um dos seguintes métodos para configurar a conexão SSH.

- Use o script `setup_hmc_key.pl` para configurar a conexão SSH.
  a) Efetue login no servidor no qual o agente está instalado.
  b) Abra o diretório `install_dir/aix526/ph/bin`, em que `install_dir` é o diretório de instalação do Agente HMC Base.
  c) Execute o comando `perl setup_hmc_key.pl`.
  d) Responda aos prompts e forneça o nome de host ou endereço IP de HMC; o nome de usuário de HMC, que deve ter autoridade equivalente para a autoridade `hscviewer`; e a senha para criar o par de chaves.

e) Depois de criar o par de chaves, teste a conectividade executando um comando, como `ssh hscroot@hmchost lshmc -V`.

Se o SSH estiver se conectando a este HMC pela primeira vez, inclua o HMC no arquivo `ssh known_hosts` respondendo `yes` para a seguinte mensagem:

```
A autenticidade do host 'hmchost (3.3.333.333)' não pode ser estabelecida.
A impressão digital RSA é 4c:b4:26:27:38:f3:ec:58:01:92:26:f9:61:32:bb:4d.
Tem certeza de que deseja continuar a conexão (sim/não)? yes

Aviso: Incluído permanentemente 'hmchost,3.3.333.333' (RSA) na lista de hosts conhecidos.
```

O agente agora pode usar o SSH para coletar os dados do HMC.

- Use o utilitário `ssh-keygen` para gerar chaves e configurar a conexão SSH.
  a) Efetue login no servidor no qual o agente está instalado.
  b) Use o utilitário `ssh-keygen` para gerar chaves públicas e privadas sem paráfrase. Por exemplo, o comando a seguir gera um conjunto de chaves públicas e privadas:

```
ssh-keygen -t rsa -f /.ssh/id-rsa
```

Pressione Enter quando solicitado a fornecer uma passphrase. A chave pública gerada é armazenada no arquivo `/.ssh/id-rsa.pub`. A chave privada é armazenada no arquivo `/.ssh/id-rsa`.

  c) Transfira o arquivo que contém a chave pública para o computador HMC usando utilitários como `scp`.
  d) No computador HMC, anexe o arquivo de chave pública à coleção de chaves que estão armazenadas no HMC.

As chaves armazenadas estão no arquivo `/.ssh/authorized_keys2`.

  e) Inclua o nome do host e chave para o HMC no arquivo `known_hosts`.

Este arquivo está no diretório `/.ssh`.

a. Execute o comando `ssh "user"@"hmc_hostname" -i "private_keyfile" date`.
b. Insira `yes` quando solicitado para armazenar as chaves em cache. Esse comando inclui a entrada no arquivo `known_hosts` para conexões futuras.

  f) Execute o comando `ssh "user"@"hmc_hostname" date`.

Se a data for retornada sem nenhum prompt de senha, isto indica que as chaves SSH foram configuradas com êxito.

Preparando SDK para HMC

Você deve preparar o SDK para HMC antes de iniciar a instância de agente pela primeira vez.

Sobre Esta Tarefa

Antes de iniciar sua primeira instância de agente, você deve preparar a versão correspondente do SDK para seu HMC. Após a conclusão da preparação, não é preciso repetir esta tarefa para outra instância do Agente HMC Base criada para o HMC da mesma versão. Para monitorar outra versão do HMC, repita essas tarefas para preparar novamente o SDK.

Procedimento

- No diretório *agent_dir*`/aix526/ph/bin`, execute a ferramenta de script **prepareSDK.sh** para preparar automaticamente o SDK do HMC.
  - Se aparecer a mensagem `O SDK está pronto para HMC`, a preparação está concluída.
  - Se não aparecer a mensagem `O SDK está pronto para HMC`, é possível preparar manualmente o SDK para HMC.

Para o HMC V8.5.0, conclua as seguintes etapas:

1. Use um navegador para fazer download do SDK a partir do HMC diretamente com a URL a seguir:

   ```
   https://HMC_IP:12443/rest/api/web/sdk
   ```

   Quando solicitado, insira o nome do usuário e a senha da conta `hscroot`. O nome do arquivo do SDK está no formato de `pmc_sdk_*.zip`.
2. . Descompacte o arquivo ZIP do SDK e acesse o diretório `IBM HMC REST Web Services SDK Runtime/lib/ibm3`.
3. Se ele ainda não existir, crie um subdiretório `<agent_dir>/aix526/ph/lib/my_hmc_version`, em que *my_hmc_version* é a versão do seu ambiente HMC, por exemplo, 8502. Para determinar a versão do ambiente do HMC, execute o comando a seguir:

   ```
   ssh hscroot@<HMC_IP> 'lshmc -v' | grep RM |
   awk -FR '{print $3}' | tr -d '.'
   ```
4. Copie todos os arquivos `.jar` na pasta `IBM HMC REST Web Services SDK Runtime/lib/ibm3` do SDK do HMC para o diretório *agent_dir*`/aix526/ph/lib/`*HMC_version*.

Para o HMC V8.6.0 ou V8.7.0, conclua as etapas a seguir:

1. Use um navegador para fazer download do SDK a partir do HMC diretamente com a URL a seguir:

   ```
   https://HMC_IP:12443/rest/api/web/sdk
   ```

   Quando solicitado, insira o nome de usuário e a senha da conta `hscroot`. O nome do arquivo do SDK está no formato de `pmc-rest-sdk*.zip`.
2. Descompacte o arquivo ZIP do SDK e acesse o subdiretório `lib`.
3. Se ele ainda não existir, crie um subdiretório `<agent_dir>/aix526/ph/lib/my_hmc_version`, em que *my_hmc_version* é a versão do seu ambiente HMC, por exemplo 8602 ou 87012. Para determinar a versão do ambiente do HMC, execute o comando a seguir:

   ```
   ssh hscroot@<HMC_IP> 'lshmc -v' | grep RM |
   awk -FR '{print $3}' | tr -d '.'
   ```
4. Copie todos os arquivos `.jar` na pasta `lib` do SDK do HMC para o diretório *agent_dir*`/aix526/ph/lib/`*my_hmc_version*.

Resultados
Está preparado com êxito SDK para HMC.

O que Fazer Depois
Configure o Agente HMC Base de acordo com as instruções em "Configurando o monitoramento do HMC Base" na página 261.

Configurando o HMC Console Server para monitorar Virtual I/O

Para que o Agente HMC Base possa monitorar o status do Virtual I/O, deve-se configurar o HMC Console Server.

Procedimento

Siga as etapas para configurar o HMC Console Server conforme os pré-requisitos para o Agente HMC Base para monitorar o Virtual I/O.

- Ative a função PMC do HMC Console Server e do Virtual I/O Server.

a) Efetue logon no HMC Console Server usando o navegador no modo clássico.

```
https://hmc_hostname
```

b) Clique em **Gerenciamento do HMC** > **Mudar Configurações de Monitoramento de Desempenho**.

A janela **Mudar Configurações de Monitoramento de Desempenho** é exibida.

c) Na seção **Coleta de Dados de Monitoramento de Desempenho para Gerenciar Servidores**, ative a função **Coleta** para os servidores correspondentes.

d) Clique em cada Virtual I/O Server para mostrar a janela **Propriedades da Partição** para esse servidor.

e) Sob a guia **Geral**, assegure-se de que a caixa de seleção da opção **Permitir Coleção de Informações de Desempenho** esteja selecionada.

Clique em **OK** para salvar as configurações.

Após vários minutos, é possível ver o tráfego de armazenamento e rede dos servidores correspondentes na página **Monitoramento de Desempenho**.

- Assegure-se de que o usuário do HMC para Agente HMC Base tenha o privilégio correto.
  a) Ao incluir ou editar o usuário, assegure-se de que o usuário tenha a função **hmcviewer** e de que a opção **AllSystemResource** para esse usuário esteja ativada.
  b) Na janela **Propriedades do Usuário**, ative a opção **Permitir Acesso Remoto via Web**.

Ativando o monitoramento de utilização de memória e CPU

Se a coleta de dados para utilização de memória e CPU estiver desativada, os dados de utilização de memória e CPU de cada servidor de energia não serão exibidos na IU.

Procedimento

Use um dos métodos a seguir para ativar o monitoramento de utilização de memória e CPU.

- Ative o monitoramento de utilização de memória e CPU executando o seguinte comando de gerenciamento do HMC `chlparutil`.

```
chlparutil-r config -m <CECname> -s <the sample rate in seconds, always 60>
```

- Ative o monitoramento de utilização de memória e CPU no HMC Console Server.
  a) Efetue logon no HMC Console Server com modo clássico.
  b) Clique no nó **Servidores** na árvore de navegação.
  c) Selecione o servidor e acesse **Operações** > **Dados de Utilização** > **Mudar a Taxa de Amostra**.
  d) Configure uma taxa de amostragem.
  A taxa de amostragem fica desativada por padrão. É possível configurar a taxa com valores apropriados, por exemplo, `30 minutos`.

Configurando o monitoramento do Servidor HTTP

O Monitoring Agent for HTTP Server é iniciado automaticamente após a instalação. Para ativar a coleta de dados, certifique-se de que o servidor HTTP esteja em execução e edite o arquivo de configuração do Servidor HTTP para que ele inclua uma referência ao arquivo de configuração do coletor de dados do Agente do Servidor HTTP.

Antes de Iniciar

Há dois arquivos envolvidos na configuração do Agente do Servidor HTTP. Para visualizar amostras desses arquivos, consulte Amostras. Localize e revise os seguintes arquivos:

O arquivo de configuração do coletor de dados do Agente do Servidor HTTP

Após a instalação do Agente do Servidor HTTP, ele descobre o servidor HTTP e gera um arquivo de configuração do coletor de dados no diretório *install_dir* /tmp/khu, em que *install_dir* é o diretório onde o Agente do Servidor HTTP está instalado.

Se você tiver vários Servidores HTTP em seu ambiente, será gerado um arquivo de configuração do Agente do Servidor HTTP por servidor HTTP.

O nome do arquivo de configuração do Agente do Servidor HTTP é composto de duas partes e tem o seguinte formato:

```
khu.full path of the HTTP Server configuration file name.conf
```

A primeira parte do nome do arquivo de configuração do agente é khu, em que hu é o código do agente do servidor HTTP.
A segunda parte do nome do arquivo de configuração do agente é criada usando o caminho completo e nome do arquivo de configuração do servidor HTTP, em que / é substituído por . . Por exemplo, os nomes de arquivos possíveis são os seguintes:

Linux AIX
```
khu.usr.local.apache24.conf.httpd.conf
```

Windows
```
khu.C.Program Files.IBM.HTTPServer.conf.httpd.conf
```

O arquivo de configuração do coletor de dados do Agente do Servidor HTTP contém os seguintes elementos:

- Detalhes sobre o caminho do arquivo httpd.conf usado pelo HTTP Server, por exemplo, `KhuShmemPath "/IBM/HTTPServer/conf/httpd.conf"`.
- Local da biblioteca a ser carregada
- Permissões que estão associadas à memória compartilhada

O arquivo de configuração do servidor HTTP

Cada servidor HTTP possui um arquivo de configuração que, por padrão, é chamado *http_server_install_dir* /conf/httpd.conf, em que *http_server_install_dir* é o diretório no qual o Servidor HTTP está instalado. Em alguns ambientes, esse nome de arquivo pode ser customizado. Verifique o nome exato do arquivo com o administrador do servidor HTTP.

Sobre Esta Tarefa

Ative o Agente do Servidor HTTP para coleta de dados nas seguintes situações:

- Depois de instalar o Agente do Servidor HTTP
- Depois de fazer upgrade para o Agente do Servidor HTTP versão 1.0.0.4, o novo alias faz os nós existentes do Agente do Servidor HTTP ficarem off-line no Console do Cloud APM.
- Depois de fazer upgrade da versão 1.0.0.4, os nós do Agente do Servidor HTTP existentes podem tornar-se off-line no Console do Cloud APM. Isso pode ocorrer se você tiver várias instâncias do servidor HTTP com nomes de arquivo de configuração do agente semelhantes, por exemplo, `httpd` e `httpd01`.

A ferramenta de utilitário de rede de linha de comandos netstat é necessária para que o Agente do Servidor HTTP descubra com êxito o servidor HTTP em execução.

Importante: Para resolver o problema de nó do agente off-line que ocorre após o upgrade, é preciso incluir a nova instância do servidor HTTP no Console do Cloud APM após a conclusão dessa tarefa.

Procedimento

1. Para ativar a coleta de dados, é preciso referenciar o arquivo de configuração do coletor de dados no arquivo de configuração do servidor HTTP usando a instrução `Include`. Anexe a instrução a seguir ao final do arquivo de configuração do servidor HTTP:

```
Inclua "install_dir/tmp/khu/khu.full path of the HTTP Server configuration file name.conf"
```

Por exemplo,

Linux AIX Se você tiver um IBM HTTP Server que está instalado no diretório `/opt/IBM/HTTPServer` e o arquivo de configuração do coletor de dados estiver no seguinte diretório:

```
/opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf
```

Anexe a seguinte instrução ao arquivo de configuração do servidor HTTP `/opt/IBM/HTTPServer/conf/httpd.conf`:

```
Include "/opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf"
```

Windows Se você tiver um IBM® HTTP Server que está instalado no diretório `C:\ProgramFiles\IBM\HTTPServer` e o arquivo de configuração do coletor de dados estiver no seguinte diretório:

```
C:\IBM\APM\tmp\khu\khu.C.Program Files.IBM.HTTPServer.conf.httpd.conf
```

Anexe a seguinte instrução ao arquivo de configuração do servidor HTTP `C:\Program Files\IBM\HTTPServer\conf\httpd.conf`:

```
Include "C:\IBM\APM\tmp\khu\khu.C.Program Files.IBM.HTTPServer.conf.httpd.conf"
```

2. Altere o diretório a seguir:

```
HTTP_server_installation_directory/bin
```

3. Reinicie o servidor HTTP. Por exemplo:

Linux AIX

```
./apachectl -k stop
./apachectl -k start
```

Windows

```
httpd.exe -k stop
httpd.exe -k start
```

Resultados
Você configurou o agente com sucesso.

O que Fazer Depois
Agora, é possível verificar se os dados do Agente do Servidor HTTP são exibidos no console do Cloud APM. Para obter instruções sobre como iniciar o console do Cloud APM, consulte Iniciando o console do Cloud APM. Para obter informações sobre o uso do Editor de aplicativos, consulte Gerenciando aplicativos.

Nota: Se não houver tráfego no servidor HTTP, você não verá dados no Console do Cloud APM.

Módulo de Tempo de Resposta do IBM HTTP Server

Ao instalar o agente Response Time Monitoring para trabalhar com o Módulo de Tempo de Resposta do IBM HTTP Server, ele irá monitorar todas as portas para solicitações HTTP e HTTPS.

Módulo de Tempo de Resposta do IBM HTTP Server

O Módulo de Tempo de Resposta do IBM HTTP Server é uma parte do Agente do HTTP Server. Se o Agente do HTTP Server for instalado e configurado antes ou ao mesmo tempo que o agente Response Time Monitoring no Apache HTTP Server ou IBM HTTP Server no AIX, Linux ou Windows, o Módulo de Tempo de Resposta do IBM HTTP Server será ativado automaticamente. Para obter uma descrição da funcionalidade Módulo de Tempo de Resposta do IBM HTTP Server, consulte "Configurando o Módulo de Tempo de Resposta do IBM HTTP Server" na página 694.

Arquivo de configuração do coletor de dados

Após a instalação do Agente do Servidor HTTP, ele descobre o servidor HTTP e gera um arquivo de configuração do coletor de dados no diretório *install_dir* /tmp/khu, em que *install_dir* é o diretório onde o Agente do Servidor HTTP está instalado.

Para o Servidor HTTP Apache, o arquivo de configuração do coletor de dados é:
`khu.usr.local.apache24.conf.httpd.conf`
Para o IBM HTTP Server, o arquivo de configuração do coletor de dados é:
`khu.opt.IBM.HTTPServer.conf.httpd.conf`

Plugins

O Agente do HTTP Server e composto de dois plug-ins:

1. `khu_module` - este é o Agente do HTTP Server. Esse plug-in é responsável por todos os painéis associados ao Agente do HTTP Server. Para obter mais informações, consulte Referência do Agente do Servidor HTTP.
2. `wrt_module` - é o Módulo de Tempo de Resposta do IBM HTTP Server

Esses dois plug-ins são indicados no arquivo de configuração do coletor de dados da seguinte forma:

```
LoadModule khu_module

LoadModule wrt_module
```

Ativar coleta de dados

Para ativar a coleta de dados, é preciso referenciar o arquivo de configuração do coletor de dados no arquivo de configuração do servidor HTTP usando a instrução `Include`. Anexe a instrução a seguir ao final do arquivo de configuração do servidor HTTP:

```
include /opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf
```

Para obter mais informações, consulte “Configurando o monitoramento do Servidor HTTP” na página 266.

Quando a coleta de dados é ativada, o Painel do usuário final é preenchido.

Amostras de código do Agente do Servidor HTTP

Há dois arquivos envolvidos na configuração do Agente do Servidor HTTP. Eles são o arquivo de configuração do coletor de dados do Agente do Servidor HTTP e o arquivo de configuração do servidor HTTP. Uma amostra para o arquivo de mapeamento de alias da Instância também é fornecido para ajudar a explicar como o alias funciona.

Amostras do arquivo do coletor de dados do Agente do Servidor HTTP

Para o IBM HTTP Server versão 8 e mais recente, 64 bits, o Agente do Servidor HTTParquivo de configuração do coletor de dados contém essas informações:

```
#
# Configurações para o módulo Monitoring Agent for HTTP Server.
#

LoadModule khu_module "/tmp/ihs/lx8266/hu/lib/khuapache22dc_64.so"

<IfModule mod_khu.c>
   KhuShmemPerm 660
   KhuShmemPath "/opt/IBM/IHS/conf/httpd.conf"
   KhuCpsPath "/tmp/ihs/tmp/khu/khu_cps.properties"
</IfModule>

Alias /khu "/tmp/ihs/lx8266/hu/etc"
<Directory "/tmp/ihs/lx8266/hu/etc">
  Order deny,allow
  Allow from all
  #Requerer todos concedidos
</Directory>
```

```
LoadModule wrt_module /tmp/ihs/lx8266/hu/lib/mod_wrt_ap22_64.so
WrtOriginID HU:tivvm09_httpd:HUS
```

Para o IBM HTTP Server versão 7, de 32 bits, o arquivo de configuração contém essas informações:

```
#
# Configurações para o módulo Monitoring Agent for HTTP Server.
#

LoadModule khu_module "/tmp/ihs/lx8266/hu/lib/khuapache22dc_32.so"

<IfModule mod_khu.c>
 KhuShmemPerm 660
 KhuShmemPath "/opt/IBM/HTTPServer/conf/httpd.conf"
 KhuCpsPath "/tmp/ihs/tmp/khu/khu_cps.properties"
</IfModule>

Alias /khu "/tmp/ihs/lx8266/hu/etc"
<Directory "/tmp/ihs/lx8266/hu/etc">
  Order deny,allow
  Allow from all
  #Requerer todos concedidos
</Directory>

LoadModule wrt_module /tmp/ihs/lx8266/hu/lib/mod_wrt_ap22.so
WrtOriginID HU:linux_httpd:HUS
```

Para o Apache versão 2.4, 64 bits, o arquivo de configuração do Agente do Servidor HTTP contém essas informações:

```
#
# Configurações para o módulo Monitoring Agent for HTTP Server.
#

LoadModule khu_module "/tmp/ihs/lx8266/hu/lib/khuapache24dc_64.so"

<IfModule mod_khu.c>
 KhuShmemPerm 660
 KhuShmemPath "/usr/local/apache24/conf/httpd.conf"
</IfModule>

Alias /khu "/tmp/ihs/lx8266/hu/etc"
<Directory "/tmp/ihs/lx8266/hu/etc">
  Order deny,allow
  Allow from all
  Requerer todos concedidos
</Directory>

LoadModule wrt_module /tmp/ihs/lx8266/hu/lib/mod_wrt_ap24_64.so
WrtOriginID HU:linux-tzsi_httpd:HUS
```

Amostra de arquivo de mapeamento alias da Instância

```
# Mapeamento do alias de instância do Monitoring Agent for HTTP Server
# INSTANCE: descoberta automaticamente pelo agente. NÃO modificar.
# ALIAS: nome alternativo para a instância. O nome será exibido em um painel de IU do APM.
Ele deve ser exclusivo
# entre todas as instâncias, ter menos de 10 caracteres e consistir em apenas caracteres
alfanuméricos.
#
INSTANCE.1=/usr/local/apache24/conf/httpd.conf
ALIAS.1=httpd

INSTANCE.1=/usr/local/apache24/conf/admin.conf
ALIAS.1=admin
```

Configurando o monitoramento do IBM Cloud

O Monitoring Agent for IBM Cloud coleta o inventário de máquina virtual e as métricas de sua conta do IBM Cloud (SoftLayer). Use o agente IBM Cloud para rastrear quantos dispositivos virtuais você tem

configurados e em execução no IBM Cloud. É possível ver quais recursos são alocados para cada dispositivo virtual na página detalhada do painel, que também mostra informações como o data center em que um dispositivo está localizado, o sistema operacional e a largura da banda da rede pública projetada para o mês.

Antes de Iniciar

- Leia o tópico "Configurando o monitoramento do IBM Cloud" na página 270 inteiro para determinar o que é necessário para concluir a configuração.
- Estas instruções são para a liberação mais atual do agente, exceto conforme indicado.
- Certifique-se de que os requisitos do sistema para o IBM Cloud agent sejam atendidos em seu ambiente. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o IBM Cloud agent.
- Assegure-se de que as seguintes informações estejam disponíveis:
  - Um nome de usuário para um usuário com pelo menos permissões de Auditor.
  - A Chave de API para o IBM Cloud para esse usuário associado.

Sobre Esta Tarefa

O IBM Cloud agent é um agente de múltiplas instâncias e também um agente do subnó. Depois de configurar instâncias de agente, você deve iniciar cada instância de agente manualmente.

Procedimento

1. Configure o agente nos sistemas Windows com a janela **IBM Performance Management** ou o arquivo de resposta silencioso.
   - "Configurando o agente nos sistemas Windows" na página 271.
   - "Configurando o agente usando o arquivo de resposta silencioso" na página 273.
2. Configure o agente nos sistemas Linux com o script que solicita respostas ou com o arquivo de resposta silencioso.
   - "Configurando o agente respondendo aos prompts" na página 272.
   - "Configurando o agente usando o arquivo de resposta silencioso" na página 273.

O que Fazer Depois

No Console do Cloud APM, acesse seu Application Performance Dashboard para visualizar os dados que foram coletados. Para obter informações adicionais sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Se você não conseguir visualizar os dados nos painéis do agente, primeiro verifique os logs de conexão do servidor e, em seguida, os logs do provedor de dados. Os caminhos padrão para esses logs são listados aqui:

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Para obter ajuda com a resolução de problemas, consulte o Fórum do Cloud Application Performance Management.

Configurando o agente nos sistemas Windows

É possível configurar o IBM Cloud agent em sistemas operacionais Windows usando a janela IBM Cloud Application Performance Management. Após fazer a atualização dos valores de configuração, deve-se iniciar o agente para salvar os valores atualizados.

Procedimento

1. Clique em **Iniciar** > **Todos os programas** > **Agentes do IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito no modelo **Monitoring Agent for IBM Cloud** e, em seguida, clique em **Configurar agente**.

   Lembre-se: Depois de configurar uma instância de agente pela primeira vez, a opção **Configurar agente** está indisponível. Para configurar a instância do agente novamente, clique nela e, em seguida, clique em **Reconfigurar ...**.
3. Insira um nome de instância exclusivo e, em seguida, clique em **OK**. Use apenas letras latinas, numerais arábicos e o caractere de hífen ou de menos no nome da instância. Exemplo, `icloud-inst`.
4. Clique em **Avançar** na janela de nome da instância de agente.
5. Pressione **Novo** e insira as configurações de nome de usuário e chave de API do IBM Cloud SoftLayer, em seguida, clique em **Avançar**.
6. Clique em **OK** para concluir a configuração.
7. Na janela IBM Cloud Application Performance Management, clique com o botão direito na instância configurada e, em seguida, clique em **Iniciar**.

Configurando o agente respondendo aos prompts

Após a instalação do IBM Cloud agent, deve-se configurá-lo antes de iniciar o agente. Se o IBM Cloud agent estiver instalado em um computador Linux local, será possível seguir essas instruções para configurá-lo interativamente através de prompts da linha de comandos.

Sobre Esta Tarefa

Lembre-se: Se estiver reconfigurando uma instância do agente configurada, o valor que é definido na última configuração será exibido para cada configuração. Se desejar limpar um valor existente, pressione a tecla Espaço quando a configuração for exibida.

Procedimento

Siga essas etapas para configurar o IBM Cloud agent executando um script e respondendo aos prompts.

1. Execute o seguinte comando:

   ```
   install_dir/bin/ibm_cloud-agent.sh config instance_name
   ```

   em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome que você deseja fornecer para a instância de agente.

   Exemplo

   ```
   /opt/ibm/apm/agent/bin/ibm_cloud-agent.sh config icloud-inst
   ```
2. Responda aos prompts para configurar valores de configuração para o agente.

   Consulte “Parâmetros de Configuração para o IBM Cloud agent” na página 274 para obter uma explicação de cada um dos parâmetros de configuração.
3. Execute o comando a seguir para iniciar o agente:

   ```
   install_dir/bin/ibm_cloud-agent.sh start
   instance_name
   ```

   em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome da instância de agente.

   Exemplo

   ```
   /opt/ibm/apm/agent/bin/ibm_cloud-agent.sh start icloud-inst
   ```

Configurando o agente usando o arquivo de resposta silencioso

O arquivo de resposta silencioso contém os parâmetros de configuração do agente. É possível editar o arquivo de resposta silencioso para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

O arquivo silencioso de resposta contém os parâmetros de configuração do agente com valores padrão que são definidos para alguns parâmetros. É possível editar o arquivo silencioso de resposta para especificar os valores diferentes para os parâmetros de configuração.

Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

- Configure o IBM Cloud agent no modo silencioso:
  a) Abra o arquivo `ibm_cloud_silent_config.txt` em um dos caminhos a seguir em um editor de texto.
     – Linux *install_dir*`/samples/ibm_cloud_silent_config.txt`

       Exemplo, `/opt/ibm/apm/agent/samples/ibm_cloud_silent_config.txt`
     – Windows *install_dir*`\samples\ibm_cloud_silent_config.txt`

       Exemplo, `C:\IBM\APM\samples\ibm_cloud_silent_config.txt`

     em que *install_dir* é o caminho no qual o agente está instalado.
  b) No arquivo `ibm_cloud_silent_config.txt`, especifique valores para todos os parâmetros obrigatórios e modifique os valores padrão de outros parâmetros, conforme necessário.

     Consulte a seção "Parâmetros de Configuração para o IBM Cloud agent" na página 274 para obter uma explicação de cada um dos parâmetros de configuração.
  c) Salve e feche o arquivo `ibm_cloud_silent_config.txt` e execute o seguinte comando:
     – Linux *install_dir*`/bin/ibm_cloud-agent.sh config` **instance_name** *install_dir*`/samples/ibm_cloud_silent_config.txt`

       Exemplo, **/opt/ibm/apm/agent/bin/ibm_cloud-agent.sh config icloud-inst /opt/ibm/apm/agent/samples/ibm_cloud_silent_config.txt**
     – Windows *install_dir*`\bin\ibm_cloud-agent.bat config` **instance_name** *install_dir*`\samples\ibm_cloud_silent_config.txt`

       Exemplo, **C:\IBM\APM\bin\ibm_cloud-agent.bat config icloud-inst C:\IBM\APM\samples\ibm_cloud_silent_config.txt**

     em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome que você deseja fornecer para a instância de agente.

     Importante: Assegure que você inclua o caminho absoluto no arquivo silencioso de resposta. Caso contrário, os dados do agente não serão mostrados nos painéis.
  d) Execute o comando a seguir para iniciar o agente:
     – Linux *install_dir*`/bin/ibm_cloud-agent.sh start` **instance_name**

       Exemplo, **/opt/ibm/apm/agent/bin/ibm_cloud-agent.sh start icloud-inst**
     – Windows *install_dir*`\bin\ibm_cloud-agent.bat start` **instance_name**

       Exemplo, **C:\IBM\APM\bin\ibm_cloud-agent.bat start icloud-inst**

em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome da instância de agente.

Parâmetros de Configuração para o IBM Cloud agent

Os parâmetros de configuração para o IBM Cloud agent são exibidos em uma tabela.

1. IBM Cloud Configuration - Configurações para monitorar instâncias do IBM Cloud remotamente. As instâncias são descobertas automaticamente para a chave API que você deseja configurar.

Tabela 23. Configuração do IBM Cloud

Nome do parâmetro	Descrição	Nome do parâmetro do arquivo de configuração silenciosa
NomeUsuário	O nome de usuário para a conta do IBM SoftLayer que é usado para recuperar métricas da API do IBM Cloud.	**KFS_USERNAME**
Chave de API	A chave API específica do usuário que é necessária para concluir a autenticação. As Chaves de API são geradas e podem ser recuperadas por meio do IBM SoftLayer Customer Portal.	**KFS_API_KEY_PASSWORD**

Configurando o monitoramento do IBM Integration Bus

O IBM Integration Bus agent é um agente de múltiplas instâncias. Você deve criar uma primeira instância do agente e iniciá-la manualmente.

Antes de Iniciar

- As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte “Histórico de Mudanças” na página 50.
- Certifique-se de que os requisitos do sistema para o IBM Integration Bus agent sejam atendidos em seu ambiente. Para obter informações atualizadas sobre requisitos do sistema, consulte o Relatório detalhado de requisitos do Sistema para o IBM Integration Bus agent.

Sobre Esta Tarefa

O procedimento a seguir é um roteiro para configurar o IBM Integration Bus agent, que inclui etapas necessárias e opcionais. Conclua as etapas necessárias de acordo com suas necessidades.

Procedimento

1. Certifique-se de que o ID do usuário que será usado para iniciar e parar o IBM Integration Bus agent pertença aos grupos de usuários **mqm** e **mqbrkrs**.
2. Windows
   Se o IBM MQ (WebSphere MQ) estiver instalado no sistema Windows, inclua o caminho da biblioteca do IBM MQ (WebSphere MQ) na variável de ambiente **PATH**. Para que o IBM Integration Bus agent possa carregar as bibliotecas do IBM MQ (WebSphere MQ) necessárias para iniciar.
   a) Inclua o caminho da biblioteca do IBM MQ (WebSphere MQ) no início da variável de ambiente **PATH**.

      Por exemplo, se o caminho da instalação do IBM MQ (WebSphere MQ) for `C:\IBM\WMQ75`, inclua `C:\IBM\WMQ75\bin` no início da variável de ambiente **PATH** do sistema Windows.
   b) Reinicie o sistema Windows para que as mudanças entrem em vigor.

3. Configure o IBM Integration Bus agent especificando os seguintes parâmetros de configuração. Também existem alguns parâmetros de configuração opcionais que podem ser especificados para o agente. Para obter instruções detalhadas, consulte "Configurando o IBM Integration Bus agent" na página 275.
   - ID do Agente
   - O diretório de instalação de nós de integração (brokers) que devem ser monitorados
   - O caminho da biblioteca de 64 bits do IBM MQ (WebSphere MQ)
4. Configure o IBM Integration Bus para ativar os dados que você deseja monitorar. Consulte "Configurando o IBM Integration Bus para ativação de dados" na página 279.
5. Se você ativou a coleta de dados de captura instantânea para seu nó de integração (broker), configure o IBM Integration Bus agent para não armazenar dados de captura instantânea. Para obter instruções, veja "Desativando a coleta de dados de captura instantânea para o agente" na página 286.
6. Opcional: Para configurar o IBM Integration Bus agent para ativar o rastreamento de transação, use a página **Configuração do agente**. Para obter instruções, veja "Configurando o rastreamento de transações para o IBM Integration Bus agent" na página 286.
7. Opcional: Se não precisar mais da função de rastreamento de transação ou desejar desinstalar o IBM Integration Bus agent, desative o rastreamento de transação para o IBM Integration Bus e remova a saída de usuário fornecida pelo agente. Para obter instruções, consulte "Desativando o rastreamento de transação" na página 285 e "Removendo a saída de usuário KQIUserExit" na página 288.

Configurando o IBM Integration Bus agent

Deve-se designar um nome de instância para o IBM Integration Bus agent e configurar o agente antes de poder iniciar o monitoramento de seu ambiente IBM Integration Bus.

Antes de Iniciar

- Certifique-se de que o ID do usuário usado para iniciar e parar o agente pertença aos grupos de usuários **mqm** e **mqbrkrs**.
- Windows Se o IBM MQ (WebSphere MQ) estiver instalado no sistema Windows, inclua o caminho da biblioteca do IBM MQ (WebSphere MQ) na variável de ambiente **PATH**. Para que o IBM Integration Bus agent possa carregar as bibliotecas do IBM MQ (WebSphere MQ) necessárias para iniciar.
  1. Inclua o caminho da biblioteca do IBM MQ (WebSphere MQ) no início da variável de ambiente **PATH**.

     Por exemplo, se o caminho da instalação do IBM MQ (WebSphere MQ) for `C:\IBM\WMQ75`, inclua `C:\IBM\WMQ75\bin` no início da variável de ambiente **PATH** do sistema Windows.
  2. Reinicie o sistema Windows para que as mudanças entrem em vigor.
- Pode ser necessário fornecer as seguintes informações, de acordo com seu ambiente durante a configuração do agente. Se você não souber o valor de configuração apropriado para especificar, reúna as informações do administrador do IBM MQ (WebSphere MQ) e do IBM Integration Bus.
  - Se o IBM MQ (WebSphere MQ) estiver instalado no mesmo sistema com o IBM Integration Bus agent, é preciso fornecer o caminho da biblioteca de 64 bits do IBM MQ (WebSphere MQ).
  - Se o IBM Integration Bus agent estiver configurado para monitorar os nós de integração do IBM Integration Bus V10 ou IBM App Connect Enterprise V11, será necessário fornecer o diretório de instalação para o IBM Integration Bus V10 ou IBM App Connect Enterprise V11.
  - Se desejar que o IBM Integration Bus agent monitore alguns nós de integração (brokers) específicos em vez de todos no mesmo sistema, é preciso fornecer o nome e caminho da instalação de cada nó de integração (broker).

Sobre Esta Tarefa

O IBM Integration Bus agent é um agente de múltiplas instâncias; você deve criar a primeira instância e iniciar o agente manualmente.

É possível optar por configurar o agente com ou sem interações em sistemas UNIX ou Linux. Em sistemas Windows, é possível configurar o agente somente sem interações.

- Para configurar o agente com interação, execute o script de configuração e responda aos prompts. Consulte "Configuração interativa" na página 276.
- Para configurar o agente sem interação, edite o arquivo silencioso de resposta e execute o script de configuração. Consulte "Configuração silenciosa" na página 277.

Importante: Se você também instalou o ITCAM Agent for WebSphere Message Broker, que é entregue como um dos produtos ITCAM for Applications no mesmo sistema que o IBM Integration Bus agent, que é entregue no Cloud APM, não use-os para monitorar o mesmo nó de integração (broker) no sistema.

Configuração interativa

Procedimento

Para configurar o agente executando o script e respondendo aos prompts, conclua as seguintes etapas:

1. Insira o seguinte comando:

   ```
   install_dir/bin/iib-agent.sh config instance_name
   ```

   em que *instance_name* é o nome que você deseja fornecer à instância de agente.

   Importante: A configuração interativa não é suportada em sistemas Windows.
2. Depois de confirmar que deseja configurar o IBM Integration Bus agent, especifique os valores de configuração para configurações gerais do agente.
   a) Quando for solicitado o parâmetro **Agent Id**, especifique uma sequência alfanumérica exclusiva com um comprimento máximo de 8 caracteres.

      Lembre-se: O comprimento máximo do ID do agente é mudado para oito caracteres a partir do IBM Integration Bus agent versão 7.3.0.1. Para versões anteriores, o comprimento máximo do ID do agente é quatro caracteres.

      O nome do sistema gerenciado inclui o ID de agente especificado, por exemplo, *monitoredbrokername*:*agentID*:KQIB, em que *monitoredbrokername* é o nome do nó de integração (broker) monitorado.
   b) Quando for solicitado o parâmetro **IIB version 10 or ACE version 11** Install Directory, se você quiser monitorar os nós de integração do IBM Integration Bus V10, ou IBM App Connect Enterprise V11, especifique o diretório de instalação do IBM Integration Bus V10 ou IBM App Connect Enterprise V11. Por exemplo, `/opt/ibm/mqsi/ace-11.0.0.3`. Se não quiser monitorar o IBM Integration Bus V10 e o IBM App Connect Enterprise V11, pressione Enter para aceitar o padrão.

      Lembre-se: É possível especificar apenas um diretório de instalação para o parâmetro **IIB version 10 or ACE version 11** do Install Directory. Caso tenha instalado o IBM Integration Bus V10 ou IBM App Connect Enterprise V11 em diretórios diferentes e queira monitorar todos eles, crie várias instâncias do agente e especifique um diretório de instalação do IBM Integration Bus V10 ou do IBM App Connect Enterprise V11 para cada instância do agente.
3. Opcional: Use a seção **Configurações do broker monitorado** para especificar se você deseja usar esse agente para monitorar somente alguns nós de integração (brokers) específicos.

   Por padrão, todos os nós de integração (brokers) que estão em execução no mesmo sistema host que o IBM Integration Bus agent são monitorados, conforme determinado pela autodescoberta. Se desejar que o agente monitore alguns nós de integração (brokers) específicos, especifique o nome do nó de integração (broker) que você deseja monitorar e defina a configuração de **Coletar dados do nó** como No, que é o valor padrão, na seção **Configurações do broker monitorado**. Pode haver várias seções de **Configurações do Broker Monitorado**. Cada seção controla as configurações de monitoramento para um nó de integração (broker).

   Dica: É possível especificar mais de uma seção **Configurações do Broker Monitorado**. Ao editar a seção **Configurações do Broker Monitorado**, as opções a seguir estão disponíveis:

- Incluir: crie uma seção **Configurações do broker monitorado** para configurar para outro nó de integração (broker).
- Editar: Modifique as configurações da seção **Configurações do Broker Monitorado** atual.
- Del: Exclua a seção **Configurações do Broker Monitorado** atual.
- Avançar: Mova para a próxima seção **Configurações do Broker Monitorado**.
- Sair: Saia da definição de **Configurações do Broker Monitorado**.

4. Se você confirmar que o IBM MQ (WebSphere MQ) está instalado no mesmo sistema, será solicitado o parâmetro **WebSphere MQ 64-bit library path**. Pressione Enter para aceitar o valor padrão, que é o caminho da biblioteca de 64 bits do IBM MQ (WebSphere MQ) descoberto automaticamente pelo agente. Se nenhum valor padrão for exibido, será preciso fornecer o caminho da biblioteca de 64 bits do IBM MQ (WebSphere MQ) antes de continuar com a próxima etapa. Por exemplo, `/opt/mqm8/lib64`.

   Lembre-se: Se seus nós de integração (brokers) usam diferentes versões de gerenciadores de filas, especifique a versão mais recente do caminho da biblioteca de 64 bits do IBM MQ (WebSphere MQ) para esse parâmetro.
5. Após a conclusão da configuração, insira o seguinte comando para iniciar o agente:

```
install_dir/bin/iib-agent.sh start
instance_name
```

Configuração silenciosa

Procedimento

Para configurar o agente ao editar o arquivo de resposta silenciosa e executar o script sem nenhuma interação, conclua as seguintes etapas:

1. Abra o seguinte arquivo de resposta silencioso do agente em um editor de texto.
   - Linux AIX *install_dir*/samples/iib_silent_config.txt
   - Windows *install_dir*\tmaitm6_x64\samples\qi_silent_config.txt

   em que *install_dir* é o diretório de instalação do IBM Integration Bus agent. O diretório de instalação padrão é como a seguir:
   - Linux AIX /opt/ibm/apm/agent
   - Windows C:\IBM\APM
2. Para o parâmetro **agentId**, especifique uma sequência alfanumérica exclusiva com um comprimento máximo de 8 caracteres como um breve identificador para o agente.

   Lembre-se: O comprimento máximo do ID do agente é mudado para oito caracteres a partir do IBM Integration Bus agent versão 7.3.0.1. Para versões anteriores, o comprimento máximo do ID do agente é quatro caracteres.

   O nome do sistema gerenciado inclui o ID de agente especificado, por exemplo, *monitoredbrokername*:*agentID*:KQIB, em que *monitoredbrokername* é o nome do nó de integração (broker) monitorado.
3. Se quiser monitorar os nós de integração do IBM Integration Bus V10 ou IBM App Connect Enterprise V11, especifique o diretório de instalação para o IBM Integration Bus V10 ou IBM App Connect Enterprise V11 para o parâmetro **defaultWMBInstallDirectory**. Por exemplo, `C:\Program Files\IBM\ACE\11.0.0.3\` para um sistema Windows ou `/opt/ibm/mqsi/ace-11.0.0.3` para um sistema Linux. Se você não quiser monitorar o IBM Integration Bus V10 e o IBM App Connect Enterprise V11, esse parâmetro não será necessário, pois o IBM Integration Bus agent pode descobrir automaticamente os nós de integração (brokers) de versões anteriores.

   Lembre-se: É possível especificar somente um diretório de instalação para o parâmetro **defaultWMBInstallDirectory**. Caso tenha instalado o IBM Integration Bus V10 ou IBM App

Connect Enterprise V11 em diretórios diferentes e queira monitorar todos eles, crie várias instâncias do agente e especifique um diretório de instalação do IBM Integration Bus V10 ou do IBM App Connect Enterprise V11 para cada instância do agente.

4. Opcional: Especifique se desejar usar esse agente para monitorar somente alguns nós de integração (brokers) específicos.

   Por padrão, todos os nós de integração (brokers) que estão em execução no mesmo sistema host que o IBM Integration Bus agent são monitorados, conforme determinado pela autodescoberta. Para monitorar nós de integração (brokers) específicos, configure os parâmetros **collectNodeData** e **WMBInstallDirectory** para cada nó de integração (broker) que você deseja monitorar.

   collectNodeData
   Especifica se os dados de definição de nó são coletados para o nó de integração (broker) monitorado. A sintaxe é `collectNodeData.`*`brkr_name`*`=NO|YES`, em que *brkr_name* é o nome do nó de integração (broker).

   O valor padrão é NO. É recomendado usar o valor padrão porque os dados de definição de nó não são suportados no Console do Cloud APM.

   WMBInstallDirectory
   O diretório de instalação do nó de integração (broker) a ser monitorado. A sintaxe é `WMBInstallDirectory.`*`brkr_name=broker_install_dir`*, em que *broker_install_dir* é o diretório de instalação do nó de integração (broker) a ser monitorado.

   Lembre-se: Para um nó de integração da versão 10, o parâmetro **WMBInstallDirectory** pode substituir o parâmetro **defaultWMBInstallDirectory** configurado na etapa anterior.

   Por exemplo, para monitorar somente dois nós de integração (brokers) chamados BK1 e BK2, configure os parâmetros conforme a seguir:

   ```
   collectNodeData.BK1=NO
   collectNodeData.BK2=NO
   WMBInstallDirectory.BK1=BK1_install_dir
   WMBInstallDirectory.BK2=BK2_install_dir
   ```

5. Para monitorar brokers que são anteriores ao IBM Integration Bus V10, especifique o caminho da biblioteca de 64 bits do IBM MQ(WebSphere MQ) para o parâmetro **WMQLIBPATH**. Por exemplo, `C:\Program Files\IBM\WebSphere MQ\bin64` para um sistema Windows ou `/opt/mqm8/lib64` para um sistema Linux.

   Lembre-se: Se seus nós de integração (brokers) usam diferentes versões de gerenciadores de filas, especifique a versão mais recente do caminho da biblioteca de 64 bits do IBM MQ (WebSphere MQ) para esse parâmetro.

6. Salve e feche o arquivo de resposta silencioso do agente e, em seguida, insira o comando a seguir:

   - Linux AIX *`install_dir`*`/bin/iib-agent.sh config `*`instance_name path_to_responsefile`*
   - Windows *`install_dir`*`\BIN\iib-agent.bat config "`*`instance_name path_to_responsefile`*`"`

   em que *instance_name* é o nome da instância que você configura e *path_to_responsefile* é o caminho completo do arquivo de resposta silencioso.

   Aviso: Em sistemas Windows, não inclua aspas duplas ("") que delimitam o caminho completo para o arquivo de resposta silencioso, já que isso causará um erro de configuração.

7. Após a conclusão da configuração, insira o seguinte comando para iniciar o agente:

   - Linux AIX

     ```
     install_dir/bin/iib-agent.sh start
     instance_name
     ```

   - Windows

```
install_dir\bin\iib-agent.bat start instance_name
```

Resultados

Agora, é possível efetuar login no Console do Cloud APM e usar o Editor de aplicativos para incluir a instância do IBM Integration Bus agent no Application Performance Dashboard. Para obter instruções sobre como iniciar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975. Para obter informações sobre como usar o Editor de aplicativos, consulte "Gerenciando aplicativos" na página 1098.

Lembre-se: Sempre que você atualizar ou migrar um nó de integração (broker) monitorado, deve reiniciar o IBM Integration Bus agent após o upgrade ou migração do nó de integração (broker).

O que Fazer Depois

A próxima etapa é configurar o IBM Integration Bus para ativação de dados. Os seguintes dados estarão disponíveis no Application Performance Dashboard somente após terem sido ativados no IBM Integration Bus:

- Contabilidade e estatísticas de archive
- Estatísticas de recursos da JVM
- Rastreamento de transação

Para obter instruções, veja "Configurando o IBM Integration Bus para ativação de dados" na página 279.

Configurando o IBM Integration Bus para ativação de dados

Para que alguns dados estejam disponíveis no Console do Cloud APM, deve-se configurar o IBM Integration Bus para ativar a coleta de dados necessária.

Antes de Iniciar

Certifique-se de que o IBM Integration Bus agent esteja configurado.

Lembre-se: A ativação do rastreamento de transação requer que o nó de integração (broker) seja reiniciado.

Sobre Esta Tarefa

As estatísticas de archive e as estatísticas de recursos podem ser monitoradas pelo IBM Integration Bus agent somente após a ativação da coleta de dados para o nó de integração (broker). Da mesma forma, se você desejar ver o rastreamento de transação nos painéis de middleware e de topologia, é preciso ativar o rastreamento de transação no nó de integração (broker) antes de ativar o rastreamento de transação para o IBM Integration Bus agent.

Decida que tipo de dados você deseja monitorar com o IBM Integration Bus agent e conclua as seguintes etapas, de acordo com suas necessidades.

Servidores de integração pertencentes ao nó de integração têm um arquivo de configuração `server.conf.yaml` padrão para cada servidor de integração armazenado em um subdiretório do diretório de nós de integração. Quaisquer propriedades que você configurar para o nó de integração no arquivo `node.conf.yaml` serão herdadas pelos servidores de integração que ele possui. Entretanto, é possível alterar as propriedades do servidor de integração modificando-as nesse arquivo `server.conf.yaml`. (Para obter mais informações, consulte Configurando um nó de integração modificando o arquivo node.conf.yaml na documentação do IBM App Connect Enterprise.)

Procedimento

- Para ativar a coleta de dados de estatísticas de archive para o nó de integração (broker), consulte "Ativando a coleta de dados de contabilidade e estatísticas de archive" na página 280.

- Para ativar os dados de estatísticas de recursos para um nó de integração (broker), consulte "Ativando estatísticas de recursos da JVM" na página 283.
- Para ativar o rastreamento de transação para fluxos de mensagens em um nó de integração (broker), consulte "Ativando o rastreamento de transações" na página 284.
- Se você não desejar mais os dados de rastreamento de transação, lembre-se de desativar o rastreamento de transação para o nó de integração (broker) no qual ele foi ativado. Consulte "Desativando o rastreamento de transação" na página 285.

Ativando a coleta de dados de contabilidade e estatísticas de archive

Sobre Esta Tarefa

Para ativar a coleta de contabilidade e estatísticas de archive para fluxos de mensagens que pertencem ao nó de integração (broker), emita o comando **mqsichangeflowstats** a partir do diretório `bin` do diretório de instalação do nó de integração (broker).

Lembre-se: Emita o comando **mqsichangeflowstats** para o nó de integração (broker) de acordo com seus requisitos para monitoramento de dados. É recomendado ativar apenas as estatísticas que precisar, já que pode haver muitos dados e processamento quando há muitos fluxos de mensagens. Para obter informações detalhadas sobre o comando **mqsichangeflowstats**, consulte a documentação do IBM Integration Bus.

Importante: O IBM Cloud Application Performance Management não suporta dados de contabilidade e estatísticos de captura instantânea devido à quantia de dados e ao processamento necessários para o intervalo de captura instantânea configurado de 20 segundos. Os dados do archive fornecem os mesmos atributos exatos que os dados de captura instantânea, e são mais adequados para o monitoramento de produção regular fornecido pelo IBM Cloud Application Performance Management. Se você ativou a coleta de dados de captura instantânea para o nó de integração (broker), lembre-se de configurar o IBM Integration Bus agent para não armazenar os dados de captura instantânea. Para obter instruções, veja "Desativando a coleta de dados de captura instantânea para o agente" na página 286.

Procedimento

- Para obter a maioria dos dados para fluxos de mensagens, emita o seguinte comando. Esse comando é recomendado porque ele não ativa a maioria das estatísticas detalhadas do terminal que fornecem contagens de chamadas por terminal por nó. O nível de terminal consome uma grande quantidade de armazenamento.

```
mqsichangeflowstats BrokerName -a -g -j
-c active -t none -n basic -o xml
```

- No ACE versão 11, para obter a maioria dos dados para fluxos de mensagens, modifique o arquivo `node.conf.yaml` ou `server.conf.yaml` da seguinte forma. Essas propriedades são recomendadas porque não ativam as estatísticas de terminal mais detalhadas que fornecem contagens de chamadas por terminal por nó. O nível de terminal consome uma grande quantidade de armazenamento.

```
Estatísticas:
  # Os fluxos da mensagem do aplicativo herdarão, por padrão, os valores Snapshot e Archive
  # configurado aqui
  Snapshot:
    #publicationOn: 'inactive' # escolha 1 de : active|inactive, padrão inactive
                               # Assegure Events.OperationalEvents.MQ|MQTT
                               # é configurado para outputFormat json,xml
    #accountingOrigin: 'none' # escolha 1 de : none|basic
    #nodeDataLevel: 'none' # escolha 1 de : none|basic|advanced
    #outputFormat: 'usertrace' # lista separada por vírgula de :
                               #csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none' # escolha 1 de : none|basic
  Arquivo:
    archivalOn: 'active'     # choose 1 of : active|inactive,
                             # default inactive
                               # Assegure Events.OperationalEvents.MQ|MQTT
                               # é configurado para outputFormat xml
    #accountingOrigin: 'none' # escolha 1 de : none|basic
    #majorInterval: 60 # Configura o intervalo em minutos em que
```

```
                              # estatísticas de archive são publicadas
    nodeDataLevel: 'basic'          # choose 1 of : none|basic|advanced
    outputFormat: 'xml' # lista separada por vírgula de : csv,xml,usertrace
    #threadDataLevel: 'none' # escolha 1 de : none|basic
```

Nota: Se quiser desativar essa configuração, comente as linhas de **archivalOn: 'active'**, **nodeDataLevel: 'basic'** e **outputFormat: 'xml'**.

- Para obter todos os dados suportados pelo IBM Integration Bus agent, emita o seguinte comando:

```
mqsichangeflowstats
BrokerName -a -g -j -c active -t none -n advanced
-o xml
```

- No ACE versão 11, para obter todos os dados suportados pelo IBM Integration Bus agent, modifique o arquivo `node.conf.yaml` ou `server.conf.yaml` da seguinte forma:

```
Estatísticas:
  # Os fluxos da mensagem do aplicativo herdarão, por padrão, os valores Snapshot e Archive
  # configurado aqui
  Instantâneo:
    #publicationOn: 'inactive' # escolha 1 de : active|inactive, padrão inactive
                               # Assegure Events.OperationalEvents.MQ|MQTT
                               # é configurado para outputFormat json,xml
    #accountingOrigin: 'none' # escolha 1 de : none|basic
    #nodeDataLevel: 'none' # escolha 1 de : none|basic|advanced
    #outputFormat: 'usertrace' # lista separada por vírgula de :
                               # csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none' # escolha 1 de : none|basic
  Arquivo:
    archivalOn: 'active' # escolha 1 de : active|inactive, padrão inactive
                               # Assegure Events.OperationalEvents.MQ|MQTT
                               # é configurado para outputFormat xml
    #accountingOrigin: 'none' # escolha 1 de : none|basic
    #majorInterval: 60 # Configura o intervalo em minutos em que
                              # estatísticas de archive são publicadas
    nodeDataLevel: 'advanced'     # choose 1 of : none|basic|advanced
    outputFormat: 'xml' # lista separada por vírgula de : csv,xml,usertrace
    #threadDataLevel: 'none' # escolha 1 de : none|basic
```

Nota: Se quiser desativar essa configuração, comente as linhas de **archivalOn: 'active'**, **nodeDataLevel: 'advanced'** e **outputFormat: 'xml'**.

- Para reduzir a quantia de dados, mas ainda monitorar razoavelmente todos os fluxos de mensagens sem detalhes adicionais, emita o seguinte comando:

```
mqsichangeflowstats BrokerName -a -g -j
-c active -t none -n none -o xml
```

- No ACE versão 11, para reduzir a quantidade de dados, mas continuar monitorando de forma razoável todos os fluxos de mensagens sem detalhes adicionais, modifique o arquivo `node.conf.yaml` ou `server.conf.yaml` da seguinte forma:

```
Estatísticas:
  # Os fluxos da mensagem do aplicativo herdarão, por padrão, os valores Snapshot e Archive
  #set here
  Instantâneo:
    #publicationOn: 'inactive' # escolha 1 de : active|inactive, padrão inactive
                               # Assegure Events.OperationalEvents.MQ|MQTT
                               # é configurado para outputFormat json,xml
    #accountingOrigin: 'none' # escolha 1 de : none|basic
    #nodeDataLevel: 'none' # escolha 1 de : none|basic|advanced
    #outputFormat: 'usertrace' # lista separada por vírgula de :
                               # csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none' # escolha 1 de : none|basic
  Arquivo:
    archivalOn: 'active' # escolha 1 de : active|inactive, padrão inactive
                               # Assegure Events.OperationalEvents.MQ|MQTT
                               # é configurado para outputFormat xml
    #accountingOrigin: 'none' # escolha 1 de : none|basic
    #majorInterval: 60 # Configura o intervalo em minutos em que
                              # estatísticas de archive são publicadas
    nodeDataLevel: 'none'          # choose 1 of : none|basic|advanced
    outputFormat: 'xml' # lista separada por vírgula de : csv,xml,usertrace
    #threadDataLevel: 'none' # escolha 1 de : none|basic
```

Nota: Se quiser desativar essa configuração, comente as linhas de **archivalOn: 'active'**, **nodeDataLevel: 'none'** e **outputFormat: 'xml'**.

- Se você tiver uma grande quantidade de fluxos de mensagens e desejar reduzir a quantidade de dados, é possível especificar quais fluxos de mensagens monitorar, substituindo a opção `-g` ou `-j` nos comandos mencionados anteriormente.
  - Para especificar um servidor de integração específico (grupo de execução) para ativação, substitua `-g` por `-e` *`IntegrationServerName`*.
  - Para identificar um fluxo de mensagens específico para ativação, substitua `-j` por `-f` *`MessageFlowName`*.
  - Se você agrupou fluxos de mensagens em aplicativos, para especificar um determinado aplicativo para ativação, inclua `-k` *`ApplicationName`* na opção `-j`.
- O IBM Integration Bus agent coleta dados de contabilidade e de estatísticas de archive no intervalo de 5 minutos. Para configurar o intervalo em que o nó de integração (broker) produz dados de contabilidade e de estatísticas de archive para o mesmo intervalo, emita o seguinte comando com o nó de integração (broker) parado e, em seguida, reinicie o nó de integração (broker):

```
mqsichangebroker BrokerName -v 5
```

- No ACE versão 11, o IBM Integration Bus agent coleta dados de contabilidade e de estatísticas de archive no intervalo de 5 minutos. Para configurar o intervalo no qual o nó de integração (broker) produz os dados estatísticos e contábeis do archive para o mesmo intervalo, modifique o arquivo `node.conf.yaml` ou `server.conf.yaml` da seguinte forma:

```
Estatísticas:
  # Os fluxos da mensagem do aplicativo herdarão, por padrão, os valores Snapshot e Archive
  # configurado aqui
  Instantâneo:
    #publicationOn: 'inactive' # escolha 1 de : active|inactive, padrão inactive
                               # Assegure Events.OperationalEvents.MQ|MQTT
                               # é configurado para outputFormat json,xml
    #accountingOrigin: 'none' # escolha 1 de : none|basic
    #nodeDataLevel: 'none' # escolha 1 de : none|basic|advanced
    #outputFormat: 'usertrace' # lista separada por vírgula de :
                               # csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none' # escolha 1 de : none|basic
  Arquivo:
    archivalOn: 'active' # escolha 1 de : active|inactive, padrão inactive
                               # Assegure Events.OperationalEvents.MQ|MQTT
                               # é configurado para outputFormat xml
    #accountingOrigin: 'none' # escolha 1 de : none|basic
    majorInterval: 5         # Sets the interval in minutes at which
                             # estatísticas de archive são publicadas
    nodeDataLevel: 'none'         # choose 1 of : none|basic|advanced
    outputFormat: 'xml' # lista separada por vírgula de : csv,xml,usertrace
    #threadDataLevel: 'none' # escolha 1 de : none|basic
```

Resultados

Quando o IBM Integration Bus agent estiver configurado e iniciado, os dados de contabilidade e de estatísticas de fluxo de mensagens são exibidos nos seguintes widgets de grupo:

- Painel do Fluxo de Mensagens
  - Confirmações e Restaurações
  - Microssegundos de CPU
  - Microssegundos Decorridos
  - Taxa de Bytes de Entrada
  - Taxa da Mensagem de Entrada
  - Tamanho da Mensagem de Entrada
  - Microssegundos da CPU de Espera da Mensagem de Entrada
  - Microssegundos Decorridos de Espera da Mensagem de Entrada

  - Erros do Fluxo de Mensagens
  - Estatísticas do Nó de Processamento de Mensagens
- Painel do Nó de Processamento
  - Microssegundos de CPU
  - Microssegundos Decorridos
  - Chamadas
  - Status do Nó de Processamento
  - Estatísticas do Terminal

Ativando estatísticas de recursos da JVM

Sobre Esta Tarefa
Para ativar estatísticas de recursos da JVM para servidores de integração que pertencem ao nó de integração (broker), emita o comando **mqsichangeresourcestats** a partir do diretório `bin` do diretório de instalação do nó de integração (broker).

Lembre-se: As estatísticas de recursos da JVM são consideradas opcionais porque somente alguns atributos de dados são exibidos para o alto custo do agente que processa esses dados a cada 20 segundos. Assegure-se de considerar se realmente precisa dos dados estatísticos do recurso da JVM.

Procedimento

- Para ativar as estatísticas em todos os servidores de integração no nó de integração (broker), emita o seguinte comando:

```
mqsichangeresourcestats BrokerName -c
active
```

- No ACE versão 11, para ativar as estatísticas em todos os servidores de integração no nó de integração (broker), modifique o arquivo `node.conf.yaml`, conforme a seguir:

```
Estatísticas:
  # Os fluxos da mensagem do aplicativo herdarão, por padrão, os valores Snapshot e Archive
  # configurado aqui
  Instantâneo:
    #publicationOn: 'inactive' # escolha 1 de : active|inactive, padrão inactive
                               # Assegure Events.OperationalEvents.MQ|MQTT
                               # é configurado para outputFormat json,xml
    #accountingOrigin: 'none' # escolha 1 de : none|basic
    #nodeDataLevel: 'none' # escolha 1 de : none|basic|advanced
    #outputFormat: 'usertrace' # lista separada por vírgula de :
                               # csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none' # escolha 1 de : none|basic
  Arquivo:
    archivalOn: 'active' # escolha 1 de : active|inactive, padrão inactive
                               # Assegure Events.OperationalEvents.MQ|MQTT
                               # é configurado para outputFormat xml
    #accountingOrigin: 'none' # escolha 1 de : none|basic
    majorInterval: 5 # Configura o intervalo em minutos em que
                           # estatísticas de archive são publicadas
    nodeDataLevel: 'advanced' # escolha 1 de : none|basic|advanced
    outputFormat: 'xml' # lista separada por vírgula de : csv,xml,usertrace
    threadDataLevel: 'basic' # escolha 1 de : none|basic
   Recurso:
     reportingOn: true # escolha 1 de : true|false, padrão false
......
```

Nota: Se você deseja desativar essa configuração, comente **reportingOn: true**.

- Para ativar as estatísticas para um servidor de integração especificado no nó de integração (broker), emita o seguinte comando:

```
mqsichangeresourcestats BrokerName -e
IntegrationServerName -c active
```

- No ACE versão 11, para ativar as estatísticas para um determinado servidor de integração no nó de integração (broker), modifique o arquivo `server.conf.yaml`, conforme a seguir:

```
Estatísticas:
  # Os fluxos da mensagem do aplicativo herdarão, por padrão, os valores Snapshot e Archive
  # configurado aqui
  Instantâneo:
    #publicationOn: 'inactive' # escolha 1 de : active|inactive, padrão inactive
                               # Assegure Events.OperationalEvents.MQ|MQTT
                               # é configurado para outputFormat json,xml
    #accountingOrigin: 'none' # escolha 1 de : none|basic
    #nodeDataLevel: 'none' # escolha 1 de : none|basic|advanced
    #outputFormat: 'usertrace' # lista separada por vírgula de :
                               # csv,bluemix,json,xml,usertrace
    #threadDataLevel: 'none' # escolha 1 de : none|basic
  Arquivo:
    archivalOn: 'active' # escolha 1 de : active|inactive, padrão inactive
                               # Assegure Events.OperationalEvents.MQ|MQTT
                               # é configurado para outputFormat xml
    #accountingOrigin: 'none' # escolha 1 de : none|basic
    majorInterval: 5 # Configura o intervalo em minutos em que
                           # estatísticas de archive são publicadas
    nodeDataLevel: 'advanced' # escolha 1 de : none|basic|advanced
    outputFormat: 'xml' # lista separada por vírgula de : csv,xml,usertrace
    threadDataLevel: 'basic' # escolha 1 de : none|basic
  Recurso:
    reportingOn: true # escolha 1 de : true|false, padrão false
```

Nota: Se você deseja desativar essa configuração, comente **reportingOn: true**.

Resultados

Os dados de estatísticas de recursos do JVM são exibidos nos seguintes widgets de grupo:

- Contagem de Coletas de Lixo
- Duração da Coleta de Lixo
- Memória Não Heap da JVM
- Memória Heap da JVM

Ativando o rastreamento de transações

Antes de Iniciar

1. Certifique-se de que o IBM Integration Bus agent esteja instalado. Uma saída de usuário denominada `KQIUserExit` é fornecida para ativar o IBM Integration Bus para rastreamento de transação.
2. Certifique-se de que o usuário que irá iniciar o nó de integração (broker) tenha acesso ao diretório do módulo de Saída de usuário KQI. Ou seja, certifique-se de incluir o ID do usuário que é usado para iniciar o nó de integração (broker) para o grupo com o qual foi instalado o IBM Integration Bus agent.

Sobre Esta Tarefa

Deve-se implementar a saída de usuário `KQIUserExit` no nó de integração (broker). Caso contrário, nenhum dado estará disponível nos painéis de middleware e topologia, mesmo após você ter ativado o IBM Integration Bus agent para o rastreamento de transações.

Dica: Os nós do IBM Integration Bus a seguir estão incluídos nos painéis de middleware e topologia pela saída de usuário `KQIUserExit` como serviços não instrumentados:

- Nós de banco de dados e de cálculo quando uma origem de dados ODBC for especificada
- Nós TCP/IP
- Nós de arquivos para servidores FTP ou FTPS remotos
- Nós MQ, a menos que já tenham sido instrumentados

Procedimento

Para ativar o rastreamento da transação para o IBM Integration Bus, conclua as seguintes etapas:

1. Linux AIX
   Feche qualquer shell de broker que tenha carregado o ambiente MQSI.
2. Abra um console do comando do IBM Integration Bus com um dos seguintes métodos. Se você tiver várias versões de nós de integração (brokers) instaladas, certifique-se de iniciar o console de comando para a versão correta.
   - Windows Clique em **Iniciar** > **IBM Integration Bus** > **IBM Integration Console**
   - Linux AIX No diretório `bin` do diretório de instalação do nó de integração (broker), emita o comando **mqsiprofile**.
3. Pare o nó de integração (broker) que você deseja configurar com o comando **mqsistop**.
4. Ative o rastreamento de transação para o fluxo de mensagens no nó de integração (broker), incluindo a saída de usuário KQIUserExit com o comando **mqsichangebroker**.
   - Para ativar o rastreamento de transação para todos os fluxos de mensagens no nó de integração (broker), execute o seguinte comando:

     ```
     mqsichangebroker broker_name -e "KQIUserExit"
     ```

   - Para ativar o rastreamento de transação para um fluxo de mensagens específico no nó de integração (broker), execute o seguinte comando:

     ```
     mqsichangeflowuserexits broker_name -e execution_group_name -k application_name -f
     message_flow_name -a "KQIUserExit"
     ```

5. Como alternativa, no Ace versão 11, ative o rastreamento de transação para o fluxo de mensagens no nó de integração (broker) incluindo o `KQIUserExit` no arquivo `node.conf.yaml` ou arquivo `server.conf.yaml`.

   ```
   UserExits:
   activeUserExitList: 'KQIUserExit' # Especifique o nome
   #de uma saída de usuário instalada para ativar.
   ```

   Nota: Se quiser desativar o rastreamento de transação, comente **activeUserExitList: 'KQIUserExit'**.
6. Reinicie o nó de integração (broker) com o comando **mqsistart**.

Desativando o rastreamento de transação

Procedimento

Para desativar o rastreamento de transações para o IBM Integration Bus, conclua as etapas a seguir:

1. Abra um console do comando do IBM Integration Bus com um dos seguintes métodos. Se você tiver várias versões de nós de integração (brokers) instaladas, certifique-se de iniciar o console de comando para a versão correta.
   - Windows Clique em **Iniciar** > **IBM Integration Bus** > **IBM Integration Console**
   - Linux AIX No diretório `bin` do diretório de instalação do nó de integração (broker), emita o comando **mqsiprofile**.
2. Desative o rastreamento de transação para o fluxo de mensagens em um nó de integração (broker) com um dos seguintes métodos:
   - Para desativar o rastreamento de transações para um fluxo de mensagens específico, use o comando **mqsichangeflowuserexits**:

     ```
     mqsichangeflowuserexits broker_name -e execution_group_name
     -f message_flow_name -a ""
     ```

- Para desativar o rastreamento de transação para todos os fluxos de mensagens no nó de integração (broker), primeiro pare o nó de integração (broker) com o comando **mqsistop** e, em seguida, emita o comando **mqsichangebroker**:

```
mqsichangebroker broker_name -e ""
```

O que Fazer Depois

- Para rastreamento de transação, depois de ativar o rastreamento de transação para o IBM Integration Bus, também é preciso ativar o rastreamento de transação para o agente. Para obter instruções, veja "Configurando o rastreamento de transações para o IBM Integration Bus agent" na página 286.
- Se você ativou a coleta de dados de captura instantânea para seu nó de integração (broker), configure o IBM Integration Bus agent para não armazenar dados de captura instantânea. O Cloud APM não suporta dados de contabilidade e estatísticos de captura instantânea devido à quantia de dados e ao processamento necessários para o intervalo de captura instantânea configurado de 20 segundos. Para obter instruções, veja "Desativando a coleta de dados de captura instantânea para o agente" na página 286.

Desativando a coleta de dados de captura instantânea para o agente

O Cloud APM não suporta dados de contabilidade e estatísticos de captura instantânea devido à quantia de dados e ao processamento necessários para o intervalo de captura instantânea configurado de 20 segundos. Caso você tenha ativado a coleta de dados de captura instantânea para o broker, lembre-se de configurar o IBM Integration Bus agent para não armazenar os dados de captura instantânea.

Procedimento

1. Abra o arquivo de configuração do agente em um editor de texto. O arquivo de configuração do agente está em um dos seguintes diretórios, dependendo do sistema operacional:
   - Linux AIX *install_dir*/config/<*hostname*>_qi_<*instance_name*>.cfg
   - Windows *install_dir*\TMAITM6_x64\<*hostname*>_qi_<*instance_name*>.cfg

   em que *install_dir* é o diretório de instalação do agente; *hostname* é o nome do host do sistema operacional; *instance_name* é o nome da instância do agente.
2. Edite o arquivo incluindo o seguinte parâmetro na seção KqiAgent:

```
defaultRetainRecentSnapshotSamples=0
```

   Por exemplo:

```
INSTANCE=inst1 [
SECTION=KqiAgent [ { agentId=inst1 } { instName=inst1 }
{defaultRetainRecentSnapshotSamples=0}]
SECTION=MonitorBroker:BRK1 [ { collectNodeData=NO } ]
SECTION=MonitorBroker:BRK2 [ { collectNodeData=NO } ]
]
```

3. Salve e feche o arquivo.
4. Reinicie o agente IBM Integration Bus agent para que as mudanças tenham efeito.

Configurando o rastreamento de transações para o IBM Integration Bus agent

Os dados de rastreamento de transações para o IBM Integration Bus podem ser exibidos nos painéis de middleware e de topologia após a ativação da coleta de dados na página **Configuração do agente** para o IBM Integration Bus agent.

Antes de Iniciar

- Certifique-se de que o rastreamento de transação esteja ativado para o IBM Integration Bus com a saída de usuário fornecida pelo agente chamada `KQIUserExit`. Se você não tiver feito isso, siga as instruções em "Ativando o rastreamento de transações" na página 284.
- Certifique-se de que o IBM Integration Bus agent esteja configurado corretamente. Se você não tiver feito isso, siga as instruções em "Configurando o IBM Integration Bus agent" na página 275.

Procedimento

Para configurar o rastreamento de transação para o IBM Integration Bus agent, conclua as etapas a seguir:

1. A partir da barra de navegação, clique em **Configuração do Sistema** > **Configuração do Agente**.
   A página **Configuração do Agente** é exibida.
2. Clique na guia **IBM Integration Bus**.
3. Selecione as caixas de seleção para as instâncias do agente e execute uma das ações a seguir a partir da lista de **Ações**:
   - Para ativar o rastreamento de transações, clique em **Configurar rastreamento de transações** > **Ativado**. O status na coluna **Rastreamento de Transação** é atualizado para Ativado.
   - Para desativar os dados de rastreamento de transações, clique em **Configurar Rastreamento de Transação** > **Desativado**. O status na coluna **Rastreamento de Transação** é atualizado para Desativado.

Resultados

Você configurou o rastreamento de transação para as instâncias de agente selecionadas. Os dados de rastreamento de transação podem ser exibidos nos painéis de middleware e topologia após você ativar a coleta de dados. Veja informações adicionais na publicação "Incluindo aplicativos middleware no Painel de Desempenho do Aplicativo " na página 96.

Especificando um nome do sistema gerenciado exclusivo para o IBM Integration Bus agent

O nome da instância do IBM Integration Bus agent exibido no Console do Cloud APM também é conhecido como o nome do sistema gerenciado (MSN). É possível usar o parâmetro de configuração do agente para especificar um MSN exclusivo para cada instância do agente.

Sobre Esta Tarefa

Quando o IBM Integration Bus agent é iniciado, ele registra o MSN no formato de *monitoredbrokername*:*agentID*:KQIB para cada instância do agente, em que *monitoredbrokername* é o nome do broker monitorado e *agentID* é o ID do agente que é configurado pelo parâmetro de configuração do agente. O comprimento máximo do MSN é de 32 caracteres. Se o comprimento do MSN exceder 32 caracteres, ele será truncado.

Um MSN exclusivo pode ser necessário nas seguintes circunstâncias:

- Você está executando mais de um IBM Integration Bus agent no mesmo sistema.
- Você está executando mais de um broker monitorado com o mesmo nome em sistemas diferentes.

Para especificar um ID de agente para obter um MSN exclusivo, use a opção **`Agent Id`** durante a configuração interativa ou use o parâmetro **`agentId`** no arquivo de resposta silencioso.

Lembre-se: Se você não tiver configurado o IBM Integration Bus agent pela primeira vez após a instalação, siga as etapas conforme documentado em "Configurando o IBM Integration Bus agent" na página 275.

Procedimento

- Para usar a opção **Agent Id** durante a configuração interativa, conclua as seguintes etapas:
  a) Insira o seguinte comando:

  ```
  install_dir/bin/iib-agent.sh config instance_name
  ```

  em que *instance_name* é o nome da instância de agente para a qual você deseja especificar um ID de agente.
  b) Siga as opções para configurar a instância de agente.
  Se nenhuma mudança for necessária para uma opção, use o valor padrão.
  c) Quando a opção `Agent Id` aparece, especifique o qualificador intermediário para o nome do sistema gerenciado.
  O formato válido é uma sequência alfanumérica com um comprimento máximo de oito caracteres.
- Para usar o parâmetro **agentId** no arquivo de resposta silencioso, conclua as seguintes etapas:
  a) Abra o seguinte arquivo de resposta silencioso do agente em um editor de texto.
  – Linux AIX *install_dir*/samples/iib_silent_config.txt
  – Windows *install_dir*\tmaitm6_x64\samples\qi_silent_config.txt
  b) Especifique um ID de agente para o parâmetro **agentId**.
  O formato válido é uma sequência alfanumérica com um comprimento máximo de oito caracteres.
  c) Salve e feche o arquivo de resposta silencioso e, em seguida, execute o seguinte comando a partir da linha de comandos:
  – Linux AIX *install_dir*/bin/iib-agent.sh config *instance_name path_to_responsefile*
  – Windows *install_dir*\BIN\iib-agent.bat config "*instance_name path_to_responsefile*"
  em que *instance_name* é o nome da instância que você configura e *path_to_responsefile* é o caminho completo do arquivo de resposta silencioso.

  Aviso: Em sistemas Windows, não inclua aspas duplas ("") que delimitam o caminho completo para o arquivo de resposta silencioso, já que isso causará um erro de configuração.
  d) Após a conclusão da configuração, insira o seguinte comando para iniciar o agente:
  – Linux AIX

  ```
  install_dir/bin/iib-agent.sh start
  instance_name
  ```

  – Windows

  ```
  install_dir\bin\iib-agent.bat start instance_name
  ```

O que Fazer Depois
Efetue login no Console do Cloud APM. Se a instância de agente com um MSN anterior ainda for exibida como off-line, edite seu aplicativo para removê-la e, em seguida, inclua a nova instância de agente com o ID de agente designado.

Removendo a saída de usuário KQIUserExit

Antes de desinstalar o IBM Integration Bus agent, primeiro você deve remover a saída de usuário `KQIUserExit`.

Procedimento

Conclua as seguintes etapas para remover a saída de usuário `KQIUserExit` implementada no IBM Integration Bus para rastreamento de transação:

1. Navegue para o diretório `bin` do IBM Integration Bus agent.
   - Windows *agent_install_dir*`\arch\qi\bin`
   - Linux AIX *agent_install_dir*`/arch/qi/bin`

   em que:
   - *agent_install_dir* é o diretório de instalação do agente. O padrão é `C:\IBM\APM` nos sistemas Windows e `/opt/ibm/apm/agent` nos sistemas Linux e AIX.
   - *arch* é o código de arquitetura da plataforma. Por exemplo, lx8266 representa o Linux Intel v2.6 (64 bits). Para obter uma lista completa dos códigos de arquitetura, consulte o arquivo *agent_install_dir*`/archdsc.tbl`.
2. Execute o script **configDC** para remover a biblioteca de saída de usuário de forma interativa:
   - Windows

     ```
     configDC.bat –disable iib_install_dir
     ```
   - Linux AIX

     ```
     ./configDC.sh –disable iib_install_dir
     ```

   em que *iib_install_dir* é o diretório de instalação do IBM Integration Bus.

Exemplo

O exemplo a seguir remove a saída de usuário fornecida pelo agente para brokers versão 9.0 que estão instalados em um sistema AIX:

```
cd /opt/IBM/ITM/aix513/qi/bin
./configDC.sh –disable /opt/IBM/mqsi/9.0
```

Configurando o monitoramento do IBM MQ Appliances

O Agente do MQ Appliance é um agente de várias instâncias. Após a instalação, deve-se configurar o agente criando uma instância de agente antes de poder iniciar o monitoramento com o agente.

Antes de Iniciar

- Estas instruções são para a liberação mais atual do agente, exceto conforme indicado.

Procedimento

- Nos sistemas Linux e UNIX, é possível configurar o agente com o script de configuração que solicita respostas ou com o arquivo de resposta silencioso.
  - “Configurando o agente respondendo aos prompts” na página 290
  - “Configurando o agente usando o arquivo silencioso de resposta” na página 290
- Nos sistemas Windows, é possível configurar o agente apenas com o arquivo de resposta silencioso.
  - “Configurando o agente usando o arquivo silencioso de resposta” na página 290

O que Fazer Depois

No Console do Cloud APM, acesse o Painel de desempenho do aplicativo para visualizar os dados que foram coletados. Para obter informações adicionais sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Se você não conseguir visualizar os dados nos painéis do agente, primeiro verifique os logs de conexão do servidor e, em seguida, os logs do provedor de dados. Os caminhos padrão para esses logs são listados aqui:

- Linux AIX `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Configurando o agente respondendo aos prompts

Deve-se designar um nome de instância para o Agente do MQ Appliance e configurar o agente antes que ele possa iniciar o monitoramento de seu IBM® MQ Appliances.

Procedimento

Para configurar o agente executando o script e respondendo aos prompts, conclua as seguintes etapas:

1. Execute o seguinte comando:

   ```
   install_dir /bin/mq_appliance-agent.sh config  instance_name
   ```

   em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome que você deseja fornecer para a instância de agente.

   Por exemplo:

   ```
   /opt/ibm/apm/agent/bin/mq_appliance-agent.sh config AQM904
   ```

2. Responda aos prompts para configurar valores de configuração para o agente.

   Consulte "Parâmetros de Configuração para o Agente do MQ Appliance" na página 292 para obter uma explicação de cada um dos parâmetros de configuração.

3. Execute o comando a seguir para iniciar o agente:

   ```
   install_dir /bin/mq_appliance-agent.sh start  instance_name
   ```

   Por exemplo:

   ```
   /opt/ibm/apm/agent/bin/mq_appliance-agent.sh start AQM904
   ```

Resultados

Agora, é possível efetuar login no console do Cloud APM e usar o Editor de aplicativos para incluir a instância do Agente do MQ Appliance no Painel de Desempenho do Aplicativo. Para obter instruções sobre como iniciar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975. Para obter informações sobre como usar o Editor de aplicativos, consulte "Gerenciando aplicativos" na página 1098.

Configurando o agente usando o arquivo silencioso de resposta

O arquivo de resposta silencioso contém os parâmetros de configuração do agente. É possível editar o arquivo de resposta silencioso para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

O arquivo silencioso de resposta contém os parâmetros de configuração do agente com valores padrão que são definidos para alguns parâmetros. É possível editar o arquivo silencioso de resposta para especificar os valores diferentes para os parâmetros de configuração.

Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

Para configurar o agente editando o arquivo silencioso de resposta e executando o script sem interação, conclua as seguintes etapas:

1. Abra o arquivo `mq_appliance_silent_config.txt` em um dos diretórios a seguir em um editor de texto.
   - Linux AIX *install_dir*`/samples/mq_appliance_silent_config.txt`
   - Windows *install_dir*`\samples\mq_appliance_silent_config.txt`

   em que, *install_dir* é o diretório de instalação do agente. Por exemplo, `/opt/ibm/apm/agent`.
2. No arquivo `mq_appliance_silent_config.txt`, especifique valores para todos os parâmetros obrigatórios e modifique os valores padrão de outros parâmetros, conforme necessário.

   Consulte "Parâmetros de Configuração para o Agente do MQ Appliance" na página 292 para obter uma explicação de cada um dos parâmetros de configuração.
3. Salve e feche o arquivo `mq_appliance_silent_config.txt` e execute o comando a seguir:
   - Linux AIX

     ```
     install_dir /bin/mq_appliance-agent.sh config  instance_name  path_to_silent_file
     ```
   - Windows

     ```
     install_dir \bin\mq_appliance-agent.bat config  instance_name  path_to_silent_file
     ```

   em que:
   - *instance_name* é o nome que você deseja fornecer para a instância de agente. Por exemplo, `AQM904`.
   - *path_to_silent_file* é o caminho para o arquivo `mq_appliance_silent_config.txt`. Por exemplo, `/opt/ibm/apm/agent/samples/mq_appliance_silent_config.txt`.
4. Após a conclusão da configuração, execute o comando a seguir para iniciar o agente:
   - Linux AIX

     ```
     install_dir /bin/mq_appliance-agent.sh start  instance_name
     ```
   - Windows

     ```
     install_dir \bin\mq_appliance-agent.bat start  instance_name
     ```

Resultados

Agora, é possível efetuar login no console do Cloud APM e usar o Editor de aplicativos para incluir a instância do Agente do MQ Appliance no Painel de Desempenho do Aplicativo. Para obter instruções sobre como iniciar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975. Para obter informações sobre como usar o Editor de aplicativos, consulte "Gerenciando aplicativos" na página 1098.

Parâmetros de Configuração para o Agente do MQ Appliance

Os parâmetros de configuração para o Agente do MQ Appliance são exibidos em tabelas que os agrupam de acordo com as seções.

- Tabela 24 na página 292: propriedades para receber eventos SNMP e decodificar eventos V3.
- Tabela 25 na página 293: propriedades para configurações Java.
- Tabela 26 na página 293: propriedades para o servidor proxy usado pelos provedores HTTP.
- Tabela 27 na página 293: propriedades para o servidor HTTP.
- Tabela 28 na página 294: propriedades para conexão com o dispositivo MQ.

Tabela 24. Parâmetros de configuração de evento SNMP

Nome de parâmetro	**Descrição**	**Nome do parâmetro no arquivo de configuração silenciosa**
Número da Porta	O número da porta que é usada para atender eventos SNMP. O padrão é 162.	KQZ_SNMPEVENT_PORT
Nível de Segurança	O nível de segurança que é usado para conexão com o evento SNMP. Pode ser um dos seguintes valores: • 1 = noAuthNoPriv • 2 = authNoPriv • 3 = authPriv O padrão é 2.	KQZ_SNMPEVENT_ SECURITY_LEVEL
Nome do Usuário	O nome do usuário que é usado para conexão com o agente do SNMP. O padrão é `snmpuser`.	KQZ_SNMPEVENT _USER_NAME
Protocolo de Autorização	O protocolo de autorização que é usado para se conectar ao agente do SNMP. Pode ser um dos seguintes valores: • 1 = MD5 • 2 = SHA O padrão é 2.	KQZ_SNMPEVENT_AUTH _PROTOCOL
Senha de Autorização	A passphrase de autorização que é usada para conexão com o agente do SNMP.	KQZ_SNMPEVENT_AUTH _PASSWORD
Senha Privativa	A passphrase de privacidade que é usada para conectar-se ao agente do SNMP.	KQZ_SNMPEVENT_PRIV _PASSWORD
Arquivo de Configuração do Trap	O local do arquivo de configuração de trap.	KQZ_SNMPEVENT_ TRAPCNFG_FILE

Tabela 25. Parâmetros de configuração Java

Nome de parâmetro	**Descrição**	**Nome do parâmetro no arquivo de configuração silenciosa**
Nível de rastreio de Java	O nível de rastreio que é usado pelos provedores Java. Pode ser um dos seguintes valores: • 1 = Desligado • 2 = Erro • 3=Warning • 4 = Informações • 5 = Depuração Mínima • 6 = Depuração Média • 7 = Depuração Máxima • 8=All O padrão é 2.	JAVA_TRACE _LEVEL

Tabela 26. Parâmetros de configuração do servidor proxy

Nome de parâmetro	**Descrição**	**Nome do parâmetro no arquivo de configuração silenciosa**
Nome do Host do Proxy	O nome do host do servidor proxy.	KQZ_HTTP _PROXXY_HOSTNAME
Porta de Proxy	O número da porta do servidor proxy. O padrão é 80.	KQZ_HTTP_PROXY_PORT
Nome de Usuário do Proxy	O nome de usuário para o servidor proxy.	KQZ_HTTP _PROXY_USER
Senha Proxy	A senha para o servidor proxy.	KQZ_HTTP _PROXY_PASSWORD

Tabela 27. Parâmetros de configuração do servidor HTTP

Nome de parâmetro	**Descrição**	**Nome do parâmetro no arquivo de configuração silenciosa**
Nome de usuário de HTTP	O nome do usuário para acessar a interface de Gerenciamento de REST do MQ Appliance.	KQZ_HTTP _USER
Senha de HTTP	A senha para acessar a interface de Gerenciamento de REST do MQ Appliance.	KQZ_HTTP _PASSWORD
Validação de Certificado Ativada	Se a validação do certificado deve ser ativada. Pode ser um dos seguintes valores: • 1=true • 2=false O padrão é 2.	KQZ_HTTP_CERTIFICATE _VALIDATION

Tabela 28. Parâmetros de configuração de conexão do dispositivo MQ		
Nome de parâmetro	**Descrição**	**Nome do parâmetro no arquivo de configuração silenciosa**
Host do Appliance ou Endereço IP	O nome do host ou o endereço IP do dispositivo MQ. O padrão é `https://hostnameoripaddress: https://9.123.123.123.`	KMK_APPLIANCE _HOST_OR _IP_ADDRESS.arm1
Número da Porta do Dispositivo	O número da porta para conexão HTTPS com o dispositivo MQ. O padrão é 5554.	KMK_APPLIANCE _PORT_NUMBER.arm1
Nome do Usuário do Dispositivo	O nome do usuário que é usado para conexão com o dispositivo MQ.	KMK_APPLIANCE _USER_NAME.arm1
Senha do Usuário do Dispositivo	A senha para o usuário do dispositivo MQ.	KMK_APPLIANCE _USER_PASSWORD.arm1
Identificação do Host do Agente	O nome do host do sistema no qual o Agente do MQ Appliance está em execução. O padrão é `9.123.123.111`.	KMK_APM_ AGENT_IDENTIFICATION .arm1
Validação de Certificado Ativada	Se a validação de certificado deve ser ativada para conexão HTTP. • 1=true • 2=false O padrão é 2.	KMK_CERTIFICATE _VALIDATION_ ENABLED.arm1

Configurando o monitoramento do InfoSphere DataStage

Você deve configurar o DataStage agent para que o agente possa coletar dados para monitorar o funcionamento e o desempenho dos recursos do servidor DataStage.

Antes de Iniciar

Revise os pré-requisitos de hardware e de software, consulte Software Product Compatibility Reports para o agente DataStage

Sobre Esta Tarefa

O DataStage agent é um agente de múltiplas instâncias. Você deve criar a primeira instância e iniciar o agente manualmente.

Muitas vezes, a versão do produto e a versão do agente diferem. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte o “Histórico de Mudanças” na página 50.

Configurando o agente nos sistemas Windows

É possível usar a janela do IBM Cloud Application Performance Management para configurar o agente em sistemas Windows.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito em **Modelo** na coluna **Tarefa/Subsistema** e clique em **Configurar usando padrões**.

   A janela **Monitoring Agent for DataStage** é aberta.
3. No campo **Inserir um nome de instância exclusivo**, digite um nome de instância do agente e clique em **OK**.
4. Na janela **Monitoring Agent for DataStage**, especifique valores para os parâmetros de configuração e clique em **OK**.

   Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração do agente" na página 297.
5. Na janela **IBM Performance Management**, clique com o botão direito na instância de agente criada e clique em **Iniciar** para iniciar o agente.

Configurando o agente nos sistemas Linux

Para configurar o agente em sistemas operacionais Linux, você deve executar o script e responder aos prompts.

Procedimento

1. Na linha de comandos, mude o caminho para o diretório de instalação do agente.
   Exemplo: `/opt/ibm/apm/agent/bin`
2. Execute o comando a seguir em que instance_name é o nome que deseja dar à instância:
   `./datastage-agent.sh config instance_name`
3. Quando a linha de comandos exibir a seguinte mensagem, digite 1 e insira:

   ```
   Edit 'Monitoring Agent for DataStage' setting? [1=Yes, 2=No]
   ```
4. Especifique valores para os parâmetros de configuração quando solicitado.

   Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração do agente" na página 297.
5. Execute o comando a seguir para iniciar o agente:

   `./datastage-agent.sh start instance_name`

Configurando Variáveis de Ambiente

É possível configurar variáveis de ambiente para mudar o comportamento do DataStage agent.

Procedimento

1. Abra o arquivo a seguir em um editor de texto:
   a) Windows *install_dir*\TMAITM6_x64\KDTENV_*instance_name*
   b) Linux *install_dir*/config/.dt.environment
2. Edite as variáveis de ambiente a seguir:
   - **KDT_FIRST_COLLECTION_INTERVAL**: o intervalo de tempo em segundos para a primeira coleta de dados. Configure esse intervalo de tempo para uma duração pela qual o agente coletaria dados anteriores da Tarefa no tempo especificado até que o agente seja iniciado. O valor padrão é 300 segundos (5 minutos). Portanto, se o agente iniciar às 14h, ele coletará os dados de execução da Tarefa de 13h55 às 14h. Isso é para evitar que a tempestade de dados da tarefa histórica seja executada quando o agente iniciar a coleta de dados. Toda coleta de dados do agente subsequente para execuções de tarefas busca apenas as execuções de tarefas recém-incluídas que ocorreram desde a última coleta.

- **KDT_SSL_CONTEXT**: o protocolo SSL que está ativado na Camada de Serviço (WebSphere Application Server). O valor padrão é TLS.
- **KDT_META_SCHEMA_NAME**: o nome do esquema do banco de dados que é criado para o repositório de metadados. O valor padrão é DSODB para Db2 e `xmeta` para bancos de dados MSSQL e Oracle.
- **KDT_DATABASE_SERVICE_NAME**: o banco de dados ou nome do serviço que é usado pelo agente para se conectar ao repositório de metadados. O valor padrão é XMETA para Db2, `xmeta` para MSSQL e `ORCL` para bancos de dados Oracle.
- **KDT_DISABLED_ATTRIBUTEGROUP**: Uma lista separada por vírgulas de grupos de atributos cuja coleta de dados precisa estar indisponível. Os valores a seguir podem ser configurados como únicos ou múltiplos para o grupo de atributos respectivo: `JobRuns`, `JobProperties`, `JobRunLog`, `JobStages`, `JobParameters`, `EngineSystemConfiguration`, `EngineSystemResources`, `EngineServiceStatus`, `EngineStatusSummary`, `JobActivity`, `AgentConfiguration` e `JobConfiguration`.

Configurando o agente usando o arquivo silencioso de resposta

O arquivo silencioso de resposta contém os parâmetros de configuração do agente. É possível editar o arquivo silencioso de resposta para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

É possível usar o arquivo de resposta silencioso para configurar o DataStage agent em sistemas Linux e Windows. Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

1. Em um editor de texto, abra o arquivo de configuração silencioso que está disponível no seguinte local e especifique valores para todos os parâmetros:

   Windows *install_dir*\samples\datastage_silent_config.txt
   Linux *install_dir*\samples\datastage_silent_config_UNIX.txt

   Windows `C:\IBM\APM\samples`

   Linux `/opt/ibm/apm/agent/samples`

   Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração do agente" na página 297.
2. Na linha de comandos, mude o caminho para *install_dir*\bin.
3. Execute o seguinte comando:

   Windows `datastage-agent.bat config` *instance_name install_dir*`\samples\datastage_silent_config.txt`
   Linux `datastage-agent.sh config` *instance_name install_dir*`\samples\datastage_silent_config_UNIX.txt`
4. Inicie o agente.

   Windows Na janela **IBM Performance Management**, clique com o botão direito na instância do agente criada e clique em **Iniciar**.
   Linux Execute o seguinte comando: `./datastage-agent.sh start` *instance_name*

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Parâmetros de configuração do agente

Ao configurar o DataStage agent, é possível mudar a camada de serviço, o repositório de metadados e os parâmetros de configuração avançada.

Parâmetros de configuração da camada de serviço

Os parâmetros de configuração que são necessários para o agente se conectar à camada de serviço.

A tabela a seguir contém descrições detalhadas dos parâmetros de configuração da camada de serviço do DataStage agent.

Tabela 29. Nomes e descrições dos parâmetros de configuração da camada de serviço

Nome do parâmetro	Descrição	Campo obrigatório
Nome do Host	Nome do host do computador no qual a camada de serviço está instalada. Se o computador for parte de um domínio, forneça o nome completo do domínio (FQDN). O valor padrão é localhost.	Sim
Porta HTTPS	Porta HTTPS para a interface REST no computador onde a camada de serviço está instalada. O valor padrão é 9443.	Sim
Nome do Usuário do WAS	O nome de usuário para conectar-se ao WebSphere Application Server. O valor padrão é wasadmin.	Sim
Senha do WAS	A senha para se conectar ao WebSphere Application Server.	Sim
Confirmar senha do WAS	A senha especificada no campo **Senha do WAS**.	Sim

Parâmetros de configuração de repositório de metadados

Os parâmetros de configuração que são necessários para o agente se conectar ao repositório de metadados.

A tabela a seguir contém descrições detalhadas dos parâmetros de configuração do repositório de metadados do DataStage agent.

Tabela 30. Nomes e descrições dos parâmetros de configuração do repositório de metadados

Nome de parâmetro	Descrição	Campo obrigatório
Tipo de Banco de dados	Tipo de banco de dados do repositório de metadados. Db2O valor padrão é 1.	Sim
Nome do Host	Nome do host do computador no qual o repositório de metadados está instalado. Se o computador for parte de um domínio, forneça o nome completo do domínio (FQDN). O valor padrão é localhost.	Sim
Porta do Banco de Dados	Porta do banco de dados no repositório de metadados para conexão JDBC. O valor padrão é 50000.	Sim
Nome de Usuário do Banco de Dados	O nome de usuário para conectar-se ao banco de dados de operações. O valor padrão é dsodb.	Sim
Senha do Banco de Dados	A senha para conectar-se ao banco de dados de operações.	Sim
Confirmar Senha do Banco de Dados	A senha especificada no campo **Senha do banco de dados**.	Sim

Tabela 30. Nomes e descrições dos parâmetros de configuração do repositório de metadados (continuação)		
Nome de parâmetro	**Descrição**	**Campo obrigatório**
Caminho do Driver JDBC	Caminho para o driver JDBC, incluindo o arquivo jar. Por exemplo, /home/jars/db.jar no Linux.	Sim

Parâmetros de Configuração Avançada

Tabela 31. Nomes e descrições dos parâmetros de configuração avançada		
Nome de parâmetro	**Descrição**	**Campo obrigatório**
Nível de rastreio de Java	Os níveis de rastreio que são usados pelos provedores Customizados Java. O valor padrão é 2.	Sim

Parâmetros de configuração do Cliente API Java

Tabela 32. Nomes e descrições dos parâmetros de configuração do Cliente API Java		
Nome de parâmetro	**Descrição**	**Campo obrigatório**
Caminho da classe para JARs externos		NÃO

Configurando o Internet Service Monitor

O Monitoramento de Serviço da Internet Agent oferece a capacidade de determinar se um serviço específico tem o desempenho adequado, identificar áreas de problemas e relatar o desempenho do serviço avaliado com relação aos acordos de Nível de Serviço. O agente de Monitoramento de Serviço da Internet funciona emulando as ações de um usuário real. Ele pesquisa e testa regularmente os serviços da Internet para verificar seu status e desempenho.

Visão Geral

Ao monitorar serviços da Internet, você define o que será monitorado, para quem e quando. É possível configurar os monitores por meio da interface com o usuário de configuração do agente de Monitoramento de Serviço da Internet.

O monitor testa os serviços da Internet específicos e encaminha os resultados dos testes para o Databridge. Os monitores emulam as ações de um usuário real do serviço.

Por exemplo, o monitor HTTP tenta acessar periodicamente uma página da web emulando as solicitações que um navegador da web geralmente envia quando um usuário vai para a página. O monitor grava o resultado do teste, que é enviado a Databridge.

Monitoramento de Serviço da

Cada monitor é criado para testar um tipo de protocolo ou serviço. Por exemplo, o monitor HTTP testa a disponibilidade de recursos como páginas da Web sobre Protocolo de Transporte de Hipertexto e o monitor FTP testa a transferência de arquivos entre hosts executando o Protocolo de Transferência de Arquivos.

Um monitor pode testar muitas instâncias diferentes do mesmo serviço, como uma série de páginas da Web servidas por uma variedade de hosts.

Monitoramento de Serviço da

Usando o intervalo de monitores do Internet Service Monitoring, é possível customizar o tipo de monitoramento de serviço da web fornecido, do monitoramento básico de serviço da Internet que testa a disponibilidade de uma página da web à combinação de sequências de testes.

O monitoramento de serviço da Internet usa uma consulta de alto volume e de baixa complexidade para testar a disponibilidade dos serviços da Web. Por exemplo, se você desejar monitorar a disponibilidade geral de um website, você pode usar o monitor HTTP para pesquisar várias URLs em intervalos regulares.

Usando uma combinação de monitores, você pode criar um nível de monitoramento de serviço adequado às suas necessidades:

- Monitores HTTP e HTTPS

  Monitore a disponibilidade de recursos com HTTP ou HTTPS executando testes básicos, de pedido único, em alto volume.

- Monitor de Transação (TRANSX)

  Combine sequências de testes realizados por um grupo de monitores simulando as ações de um usuário real. Por exemplo, discando um serviço, acessando um número de páginas em vários websites e, em seguida, acessando serviços de e-mail.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte o “Histórico de Mudanças” na página 50.

Configurando o Internet Service Monitoring por meio da interface com o usuário

Para monitorar serviços da Internet, crie perfis de usuário, elementos de perfil e planejamentos de monitoramento. Configure perfis de usuário, elementos de perfil e planejamentos de monitoramento usando a interface com o usuário do Monitoramento de Serviço da Internet.

Sobre Esta Tarefa

Um perfil do usuário é um cliente, ou um departamento, ou um grupo de serviços para o qual você monitora a Internet ou os serviços da web. Para cada perfil do usuário, o usuário precisa definir um ou mais elementos de perfil. Por exemplo, o usuário pode definir um elemento de perfil para monitorar uma página da Web entregue através de um serviço HTTP ou um elemento de perfil para monitorar a disponibilidade de um serviço FTP. Os perfis de usuário geralmente contêm vários elementos de perfil, cada elemento de perfil testa um dos serviços fornecidos a esse usuário. Cada perfil de usuário também possui um planejamento de monitoramento associado que determina em qual dia e horário os testes definidos no perfil devem ser executados.

Para acessar a janela de configuração do Monitoramento de Serviço da Internet Agent por meio do painel do IBM Application Performance Management, use o método a seguir:

Procedimento

1. No painel do Application Performance Management, clique no ícone  . Clique em **Configuração do agente**.

   A janela de configuração do agente é aberta.
2. Clique na guia **ISM** para configurar o Agente Monitoramento de Serviço da Internet.

   É possível criar, editar, excluir, atualizar, planejar e filtrar os perfis de usuário. Implemente os perfis de usuário criados no sistema gerenciado selecionado. A versão exibida é a versão do sistema gerenciado. O nome do perfil indica o perfil do usuário implementado com relação aos sistemas gerenciados selecionados. Siga estas etapas para configurar qualquer um dos perfis e implementar nos sistemas gerenciados.

3. Para incluir um perfil, clique no ícone  . Insira o **Nome do perfil** e a **Descrição** na caixa de diálogo.
4. Clique em **Avançar**.
5. Selecione um monitor na lista suspensa de monitores e clique em **Avançar**.
6. Forneça os valores dos campos e clique em **Incluir**.

   Vários monitores podem ser selecionados para um perfil. Consulte "Monitores Monitoramento de Serviço da Internet Disponíveis" na página 303 para conhecer os monitores disponíveis.
7. Clique em **Concluído**.
8. Clique no ícone  .
9. No campo **Filtrar**, procure os perfis de usuário por nome.
10. Para implementar o perfil criado em um sistema gerenciado, marque a caixa de seleção dos perfis criados, que devem ser configurados, e selecione um sistema gerenciado. Clique em **Implementar** para implementar o perfil no nome do sistema gerenciado selecionado.

Editando perfil
Todos os perfis de usuário que são criados são editáveis.

Sobre Esta Tarefa

Use o procedimento a seguir para editar os perfis.

Procedimento

1. Selecione **nome do perfil** e clique em  .
2. Selecione um serviço para editar e clique em **Editar**.

   a. Inclua um monitor usando o ícone  e exclua o monitor usando 

   b. Para renomear um perfil, dê um clique duplo no campo de texto **Nome do Perfil**, modifique o nome do perfil e clique em **Renomear Perfil**.
3. Edite os valores para o serviço selecionado.

   Nota:

   - Para ativar o campo de senha para edição, clique duas vezes no campo de texto **username**. O usuário pode editar ou incluir o nome de usuário e alterar a senha.
   - Para ativar o campo **sslkeypassword** para edição, dê um clique duplo em seu texto para alterar a chave secreta.
4. Clique em **Salvar** e no ícone  para atualizar.

Planejando um Perfil
Os perfis que são criados podem ser planejados para serem implementados em uma data e hora específicas.

Sobre Esta Tarefa

Use o procedimento a seguir para planejar perfis.

Procedimento

1. Selecione **nome do perfil**.
2. Clique no botão **Planejamento**.
3. Planeje o perfil selecionando o dia com relação ao horário. O usuário pode arrastar a grade para selecionar qualquer horário desejado.
4. Clique em **Salvar**.
5. Clique no ícone  para atualizar.

Excluindo um Perfil
Os perfis que são criados podem ser excluídos permanentemente.

Sobre Esta Tarefa

Use o procedimento a seguir para excluir o perfil.

Procedimento

1. Selecione **nome do perfil**.
2. Clique no ícone para excluir o perfil.

Grupos OID
Os grupos OID (Object Identifier) são parâmetros opcionais específicos do monitor. Eles definem conjuntos de um ou mais OIDs de objetos MIB (Management Information Base) de um dispositivo. O monitor SNMP usa os grupos OID para recuperar dados desses objetos MIB cujos OIDs aparecem em um grupo OID especificado.

Os detalhes dos objetos MIB dos quais o monitor extrai dados são os seguintes:

- Valor de OID

  O identificador numérico da instância do objeto MIB expresso utilizando a notação ASN.1, por exemplo `.1.3.6.1.2.1.1.2.0`, ou o nome de objeto, por exemplo `sysObjectID.0`

  Nota: Ao usar a notação ASN.1, você deverá incluir o caractere `.` de orientação no OID.

  Nota: Você pode usar apenas um nome de instância de objeto para especificar o valor OID se o documento MIB que define o nome estiver acessível pelo monitor. O diretório padrão para documentos MIB é `$ISHOME/mibs`.
- Nome OID

  O nome do objeto MIB, por exemplo, `sysObjectID`. Esse nome é usado nas classificações em nível de serviço e nos elementos do monitor `$oidNamen`.
- Unidade OID

  As unidades de dados contidas no objeto MIB. Por exemplo, segundos, bytes ou bits por segundo (BPS). Configure como BPS para permitir o cálculo de bits por segundo para o OID. Os valores dos bits por segundo são calculados desta forma:

  ```
  current_poll_value - prev_poll_value) / poll_interval * 8
  ```
- Seletor

  O valor do índice do objeto MIB. A tabela a seguir mostra um exemplo que faz o seletor procurar todas as linhas `ifDescr` para o valor `FastEthernet0/1`, fornecendo um índice de linha de 2. Em seguida, a linha `ifPhysAddress.2` é consultada e o valor `0:6:53:34:d2:a1` é retornado. Dessa forma, o índice 2 não é especificado diretamente, de modo que se o índice para `FastEthernet0/1` mudar, os grupos OID não precisarão ser reconfigurados.

Tabela 33. Uso do Valor de Índice

Objeto MIB	**Valor do Objeto MIB**
Valor OID	`ifPhysAddress`
Nome OID	`FastEthernet0/1PhysicalAddress`
Unidade OID	`string`
Seletor	`ifDescr=FastEthernet0/1`

Criando o grupo OID e o objeto MIB
Os grupos OID são criados globalmente e podem ser usados por todos os perfis de usuário que monitoram dispositivos ativados por SNMP

Procedimento

Conclua as etapas a seguir para criar um grupo OID e um objeto MIB.

1. Clique no botão **OIDs** para criar um grupo OID no painel do Agente Monitoramento de Serviço da Internet.
2. Clique no ícone  e insira o nome do grupo OID no campo **Nome do Grupo OID**.
3. Clique no ícone  para incluir o objeto MIB.
   a. Insira o **Valor**, **Nome**, **Unidade** e **Seletor** para o objeto MIB.
   b. Clique em **Incluir**.

   O objeto MIB é criado com sucesso.
4. Clique no ícone  para atualizar.
   O grupo OID é criado com sucesso
5. Selecione um **Nome do Grupo OID** e clique em **Visualizar** para ver a lista de todos os objetos MIB criados sob o **Grupo OID** selecionado.
6. Clique em **Fechar**.

Editando o grupo OID e o objeto MIB
É possível editar os grupos OID. Os objetos MIB também podem ser editados ao criar o grupo OID ou depois de criar o grupo OID.

Procedimento

Conclua as etapas a seguir para editar um grupo OID.

1. Clique no botão **OIDs** para editar um grupo OID no painel Agente Monitoramento de Serviço da Internet.
2. Selecione o nome do grupo OID na lista **Nome do Grupo OID** e clique no ícone  .
3. Selecione o valor de **Editar Grupo OID** e clique no ícone  .
4. Modifique os campos do objeto MIB de acordo com seu requisito e clique no botão **Salvar**.
5. Clique em **Salvar** na página pop-up **Grupos OID**.
6. Clique em **Fechar**.

Excluindo o grupo OID
Os objetos MIB estão contidos em grupos OID e são utilizados pelo monitor SNMP para obter dados. É possível excluir objetos MIB individuais de um grupo OID ou excluir todos os objetos MIB excluindo o grupo OID inteiro.

Procedimento

Conclua as etapas a seguir para excluir um grupo OID.

1. Para excluir o grupo ODI, clique no botão **OIDs** no painel Agente Monitoramento de Serviço da Internet.
2. Selecione o Nome do Grupo OID na lista **Nome do Grupo OID** e clique no ícone  .
   O grupo OID é excluído juntamente com o objeto MIB.
3. Clique em **Fechar**.

Excluindo o objeto MIB

Procedimento

Conclua as etapas a seguir para excluir o grupo MIB.

1. Para excluir o objeto MIB, clique no botão **OIDs** no painel Agente Monitoramento de Serviço da Internet.
2. Selecione o Nome do Grupo OID na lista **Nome do Grupo OID** e clique no ícone .
3. Selecione o valor do objeto MIB e clique no ícone .
   O objeto MIB é excluído.
4. Clique em **Salvar** na página pop-up **Editar Grupo OID**.
5. Clique em **Fechar**.

Monitores Monitoramento de Serviço da Internet Disponíveis

agente de Monitoramento de Serviço da Internet é um conjunto de monitores que cobre uma vasta gama de serviços de Internet.

A tabela a seguir lista os monitores disponíveis em agente de Monitoramento de Serviço da Internet e os tipos de serviços que eles monitoram.

Tabela 34. Monitores de serviços da Internet disponíveis

Nome do Monitor	**Tipo de serviço monitorado**
DHCP	DHCP (Dynamic Host Configuration Protocol). Para configurar o DHCP, consulte “Monitor DHCP” na página 316.
DNS	Serviço de Nome de Domínio. Para configurar o DNS, consulte “Monitor DNS” na página 318.
FTP	Protocolo de Transporte de Arquivo. Para configurar o FTP, consulte “Monitor FTP” na página 323.
HTTP	Protocolo de Transporte de Hipertexto. Para configurar o HTTP, consulte “Monitor HTTP” na página 328.
HTTPS	Protocolo de Transporte de Hipertexto (Seguro). Para configurar o HTTPS, consulte “Monitor HTTPS” na página 338.
ICMP	Internet Control Message Protocol. Para configurar o ICMP, consulte “Monitor ICMP” na página 343.
LDAP	Lightweight Directory Access Protocol. Para configurar o LDAP, consulte “LDAP Monitor” na página 348.
IMAP4	Internet Message Access Protocol. Para configurar o IMAP4, consulte “monitor IMAP4” na página 354.
NTP	Network Time Protocol. Para configurar o NTP, consulte “Monitor NTP” na página 359.

Tabela 34. Monitores de serviços da Internet disponíveis (continuação)	
Nome do Monitor	**Tipo de serviço monitorado**
NNTP	Network News Transport Protocol. Para configurar o NNTP, consulte "Monitor NNTP" na página 362.
POP3	Post Office Protocol. Para configurar o POP3, consulte "Monitor POP3" na página 367.
RADIUS	Remote Authentication Dial-In User Service. Para configurar o RADIUS, consulte "Monitor RADIUS" na página 372.
RPING	Remote Ping (Cisco, Juniper e RFC2925). Para configurar o RPING, consulte "Monitor RPING" na página 377.
RTSP	Protocolo de Fluxo em Tempo Real. Para configurar o RTSP, consulte "Monitor RTSP" na página 383.
SAA	Cisco Service Assurance Agent. Até configurar o SAA, consulte "monitor SAA" na página 388.
SIP	Protocolo de Inicialização de Sessão. Até configurar o SIP, consulte "Monitor SIP" na página 404
SMTP	Protocolo simples de transporte de correio. Para configurar o SMTP, consulte "Monitor SMTP" na página 409.
SNMP	Protocolo Simples de Gerenciamento de Rede. Até configurar o SNMP, consulte "Monitor SNMP" na página 414.
SOAP	Protocolo de sistema de mensagens baseado em XML. Até configurar o SOAP, consulte "Monitor SOAP" na página 418.
TCPPort	Protocolo de Controle de Transmissão. Para configurar o TCPPort, consulte "Monitor TCPPort" na página 423
TFTP	Protocolo de Transferência de Arquivo Trivial. Até configurar o TFTP, consulte "Monitor TFTP" na página 427.
TRANSX	Transações. Para configurar o TRANSX, consulte "Monitor TRANSX" na página 432.

Arquivos

Arquivo Executável

Cada monitor de serviço da Internet consiste de um arquivo executável, arquivo de propriedades, arquivo de regras e arquivo de log.

Os arquivos executáveis do monitor estão localizados no diretório `$ISHOME/platform/arch/bin`. O valor de `arch` é o código de arquitetura para o sistema operacional Windows - `win 32`.

Arquivo de propriedades

O arquivo de propriedades é um arquivo de texto e inclui configurações padrão que são precedidas por um símbolo de travessão.

Para alterar uma configuração, mude a configuração padrão e remova o símbolo de hash ou copie e cole a linha que contém as configurações padrão, faça a mudança e remova o símbolo de hash. Isso permite que você restaure os padrões posteriormente. Os arquivos de propriedades do monitor estão localizados no diretório `$ISHOME/etc/props`.

Arquivo de Regras

Arquivos de regras são semelhantes a arquivos de regras de sonda IBM Application Performance Management Netcool/OMNIbus. Para obter mais informações sobre sua sintaxe, consulte o *IBM Application Performance Management Netcool/OMNIbus Probe and Gateway Guide*.

Os arquivos de regras do monitor estão localizados no diretório `$ISHOME/etc/rules`.

Arquivo de log

Os arquivos de log armazenam mensagens sobre a operação do monitor.

Os arquivos de log do monitor estão localizados no diretório `$ISHOME/log`. A propriedade `MessageLog` determina o local e o nome do arquivo de log. A propriedade `MessageLevel` seleciona o nível de informações que são gravadas no arquivo de log, por exemplo, mensagens de depuração detalhadas ou mensagens de erro irrecuperável. A propriedade `MaxLogFileSize` determina o tamanho do arquivo de log antes da rolagem.

O nome padrão do arquivo de log é `name.log`, em que *name* é o nome do monitor.

Recursos Comuns

Existem vários recursos que são comuns para todos os monitores de serviço de Internet. Esses recursos consistem em propriedades, resultados produzidos pelos monitores e mensagens de status.

Esta seção descreve as propriedades de todos os monitores. As propriedades específicas do monitor são descritas nas seções individuais do monitor.

Na tabela a seguir, os parâmetros de propriedade padrão são sublinhados onde aplicável.

Tabela 35. Propriedades Comuns

Nome da propriedade	Parâmetro de propriedade	Descrição
`AddRoute`	`0`|`1`	Cria uma rota do endereço IP da interface de rede usada pelo monitor ao endereço IP do host monitorado. `0` - desativado `1` - ativado (o monitor usa a rota especificada no elemento de perfil e não sobre outra interface de rede). **Nota:** Essa propriedade não é suportada nas plataformas AIX e HP-UX.
`BridgeIPAddress`	não-aplicável	Especifica o endereço IP do Databridge. Essa propriedade não é configurável; o Databridge está sempre no host local.

Tabela 35. Propriedades Comuns (continuação)

Nome da propriedade	Parâmetro de propriedade	Descrição
BridgePort	integer	O número da porta usado pelo Databridge. Configure esta propriedade para o mesmo valor da propriedade SocketPort do Databridge. Padrão: 9510
BridgeSSLAuthenticatePeer	0|1	Se você desejar configurar a autenticação SSL entre o monitor e a ponte, ou entre a ponte e o agente, configure BridgeSSLAuthenticatePeer como 1 e reinicie a ponte. Essa ação autentica os certificados do servidor. Os certificados são armazenados no BridgeSSLTrustStore. 0 - desativado 1 - ativado
BridgeSSLCertificateFile	string	Especifica o caminho e o nome de arquivo do certificado digital Bridge SSL. Padrão: $ISHOME/certificates/monitorCert.pem
BridgeSSLCipherSet	string	Especifica um CipherSet. Se você atualizar esse valor, use a sintaxe Cipher definida na documentação do OpenSSL. **Nota:** Configure o mesmo valor no agente de monitoramento de serviço da Internet, todos os monitores e o Databridge. Padrão: RC4:3DES:DES:+EXP
BridgeSSLDisableSSLv2	0|1	Determina quais tipos de soquetes são aceitos. • Se configurado como 0, SSLv2 e SSLv3 são aceitos. • Se configurado como 1, os soquetes serão abertos somente no SSLv3. **Restrição:** Configure o mesmo valor no agente de monitoramento de serviço da Internet, todos os monitores e o Databridge.
BridgeSSLEncryption	0|1	Ativa a criptografica Bridge SSL. Configure esta propriedade para o mesmo valor da propriedade correspondente do Databridge. 0 - desativado 1 - ativado **Nota:** Configure o mesmo valor para todos os monitores.

Tabela 35. Propriedades Comuns (continuação)

Nome da propriedade	Parâmetro de propriedade	Descrição
`BridgeSSLKeyFile`	string	O caminho e o nome de arquivo do arquivo de chave privada Bridge SSL. Padrão: `$ISHOME/certificates/monitorKey.pem`
`BridgeSSLKeyPassword`	string	A senha usada para criptografar a chave privada Bridge SSL. Padrão: `tivoli`
`BridgeSSLTruststore`	string	O caminho e nome de arquivo do arquivo de certificação confiável para autenticação. Isso é necessário apenas ao usar a configuração `BridgeSSLAuthenticatePeer`. Se você desejar configurar a autenticação SSL entre o monitor e a ponte, ou entre a ponte e o agente, configure `BridgeSSLAuthenticatePeer` como 1 e reinicie a ponte. Essa ação autentica os certificados do servidor. É possível armazenar certificados no `SSLTrustStoreFile` e no `SSLTrustStorePath`. Padrões: • `SSLTrustStoreFile`, `$ISHOME/certificates/trust.pem` • `SSLTrustStorePath`, `$ISHOME/certificates/` Para incluir novos certificados, conclua uma das etapas a seguir: • Inclua um certificado no final da lista no arquivo de texto `SSLTrustStoreFile`. • Inclua um certificado no diretório `SSLTrustStorePath` e execute o comando OpenSSL `c_rehash` *`certificate_dir`* para executar hash nos certificados.
`BridgeTimeout`	integer	O tempo, em segundos, que o monitor aguarda por uma resposta do Databridge.
`ConfigFile`	string	Use para apontar para um arquivo de configuração de monitor. Padrão: em branco (sequência vazia).
`ConfigurationCheckInterval`	integer	O intervalo (em segundos) no qual o monitor verifica alterações no perfil. Padrão: 1

Tabela 35. Propriedades Comuns (continuação)

Nome da propriedade	Parâmetro de propriedade	Descrição
Datalog	0|1	Força o monitor a efetuar log dos dados de desempenho em um arquivo de datalog. Os dados de desempenho são registrados em: $ISHOME/datalogs/*userprofile* 0 - desativado 1 - ativado
DatalogFormat	string	Define o formato do arquivo de datalog. O parâmetro é uma lista de elementos separados por espaço, os valores dos quais devem ser armazenados no arquivo de datalog. Para cada resultado de pesquisa gravado no arquivo datalog, o tempo atual ($time) e o tempo gasto ($totalTime) são registrados, seguidos por todos os elementos definidos nesta propriedade.
DatalogNameFormat	string	Formato do nome do arquivo do datalog.
Domain	string	Especifica o nome de domínio do host executando o monitor. Se essa propriedade não estiver configurada, o monitor tentará adivinhar o nome de domínio usando as configurações NIS e DNS.
DumpProps	não-aplicável	Exibe uma lista de todas as propriedades para um monitor.
FullHostInfo	0|1	Especifica se o elemento $host deve ou não ser mapeado para um elemento de endereço IP $hostIP (se $host for um nome DNS) ou para um elemento de nome DNS (se $host for um endereço IP). 0 - desativado 1 - ativado **Nota:** Não está disponível no monitor TRANSX.
ID do Grupo	string	O ID do grupo com o qual o monitor deve executar.
Auxílio	0|1	Exibe a ajuda para as opções da linha de comandos sem executar o monitor. 0 - desativado 1 - ativado
IdentifierChecksumFields	string	Descontinuado.

Tabela 35. Propriedades Comuns (continuação)

Nome da propriedade	Parâmetro de propriedade	Descrição
IgnoreUnmatchedDVC	0|1	Se uma classificação em nível de serviço específica não for correspondida e um elemento não for criado pelo monitor, ignore esse elemento no cálculo de nível de serviço. **Dica:** Nos releases anteriores doagente de Monitoramento de Serviço da Internet, as classificações em nível de serviço foram chamadas de Discrete Value Classifications (DVCs). 0 - desativado 1 - ativado
IpAddress	string	Especifica o endereço IP da interface de rede que o monitor usa durante os testes. Se essa propriedade não estiver configurada, o monitor tentará determinar o endereço IP da máquina host usando uma consulta de nome de host. Essa tentativa pode falhar se a máquina host tiver mais de uma interface de rede.
Manager	string	Especifica o nome do aplicativo de gerenciamento, que é usado na segunda duplicação do evento ObjectServer.
MaxCCA	integer	Configura o número máximo de conexões simultâneas que o monitor pode ter ao mesmo tempo. Observe que, se você configurar esse valor muito alto, você poderá afetar severamente o desempenho do monitor. Essa propriedade não está disponível para o monitor ICMP. Padrão: 10
MaxLogFileSize	integer	O tamanho máximo (em bytes) do arquivo de log. Padrão: 1048576
MessageLevel	string	O nível mais baixo de mensagens que serão enviadas para o log de mensagem. Valores, na ordem crescente de gravidade, são: debug, info, warn, error, e fatal. Padrão: warn
MessageLog	string	Local do arquivo de log. Padrão: $ISHOME/log/*monitor*.log

Tabela 35. Propriedades Comuns (continuação)

Nome da propriedade	Parâmetro de propriedade	Descrição
`MinPoll`	integer	Define o intervalo de sondagem mínimo permitido. Se algum arquivo de configuração do monitor tiver um intervalo de pesquisa configurado para um valor menor que esse, o valor no arquivo de configuração será substituído. Padrão: `60`
`MsgDailyLog`	integer	Ativa a geração de um arquivo de log diário. Padrão: `0` -Log Diário Desativado
`MsgTimeLog`	string	Especifica o tempo (no formato 24 horas `HHMM`) depois do qual o monitor gerará um log diário, se MsgDailyLog estiver ativado. Padrão: `0000` -12 meia-noite
`Nome`	string	O nome do monitor. Configurar essa propriedade reconfigura as propriedades `PropsFile`, `RulesFile` e `MessageLog` para seus padrões.
`NewProfileCheckMultiple`	integer	Vários, que indica a frequência na qual o monitor verifica novos arquivos de configuração ao verificar alterações de perfil. Padrão: `10`
`NoRecover`	integer	Instrui o monitor a não recuperar o arquivo de armazenamento e redirecionamento. Padrão: `0` -a recuperação não é suprimida
`Pause`	integer	Configura o intervalo (em segundos) no qual um monitor distribui encadeamentos. Configurar essa propriedade para valores superior, como 100 ou mais, força o monitor a distribuir encadeamento em uma taxa mais lenta. Aumentar o valor geralmente só é necessário em sistemas lentos. Essa propriedade não é suportada no monitor ICMP. Padrão: `50`
`PreviousFields`	string	Elementos especificados por essa propriedade (usando o formato "`<element>, <element>, …`") são armazenados para uma pesquisa e prefixados com a sequência `previous`.

Tabela 35. Propriedades Comuns (continuação)		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
`Profile`	string	O nome do perfil do cliente, ou dos perfis, a ser usado. A cadeia pode ser um único nome de perfil, uma lista separada por espaço de nomes de perfis ou `*`, que força o monitor a usar todos os perfis disponíveis. Padrão: `*`
`ProfileUpdateTimeout`	integer	O número de milissegundos que um arquivo de perfil deve permanecer estático antes de ele poder ser lido por um monitor e atualizado. O intervalo permitido é de `1-20000` milissegundos. Padrão: `100`
`PropsFile`	string	O nome do arquivo de propriedades. Padrão: `$ISHOME/etc/props/`*`monitor`*`.props`
`QFile`	string	Configura o nome do arquivo de armazenamento e redirecionamento. Padrão: `$ISHOME/var/`*`monitor`*`.saf`.
`QSize`	integer	Configura o tamanho reservado (em bytes) do arquivo de armazenamento e redirecionamento. Padrão: `10240000`
`ID do usuário`	string	O ID do usuário com o qual o monitor deve executar. **Nota:** Não use essa propriedade com o monitor DHCP.
`Version`	não-aplicável	Imprime a versão do monitor sem executar o monitor.

Elementos do Monitor Comum

Esta seção descreve os elementos produzidos por todos os monitores. Elementos específicos do monitor são descritos nas seções individuais do monitor. Os elementos produzidos podem ser visualizados no painel do Monitoramento de Serviço da Internet Agent.

Se você usar o IBM Application Performance Management, os elementos que podem ser visualizados no painel do agente como atributos são determinados por um arquivo de mapeamento gerado pelo agente de monitoramento de serviço da Internet. Esse arquivo de mapeamento não é configurável.

Tabela 36 na página 312 lista os elementos produzidos por todos os monitores. Os elementos indicados por um asterisco (*) são atributos de espaço de trabalho. Os nomes dos atributos são mostrados entre colchetes. A ausência de um asterisco indica que não há atributo de espaço de trabalho equivalente. Os atributos mostrados entre colchetes, mas sem um elemento, indicam que eles estão disponíveis apenas como atributos de área de trabalho, não há elemento equivalente.

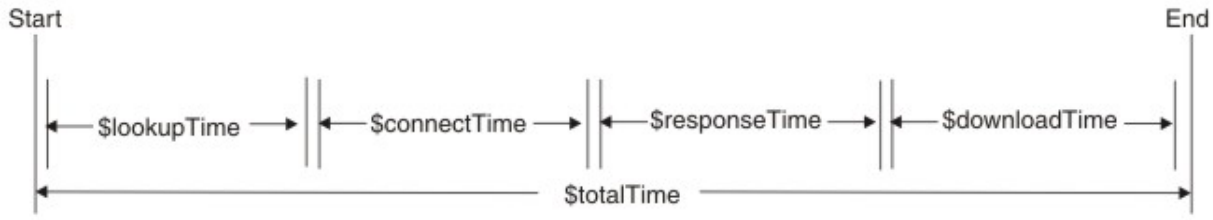
Tabela 36. Elementos do Monitor Comum	
Nome do elemento	**Descrição do elemento**
$consecutiveFailures	Se $failureRetests for diferente de zero e o teste falhar de acordo com a classificação em nível de serviço, esse elemento será criado começando com o valor de 1. O valor aumenta até que o teste não falhe mais, em cujo ponto $consecutiveFailures é configurado como 0 ou até a seguinte pesquisa. Se, nesta sondagem, o nível de serviço for transmitido ou começar a aumentar novamente, o elemento não será mais criado. Se o valor deste elemento exceder o valor de $failureRetests, o valor de $consecutiveFailures será reconfigurado como 1. **Nota:** O monitor TRANSX não gera esse elemento.
$datalogPath* (guid)	O caminho para o arquivo de diálogo usado pelo monitor. O atributo de espaço de trabalho usa os últimos 100 caracteres do caminho.
$description* (Description)	Contém a descrição de texto fornecida no campo **Descrição** do elemento de perfil do monitor.
$failureRetestInterval	O intervalo de sondagem usado durante o novo teste com falha. Isso é válido somente se $failureRetests for maior que 0. Se o intervalo de novo teste for maior que o intervalo de pesquisa normal, ele será configurado igual ao intervalo de pesquisa normal. **Nota:** O monitor TRANSX não gera esse elemento.
$failureRetests	O número de falhas no nível de serviço que precisa ser excedido antes de um evento com falha ser registrado e enviado ao ObjectServer. **Nota:** O monitor TRANSX não gera esse elemento.
$host* (Host)	O nome do host ou servidor. Armazenado no arquivo de configuração.
$hostName	Contém o nome do host do elemento $host (se $host for um endereço IP).
$hostIP	Contém o IP do host de $host (se $host for um nome DNS).
$identchecksum* (Identchecksum)	O identificador do elemento de perfil.
$lastServiceLevel* (LastServiceLevel)	O número do nível de serviço da sondagem anterior. Isso será limpo se houver alterações no perfil.
$lastServiceLevelCounter	O serviceLevelCounter na sondagem anterior. Isso será reconfigurado se houver alterações no perfil.
$monitorDNSdomain	O nome de domínio da máquina que executa o monitor, como usado pelo DNS.

Tabela 36. Elementos do Monitor Comum (continuação)	
Nome do elemento	**Descrição do elemento**
$monitorHost* (MonitorLocation)	O nome do host que está executando o monitor.
$monitorNISdomain	O nome do domínio do host que executa o monitor, como usado pelo NIS (Network Information Service).
$monitorDomain	Substitui as configurações $monitorDNSdomain e $monitorNISdomain .
$message* (ResultMessage)	Uma cadeia de texto que descreve o resultado da sondagem. Por exemplo, Falha na conexão, OK ou Êxito.
(Node)	O nome do sistema no qual o Internet Service Monitoring está em execução. Este atributo é incluído pelo agente de monitoramento de serviço da Internet.
$pollInterval	O intervalo de sondagem especificado em cada monitor.
$resultString* (ResultString)	Uma cadeia de texto que indica a classificação em nível de serviço aplicada aos resultados da sondagem. Por exemplo, TotalTime > 20.
$service* (Service)	O nome do serviço que está sendo monitorado. Por exemplo, FTP ou HTTP.
$serviceLevel* (ServiceLevel)	O número do nível de serviço da sondagem, como definido na classificação em nível de serviço: 0 -Desconhecido 1 -Bom 2 -Marginal 3 -Falhou
$serviceLevelCounter	O número de vezes que o número em nível de serviço permaneceu inalterado.
(ServiceLevelString)	A cadeia associada com o nível de serviço retornado (Unknown, Good, Marginal, ou Failed).
$startTimePoll	O horário em que a pesquisa foi iniciada.
$time	A hora do UNIX, em segundos, na qual a sondagem ocorreu.
$timeStamp* (Timestamp)	A data e hora nas quais o teste foi executado. O formato do registro de data e hora usa configurações locais.
$transxName	O nome da transação. Isso é produzido por um monitor se ele for usado em uma transação.
Detalhes do Perfil	

Tabela 36. Elementos do Monitor Comum (continuação)	
Nome do elemento	**Descrição do elemento**
`$profile*` (`IsmProfile`)	O nome do perfil do usuário.
Sincronizações - para obter informações sobre como as sincronizações são medidas, consulte "Cálculos de Tempo" na página 314.	
`$timeout`	O número de segundos em que o servidor deve responder. Obtido a partir do arquivo de configuração.
`$totalTime*` (`TotalTime`)	O tempo total obtido para executar uma operação em segundos. Inclui todas os tempos de consulta, conexão e download, quando aplicável, e o tempo de processamento do ínterim.

Cálculos de Tempo

Os monitores tentam dividir o tempo que levam para concluir uma sondagem em estágios com tempos diferentes. Por exemplo, isso pode incluir o tempo gasto para obter um endereço IP do host ou o tempo gasto para se conectar com êxito a um host.



`$totalTime` é sempre um pouco maior que a soma dos outros tempos, pois inclui o gasto adicional sobre as atividades do monitor, como o processamento de dados recebidos e o desempenho de chamadas do sistema. `$totalTime` é medido em segundos.

Mensagens de Status
Os monitores retornam as mensagens de status geradas após cada teste de serviço. As mensagens de status indicam o resultado dos testes.

As mensagens geralmente se originam do serviço monitorado ou do ambiente de rede fora do monitor. Tabela 37 na página 315 descreve as mensagens de status comuns retornadas pelos monitores no atributo `ResultMessage` durante o uso do IBM Application Performance Management. Mensagens de status específicas do monitor são descritas nas seções individuais do monitor.

Além das mensagens fornecidas pelos monitores individuais, alguns monitores, como o monitor de HTTP, relatam mensagens para o sistema operacional subjacente. Por exemplo, se a conexão TCP falhar, o agente de Monitoramento de Serviço da Internet usará a sequência definida pelo sistema operacional, como **`conexão recusada`**, **`tempo limite`**, **`rede inacessível`** e outras sequências.

Tabela 37. Mensagens de Status Comuns

Mensagem	**Descrição**
OK	O pedido do monitor foi bem-sucedido. Os monitores podem ter outras mensagens de status que indicam que um processo foi bem-sucedido. Consulte a seção *Mensagens de Status* para cada monitor.
Resposta recebida para pedidos não originários deste monitor - ignorada	Recebida uma resposta do servidor para uma mensagem que não foi originada no monitor designado.
Conexão com falha Connect to server failed	O monitor falhou ao se conectar ao servidor. Consulte o arquivo de log para obter mais informações.
Conexão encerrada inesperadamente	A conexão com o servidor foi interrompida.
Connection timed out	A conexão foi bem-sucedida, mas depois o servidor parou de responder.
Conexão fechada por host externo	O host remoto fechou a conexão antes que o monitor esperasse.
Tempo limite esgotado ao aguardar leitura/gravação	Uma conexão de dados para o servidor monitorado foi estabelecida, mas parou de responder.
Nenhuma resposta do servidor	Tempo de pedido esgotado.
Erro de formato Server Failure No such host or domain Not Implemented Pedido recusado Erro Desconhecido	Erro retornado pelo servidor monitorado.

Tabela 37. Mensagens de Status Comuns (continuação)	
Mensagem	**Descrição**

`A rede está inativa`
`Network is unreachable`
`Network dropped connection on reset`
`O software causou a interrupção da conexão`
`Reconfiguração de conexão por ponto`
`Tempo limite de conexão atingido`
`Conexão recusada`
`O host está inativo`
`No route to host`
`Conexão liberada pelo ponto remoto`
	Há um problema com a rede.

Monitor DHCP

O monitor DHCP verifica a disponibilidade e o tempo de resposta dos servidores DHCP.

Você designa classificações de nível de serviço de acordo com o tempo levado para o servidor DHCP responder a uma solicitação do monitor DHCP usando o tempo total, de consulta ou de resposta.

Tabela 38. Arquivos do Monitor DHCP	
Arquivos do Monitor	**Nome ou Local**
Monitor executável	`nco_m_dhcp`
Arquivo de Propriedades	`$ISMHOME/etc/props/dhcp.props`
Arquivo de regras	`$ISMHOME/etc/rules/dhcp.rules`
Arquivo de log	`$ISMHOME/log/dhcp.log`

Diretrizes para Configurar o Monitor DHCP

O monitor DHCP testa serviços DHCP atuando como um cliente DHCP limitado. Ele envia uma solicitação DHCP INFORM para o servidor DHCP de destino na mesma rede usando UDP como o protocolo de transporte sobre uma conexão estabelecida e espera um DHCP ACK correspondente do servidor. O monitor não solicita um endereço IP, nem afeta a validação em endereços IP existentes.

Nota: Servidores DHCP monitorados devem suportar pedidos DHCP INFORM e serem compatíveis com RFC2131.

O monitor DHCP deve ser executado como `raiz` porque liga-se a uma porta menor que 1024.

Limitação

O monitor DHCP não pode usar qualquer interface de rede configurada usando um cliente DHCP. Em vez disso, configure o monitor para usar uma interface de rede cujo endereço IP não seja designado dinamicamente.

Configurando o Teste de Serviço de Monitor DHCP

Tabela 39. Configuração do monitor DHCP	
Campo	**Descrição**
Servidor	O nome do host do servidor DHCP. O exemplo é dhcp1.mycompany.com
localip	A interface de rede do endereço IP que o monitor usa para executar o teste. O exemplo é 192.168.n.n
description	Um campo de texto para fornecer informações descritivas sobre o elemento. O exemplo é o monitor DHCP
port	O número da porta do servidor DHCP e o valor padrão é 67.
localport	O número da porta que o monitor usa para executar o teste e o valor padrão é 68.
timeout	O tempo, em segundos, a aguardar até que o servidor responda e o valor padrão é 30.
tentar novamente	O número de vezes que o monitor deve tentar novamente a conexão com o servidor DHCP antes de encerrar. O valor padrão é 0. O exemplo é 2.
Pesquisar	O tempo, em segundos, entre cada pesquisa do servidor usando o atual elemento de perfil. O valor padrão é 300.
failureretests	O número de vezes para novo teste antes de indicar uma falha e o valor padrão é 0.
Intervalo de retestagem	O tempo, em segundos, a aguardar entre cada teste novo na falha e o valor padrão é 30.

Além dos resultados de teste comuns a todos os elementos, o monitor DHCP gera um conjunto de resultados de teste contendo dados específicos para os testes de serviço DHCP.

Tabela 40. Elementos do monitor DHCP	
Elemento	**Descrição**
`$clientIP* ClientIp`	O endereço IP do host no qual o monitor está em execução.
`$lookupTime*(LookupTime)`	O tempo utilizado para obter o endereço IP do servidor host.
`$responseTime* ResponseTime`	O tempo entre quando a conexão é estabelecida e o primeiro byte de dados é recebido.
`$retries`	O número máximo de novas entradas, como especificado durante a configuração do elemento.
`$router`	O endereço IP do roteador, como retornado pelo servidor DHCP.

Mensagens de Status

O monitor DHCP fornece mensagens de status no atributo `ResultMessage` ao usar o IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

Tabela 41. Mensagens de Status do Monitor DHCP

Mensagem	**Descrição**
`DHCPACK recebido DHCPNAK recebido`	Um servidor DHCP responde à solicitação de informação do DHCP enviada pelo monitor.
`Este monitor requer privilégios de administrador para executar`	Efetue login como root.
`MENSAGEM DHCP válida não recebida`	Resposta não reconhecida a partir do servidor DHCP.
`TIPO DE MENSAGEM DHCP válido não recebido`	Resposta não-reconhecida do servidor DHCP (`DHCPACK` ou `DHCPNAK` esperado).
`ID de transação inválido` `Resposta recebida para pedidos não originários deste monitor - ignorada`	Recebida uma resposta de um servidor DHCP para uma mensagem que não foi originada nesse monitor.
`Código de operação não esperado retornado`	Uma mensagem inesperada foi recebida nesta porta.
`Conexão com falha`	O nome do servidor especificado é inválido.
`Falha ao enviar pedido para o servidor DHCP`	O sistema operacional não pode identificar especificamente porque a solicitação não pode ser enviada para o servidor, portanto, retorna essa mensagem de status que indica um problema com a rede.
`Nenhuma resposta do servidor`	O servidor DHCP não está respondendo.

Monitor DNS

O monitor DNS usa o serviço DNS (Domain Name System) para localizar informações sobre um ou mais hosts.

O monitor DNS usa o endereço IP do host para procurar o nome do host ou o nome do host para procurar o endereço IP. O monitor mede o desempenho do serviço gravando o resultado da procura e os tempos de resposta. O monitor também grava detalhes de cada consulta enviada para o servidor.

Tabela 42. Resumo do arquivo do monitor DNS

Arquivos do Monitor	**Nome ou Local**
Monitor executável	`nco_m_dns`
Arquivo de Propriedades	`$ISMHOME/etc/props/dns.props`
Arquivo de regras	`$ISMHOME/etc/rules/dns.rules`
Arquivo de log	`$ISMHOME/log/dns.log`

Diretrizes para Configurar o Monitor DNS

O monitor DNS pode ser configurado para consultar o endereço IP ou nome de host do host de destino. Dependendo do tipo de consulta, o monitor se comunica com o servidor DNS de uma maneira diferente.

Consulta de endereço IP

Ao executar um teste de consulta de endereço IP, é fornecido ao monitor um nome de host, que ele usa para localizar um endereço IP.

O monitor testa o DNS como a seguir:

1. O monitor consulta o servidor DNS usando o nome completo do HostA (`hosta.dev.net`) para solicitar seu endereço IP.

   Se o servidor DNS puder localizar o endereço IP do host, ele o retornará ao monitor. Se o servidor DNS não conseguir localizar o endereço IP do host, ele retornará uma mensagem contendo detalhes da pesquisa com falha para o monitor.

   Se o pedido atingir o tempo limite, o monitor tentará novamente (se novas tentativas estiverem configuradas). Se não forem feitas novas tentativas, o monitor criará um evento com falha.

   Se o nome do host especificado na configuração for um nome de domínio, como `mycompany.com`, e não um nome de host completo, como `hostx.mycompany.com`, o monitor recuperará as informações sobre todo o domínio. Essas informações serão armazenadas em dois elementos extras: `$domainNameServer` e `$domainNameAddr`.
2. Se a mensagem retornada para o monitor contiver um nome canônico, o monitor concluirá que o nome fornecido no arquivo de configuração deverá ter sido um alias. O monitor envia o nome canônico para o servidor DNS para solicitar o endereço IP do host.

   Se o servidor DNS localizar o endereço IP do host usando seu nome canônico, ele o retornará ao monitor. Se o servidor DNS não conseguir localizar o endereço IP do host, ele retornará uma mensagem contendo detalhes da pesquisa com falha para o monitor.
3. Se as duas primeiras tentativas de consultar o servidor DNS falharem, o monitor enviará o endereço IP do Servidor DNS (`192.168.n.n`) para o servidor DNS e solicitará seu nome completo do host.

   Se o servidor DNS puder localizar seu próprio nome completo de host, ele o retornará ao monitor. Se o servidor DNS não puder localizar seu próprio nome completo do host, ele retornará uma mensagem contendo detalhes da procura com falha. A solicitação para o nome completo do host do servidor (uma solicitação de consulta de DNS reverso) não é suportada em todos os tipos de servidores DNS. Se o servidor DNS de destino não suportar consultas reversas, será possível evitar que o monitor DNS envie essa solicitação configurando a propriedade `LookupServerName` como `0`.

Consulta Recursiva

Consultas não-recursivas apresentam uma imagem mais precisa de como o servidor DNS está executando, considerando que elas dão uma melhor indicação do desempenho DNS que aplicativos da Internet (e, portanto, usuários) estão tendo. O monitor DNS suporta tanto consultas recursivas quanto consultas não-recursivas.

Geralmente é como aplicativos da Internet que fazem consultas DNS trabalham. Por exemplo, um navegador da web sempre especifica consultas recursivas quando ele está tentando resolver a parte do host de uma URL.

Se um servidor DNS não puder responder a uma consulta porque ele não contém uma entrada para o host em seu banco de dados, ele poderá consultar recursivamente os servidores DNS mais para cima na hierarquia.

Tipos de Consultas DNS

O monitor DNS suporta um intervalo de tipos de consultas DNS. Use o código de consulta ao especificar o tipo de consulta DNS.

Tabela 43. Tipos de Consultas DNS

Código de Consulta	**Tipo de Consulta**
A	Endereço do Host

Tabela 43. Tipos de Consultas DNS (continuação)	
Código de Consulta	**Tipo de Consulta**
NS	Servidor de nomes Autoritativo
MD	Destino do Correio
MF	Encaminhador de
CNAME	Nome canônico para um alias
SOA	Início de uma zona de autoridade
MB	Nome do domínio da caixa de Correio
MG	Membro do grupo de correio
MR	Nome de domínio da renomeação de e-mail.
NULL	RR Nulo
WKS	Descrição do Serviço Bem Conhecidos
PTR	Ponteiro do nome de domínio
HINFO	Informações do host
MINFO	Informações da Caixa de Correio ou da Lista de Corre
MX	Troca de Corre
TXT	Sequências de texto
AXFR	Transferência de uma zona inteira
MAILB	Registros relacionados à caixa de correio
MAILA	RR do agente de correio
ANY	Todos os registros

Configurando testes do Serviço do Monitor DNS

Use os parâmetros de configuração do monitor DNS para definir testes de serviços DNS.

Tabela 44. Tabela 3. Configuração do Monitor DNS	
Campo	**Descrição**
servidor	O endereço IP do servidor DNS primário. O exemplo é 192.168.n.n
host	O nome do host do host de destino. O exemplo é www.myconpany.com
description	Um campo de texto para fornecer informações descritivas sobre o elemento. O exemplo é monitor DNS.
recursivelookups	Ativa ou desativa consultas recursivas. • `recurse` (use `true` em ismbatch). • `norecurse` (use `false` em ismbatch). Padrão: `recurse` .
port	Porta no servidor DNS na qual o monitor atende e o valor padrão é 53.

Tabela 44. Tabela 3. Configuração do Monitor DNS (continuação)	
Campo	**Descrição**
IP local	Especifica o endereço IP da interface de rede na máquina host utilizada ao qual o monitor será ligado ao executar o teste. Se a propriedade `IpAddress` do monitor estiver configurada, ela substituirá o valor desse campo.
Tipo de consulta	O tipo de consulta DNS usada no teste. Para obter uma lista de tipos de consulta suportados, consulte Tabela 43 na página 319.
timeout	O tempo, em segundos, para aguardar para que o servidor responda. Padrão: `10`.
tentar novamente	O número de vezes em que o monitor deve tentar novamente para entrar em contato com o servidor DNS antes de sair.
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: `300` .
failureretests	O número de vezes para testar novamente antes de indicar uma falha. Padrão: `0` .
retestinterval	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: `10`.

Monitorando elementos

Além dos resultados de teste comuns a todos os elementos, o monitor DNS gera um conjunto de resultados de teste que contém dados específicos sobre o teste de serviço DNS.

Tabela 45. Tabela 4.Elementos do Monitor DNS	
Elemento	**Descrição**
`$authoritative`	Este elemento só é criado se as informações recuperadas vierem de um servidor DNS com autoridade. Se o servidor DNS não tiver sido autorizado, esse elemento não será criado.
`$domainEmailAddr`	O endereço de contato do domínio de destino.
`$domainNameServer`	O nome do servidor DNS para o domínio de destino.
`$fromAliasTime`	O tempo entre a emissão de um pedido para um nome canônico, recebido de uma consulta anterior, e o recebimento de um endereço IP.
`$localIP`	O endereço IP local com o qual o monitor está configurado para utilizar. Isto pode ser em branco em uma máquina com apenas uma interface.
`$lookup*` (`HostLookup`)	O nome do host ou endereço IP do host de destino que o monitor está tentando localizar.
`$lookupCName`	O nome do host oficial do host de destino. Esse elemento é criado apenas se o nome do host oficial for diferente do nome do host no `$lookupName`.
`$lookupIP*` (`HostIp`)	O endereço IP do host de destino.

Tabela 45. Tabela 4.Elementos do Monitor DNS (continuação)	
Elemento	**Descrição**
$lookupName* (Host)	O nome do host integral do host de destino.
$mxRecords	O número de registros MX localizados.
$port	A porta na qual o serviço é monitorado.
$queryType	O tipo de consulta DNS usada no teste. Para obter uma lista de tipos de consulta suportados. Consulte Tabela 43 na página 319.
$responseTime*(ResponseTime)	O tempo entre o monitor que emite um pedido para o servidor DNS e o recebimento de uma resposta dele.
$retries	O número máximo de novas entradas, como especificado no elemento de perfil.
$serverIP	O endereço IP do servidor DNS.
$serverName	O nome do host do servidor DNS.
$serverTime	Hora na qual o servidor resolverá seu próprio nome.

Manipulação de registro MX

Dois elementos são criados para cada registro MX localizado pelo monitor DNS: $mxHostn e $mxPreferencen.

$mxHostn armazena o nome do host de um registro MX. $mxPreferencen contém a ponderação de preferência do host. n faz a incrementação de cada par de registro para diferenciá-los. O monitor armazena o número total de registros MX para um determinado host no elemento $mxRecords. Os pares de registro são armazenados na ordem decrescente de preferência do MX.

Mensagem de status

O monitor DNS fornece mensagens de status no atributo ResultMessage ao usar o IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

Tabela 46. Tabela 5.Mensagens de Status do Monitor DNS	
Mensagem	**Descrição**
Domain information received	A solicitação para um nome de domínio foi bem-sucedida.
Com Êxito	A solicitação foi bem-sucedida.
Resposta Inválida	Resposta não reconhecida a partir do servidor DNS.
Conexão com falha	O nome do servidor especificado é inválido.
Nenhuma resposta do servidor	Tempo de pedido esgotado.
Falha ao enviar pedido de DNS	Há um problema com a rede.
No such domain (no recursion)	O nome de domínio está incorreto.

Propriedades

As propriedades específicas para o monitor DNS são descritas na tabela a seguir.

Tabela 47. Propriedades do Monitor DNS		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
`AcceptCNAME`	`0`|`1`	Se ativado, o monitor DNS aceita o nome canônico na resposta DNS e não executa nenhuma consulta adicional.
`DNSQueryType`	string	O tipo de consulta DNS utilizado em testes. Consulte Tabela 43 na página 319 para obter uma lista de tipos de consulta suportados. Padrão: `ANY`.
`LookupServerName`	`0`|`1`	Ativa a consulta DNS reversa no endereço IP do servidor DNS. `0` - desativado `1` - ativado

Monitor FTP

O monitor FTP testa os serviços FTP fazendo upload ou download dos arquivos para ou dos servidores FTP. Ele monitora o desempenho do serviço gravando o tempo de resposta e a taxa de transferência de dados e monitora o espaço em disco e a integridade do arquivo.

Tabela 48. Resumo do Monitor FTP	
Arquivos do Monitor	**Nome ou local**
Monitor executável	`nco_m_ftp`
Arquivo de Propriedades	`$ISHOME/etc/props/ftp.props`
Arquivo de regras	`$ISHOME/etc/rules/ftp.rules`
Arquivo de log	`$ISHOME/log/ftp.log`

Diretrizes para Configurar o Monitor de FTP

O monitor FTP testa a disponibilidade de um servidor FTP fazendo upload de um arquivo para o servidor usando um comando FTP STOR ou fazendo download de um arquivo do servidor usando um comando FTP RETR.

Configurando testes do Serviço de Monitoramento FTP

Os parâmetros de configuração do monitor FTP são descritos na tabela a seguir.

Tabela 49. Configuração do Monitor de FTP	
Campo	**Descrição**
Servidor	O endereço IP do servidor FTP de destino ou a máquina da qual deseja enviar por FTP. O exemplo é `ftp.mycompany.com`

Tabela 49. Configuração do Monitor de FTP (continuação)	
Campo	**Descrição**
localfile	Para operações GET do FTP, esse campo especifica o nome e o caminho para o qual o arquivo é transferido por download. Para operações PUT do FTP, esse campo especifica o nome e o caminho do arquivo transferido por upload para o servidor FTP. O valor padrão é FULL PATHNAME. O exemplo é `$ISMHOME/etc/ism/downloads/ftp-test.tar.Z`
remotefile	Para operações GET do FTP, esse campo especifica o nome e o caminho do arquivo transferido por download do servidor. Para operações PUT do FTP, esse campo especifica o nome e o caminho para o qual o arquivo é transferido por upload no servidor FTP. O valor padrão é FULL PATHNAME. O exemplo é `/sales/prodlist.tar.Z`
description	Um campo de texto para fornecer informações descritivas sobre o elemento.
port	A porta padrão que o servidor FTP usa. Padrão: `21`
nome do usuário	O nome de usuário utilizado para efetuar logon no servidor FTP de destino.
senha	A senha utilizada para efetuar logon no servidor FTP de destino. Deixe-a em branco se a conta do FTP não exigir uma senha.
comando	O comando FTP a ser utilizado pelo monitor: • GET ou RECV - Faz download de um arquivo do servidor FTP de destino • SEND ou PUT - Faz upload de um arquivo para o servidor FTP de destino Padrão: GET.
Tipo de conexão	Especifica o tipo de conexão que o monitor deve estabelecer com o servidor ao tentar transferir o arquivo: • `Ativo` • `Passive` Padrão: `Active`.
timeout	O tempo, em segundos, para aguardar para que o servidor responda. Padrão: `30`.
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: `300`

Tabela 49. Configuração do Monitor de FTP (continuação)	
Campo	**Descrição**
failureretests	O número de vezes para testar novamente antes de indicar uma falha. Padrão: `0`.
retestinterval	O período de tempo em segundos a aguardar entre cada novo teste de falha. Padrão: `10`.

Correspondência de Expressões Comuns

Você pode desempenhar uma procura de expressão comum nas informações transferidas por download digitando até 50 expressões comuns diferentes. O monitor FTP tenta corresponder o conteúdo recuperado a cada uma das expressões comuns.

Se uma correspondência para uma expressão comum especificada for encontrada, as linhas correspondentes (ou o máximo que couber no buffer interno do monitor) serão retornadas no elemento `$regexpMatchn` correspondente. Se a expressão comum corresponder mais de uma vez nas informações transferidas por download, apenas a primeira será retornada. O status de cada teste de expressão regular é indicado pelos elementos `$regexpStatusn`. Você pode utilizar as correspondências de expressões comuns e suas informações de status como critérios para as classificações em nível de serviço.

Expressões comuns executam correspondência de cadeia no conteúdo transferido por download durante testes de serviços. Essas expressões podem conter um ou mais operadores de expressões comuns, que determinam qual conteúdo será correspondido pela expressão.

Nota: A sintaxe de expressão regular pode ser usada para corresponder sequências somente em linhas únicas. O Internet Service Monitoring não pode corresponder às sequências que incluem novas linhas ou retornos de linha. Use várias expressões regulares para corresponder às sequências que cobrem várias linhas. Também é possível usar as regras do SLC para aumentar os alarmes com base no resultado de diversas expressões regulares.

Tabela 50. Operadores de Expressão Comum	
Caractere	**Descrição**
.	Corresponde a qualquer caractere único. Por exemplo, a expressão comum `r.t` corresponde às sequências `rat`, `rut`, `r t`, mas não à `root`.
$	Corresponde ao final de uma linha. Por exemplo, a expressão comum `dog$` corresponde ao fim da cadeia `it's a dog` mas não à cadeia `There are a lot of dogs`.
^	Corresponde ao início de uma linha. Por exemplo, a expressão comum `^When in` corresponde ao início da sequência `When in the course of human events`, mas não corresponderia à sequência `What and When in the`.
*	Corresponde a zero ou mais ocorrências do caractere que o precede imediatamente. Por exemplo, a expressão comum `.*` corresponde a qualquer número de qualquer caractere.

Tabela 50. Operadores de Expressão Comum (continuação)	
Caractere	**Descrição**
\	Trata o caractere subseqüente como um caractere comum. Por exemplo, \$ corresponde ao caractere de sinal de dólar ($), não ao final de uma linha. Da mesma forma, a expressão \. corresponde ao caractere de ponto em vez de qualquer caractere único.
[]	Corresponde a algum dos caracteres entre colchetes. Por exemplo, a expressão comum r[aou]t corresponde a rat, rot, e rut, mas não a rit. Especifique os intervalos de caracteres usando um hífen. Por exemplo, a expressão comum [0-9] corresponde a algum dígito. Também é possível especificar vários intervalos. Por exemplo, a expressão regular [A-Za-z] corresponde a quaisquer letras maiúsculas e minúsculas.
|	Corresponde frases contendo uma das condições especificadas. Por exemplo, him|her corresponde à linha it belongs to him e à linha it belongs to her, mas não corresponde à linha it belongs to them.

Nota: Se você preferir as sequências de dados de saída com curly braces{} ou double quotes "", então será necessário incluir um caractere de escape backslash \ antes de cada curly brace e double quote na expressão regular.

Por exemplo, se a sequência de dados for {"templates":true,"mongodb":true,"ldap":true,"ucd":true,"github":true}, a expressão regular aparecerá como \{\"templates\":true,\"mongodb\":true,\"ldap\":true,\"ucd\":true,\"github\":true\}

Elementos do Monitor

Além dos resultados de teste comuns a todos os elementos, o monitor FTP gera um conjunto de resultados de teste contendo dados específicos para testes de serviço do FTP.

Tabela 51. Elementos do Monitor FTP	
Elemento	**Descrição**
$bytesPerSec*(BytesPerSec)	O número médio de bytes transferidos por segundo.
$bytesTransfered* (BytesTransferred)	O número de bytes transferidos por upload ou download.
$checksum	O elemento Checksum normalmente não fornece valores significativos para classificações em nível de serviço porque os valores de soma de verificação não são conhecidos quando o elemento de perfil é criado (o monitor calcula valores de soma de verificação enquanto os testes estão em andamento). Os elementos de monitor $checksum e $previousChecksum destinam-se ao enriquecimento do alerta usando o arquivo de regras do monitor.
$command* (FtpCommand)	O comando FTP emitido pelo monitor.

Tabela 51. Elementos do Monitor FTP (continuação)	
Elemento	**Descrição**
$connectionType* (FtpConnection)	O tipo de conexão de dados utilizada. Isso pode ser ACTIVE ou PASSIVE.
$connectTime*(ConnectTime)	O tempo utilizado para conectar-se ao servidor FTP.
$downloadTime	O tempo utilizado para fazer download do arquivo.
$localFile* (FtpLocalFile)	O nome do caminho completo do arquivo armazenado no host local. Esse elemento é obtido do arquivo de configuração.
$lookupTime*(LookupTime)	O tempo utilizado para consultar o endereço IP do servidor FTP.
$previousChecksum	O elemento PreviousChecksum normalmente não fornece valores significativos para classificações em nível de serviço porque os valores de soma de verificação não são conhecidos quando o elemento de perfil é criado (o monitor calcula os valores de soma de verificação enquanto os testes estão em andamento). Os elementos do monitor $previousChecksum e $checksum são destinados ao enriquecimento do alerta usando o arquivo de regras do monitor.
$regexp*n*	A expressão regular.
$regexpMatch*n*	O conteúdo da linha que corresponde à expressão comum.
$regexpStatus*n*	O status da correspondência da expressão comum: NONE - Não há nenhuma verificação de expressão comum configurada MATCHED - Foi localizada uma correspondência para a expressão comum FAILED - Uma correspondência não foi localizada para a expressão comum
$remoteFile* (FtpRemoteFile)	Nome do caminho completo do arquivo armazenado no host remoto (o servidor FTP). Esse elemento é retirado do arquivo de configuração.
$responseTime*(ResponseTime)	O tempo utilizado, após a criação de uma conexão, até o recebimento do primeiro byte do arquivo de destino.
$status	O código de status retornado pelo servidor FTP.
$transferTime*(TransferTime)	Configura o valor como $uploadTime ou $downloadTime.
$uploadTime	O tempo utilizado para fazer upload do arquivo.
$username	Nome do usuário (nome da conta) usado pelo monitor para efetuar login no host de destino. Esse elemento será retirado do arquivo de configuração se $message contiver OK.

Mensagens de Status

O monitor FTP fornece mensagens de status no atributo ResultMessage ao usar o IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

Tabela 52. Mensagens de Status do Monitor FTP	
Mensagem	**Descrição**
OK	A solicitação de FTP foi bem-sucedida.

Tabela 52. Mensagens de Status do Monitor FTP (continuação)	
Mensagem	**Descrição**
`Não é possível abrir o arquivo local para leitura/gravação`	Consulte o arquivo de log do monitor FTP para obter informações adicionais.
`Não é possível ler/gravar no arquivo local`	
`Unable to read from data connection`	Foi estabelecida uma conexão de dados com o servidor FTP, mas ocorreu um problema.
`Unable to upload to ftp server`	
`Tempo limite esgotado ao aguardar leitura/gravação`	
`Conexão fechada por host externo`	A conexão com o servidor FTP foi interrompida.
`Conexão encerrada inesperadamente`	
`Conexão com falha`	Houve falha de conexão do monitor com o servidor FTP. Consulte o arquivo de log do monitor FTP para obter informações adicionais.

Monitor HTTP

O monitor HTTP verifica a disponibilidade e o tempo de resposta de servidores da Web.

Ele pode monitorar páginas da web individuais, incluindo o uso de CGI, que normalmente exigiria que o usuário insira dados nos campos. Ele também pode monitorar o tempo de download dos elementos, como imagens em uma página da Web.

Tabela 53. Resumo do Arquivo do Monitor HTTP	
Arquivos do Monitor	**Nome ou local**
Monitor executável	`nco_m_http`
Arquivo de Propriedades	`$ISHOME/etc/props/http.props`
Arquivo de regras	`$ISHOME/etc/rules/http.rules`
Arquivo de log	`$ISHOME/log/http.log`

Diretrizes para configurar o monitor HTTP

Os monitores HTTP e HTTPS verificam a disponibilidade e o tempo de resposta dos servidores da Web. Use o monitor HTTP nas seguintes situações:

- O Web site de destino é estático.

  Para Web sites dinâmicos, utilize o monitor TRANSX.
- O Web site de destino é servido sobre o protocolo HTTP.

  Para websites que entregam conteúdo por meio do protocolo HTTPS, selecione o monitor HTTPS.
- Para executar o monitoramento em várias plataformas.
- Onde a velocidade é um fator determinante (o monitor HTTP fornece alto desempenho).

Tipos de solicitação de HTTP

O monitor HTTP emula um navegador da Web que suporta o protocolo HTTP/1.0. Para testar o servidor da Web, o monitor envia a ele uma solicitação para uma página da web utilizando qualquer um dos seguintes tipos de solicitação de HTTP:

- HEAD

O comando HEAD tenta acessar uma página da Web e retorna o cabeçalho HTTP. A emissão do comando HEAD é a forma mais rápida de verificar se uma página da Web pode ser acessada.

- GET

  O comando GET tenta acessar a página da Web e retorna a página toda, incluindo o cabeçalho HTTP. Ele não tenta retornar arquivos associados à página, como imagens.

- GETALL

  O comando GETALL tenta acessar a página da Web e retorna a página inteira, incluindo o cabeçalho HTTP, plano de fundo, imagens, applets, quadros, arquivos de folhas de estilo em cascata (CSS) e scripts. Tal como os comandos HEAD e GET, esse comando também verifica se a página da Web está acessível, mas como o comando GETALL retorna a página inteira e todos os arquivos associados, isso pode dar uma indicação mais realística do tempo gasto para acessar a página. O monitor também utiliza diversos encadeamentos durante um comando GETALL para correspondência mais precisa do comportamento dos navegadores da Web.

- POST

  O comando POST tenta acessar uma página da Web que contém um formulário HTTP e preenche os campos desse formulário. Inclua o texto do corpo para a solicitação POST na guia **Corpo** na configuração do agente de Monitoramento de Serviço da Internet ou use o grupo @Body na configuração do agente de Monitoramento de Serviço da Internet ou ismbatch. Como alternativa, é possível usar os parâmetros FORM. Não é possível usar os parâmetros Body Text e FORM na solicitação POST.

Utilizando um Servidor Proxy

Você pode testar a disponibilidade de páginas da Web através de um servidor proxy. Quando você configura o monitor para usar um proxy, ele envia solicitações de HTTP por meio do proxy. Se necessário, você pode ignorar o cache proxy. Você configura os parâmetros para o servidor proxy na guia **Detalhes do Proxy**. O monitor HTTP suporta acesso autenticado a servidores proxy. Essa autenticação é independente de qualquer autenticação requerida pela página da web de destino.

Elementos do Servidor Proxy

Em versões anteriores, quando você configurou um elemento de perfil para usar um servidor proxy, por padrão, o monitor HTTP inseriu o nome e a porta do servidor proxy nos elementos $server e $port, em vez do nome e da porta do servidor de destino desejado. Para preservar o valor do nome e da porta do servidor de destino desejado em versões anteriores, configure a propriedade generateProxyTokens para 1 ou inicie o monitor com o parâmetro de linha de comandos -generateproxytokens

Além de preservar os valores dos elementos $server e $port quando essa propriedade ou parâmetro da linha de comandos for configurado, o monitor gera os elementos $proxyServer, $proxyPort, $proxyAuthType, $proxyUsername e $proxyCache.

Autenticação

Se a página da web que você deseja monitorar, ou o servidor proxy que você deseja testar, requerer autenticação, especifique as credenciais para acessar a página nos campos de parâmetro authenticationtype, username e password na guia Avançado ou Detalhes do Proxy.

Para desativar autenticação, configure authenticationtype como NENHUMA.

Para selecionar autenticação básica:

1. Configure authenticationtype como BASIC.
2. Configure username e password para os campos necessários à página da Web ou ao servidor proxy.

Para selecionar NTLM:

1. Configure authenticationtype como NTLMv1 ou NTLMv2.

2. Configure `username` e `password` para os campos necessários à página da Web ou ao servidor proxy.

Nota:

O monitor limita o comprimento dos pedidos HTTP para 4096 caracteres. Se o comprimento dos dados do formulário adicional resultar em um comprimento de solicitação que excede esse limite, o monitor não incluirá os dados de formulário adicionais na solicitação.

Configurando o Teste de Serviço do Monitor HTTP

Utilize os parâmetros de configuração do monitor HTTP para definir testes de serviço do HTTP.

Tabela 54. Configuração do Monitor HTTP

Campo	**Descrição**
servidor	O nome do host do servidor a ser monitorado. Por exemplo, `www.mycompany.com`
página	A URL da página a ser monitorada. O exemplo é `index.html`
description	Um campo de texto para fornecer informações descritivas sobre o elemento. O exemplo é `monitoramento por meio de um servidor proxy`
port	A porta a ser utilizada no servidor HTTP. Padrão: `80`
IP local	Especifica o endereço IP da interface de rede utilizada pelo monitor para o teste. Se esse campo estiver vazio, o monitor utilizará a interface especificada pela propriedade `IpAddress`.
versão	A versão do protocolo HTTP a ser utilizada: • `1.0` • `1.1` Padrão: `1.0`
comando	O tipo de pedido de HTTP: • `HEAD` • `GET` • `GETALL` • `POST` Padrão: `GET`
formname	Quando usado em uma transação, o monitor HTTP varre o formulário especificado para obter valores padrão. Quaisquer valores localizados serão concluídos automaticamente na próxima etapa HTTP na transação.
Tipo de autenticação	Especifica o mecanismo de autenticação de solicitação/resposta para autenticação de usuários da rede: • `NONE` -Sem autenticação • `BASIC` • `NTLMv1` - Autenticação de desafio/resposta do Windows NTLM versão 1 • `NTLMv2` - Windows NTLM versão 2 Padrão: `NONE`

Tabela 54. Configuração do Monitor HTTP (continuação)	
Campo	**Descrição**
nome do usuário	O nome de usuário (nome da conta) para o monitor a ser usado para efetuar login no servidor.
senha	A senha correspondente ao nome do usuário que o monitor usará para efetuar login no servidor.
timeout	O tempo, em segundos, para aguardar para que o servidor responda. Padrão: `30`
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: `300` .
failureretests	O número de vezes para testar novamente antes de indicar uma falha. Padrão: `0`
Intervalo de retestagem	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: `10`
verifycertificate	É por padrão desativado.
Detalhes do Proxy	
servidor	O nome do host do servidor proxy.
port	A porta a ser utilizada no servidor proxy. Padrão: `8080`
Tipo de autenticação	O tipo de autenticação do servidor para o servidor proxy. Para obter mais informações, consulte o `authenticationtype` anterior. Padrão: `NONE`
nome do usuário	Usado pelo monitor junto com a senha para login no servidor proxy.
senha	Usado pelo monitor junto com o nome do usuário para efetuar login no servidor proxy e o rótulo é password.
useproxy	Configura o monitor para executar o pedido utilizando um servidor proxy. • `proxy` (use `true` em ismbatch) • `noproxy` (use `false` em ismbatch) Padrão: `noproxy`

Tabela 54. Configuração do Monitor HTTP (continuação)	
Campo	**Descrição**
hostnamelookuppreference	Determina qual versão de IP, IPv6 ou IPv4, é aplicado no nome do host fornecido. As opções são: • `default` configura o monitor para utilizar configurações de propriedades em todo o monitor. Este é o padrão. • `4Then6` seleciona IPv4 e, em seguida, IPv6. Utiliza endereços IPv4, se eles estiverem disponíveis. Se não forem localizados endereços IPv4, endereços IPv6 serão utilizados. • 6Then4 seleciona IPv6 e, em seguida, IPv4. Utiliza endereços IPv6, se eles estiverem disponíveis. Se não forem localizados endereços IPv6, endereços IPv4 serão utilizados. • `40nly` seleciona apenas IPv4. Usa endereços IPv4 apenas. Se não houver endereços IPv4, a pesquisa retorna um erro. • `60nly` seleciona apenas IPv6. Usa apenas endereços IPv6. Se não houver endereços IPv6, a pesquisa retorna um erro. • `60r4` seleciona IPv4 ou IPv6. Usa o primeiro endereço retornado a partir do nome do host.
nocache	Por padrão, ele é configurado para cache.

Expressão Regular

Você pode desempenhar uma procura de expressão comum nas informações transferidas por download digitando até 50 expressões comuns diferentes. O monitor HTTP tenta corresponder o conteúdo recuperado a cada uma das expressões comuns. Se uma correspondência para uma expressão comum especificada for encontrada, as linhas correspondentes (ou o máximo que couber no buffer interno do monitor) serão retornadas no elemento `$regexpMatchn` correspondente. Se a expressão comum corresponder mais de uma vez nas informações transferidas por download, apenas a primeira será retornada. O status de cada teste de expressão regular é indicado pelos elementos `$regexpStatusn`. Você pode utilizar as correspondências de expressão comum e suas informações de status como critérios para classificações em nível de serviço. Consulte Tabela 50 na página 325 para obter informações sobre a sintaxe de expressão regular,

Parâmetro de cabeçote e de formulário

O monitor HTTP pode enviar dados extras nos campos de cabeçalho e corpo da mensagem de pedidos de HTTP.

Os parâmetros para esses dados extras são configurados na guia Parâmetros. Os parâmetros são Nome, Valor e Tipo e operam da seguinte maneira:

- Os pares nome-valor do tipo HEAD especificam campos de cabeçalho adicionais, como `User-Agent` e `Referer`, incluídos em todas as solicitações de HTTP enviadas pelo monitor. Campos de cabeçalho podem ser especificados para qualquer tipo de método de HTTP (`GET`, `GETALL`, `HEAD` ou `POST`).

  Para o ITCAM for Transactions V7.4.0.1 e mais recente, o parâmetro de cabeçalho do agente do usuário padrão, `Mozilla/5.0 (ISM-MONITOR)` é incluído para cada novo elemento HTTP ou HTTPS. O cabeçalho do agente do usuário padrão é para que os monitores HTTP e HTTPS possam ser usados para websites que alternam conteúdo com base no cliente do navegador.
- Pares nome-valor do tipo FORM especificam dados extras incluídos no corpo da mensagem de solicitações `POST` de HTTP enviadas pelo monitor. Se a página de destino contiver um formulário correspondente ao nome especificado no campo formname, o monitor tratará quaisquer pares nome-valor no formulário como se eles estivessem configurados no elemento de perfil.

Nota:

O monitor limita o comprimento dos pedidos HTTP para 4096 caracteres. Se o comprimento dos dados do formulário adicional resultar em um comprimento de solicitação que excede esse limite, o monitor não incluirá os dados de formulário adicionais na solicitação.

Elementos do Monitor

Além dos resultados de teste comuns a todos os elementos, o monitor HTTP gera um conjunto de resultados de teste contendo dados específicos para testes de serviço do HTTP. Os elementos indicados por um asterisco (*) estão disponíveis como atributo. Os nomes dos atributos são mostrados entre colchetes. A ausência de um asterisco indica que não há nenhum atributo equivalente. Os atributos mostrados no colchete, mas sem um elemento, indicam que eles só estão disponíveis como atributos, não há elemento equivalente.

Tabela 55. Elementos do Monitor HTTP

Elemento	**Descrição**
$bytesPerSec*(BytesPerSec)	O número médio de bytes transferidos por segundo.
$bytesTransfered*(BytesTransferred)	O número de bytes transferidos por upload ou download.
$checksum	O elemento Checksum normalmente não fornece valores significativos para as classificações de nível de serviço, porque os valores de soma de verificação não são conhecidos quando o elemento de perfil é criado (o monitor calcula valores de soma enquanto os testes estão em andamento). O monitor $checksum e $previousChecksum elementos são destinados ao enriquecimento de alertas usando o arquivo de regras do monitor.
$command	O comando HTTP emitido pelo monitor. Por exemplo, HEAD, GET, GETALL ou POST.
$connectTime*(ConnectTime)	O tempo utilizado para conectar-se ao servidor.
$downloadTime*(DownloadTime)	O tempo utilizado para fazer download do arquivo.
(Elements)	O número de elementos de página recebidos.
$formname	O nome do formulário utilizado em uma ação POST.
$lastStatus*(PageStatus)	Se um elemento de perfil recuperar várias páginas, esse elemento conterá a sequência de resultados da última página recuperada. Esse valor é o mesmo que o de $urlResult*n* em que *n* é igual ao valor de $pageCount.
$lastModified	O valor do campo de cabeçalho HTTP Last-Modified da primeira página recuperada.
$page* (Page)	A página acessada no servidor HTTP.
$pageCount	O número total de recursos transferidos por download durante um teste GETALL, excluindo a própria página de teste. Se a página testada não se referir a nenhum outro recurso, esse elemento não é gerado.

Tabela 55. Elementos do Monitor HTTP (continuação)	
Elemento	**Descrição**
$port*(Port)	A porta utilizada para acessar o servidor HTTP. Se o teste utilizou um servidor proxy, esse será o valor da porta no servidor proxy para o qual a solicitação foi enviada. Para preservar a porta do servidor de destino desejado, configure a propriedade generateProxyTokens para 1 ou inicie o monitor com o parâmetro da linha de comandos -generateproxytokens
$previousChecksum	O elemento PreviousChecksum normalmente não fornece valores significativos para classificações em nível de serviço porque as verificações não são conhecidas quando o elemento de perfil é criado (o monitor calcula valores de soma enquanto os testes estão em andamento). Os elementos do monitor $previousChecksum e $checksum elementos são destinados ao enriquecimento de alertas usando o arquivo de regras do monitor.
$proxyAuthType	O tipo de autenticação do servidor para o servidor proxy.
$proxyCache	O valor true indica que o servidor proxy recuperou a página da Web a partir do servidor, em vez de a partir do seu próprio cache.
$proxyPort	O número da porta do servidor proxy ao qual o pedido foi submetido.
$proxyServer	O nome do host do servidor proxy.
$proxyUsername	Usado pelo monitor junto com a senha para efetuar login no servidor proxy.
$regexpMatch*n*	O conteúdo da linha que corresponde à expressão comum.
$regexp*n*	A expressão regular.
$regexpMatch*n*	O conteúdo da linha que corresponde à expressão comum.
$regexpStatus*n*	O status da correspondência da expressão comum: NONE - Não há nenhuma verificação de expressão comum configurada MATCHED - Foi localizada uma correspondência para a expressão comum FAILED - Uma correspondência não foi localizada para a expressão comum
$responsetime* (ResponseTime)	O tempo utilizado, após a criação de uma conexão, até o recebimento do primeiro byte da página.
$timeSinceModification	O tempo decorrido desde que a página foi modificada pela última vez. Este é o diferença entre o horário do teste e o valor do campo do cabeçalho HTTP Last-Modified da primeira página recuperada.
$urlDownloadTimes*n** (UrlDownloadTime)	Tempo de download da URL de cada elemento de um pedido GETALL. Cada elemento é enumerado a partir de 000 ($urlDownloadTime000, $urlDownloadTime001, $urlDownloadTime002, etc.).
$url*n** (Url)	URL de cada página de um teste GETALL. Cada página é enumerada a partir de 000 ($url000, $url001, $url002, etc.).

Tabela 55. Elementos do Monitor HTTP (continuação)	
Elemento	**Descrição**
$urlResult*n** (UrlResultString)	Cadeia de resultados de cada página transferida por download em um pedido GETALL. Cada resultado é numerado, começando com 000 ($urlResult000, $urlResult001, $urlResult002, e assim por diante).
$username	O nome utilizado para acessar páginas que exigem autenticação do usuário.

Mensagem de status

O monitor HTTP fornece mensagens de status no atributo ResultMessage ao usar o IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

Tabela 56. Tabela 4. Mensagens de Status do Monitor HTTP	
Mensagem	**Descrição**
Ok	O pedido do monitor foi bem-sucedido.
Formulário não localizado	A página solicitada não pode ser localizada.
Initialise Fetch Page Failed	Memória insuficiente para alocar espaço para o mecanismo de busca da página HTTP. A mensagem da linha anterior deve conter informações adicionais.
Connection Failed	O monitor não conseguiu conectar-se por outros motivos que não inatividade do link, reconfiguração da conexão, link inatingível, tempo de conexão esgotado, conexão finalizada ou inatividade do host. Consulte o arquivo de log do monitor HTTP para obter informações adicionais.

Parâmetros de formulário e correspondência de expressão regular

Monitore a operação do formulário http://support.mycompany.com/cgi-bin/search.cgi enviando pedidos HTTP POST com o parâmetro de formulário search=ism e use uma expressão comum para corresponder à cadeia Your search was successful na resposta. Se essa cadeia for retornada na resposta, classifique o nível de serviço como Válido e como Falha, caso contrário.

Crie um novo elemento de perfil HTTP e configure os campos conforme mostrado na tabela a seguir.

Tabela 57. Exemplo de elemento de perfil de formulário HTTP	
Campo de configuração do elemento de perfil	**Valor**
servidor	support.mycompany.com
página	/cgi-bin/search.cgi
description	Exemplo - parâmetros de formulário e expressões comuns
Detalhes da Expressão Regular	
correspondência 1	Your search was successful
Detalhes da Classificação de Nível de	
declaração	Regexp Status 1 = MATCHED then status GOOD
Detalhes de Head e Form	

Tabela 57. Exemplo de elemento de perfil de formulário HTTP (continuação)	
Campo de configuração do elemento de perfil	**Valor**
name	procura
valor	ism
type	FORM

Propriedades

As propriedades e as opções da linha de comandos específicas do monitor HTTP são descritas na tabela a seguir.

Tabela 58. Propriedades do Monitor HTTP		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
AllowDuplicateDownload	0|1	Força o download da página sempre que é localizada. 0 -desativado (transferido por download apenas uma vez) 1 - ativado
ForceHTMLParse	0|1	Força as páginas que não possuem o tipo de conteúdo text/html a serem analisadas como HTML. 0 - desativado 1 - ativado
GenerateProxyTokens	0|1	Especifica se o monitor gerará elementos adicionais contendo informações sobre o servidor proxy se um servidor proxy for utilizado em um teste. 0 - desativado 1 - ativado (os elementos adicionais $server e $port contêm valores para o servidor proxy)
GETALLThreadNum	1|2|3|4|5	Especifica o número de encadeamentos separados a serem utilizados durante um pedido GETALL.
GetLinkTags	0|1	Ativa o download de folhas de estilo vinculadas de pedidos GETALL: 0 - desativado 1 - ativado (se a página de destino contiver uma tag link com o valor de atributo rel=stylesheet, o monitor tentará fazer download do recurso referido pelo atributo link tag's href)

Tabela 58. Propriedades do Monitor HTTP (continuação)

Nome da propriedade	Parâmetro de propriedade	Descrição
HostnameLookupPreference	string	Determina qual versão de IP, IPv6 ou IPv4, é aplicado no nome do host fornecido. Os possíveis valores são: • 4Then6 seleciona IPv4 e, em seguida, IPv6. Utiliza endereços IPv4, se eles estiverem disponíveis. Se não forem localizados endereços IPv4, endereços IPv6 serão utilizados. • 6Then4 seleciona IPv6 e, em seguida, IPv4. Utiliza endereços IPv6, se eles estiverem disponíveis. Se não forem localizados endereços IPv6, endereços IPv4 serão utilizados. • 4Only seleciona apenas IPv4. Usa endereços IPv4 apenas. Se não houver endereços IPv4, a pesquisa retorna um erro. • 6Only seleciona apenas IPv6. Usa apenas endereços IPv6. Se não houver endereços IPv6, a pesquisa retorna um erro. • 6Or4 seleciona IPv4 ou IPv6. Usa o primeiro endereço retornado a partir do nome do host. Padrão: 4Then6
Ipv6Address	integer	O endereço local a ser conectado como uma origem das solicitações de HTTP quando usar o IPv6 HTTP. Padrão: nenhum endereço
NoParseExtensions	string	Uma lista separada por vírgula de extensões de arquivo que indicam tipos de arquivos que o monitor não analisará, mas dos quais fará download.
Diretório de Saída	string	Especifica o diretório de saída a ser utilizado se OutputResult for true (configurado como 1). Padrão: $ISHOME/var
OutputResult	0|1	Especifica se o monitor salvará os dados recebidos do serviço. 0 - desativado 1 - ativado
RelativeRedirects	0|1	Permite que os campos Localização nos códigos de status HTTP 301 e HTTP 302 contenham URLs relativas em vez de URLs absolutas. 0 -URLs absolutas 1 -URLs relativas

Tabela 58. Propriedades do Monitor HTTP (continuação)		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
RFCPOST	0|1	Especifica que o monitor deve seguir a RFC1945 e a RFC2616 e enviar um segundo POST após um redirecionamento. Muitos servidores da web não esperam um POST após um redirecionamento e a maioria dos navegadores não segue os RFCs. 0 - desativado 1 - ativado

Monitor HTTPS

Os monitores HTTP e HTTPS verificam a disponibilidade e o tempo de resposta dos servidores da Web. Ele pode monitorar páginas da web individuais, incluindo as que usam formulários HTML, que normalmente requerem que o usuário insira dados nos campos.

Nota: O monitor HTTPS trabalha da mesma maneira que o monitor HTTP, mas ele se comunica com o servidor HTTP usando a versão 2 ou 3 do protocolo SSL (Secure Sockets Layer), que criptografa todas as comunicações entre o servidor e o monitor.

Tabela 59. Resumo do Arquivo do Monitor HTTPS	
Arquivos do monitor.	**Nome ou local**
Monitor executável	`nco_m_https`
Arquivo de Propriedades	`$ISHOME/etc/props/https.props`
Arquivo de regras	`$ISHOME/etc/rules/https.rules`
Arquivo de log	`$ISHOME/log/https.log`

Diretrizes para configurar o monitor HTTPS

Os monitores HTTP e HTTPS verificam a disponibilidade e o tempo de resposta dos servidores da Web. Use o monitor HTTPS nas seguintes situações:

- O Web site de destino é estático.

  Para Web sites dinâmicos, utilize o monitor TRANSX.
- O Web site de destino é fornecido sobre o protocolo HTTPS.

  Para websites que entregam conteúdo por meio do protocolo HTTP, selecione o monitor HTTP.
- Para executar o monitoramento em várias plataformas.
- Onde a velocidade for um fator determinante (o monitor HTTPS fornece alto desempenho).

Certificado do lado do cliente

O monitor possibilita o monitoramento de servidores que requerem certificados do lado do cliente para autenticação mútua.

Especifique o arquivo de certificado SSL, o arquivo-chave e a senha de chave ao criar um elemento de perfil.

Os certificados devem estar no formato Privacy Enhanced Mail (PEM). Se seu certificado estiver em outro formato, você deve convertê-lo ao formato PEM. Certificados podem ser convertidos usando software, como openSSL, disponível no http://www.openssl.org.

Nota: Se você sempre utilizar o mesmo certificado, chave e senha em todos os elementos do perfil, especifique-os utilizando as propriedades do monitor em vez de defini-las em cada elemento de perfil criado.

Configurando testes de serviço do monitor HTTPS

Use os parâmetros de configuração do monitor HTTPS para definir os testes de serviço do HTTPS.

Tabela 60. Configuração do Monitor HTTPS

Campo	Descrição
servidor	O nome do host do servidor a ser monitorado. O exemplo é `www.myconpany.com`
página	A URL da página a ser monitorada. O exemplo é `/secure/`
description	Um campo de texto para fornecer informações descritivas sobre o elemento.
port	A porta a ser utilizada no servidor. Padrão: 443
IP local	Especifica o endereço IP da interface de rede utilizada pelo monitor para o teste. Se esse campo estiver vazio, o monitor usará o especificado pela propriedade `IpAddress`.
versão	A versão do protocolo HTTPS a ser utilizada: • `1.0` • `1.1` Padrão: `1.0`
comando	O tipo de pedido: • `HEAD` • `GET` • `GETALL` • `POST` Padrão: `GET`
formname	Quando usado em uma transação, o monitor HTTPS varre o formulário especificado para obter valores padrão. Quaisquer valores localizados são concluídos automaticamente na próxima HTTPS na transação.
Tipo de autenticação	Especifica o mecanismo de autenticação de resposta de segurança para autenticar usuários de rede: • `NONE` -Nenhuma autenticação. • `BASIC` • `NTLMv1` - Autenticação de desafio/resposta do Windows NTLM versão 1. • `NTLMv2` - Windows NTLM versão 2. Padrão: `NONE`
nome do usuário	O nome de usuário (nome da conta) para o monitor a ser usado para efetuar login no servidor HTTPS.

Tabela 60. Configuração do Monitor HTTPS (continuação)	
Campo	**Descrição**
senha	A senha correspondente ao nome de usuário para o monitor a ser usado para efetuar login no servidor HTTPS.
sslcertificatefile	O caminho e o nome do arquivo do certificado digital usado no elemento de monitor. Se o caminho não for absoluto, o monitor o interpretará com relação ao diretório ativo (`$ISMHOME/platform/arch/bin`). Se você não especificar um arquivo de certificado, o monitor usará o certificado especificado pela propriedade do monitor `SSLCertificateFile`.
sslkeyfile	O caminho e o nome do arquivo que contém a chave privada SSL, que é usada para identificar o servidor e assinar as mensagens SSL.
Senha da chave do sll	A senha utilizada para criptografar a chave privada SSL.
timeout	O tempo, em segundos, para aguardar para que o servidor responda. Padrão: `30`
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: `300`
failureretests	O número de vezes para testar novamente antes de indicar uma falha. Padrão: `0`
Intervalo de retestagem	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: `10`
Detalhes do Proxy	
servidor	O nome do host do servidor proxy.
port	A porta a ser utilizada no servidor proxy.
Tipo de autenticação	O tipo de autenticação do servidor para o servidor proxy HTTPS. Consulte authenticationtype para obter informações adicionais.
nome do usuário	O nome do usuário para o monitor a ser usado para efetuar login no servidor proxy HTTPS.
senha	A senha para o monitor a ser usado para efetuar login no servidor proxy HTTPS.
useproxy	Configura o monitor para executar a solicitação usando um servidor proxy. • `proxy` (use `true` em ismbatch) • `noproxy` (use `false` em ismbatch) O padrão é `noproxy`

Tabela 60. Configuração do Monitor HTTPS (continuação)	
Campo	**Descrição**
hostnamelookuppreference	Determina qual versão de IP, IPv6 ou IPv4, é aplicada ao nome do host fornecido. As opções são: • `default` configura o monitor para utilizar configurações de propriedades em todo o monitor. Este é o padrão. • `4Then6` seleciona IPv4 e, em seguida, IPv6. Utiliza endereços IPv4, se eles estiverem disponíveis. Se não forem localizados endereços IPv4, endereços IPv6 serão utilizados. • `6Then4` seleciona IPv6 e, em seguida, IPv4. Utiliza endereços IPv6, se eles estiverem disponíveis. Se não forem localizados endereços IPv6, endereços IPv4 serão utilizados. • `4Only` seleciona apenas IPv4. Usa endereços IPv4 apenas. Se não houver endereços IPv4, a pesquisa retorna um erro. • `6Only` seleciona apenas IPv6. Usa apenas endereços IPv6. Se não houver endereços IPv6, a pesquisa retorna um erro. • `6or4` seleciona IPv4 ou IPv6. Usa o primeiro endereço retornado do nome do host.

Correspondência de Expressões Comuns

Você pode desempenhar uma procura de expressão comum nas informações transferidas por download digitando até 50 expressões comuns diferentes. O monitor HTTPS tenta fazer a correspondência dos conteúdos que são recuperados com cada expressão regular.

Se uma correspondência para uma expressão comum especificada for encontrada, as linhas correspondentes (ou o máximo que couber no buffer interno do monitor) serão retornadas no elemento `$regexpMatchn` correspondente. Se a expressão comum corresponder mais de uma vez nas informações transferidas por download, apenas a primeira correspondência será retornada. O status de cada teste de expressão regular é indicado pelos elementos `$regexpStatusn`. Você pode utilizar as correspondências de expressões comuns e suas informações de status como critérios para as classificações em nível de serviço.

Para obter mais informações, consulte Tabela 50 na página 325.

Parâmetro de cabeçote e de formulário

Semelhante ao monitor HTTP, o monitor HTTPS pode enviar dados extras nos campos de cabeçalho e no corpo da mensagem de pedidos de HTTP.

Para obter detalhes sobre parâmetros de título e de formulário, consulte Parâmetro de título e formulário HTTP.

Elementos do monitor

Tabela 61. Elementos do Monitor SSL HTTPS	
Elemento	**Descrição**
$SSLcertificateSerialNumber	O número de série do certificado X509 apresentado pelo servidor.
$SSLcipherSuiteCount	O número de conjuntos de criptografia disponíveis na conexão.
$SSLcipherSuiteList	A lista de conjuntos de criptografia disponíveis na conexão.
$SSLcipherSuiteName	O conjunto de criptografia selecionado para a conexão.

Tabela 61. Elementos do Monitor SSL HTTPS (continuação)	
Elemento	**Descrição**
$SSLeffectiveSessionKeyBits	O número de bits na chave de sessão. Normalmente, é 128 ou 168, ou 40 para versões de exportação.
$SSLHandshakeTime* (SslHandshakeTime)	O tempo utilizado para estabelecer a conexão SSL.
$SSLissuerName	O nome do emissor da certificação no formato X509 do servidor.
$SSLprotocolVersion	A versão de SSL que está sendo utilizada, v2 ou v3.
$SSLpublicKeyLengthBits	O tamanho da chave pública do servidor. Normalmente, é 1024 bits, exceto onde for utilizado um conjunto de criptografia de especificação de exportação.
$SSLserverCertificateValidFrom	A data a partir da qual o certificado de servidor é válido.
$SSLserverCertificateValidTo	A data até a qual o certificado de servidor é válido.
$SSLserverName	Nome do servidor SSL.
$SSLsubjectName	O nome do assunto da certificação do formato X509. Normalmente, é o nome da organização que controla o servidor.

Elementos indicados por um asterisco (*) estão disponíveis como atributos. Os nomes dos atributos são mostrados entre colchetes. A ausência de um asterisco indica que não há nenhum atributo equivalente. Atributos mostrados entre colchetes, mas sem um elemento, indicam que eles estão disponíveis somente como atributos e que não há elementos equivalentes.

O monitor HTTPS produz os mesmos elementos extras que o monitor HTTP, conforme descrito em Tabela 55 na página 333. Além disso, ele produz os elementos que estão relacionados com o SSL se um certificado de lado do cliente for usado no teste, conforme descrito em Tabela 61 na página 341.

Além dos resultados de teste comuns a todos os elementos, o monitor HTTPS gera um conjunto de resultados de teste contendo dados específicos para testes de serviço do HTTPS.

Mensagem de Status

O monitor HTTPS fornece mensagens de status no atributo `ResultMessage` ao usar o IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

Além das mensagens de status HTTP, o monitor HTTPS também gera as mensagens que são listadas no Tabela 62 na página 342.

Tabela 62. Mensagens de Status do Monitor HTTPS	
Mensagem	**Descrição**
OK	O monitor que é conectado ao servidor com sucesso.
`SSL handshake failed`	O monitor não conseguiu inicializar a conectividade SSL depois de estabelecer uma conexão com o servidor.
`Conexão com falha`	O monitor não conseguiu conectar-se por outros motivos que não inatividade do link, reconfiguração da conexão, link inatingível, tempo de conexão esgotado, conexão finalizada ou inatividade do host. Consulte o arquivo de log do monitor HTTP para obter informações adicionais.

Propriedades

O monitor HTTPS possui as mesmas propriedades que o monitor HTTP.

Para obter detalhes sobre as opções de propriedades que são as mesmas que o monitor HTTP, consulte Tabela 58 na página 336. A Tabela 5 lista algumas propriedades adicionais que são específicas para HTTPS.

Tabela 63. Propriedades específicas do monitor HTTPS

Nome da propriedade	Parâmetro de propriedade	Descrição
SSLCertificate File	string	O caminho e o nome do arquivo do certificado digital usado se nenhum certificado for especificado explicitamente para um elemento HTTPS durante sua criação. Se o caminho não for absoluto, o monitor o interpretará com relação ao diretório ativo (`$ISHOME/platform/arch/bin`).
SSLCipherSuite	string	O conjunto de criptografia a ser utilizado para operações SSL. Padrão: `RC4:3DES:DES:+EXP`
SSLDisableTLS	integer	Desativa o TLSv1 para suporte de legado. Padrão: `0` - O TLSv1 está ativado. 1 -TLSv1 está desativado.
SSLKeyFile	string	O arquivo que contém a chave privada SSL.
SSLKeyPassword	string	A senha utilizada para criptografar a chave privada SSL.

Ternos de Cifra

A propriedade `SSLCipherSuite` especifica o conjunto de criptografia usado pelo monitor HTTPS. Para obter mais informações sobre as configurações de SSL, consulte "Configuração de SSL no Internet Service Monitoring" na página 436.

Monitor ICMP

O monitor ICMP testa o desempenho do serviço Internet Control Message Protocol em execução em uma rede. Para isso, o monitor usa o comando ICMP echo.

A tabela a seguir lista os arquivos do monitor ICMP.

Tabela 64. Arquivos do Monitor ICMP

Arquivos do Monitor	Nome ou local
Monitor executável	`nco_m_icmp`
Arquivo de Propriedades	`$ISHOME/etc/props/icmp.props`
Arquivo de regras	`$ISHOME/etc/rules/icmp.rules`
Arquivo de log	`$ISHOME/log/icmp.log`

Diretrizes para configurar o monitor ICMP

O monitor ICMP emite solicitações de repetição do ICMP (comumente chamadas de `pings`) para hosts de destino e aguarda por uma resposta de resposta de eco. Ele registra tempos de consulta, tempos de roundtrip e métricas de taxa de sucesso que fornecem uma indicação de quão bem a rede

está executando. Quando o monitor emite um pedido de eco, o pedido pode passar por um ou mais roteadores antes de chegar ao host de destino. Esses roteadores podem responder ao monitor antes que o host de destino receba o pedido echo. Se um pedido echo emitido pelo monitor for transmitido através de um roteador, o roteador poderá emitir uma resposta para o monitor. Essa resposta pode indicar que o roteador não pode localizar o host de destino ou que o roteador está muito ocupado para processar a solicitação. É possível que o monitor possa receber respostas de vários roteadores antes de receber uma resposta de repetição do host de destino. Se o monitor receber uma resposta echo bem-sucedida do host de destino, ele registrará o tempo gasto. Se o monitor não receber uma resposta do servidor de destino dentro do período de tempo limite especificado, a solicitação será registrada como com falha. É possível configurar o monitor para enviar diversas solicitações repetidas do ICMP para o mesmo destino em cada teste. O monitor registra estatísticas para cada uma das solicitações enviadas.

Nota: Execute o monitor ICMP como `root`, pois ele abre um soquete bruto para enviar pacotes ICMP.

Configurando Testes de Serviço do Monitor ICMP

Utilize os parâmetros de configuração do monitor ICMP para definir testes de serviço. Quando você configura o monitor, os valores padrão são mostrados para os parâmetros de intervalo de sondagem e de tempo limite. Esses padrões são 30 e 300 segundos respectivamente. Outros padrões listados na tabela não são mostrados durante a configuração, mas são aplicados quando os detalhes de configuração são salvos se nenhum valor tiver sido especificado.

A tabela a seguir lista as configurações do monitor ICMP.

Tabela 65. Configuração do Monitor ICMP

Campo	**Descrição**
servidor	O nome do host ou o endereço IP do servidor para o qual as solicitações de eco são enviadas. O exemplo é `test.myconpany.com`
description	Um campo de texto para fornecer informações descritivas sobre o elemento.
timeout	O tempo, em segundos, para aguardar que o servidor responda cada solicitação de eco. Padrão: `10`
numberofpings	O número de solicitações de eco a serem enviadas. Padrão: 5
packetinterval	O tempo, em segundos, para aguardar entre o envio de solicitações de eco. Padrão: 1
packetsize	O tamanho, em bytes, de cada solicitação de eco enviada. Padrão: 64
typeofservice	Configura o campo Tipo de Serviço na camada IP. Ambos os valores Tipo de Serviço (TOS) do estilo IPv4 e Campo de Serviço Diferenciado DSCP podem ser digitados. Os valores válidos são `0` -`255`.
tentar novamente	O número de vezes que o monitor deve tentar novamente cada solicitação de eco antes de encerrar. Padrão: `0`
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: `300`

Tabela 65. Configuração do Monitor ICMP (continuação)	
Campo	**Descrição**
failureretests	O número de vezes para testar novamente antes de indicar uma falha. Padrão: `0`
retestinterval	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: `10`
hostnamelookuppreference	Determina qual versão de IP, IPv6 ou IPv4, é aplicado no nome do host fornecido. As opções são: • `default` configura o monitor para utilizar configurações de propriedades em todo o monitor. Este é o padrão. • `4Then6` seleciona IPv4 e, em seguida, IPv6. Utiliza endereços IPv4, se eles estiverem disponíveis. Se não forem localizados endereços IPv4, endereços IPv6 serão utilizados. • `6Then4` seleciona IPv6 e, em seguida, IPv4. Utiliza endereços IPv6, se eles estiverem disponíveis. Se não forem localizados endereços IPv6, endereços IPv4 serão utilizados. • `40nly` seleciona apenas IPv4. Usa endereços IPv4 apenas. Se não houver endereços IPv4, a pesquisa retorna um erro. • `60nly` seleciona apenas IPv6. Usa apenas endereços IPv6. Se não houver endereços IPv6, a pesquisa retorna um erro. • `60r4` seleciona IPv4 ou IPv6. Usa o primeiro endereço retornado a partir do nome do host.

Nota: Monitore a disponibilidade do host `test.mycompany.com` verificando os tempos de resposta em intervalos de 10 minutos. Tente se conectar ao servidor dentro de 30 segundos e, se o tempo limite for atingido, tente novamente mais duas vezes. Se ele ainda falhar, repita o teste três vezes com 5 segundos entre cada nova tentativa.

Elementos do Monitor

Além dos resultados de teste comuns a todos os elementos, o monitor ICMP gera um conjunto de resultados de teste contendo dados específicos para testes de serviço do ICMP.

A tabela a seguir descreve os elementos adicionais para o monitor ICMP.

Elementos indicados por um asterisco (*) estão disponíveis como atributos. Os nomes dos atributos são mostrados entre parênteses abaixo do elemento. A ausência de um asterisco indica que não há nenhum atributo equivalente. Os atributos mostrados no colchete, mas sem um elemento, indicam que eles só estão disponíveis como atributos, não há elemento equivalente.

Tabela 66. Elementos do Monitor ICMP	
Elemento	**Descrição**
`$averageRTT*` (`AverageRTT`)	O tempo médio de roundtrip em segundos.
`$endTime`	A hora de recebimento da resposta no UNIX.

Tabela 66. Elementos do Monitor ICMP (continuação)	
Elemento	**Descrição**
`$jitter`	O valor absoluto da diferença entre os horários de chegada de duas solicitações de eco ICMP adjacentes, menos seus horários de partida. Esse valor é calculado de acordo com a fórmula especificada no RFC2598. O elemento será criado apenas se o número de solicitações de eco for maior que um. Se mais de duas solicitações de eco forem usadas, o valor será o jitter médio entre todos os pares de solicitações de eco.
`$lookupTime*(LookupTime)`	O tempo utilizado para obter o endereço IP do servidor host.
`$maxRTT*` (`MaxRTT`)	O tempo máximo de roundtrip em segundos.
`$minRTT*` (`MinRTT`)	O tempo mínimo de roundtrip em segundos.
`$numberPackets`	O número de solicitações de eco ICMP enviadas, conforme especificado no elemento de perfil.
`$packetInterval`	O tempo entre o envio de cada solicitação de eco ICMP, conforme especificado no elemento de perfil.
`$packetRetries`	O número de vezes que o monitor tentou reenviar as solicitações de eco ICMP antes de ser encerrado.
`$packetSize`	O tamanho (em bytes) de cada solicitação de eco ICMP, conforme especificado no elemento de perfil.
`$pingAttempts Failed`	O número de tentativas feitas para a primeira solicitação de eco ICMP sem êxito.
`$pingAttempts Responded`	O número de tentativas feitas para a primeira solicitação de eco ICMP bem-sucedida.
`$pingMessageFailed`	A mensagem retornada para a primeira solicitação de eco ICMP sem êxito.
`$pingMessage Responded`	A mensagem retornada para a primeira solicitação de eco ICMP bem-sucedida.
`$pingReceivedTime Failed`	O horário do UNIX em que a primeira resposta de eco sem êxito foi recebida.
`$pingReceivedTime Responded`	O horário do UNIX em que a primeira resposta de eco bem-sucedida foi recebida.
`$pingRespondIP Failed`	O endereço IP que respondeu à primeira solicitação de eco ICMP sem êxito.
`$pingRespondIP Responded`	O endereço IP que respondeu à primeira solicitação de eco ICMP bem-sucedida.
`$pingRTTFailed`	O tempo de roundtrip para a primeira solicitação de eco ICMP sem êxito em segundos.
`$pingRTTResponded`	O tempo de roundtrip para a primeira solicitação de eco ICMP bem-sucedida em segundos.
`$pingSentTime Failed`	O horário do UNIX em que a primeira solicitação de eco ICMP sem êxito foi enviada.

Tabela 66. Elementos do Monitor ICMP (continuação)	
Elemento	**Descrição**
$pingSentTime Responded	O horário do UNIX em que a primeira solicitação de eco ICMP bem-sucedida foi enviada.
$pingsFailed	O número de solicitações de eco ICMP enviadas, para que não houvesse nenhuma resposta de eco.
$pingsResponded	O número de respostas de eco válidas recebidas.
$pingTime	O tempo levado para receber a resposta de eco após enviar a solicitação de eco ICMP.
$respondPercent* ($RespondPercent)	A porcentagem de solicitações de eco ICMP enviadas para que houvesse uma resposta.
$responseTime	O tempo gasto para que o host de destino responda a uma solicitação de eco ICMP.
$sentTime	O horário do UNIX em que as solicitações de eco ICMP foram enviadas.
$spreadRTT	A diferença entre $maxRTT e $minRTT.
$startTime	O tempo UNIX que o teste iniciou.
$totalHostTime	O tempo levado para receber a resposta de eco após iniciar o teste.
$typeOfService	O campo Tipo de Serviço na camada IP, conforme especificado ao incluir um novo elemento ICMP. Para obter detalhes, consulte "Monitor ICMP" na página 343.

O monitor ICMP cria um conjunto separado de elementos $pingname para registrar os resultados para cada solicitação de repetição do ICMP enviada durante o teste. O número de solicitações enviadas é indicado por $numberPackets. Por exemplo, para o elemento $pingRTT, se $numberPackets for 3, o monitor criará três elementos ($pingRTT1, $pingRTT2 e $pingRTT3), contendo a medição do tempo de roundtrip para as três solicitações de repetição do ICMP enviadas.

Mensagem de status

O monitor ICMP fornece mensagens de status no atributo ResultMessage ao usar o IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

A tabela a seguir descreve as mensagens de status do ICMP.

Tabela 67. Mensagens de Status do Monitor ICMP	
Mensagem	**Descrição**
Pings Complete	O pedido de eco do ICMP foi bem-sucedido.
ICMP echo failed	O monitor não pode emitir a solicitação de repetição do ICMP porque há um problema com o host do monitor ou sua conexão com a rede.
Tempo limite esgotado	O pedido de eco ICMP atingiu o tempo limite.
Inalcançável	Esta mensagem é retornada de um roteador e não é necessariamente exata.
Source quench	Um roteador está muito ocupado para processar a solicitação de eco ICMP.

Tabela 67. Mensagens de Status do Monitor ICMP (continuação)	
Mensagem	**Descrição**
`Time exceeded`	Essa mensagem é retornada de um roteador. Ela indica que a solicitação de eco ICMP foi encaminhada em torno da rede muitas vezes.
`Parameter problem`	Essa mensagem é retornada de um roteador. Isso indica que o roteador não pode processar a solicitação de repetição do ICMP. Isso pode ser porque a mensagem foi corrompida.

Propriedades

As propriedades específicas para o monitor ICMP são descritas a seguir.

Tabela 68. Propriedades do ICMP		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
`EventsPerSec`	não-aplicável	Essa propriedade não é suportada.
`IntraPingWait`	integer	O intervalo de tempo mínimo em milissegundos entre todos os pings enviados pelo monitor IMCP. Use para ajustar seu sistema para distribuir o tráfego de rede em um período mais longo. Por exemplo, em um ambiente com milhares de hosts de ICMP destinados, configure `IntraPingWait` como 3. Padrão: `0`
`Ipv6Address`	integer	O endereço local a ser ligado como uma origem para solicitações de eco ICMP ao usar o IPv6 de ICMP. Padrão: nenhum endereço
`MaxDNSResolvingThreads`	integer	O número máximo de encadeamentos a serem usados pelo Resolvedor DNS. Padrão: `20`
`MaxPacketSize`	integer	O tamanho máximo do pacote ICMP em bytes.
`PingsPerSec`	integer	O número de solicitações de eco que o monitor tenta enviar por segundo. O número de solicitações reais enviadas dependentes de CPU e de carregamento de rede. Padrão: `100`
`SocketBufferSize`	integer	O tamanho do buffer do soquete de recebimento (em kilobytes). Padrão: `32`

LDAP Monitor

O monitor LDAP testa a operação de servidores LDAP (Lightweight Directory Access Protocol).

A tabela a seguir lista os arquivos do monitor LDAP.

Tabela 69. Arquivos do Monitor LDAP	
Arquivos do Monitor	**Nome ou local**
Monitor executável	`nco_m_ldap`
Arquivo de Propriedades	`$ISHOME/etc/props/ldap.props`
Arquivo de regras	`$ISHOME/etc/rules/ldap.rules`
Arquivo de log	`$ISHOME/log/ldap.log`

Diretrizes para configurar o monitor LDAP

O monitor LDAP testa os serviços LDAP conectando-se a um servidor LDAP e tentando localizar uma entrada específica. Se o servidor obtiver êxito na localização da entrada, ele retorna o conteúdo dessa entrada para o monitor. O monitor LDAP pode usar SSL para autenticar e se conectar ao servidor LDAP.

Para configurar o monitor LDAP, é necessário entender como o protocolo LDAP e o serviço de diretório monitorado funcionam. LDAP é um protocolo da Internet para acessar e gerenciar Serviços de Diretório. Um serviço de diretório é um aplicativo de banco de dados distribuído. Um diretório consiste de entradas. Por exemplo, um diretório pode conter entradas relacionadas aos funcionários ou recursos de uma organização. Cada entrada contém um conjunto de atributos, por exemplo, as entradas em um diretório de funcionários pode conter o nome, número de telefone e endereço de um funcionário.

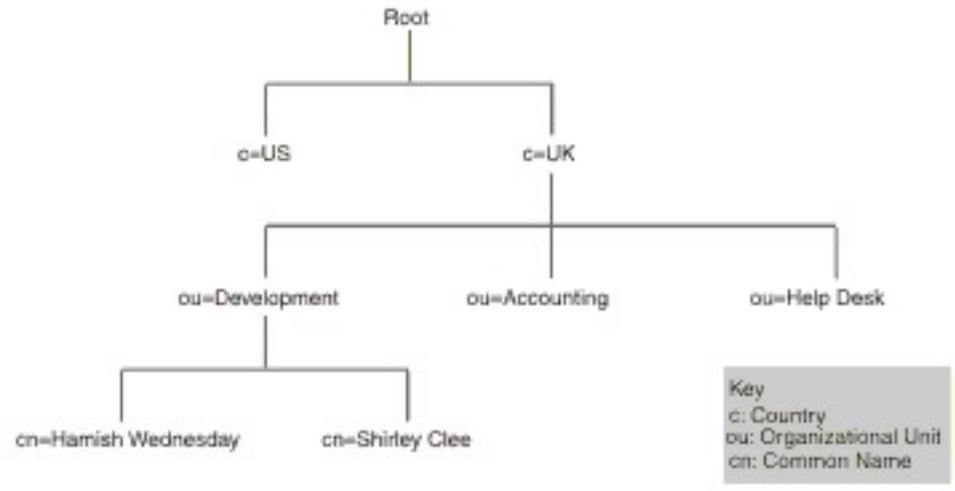
Serviços de Diretório Individuais podem ser construídos diferentemente, portanto, o procedimento de monitoramento também pode ser diferente.

Versões LDAP

O monitor LDAP suporta a versão 2 e 3 do LDAP. Por padrão, o monitor tenta se conectar ao servidor LDAP de destino que usa a versão 3 e, depois, retrocede automaticamente para a versão 2 se a tentativa falhar. Você pode forçar o monitor a sempre usar a versão 2 configurando a propriedade **NOLDAPV3**.

Serviço de Diretório de Exemplo

Este exemplo de serviço de diretório armazena os detalhes pessoais de todos os funcionários. O diretório é dividido em países e depois em departamentos. Os funcionários e seus atributos são armazenados em cada departamento.



A imagem de exemplo da hierarquia de diretório mostra uma extração de um diretório de exemplo. Esta figura mostra uma estrutura de diretório. No apex, o nível é raiz. Os dois subdiretórios representam países e são rotulados como UK e US. O subdiretório UK é dividido em outros três subdiretórios representando as unidades de organização. Eles são rotulados como Development,

Accounting e Help Desk. Dentro da unidade de organização Development, há dois subdiretórios para nomes comuns, que são Shirley Clee e Hamish Wednesday.

Entidades são referenciadas por seus nomes distintos. Um nome distinto é a rota para a entidade. Por exemplo, os nomes distintos do departamento de contabilidade e Hamish Wednesday seriam:

```
dn="ou=accounting, c=UK"
dn="cn=Hamish Wednesday, ou=Development, c=UK"
```

A entrada para cada funcionário tem vários atributos. Por exemplo, a entrada para Hamish Wednesday contém os seguintes detalhes.

```
cn: Hamish Wednesday
uid: ham
mail: HWednesday@development.mycompany.com
telephoneNumber: 88 88 55 44
```

Cada entidade na hierarquia de diretório pode ser protegida por um nome de usuário (no LDAP, é um nome distinto) e senha. O monitor usa esse nome de usuário e senha para acessar o servidor LDAP.

Quando o monitor acessa o servidor, ele indica onde na hierarquia de diretório a procura pela entidade de destino começa. Isso é especificado no campo searchBase como um nome distinto. Por exemplo, a procura poderia começar no nível de departamento:

```
ou=Accounting, c=UK
```

Nota: As entidades que englobam um nome distinto estão na ordem inversa. Ou seja, elas começam no ponto mais baixo na hierarquia e, em seguida, listam cada entidade precedente.

A entidade de destino é transmitida ao servidor no campo de filtro. Esse campo contém um atributo da entidade de destino. Por exemplo, para procurar pela entidade Hamish Wednesday's, o campo de filtro pode conter:

```
(uid=ham)
```

O servidor LDAP usa os campos que são fornecidos pelo monitor para procurar a entidade de destino. O resultado da procura é retornado para o monitor.

Se a procura for bem-sucedida, o servidor também retornará os atributos da entidade de destino. O monitor os converterá em elementos cujos nomes são criados dinamicamente. Por exemplo, o monitor converteria a entrada para Hamish Wednesday em:

```
$dnMatched = "cn=Hamish Wednesday, ou=Development, c=UK"
$cn = "Hamish Wednesday"
$uid = "ham"
$mail = "HWednesday@development.mycompany.com"
$telephoneNumber = "88 88 55 44"
```

Autenticação LDAP

A Autenticação de Servidor LDAP SSL conta com certificados de chave pública-privada, assinados por autoridades de certificação, como Verisign e Thawte. Para a autenticação SSL, o monitor LDAP usa o banco de dadosNetscape cert7db de certificados públicos para verificar as assinaturas do certificado do servidor LDAP emitidas pelas autoridades de certificação.

Se você estiver usando certificados assinados por uma autoridade de certificação reconhecida por Netscape, como Verisign ou Thawte, o monitor LDAP os reconhecerá automaticamente. Se você estiver usando certificados assinados por sua organização ou por uma organização que não esteja no banco de dados Netscape, será preciso incluí-los no banco de dados cert7db.

Use o utilitário certutil, disponível no Netscape, para incluir seus certificados no banco de dados. O banco de dados cert7db para o monitor LDAP está no arquivo `$ISHOME/certificates/cert7.db`.

Para monitorar servidores LDAP protegidos por criptografia SSL ou TLS, configure as variáveis de ambiente, conforme descrito na tabela a seguir:

Tabela 70. Variáveis de Ambiente Necessárias para Monitorar Servidores LDAP Protegidos		
Variável	**Descrição**	**Configuração**
LDAPTLS_CACERT	Especifica o arquivo que contém os certificados CA	Arquivo contendo o certificado do servidor. Por exemplo, `cacert.pem`.
LDAPTLS_REQCERT	Especifica as verificações para executar em um certificado do servidor	Selecione a partir de `never` | `allow` | `try` | `demand`.

Para obter mais informações, consulte http://www.openldap.org.

Propriedades

Propriedades que são específicas do monitor LDAP são descritas na seguinte tabela:

Tabela 71. opções de propriedades do monitor LDAP		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
NOLDAPV3	0|1	Força o monitor a utilizar LDAP v2 em vez de LDAP v3. 0 - use LDAP v3 1 - use LDAP v2

Conjuntos de Criptografia

A propriedade `SSLCipherSuite` especifica o conjunto de criptografia usado pelo monitor LDAP. Para obter mais informações sobre as configurações de SSL, consulte "Configuração de SSL no Internet Service Monitoring" na página 436.

Configurando testes de serviço do monitor LDAP

Utilize os parâmetros de configuração do monitor LDAP para definir testes de serviço.

Quando você configura o monitor, os valores padrão mostrados para os parâmetros de tempo limite são de 30 segundos e o parâmetro de intervalo é de 300 segundos. Outros padrões listados na tabela não são mostrados durante a configuração, mas são aplicados quando detalhes de configuração são salvos, caso o valor não seja especificado.

A tabela a seguir descreve as configurações do monitor LDAP:

Tabela 72. Configuração do Monitor LDAP	
Campo	**Descrição**
server	O nome ou o endereço IP do servidor LDAP a ser monitorado. Por exemplo, `ldap.mycompany.in`.
searchbase	O nome distinto do local do qual iniciar a procura. Por exemplo, `ou=Accounting, c=UK`.
filtrar	Um atributo da entidade de destino na qual procurar. Por exemplo, `(uid=ham)`.
description	Um campo de texto para fornecer informações descritivas sobre o elemento. Por exemplo, `LDAP monitor`.
Ativo	Seleciona se o elemento de perfil deve ser ativado após ser criado. Por exemplo, `Selected`.

Tabela 72. Configuração do Monitor LDAP (continuação)	
Campo	**Descrição**
port	A porta do servidor LDAP à qual se conectar. É necessário especificar a porta SSL se estiver utilizando a autenticação SSL. Padrão: 389
username	O nome do usuário usado para efetuar login no serviço de diretório. O formato do nome do usuário depende da configuração de Tipo de Autenticação. Você pode especificar um domínio Windows, isto é, `DOMAIN\username`. Por exemplo, `jbloggs`.
senha	A senha utilizada para efetuar login para o serviço de diretório, se necessário. Por exemplo, `secret9`.
Tipo de autenticação	O método de autenticação LDAP a ser utilizado: • SIMPLE (senha de texto sem formatação ou anônima) • SSL-SIMPLE • SASL-DIGEST-MD5 **Nota:** A autenticação SASL-DIGEST-MD5 não está disponível no sistema operacional Linux. Se você configurar o tipo de autenticação para SIMPLE ou SSL-SIMPLE, insira o nome do usuário em formato de nome distinto. Se você configurar o tipo de autenticação para SASL-DIGEST-MD5, insira o nome do usuário como SASL bind-ids. Para efetuar login no servidor LDAP como um usuário anônimo, configure o tipo de autenticação para SIMPLE e deixe os campos de nome de usuário e senha em branco. Padrão: SIMPLE
saslrealm	A região de autenticação para o servidor LDAP; geralmente o nome de domínio completo do servidor. Se quiser compartilhar as senhas entre vários sistemas, você deverá usar um nome de domínio. Por exemplo, `mycompany.com`.
timeout	O tempo, em segundos, para aguardar para que o servidor responda. Padrão: 30
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: 300
failureretests	O número de vezes para retestagem antes de a falha ser indicada. Padrão: 0
Intervalo de retestagem	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: 10

Classificações em Nível de Serviço

As opções de classificação em nível de serviço disponíveis para o monitor LDAP são:

```
totalTime
connectTime
```

```
searchTime
initTime
dnMatched
Mensagem
```

Nas classificações em nível de serviço:

- Especifique classificações de nível de serviço extra inserindo manualmente o nome do elemento de monitor. O nome deve corresponder ao nome mostrado para o elemento na seção Elementos do Monitor.
- `message` pode ser qualquer mensagem encaminhada no elemento **`$message`** para o servidor IBM Application Performance Management se usado em qualquer widget. Para obter uma lista de valores possíveis, consulte Mensagens de status.
- O operando é uma cadeia ou um número positivo.

Elementos do Monitor

Além dos resultados de testes comuns a todos os elementos, o monitor LDAP gera um conjunto de resultados de teste contendo dados específicos para os testes de serviço LDAP.

A tabela a seguir lista os elementos adicionais para o monitor LDAP.

Tabela 73. Elementos do Monitor LDAP

Elemento	**Descrição**
$authentication	O tipo de método de autenticação de usuário exigido pelo servidor LDAP (Standard ou CRAM-MD5).
$connectTime* (ConnectTime)	O tempo utilizado para conectar-se ao servidor LDAP.
$distinguishedName* (UserName)	O nome distinto utilizado para efetuar login no serviço de diretório.
$dnMatched	A entidade correspondida na procura.
$filter* (SrchFilter)	O atributo utilizado para localizar a entidade de destino.
$initTime* (InitTime)	O tempo utilizado para inicializar o cliente LDAP.
$port* (Port)	A porta no servidor LDAP à qual o monitor é conectado.
$saslRealm	A região SASL que você especificou após um novo elemento LDAP ser incluído.
$searchBase* (SearchBase)	O nome distinto da entidade a partir da qual a procura foi iniciada.
$searchTime* (SearchTime)	O tempo utilizado para concluir a procura.

Mensagens de Status

O monitor LDAP fornece mensagens de status no atributo **ResultMessage** ao usar IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

A tabela a seguir descreve as mensagens de status LDAP.

Tabela 74. Mensagens de Status do Monitor LDAP

Mensagem	**Descrição**
`Pesquisa com êxito`	A solicitação foi bem-sucedida.
`Falha na procura`	O pedido falhou.
`Sem correspondência`	O servidor pode não localizar uma entrada correspondente no critério de procura.
`Conexão expirada`	A conexão foi bem-sucedida, mas depois o servidor parou de responder.
`Falha na inicialização - foi especificado um tipo de autenticação não identificado`	Ocorrerá se for utilizado um tipo de autenticação não suportado pelo monitor LDAP.
`Falha na inicialização do cliente`	A inicialização das estruturas do LDAP falhou por causa de memória inadequada.
`Falha na ligação (autenticação)`	O servidor que está aguardando a conclusão da ligação expirou o tempo limite.
`A ligação SASL não é possível porque o servidor não suporta LDAPv3`	O servidor deve suportar LDAPv3 para criar uma ligação SASL.
`A ligação SASL não é possível porque 'bind_id' (nome do usuário), senha ou sasl_realm está em branco`	Para que uma ligação ocorra, todos os campos de autenticação devem ter um valor. Portanto, uma ligação SASL não será possível se o usuário tiver efetuado login anonimamente (com texto sem formatação) usando o tipo de autenticação SIMPLE.
`Erro de ligação de SASL`	O motivo para a falha de ligação SASL não poder ser identificada.
`Erro de autorização da ligação SASL`	A ligação SASL falhou porque as credenciais de autorização estavam incorretas.

monitor IMAP4

O monitor IMAP4 funciona com o monitor SMTP para testar a disponibilidade e o tempo de resposta de um serviço de e-mail IMAP4.

A tabela a seguir lista os arquivos do monitor IMAP4.

Tabela 75. arquivos do monitor IMAP4

Arquivos do Monitor	**Nome ou local**
Monitor executável	`nco_m_imap4`
Arquivo de Propriedades	`$ISHOME/etc/props/imap4.props`

Tabela 75. arquivos do monitor IMAP4 (continuação)	
Arquivos do Monitor	**Nome ou local**
Arquivo de regras	`$ISHOME/etc/rules/imap4.rules`
Arquivo de log	`$ISHOME/log/imap4.log`

Diretrizes para Configurar o Monitor IMAP4

O monitor IMAP4 trabalha com o monitor SMTP monitorando a caixa de correio para a qual o monitor SMTP envia mensagens de teste e medindo a quantidade de tempo levada para entregar essas mensagens.

Nota: Assegure-se de que os relógios do sistema no computador host do monitor e no servidor de e-mail estejam sincronizados para que o cálculo de tempo de entrega funcione corretamente.

Quando o monitor IMAP4 lê o conteúdo da caixa postal, ele gera dois tipos diferentes de eventos:

- Eventos Específicos da Mensagem

  O monitor IMAP4 cria um evento específico de mensagem para cada mensagem de e-mail que é transferida por download da caixa de correio. Neste tipo de evento, o monitor configura o elemento `$message` para `Mensagem Transferida por Download com Êxito`. O elemento `$timeToDeliver` é calculado como o tempo gasto até que a mensagem passe pelo monitor SMTP que a emitiu e a caixa postal que a recebeu. O elemento `$hopCount` indica o número de hosts da mensagem ignorados até chegar na caixa postal.
- Eventos de resumo

  O monitor cria um evento de resumo quando processa todas as mensagens na caixa postal. Neste tipo de evento, o elemento `$message` indica o número total de mensagens transferidas por download com êxito da caixa postal e o elemento `$totaltime` indica o tempo gasto para concluir os pedidos. O `$totaltime` está em segundos.

Correio Seguro

O monitor IMAP4 suporta conexões com serviços de correios seguros. Ele pode se conectar usando SSL/TLS, ou o comando STARTTLS. Ao definir um elemento de perfil, use o campo securitytype para selecionar a segurança apropriada. Se o servidor de e-mail requerer um certificado de lado do cliente para criptografia SSL, use as propriedades SSL para especificar um arquivo de certificado, arquivo-chave, senha de chave e conjunto de criptografia.

Certificados do lado do cliente

O monitor IMAP4 possibilita o monitoramento de servidores que requerem certificados do lado do cliente para autenticação mútua.

Especifique o arquivo de certificado SSL, o arquivo-chave e a senha de chave ao criar um elemento de perfil.

Os certificados devem estar no formato Privacy Enhanced Mail (PEM). Se seu certificado estiver em outro formato, você deve convertê-lo ao formato PEM. Os certificados podem ser convertidos usando um software como o openSSL, que está disponível em http://www.openssl.org.

Nota: Se você sempre utilizar o mesmo certificado, chave e senha em todos os elementos do perfil, especifique-os utilizando as propriedades do monitor em vez de defini-las em cada elemento de perfil criado.

Caixas de correio

Após o monitor IMAP4 processar as informações contidas em um e-mail enviado pelo monitor SMTP, ele o excluirá da caixa de correio. É possível usar qualquer caixa de correio existente para armazenar mensagens de e-mail entre os dois monitores, mesmo se a caixa de correio pertencer a um usuário real. No entanto, é recomendável criar uma conta de caixa de correio especial para teste de serviço.

Configurando Testes de Serviço do Monitor IMAP4

Utilize os parâmetros de configuração do monitor IMAP4 para definir testes de serviço.

Quando você configura o monitor, os valores padrão são mostrados para os parâmetros de intervalo de sondagem e de tempo limite. Esses padrões são 30 e 300 segundos respectivamente. Outros padrões listados na tabela não são mostrados durante a configuração, mas são aplicados quando os detalhes de configuração são salvos se nenhum valor tiver sido especificado.

Tabela 76. Configuração do Monitor IMAP4

Campo	**Descrição**
servidor	O endereço IP do servidor de e-mail. O exemplo é `test.mycompany.com`
description	Um campo de texto para fornecer informações descritivas sobre o elemento.
port	A Porta IP do Servidor IMAP4. Padrão: `143`
securitytype	O tipo de conexão segura aberta com o servidor de e-mail: • `NONE` - Conectar sem segurança. • `SSL` - Enviar um `hello` SSLv2 e, em seguida, negociar SSLv2, SSLv3 ou TLSv1. • `STARTTLS` - Conectar sem segurança, emitir um comando `STARTTLS` e, em seguida, estabelecer uma conexão no TLSv1. Padrão: `NONE`
nome do usuário	O nome da caixa de correio.
senha	A senha utilizada para efetuar login na caixa postal, se necessário.
Tipo de autenticação	O método de autenticação a ser usado (`STANDARD` ou `CRAM_MD5`) Padrão: `STANDARD`
Segredo compartilhado	O segredo compartilhado para a autenticação CRAM_MD5, se aplicável.
timeout	O tempo, em segundos, para aguardar para que o servidor responda. Padrão: `30`
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: `300`
failureretests	O número de vezes para testar novamente antes de indicar uma falha. Padrão: `0`
retestinterval	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: `10`

Correspondência de Expressões Comuns

Você pode desempenhar uma procura de expressão comum nas informações transferidas por download digitando até 50 expressões comuns diferentes. O monitor tenta corresponder o conteúdo recuperado a cada uma das expressões comuns.

Se uma correspondência para uma expressão comum especificada for encontrada, as linhas correspondentes (ou o máximo que couber no buffer interno do monitor) serão retornadas no elemento `$regexpMatchn` correspondente. Se a expressão comum corresponder mais de uma vez nas informações transferidas por download, apenas a primeira será retornada. O status de cada teste de expressão regular é indicado pelos elementos `$regexpStatusn`. Você pode utilizar as correspondências de expressões comuns e suas informações de status como critérios para as classificações em nível de serviço.

Para obter informações sobre a sintaxe das expressões comuns, consulte o Tabela 50 na página 325.

Elementos do Monitor

Além dos resultados de teste comuns a todos os elementos, o monitor IMAP4 gera um conjunto de resultados de teste que contém dados específicos aos testes de serviços do IMAP4.

A tabela a seguir descreve os elementos adicionais para o monitor IMAP4.

Elementos indicados por um asterisco (*) estão disponíveis como atributos. Os nomes dos atributos são mostrados entre colchetes. A ausência de um asterisco indica que não há nenhum atributo equivalente. Os atributos mostrados no colchete, mas sem um elemento, indicam que eles só estão disponíveis como atributos, não há elemento equivalente.

Tabela 77. Elementos do Monitor IMAP4

Elemento	**Descrição**
`$authentication`	O tipo de método de autenticação de usuário exigido pelo servidor IMAP4 (Padrão ou CRAM-MD5).
`$bytesPerSec`	O número médio de bytes transferidos por segundo.
`$bytesTransferred`	O número de bytes transferidos por upload ou download.
`$connectTime`	O tempo utilizado para conectar-se ao servidor IMAP4.
`$downloadTime*` (`DownloadTime`)	O tempo utilizado para fazer download do arquivo.
`$hopCount`	O número de hosts que a mensagem saltou para chegar à caixa postal.
`$inEvent`	Indica que esse evento faz parte de vários eventos. `1` indica que não é o evento final. `0` indica que é o evento final.
`$lookupTime*`(`LookupTime`)	O tempo utilizado para obter o endereço IP do servidor host.
`$port*`(`Port`)	A porta na qual o serviço é monitorado.
`$responseTime*` (`ResponseTime`)	O tempo entre quando a conexão é estabelecida e o primeiro byte de dados é recebido.
`$security`	O tipo de conexão segura aberta com o servidor de e-mail especificado ao incluir um elemento IMAP (`NONE`, `STARTTLS` ou `SSL`).
`$sentTo*`(`SentTo`)	O endereço de e-mail usado pelo monitor SMTP para enviar a mensagem original.
`$smtpServer`	O nome do servidor SMTP a partir do qual o e-mail foi enviado.

Tabela 77. Elementos do Monitor IMAP4 (continuação)	
Elemento	**Descrição**
$SSLHandshakeTime* (SslHandshakeTime)	O tempo utilizado para estabelecer a conexão SSL.
$timeToDeliver	O tempo que uma mensagem de e-mail leva entre um monitor SMTP e sua caixa de correio de destino.
$user*(ImapUser)	O nome de usuário (nome da conta) usado pelo monitor para efetuar login no servidor IMAP4.

Mensagem de status

O monitor IMAP fornece mensagens de status no atributo ResultMessage ao usar o IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

A tabela a seguir descreve as mensagens de status IMAP4.

Tabela 78. Mensagens de Status do Monitor IMAP4	
Mensagem	**Descrição**
Message successfully downloaded	A mensagem foi transferida por download com êxito.
Downloaded x messages	Indica quantas mensagens foram transferidas por download com êxito da caixa postal.
Server not IMAP4rev1 compliant	O servidor IMAP4 não está em conformidade com a especificação IMAP4 (RFC2060).
Server does not support STARTTLS capability	O servidor não está configurado corretamente.
Unable to log into server	O monitor não pode efetuar login no servidor IMAP.
Unrecognised response to STATUS command	O monitor não reconhece o valor retornado pelo servidor.
Unrecognised response to FETCH INTERNALDATE command	
Failed to obtain Actual-Time-Sent header	O monitor não obteve a resposta esperada do servidor.
Failed to obtain Actually-To header	
Failed to obtain SMTP-Server header	

Propriedades

As propriedades e as opções da linha de comandos específicas ao monitor IMAP4 são descritas na tabela a seguir.

Tabela 79. propriedades do monitor IMAP4		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
`Originator`	string	Especifica o campo `From` para correspondência ao recuperar as mensagens de e-mail de teste enviadas pelo monitor SMTP. O monitor recupera apenas as mensagens em que o campo De corresponde à cadeia no Originator. O Originator do IMAP4 deve corresponder ao Originator no monitor SMTP. Padrão: `SMTP-Monitor`
`SSLCertificate File`	string	O caminho e o nome do arquivo de certificado digital utilizados se nenhum certificado for especificado explicitamente para um elemento HTTPS durante sua criação. Se o caminho não for absoluto, o monitor o interpretará com relação ao diretório ativo (`$ISHOME/platform/arch/bin`).
`SSLCipherSuite`	string	O conjunto de criptografia a ser utilizado para operações SSL. Para obter uma descrição de valores possíveis, consulte Conjuntos de cifras. Padrão: `RC4:3DES:DES:+EXP`
`SSLDisableTLS`	integer	Desativa o TLSv1 para suporte de legado. Padrão: `0` -TLSv1 está ativado. 1 -TLSv1 está desativado.
`SSLKeyFile`	string	O arquivo que contém a chave privada SSL.
`SSLKeyPassword`	string	A senha utilizada para criptografar a chave privada SSL.

Conjuntos de Criptografia

A propriedade `SSLCipherSuite` especifica o conjunto de criptografia utilizado pelo monitor IMAP4. Para obter mais informações sobre as configurações de SSL, consulte "Configuração de SSL no Internet Service Monitoring" na página 436.

Monitor NTP

O monitor Network Time Protocol (NTP) consulta um servidor NTP usando UDP (User Datagram Protocol) para determinar se o servidor está fornecendo o horário correto.

O NTP usa Hora Universal Coordenada para sincronizar os relógios do computador para milissegundo.

A tabela a seguir lista os arquivos do monitor NTP.

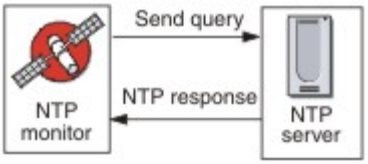
Tabela 80. Arquivos do Monitor NTP	
Arquivos de Monitor	**Nome e Local**
Monitor executável	`nco_m_ntp`
Arquivo de Propriedades	`$ISHOME/etc/props/ntp.props`

Tabela 80. Arquivos do Monitor NTP (continuação)	
Arquivos de Monitor	**Nome e Local**
Arquivo de regras	`$ISHOME/etc/ntp.rules`
Arquivo de log	`$ISHOME/log/ntp.log`

Diretrizes para configurar o monitor NTP

O monitor NTP adquire dados enviando uma consulta para um servidor NTP, que retorna um pacote de respostas UDP com o tempo atual (como visto pelo servidor NTP).

A imagem a seguir mostra um exemplo das mensagens que são trocadas entre o monitor e o servidor NTP.



Configurando testes de serviço do monitor NTP

Utilize os parâmetros de configuração do monitor NTP para definir testes de serviço.

A tabela a seguir descreve as configurações de NTP:

Tabela 81. Configuração do NTP	
Campo	**Descrição**
servidor	O nome do host do servidor NTP. Por exemplo, `ntp.mycompany.com`.
description	Um campo de texto para fornecer informações descritivas sobre o elemento. Por exemplo, `NTP monitor`.
port	A porta no servidor NTP que será usada. Padrão: `123`
IP local	Especifica o endereço IP da interface de rede no sistema host ao qual o monitor é vinculado ao executar o teste. Se a propriedade `IpAddress` do monitor estiver configurada, ela substituirá o valor deste campo. Por exemplo, `102.168.n.n`.
versão	A versão do servidor NTP a ser utilizada (1, 2, 3 ou 4). Padrão: `1`
timeout	O tempo, em segundos, para aguardar para que o servidor responda. Padrão: `10`
tentar novamente	O número de vezes que o monitor tenta contatar o servidor NTP novamente. Padrão: `0`

Tabela 81. Configuração do NTP (continuação)	
Campo	**Descrição**
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: `300`
failureretests	O número de vezes para retestagem antes de a falha ser indicada. Padrão: `0`
retestinterval	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: `10`

Classificação de nível de serviço

As classificações de nível de serviço definem as regras para determinar o nível de serviço que é fornecido sobre o NTP.

As opções de classificação em nível de serviço disponíveis para o monitor NTP são:

```
totalTime
responseTime
lookupTime
Deslocamento
adjustedOffset
Mensagem
```

Nas classificações em nível de serviço:

- Especifique mais classificações de nível de serviço inserindo manualmente o nome do elemento de monitor. O nome deve corresponder ao nome mostrado para o elemento na seção Elementos do Monitor.
- `message` pode ser qualquer mensagem encaminhada no elemento `$message` para o servidor IBM Application Performance Management se usado em qualquer widget. Para obter uma lista de valores possíveis, consulte Mensagens de status.
- O operando é uma cadeia ou um número positivo.

Elementos do Monitor

Além dos resultados de teste comuns a todos os elementos, o monitor NTP gera um conjunto de resultados de teste que contém dados específicos para testes de serviço NTP.

A tabela a seguir descreve os elementos adicionais para o monitor NTP.

Tabela 82. Elementos do Monitor NTP	
Elemento	**Descrição**
`$adjustedOffset`	O deslocamento de tempo do servidor em segundos.
`$localIP`	O endereço IP local com o qual o monitor está configurado para utilizar. Ele pode ficar em branco em sistemas com somente uma interface.
`$lookupTime*` (`LookupTime`)	O tempo utilizado para obter o endereço IP do servidor host.
`$ntpVersionIn`	A versão de protocolo utilizada na resposta do servidor.

Tabela 82. Elementos do Monitor NTP (continuação)	
Elemento	**Descrição**
`$ntpVersionOut`	A versão de protocolo usada para envio.
`$offset`	A diferença de horário entre o servidor NTP e o sistema que executa o monitor em segundos.
`$port*` (`Porta`)	A porta a ser utilizada no servidor NTP.
`$responseTime*` (`ResponseTime`)	O tempo entre a conexão do monitor ao NTP e o recebimento de uma resposta.
`$retries`	O número de vezes de tentativas de envio de um pedido se nenhum ID de resposta for recebido.

Mensagens de Status

O monitor NTP fornece mensagens de status no atributo `ResultMessage` ao usar IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

A tabela a seguir descreve as mensagens de status NTP.

Tabela 83. Mensagens de Status do Monitor NTP	
Mensagem	**Descrição**
`Consulta bem-sucedida`	O servidor NTP forneceu a resposta esperada.
`Conexão com falha`	Não é possível inicializar um soquete UDP.
`Falha ao enviar pedido para o servidor NTP`	Não é possível gravar no soquete UDP.
`Nenhuma resposta do servidor`	O servidor NTP não respondeu.

Monitor NNTP

O monitor NNTP testa a disponibilidade de um serviço NNTP lendo e postando em um grupo de notícias.

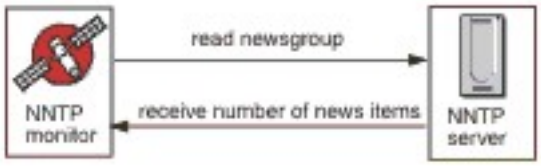
A tabela a seguir lista os arquivos do monitor NNTP.

Tabela 84. Arquivos do Monitor NNTP	
Arquivos do Monitor	**Nome ou local**
Monitor executável	`nco_m_nntp`
Arquivo de Propriedades	`$ISHOME/etc/props/nntp.props`
Arquivo de regras	`$ISHOME/etc/rules/nntp.rules`
Arquivo de log	`$ISHOME/log/nntp.log`

Recomendações para Configuração do Monitor NNTP

O monitor NNTP testa os serviços NNTP postando e lendo a partir de um servidor NNTP. Cada elemento de perfil criado para o monitor executa uma operação de leitura ou postagem.

Em uma operação de leitura, o monitor se conecta ao serviço NNTP para verificar se um determinado grupo de notícias de Internet existe. Se o grupo de notícias existir, o monitor grava o número de novos itens nele. Ele também tenta registrar o último item de notícias incluído no grupo de notícias. A imagem a seguir mostra a operação de leitura.



Em uma operação de postagem, o monitor verifica se o grupo de notícias existe e tenta gravar uma mensagem de teste nele. O assunto da mensagem de teste é `Mensagem de Teste do Monitor NNTP`. A imagem a seguir mostra a pós-operação.

Cada elemento de perfil especifica um `username` e `password` fornecido pelo monitor ao acessar um servidor NNTP. O monitor usa o sistema de autenticação de texto sem formatação.

```
AUTHINFO USER username
AUTHINFO PASS password
```

Em que `username` e `password` são especificados no elemento de perfil do monitor.

Propriedades

As opções de propriedades específicas para o monitor NNTP são descritas na tabela a seguir.

Tabela 85. Opções de propriedades do monitor NNTP

Nome da propriedade	Parâmetro de propriedade	Descrição
OutputDirectory	string	Especifica o diretório de saída a ser utilizado se **`OutputResult`** for true (configurado como 1). Padrão: `$ISHOME/var`
OutputResult	0|1	Especifica que o monitor pode salvar os dados que recebe do serviço. 0 - desativado 1 - ativado

Configurando testes de serviço de monitor NNTP

Utilize os parâmetros de configuração do monitor NNTP para definir testes de serviço.

A tabela a seguir lista as configurações do monitor NNTP.

Tabela 86. Configuração do Monitor NNTP	
Campo	**Descrição**
servidor	O endereço IP do servidor NNTP. Por exemplo, `news.mycompany.com`.
newsgroup	O nome do grupo de notícias que o monitor usa para postar e ler mensagens de teste. Por exemplo, `mycompany.test`.
description	Um campo de texto para fornecer informações descritivas sobre o elemento. Por exemplo, READ.
port	O número da porta do servidor NNTP. Padrão: 119
nome do usuário	O nome de usuário utilizado para autenticar-se no servidor NNTP.
senha	A senha do nome de usuário usada para autenticação com o servidor NNTP.
ação	Indica se um artigo deve ser postado ou recuperado. Pode ser READ ou POST. Padrão: POST
timeout	O tempo, em segundos, para aguardar para que o servidor responda. Padrão: 30
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: 300
failureretests	O número de vezes para retestagem antes de a falha ser indicada. Padrão: 0
retestinterval	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: 10

Expressão regular correspondente

É possível executar uma procura de expressão regular nas informações sendo transferidas por download inserindo até 50 expressões regulares diferentes. O monitor NNTP tenta fazer a correspondência dos conteúdos recuperados para cada expressão regular.

Se uma correspondência para uma expressão comum especificada for encontrada, as linhas correspondentes (ou o máximo que couber no buffer interno do monitor) serão retornadas no elemento `$regexpMatchn` correspondente. Se a expressão comum corresponder mais de uma vez nas informações transferidas por download, apenas a primeira será retornada. O status de cada teste de expressão regular é indicado pelos elementos `$regexpStatusn`. Você pode utilizar as correspondências de expressões comuns e suas informações de status como critérios para as classificações em nível de serviço.

Para obter mais informações, consulte Tabela 50 na página 325.

Classificações em Nível de Serviço

As classificações de nível de serviço definem as regras para determinar o nível de serviço que é fornecido sobre o NNTP.

As opções de classificação em nível de serviço disponíveis para o monitor NNTP são:

```
totalTime
lookupTime
connectTime
transferTime
responseTime
status
bytesTransferred
bytesPerSec
newsItems
esperado
lastLineReceived
checksum
previousChecksum
regexpMatch1 a 3
regexpStatus1 a 3
Mensagem
```

Nas classificações em nível de serviço:

- Especifique mais classificações de nível de serviço inserindo manualmente o nome do elemento de monitor. O nome deve corresponder ao nome mostrado para o elemento na seção Elementos do Monitor.
- `message` pode ser qualquer mensagem encaminhada no elemento `$message` para o servidor IBM Application Performance Management se usada em um widget. Para obter uma lista de valores possíveis, consulte Mensagens de status.
- O operando é uma cadeia ou um número positivo.
- Os códigos de `status` 220 e 240 indicam êxito. Consulte o protocolo NNTP para obter outros códigos de status retornados pela operação.
- `egexpStatus`*n* pode ter os seguintes valores:
  - `NONE`: Não há nenhuma verificação de expressão comum configurada
  - `MATCHED`: Foi localizada uma correspondência para a expressão comum
  - `FAILED`: Não foi localizada uma correspondência para a expressão comum
- Avalie as correspondências de expressão regular que usam expressões de teste no formato:

  ```
  regexpMatchn [contains|!contains] expressão
  ```

  Use os operadores `contains` e `!contains` no lugar de = e `!=`, pois normalmente o `regexpMatch`*n* contém a linha inteira que corresponde à expressão regular em vez de apenas a parte correspondente, assim, os operadores = e `!=` geralmente não correspondem à expressão.
- Normalmente, os elementos `Checksum` e `PreviousChecksum` não fornecem valores significativos para as classificações em nível de serviço porque seus valores totais de verificação não são conhecidos durante a criação do elemento do perfil (o monitor calcula os valores totais de verificação durante o progresso dos testes). Os elementos de monitor `$checksum` e `$previousChecksum` destinam-se ao enriquecimento de alerta usando o arquivo de regras do monitor.

Elementos do Monitor

Além dos resultados de teste comuns a todos os elementos, o monitor NNTP gera um conjunto de resultados de teste que contém dados específicos para testes de serviço NNTP.

A tabela a seguir descreve os elementos adicionais para o monitor NNTP.

Tabela 87. Elementos do monitor NNTP

Elemento	Descrição
`$action*` (`NntpAction`)	A ação utilizada pelo monitor. Pode ser READ ou POST.

Tabela 87. Elementos do monitor NNTP (continuação)	
Elemento	**Descrição**
$bytesPerSec	O número médio de bytes transferidos por segundo.
$bytesTransferred	O número de bytes transferidos por upload ou download.
$checksum	Normalmente, o elemento Checksum não fornece valores significativos para as classificações em nível de serviço porque seus valores totais de verificação não são conhecidos durante a criação do elemento do perfil (o monitor calcula os valores totais de verificação durante o progresso dos testes). Os elementos de monitor $checksum e $previousChecksum destinam-se ao enriquecimento de alerta usando o arquivo de regras do monitor.
$connectTime* (ConnectTime)	O tempo utilizado para estabelecer uma conexão com o servidor NNTP.
$downloadTime	O tempo utilizado para fazer download do arquivo.
$group* (NntpGroup)	O nome do grupo de notícias monitorado.
$lastLineReceived	Esse elemento será configurado apenas se o elemento $message contiver a mensagem Falha na Espera. Se configurado, ele conterá a resposta do servidor NNTP.
$lookupTime* (LookupTime)	O tempo utilizado para consultar o endereço IP do servidor.
$newsItems	O número de novos itens no grupo de notícias.
$password	A senha utilizada para autenticar o monitor.
$previousChecksum	Normalmente, o elemento PreviousChecksum não fornece valores significativos para as classificações em nível de serviço porque seus valores totais de verificação não são conhecidos durante a criação do elemento do perfil (o monitor calcula os valores totais de verificação durante o progresso dos testes). Os elementos de monitor $previousChecksum e $checksum destinam-se ao enriquecimento de alerta usando o arquivo de regras do monitor.

Tabela 87. Elementos do monitor NNTP (continuação)	
Elemento	**Descrição**
`$responseTime*` (`ResponseTime`)	O tempo utilizado, após a criação de uma conexão, até o recebimento do primeiro byte do artigo de destino.
`$status`	O código de status retornado pelo servidor NNTP.
`$transferTime*` (`TransferTime`)	Configura o valor como `$uploadTime` ou `$downloadTime`.
`$uploadTime`	O tempo utilizado para fazer upload do arquivo.
`$username`	O nome de usuário utilizado para autenticar o monitor.
Se `$message` contiver `$ExpectFailed`	
`$expected`	O texto que o monitor estava esperando na conexão, quando esta falhou.
`$lastLineReceived`	A última linha de texto na conexão que o monitor recebeu do servidor NNTP.

Mensagens de Status

O monitor NNTP fornece mensagens de status no atributo `ResultMessage` ao usar IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

A tabela a seguir descreve as mensagens de status NNTP.

Tabela 88. Mensagens de Status do Monitor NNTP	
Mensagem	**Descrição**
`Artigo Postado`	A ação POST do NNTP foi bem-sucedida.
`Artigo Recuperado`	A ação READ do NNTP foi bem-sucedida.
`Não encontrado`	O artigo pode não ter sido localizado.
`Falha na espera`	O pedido de NNTP falhou.
`Tempo limite esgotado aguardando leitura`	Uma conexão de dados com o servidor foi estabelecida, mas parou de responder.
`Conexão com falha`	O monitor falhou ao se conectar ao servidor. Para obter informações adicionais, consulte o arquivo de log.
`Conexão fechada por host externo`	O host remoto encerrou a conexão antes do esperado pelo monitor.

Monitor POP3

O monitor POP3 funciona junto com o monitor SMTP para testar a disponibilidade e o tempo de resposta de um serviço de e-mail POP3.

A tabela a seguir lista os arquivos de monitor POP3.

Tabela 89. Arquivos do Monitor POP3	
Arquivos do Monitor	**Nome ou local**
Monitor executável	`nco_m_pop3`
Arquivo de Propriedades	`$ISHOME/etc/props/pop3.props`
Arquivo de regras	`$ISHOME/etc/rules/pop3.rules`
Arquivo de log	`$ISHOME/log/pop3.log`

Diretrizes para Configurar o Monitor POP3

O monitor POP3 opera junto com o monitor SMTP monitorando a caixa de correio para a qual o monitor SMTP envia mensagens de teste e medindo esse tempo gasto para entregar essas mensagens.

Nota: Assegure-se de que os relógios do sistema no computador host do monitor e no servidor de e-mail estejam sincronizados para que o cálculo de tempo de entrega funcione corretamente.

Quando o monitor POP3 lê o conteúdo da caixa postal, ele gera dois tipos diferentes de eventos:

- Eventos Específicos da Mensagem

  O monitor POP3 cria um evento específico de mensagem para cada mensagem de e-mail que ele transfere por downloads da caixa de correio. Neste tipo de evento, o monitor configura o elemento `$message` para `Mensagem Transferida por Download com Êxito`. O elemento `$timeToDeliver` é calculado como o tempo gasto até que a mensagem passe pelo monitor SMTP que a emitiu e a caixa postal que a recebeu. O elemento `$hopCount` indica o número de hosts da mensagem ignorados até chegar na caixa postal.
- Eventos de resumo

  O monitor cria um evento de resumo quando processa todas as mensagens na caixa postal. Neste tipo de evento, o elemento `$message` indica o número total de mensagens transferidas por download com êxito da caixa postal e o elemento `$totaltime` indica o tempo gasto para concluir os pedidos. O `$totaltime` está em segundos.

Correio Seguro

O monitor POP3 suporta conexões com serviços de correios seguros. Ele pode se conectar usando SSL/TLS, ou o comando STARTTLS. Ao definir um elemento de monitor POP3, use o campo Tipo de segurança para selecionar a segurança apropriada. Se o servidor de e-mail requer um certificado de lado do cliente para criptografia SSL, use a propriedade SSL`name` ou as opções de linha de comando para especificar um arquivo de certificado, um arquivo-chave, uma senha de chave e um conjunto de cifras.

Certificado do lado do cliente

O monitor POP3 possibilita o monitoramento de servidores que requerem certificados do lado do cliente para autenticação mútua. Especifique o arquivo de certificado SSL, o arquivo-chave e a senha de chave ao criar um elemento de perfil. Os certificados devem estar no formato Privacy Enhanced Mail (PEM). Se o seu certificado estiver em outro formato, você deverá convertê-lo para o formato PEM. Os certificados podem ser convertidos usando um software como o openSSL, que está disponível em http://www.openssl.org.

Nota: Se você sempre utilizar o mesmo certificado, chave e senha em todos os elementos do perfil, especifique-os utilizando as propriedades do monitor em vez de defini-las em cada elemento de perfil criado.

Configurando Testes do Monitor POP3

Nota: Monitore a operação do servidor de e-mail `mail.mycompany.com` configurando o monitor SMTP para enviar mensagens para uma caixa postal de teste e configurando o monitor POP3 para

recuperar as mensagens. A caixa postal de teste tem o endereço `ismtest@mycompany.com` e as credenciais `ismtest/secret1`. Use um tempo limite de conexão de 20 segundos, 2 novos testes com falha e um intervalo de novo teste de 5 segundos em cada extremidade e teste os serviços a cada dez minutos. Use as classificações em nível de serviço padrão fornecidas pelos elementos de perfil.

Tabela 90. Configuração do Monitor POP3

Campo	**Descrição**
servidor	O endereço IP do servidor de e-mail. O exemplo é `mail.mycompany.com`
description	Um campo de texto para fornecer informações descritivas sobre o elemento.
port	O número da porta do servidor de e-mail. Padrão: `110`
securitytype	O tipo de conexão segura aberta com o servidor de e-mail: • `NONE` -Conectar-se sem segurança • `SSL` - Enviar um SSLv2 `hello` e, em seguida, negociar SSLv2, SSLv3 ou TLSv1 • `STARTTLS` - Conectar sem segurança, emitir um comando STLS e, em seguida, estabelecer uma conexão no TLSv1. Esse é o tipo de segurança mais seguro. • `NONE` -Conectar-se sem segurança Padrão: `NONE`
nome do usuário	O nome da caixa de correio.
senha	A senha utilizada para efetuar login na caixa postal, se necessário.
Tipo de autenticação	O método de autenticação a ser usado e o rótulo é Tipo de autenticação: • `STANDARD` - Usa uma troca de usuário/transmissão em que a senha não está criptografada. Isso é apropriado para uso intermitente de POP3. • `APOP` - Usa o local onde o cliente POP3 se conecta ao servidor regularmente. Isso oferece um nível maior de segurança do que o padrão. Assegure-se de especificar um APOP Shared Secret se selecionar APOP. Observe que nem todos os servidores suportam APOP. Padrão: `STANDARD`.
Segredo compartilhado	O segredo compartilhado para autenticação APOP, aplicável somente se você estiver usando o tipo de autenticação APOP. A cadeia deve ter no mínimo oito caracteres e estar oculta na interface com o usuário.
timeout	O tempo, em segundos, para aguardar para que o servidor responda. Padrão: `30`
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: `300`

Tabela 90. Configuração do Monitor POP3 (continuação)	
Campo	**Descrição**
failureretests	O número de vezes para testar novamente antes de indicar uma falha. Padrão: `0`
retestinterval	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: `10`
verifycertificate	O certificado de verificação do servidor. Padrão: `Desativado`

Utilize os parâmetros de configuração do monitor POP3 para definir testes de serviço.

Correspondência de Expressões Comuns

Você pode desempenhar uma procura de expressão comum nas informações transferidas por download digitando até 50 expressões comuns diferentes. O monitor tenta corresponder o conteúdo recuperado a cada uma das expressões comuns.

Se uma correspondência para uma expressão comum especificada for encontrada, as linhas correspondentes (ou o máximo que couber no buffer interno do monitor) serão retornadas no elemento `$regexpMatchn` correspondente. Se a expressão comum corresponder mais de uma vez nas informações transferidas por download, apenas a primeira será retornada. O status de cada teste de expressão regular é indicado pelos elementos `$regexpStatusn`. Você pode utilizar as correspondências de expressões comuns e suas informações de status como critérios para as classificações em nível de serviço.

Para obter informações sobre a sintaxe das expressões comuns, consulte o Tabela 50 na página 325.

Elementos do Monitor

Além dos resultados de teste comuns a todos os elementos, o monitor POP3 gera um conjunto de resultados de teste contendo dados específicos para testes de serviço do POP3.

A Tabela 1 descreve os elementos adicionais para o monitor POP3.

Elementos indicados por um asterisco (*) estão disponíveis como atributos. Os nomes dos atributos são mostrados entre colchetes. A ausência de um asterisco indica que não há nenhum atributo equivalente. Os atributos mostrados no colchete, mas sem um elemento, indicam que eles só estão disponíveis como atributos, não há elemento equivalente.

Tabela 91. Elementos do Monitor IMAP4	
Elemento	**Descrição**
`$authentication`	O tipo de método de autenticação de usuário exigido pelo servidor IMAP4 (Padrão ou CRAM-MD5).
`$bytesPerSec`	O número médio de bytes transferidos por segundo.
`$bytesTransferred`	O número de bytes transferidos por upload ou download.
`$connectTime`	O tempo utilizado para conectar-se ao servidor IMAP4.
$downloadTime * (`DownloadTime`)	O tempo utilizado para fazer download do arquivo.
`$hopCount`	O número de hosts que a mensagem saltou para chegar à caixa postal.

Tabela 91. Elementos do Monitor IMAP4 (continuação)	
Elemento	**Descrição**
$inEvent	Indica que esse evento faz parte de vários eventos. 1 indica que não é o evento final, 0 indica que é o evento final.
$lookupTime*(LookupTime)	O tempo utilizado para obter o endereço IP do servidor host.
$port*(Port)	A porta na qual o serviço é monitorado.
$responseTime* (ResponseTime)	O tempo entre quando a conexão é estabelecida e o primeiro byte de dados é recebido.
$security	O tipo de conexão segura aberta com o servidor de e-mail especificado ao incluir um elemento IMAP (NONE, STARTTLS ou SSL).
$sentTo*(SentTo)	O endereço de e-mail usado pelo monitor SMTP para enviar a mensagem original.
$smtpServer	O nome do servidor SMTP a partir do qual o e-mail foi enviado.
$SSLHandshakeTime* (SslHandshakeTime)	O tempo utilizado para estabelecer a conexão SSL.
$timeToDeliver	O tempo que uma mensagem de e-mail leva entre um monitor SMTP e sua caixa de correio de destino.
$user*(ImapUser)	O nome de usuário (nome da conta) usado pelo monitor para efetuar login no servidor IMAP4.

Mensagem de status

O monitor POP3 fornece mensagens de status no atributo ResultMessage ao usar o IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

A tabela a seguir descreve as mensagens de status POP3.

Tabela 92. Mensagens de Status do Monitor POP3	
Mensagem	**Descrição**
Message successfully downloaded	A solicitação POP3 foi bem-sucedida.
Downloaded x messages	Indica quantas mensagens foram transferidas por download da caixa postal.
Tempo limite esgotado ao aguardar leitura/gravação	Uma conexão de dados foi estabelecida com o servidor, mas ele parou de responder.
Conexão fechada por host externo	O host remoto fechou a conexão antes que o monitor esperasse.
Conexão com falha	O monitor falhou ao se conectar ao servidor. Consulte o arquivo de log para obter mais informações.
APOP não suportado pelo servidor	O método de autenticação APOP não é suportado pelo servidor. Em vez disso, use o tipo de autenticação Padrão.
Serviço APOP não disponível	A implementação do servidor APOP não é suportada pelo monitor. Em vez disso, use o tipo de autenticação Padrão.

Tabela 92. Mensagens de Status do Monitor POP3 (continuação)	
Mensagem	**Descrição**
`O servidor não suporta o recurso STLS`	O servidor não suporta STARTTLS. Utilize um tipo de segurança diferente.

Propriedades

As propriedades específicas para o monitor POP3 são descritas na tabela a seguir.

Tabela 93. Propriedades do Monitor POP3 e Opções da Linha de Comandos		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
`SSLCertificate File`	string	O caminho e o nome do arquivo de certificado digital utilizados se nenhum certificado for especificado explicitamente para um elemento POP3 durante sua criação. Se o caminho não for absoluto, o monitor interpretará isso em relação ao diretório ativo (`$ISHOME/platform/`*`arch`*`/bin`).
`SSLCipherSuite`	string	O conjunto de criptografia a ser utilizado para operações SSL. Padrão: `RC4:3DES:DES:+EXP`. Consulte Conjuntos de cifras para obter uma descrição dos valores possíveis.
`SSLDisableTLS`	integer	Desativa o TLSv1 para o suporte legado. Padrão: `0` -TLSv1 está ativado. Configurar como `1` para desativar o TLSv1.
`SSLKeyFile`	string	O arquivo que contém a chave privada SSL.
`SSLKeyPassword`	string	A senha utilizada para criptografar a chave privada SSL.

Conjuntos de Criptografia

A propriedade `SSLCipherSuite` especifica o conjunto de criptografia utilizado pelo monitor POP3. Para obter mais informações sobre as configurações de SSL, consulte “Configuração de SSL no Internet Service Monitoring” na página 436.

Monitor RADIUS

O Remote Authentication Dial-In User Service (RADIUS) fornece autenticação para acesso remoto a serviços. O monitor RADIUS simula um sistema do cliente que acessa um serviço RADIUS e retorna dados sobre o desempenho do serviço.

A tabela a seguir lista os arquivos do monitor RADIUS.

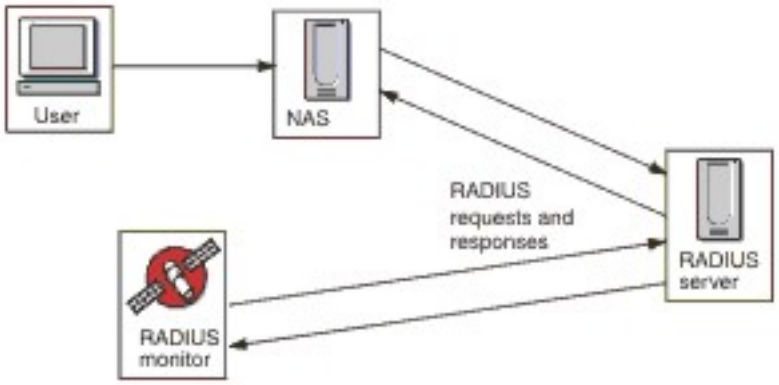
Tabela 94. Arquivos do Monitor RADIUS	
Monitorar Arquivos	**Nome e Local**
Monitor executável	`nco_m_radius`
Arquivo de Propriedades	`$ISHOME/etc/props/radius.props`

Tabela 94. Arquivos do Monitor RADIUS (continuação)	
Monitorar Arquivos	**Nome e Local**
Arquivo de regras	`$ISHOME/etc/rules/radius.rules`
Arquivo de log	`$ISHOME/log/http.log`

Diretrizes para a configuração do monitor Radius

O monitor RADIUS simula a operação de um NAS (Network Access Server), enviando pedidos a um servidor RADIUS.

O monitor RADIUS utiliza UDP para enviar solicitações para o servidor RADIUS e gera eventos que contêm os resultados dessas solicitações e dados sobre o desempenho do servidor. A imagem a seguir mostra a operação do monitor.



O monitor pode testar as operações de autenticação e contabilidade dos servidores RADIUS:

- Access-Request usando Password Authentication Procedure (PAP)
- Access-Request usando Challenge-Handshake Authentication Protocol (CHAP)
- Pedidos-Contabilidade: Início, Parada, Contabilidade Ativada, Contabilidade Desativada

Propriedades

As opções de propriedades específicas para o monitor RADIUS estão descritas na seguinte tabela.

Tabela 95. Opções de propriedades do monitor RADIUS		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
`FramedServiceRequest`	`0|1`	Quando essa propriedade é configurada como 1, o monitor seleciona o tipo de serviço Em quadro configurado nos Pedidos de Acesso. `0` - desativado 1 - ativado

Configurando testes de serviço do monitor Radius

Utilize os parâmetros de configuração do monitor RADIUS para definir testes de serviço.

A tabela a seguir descreve as configurações do monitor Radius:

Tabela 96. Configuração do Monitor RADIUS	
Campo	**Descrição**
servidor	O endereço IP do servidor RADIUS.
Segredo compartilhado	O segredo compartilhado usado para autenticar o monitor.
nome do usuário	O nome do usuário fornecido pelo monitor para autenticar o servidor RADIUS.
senha	A senha fornecida pelo monitor para autenticar o servidor RADIUS.
description	Um campo de texto para fornecer informações descritivas sobre o elemento.
requesttype	Especifica o tipo de pedido enviado para o servidor RADIUS: • `Authenticate (CHAP)` • `Authenticate (PAP)` • `Accounting` Padrão: `Authenticate(CHAP)`
port	A porta para usar para a conexão com o servidor RADIUS. Padrão: 1812
IP local	Especifica o endereço IP da interface de rede no sistema host ao qual o monitor é vinculado ao executar o teste. Se a propriedade `IpAddress` do monitor estiver configurada, ela substituirá o valor desse campo.
loginhost	Configura o valor do atributo `Login-IP-Host` no Pedido de Acesso.
calledstation	Configura o valor do atributo `Called-Station-Id` no Pedido de Acesso.
callingstation	Configura o valor do atributo `Calling-Station-Id` no Pedido de Acesso.
accountsessionid	Configura o valor do atributo `Acct-Session-Id` em pacotes de Pedido de Contabilidade enviados ao servidor de contabilidade. **Nota:** Esse campo aplica-se apenas ao tipo de pedido `Accounting`.
accountstatustype	Configura o valor do atributo `Acct-Status-Type` em pacotes de Pedido de Contabilidade enviados ao servidor de contabilidade: • `Iniciar` • `Stop` • `Accounting On` • `Accounting Off` **Nota:** Esse campo aplica-se apenas ao tipo de pedido `Accounting`. Padrão: `Start`

Tabela 96. Configuração do Monitor RADIUS (continuação)	
Campo	**Descrição**
accountsessiontime	Configura o valor do atributo `Acct-Session-Time` (em segundos) em pacotes de pedido de contabilidade enviados ao servidor de contabilidade. **Nota:** Esse campo aplica-se apenas ao tipo de pedido `Accounting`.
nasip	O atributo `NAS-IP-Address` enviado pelo monitor RADIUS como parte de um pacote Access-Request.
nasport	O atributo `NAS-Port` enviado pelo monitor RADIUS como parte de um pacote Access-Request.
timeout	O tempo, em segundos, para aguardar para que o servidor responda. Padrão: `10`
tentar novamente	O número de vezes de novas tentativas de conexão com o servidor RADIUS se houver algum problema. Padrão: `0`
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: `300`
failureretests	O número de vezes para retestagem antes de a falha ser indicada. Padrão: `0`
retestinterval	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: `10`

Classificação de nível de serviço

As classificações de nível de serviço definem as regras para determinar o nível de serviço fornecido pelo serviço RADIUS.

As opções de classificação em nível de serviço disponíveis para o monitor RADIUS são:

```
totalTime
lookupTime
responseTime
Mensagem
```

Nas classificações em nível de serviço:

- Especifique mais classificações de nível de serviço inserindo manualmente o nome do elemento de monitor. O nome deve corresponder ao nome mostrado para o elemento na seção Elementos do Monitor.
- `message` pode ser qualquer mensagem encaminhada no elemento `$message` para o servidor IBM Application Performance Management se usado em qualquer widget. Para obter uma lista de valores possíveis, consulte Mensagens de status.
- O operando é uma cadeia ou um número positivo.

Elementos do Monitor

Além dos resultados de teste comuns a todos os elementos, o monitor RADIUS gera um conjunto de resultados de teste contendo dados específicos para os testes de serviço RADIUS.

A tabela a seguir descreve os elementos adicionais para o monitor RADIUS.

Tabela 97. Elementos do Monitor RADIUS

Elemento	**Descrição**
`$accountSessionId`	Identificador exclusivo utilizado para corresponder registros de início e parada.
`$accountSessionTime`	Quando `accountStatusType` é configurado para `Stop`, este campo mostra a quantidade de tempo que o usuário recebe o serviço, em segundos.
`$accountStatusType`	Indica se este é o início do serviço do usuário (`start`) ou o fim (`stop`).
`$calledStationId`	O monitor RADIUS envia calledStationId como parte de um pacote Access-Request. Ele será usado se o servidor RADIUS exigir e não será usado se `callingStationId` for usado.
`$callingStationId`	O monitor RADIUS envia `callingStationId` como parte de um pacote Access-Request. Ele será usado se o servidor RADIUS exigir e não será usado se `calledStationId` for usado.
`$localIP`	O endereço IP local com o qual o monitor está configurado para utilizar. Ele pode ficar em branco em sistemas com somente uma interface.
`$loginIPHost*` (`LoginIpHost`)	O monitor RADIUS envia loginIPHost como parte de um pacote Access-Request. Ele pode ser requerido por servidores sendo monitorados.
`$lookupTime*` (`LookupTime`)	O tempo utilizado para obter o endereço IP do servidor host.
`$nasPort*` (`NasPort`)	O parâmetro `NAS Port` enviado pelo monitor RADIUS como parte de um pacote Access-Request. Padrão: `0`.
`$password`	A senha utilizada para autenticar o monitor.
`$port*` (`Porta`)	A porta na qual o serviço é monitorado.
`$requestType`	Indica o tipo de solicitação selecionado para o elemento, `PAP`, `CHAP` ou `Accounting`.
`$responseTime`	O tempo levado entre o envio de uma solicitação para o servidor RADIUS e o recebimento de uma resposta.
`$retries`	O número máximo de novas tentativas.

Tabela 97. Elementos do Monitor RADIUS (continuação)	
Elemento	**Descrição**
`$secret`	A senha de segredo compartilhado retirada do arquivo de configuração.
`$username*` (`RadiusUser`)	O nome de usuário utilizado para autenticar o monitor.

Mensagens de Status

O monitor RADIUS fornece mensagens de status no atributo `ResultMessage` durante o uso do IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

A tabela a seguir descreve as mensagens de status do monitor RADIUS

Tabela 98. Mensagens de Status do Monitor RADIUS	
Mensagem	**Descrição**
`Autenticação CHAP - Acesso concedido`	O monitor foi autenticado (utilizando CHAP). Será retornado somente se o tipo de solicitação CHAP foi usado.
`Autenticação PAP - Acesso concedido`	O monitor foi autenticado (utilizando PAP). Será retornado somente se o tipo de solicitação PAP foi usado.
`Resposta de contabilidade recebida`	Uma resposta de contabilidade foi recebida do servidor. A transação continua.
`Conexão com falha`	O nome do servidor especificado é inválido.
`Falha ao enviar pedido para o servidor RADIUS`	Pode não gravar o pacote UDP na rede. Não há mais informações de erro disponíveis.
`Nenhuma resposta do servidor`	O servidor RADIUS não está respondendo.
`Identificador incorreto retornado`	Houve uma resposta do servidor a um pedido que não foi enviada do monitor.
`Autenticador de resposta inválido`	A resposta continha uma autorização que não era esperada. Isso pode ter sido causado por uma senha ou segredo compartilhados incorretos.
`Resposta não reconhecida`	O servidor não reconheceu o pacote enviado.
`Autenticação PAP - Acesso negado`	O monitor não foi autenticado (utilizando PAP).
`Autenticação CHAP - Acesso negado`	O monitor não foi autenticado (utilizando CHAP).

Monitor RPING

O monitor RPING testa a disponibilidade de dispositivos de rede efetuando ping remotamente de um roteador. Ele fornece os dados de desempenho dos tempos de roundtrip mínimo, médio e máximo.

O monitor suporta roteadores Cisco, Juniper e roteadores compatíveis com RFC2925.

A tabela a seguir lista os arquivos do monitor RPING.

Tabela 99. Arquivos do Monitor RPING

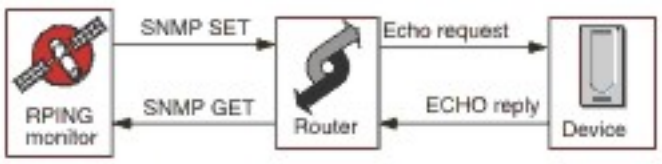
Arquivos do Monitor	**Nome ou local**
Monitor executável	`nco_m_rping`
Arquivo de Propriedades	`$ISHOME/etc/ims/props/rping.props`
Arquivo de regras	`$ISHOME/etc/ims/rules/rping.rules`
Arquivo de log	`$ISHOME/log/rping.log`
Arquivos de Script	`$ISHOME/scripts/rping/cisco.s` (script SNMP para roteadores Cisco) `$ISHOME/scripts/rping/juniper.s` (script SNMP para roteadores Juniper) `$ISHOME/scripts/rping/rfc2925.s` (script SNMP para roteadores compatíveis com RFC2925)

Diretrizes para configurar o monitor RPING

O monitor RPING adquire dados configurando o roteador para efetuar ping de um dispositivo de rede, sondando periodicamente o roteador para obter os resultados dos pings.

O monitor configura os testes de ping usando um comando SNMP SET para criar uma linha de controle no MIB do ping do roteador e, em seguida, recupera os dados de ping do MIB usando comandos SNMP GET. Toda a comunicação com o roteador é pelo SNMP.

A imagem a seguir mostra um exemplo das mensagens que são trocadas entre o monitor e o dispositivo de rede.



Ativando Pedido Ping Remoto em Roteadores Cisco

Por padrão, os pedidos SNMP de ping remoto em roteadores Cisco estão desativados. No entanto, para que o monitor RPING faça um pedido SNMP SET e inicie o ping, esse pedido deve estar ativado.

Para ativar o pedido, efetue login no roteador Cisco e digite os seguintes comandos:

```
ativando
config terminal
snmp-server community communitystring rw
write mem
Efetue logout
```

A sequência de comunidades configurada no roteador deve corresponder à inserida no campo Sequência de Comunidades R/W de qualquer elemento de perfil RPING criado para esse roteador. A linha write mem garante que as configurações sejam salvas quando o roteador for reiniciado.

Ativando o Pedido de Ping Remoto em Roteadores Juniper

Por padrão, solicitações SNMP de ping remotas em roteadores Juniper ficam desativadas. Para o monitor RPING operar usando um roteador Juniper, deve-se ativar solicitações SNMP.

Para ativar uma solicitação SNMP no roteador, assegure-se de que a seção SNMP da configuração do JUNOS seja correspondente:

```
[edit snmp]
view ping-mib-view {
  oid .1.3.6.1.2.1.80 include; # pingMIB
  oid jnxPingMIB include; # jnxPingMIB
}
community communitystring {
  authorization read-write;
  view ping-mib-view;
}
```

A sequência de comunidades configurada no roteador deve corresponder à sequência inserida no campo de sequência de comunidades de quaisquer elementos de perfil RPING configurados para esse roteador.

Propriedades

As opções de propriedades específicas para o monitor RPING são descritas na tabela a seguir.

Tabela 100. Opções de propriedades de RPING

Nome da propriedade	Parâmetro de propriedade	Descrição
MibDir	sequência	O diretório contendo os arquivos MIB usados pelo monitor. Padrão: `$ISHOME/mibs`.

Configurando Testes de Serviço do Monitor RPING

Utilize os parâmetros de configuração do monitor RPING para definir testes de serviço.

Tabela 101. Configuração do Monitor RPING

Campo	Descrição
servidor	O nome ou o endereço IP do roteador. Por exemplo, `rt1.mycompany.com`.
routertype	O tipo de roteador: • CISCO • Juniper • RFC2925
host	O nome ou endereço IP do servidor no qual você deseja que o roteador faça ping.
sequência de comunidades	Especifica a sequência de comunidades SNMP usada para comunicação com o roteador. Por exemplo, `server1.mycompany.com`.
description	Um campo de texto para fornecer informações descritivas sobre o elemento. Por exemplo, `RPING monitor`.
vpn	O nome opcional de um VPN para usar para o envio de pings. O roteador usa o VPN especificado em vez do roteamento padrão configurado.

Tabela 101. Configuração do Monitor RPING (continuação)	
Campo	**Descrição**
versão	A versão SNMP a ser usada: 1 - SNMPv1 2 - SNMPv2c 3 - SNMPv3 Padrão: 2
numberofpings	O número de pings a ser enviado. Padrão: 5
packetsize	O tamanho dos pacotes que serão enviados, em bytes. Padrão: 64
packettimeout	O tempo de espera entre os pings em segundos. Padrão: 500
securityname†	O nome do usuário para a sessão SNMP.
authenticationphrase†	A senha de autenticação para o usuário.
privacyphrase†	A senha de privacidade para o usuário.
authenticationprotocol†	O protocolo a ser usado para autenticar o usuário: • MD5 • SHA1 Padrão: MD5
privacyprotocol†	O protocolo a ser utilizado para criptografar a sessão. Padrão: DES
timeout	O tempo, em segundos, entre cada sondagem. Padrão: 10
tentar novamente	O número de vezes que o monitor tenta entrar em contato com o servidor. Padrão: 3
Pesquisar	O tempo de espera entre os pings em segundos. Padrão: 300
failureretests	O número de vezes para retestagem antes de a falha ser indicada. Padrão: 0
retestinterval	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: 10

Tabela 101. Configuração do Monitor RPING (continuação)	
Campo	**Descrição**
† Aplicável apenas ao SNMPv3.	

Classificação de nível de serviço

As classificações de nível de serviço definem as regras para determinar o nível de serviço que é fornecido sobre o RPING.

As opções de classificação em nível de serviço disponíveis para o monitor RPING são:

```
totalTime
lookupTime
numPacketSent
numPacketsRecv
maxRTT
minRTT
averageRTT
respondPercent
Mensagem
```

Nas classificações em nível de serviço:

- Especifique mais classificações de nível de serviço inserindo manualmente o nome do elemento de monitor. O nome deve corresponder ao nome mostrado para o elemento na seção Elementos do Monitor.
- `message` pode ser qualquer mensagem encaminhada no elemento **`$message`** para o servidor IBM Application Performance Management se usado em qualquer widget. Para obter uma lista de valores possíveis, consulte Mensagens de status.
- O operando é uma cadeia ou um número positivo.

Elementos do Monitor

Além dos resultados de teste comuns a todos os elementos, o monitor RPING gera um conjunto de resultados de teste que contêm dados específicos para testes de serviço RPING.

A tabela a seguir lista os elementos adicionais para o monitor RPING.

Tabela 102. Elementos do Monitor RPING	
Elemento	**Descrição**
$authProto	O protocolo de autenticação especificado durante a criação do elemento.
(AverageRTT)	O tempo médio de roundtrip em segundos.
$community	A sequência da comunidade SNMP para o roteador.
$communityString	A sequência de comunidades SNMP usada para comunicação com o roteador.
(MaxRTT)	O tempo máximo de roundtrip em segundos.
(MinRTT)	O tempo mínimo de roundtrip em segundos.
$numPacketSent	O número de pacotes enviados pelo monitor.
$numPings	O número de pings enviados, conforme especificado durante a inclusão do elemento RPING.
$packetSize	O tamanho dos pacotes a serem enviados.

Tabela 102. Elementos do Monitor RPING (continuação)	
Elemento	**Descrição**
$packetTimeout	O tempo de espera entre o envio dos pacotes.
$privProto	O protocolo de privacidade especificado durante a criação do elemento.
$remoteHost* (RemoteHost)	O nome ou endereço IP do servidor no qual você deseja que o roteador faça ping.
(RespondPercent)	A porcentagem de pings enviados para os quais houve uma resposta.
$routerMan* (RouterName)	O tipo de roteador selecionado durante a inclusão do elemento RPING: • CISCO • Juniper • RFC2925
$securityName	O nome do usuário de segurança especificado durante a criação do elemento.
(SnmpVersion)	A versão do SNMP utilizada para enviar pacotes SNMP (versão 1, 2c ou 3).
(SourceRouter)	O nome ou o endereço IP do roteador.
$timeout	O número de segundos em que o servidor deve responder. Obtido a partir do arquivo de configuração.
$vpn* (Vpn)	O nome da VPN especificado no campo **vpn** do elemento de perfil RPING.

Mensagens de Status

O monitor RPING fornece mensagens de status no atributo **ResultMessage** durante o uso do IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

A tabela a seguir descreve as mensagens de status NNTP.

Tabela 103. Mensagens de Status do Monitor RPING	
Mensagem	**Descrição**
`Resposta Obtida`	O monitor recebeu uma resposta do dispositivo Cisco.
`Erro no pacote - encadeamento de saída`	Houve um erro em um dos pacotes.
`Tempo limite esgotado ao tentar conjuntos iniciais`	Não houve resposta do roteador durante a tentativa de criar o campo `rowEntry`.
`Erro Interno`	Erro no roteador.
`Sondagem do host não concluída`	O dispositivo de rede não concluiu os pings.

Tabela 103. Mensagens de Status do Monitor RPING (continuação)	
Mensagem	**Descrição**
`Falha na Resposta` `Falha na operação`	O roteador não conseguiu executar ping no dispositivo de rede.
`Tempo limite esgotado nos pedidos Get`	O monitor atingiu o tempo limite quando você tentou obter os resultados do roteador.

Monitor RTSP

O monitor Real Time Streaming Protocol (RTSP) testa a reprodução de conexão de áudio e vídeo em servidores de fluxo. Ele coleta informações sobre arquivos de mídia e inicia a reprodução da conexão, pausa e final de uma sessão de fluxo.

A tabela a seguir lista os arquivos do monitor RTSP.

Tabela 104. Arquivos do Monitor RTSP	
Arquivos do Monitor	**Nome ou local**
Monitor executável	`nco_m_rtsp`
Arquivo de Propriedades	`$ISHOME/etc/props/rtsp.props`
Arquivo de regras	`$ISHOME/etc/rules/rtsp.rules`
Arquivo de log	`$ISHOME/log/rtsp.log`

Recomendações para Configuração do Monitor RTSP

O monitor RTSP se conecta ao servidor de fluxo no modo DESCRIBE ou PLAY. O monitor faz download das informações ou estatísticas entregues por servidores RTSP genuínos, como Darwin.

Modo DESCRIBE

No modo DESCRIBE, o monitor RTSP se conecta ao servidor de fluxo e solicita informações sobre os fluxos e arquivos de áudio e vídeo.

O servidor retorna um código de status no qual o valor `200` indica um arquivo que pode ser transferido por download e no qual outros valores indicam o motivo pelo qual o arquivo solicitado não pode ser reproduzido.

No entanto, as estatísticas relacionadas à reprodução não são relatadas nesse modo, e a função básica dos servidores que suportam RTSP pode ser testada.

Modo PLAY

No modo PLAY, o monitor RTSP se conecta ao servidor de fluxo da mesma maneira que no modo DESCRIBE e, depois, transmite o arquivo para fornecer estatísticas sobre os downloads solicitados.

Propriedades

As opções de propriedades específicas para o monitor RTSP estão descritas na seguinte tabela.

Tabela 105. Opções de propriedades do monitor RTSP		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
StreamingSocket BufferSize	integer	O tamanho do buffer de soquete de streaming, com um intervalo de 8 a 64 KB. Padrão: 8

Configurando Testes de Serviço do Monitor RTSP

Utilize os parâmetros de configuração do monitor RTSP para definir testes de serviço.

A tabela a seguir lista as configurações do monitor RTSP monitor:

Tabela 106. Configuração do Monitor RTSP	
Campo	**Descrição**
servidor	O sistema de destino que executa o servidor de fluxo. Por exemplo, `rtsp.mymusic.com`.
remotefile	O arquivo que é transferido por download. Por exemplo, `singalong.mp3`.
description	Um campo de texto para fornecer informações descritivas sobre o elemento. Por exemplo, RTSP `monitor`.
port	A porta à qual o monitor é conectado no sistema de destino. Padrão: 554
ação	A ação executada pelo servidor no fluxo: • DESCRIBE • JOGAR Padrão: DESCRIBE
duration	A parte do fluxo, em segundos, reproduzida pelo servidor. Padrão: 5
maxbandwidth	A largura máxima de banda, em bits por segundo, utilizada para fluxo contínuo. Padrão: 1500000
timeout	O tempo de espera, em segundos, pela resposta do servidor RTSP. Padrão: 10
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: 300
failureretests	O número de vezes para retestagem antes de a falha ser indicada. Padrão: 0

Tabela 106. Configuração do Monitor RTSP (continuação)	
Campo	**Descrição**
Intervalo de retestagem	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: 10

Classificações em Nível de Serviço

As classificações de nível de serviço definem as regras para determinar o nível de serviço fornecido por RTSP.

As opções de classificação em nível de serviço disponíveis para o monitor RTSP são:

```
totalTime
lookupTime
connectTime
responseTime
sdpDownloadTime
playbackTime
status
percentPacketsLost
Mensagem
```

Nas classificações em nível de serviço:

- Especifique mais classificações de nível de serviço inserindo manualmente o nome do elemento de monitor. O nome deve corresponder ao nome mostrado para o elemento na seção de elementos de monitor.
- `message` pode ser qualquer mensagem encaminhada no elemento **`$message`** para o servidor IBM Application Performance Management se usado em qualquer widget. Para obter uma lista de possíveis valores, consulte Mensagens de status.
- O operando é uma cadeia ou um número positivo.
- Um código de status de 200 indica sucesso. Consulte o protocolo RTSP para obter outros códigos de status retornados pela operação.

Elementos do Monitor

Além dos resultados de testes comuns a todos os elementos, o monitor RTSP gera um conjunto de resultados de testes que contêm dados específicos para os testes de serviço RTSP.

A tabela a seguir descreve os elementos adicionais para o monitor RTSP.

Tabela 107. Elementos do Monitor RTSP	
Elemento	**Descrição**
$action	A ação utilizada pelo monitor.
$averageBandwidth	A média total de largura de banda, em bits.
$bytesReceived	O número total de bytes recebidos.
$connectTime* (`ConnectTime`)	O tempo gasto para estabelecer um conexão com o servidor de destino.
$describeStageStatus	Código de status de um estágio da conversação RTSP.
`$filename`	O nome do arquivo de mídia.

Tabela 107. Elementos do Monitor RTSP (continuação)	
Elemento	**Descrição**
$lookupTime* (LookupTime)	O tempo utilizado para obter o endereço IP do servidor host.
$maxBandwidth	A largura da banda máxima usando a interface de configuração.
$mediaResponseTime	O tempo utilizado pelo servidor para iniciar o fluxo contínuo do arquivo solicitado.
$numberOfStreams	O número de fluxos integrados à mídia.
$percentPacketsLost	A porcentagem de pacotes perdidos.
$playbackTime* (PlaybackTime)	O tempo que representa a soma de setupResponseTime e mediaResponseTime.
$playStageStatus	Código de status de um estágio da conversação RTSP.
$port	A porta usada para acessar o servidor do monitor.
$responseTime* (ResponseTime)	O tempo entre o estabelecimento da conexão e o recebimento do primeiro byte de dados.
$sdpDownloadTime* (SdpDownloadTimed)	O tempo utilizado para fazer download de dados sobre o arquivo de mídia.
$setupResponseTime	O tempo que representa parte do playbackTime. **Nota:** O elemento só é gerado quando o monitor RTSP está operando no modo PLAY.
$setupStageStatus	Código de status de um estágio da conversação RTSP.
$status	O código de status retornado pelo servidor RTSP.
$streamingTime	O tempo utilizado pelo servidor para concluir o fluxo contínuo do arquivo solicitado.
$streamLength	A duração do fluxo mais longo no arquivo de mídia.
$teardownStageStatus	Código de status de um estágio da conversação RTSP.
$totalBandwidthRequired	A largura de banda total, em kilobits por segundo.
$totalPacketsLost	O número total de pacotes perdidos.
$totalPacketsReceived	O número de pacotes recebidos.

Mensagens de Status

O monitor RTSP fornece mensagens de status no atributo **ResultMessage** durante o uso do IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

Tabela 108. Mensagens de Status do Monitor RTSP

Mensagem	**Descrição**
Ok	A solicitação foi bem-sucedida.
Conexão com falha	O monitor falhou ao se conectar ao servidor. Para obter informações adicionais, consulte o arquivo de log.
Conexão fechada por host externo	A conexão com o servidor RTSP foi interrompida.
Tempo limite esgotado ao aguardar leitura/gravação	Foi estabelecida uma conexão de dados com o servidor RTSP, mas ocorreu um problema.
Falha na reprodução - nenhum fluxo	O monitor recebeu uma resposta, mas não havia nenhum áudio ou vídeo disponível para reprodução.
Falha de select() no soquete RTSP (estágio PLAY)	O soquete foi fechado no servidor remoto ou esgotou o tempo limite de espera por uma resposta.
A resposta do Servidor RTSP não está no formato esperado	A resposta do servidor estava em um formato não suportado pelo monitor.
Redirecionamento solicitado pelo servidor não suportado pelo cliente	A resposta do servidor não é suportada pelo cliente.
O servidor não pode preencher o pedido do cliente	A solicitação falha e nenhuma informação adicional é disponibilizada.
Erro no Servidor	Houve um problema com o servidor e o pedido falhou. Um código de 500 ou maior foi retornado pelo servidor. Para obter mais informações, consulte o protocolo RTSP (RFC 2326).

Tabela 108. Mensagens de Status do Monitor RTSP (continuação)	
Mensagem	**Descrição**
O cabeçalho de resposta CSeq do RTSP não corresponde ao pedido CSeq	O servidor RTSP está configurado de forma inválida e não está funcionando corretamente.
Resposta corrompida do servidor RTSP	
Descrição corrompida da sessão	
A resposta CSeq de RTSP SETUP não corresponde ao pedido CSeq	
Resposta de RTSP SETUP, cadeia de sessão incompleta	
Resposta de RTSP SETUP, o ID de sessão foi alterado na mesma sessão	
A resposta de RTSP SETUP não contém portas do servidor às quais conectar-se	
A resposta de RTSP SETUP não contém o par de portas do servidor às quais conectar-se	
A resposta CSeq de RTSP PLAY não corresponde ao pedido CSeq	
Resposta de RTSP PLAY, cadeia de sessão incompleta	
Resposta de RTSP PLAY, o ID de sessão foi alterado na mesma sessão	
Resposta de RTSP PLAY, cadeia de informações de RTP incompleta	
A resposta de RTSP PLAY não valida seqnum de RTP na resposta de informações de RTP	
A resposta de RTSP PLAY não valida o tempo de RTP na resposta de informações de RTP	

monitor SAA

O Cisco Service Assurance Agent (SAA) é um agente de monitoramento de desempenho para produtos Cisco para IOS versão 12.2(2) e acima.

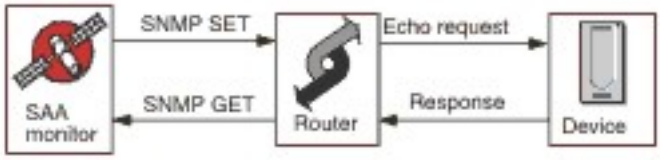
O monitor SAA usa o recurso Cisco Service Assurance Agent para testar várias sincronizações entre roteadores Cisco.

Tabela 109. Resumo do Monitor SAA	
Arquivos do Monitor	**Nome ou local**
Nome do executável	`nco_m_saa`
Arquivo de Propriedades	`$ISHOME/etc/props/saa.props`
Arquivo de regras	`$ISHOME/etc/rules/saa.rules`
Arquivo de log	`$ISHOME/log/saa.log`
Diretório de Scripts	`$ISHOME/scripts/saa/`

Recomendações para Configuração do Monitor SAA

O monitor SAA configura um SAA do roteador para testar a disponibilidade de outro dispositivo de rede ou serviço usando eco solicitações ou eco respostas cronometradas que estão definidas no Management Information Base (MIB) do Monitor de Tempo de Resposta do Cisco. O monitor usa Protocolo Simples de Gerenciamento de Rede para se comunicar com o Service Assurance Agent.

A imagem a seguir demonstra a operação do monitor SAA.



Operação

O monitor SAA configura o Service Assurance Agent para executar eco testes, chamados análises, em outros dispositivos de rede. Você pode configurar um intervalo de sondagens diferentes, cada uma delas usando um protocolo diferente.

Todas as sondas podem operar em qualquer destino ativado por IP, exceto Jitter, o que requer outro roteador de resposta Cisco para SAA.

Cada elemento de perfil do monitor inicia uma análise do Service Assurance Agent em um roteador na inicialização e, com cada pesquisa sucessiva, coleta informações de resultado e reagenda a análise. Se uma análise parar inesperadamente, o monitor a reinicia imediatamente. Quando os testes de análise são concluídos, eles vão para o estado inativo até a próxima pesquisa do monitor. Na próxima pesquisa do monitor, os dados do resultado são coletados e outro ciclo de testes é iniciado. Durante cada pesquisa, o monitor verifica o estado da análise. Se a análise ainda estiver em execução, o monitor a interrompe e, em seguida, pesquisa no Management Information Base (MIB) os dados resultantes e as informações de erro do último ciclo. Depois, ele reagenda a análise, reconfigura os dados estatísticos e reativa a análise, que é executada no modo não assistido até a próxima pesquisa do monitor.

Para impedir a possibilidade de deixar processos não-controlados no roteador, o monitor inicia sondas com um span com vida predefinida que é estendido em cada sonda do monitor. Se o monitor for finalizado, ele continuará em execução até seu tempo de vida expirar. Depois, ele muda para o estado inativo até que o tempo limite de idade seja atingido e o roteador termine o processo.

Isso não é necessário para o IOS pré-configurado e o Service Assurance Agent, pois o monitor automaticamente configura, controla e limpa as análises no tempo de execução. Isso inclui a configuração de roteadores de resposta que são necessários por alguns tipos de sondas.

Persistência da Análise

A propriedade do monitor ProbePersist controla a persistência da análise nas pesquisas do monitor. Se a persistência da análise não estiver ativada, as análises começarão em cada pesquisa e terminarão imediatamente após produzir os resultados do teste.

Carregamento do Roteador
Às vezes, operações de sonda podem ser afetadas pelo carregamento do roteador. A propriedade StatusWait aguarda as análises mudarem de um estado para o outro antes de uma operação ser considerada falha.

Tipos de Análise
Os tipos de análises disponíveis com o monitor SSA são listados a seguir:

- DHCP
- DLSW
- DNS
- FTP
- Pedidos de HTTP Get
- ICMP Echo
- ICMP Path Echo
- Jitter
- UDP Echo
- SNA-Echo
- VOIP

Eco análises executam testes com base em um intervalo de tempo, enquanto análises Jitter, VOIP e HTTP executam testes através de uma única operação.

Propriedades SAA
Deve-se configurar as propriedades do monitor SAA.

A tabela a seguir descreve as propriedades do monitor SAA.

Tabela 110. Propriedades do monitor SAA

Nome da propriedade	Parâmetro de propriedade	Descrição
AgeOut	integer	O número máximo de segundos que uma análise permanece inativa antes de parar. O padrão é 600.
MibDir	string	O diretório usado para arquivos MIB. O caminho padrão é `$ISHOME/mibs`
ProbeLife	integer	O número máximo de segundos que uma análise permanece ativa quando não assistida. O padrão é 600.
ProbePersist	0|1	As análises podem ser executadas em dois modos. Elas executam um ciclo de teste único por pesquisa de monitor ou são iniciadas uma vez e reagendadas a cada pesquisa. • 0 indica um ciclo de teste único • 1 indica um reagendamento a cada pesquisa
StatusWait	integer	O número de segundos que um monitor aguarda uma análise para concluir qualquer ação antes de falhar.

Configurando testes de serviço do monitor SAA
É necessário configurar os parâmetros do monitor SAA para definir testes de serviço.

A tabela a seguir descreve os campos de configuração do monitor SAA.

Tabela 111. Configuração do Monitor SAA

Campo	**Descrição**
servidor	O nome ou endereço IP do roteador Cisco.
sequência de comunidades	A sequência da comunidade SNMP para o roteador.
probetype	O tipo de sondagem SAA aplicável ao elemento do perfil.
description	Um campo de texto que fornece informações descritivas do elemento.
Ativo	Indica se o elemento do perfil está ativo.
port	A porta utilizada para acessar o roteador. A porta padrão é 161.
versão	A versão SNMP a ser usada: • 1 é usado para SNMPv1 • 2 é usado para SNMPv2c • 3 é usado para SNMPv3 O padrão é 1.
probeid	Especifica um valor usado para gerar o índice de linha de controle de análise.
securityname†	O nome do usuário para a sessão SNMP.
authenticationphrase†	A senha de autenticação para o usuário.
privacyphrase†	A senha de privacidade para o usuário.
authenticationprotocol†	Os protocolos usados para autenticar os usuários da seguinte forma: • MD5 • SHA1 O padrão é MD5.
privacyprotocol†	O protocolo a ser utilizado para criptografar a sessão. Este é o DES.
timeout	O tempo, em segundos, para aguardar até que o roteador responda. O padrão é 5.
tentar novamente	O número de vezes que o monitor tenta contatar novamente o roteador antes de encerrar. O padrão é 0.
Pesquisar	O tempo, em segundos, entre cada sondagem. O padrão é 300
failureretests	O número de vezes para retestagem antes de indicar falha. O padrão é 0..
Intervalo de retestagem	O tempo de espera, em segundos, entre cada novo teste que falha. O padrão é 10 minutos.

Nota: † Aplicável apenas ao SNMPv3.

Configuração do Tipo de Análise

A configuração de análise é diferente para cada tipo de análise e o agente Monitoramento de Serviço da Internet fornece um conjunto de campos de configuração específico para cada tipo. Para criar um elemento de perfil, selecione um tipo de análise e forneça a configuração apropriada para esse tipo. Para obter informações sobre itens de configuração individuais, consulte o documento MIB do Cisco Response Time Monitor.

Classificação de nível de serviço

A classificação de nível de serviço define as regras para determinar o nível de serviço fornecido por um dispositivo de rede.

As opções de classificação de nível de serviço disponíveis para o monitor SAA são as seguintes:

```
totalTime
errTotal
numRTT
minRTT
maxRTT
avgRTT
minPosJitterSD
maxPosJitterSD
minNegJitterSD
maxNegJitterSD
minPosJitterDS
maxPosJitterDS
minNegJitterDS
maxNegJitterDS
packetLossSD
packetLossDS
packetOutOfSequence
packetMIA
packetLateArrival
minDelaySD
maxDelaySD
minDelayDS
maxDelayDS
avgPosJitterSD
avgPosJitterDS
avgNegjitterSD
avgNegJitterDS
avgDelaySD
avgDelayDS
devPosJitterSD
devPosJitterDS
devNegJitterSD
devNegJitterDS
devDelaySD
devDelayDS
MOS
ICPIF
mMinRTT
httpRTT
dnsRTT
tcpConnectRTT
transactionRTT
Mensagem
```

Nas classificações em nível de serviço:

- Especifique mais classificações de nível de serviço inserindo manualmente o nome do elemento de monitor. O nome deve corresponder ao nome mostrado para o elemento na seção Elementos do Monitor.
- `message` pode ser qualquer mensagem encaminhada no elemento **`$message`** para o servidor IBM Application Performance Management se usado em qualquer widget. Para obter uma lista de possíveis valores, consulte “Mensagens de Status” na página 404.
- O operando é uma cadeia ou um número positivo.

Elementos do Monitor
Além dos resultados de testes comuns a todos os elementos, o monitor SAA gera um conjunto de resultados de testes que contém dados específicos para o tipo de análise em uso.

Análises de DHCP
As análises de DHCP geram múltiplos elementos.

A tabela a seguir descreve os elementos da análise de DHCP.

Tabela 112. Elementos da Análise de DHCP	
Elemento	**Descrição**
$authProto	O protocolo de autenticação especificado durante a criação do elemento.
$community	A comunidade utilizada para enviar pedidos de SNMP para o SAA.
$port	A porta usada para se conectar ao SAA.
$privProto	O protocolo de privacidade especificado durante a criação do elemento.
$probeType	dhcp
$securityName	O nome do usuário de segurança especificado durante a criação do elemento.
$snmpVersion (SnmpVersion)	A versão do SNMP utilizada para enviar pacotes SNMP (versão 1, 2c ou 3).
(SourceRouter)	O nome do roteador utilizado para enviar pedidos de DHCP.
$totalRTT † (TotalRTT)	O tempo total de roundtrip levado para obter um IP do servidor DHCP em segundos.

Nota: † indica que o elemento está disponível para classificações em nível de serviço.

Análises de DLSW
As análises de DLSW geram múltiplos elementos.

A tabela a seguir descreve os elementos da análise de DLSW.

Tabela 113. Elementos da Análise de DLSW	
Elemento	**Descrição**
$authProto	O protocolo de autenticação especificado durante a criação do elemento.
$avgRTT* † (AverageRTT)	O tempo médio de roundtrip em segundos.
$community	A comunidade utilizada para enviar pedidos de SNMP para o SAA.
$errTotal* † (ErrorTotal)	O número total de pacotes com erros.
$maxRTT* † (MaximumRTT)	O maior tempo de roundtrip em segundos.
$minRTT* † (MinimumRTT)	O menor tempo de roundtrip em segundos.
$numRTT†	O número de roundtrips bem-sucedidos.

Tabela 113. Elementos da Análise de DLSW (continuação)	
Elemento	**Descrição**
$port	A porta usada para se conectar ao SAA.
$privProto	O protocolo de privacidade especificado durante a criação do elemento.
$probeType †	dlsw
$securityName	O nome do usuário de segurança especificado durante a criação do elemento.
$snmpVersion (SnmpVersion)	A versão do SNMP utilizada para enviar pacotes SNMP (versão 1, 2c ou 3).
(SourceRouter)	O roteador utilizado para executar o teste SAA.
$sumOfRTT (TotalRTT)	A soma de todos os tempos de roundtrip em segundos.
(TargetHost)	O nome ou o endereço IP do host no qual o SAA de destino está sendo executado.

Nota: † indica que o elemento está disponível para classificações em nível de serviço.

Análises de DNS
Análises de DNS geram inúmeros elementos.

A tabela a seguir descreve os elementos da análise de DNS.

Tabela 114. Elementos da Análise de DNS	
Elemento	**Descrição**
$authProto	O protocolo de autenticação especificado durante a criação do elemento.
$community	A comunidade utilizada para enviar pedidos de SNMP para o SAA.
$dnsHost (Host)	O host a ser resolvido no servidor.
$dnsServer	O IP do servidor DNS.
(HostLookup)	O endereço IP do host.
$port	A porta usada para se conectar ao SAA.
$privProto	O protocolo de privacidade especificado durante a criação do elemento.
$probeType	dns
$securityName	O nome do usuário de segurança especificado durante a criação do elemento.
$snmpVersion (SnmpVersion)	A versão do SNMP utilizada para enviar pacotes SNMP (versão 1, 2c ou 3).
(SourceRouter)	O nome do roteador utilizado para enviar pedidos de DNS.

Tabela 114. Elementos da Análise de DNS (continuação)	
Elemento	**Descrição**
$totalRTT † (TotalRTT)	O tempo total de roundtrip para a consulta de DNS em segundos.

Nota: † indica que o elemento está disponível para classificações em nível de serviço.

Análises de FTP
Análises de FTP geram inúmeros elementos.

A tabela a seguir descreve os elementos da análise de FTP.

Tabela 115. Elementos da Análise de FTP	
Elemento	**Descrição**
$activePassive	O tipo de conexão utilizado no teste, `Active` ou `Passive`. Padrão: `Passive`
$authProto	O protocolo de autenticação especificado durante a criação do elemento.
$community	A comunidade utilizada para enviar pedidos de SNMP para o SAA.
$errorStatus	A cadeia de resultados que indica o status do teste (do objeto MIB `rttMonLatestRttOperSense`).
$ftpFile	O nome do arquivo de teste recuperado durante o teste.
$ftpUrl (FtpUrl)	A URL utilizada no teste FTP.
$port	A porta usada para se conectar ao SAA.
$privProto	O protocolo de privacidade especificado durante a criação do elemento.
$securityName	O nome do usuário de segurança especificado durante a criação do elemento.
$snmpVersion (SnmpVersion)	A versão do SNMP utilizada para enviar pacotes SNMP (versão 1, 2c ou 3).
(SourceRouter)	O nome do roteador utilizado para enviar pedidos de FTP.
$totalRTT (TotalRTT)	O tempo de conclusão do teste (do objeto MIB `rttMonLatestRttOperCompletionTime`) em segundos.

Análises de HTTP-Get
As análises de HTTP-Get geram múltiplos elementos.

A tabela a seguir descreve os elementos da análise de HTTP-Get.

Tabela 116. Elementos da Análise de HTTP-Get	
Elemento	**Descrição**
$authProto	O protocolo de autenticação especificado durante a criação do elemento.

Tabela 116. Elementos da Análise de HTTP-Get (continuação)	
Elemento	**Descrição**
$community	A comunidade utilizada para enviar pedidos de SNMP para o SAA.
$dnsRTT † (DnsRTT)	O tempo de roundtrip para executar a consulta de DNS em segundos.
$httpRTT † (HttpRTT)	O tempo de roundtrip para executar a operação HTTP em segundos.
(HttpUrl)	A URL que é monitorada.
$messageBodyBytes	O tamanho do corpo da mensagem recebido.
$numRTT†	O número de roundtrips bem-sucedidos.
$port	A porta usada para se conectar ao SAA.
$privProto	O protocolo de privacidade especificado durante a criação do elemento.
$probeType	http-get
$securityName	O nome do usuário de segurança especificado durante a criação do elemento.
(SourceRouter)	O nome do roteador utilizado para enviar pedidos de HTTP.
$snmpVersion (SnmpVersion)	A versão do SNMP utilizada para enviar pacotes SNMP (versão 1, 2c ou 3).
$targetHost	O nome do host do serviço que está sendo testado.
$tcpConnectRTT † (TcpConnectRTT)	O tempo de roundtrip para se conectar ao servidor HTTP em segundos.
$transactionRTT † (TransactionRTT)	O tempo de roundtrip para fazer download do objeto especificado pela URL em segundos.

Nota: † indica que o elemento está disponível para classificações em nível de serviço.

Análises de ICMP-Echo
Análises de ICMP-Echo geram inúmeros elementos.

A tabela a seguir descreve os elementos da análise de ICMP-Echo.

Tabela 117. Elementos da Análise de ICMP-Echo	
Elemento	**Descrição**
$authProto	O protocolo de autenticação especificado durante a criação do elemento.
$avgRTT † (AverageRTT)	O tempo médio de roundtrip em segundos.
$community	A comunidade utilizada para enviar pedidos de SNMP para o SAA.

Tabela 117. Elementos da Análise de ICMP-Echo (continuação)	
Elemento	**Descrição**
$errBusies	O número de pings que falharam devido a um ping anterior incompleto.
$errDisconnects	O número de pings que falharam através de desconexões.
$ErrDrops	O número de pings que falharam por causa da indisponibilidade de um recurso interno.
$errNoConnects	O número de pings que falharam porque uma conexão com o destino não pôde ser estabelecida.
$errSequences	O número de pings que falharam por causa do recebimento de um ID de seqüência inesperado.
$errTimeouts	O número de pings que falharam por tempos limite.
$errTotal † (ErrorTotal)	O número total de pacotes com erros.
$errVerifies	O número de pings que falharam porque os dados recebidos não eram os mesmos que os dados esperados.
$maxRTT † (MaximumRTT)	O maior tempo de roundtrip em segundos.
$minRTT † (MinimumRTT)	O menor tempo de roundtrip em segundos.
$numRTT †	O número de roundtrips bem-sucedidos.
$port	A porta usada para se conectar ao SAA.
$privProto	O protocolo de privacidade especificado durante a criação do elemento.
$probeType	O tipo de análise deve ser o seguinte: • icmp-echo • icmp-echo-path • udp-echo
$securityName	O nome do usuário de segurança especificado durante a criação do elemento.
$snmpVersion (SnmpVersion)	A versão do SNMP utilizada para enviar pacotes SNMP (versão 1, 2c ou 3).
(SourceRouter)	O nome do roteador utilizado para enviar pedidos de ICMP.
$sumOfRTT	A soma de todos os tempos de roundtrip em segundos.
$targetHost (Host)	O nome do host do serviço sendo monitorado.
$tos (Tos)	O tipo do valor de serviço.

Tabela 117. Elementos da Análise de ICMP-Echo (continuação)	
Elemento	**Descrição**
$vpn (Vpn)	O nome da VPN.

Nota: † indica que o elemento está disponível para classificações em nível de serviço.

Análises de ICMP-Path-Echo
Análises de ICMP-Patch-Echo geram múltiplos elementos.

A tabela a seguir descreve os elementos da análise de ICMP-Patch-Echo.

Tabela 118. Elementos da Análise de ICMP-Path-Echo	
Elemento	**Descrição**
$authProto	O protocolo de autenticação especificado durante a criação do elemento.
$avgRTT † (AverageRTT)	O tempo médio de roundtrip em segundos.
$community	A comunidade utilizada para enviar pedidos de SNMP para o SAA.
(HopHost*One to Eight*)	O primeiro de oito hosts que visitam utilizando ICMP Echo Path.
$maxRTT † (MaximumRTT)	O maior tempo de roundtrip em segundos.
$minRTT † (MinimumRTT)	O menor tempo de roundtrip em segundos.
$numRTT †	O número de roundtrips bem-sucedidos.
$port	A porta usada para se conectar ao SAA.
`$privProto`	O protocolo de privacidade especificado durante a criação do elemento.
$probeType	O tipo de análise é o seguinte: • `icmp-echo` • `icmp-echo-path`
$securityName	O nome do usuário de segurança especificado durante a criação do elemento.
$snmpVersion (SnmpVersion)	A versão do SNMP utilizada para enviar pacotes SNMP (versão 1, 2c ou 3).
(SourceRouter)	O nome do roteador utilizado para enviar pedidos de ICMP.
$sumOfRTT	A soma de todos os tempos de roundtrip em segundos.
$targetHost	O nome do host do serviço que está sendo testado.
$tos (Tos)	O tipo do valor de serviço.

Tabela 118. Elementos da Análise de ICMP-Path-Echo (continuação)	
Elemento	**Descrição**
$vpn (Vpn)	O nome da VPN.

Nota: † indica que o elemento está disponível para classificações em nível de serviço.

Análises de Jitter
As análises Jitter geram vários elementos.

A tabela a seguir descreve os elementos da análise de Jitter.

Tabela 119. Elementos da Análise de Jitter	
Elemento	**Descrição**
$authProto	O protocolo de autenticação especificado durante a criação do elemento.
$avgDelayDS†	A média de atraso do destino à origem em segundos.
$avgDelaySD†	O atraso médio da origem ao destino em segundos.
$avgNegJitterDS†	A média de Jitter negativo do destino à origem em segundos.
$avgNegJitterSD†	A média de Jitter negativo da origem ao destino em segundos.
$avgPosJitterDS†	A média de Jitter positivo do destino à origem em segundos.
$avgPosJitterSD†	A média de Jitter positivo da origem ao destino em segundos.
$avgRTT † (AverageRTT)	O tempo médio de roundtrip em segundos.
$community	A comunidade utilizada para enviar pedidos de SNMP para o SAA.
$devDelayDS†	O desvio padrão de atraso do destino à origem.
$devDelaySD†	O desvio padrão de atraso da origem ao destino.
$devNegJitterDS†	O desvio padrão de Jitter negativo do destino à origem.
$devNegJitterSD†	O desvio padrão de Jitter negativo da origem ao destino.
$devPosJitterDS†	O desvio padrão de Jitter positivo do destino à origem.
$devPosJitterSD†	O desvio padrão de Jitter positivo da origem ao destino.
$errDescription	Uma descrição do erro.
$errTotal (ErrorTotal)	O número total de pacotes com erros.
$maxDelayDS †	O atraso máximo do destino à origem em segundos.
$maxDelaySD †	O atraso máximo da origem ao destino em segundos.
$maxNegJitterDS †	O valor máximo de Jitter negativo do destino à origem em segundos.
$maxNegJitterSD †	O valor máximo de Jitter negativo da origem ao destino em segundos.
$maxPosJitterDS †	O valor máximo de Jitter positivo do destino à origem em segundos.

Tabela 119. Elementos da Análise de Jitter (continuação)	
Elemento	**Descrição**
$maxPosJitterSD †	O valor máximo de Jitter positivo da origem ao destino em segundos.
$maxRTT † (MaximumRTT)	O maior tempo de roundtrip em segundos.
$minDelayDS †	O atraso mínimo do destino à origem em segundos.
$minDelaySD †	O atraso mínimo da origem ao destino em segundos.
$minNegJitterDS †	O valor mínimo de Jitter negativo do destino à origem em segundos.
$minNegJitterSD †	O valor mínimo de Jitter negativo da origem ao destino em segundos.
$minPosJitterDS †	O valor mínimo de Jitter positivo do destino à origem em segundos.
$minPosJitterSD †	O valor mínimo de Jitter positivo da origem ao destino em segundos.
$minRTT † (MinimumRTT)	O menor tempo de roundtrip em segundos.
$numNegJitterDS	O número de valores Jitter negativos do destino à origem.
$numNegJitterSD	O número de valores Jitter negativos da origem ao destino.
$numOW	O número de operações unidirecionais para atraso.
$numPosJitterDS	O número de valores Jitter positivos do destino à origem.
$numPosJitterSD	O número de valores Jitter positivos da origem ao destino.
$numRTT †	O número de roundtrips bem-sucedidos.
$packetLateArrival †	O número de pacotes que chegaram depois do tempo limite.
$packetLossDS †	O número de pacotes perdidos do destino à origem.
$packetLossSD †	O número de pacotes perdidos da origem ao destino.
$packetMIA†	O número de pacotes perdidos em que a direção é desconhecida.
$packetOutOfSequence†	O número de pacotes retornados fora da ordem.
$port	A porta usada para se conectar ao SAA.
$privProto	O protocolo de privacidade especificado durante a criação do elemento.
$probeType†	Jitter
(ResponderRouter)	O nome do roteador utilizado para responder a pedidos de Jitter.
$securityName	O nome do usuário de segurança especificado durante a criação do elemento.
(SourceRouter)	O nome do roteador utilizado para enviar pedidos de Jitter.
$snmpVersion (SnmpVersion)	A versão do SNMP utilizada para enviar pacotes SNMP (versão 1, 2c ou 3).
$sum2DelayDS	A soma de quadrados de atraso do destino à origem.

Tabela 119. Elementos da Análise de Jitter (continuação)	
Elemento	**Descrição**
$sum2DelaySD	A soma de quadrados de atraso da origem ao destino.
$sum2NegJitterDS	A soma de quadrados de todos os valores Jitter negativos.
$sum2NegJitterSD	A soma de quadrados de todos os valores Jitter negativos.
$sum2PosJitterDS	A soma de quadrados de todos os valores Jitter positivos.
$sum2PosJitterSD	A soma de quadrados de todos os valores Jitter positivos.
$sum2Rtt†	A soma dos quadrados dos valores de roundtrip em segundos.
$sumDelayDS	A soma de atrasos do destino à origem em segundos.
$sumDelaySD	A soma de atrasos da origem ao destino em segundos.
$sumNegJitterDS	A soma de todos os valores de Jitter negativos em segundos.
$sumNegJitterSD	A soma de valores de Jitter negativos em segundos.
$sumPosJitterDS	A soma de todos os valores de Jitter positivos em segundos.
$sumPosJitterSD	A soma de todos os valores de Jitter positivos em segundos.
$sumRTT	A soma de todos os roundtrips em segundos.
$targetHost	O nome do host do serviço que está sendo testado.
$tos (Tos)	O tipo do valor de serviço.
$vpn (\Vpn)	O nome da VPN.

Nota: † indica que o elemento está disponível para classificações em nível de serviço.

Análises de SNA-Echo
Análises de SNA-Echo (SNA-RU-Echo, SNA-LU0-Echo, SNA-LU2-Echo, SNA-LU62-Echo e SNA-LU62Native-Echo) geram os elementos que estão listados na tabela a seguir.

A tabela a seguir descreve os elementos da análise de JSNA-Echo.

Tabela 120. Elementos da Análise de SNA-Echo	
Elemento	**Descrição**
$authProto	O protocolo de autenticação especificado durante a criação do elemento.
$avgRTT † (AverageRTT)	O tempo médio de roundtrip em segundos.
$community	A comunidade utilizada para enviar pedidos de SNMP para o SAA.
$errTotal †	O número total de pacotes com erros.
$maxRTT † (MaximumRTT)	O maior tempo de roundtrip em segundos.

Tabela 120. Elementos da Análise de SNA-Echo (continuação)	
Elemento	**Descrição**
$minRTT † (MinimumRTT)	O menor tempo de roundtrip em segundos.
$numRTT†	O número de roundtrips bem-sucedidos.
$port	A porta usada para se conectar ao SAA.
$privProto	O protocolo de privacidade especificado durante a criação do elemento.
$probeType (ProbeType)	`sna-`*`name`*`-echo`
$securityName	O nome do usuário de segurança especificado durante a criação do elemento.
(SourceRouter)	O nome do roteador utilizado para enviar pedidos de SNA.
$snmpVersion (SnmpVersion)	A versão do SNMP utilizada para enviar pacotes SNMP (versão 1, 2c ou 3).
$sumOfRTT (TotalRTT)	A soma de todos os tempos de roundtrip em segundos.
(TargetHost)	O destino do host do pedido de eco de SNA.

Nota: † indica que o elemento está disponível para classificações em nível de serviço.

Análises de UDP-Echo
As análises de UDP-Echo geram os elementos listados na tabela a seguir.

A tabela a seguir descreve os elementos da análise de UDP-Echo.

Tabela 121. Elementos da Análise de UDP-Echo	
Elemento	**Descrição**
`$authProto`	O protocolo de autenticação especificado durante a criação do elemento.
$avgRTT † (AverageRTT)	O tempo médio de roundtrip em segundos.
$community	A comunidade utilizada para enviar pedidos de SNMP para o SAA.
$errBusies	O número de pings que falharam devido a um ping incompleto anterior.
$ErrDrops	O número de pings que falharam por causa da indisponibilidade de um recurso interno.
$errTimeouts	O número de pings que falharam por tempos limite.
$errTotal † (ErrorTotal)	O número total de pacotes com erros.

Tabela 121. Elementos da Análise de UDP-Echo (continuação)	
Elemento	**Descrição**
$errVerifies	O número de pings que falharam porque os dados recebidos não eram os mesmos que os dados esperados.
$maxRTT † (MaximumRTT)	O maior tempo de roundtrip em segundos.
$minRTT † (MinimumRTT)	O menor tempo de roundtrip em segundos.
$numRTT †	O número de roundtrips bem-sucedidos.
$port	A porta usada para se conectar ao SAA.
$privProto	O protocolo de privacidade especificado durante a criação do elemento.
$probeType	`udp-echo`
`$securityName`	O nome do usuário de segurança especificado durante a criação do elemento.
$snmpVersion* (SnmpVersion)	A versão do SNMP utilizada para enviar pacotes SNMP (versão 1, 2c ou 3).
$sumOfRTT	A soma de todos os tempos de roundtrip (em segundos).
$targetHost (Host)	O nome do host do serviço que é monitorado.
$tos (Tos)	O tipo de valor de serviço.
$vpn (Vpn)	O nome da VPN.

Nota: † indica que o elemento está disponível para classificações em nível de serviço.

Análises de VOIP
As análises de VOIP geram os mesmos elementos que as análises de Jitter. Além disso, elas geram os elementos que são listados na tabela a seguir.

A tabela a seguir descreve elementos de análise VOIP.

Tabela 122. Elementos da Análise de VOIP	
Elemento	**Descrição**
$authProto	O protocolo de autenticação especificado durante a criação do elemento.
$avgRTT † (AverageRTT)	O tempo médio de roundtrip em segundos.
$community	A comunidade utilizada para enviar pedidos de SNMP para o SAA.

Tabela 122. Elementos da Análise de VOIP (continuação)	
Elemento	**Descrição**
$errTotal † (ErrorTotal)	O número total de pacotes com erros.
$ICPIF †	O valor de ICPIF.
$maxRTT † (MaximumRTT)	O maior tempo de roundtrip em segundos.
$minRTT † (MinimumRTT)	O menor tempo de roundtrip em segundos.
$MOS †	O valor do Mean Opinion Score (MOS) do teste.
$port	A porta usada para se conectar ao SAA.
$privProto	O protocolo de privacidade especificado durante a criação do elemento.
$probeType †	voip
(ResponderRouter)	O nome do roteador utilizado para responder a pedidos de VOIP.
$securityName	O nome do usuário de segurança especificado durante a criação do elemento.
$snmpVersion (SnmpVersion)	A versão do SNMP utilizada para enviar pacotes SNMP (versão 1, 2c ou 3).
(SourceRouter)	O nome do roteador utilizado para enviar os pedidos de VOIP.
(Tos)	O tipo do valor de serviço.
(Vpn)	O nome da VPN.

Nota: † indica que o elemento está disponível para classificações em nível de serviço.

Mensagens de Status
O monitor SAA fornece mensagens de status no atributo **ResultMessage** ao usar IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

A tabela a seguir descreve as mensagens de status para monitores SAA.

Tabela 123. Mensagens de Status do Monitor SAA	
Mensagem	**Descrição**
`Com Êxito`	A operação de análise foi bem-sucedida.
`Operação falha`	A operação de análise falhou.
`Status inválido`	A operação de análise falhou com um status inválido.

Monitor SIP
O monitor SIP verifica a disponibilidade de servidores Session Initiation Protocol (SIP), incluindo o tempo levado para registrar e autenticar terminais. O monitor inicia uma sessão SIP de modo que os pedidos e respostas SIP possam ser monitorados.

A tabela a seguir lista os arquivos do monitor SIP.

Tabela 124. Resumo do Arquivo do Monitor SIP	
Arquivos do Monitor	**Nome ou local**
Monitor executável	`nco_m_sip`
Arquivo de Propriedades	`$ISHOME/etc/props/sip.props`
Arquivo de regras	`$ISHOME/etc/rules/sip.rules`
Arquivo de log	`$ISHOME/log/sip.log`

Recomendações para Configuração do Monitor SIP

O monitor SIP testa a disponibilidade de um servidor SIP enviando um pedido para o URI de um dispositivo ativado por SIP, pelo servidor SIP, e recebendo, também pelo servidor SIP, respostas do dispositivo SIP.

O monitor SIP age como um User Agent Client (UAC); ele inicia as conexões utilizadas para testar serviços SIP. O User Agent Server (UAS), o receptor ou o destino da chamada podem ser qualquer dispositivo ativado por SIP, como um computador executado como softphone ou um banco de mensagens.

Ao testar um servidor SIP, o monitor assume a seguinte sequência de ações:

1. Registra-se com o servidor SIP usando as credenciais fornecidas no elemento de perfil.
2. Envia um pedido OPTIONS para o UAS.
3. Envia um pedido INVITE para o UAS.

   Registra um resultado de teste bem-sucedido se o UAS aceita o pedido.
4. Envia uma solicitação BYE para o UAS e encerra a conexão com ele.
5. Cancela o registro do servidor SIP com validade imediata.

O monitor registra a duração de cada ação que é executada no teste.

Propriedades

As opções de propriedades específicas do monitor SIP são descritas na tabela a seguir.

Tabela 125. Opções de propriedades do monitor SIP		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
ShowZeroes	0|1	Especifica a exibição de estatísticas do SIP sem valores. 0 - desativado 1 - ativado
Transportes	string	Lista os transportes de porta de protocolo locais separados por um espaço que é TCP ou UDP para o protocolo. São permitidos curingas para os números de porta. Padrão: UDP:*.

Conjuntos de Criptografia

A propriedade **SSLCipherSuite** especifica o conjunto de criptografia usado pelo monitor SIP. Para obter mais informações, consulte “Configuração de SSL no Internet Service Monitoring” na página 436.

Configurando Testes de Serviço do Monitor SIP

Utilize os parâmetros de configuração do monitor SIP para definir testes de serviço.

Tabela 126. Configuração do Monitor SIP

Campo	Descrição
servidor	Especifica o nome do servidor que será testado. Por exemplo, `sip1.mycompany.com`.
serverport	A porta pela qual o monitor de SIP pode chegar ao servidor que será testado.
nome do usuário	Especifica o número da extensão ou a identidade da conta do monitor SIP que faz a chamada. Por exemplo, `jblogg`.
target	Especifica o número da extensão de um dispositivo ativado por SIP usado para fazer uma chamada. Por exemplo, 5551234.
senha	Especifica a senha para o nome de usuário.
description	Um campo de texto para fornecer informações descritivas sobre o elemento. Por exemplo, `SIP monitor`.
proxy	O nome do host do servidor proxy. Por exemplo, `proxy.mycompany.com`.
proxyport	A porta pela qual o monitor de SIP pode chegar ao servidor proxy.
timeout	O tempo, em segundos, para aguardar para que o servidor responda. Padrão: 30
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: 300
failureretests	O número de vezes para retestagem antes de a falha ser indicada. Padrão: 0
Intervalo de retestagem	O tempo de espera, em segundos, entre cada novo teste que falha. Padrão: 10

Classificação de nível de serviço

As classificações de nível de serviço definem as regras para determinar o nível de serviço fornecido sobre o SIP.

As opções de classificação em nível de serviço disponíveis para o monitor SIP são:

```
totalTime
Mensagem
```

Nas classificações em nível de serviço:

- Especifique mais classificações de nível de serviço inserindo manualmente o nome do elemento de monitor. O nome deve corresponder ao nome mostrado para o elemento na seção Elementos do Monitor.
- `message` pode ser qualquer mensagem encaminhada no elemento **`$message`** para o servidor IBM Application Performance Management se usado em qualquer widget. Para obter uma lista de valores possíveis, consulte Mensagens de status.
- O operando é uma cadeia ou um número positivo.

Elementos do Monitor

Além dos resultados de testes comuns a todos os elementos, o monitor SIP gera um conjunto de resultados de testes contendo dados específicos para testes de serviços SIP.

A tabela a seguir descreve os elementos adicionais para o monitor SIP.

Tabela 127. Elementos do Monitor SIP

Elemento	**Descrição**
$AcceptReg	O número de pedidos de registro SIP aceitos.
$AuthTime* (AuthenticationTime)	O tempo utilizado para autorizar o monitor SIP e o dispositivo ativado pelo SIP.
$authAttempts	O número de vezes que o monitor precisou reenviar um pedido para incluir suas credenciais.
(CallSetupTime)	O tempo utilizado para configurar uma chamada.
$Invalid	O número de pedidos inválidos enviados e recebidos.
$InvalidReg	O número de pedidos de registro SIP inválidos.
$lastMethod	O último método visto pelo monitor que não era BYE ou ACK.
$lastSequence [METHOD]	A última sequência recebida para um método.
$lastStatus [METHOD]	O último status recebido para um método ou geral.
$method *METHOD*	Grupo de mensagens vistas para um método.
$optionsTime* (OptionsTime)	O tempo levado para negociar uma mudança de opções (OPTIONS para 200 OK).
$postDialTime* (PostDialTime)	O tempo levado para receber um sinal de toque após a discagem (INVITE para 180 Ringing).
$RegTime* (RegistrationTime)	O tempo utilizado para registrar o monitor SIP e o dispositivo ativado pelo SIP.
$registrationTime	O tempo levado para registrar com o servidor (REGISTER para 200 OK).
$Requests	O número de mensagens de solicitação do SIP recebidas e enviadas.
($RequestsSent)	O número de mensagens de Pedidos SIP enviadas.

Tabela 127. Elementos do Monitor SIP (continuação)	
Elemento	**Descrição**
`${request|response}[Sent|Received|Transmitted|Total][METHOD][STATUS]`	Registro de mensagens vistas para várias categorias, por exemplo, `requestSentINVITE = 1`, `responseReceived = 10` e `responseReceivedBYE200 = 1`.
$Responses	O número de mensagens de resposta do SIP recebidas e enviadas.
($ResponseReceived)	O número de mensagens de Respostas SIP recebidas.
$sessionAnswered	• 1 - se a chamada for atendida • 0 - se a chamada não for atendida
$sessionCreated	• 1 - se uma sessão for estabelecida • 0 - se uma sessão não for estabelecida
$sessionTerminated	• 1 - se a sessão terminar • 0 - se a sessão não terminar
$shutdownTime* (`ShutdownTime`)	O tempo levado para terminar a conexão (BYE para 200 OK).
$terminatedReason* (TerminatedReason)	O motivo do fechamento da conexão.
(Username)	O nome do usuário utilizado para efetuar login no servidor SIP.
(Target)	O destino no qual abrir a sessão.

Mensagens de Status

O monitor SIP fornece mensagens de status no atributo **`ResultMessage`** ao usar IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

A tabela a seguir descreve as mensagens de status do monitor SIP.

Tabela 128. Mensagens de Status do Monitor SIP	
Mensagem	**Descrição**
`Tempo limite do registro esgotado`	Houve falha do monitor ao registrar-se no servidor.
`Tempo limite do convite esgotado`	A mensagem INVITE esgotou o tempo limite.
0k	O pedido e a resposta foram bem-sucedidos.

Tabela 128. Mensagens de Status do Monitor SIP (continuação)	
Mensagem	**Descrição**
`n operation status description`	• *n* é a sequência de numeração da mensagem. • operation o tipo de mensagem. • status é o código de status. • description é uma descrição de texto sem formatação do status. Por exemplo, `1 INVITE 200 OK`.

Respostas do SIP

O monitor SIP suporta os seguintes tipos de resposta. Cada resposta possui um código de 3 dígitos:

- Respostas Informativas (100 - 199)
- Respostas Bem-sucedidas (200 - 299)
- Respostas de Redirecionamento (300 - 399)
- Respostas de Falha do Cliente (400 - 499)
- Respostas de Falha do Servidor (500 - 599)
- Respostas de Falha Global (600 - 699)

A tabela a seguir lista as respostas comuns do SIP.

Tabela 129. Respostas Comuns do SIP	
Resposta	**Descrição**
100 Tentando	A mensagem é recebida pelo dispositivo ativado por SIP, mas ainda deve ser processada.
180 Tocando	A mensagem é recebida e processada pelo dispositivo ativado por SIP. O dispositivo está tocando para alertar o usuário.
200 OK	Esse código é retornado na conclusão bem-sucedida de um método. Por exemplo, a chamada é registrada com o servidor ou o usuário respondeu a chamada.
401 Não-Autorizado	O usuário não está autorizado.
407 Autenticação de Proxy Obrigatória	Esse código é semelhante ao 401, mas indica que o usuário deve ser autenticado primeiro.
408 Tempo Limite de Solicitação	O usuário não respondeu a chamada.

Para obter uma lista completa de respostas do SIP, consulte a RFC3261.

Monitor SMTP

O monitor SMTP funciona em conjunto com os monitores IMAP4 ou POP3 para testar o desempenho de um serviço de e-mail.

A tabela a seguir lista os arquivos do monitor SMTP.

Tabela 130. Arquivos do Monitor SMTP	
Arquivos do Monitor	**Nome ou local**
Monitor executável	`nco_m_smtp`
Arquivo de Propriedades	`$ISHOME/etc/props/smtp.props`

Tabela 130. Arquivos do Monitor SMTP (continuação)	
Arquivos do Monitor	**Nome ou local**
Arquivo de regras	`$ISHOME/etc/rules/smtp.rules`
Arquivo de log	`$ISHOME/log/smtp.log`

Diretrizes para monitoramento do monitor SMTP

O monitor SMTP opera junto com os monitores POP3 ou IMAP4. Ele envia periodicamente uma mensagem de e-mail para uma caixa de correio no servidor de destino e registra o tempo levado para emitir a solicitação de e-mail de envio. O monitor POP3 ou IMAP4, então, lê as mensagens da caixa de correio e as usa para calcular o tempo de resposta e a disponibilidade do serviço de e-mail.

Nota: O monitor SMTP opera junto com os monitores POP3 ou IMAP4. Ele envia periodicamente uma mensagem de e-mail para uma caixa de correio no servidor de destino e registra o tempo levado para emitir a solicitação de e-mail de envio. O monitor POP3 ou IMAP4, então, lê as mensagens da caixa de correio e as usa para calcular o tempo de resposta e a disponibilidade do serviço de e-mail.

Caixas postais

Você pode configurar o monitor para enviar mensagens de e-mail para qualquer caixa de correio existente, mesmo que a caixa de correio pertença a um usuário real. No entanto, é recomendável criar uma conta de caixa de correio especial para teste de serviço. O parâmetro email especifica a caixa de correio do destinatário. Por padrão, o monitor envia mensagens de teste com a linha de assunto `Mensagem de teste do monitor SMTP`. Se necessário, é possível configurar elementos de perfil SMTP sem um nome de caixa de correio. Nessa configuração, o monitor simplesmente verifica se o serviço SMTP está aceitando conexões.

Mils Seguros

O monitor SMTP suporta conexões com serviços de correios seguros. Ele pode se conectar usando SSL/TLS, ou o comando STARTTLS. Ao definir um elemento de monitor SMTP, use o campo Tipo de segurança para selecionar a segurança apropriada. Se o servidor de e-mail requer um certificado de lado do cliente para criptografia SSL, use a propriedade SSL`name` ou as opções de linha de comando para especificar um arquivo de certificado, um arquivo-chave, uma senha de chave e um conjunto de cifras.

Certificado do lado do cliente

O monitor SMTP possibilita o monitoramento de servidores que requerem certificados do lado do cliente para autenticação mútua. O arquivo de certificado, o arquivo de chaves e a senha-chave são especificados quando você cria um elemento de perfil. Os certificados devem estar no formato Privacy Enhanced Mail (PEM). Se o certificado estiver em outro formato, deve-se convertê-lo para o formato PEM. Os certificados podem ser convertidos usando um software como o openSSL, que está disponível em http://www.openssl.org.

Nota: Se você sempre utilizar o mesmo certificado, chave e senha em todos os elementos do perfil, especifique-os utilizando as propriedades do monitor em vez de defini-las em cada elemento de perfil criado.

Configurar os testes de serviço do monitor SMTP

Utilize os parâmetros de configuração do monitor SMTP para definir testes de serviço. Quando você configura o monitor, os valores padrão são mostrados para os parâmetros de intervalo de sondagem e de tempo limite. Esses padrões são 30 e 300 segundos respectivamente. Se nenhum valor for especificado, outros padrões listados na tabela não serão mostrados durante a configuração, mas serão aplicados quando os detalhes de configuração forem salvos.

Tabela 131. Configuração do Monitor SMTP	
Campo	**Descrição**
servidor	O endereço IP do servidor de e-mail. O exemplo é `mail.mycompany.com`
description	Um campo de texto para fornecer informações descritivas sobre o elemento.
port	O número da porta do servidor de e-mail. Padrão: 25 Se você usar um servidor diferente de um servidor SMTP, atualize a porta na qual se conectará ao servidor. Por exemplo, se você usar um servidor IMAP4 sobre SSL para o Microsoft Exchange, especifique a porta 465.
securitytype	O tipo de conexão segura aberta com o servidor de e-mail: • `NONE` -Conectar-se sem segurança • `SSL` - Enviar um SSLv2 `hello` e, em seguida, negociar SSLv2, SSLv3 ou TLSv1 • `STARTTLS` - Conectar sem segurança, emitir um comando `STARTTLS` e, em seguida, estabelecer uma conexão no TLSv1 Padrão: `NONE`
nome do usuário	O nome de usuário utilizado para efetuar login no servidor SMTP. Usado com a autenticação `PLAIN` ou `CRAM-MD5` .
senha	A senha utilizada para efetuar login no servidor SMTP. Usado com a autenticação `PLAIN` ou `CRAM-MD5` .
Tipo de autenticação	O método para autenticar o monitor para o servidor SMTP. As opções disponíveis são: • `NONE` -Nenhuma autenticação é tentada • `PLAIN` - Autenticação de nome de usuário e senha do texto simples • `CRAM-MD5`-A autenticação CRAM-MD5 é usada O valor padrão é `NONE`.
Segredo compartilhado	A chave de segredo compartilhada para a autenticação CRAM-MD5.
email	O endereço de e-mail da caixa de correio usada pelos monitores SMTP e POP3.
timeout	O tempo de espera, em segundos, pela resposta do servidor SMTP. Padrão: `30`
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: `300`
failureretests	O número de vezes para testar novamente antes de indicar uma falha. Padrão: `0`

Tabela 131. Configuração do Monitor SMTP (continuação)	
Campo	**Descrição**
Intervalo de retestagem	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: 10

Nota: Monitore a disponibilidade do servidor de e-mail `mail.mycompany.com` tentando se conectar a ele em intervalos de 10 minutos. Use um tempo limite de conexão de 30 segundos e, se a conexão falhar, tente novamente três vezes com 5 segundos entre cada nova tentativa.

Elemento do Monitor

Além dos resultados de teste comuns a todos os elementos, o monitor SMTP gera um conjunto de resultados de teste contendo dados específicos para testes de serviço do SMTP.

A tabela a seguir descreve os elementos adicionais para o monitor SMTP.

Tabela 132. Elementos do Monitor SMTP	
Elemento	**Descrição**
`$authentication`	O tipo de método de autenticação de usuário exigido pelo servidor SMTP (`Standard` ou `APOP`).
`$bytesPerSec`	O número médio de bytes transferidos por segundo.
`$bytesTransferred`	O número de bytes transferidos por upload ou download.
`$connectTime*` (`ConnectTime`)	O tempo utilizado para conectar-se ao servidor SMTP.
`$email*` (`EmailAddress`)	O endereço de e-mail da caixa de correio para a qual o monitor envia o e-mail de teste.
`$lookupTime*` (`LookupTime`)	O tempo utilizado para obter o endereço IP do servidor host.
`$port*` (`Porta`)	A porta na qual o serviço é monitorado.
`$responseTime*` (`ResponseTime`)	O tempo gasto, após a criação de uma conexão, até que o primeiro byte do e-mail de teste possa ser enviado para o servidor SMTP.
`$security`	O tipo de conexão segura aberta com o servidor de e-mail (`NONE`, `STARTTLS` ou `SSL`) conforme configurado no campo **securitytype** do elemento de perfil.
`$SSLHandshakeTime*` (`SslHandshakeTime`)	O tempo utilizado para estabelecer a conexão SSL.
`$status*` (`ResultStatus`)	O código de status retornado pelo servidor SMTP.

Tabela 132. Elementos do Monitor SMTP (continuação)	
Elemento	**Descrição**
$uploadTime* (UploadTime)	O tempo utilizado para fazer upload do arquivo.
$user* (SmtpUser)	O nome de usuário (nome da conta) usado pelo monitor para efetuar login no servidor SMTP.

Mensagem de status

O monitor SMTP fornece mensagens de status no elemento $message ao usar o IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

Propriedades

As propriedades específicas para o monitor SMTP são descritas na tabela a seguir.

Tabela 133. Propriedades do Monitor SMTP e Opções da Linha de Comandos		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
MailMessage Path	string	Caminho para um arquivo que contém texto para enviar no e-mail de teste. Uma mensagem padrão será enviada se ele não estiver configurado.
Originator	string	Especifica o campo From a ser configurado ao enviar o e-mail de teste. Certifique-se de que corresponda à cadeia correspondente no monitor IMAP4. Padrão: SMTP-Monitor.
SSLCertificate File	string	O caminho e o nome do arquivo de certificado digital utilizado se nenhum certificado for especificado explicitamente para um elemento SMTP durante sua criação. Se o caminho não for absoluto, o monitor o interpretará com relação ao diretório ativo ($ISHOME/platform/arch/bin).
SSLCipherSuite	string	O conjunto de criptografia a ser utilizado para operações SSL. Para obter uma descrição dos valores possíveis, consulte Conjuntos de cifras. Padrão: RC4:3DES:DES:+EXP
SSLDisableTLS	integer	Desativa o TLSv1 para o suporte legado. Padrão: 0 -TLSv1 está ativado. 1 TLSv1 está desativado.
SSLKeyFile	string	O arquivo que contém a chave privada SSL.
SSLKeyPassword	string	A senha utilizada para criptografar a chave privada SSL.
UseBody	integer	Especifica onde o monitor grava informações de rastreamento na mensagem de correio, no cabeçalho do email ou no corpo do email. Padrão: 0 - as informações são incluídas no cabeçalho do email. 1 - grave informações no corpo do e-mail.

Conjuntos de Criptografia

A propriedade `SSLCipherSuite` especifica o conjunto de criptografia utilizado pelo monitor SMTP. Para obter mais informações sobre as configurações de SSL, consulte "Configuração de SSL no Internet Service Monitoring" na página 436.

Monitor SNMP

O monitor SNMP testa os dispositivos ativados por SNMP para dados de falha e desempenho.

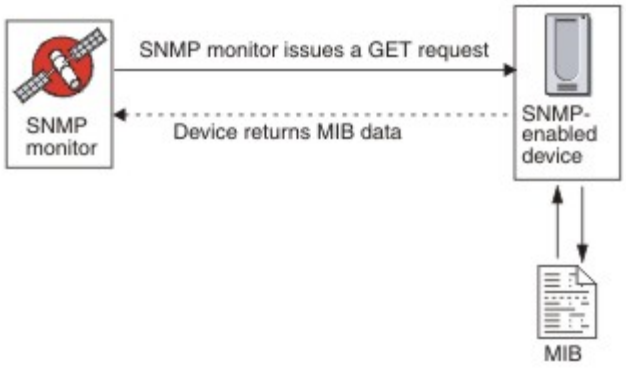
A tabela a seguir lista os arquivos do monitor SNMP.

Tabela 134. Resumo do Monitor SNMP

Arquivos do Monitor	**Nome ou local**
Monitor executável	`nco_m_snmp`
Arquivo de Propriedades	`$ISHOME/etc/props/snmp.props`
Arquivo de regras	`$ISHOME/etc/rules/snmp.rules`
Arquivo de log	`$ISHOME/log/snmp.log`

Diretrizes para a configuração do monitor SNMP

O monitor SNMP adquire dados dos dispositivos ativados por SNMP enviando solicitações SNMP GET para um ou mais objetos contidos no MIB do dispositivo. O dispositivo retorna então os dados MIB para o monitor SNMP. O monitor SNMP suporta versões SNMP 1, 2c e 3.



Propriedades

As opções de propriedades específicas para o monitor SNMP estão descritas na tabela a seguir.

Tabela 135. Opções de propriedades do monitor SNMP

Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
Valor InvalidBps	integer	Especifica um valor de número inteiro que é substituído para cálculos de valor de bits por segundo (Bps) quando apenas um ponto de dados está disponível.
MibDir	string	Especifica o diretório que contém documentos MIB usados pelo monitor. Padrão: `$ISHOME/mibs`.

Tabela 135. Opções de propriedades do monitor SNMP (continuação)		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
StripQuotes	`0|1`	Extrai caracteres de aspas dos dados de número inteiro. `0` - desativado 1 -ativado
Limite de Rolagem	integer	O valor que um delta deve atender ou exceder se a rolagem acontecer antes da reconfiguração de um roteador. Padrão: `0` (nunca deslocar)

Configurando Testes de Serviço do Monitor SNMP

Utilize os parâmetros de configuração do monitor SNMP para definir testes de serviço.

Tabela 136. Configuração do Monitor SNMP	
Campo	**Descrição**
servidor	O servidor para enviar pedidos GET do SNMP to.
objectgroupname	O nome do texto para o grupo de OIDs a serem incluídos no pedido GET.
sequência de comunidades	A sequência da comunidade de leitura/gravação SNMP para o servidor SNMP no cliente. **Nota:** Use o caractere de acento circunflexo (^) nos nomes de comunidade com cautela; consulte Nomes de comunidade para obter informações adicionais.
description	Um campo de texto para fornecer informações descritivas sobre o elemento.
port	A porta a ser utilizada no servidor. Padrão: 161
versão	A versão SNMP a ser usada: 1 - SNMPv1 2 - SNMPv2c 3 - SNMPv3 Padrão: 1
securityname†	O nome do usuário para a sessão SNMP.
authenticationphrase†	A senha de autenticação para o usuário.
privacyphrase†	A senha de privacidade para o usuário.
authenticationprotocol†	O protocolo a ser usado para autenticar o usuário: • MD5 • SHA1 Padrão: MD5

Tabela 136. Configuração do Monitor SNMP (continuação)

Campo	Descrição
privacyprotocol†	O protocolo a ser utilizado para criptografar a sessão. Padrão: DES
timeout	O tempo, em segundos, para aguardar para que o servidor responda. Padrão: 20
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: 300
tentar novamente	O número de vezes que o monitor tenta contatar o servidor novamente antes de encerrar. Padrão: 0
failureretests	O número de vezes para retestagem antes de a falha ser indicada. Padrão: 0
Intervalo de retestagem	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: 10
hostnamelookuppreference	Determina qual versão de IP, IPv6 ou IPv4, é aplicada ao nome do host fornecido. As opções são: • `default` configura o monitor para utilizar configurações de propriedades em todo o monitor. Este é o padrão. • `4Then6` seleciona IPv4 e, em seguida, IPv6. Utiliza endereços IPv4, se eles estiverem disponíveis. Se não forem localizados endereços IPv4, endereços IPv6 serão utilizados. • `6Then4` seleciona IPv6 e, em seguida, IPv4. Utiliza endereços IPv6, se eles estiverem disponíveis. Se não forem localizados endereços IPv6, endereços IPv4 serão utilizados. • `40nly` seleciona apenas IPv4. Usa endereços IPv4 apenas. Se não houver endereços IPv4, a pesquisa retorna um erro. • `60nly` seleciona apenas IPv6. Usa apenas endereços IPv6. Se não houver endereços IPv6, a pesquisa retorna um erro. • `60r4` seleciona IPv4 ou IPv6. Usa o primeiro endereço retornado do nome do host.
† Aplicável apenas ao SNMPv3.	

Nomes de comunidades

Monitoramento de Serviço da Internet usa o caractere de acento circunflexo (^) como um caractere de escape, já que envia informações para o dispositivo de destino. Se um nome de comunidade contiver um til, você deverá digitar dois tils em uma linha (^^) para que o nome fique correto no roteador. Por exemplo, para que o nome da comunidade a$^&b fique correto quando enviado para o dispositivo, use a$^^&b.

Classificações em Nível de Serviço

As classificações em nível de serviço definem as regras para determinar o nível de serviço.

As opções de classificação em nível de serviço disponíveis para o monitor SNMP são:

```
totalTime
Mensagem
```

Nas classificações em nível de serviço.

- Especifique mais classificações de nível de serviço inserindo manualmente o nome do elemento de monitor. O nome deve corresponder ao nome mostrado para o elemento na seção Elementos do Monitor.
- `message` pode ser qualquer mensagem encaminhada no elemento **`$message`** para o servidor IBM Application Performance Management se usado em qualquer widget. Para obter uma lista de valores possíveis, consulte Mensagens de status.
- O operando é uma cadeia ou um número positivo.
- oidName é o nome designado a um objeto MIB no campo Nome do OID definido no grupo OID.

Elementos do Monitor

Além dos resultados de teste comuns a todos os elementos, o monitor SNMP gera um conjunto de resultados de teste contendo dados específicos para os testes de serviço SNMP.

A tabela a seguir descreve os elementos adicionais para o monitor SNMP.

Tabela 137. Elementos do Monitor SNMP

Elemento	**Descrição**
$community	A cadeia de comunidades SNMP para o servidor SNMP no cliente.
$numOids	O número de OIDs utilizados na consulta.
$oidGroupName* (OidGroup)	O nome do grupo OID. O grupo de OIDs contém os OIDs que o monitor está sondando.
$oidName*0 a n** (OIDName*Zero a Nove*)	O nome do primeiro ao último objeto MIB no grupo de OIDs. É indicado por um número durante o uso do Netcool/OMNIbus e por um texto alfabético (zero a nove) durante o uso do IBM Application Performance Management.
$oidNames	Os nomes de cada OID separados por uma barra vertical (|).
$oidReturnValues*0 a n** (snmpResult*Zero a Nove*)	Os dados que são retornados pelo comando SNMP GET para o primeiro objeto MIB no grupo OID. Isto é indicado por um número ao utilizar o Netcool/OMNIbus e por texto alfabético (zero a nove) ao utilizar o IBM Application Performance Management.
$oidUnit*0 a n*	As unidades do primeiro ao último objeto MIB no grupo de OID indicado por um número.
$oidUnits	As unidades de cada OID, separadas por um caractere de barra vertical (|).
$port	A porta na qual o serviço é monitorado.
$snmpVersion* (SnmpVersion)	Versão do SNMP utilizada para enviar pacotes SNMP configurados no perfil (Versão 1, 2c ou 3).

Mensagem de status

O monitor SNMP fornece mensagens de status no atributo `ResultMessage` durante o uso do IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

A tabela a seguir descreve as mensagens de status do monitor SNMP.

Tabela 138. Mensagens de Status do Monitor SNMP

Mensagem	**Descrição**
`Obtenção bem-sucedida`	A consulta do agente do SNMP foi bem-sucedida.
`Falha ao abrir sessões snmp` `Sessão SNMP - falha ao iniciá-la`	Não é possível inicializar a sessão SNMP.
`Erro no pacote`	Não é possível criar um pacote SNMP válido.
`Tempo limite esgotado ao aguardar resposta`	Nenhuma resposta recebida do agente do SNMP.
`Erro Interno`	Esse era um erro interno do monitor. Para obter informações adicionais, entre em contato com o Suporte Técnico IBM.
`Erro ao Processar o OID`	Houve um erro ao processar um dos `OIDs`.
`ERRO: OIDs em Excesso`	O monitor está configurado para solicitar muitos `OIDs` de uma vez. O máximo é `100`.
`ERRO: Incompatibilidade de PDU recebida com PDU enviada`	A Protocol Data Unit (PDU) recebida pelo monitor não correspondeu com a PDU enviada ao servidor.

Monitor SOAP

O monitor SOAP verifica a disponibilidade e o tempo de resposta da interface SOAP (SOAP 1.0 e 1.1). Ele também monitora a validade de entradas SOAP (pedidos) e as saídas SOAP (respostas).

O monitor SOAP suporta os seguintes estilos de codificação de mensagem:

- RPC - Codificado
- Documento - Não Agrupado Literal
- Documento - Agrupado Literal

A tabela a seguir lista os arquivos do monitor SOAP.

Tabela 139. Resumo do Arquivo do Monitor SOAP

Arquivos do Monitor	**Nome ou local**
Monitor executável	`nco_m_soap`
Arquivo de Propriedades	`$ISHOME/etc/props/soap.props`
Arquivo de regras	`$ISHOME/etc/rules/soap.rules`
Arquivo de log	`$ISHOME/log/soap.log`

Recomendações para Configuração do Monitor SOAP

O monitor SOAP testa a operação de um serviço SOAP enviando à interface SOAP de destino uma solicitação contendo um conjunto de entradas e, depois, recebendo e analisando as saídas contidas na resposta recebida da interface. Quando uma solicitação é enviada para a interface SOAP, a solicitação pode ter falhas ou êxito. Um pedido é bem-sucedido se uma resposta for recebida e os valores na mensagem de resposta corresponderem aos valores de saída especificados. Um pedido falha se nenhum resposta for recebida ou uma resposta for recebida mas os valores em sua mensagem não corresponderem aos valores de saída.

As entradas e saídas SOAP contidas em solicitações e respostas dependem das funções do serviço SOAP em teste, e quanto você projeta um teste para um serviço SOAP, é necessário especificar entradas e saídas apropriadas para esse serviço. As entradas consistem nos nomes dos dados que serão enviados e em seus valores de entrada atribuídos. As saídas consistem nos nomes dos dados que serão recebidos e em seus valores de saída esperados. Esses nomes de dados são originados de um arquivo Web Service Description Language (WSDL) local, que você especifica ao configurar o monitor SOAP. Os nomes de dados de entrada e saída devem corresponder aos nomes e tipos de dados no arquivo WSDL. Os nomes dos dados também devem estar na mesma ordem do arquivo WSDL. Se os nomes não corresponderem, ou a ordem estiver incorreta, uma mensagem de erro será gerada quando o monitor tenta sondar a interface SOAP.

O formato de entrada é:

```
dataname:datatype=assigned_value, dataname:datatype=assigned_value, ...
```

O formato de saída é:

```
dataname:datatype=expected_value, dataname:datatype=expected_value, ...
```

Tipos de Dados SOAP

O monitor SOAP suporta tipos de dados simples, matrizes e definidos pelo usuário. Os tipos de dados simples incluem Integer, String e Boolean. Matrizes podem conter tipos de dados simples e outros tipos de matrizes e dados definidos pelo usuário.

Tabela 140. Tipos de Dados Simples

Tipos de Dados Simples			
anyURI	flutuação	idioma	Qname
booleano	gDay	long	short
byte	gMonth	Nome	string
Data	gMonthDay	NCName	hora
dateTime	gYear	negativeInteger	token
decimal	gYearMonth	NMTOKEN	unsignedByte
duplo	ID	NMTOKENS	unsignedInt
duration	IDREFS	nonNegativeInteger	unsignedLong
ENTITIES	int	nonPostiveInteger	unsignedShort
ENTITY	integer	normalizedString	

Autenticação SOAP

Se a interface SOAP que você deseja monitorar requerer autenticação HTTP básica, especifique credenciais para acessar a interface no elemento de perfil SOAP ao usar a ferramenta de configuração do Monitoramento de Serviço da Internet.

Para configurar os parâmetros de autenticação SOAP necessários:

1. Na ferramenta de Configuração Monitoramento de Serviço da Internet, selecione o elemento de perfil para o qual deseja incluir as informações sobre autenticação.
2. Na guia **Avançado**, clique no campo **Valor** para o parâmetro `nome de usuário` e insira o valor necessário.
3. Clique no campo **Valor** para o parâmetro `password` e insira o valor necessário. A senha é criptografada.
4. Clique em **OK**.

Se a autenticação não for mais necessária, exclua os valores para os parâmetros **`username`** e **`password`**.

Propriedades

As opções de propriedades específicas para o monitor SOAP são descritas na tabela a seguir.

Tabela 141. Opções de propriedades do monitor SOAP

Nome da propriedade	Parâmetro de propriedade	Descrição	Padrão
SoapParser	string	Biblioteca de análise XML.	`$ISHOME/platform/$ARCH/bin/AxisXMLParserXerces.dll`
SoapTransport	string	Biblioteca de transporte SOAP.	`$ISHOME/platform/$ARCH/bin/HTTPTransport.dll`
SoapChannel	string	Biblioteca de canal SOAP	`$ISHOME/platform/$ARCH/bin/HTTPChannel.dll`
SoapSecureChannel	string	Biblioteca de canal seguro SOAP.	`$ISHOME/platform/$ARCH/bin/HTTPSSLChannel.dll`
SoapClientLog	string	O nome do arquivo de log do cliente SOAP extra.	`$ISHOME/log/SoapClient.log`

Conjuntos de Criptografia

A propriedade `SSLCipherSuite` especifica o conjunto de criptografia usado pelo monitor SOAP.

Para obter mais informações, consulte "Configuração de SSL no Internet Service Monitoring" na página 436.

Configurando testes de serviços do monitor SOAP

Utilize os parâmetros de configuração do monitor SOAP para definir testes de serviço.

Tabela 142. Configuração do Monitor SOAP

Elemento	Descrição
wsdl	O caminho para uma cópia local do arquivo WSDL.

Tabela 142. Configuração do Monitor SOAP (continuação)	
Elemento	**Descrição**
operação	O nome da operação SOAP.
operationnamespace	O espaço de nomes da operação SOAP.
local	A URL do serviço SOAP a ser monitorado.
description	Um campo de texto para fornecer informações descritivas sobre o elemento.
timeout	O tempo, em segundos, para aguardar até que o serviço SOAP responda. Padrão: `10`
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: `300`
failureretests	O número de vezes para retestagem antes de a falha ser indicada. Padrão: `0`
Intervalo de retestagem	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: `10`
Parâmetros do Soap	

inputs	Fornece acesso ao nome, tipo e campos de valor, incluindo atributos, para entrada de SOAP. Use parâmetros de SOAP simples, complexos, ou de matriz. Por exemplo:
	• Simples: `symbol:string="IBM"`
	• Complexo:
	`outer:{item1:string,item2:string}(aaa:string='bbb')`
	`={item1(attr:string='ccc')='',`
	`item2(attr:string='ddd',attr2:string='eee')='fff'}`
	Neste exemplo os atributos entre parênteses, marcados em negrito, são opcionais.
	• Matriz: `input:int[]=[1,2,3,4]`

outputs	Fornece acesso ao nome, tipo e campos de valor, incluindo atributos, para saída de SOAP. Use parâmetros de SOAP simples, complexos, ou de matriz. Para obter mais informações sobre sintaxe, consulte os exemplos para as entradas de parâmetros SOAP.

Classificação de nível de serviço

As classificações de nível de serviço definem as regras para determinar o nível de serviço fornecido pela interface SOAP.

As opções de classificação em nível de serviço disponíveis para o monitor SOAP são:

```
totalTime
Mensagem
```

Nas classificações em nível de serviço:

- Especifique mais classificações de nível de serviço inserindo manualmente o nome do elemento de monitor. O nome deve corresponder ao nome mostrado para o elemento na seção Elementos do Monitor.
- `message` pode ser qualquer mensagem no elemento **`$message`** para o servidor IBM Application Performance Management se usado em qualquer widget. Para obter uma lista de valores possíveis, consulte Mensagens de status.

Elementos do Monitor

Além dos resultados de teste comuns a todos os elementos, o monitor SOAP gera um conjunto de resultados de teste que contêm dados específicos para testes de serviço SOAP.

A tabela a seguir lista os elementos adicionais para o monitor SOAP.

Tabela 143. Elementos do Monitor SOAP

Elemento	**Descrição**
(Location)	A URL do serviço SOAP que é monitorado.
(Operation)	O nome do serviço SOAP que é monitorado.
$outputMatch	`Sucesso` se o valor retornado corresponder ao valor de saída, caso contrário, `Falha`.
$responseValueName	O nome do valor recebido na resposta SOAP.
$soapname	O nome do contêiner na resposta SOAP. Aplicável somente à matriz e aos tipos de dados complexos definidos pelo usuário.
$soaptype	O tipo de contêiner na resposta SOAP. Aplicável somente à matriz e aos tipos de dados complexos definidos pelo usuário.
(WSDL)	O caminho para uma cópia local do arquivo WSDL.

Mensagens de Status

O monitor SOAP fornece mensagens de status no atributo **`ResultMessage`** durante o uso do IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

As mensagens são `Sucesso` se os valores retornados corresponderem aos valores de saída ou uma mensagem de erro. A mensagem de erro contém uma descrição do erro.

Exemplo

Monitore a disponibilidade da interface SOAP em intervalos de cinco minutos. Se a interface SOAP estiver indisponível, repita o teste no máximo duas vezes, aguardando cinco segundos entre cada teste repetido. Envie um pedido que inclua 1 + 2 e verifique se a resposta contém o valor 3.

Crie um elemento de perfil SOAP e configure os campos mostrados na tabela a seguir.

Tabela 144. Exemplo de Elemento de Perfil SOAP

Campo de Configuração	**Valor**
wsdl	`c:\%ISMHOME%\etc\SOAP.wsdl`
operação	add
operationnamespace	`http://localhost/SOAP/Calculator`
local	`http://serverA/SOAP/Calculator`

Tabela 144. Exemplo de Elemento de Perfil SOAP (continuação)	
Campo de Configuração	**Valor**
description	Monitor SOAP de calculadora básica
Ativo	Selected
timeout	30
Pesquisar	300
failureretests	2
Intervalo de retestagem	5
inputs	[in0=1,in1=2]
outputs	[addReturn=3]

Monitor TCPPort

O monitor TCPPort fornece cobertura para serviços que não são testados por outros monitores. Ele detecta e responde aos comandos ou cadeias em uma porta TCP. Esse monitor é particularmente útil para serviços de indicação de monitoramento.

A tabela a seguir lista os arquivos do monitor TCPPort.

Tabela 145. Arquivos do Monitor TCPPort	
Arquivos do Monitor	**Nome ou local**
Monitor executável	`nco_m_tcpport`
Arquivo de Propriedades	`$ISHOME/etc/props/tcpport.props`
Arquivo de regras	`$ISHOME/etc/rules/tcpport.rules`
Arquivo de log	`$ISHOME/log/tcpport.log`

Diretrizes para Configurar o Monitor TCPPort

O monitor TCPPort testa serviços baseados em TCP conectando-se ao serviço, monitorando mensagens recebidas do serviç e enviando respostas para ele.

Para configurar um teste, defina uma sequência de mensagens esperadas e respostas que abrangem uma interação normal nesse serviço.

Por exemplo, uma interação padrão para um serviço telnet envolve a seguinte sequência:

- O serviço telnet envia uma mensagem de login, solicitando um nome de usuário.
- O cliente envia uma resposta com um nome de usuário.
- O serviço telnet envia uma mensagem que solicita uma senha.
- O cliente envia uma resposta que contém uma senha.
- Se a tentativa de login for bem-sucedida, o serviço telnet envia algum tipo de mensagem de boas-vindas.

As propriedades **`WaitForn`** e **`Sendn`** do monitor que são especificadas definem as mensagens esperadas e as respostas para essas mensagens. Essas propriedades no arquivo de propriedades do monitor definem como o monitor interage com o serviço TCP:

- As propriedades **WaitForn** são expressões regulares. O monitor as usa para corresponder às mensagens recebidas na porta monitorada.
- As propriedades **Sendn** são sequências literais que o monitor grava na porta.

Nota: Se for necessário, é possível inserir caracteres de controle nessas propriedades usando um editor de texto que suporte inserção de caractere de controle.

O formato para definir as propriedades WaitForn e Sendn é:

```
WaitFor1: 1st received message
Send1: 1st response
WaitFor2: 2nd received message
Send2: 2nd response
...
WaitFor5: 5th received message
Send5: 5th response
```

Quando o monitor atinge a primeira propriedade **WaitFor** indefinida, pára o envio e o recebimento. Se a propriedade **MonitorDisconnect** for configurada para 0, o serviço monitorado deverá encerrar a conexão aberta pelo monitor, caso contrário, o monitor reportará a mensagem `Timed out waiting to read` em seu elemento **$message**. Com muitos serviços, a conexão pode ser encerrada com o envio de um comando `quit`. Se **MonitorDisconnect** for configurada como 1, o monitor desconectará depois que o último comando Send ou `WaitFor` for concluído ou quando o tempo limite for atingido, o que ocorrer primeiro.

Configurando o Teste de Serviço do Monitor TCPPort

Utilize os parâmetros de configuração do monitor TCPPort para definir testes de serviço.

Tabela 146. Configuração de TCPPort

Campo	Descrição
servidor	O endereço IP do sistema no qual o serviço de destino está em execução. O exemplo é `server.mycompany.com`
port	A porta na qual o serviço de destino será conectado.
description	Um campo de texto para fornecer informações descritivas sobre o elemento.
timeout	O tempo, em segundos, para aguardar para que o servidor responda. Padrão: `30`
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: `300`
failureretests	O número de vezes para retestagem antes de a falha ser indicada. Padrão: `0`
Intervalo de retestagem	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: `10`

Nota: Monitore a disponibilidade do serviço `telnet` que é executado no host `server.mycompany.com` na porta 23. Use as credenciais `user` ou `guest` para efetuar login no servidor e feche a conexão imediatamente após o login. Execute o teste em intervalos de 5 minutos e configure um tempo limite de 10 segundos nas tentativas de conexão.

1.Inclua as entradas a seguir no arquivo de propriedades TCPPort:

```
WaitFor1: ".*[Ll]ogin:"
Send1: "user"
WaitFor2: ".*[Pp]assword:"
Send2: "guest"
WaitFor3: ".*%"
Send3: "exit"
```

2.Inicie ou reinicie o monitor TCPPort.

Correspondências de expressão regular

Execute uma procura de expressão regular nas informações transferidas por download inserindo até 50 expressões regulares diferentes. O monitor TCPPort tenta corresponder ao conteúdo que são recuperados para cada uma das expressões regulares. Se uma correspondência para uma expressão comum especificada for encontrada, as linhas correspondentes (ou o máximo que couber no buffer interno do monitor) serão retornadas no elemento `$regexpMatchn` correspondente. Se a expressão comum corresponder mais de uma vez nas informações transferidas por download, apenas a primeira será retornada. O status de cada teste de expressão regular é indicado pelos elementos `$regexpStatusn`. Você pode utilizar as correspondências de expressões comuns e suas informações de status como critérios para as classificações em nível de serviço.

Para obter mais informações, consulte Tabela 50 na página 325.

Elementos do Monitor

A tabela a seguir descreve os elementos adicionais para o monitor TCPPort.

Elementos indicados por um asterisco (*) estão disponíveis como atributos. Os nomes dos atributos são mostrados entre colchetes. A ausência de um asterisco indica que não há nenhum atributo equivalente. Os atributos que são mostrados entre colchetes, mas sem um elemento, indicam que eles estão disponíveis somente como atributos e que não há elementos equivalentes.

Além dos resultados de teste comuns a todos os elementos, o monitor TCPPort gera um conjunto de resultados de teste que contêm dados específicos para testes de serviço TCPPort.

Tabela 147. Elementos do Monitor TCPPort

Elemento	Descrição
`$bytesPerSec`	O número médio de bytes transferidos por segundo.
`$bytesTransferred`	O número de bytes transferidos por upload ou download.
`$connectTime*(ConnectTime)`	O tempo gasto para estabelecer um conexão com o servidor de destino.
`$downloadTime*(DownloadTime)`	O tempo gasto para fazer download de dados.
`$lastlineThere's`	O conteúdo da última linha recebida do servidor de destino.
`$lookupTime*(LookupTime)`	O tempo utilizado para obter o endereço IP do servidor host.
`$networkError`	Contém quaisquer erros de rede durante a conexão.
`$port*` `(Porta)`	A porta no servidor de destino à qual o monitor tentou conectar-se.
`$waitingFor`	Se a conexão for finalizada antes de o monitor concluir sua sequência de esperas e envios, esse elemento terá o conteúdo da última propriedade `WaitFor`.

Mensagem de status

O monitor TCPPort fornece mensagens de status no atributo `ResultMessage` ao usar o IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

A tabela a seguir descreve as mensagens de status TCPPort.

Tabela 148. Mensagens de Status do Monitor TCPPort	
Mensagem	**Descrição**
`Ok`	A solicitação foi bem-sucedida.
`Tempo limite esgotado ao aguardar leitura/gravação`	Uma conexão de dados com o servidor foi estabelecida, mas não responde.
`Conexão encerrada inesperadamente`	A conexão com o servidor foi interrompida.
`Conexão com falha`	O monitor falhou ao se conectar ao servidor. Para obter informações adicionais, consulte o arquivo de log.
`Network connect error`	Há um problema com a rede.
`Network error whilst reading`	

Propriedades

As opções de propriedades específicas para o monitor TCPPort são descritas na tabela a seguir.

Tabela 149. Propriedades de TCPPort		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
`Desconexão do Monitor`	`0`|`1`	Especifica que o monitor deve se desconectar após o último comando Send ou `WaitFor`. Se o último comando for um Send, o monitor se desconectará imediatamente após a cadeia ser enviada. Se o último comando for um `WaitFor`, o monitor se desconectará assim que o monitor receber uma correspondência ou quando o tempo limite de sondagem for excedido. `0` -desativado (o monitor não se conecta) `1` - ativado
`OutputDirectory`	string	Especifica o diretório de saída a ser utilizado se o `OutputResult` for salvo. Padrão: `$ISHOME/var`.
`OutputResult`	`0`|`1`	Especifica que o monitor deve salvar os dados que recebe do serviço. `0` - desativado `1` -ativado
Send	*n*	Cadeia literal que o monitor grava para a porta. Consulte Diretrizes para configurar o monitor TCPPort . n é um número no intervalo de 1 a 30 inclusivo.

Tabela 149. Propriedades de TCPPort (continuação)		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
`singleLineMatch`	`0|1`	Especifica que o monitor deve retornar uma correspondência de única linha quando uma expressão comum é correspondida. `0` - desativado (várias linhas são correspondidas) `1` - ativado (uma única linha é correspondida)
`WaitFor`	*n*	A expressão comum utilizada para corresponder comandos ou cadeias na porta monitorada. Para obter mais informações, consulte Diretrizes para configurar o monitor TCPPort. n é um número de 1 - 30 inclusivo.

Conjuntos de Criptografia

A propriedade `SSLCipherSuite` especifica o conjunto de criptografia usado pelo monitor TCPPORT. Para obter mais informações sobre as configurações de SSL, consulte "Configuração de SSL no Internet Service Monitoring" na página 436.

Monitor TFTP

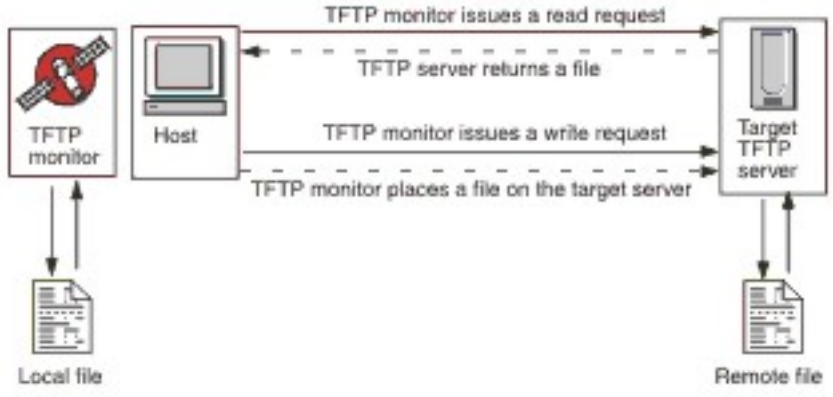
O monitor TFTP mede o desempenho do serviço Trivial File Transfer Protocol (TFTP) entre dois sistemas.

A tabela a seguir lista os arquivos do monitor TFTP.

Tabela 150. Resumo do Monitor FTP	
Arquivos do Monitor	**Nome ou local**
Nome do executável	`nco_m_tftp`
Arquivo de Propriedades	`$ISHOME/etc/props/tftp.props`
Arquivo de regras	`$ISHOME/etc/rules/tftp.rules`
Arquivo de log	`$ISHOME/log/tftp.log`

Diretrizes para configurar o monitor TFTP

O monitor TFTP transfere arquivos entre o sistema host e o servidor de destino usando solicitações READ ou WRITE do TFTP e, depois, registra o tempo de resposta e a taxa de transferência de dados. Use-o para garantir que seu servidor TFTP esteja ativo e em execução e transferindo arquivos em uma taxa aceitável.



Para fazer upload de um arquivo, o monitor envia o pedido TFTP WRITE (WRQ), e para fazer download de um arquivo, ele envia o pedido TFTP READ (RRQ). Nos clientes TFTP, a operação de upload é PUT e a operação de download é GET.

O monitor TFTP suporta os modos de transferência de arquivo octet (binário) e netascii.

Configurando testes de serviços do monitor TFTP

Utilize os parâmetros de configuração do monitor TFTP para definir testes de serviço.

Tabela 151. Configuração do Monitor TFTP

Campo	**Descrição**
servidor	O endereço IP do servidor TFTP de destino ou o sistema para o / do qual você deseja transferir arquivos.
localfile	Para operações GET, esse campo especifica o nome e o caminho para o qual o arquivo é transferido por download. Para operações PUT, esse campo especifica o nome e o caminho do arquivo que é transferido por upload para o servidor.
remotefile	Para operações GET, esse campo especifica o nome e o caminho do arquivo que é transferido por download do servidor. Para operações PUT, esse campo especifica o nome e o caminho para os quais o arquivo é transferido por upload no servidor.
description	Um campo de texto para fornecer informações descritivas sobre o monitor TFTP.
port	A porta que o servidor TFTP utiliza. Padrão: 69
IP local	O endereço IP da interface de rede do host em que o monitor abre a conexão TFTP. Se esse campo estiver vazio, o monitor usará a interface especificada pela propriedade `IpAddress`
localport	A porta que o monitor usa para estabelecer a conexão TFTP. Se o valor desse campo for `0`, o monitor selecionará uma porta apropriada.

Tabela 151. Configuração do Monitor TFTP (continuação)	
Campo	**Descrição**
comando	O comando TFTP a ser utilizado pelo monitor: • GET - Fazer download de um arquivo do servidor de destino para o host do monitor. • PUT - Fazer upload e um arquivo do host do monitor para o servidor de destino. Padrão: GET
transfermode	Especifica o formato no qual o monitor transfere o arquivo: • OCTET (8 bits) • NETASCII Padrão: OCTET
timeout	O tempo, em segundos, para aguardar até que o servidor TFTP responda. Padrão: 10
tentar novamente	O número de vezes que o monitor tenta transferir um arquivo antes de encerrar. Padrão: 3
Pesquisar	O tempo, em segundos, entre cada sondagem. Não configure esse valor muito baixo, já que pesquisas constantes podem oprimir o serviço. Padrão: 300
failureretests	O número de vezes que o monitor retesta o servidor TFTP após uma falha inicial antes de a falha ser indicada. Padrão: 0
retestinterval	O tempo, em segundos, para aguardar entre cada novo teste com falha. Padrão: 10

Classificações em Nível de Serviço

As classificações de nível de serviço definem as regras para determinar o nível de serviço fornecido por um servidor TFTP.

As opções de classificação em nível de serviço disponíveis para o monitor TFTP são:

```
totalTime
lookupTime
responseTime
transferTime
bytesTransferred
bytesPerSec
checksum
Mensagem
```

Nas classificações em nível de serviço:

- Especifique mais classificações de nível de serviço inserindo manualmente o nome do elemento de monitor. O nome deve corresponder ao nome mostrado para o elemento na seção Elementos do Monitor.
- `message` pode ser qualquer mensagem encaminhada no elemento `$message` para o servidor IBM Application Performance Management se usado em qualquer widget. Para obter uma lista de valores possíveis, consulte Mensagens de status.
- O operando é uma cadeia ou um número positivo.
- O elemento `checksum` normalmente não fornece resultados significativos para classificações de nível de serviço. Seu valor não é conhecido quando o elemento de perfil é criado. O monitor calcula valores de soma de verificação enquanto os testes estão em andamento. Esse elemento destina-se ao enriquecimento de alertas usando arquivos de regras.

Elementos do Monitor

Além dos resultados de teste comuns a todos os elementos, o monitor TFTP gera um conjunto de resultados de teste que contêm dados específicos para testes de serviço TFTP.

A tabela a seguir descreve os elementos adicionais para o monitor TFTP.

Tabela 152. Elementos do Monitor TFTP

Elemento	**Descrição**
`$bytesPerSec*` (`BytesPerSec`)	O número médio de bytes transferidos por segundo.
`$bytesTransferred*` (`BytesTransferred`)	O número de bytes transferidos por upload ou download.
`$checksum`	O valor total de verificação dos dados transferidos por download. Ele é gerado pelo monitor e é fornecido para processamento adicional usando arquivos de regras.
`$command*` (`TftpCommand`)	O comando TFTP emitido pelo monitor (`GET` ou `PUT`).
`$localFile*` (`TftpLocalFile`)	O nome do caminho completo do arquivo armazenado no host local. Esse elemento é retirado do arquivo de configuração.
`$localIP`	O endereço IP local com o qual o monitor está configurado para utilizar. Ele pode ficar em branco em sistemas com somente uma interface.
`$lookupTime*` (`LookupTime`)	O tempo utilizado para obter o endereço IP do servidor host.
`$remoteFile*` (`TftpRemoteFile`)	O nome do caminho completo do arquivo armazenado no host remoto (o servidor FTP). Esse elemento é obtido do arquivo de configuração.
(`TransferTime`)	O tempo gasto para transferir o arquivo.
(`TftpConnection`)	O formato em que o monitor transferiu o arquivo. Ele é `OCTET` (8 bits) ou `NETASCII`.

Mensagens de Status

O monitor TFTP fornece mensagens de status no atributo `ResultMessage` durante o uso do IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

Tabela 153. Mensagens de Status do Monitor TFTP

Mensagem	Descrição
Ok	O pedido de TFTP foi bem-sucedido.
FALHA: Falha na conexão	O monitor falhou ao se conectar ao servidor. Verifique se o servidor está executando.
FALHA: Erro interno do monitor tftp	Há um problema com o monitor, possivelmente causado por memória insuficiente.
FALHA: Um envio/espera com tempo limite esgotado	O pedido de TFTP falhou. Pode haver algum problema com a rede.
FALHA: Uma condição de erro não específica. A transferência deve ser interrompida	
FALHA: Recebido um pacote curto ou malformado	
FALHA: Falha ao abrir/ler/gravar no arquivo local	
FALHA: status desconhecido da tentativa de transferência	

Exemplo

Teste a disponibilidade do servidor TFTP `tftp.mycompany.com` fazendo upload do arquivo `$ISHOME/etc/testfiles/upload.txt` para `/ism/test/upload_result.txt`. Use o modo netascii para fazer upload do arquivo em intervalos de 20 minutos

Classifique o nível de serviço usando os seguintes critérios:

- Se o upload não tiver êxito, o nível de serviço será `Com Falha`
- Se o tempo total da transferência for maior que 10 segundos, o nível de serviço será `Marginal`
- Caso contrário, o nível de serviço será `Válido`

Crie um elemento de perfil de monitor TFTP e defina a configuração, conforme mostrado na tabela a seguir.

Tabela 154. Exemplo de Elemento de Perfil TFTP

Campo de Configuração	Valores
servidor	tftp.mycompany.com
localfile	`$ISHOME/etc/ism/testfiles/upload.txt`
remotefile	`/ism/test/upload_result.txt`
description	Teste do TFTP

Tabela 154. Exemplo de Elemento de Perfil TFTP (continuação)	
Campo de Configuração	**Valores**
Ativo	Selected
comando	PUT
transfermode	NETASCII
Pesquisar	1200

declaração	`If (Message != OK) then status Failed`
	`else if (TotalTime > 10) then status Marginal`
	`else status Good`

Monitor TRANSX

O monitor TRANSX simula as ações de um usuário de Internet real executando uma série de atividades, que ele executa utilizando outros Internet Service Monitors.

Por exemplo, configurar o TRANSX para acessar páginas de um website usando o monitor HTTP, fazer download de alguns arquivos e enviar ou receber usando os monitores POP3 e SMTP.

A tabela a seguir lista os arquivos do monitor TRANSX.

Tabela 155. Arquivos do Monitor TRANSX	
Arquivos do Monitor	**Nome ou local**
Monitor executável	`nco_m_transaction`
Arquivo de Propriedades	`$ISHOME/etc/props/transx.props`
Arquivo de regras	`$ISHOME/etc/rules/transx.rules`
Arquivo de log	`$ISHOME/log/transx.log`

Propriedades

Tabela 156. Propriedades do Monitor TRANSX		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
`CompleteTransax`	`0`|`1`	Especifica se a transação continuará mesmo se uma etapa falhar. • `0` -desativado (não continua) • `1` -enabled (continua)
`DetailedTimings`	`0`|`1`	Especifica que o monitor TRANSX produz logs de dados contendo sincronizações de baixa granularidade para cada etapa. As sincronizações de granularidade produzidas nos logs de dados são pré-configuradas e não podem ser modificadas. • `0` - desativado • `1` -ativado

Tabela 156. Propriedades do Monitor TRANSX (continuação)		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
`MultipleEvents`	`0`|`1`	Especifica se o monitor gerará vários eventos para os resultados da transação: • `0` - desativado (o monitor gera somente um evento contendo os resultados de todas as etapas e resultados resumidos) • `1` - ativado (o monitor gera um evento para cada etapa na transação e um evento de resumo final)
`StepPause`	integer	Especifica a duração da pausa, em segundos, entre a execução de cada etapa da transação. O comprimento da pausa não afeta o valor do elemento `$totalTime` da transação. `$totalTime` representa a soma dos elementos `$stepXTime` de uma transação. Padrão: `0`

A tabela a seguir descreve as propriedades específicas para o monitor SMTP.

Diretrizes para Configurar o Monitor TRANSX

O monitor TRANSX testa os serviços simulando um conjunto de atividades que engloba uma experiência de usuário típica. O conjunto de atividades é chamado de `transação` e cada atividade na transação é chamada de `etapa da transação`.

Os elementos de perfil TRANSX definem as transações. Cada etapa da transação configura um monitor de serviços da Internet, como HTTP, para executar a operação para essa etapa. Você configura as etapas de transação por meio do botão Editar na guia Etapas do elemento de perfil TRANSX.

As etapas são configuradas da mesma forma que você configura qualquer outro elemento de perfil. Por exemplo, os detalhes de configuração para uma etapa que envolve o monitor HTTP podem incluir parâmetros Head/Form, parâmetros do servidor proxy, expressões comuns e classificações em nível de serviço.

Quando o monitor TRANSX testa uma etapa na transação, ele registra o tempo levado e o nível de serviço para a etapa.

Nota: O monitor TRANSX requer privilégios de administrador se qualquer etapa da transação usar outro monitor, como ICMP, que requer privilégios de administrador.

Manipulando Conteúdo Dinâmico com Monitores HTTP e HTTPS

Muitos websites usam o conteúdo dinâmico para fornecer funções como interações baseadas em sessão ou região. Quando usados juntamente com o monitor TRANSX, os monitores HTTP e HTTPS podem testar páginas da web com conteúdo dinâmico, como IDs de sessão, códigos de região ou datas e horários integrados a links, cujos valores podem ser diferentes cada vez que a transação é testada.

Os recursos de conteúdo dinâmico fornecidos pelos monitores HTTP e HTTPS durante a execução no modo de transação permitem identificar conteúdo dinâmico em forma de pares nome-valor, chamado `elementos de página dinâmicos`, integrado em URLs, ou definido em elementos HTML `form`, que o monitor então extrai de uma página durante cada teste, garantindo que o valor dinâmico apropriado seja usado cada vez que uma transação é testada.

Por exemplo, considere uma página de Login do Web site, `http://www.mycompany.com/login`, que contenha um link para efetuar logon no Web site. A URL do link para a ação de login `http://`

`www.mycompany.com/doLogin?sessionID=id` inclui um ID de sessão para a transação de Login. Nesse exemplo, o par nome-valor `sessionID=id` é um elemento da página dinâmica; o valor de `id` muda toda vez que a página Login é acessada. Para testar a página Login como parte de uma transação, configure a transação para obter e usar o valor de `sessionID` sempre que a transação for testada e a insira na URL de ação de login.

O monitor TRANSX transmite elementos de página dinâmica de uma etapa de transação para outra. No exemplo de Login do Web site, a primeira etapa da transação poderia acessar a página de Login para obter o ID de sessão e, em seguida, passá-lo para uma segunda etapa, que envia a solicitação de login contendo esse ID. As operações executadas nestas etapas são:

1. Acessar a página que contém os elementos de página dinâmica, por exemplo `http://www.mycompany.com/login`
2. Enviar a ação usando os elementos de página dinâmicos, por exemplo, `http://www.mycompany.com/doLogin?sessionID=@@030671`

Quando você identifica um elemento de página dinâmico na etapa de transação, ele é passado para a próxima etapa da transação, que insere o par nome-valor em sua solicitação. O elemento é transmitido para cada transação HTTP ou HTTPS subsequente até que você o remova explicitamente.

Incluindo e Removendo Páginas Dinâmicas

Cada etapa de transação HTTP ou HTTPS consiste em um pedido, que retorna uma página HTML. Ao executar uma etapa de transação que contém elementos de página dinâmica, o monitor analisa a página HTML para localizar o par nome-valor de cada elemento e transmiti-lo para a próxima etapa de transação, que os insere em sua solicitação HTTP ou HTTPS.

Para especificar que uma etapa usa elementos da página dinâmica, configure o tipo de parâmetro para o elemento como DYNAMIC. Em seguida, especifique cada elemento dinâmico que deve ser extraído e transmitido para etapas posteriores. Identifique cada elemento dinâmico inserindo seu nome, por exemplo, `sessionID` e selecione Add To como o valor. Add To indica que o elemento deve ser transmitido para as etapas posteriores.

Nota: Para obter o nome de um elemento de página dinâmica, visualize a origem HTML da página na qual ele está localizado.

Elementos de página dinâmica são transmitidos de uma etapa de transação a outra. Se um elemento de página não precisar mais ser transmitido para uma próxima etapa, configure o Valor do elemento para Remove From. Atualize manualmente as etapas de transação subsequentes para assegurar que os elementos de página corretos sejam processados.

Use as seguintes diretrizes para incluir e remover elementos de página dinâmica:

- Se uma etapa não usar qualquer elemento de página dinâmico, não selecione DYNAMIC como o tipo de parâmetro.
- Se uma etapa precisar de um elemento da página dinâmica, a etapa que recupera a página na qual o elemento dinâmico aparece deve especificar o nome do elemento e o valor Add To.
- Se uma etapa não requerer um elemento dinâmico que seja passado de etapas anteriores, configure o valor da etapa anterior para Remover De.

GET e POST

Nos métodos GET, todos os elementos de página dinâmica são inseridos na URL de pedido automaticamente. Nos métodos POST, você deve especificar cada elemento dinâmico como um parâmetro FORM na guia Parâmetros.

O monitor insere automaticamente o valor dinâmico para cada formulário quando retorna a etapa de transação.

Criando Transação

Você define transações criando elementos de perfil TRANSX e etapas de transação usando a interface com o usuário do Internet Service Monitoring. Para obter mais informações, consulte “Criando Transações” na página 436.

Configurando o teste de serviço do monitor TANSX

Tabela 157. Configuração do Monitor TRANSX	
Campo	**Descrição**
transxname	Um nome para a transação.
description	Um campo de texto para fornecer informações descritivas sobre o elemento.
Pesquisar	O tempo, em segundos, entre cada sondagem. Padrão: 300

Nota: Monitore a disponibilidade de um website usando uma sequência de navegação na web, downloads de arquivo e e-mails enviados.

1. Crie um elemento de perfil TRANSX.
2. Crie uma etapa de transação HTTP para monitorar a disponibilidade de um website.
3. Crie uma etapa de transação FTP para monitorar o download de um arquivo.
4. Crie uma etapa de transação POP3 ou SMTP para monitorar e-mails.

Consulte a documentação de cada monitor para obter informações adicionais.

Elementos do Monitor

O monitor TRANSX gera eventos contendo os resultados de cada transação. Esses eventos contêm os resultados da transação inteira, assim como aqueles das etapas individuais da transação.

No entanto, por padrão, o monitor coloca todos os resultados da transação e da etapa em um único evento, usando a propriedade `MultipleEvents` para configurar o monitor para criar eventos individuais para cada etapa da transação e um evento resumido para a transação inteira. A Tabela 1 lista os elementos de resumo TRANSX.

Elementos indicados por um asterisco (*) estão disponíveis como atributos. Os nomes dos atributos são mostrados entre colchetes. A ausência de um asterisco indica que não há nenhum atributo equivalente. Os atributos que são mostrados entre colchetes, mas sem um elemento, indicam que eles estão disponíveis somente como atributos e que não há elementos equivalentes.

Tabela 158. Elementos do Monitor de Resumo TRANSX	
Elemento	**Descrição**
$numberOfSteps* (NumberOfSteps)	O número de etapas na transação.
$stepDescriptions	Uma lista das descrições para cada etapa, que são separadas por um caractere de barra vertical (|).
$stepTimes*(Step*1 to 10*TotalTime)	Os dados de sincronização retornados por cada etapa (1 - 10).
$stepUnits	Uma lista das unidades de cada etapa, geralmente segundos, separadas por um caractere de barra vertical (|).
(TransName)	O nome da transação conforme especificado durante a configuração da transação.
(TransStepDescription)	A descrição da etapa da transação conforme especificada durante a configuração da etapa.

Mensagem de status

O monitor TRANSX fornece mensagens de status no atributo `ResultMessage` ao usar o IBM Application Performance Management. Essas mensagens indicam o resultado do teste.

A tabela a seguir descreve as mensagens de status.

Tabela 159. Mensagens de Status do Monitor TRANSX

Mensagem	**Descrição**
`Successfully completed transaction`	A transação foi concluída com êxito.
`Error in transaction`	Houve uma falha em uma das etapas da transação.
`Service Level Failed, ending transactionService Level Failed`	O nível de serviço de uma das etapas retornou uma resposta com falha, que causou a parada da transação.

Criando Transações
As transações podem ser definidas criando elementos de perfil e etapas de transação do TRANSX usando a interface com o usuário do agente de Monitoramento de Serviço da Internet.

Procedimento

Para criar uma transação utilizando a interface:

1. Clique em **Ícone Configuração do Sistema**. Sob o qual clique em **Configuração do agente**.
   A janela de configuração do agente é aberta.
2. Clique na guia **ISM** para configurar o agente do Internet Service Monitoring.
3. Clique no ícone de mais **(+)** para criar um novo perfil. Insira o **Nome do Perfil** e **Descrição**.
4. Clique em **Avançar**.
5. Clique no Monitor **TRANSX** na lista suspensa de monitores para selecionar o Monitor TRANSX.
6. Clique em **Avançar**.
7. Insira os parâmetros obrigatórios.
8. Na guia **Avançar**, especifique o **intervalo de pesquisa**.
9. Clique no ícone de mais **(+)** na guia Etapas.
10. Clique no monitor que precisa ser selecionado na lista suspensa do monitor.
11. Clique em **Selecionar** para configurar a etapa da transação.
    a) Especifique os parâmetros obrigatórios e opcionais da mesma maneira que inseridos anteriormente para configurar os elementos de perfil.
    b) Se estiver criando etapas dinâmicas para o monitor HTTP ou HTTPS, configure os pares Nome e Valor na guia Parâmetros e selecione DYNAMIC como o tipo de parâmetro.
12. Clique em **Incluir**.
13. Clique no ícone atualizar na grade de etapas.
14. Repita as etapas de 1 a 13 para cada ajuda de transação adicional.
15. Clique em **Incluir** para concluir.
16. Clique em **Pronto** para salvar.

Resultados

Nota: Para especificar uma pausa entre cada etapa da transação, utilize a propriedade `StepPause`.

Configuração de SSL no Internet Service Monitoring
O Internet Service Monitoring usa o OpenSSL para se comunicar de forma segura com serviços de Internet normalmente remotos usando vários monitores, por exemplo, o monitor HTTPS se comunica

com um HTTPD protegido. agente de Monitoramento de Serviço da Internet também usa OpenSSL entre os monitores e o Databridge e entre o agente de Monitoramento de Serviço da Internet (KIS) e o Databridge. Especifique o conjunto de cifras que seu aplicativo usa na propriedade `SSLCipherpherSuite`.

O Databridge deve ser configurado para se comunicar de forma segura com os monitores e o agente de Monitoramento de Serviço da Internet, assim, cada monitor compartilhará um conjunto comum de propriedades relacionadas ao Databridge para gerenciar a comunicação segura com o Databridge. Alguns monitores também compartilham um conjunto semelhante, mas diferente, de propriedades relacionadas para gerenciar a comunicação segura com seus respectivos serviços de Internet em teste.

Os monitores a seguir suportam o monitoramento de serviços de Internet seguros:

- HTTPS
- IMAP4
- POP3
- SMTP

Esses monitores usam certificados. Todos os certificados são armazenados no formato X509 em arquivos Privacy Enhanced Mail (.pem) em `$ISMHOME/certificates`. O certificado para o Databridge também é armazenado no mesmo local. Por esse motivo, as propriedades a seguir são compartilhadas por todos os monitors, Databridge e agente de Monitoramento de Serviço da Internet:

- SSLTrustStore (Padrão: $ISMHOME/certificates/trust.pem)
- SSLTrustStorePath (Padrão: $ISMHOME/certificates/)

Como toda a comunicação entre os monitores e o Databridge e entre os monitores selecionados e seus serviços de Internet seguros são construídos na mesma versão do OpenSSL, eles compartilham características. Por exemplo, o nível mais alto de segurança que o Internet Service Monitoring pode fornecer é uma função do nível mais alto fornecido pelo OpenSSL subjacente. O nível mais baixo de segurança fornecido é similarmente dependente do OpenSSL subjacente.

Se o agente de Monitoramento de Serviço da Internet for atualizado e a atualização incluir uma atualização no OpenSSL subjacente, os serviços da Internet sendo monitorados podem sofrer impacto. Por exemplo:

1. O monitor HTTPS no agente de Monitoramento de Serviço da Internet V7.x.1 está monitorando um servidor HTTPD seguro.
2. Aplique uma nova versão do agente de Monitoramento de Serviço da Internet que contenha uma versão atualizada do OpenSSL, o que significa que o monitor HTTPS agora é V7.x.2.
3. Você observa que o monitor HTTPS agora está falhando ao monitorar o HTTPD protegido.

O nível de segurança do servidor HTTPD é menor que o mínimo suportado pelo agente de Monitoramento de Serviço da Internet V7.x.2 atualizado recentemente. Mesmo que a configuração do monitor HTTPS não tenha sido alterada, seu comportamento foi, pois ele depende da camada OpenSSL subjacente. A combinação mais recente do agente de Monitoramento de Serviço da Internet/HTTPS Monitor/OpenSSL é mais segura que a antiga combinação, e agora você precisa aumentar o nível de segurança do servidor HTTPD remoto.

O monitoramento de serviços de Internet seguros apresenta um dilema. O nível de segurança do agente de Monitoramento de Serviço da Internet deve ser tão baixo que pode monitorar serviços de Internet fracamente protegidos; ou deve ser tão alto quanto as configurações mínimas atualmente recomendadas? Se a primeira opção for selecionada, um agente de Monitoramento de Serviço da Internet enfraquecido poderá comprometer a segurança, possivelmente em ambas as extremidades.

A mesma versão do OpenSSL é usada por todos os monitores. Todos esses monitores compartilham um conjunto comum de propriedades do monitor para configurar o OpenSSL subjacente, que são descritas na tabela a seguir.

Tabela 160. Propriedades do monitor relacionadas ao OpenSSL

Nome da propriedade	Parâmetro de propriedade	Descrição
SSLCipherSuite	string	Especifica os conjuntos de cifras a serem usados para operações SSL entre o monitor e o serviço de Internet que está sendo monitorado. Os valores para essa propriedade devem estar no formato recomendado pelo OpenSSL. Padrão: AES:3DES:DES:!EXP:!DHE:!EDH
SSLDisableSSLv2	0 | 1	Determina qual o tipo de conexão segura a ser feita ao monitorar um serviço de Internet seguro. 0 -SSLv2 é permitido 1 – SSLv2 NÃO é permitido Padrão: 1 (SSLv2 NÃO permitido).
SSLDisableSSLv3	0 | 1	Determina qual o tipo de conexão segura a ser feita ao monitorar um serviço de Internet seguro. 0 – SSLv3 é permitido 1 – SSLv3 Não é permitido Padrão: 1 (SSLv3 NÃO permitido).
SSLDisableTLS	0|1	Determina qual o tipo de conexão segura a ser feita ao monitorar um serviço de Internet seguro. 0 -TLSv1.0 é permitido 1 -TLSv1.0 NÃO é permitido Padrão: 0 (TLSv1.0 é permitido).
SSLDisableTLS11	0|1	Determina qual o tipo de conexão segura a ser feita ao monitorar um serviço de Internet seguro. 0 -TLSv1.1 é permitido 1 -TLSv1.1 NÃO é permitido Padrão: 0 (TLSv1.1 é permitido).
SSLDisableTLS12	0|1	Determina qual o tipo de conexão segura a ser feita ao monitorar um serviço de Internet seguro. 0 – TLSv1.2 é permitido 1 -TLSv1.2 NÃO é permitido Padrão: 0 (TLSv1.2 é permitido).

Tabela 160. Propriedades do monitor relacionadas ao OpenSSL (continuação)

Nome da propriedade	Parâmetro de propriedade	Descrição
SSLCertificateFile	string	O caminho e o nome de arquivo do arquivo de certificado digital público usado pelo monitor. Quando um monitor tenta configurar uma conexão segura com um serviço da Internet, esse último pode opcionalmente solicitar que o monitor forneça seu certificado de lado do cliente, permitindo que o serviço da Internet verifique o monitor ou cliente (verificação de certificado de lado do cliente). O certificado deve estar no formato Privacy Enhanced Mail (PEM). Para o monitor HTTPS, esse valor pode ser especificado para cada elemento HTTPS no momento da criação. No entanto, se o monitor HTTPS for usar o mesmo certificado para todos os elementos, o valor no arquivo HTTPS.props será usado. Para monitores IMAP, LDAP, POP3, SIP, SMTP e SOAP, o valor é configurado em todo o monitor. Se o caminho não for absoluto, o monitor o interpretará com relação ao diretório ativo, $ISMHOME/certificates. Padrão: “”
SSLKeyFile	string	O caminho e o nome do arquivo que contém a chave privada usada pelo monitor. O monitor usa esse arquivo para criptografar mensagens que ele envia para outros. Os receptores usam o certificado digital público do monitor para decriptografar a mensagem. Padrão: monitoryKey.pem
SSLKeyPassword	string	A senha utilizada para criptografar a chave privada SSL. Padrão: “”

Tabela 160. Propriedades do monitor relacionadas ao OpenSSL (continuação)		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
SSLTrustStoreFile	string	O nome completo do arquivo que armazena todos os certificados públicos X509 dos serviços da Internet que estão sendo monitorados, como uma lista concatenada. Os certificados revogados (CRLs) também são armazenados aqui como uma lista concatenada. O Databridge também pode armazenar seu certificado público aqui. Essa propriedade aparece no arquivo `bridge.props`. Os certificados são armazenados no formato Privacy Enhanced Mail (PEM). Converta certificados obtidos em outros formatos para o formato PEM usando o software OpenSSL disponível em http://www.openssl.org. Padrão: **“$ISMHOME/certificates/trust.pem”**
SSLTrustStorePath	string	O local dos arquivos `.pem` que contêm os certificados X509 do serviço da Internet seguro que está sendo monitorado. Os certificados revogados (CRLs) também são armazenados aqui. O Databridge também pode armazenar seu certificado público aqui. Essa propriedade aparece no arquivo `bridge.props`. Se novos certificados forem incluídos nesse diretório, execute o comando openssl `rehash` para varrer o diretório e calcular um hash para cada certificado. Se as propriedades `SSLTrustStoreFile` e `SSLTrustStorePath` forem usadas, o OpenSSL usará ambas as propriedades para localizar certificados confiáveis. Padrão: “`$ISMHOME/certificates/`”
`VerifyCertificate Preference`	0|1	Ativa ou desativa a verificação do certificado fornecido pelo serviço de Internet que está sendo monitorado com relação à lista de revogação de certificado (CRL). Padrão: 0 - desativado

Conjuntos de Criptografia

Os conjuntos de cifras disponíveis para o Internet Service Monitoring são um subconjunto dos que são permitidos pelo OpenSSL. O grupo de conjuntos de cifras permitidos pelo OpenSSL muda no decorrer do tempo. À medida que novas vulnerabilidades são descobertas e as melhores práticas evoluem, o acesso a tipos específicos ou gerais de conjuntos de cifras pode ser restringido ou removido inteiramente pelo OpenSSL. Como essas versões posteriores do OpenSSL são incluídas em versões posteriores do ISM, há um fluxo no efeito, que pode impactar a configuração e operação dos monitores.

Use a propriedade do monitor SSLCipherSuite para especificar os conjuntos de cifras permitidos por um monitor a partir de todos os conjuntos de cifras disponíveis usando palavras-chave. Para especificar vários conjuntos, use uma lista de palavras-chave separadas por dois pontos. Por exemplo, a propriedade SSLCipherSuite padrão é `AES:3DES:DES:!EXP:!DHE:!EDH`. Essa seleção significa que os conjuntos de cifras que incluem AES, 3DES e DES são permitidos, mas exclui quaisquer conjuntos de cifras que usem trocas de chave EXP (Exportar (comprimentos de chave curtos)), DHE (Diffie Hellman Exchange) ou EDH (Ephemeral Diffie Hellman). Além disso, quando a conexão segura é feita entre o monitor e o serviço da Internet, o AES é usado primeiro, seguido por 3DES e, em seguida, DES, se necessário. A sintaxe para as listas de conjunto de criptografia para o agente de Monitoramento de Serviço da Internet é a mesma que para OpenSSL.

Para selecionar o conjunto correto de conjuntos de cifras para um monitor, considere o que o OpenSSL subjacente suporta, o intervalo de cifras que o serviço da Internet que está sendo monitorado suporta e os padrões de segurança de sua organização. Talvez você não consiga monitorar um site externo seguro com um nível de segurança inferior ao tolerado pelo Internet Service Monitoring ou OpenSSL. Em alguns casos, um monitor que já foi capaz de monitorar um serviço da Internet, pode falhar após o upgrade do Internet Service Monitoring porque os níveis de segurança são incompatíveis.

A tabela a seguir lista um subconjunto de conjuntos de cifras equivalente ao valor padrão para SSLCiperSuite de `AES:3DES:DES:!EXP:!DHE:!EDH` com suas propriedades. Na tabela, você verá os seguintes termos:

- Nome do Conjunto de Criptografia: descreve o conjunto de criptografia usando um nome construído a partir das palavras-chave.
- Protocolo: descreve a versão do protocolo suportado.
- Troca de Chave: descreve o sistema de troca de chave usado para criptografia e decriptografia.
- Criptografia e Comprimento da Chave: descreve o tipo de algoritmo de criptografia usado e o comprimento da chave (em bits) usada.
- MAC: descreve o Código de Autenticação de Mensagem usado para assegurar que os dados não tenham sido corrompidos.

Tabela 161. Nome do conjunto de cifras e valores de propriedades `AES:3DES:DES:!EXP:!DHE:!EDH`

Nome do Conjunto de Criptografia	Protocolo	Troca de Chave	Autenticação	Criptografia e Comprimento da Chave	Código de autenticação de mensagem
ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH	RSA	AESGCM (256)	AEAD
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	ECDH	ECDSA	AESGCM (256)	AEAD
ECDHE-RSA-AES256-SHA384	TLSv1.2	ECDH	RSA	AES (256)	SHA384
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	ECDH	ECDSA	AES (256)	SHA384
ECDHE-RSA-AES256-SHA	SSLv3	ECDH	RSA	AES (256)	SHA1
ECDHE-ECDSA-AES256-SHA	SSLv3	ECDH	ECDSA	AES (256)	SHA1
SRP-DSS-AES-256-CBC-SHA	SSLv3	SRP	DSS	AES (256)	SHA1
SRP-RSA-AES-256-CBC-SHA	SSLv3	SRP	RSA	AES (256)	SHA1

Tabela 161. Nome do conjunto de cifras e valores de propriedades AES:3DES:DES:!EXP:!DHE:!EDH (continuação)

Nome do Conjunto de Criptografia	Protocolo	Troca de Chave	Autenticação	Criptografia e Comprimento da Chave	Código de autenticação de mensagem
SRP-AES-256-CBC-SHA	SSLv3	SRP	SRP	AES (256)	SHA1
DH-DSS-AES256-GCM-SHA384	TLSv1.2	DH/DSS	DH	AESGCM (256)	AEAD
... seguido por 61 mais linhas					

A tabela a seguir lista um subconjunto de conjuntos de cifras equivalentes ao valor para `SSLCiperSuite` de `AES:3DES:!DES:!EXP:!DHE:!EDH:!SSLv2:!SSLv3` com suas propriedades. Agora alguns protocolos são eliminados e o conjunto de criptografia geral foi reduzido em 71 - 31.

*Tabela 162. Nome do conjunto de cifras e valores de propriedades **AES:3DES:DES:!EXP:!DHE:!EDH:!SSLv2:!SSLv3***

Nome do Conjunto de Criptografia	Protocolo	Troca de Chave	Autenticação	Comprimento da Criptografia e Chave	Código de autenticação de mensagem
ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	ECDH	ECDSA	AESGCM (256)	AEAD
ECDHE-RSA-AES256-SHA384	TLSv1.2	ECDH	RSA	AES (256)	SHA384
ECDHE-ECDSA-AES256-SHA384	TLSv1.2	ECDH	ECDSA	AES (256)	SHA384
DH-DSS-AES256-GCM-SHA384	TLSv1.2	DH/DSS	DH	AESGCM (256)	AEAD
DH-RSA-AES256-GCM-SHA384	TLSv1.2	DH/RSA	DH	AESGCM (256)	AEAD
DH-RSA-AES256-SHA256	TLSv1.2	DH/RSA	DH	AES (256)	SHA256
DH-DSS-AES256-SHA256	TLSv1.2	DH/DSS	DH	AES (256)	SHA256
ADH-AES256-GCM-SHA384	TLSv1.2	DH	none	AESGCM (256)	AEAD
ADH-AES256-SHA256	TLSv1.2	DH	none	AES (256)	SHA256
ECDH-RSA-AES256-GCM-SHA384	TLSv1.2	ECDH/RSA	ECDH	AESGCM (256)	AEAD
... seguido por 21 mais linhas					

Reduzindo a Vulnerabilidade

Em liberações futuras, as cifras DHE e EDH serão desativadas por padrão devido a vulnerabilidades. Para versões anteriores do agente de Monitoramento de Serviço da Internet, talvez seja necessário desativar as cifras DHE e EDH em todos os monitores. Para desativar as cifras DHE e EDH, atualize as propriedades do monitor `SSLCipherSuite` e `BridgeSSLCipherSet`.

Por exemplo, para desativar as cifras DHE e EDH no monitor HTTPS, atualize o arquivo `https.props` para incluir as propriedades a seguir:

```
SSLCipherSuite: AES:3DES:DES:!DES-CBC-SHA:!EXP:!DHE:!EDH
BridgeSSLCipherSet: AES:3DES:DES:!DES-CBC-SHA:!EXP:!DHE:!ED
```

Assegure-se de verificar se essa mudança na configuração não causa problemas de compatibilidade. Se você mudar a configuração padrão após aplicar essa correção, poderá se expor a uma vulnerabilidade de segurança. É necessário revisar seu ambiente inteiro para identificar outras áreas nas quais você ativou o protocolo de troca de chave Diffie-Hellman usado em TLS e executar ações apropriadas de mitigação e correção.

Seleção de protocolo

É possível selecionar dentre um intervalo de protocolos de comunicação segura históricos e atuais. Eles podem ser selecionados individualmente usando um conjunto de propriedades do monitor booleano:

- SSLDisableSSLv2
- SSLDisableSSLv3
- SSLDisableTLS
- SSLDisableTLS11
- SSLDisableTLS12
- BridgeSSLDisableSSLv2
- BridgeSSLDisableSSLv3

Você deve desativar o SSLv2 e o SSLv3. Esses protocolos ficaram comprometidos e possuem várias vulnerabilidades conhecidas. Elas foram desativados por padrão e são fornecidos apenas para propósitos de legado.

O Internet Service Monitoring ativa o TLS por padrão. Se você souber que os serviços de Internet que está monitorando não estão usando o TLS 1.0 e já foram atualizados para TLS 1.1 ou TLS 1.2, você deve desativar os protocolos não usados no Internet Service Monitoring.

O componente Databridge se comunica com o agente Internet Service Monitoring e com cada um dos monitores. Por padrão, essa comunicação é criptografada e TLS é o protocolo preferencial.

Armazenamentos e certificados de confiança chave

O Internet Service Monitoring armazena seus certificados em um arquivo definido pelo usuário em um local definido pelo usuário. Todos os certificados devem ser armazenados no formato Privacy Enhanced Mail (PEM). Assegure-se de que os certificados públicos obtidos de outras organizações sejam convertidos para o formato PEM. O software de conversão está disponível em http://www.openssl.org .

Os certificados confiáveis especificados usando a propriedade `SSLTrustStoreFile` são armazenados no arquivo como uma lista concatenada.

É uma boa prática armazenar as Listas de Revogação de Certificado (CRLs) no armazenamento confiável, com relação às quais os certificados podem ser validados. As Autoridades de Certificação possuem sistemas em vigor para gerar listas de certificados revogados e têm sistemas de distribuição em vigor para torná-los publicamente disponíveis. Em seguida, se um certificado estiver comprometido, ele será revogado.

Configurações de Segurança do Databridge

Todos os monitores se comunicam com o Databridge, portanto, todos os monitores têm um conjunto comum de propriedades que devem ser configuradas para gerenciar a comunicação entre os monitores e o Databridge. Por padrão, a comunicação é criptografada. O protocolo de criptografia padrão é TLS. Ao contrário das propriedades do monitor, não há nenhum mecanismo para controlar se uma determinada versão de TLS está ativada ou desativada. Todos os monitores devem ter os mesmos valores para as propriedades do Databridge, caso contrário haverá problemas de comunicação. Da mesma forma, as propriedades configuradas no arquivo .props do Databridge devem ser consistentes com aquelas dos monitores. O Databridge também se comunica com o agente Internet Service Monitoring, que tem seu próprio arquivo .props. Alguns dos valores no agente .props são relacionados ao Databridge e, como monitores, devem ter valores consistentes com aqueles no arquivo `.props` do Databridge.

Tabela 163. Propriedades do Databridge relacionadas ao OpenSSL

Nome da propriedade	Parâmetro de propriedade	Descrição
BridgeSSLEncryption	0 | 1	Determina se a comunicação com o Databridge está criptografada ou não. Isso abrange toda a comunicação do Databridge com os Monitores e o agente do Internet Service Monitoring. 0 – não criptografado 1 – criptografado **Restrição:** Configure o mesmo valor no agente do Internet Service Monitoring, em todos os monitores e no Databridge.
BridgeSSLCipherSet	string	Especifica os conjuntos de cifras a serem usados para operações SSL para e a partir do Databridge. Os valores para essa propriedade devem estar no formato recomendado pelo OpenSSL. **Restrição:** Configure o mesmo valor no agente do Internet Service Monitoring, no agente, em todos os monitores e no Databridge. Padrão: `AES:3DES:DES:!EXP:!DHE:!EDH`
BridgeSSLDisableSSLv2	0 | 1	Determina o tipo de conexão segura a ser feita de e para o Databridge. 0 – SSLv2 e SSLv3 são permitidos 1 – SSLv2 NÃO é permitido **Restrição:** Configure o mesmo valor no agente do Internet Service Monitoring, em todos os monitores e no Databridge. Padrão: 1 (SSLv2 NÃO permitido).
BridgeSSLDisableSSLv3	0 | 1	Determina o tipo de conexão segura a ser feita de e para o Databridge. 0 – SSLv3 é permitido 1 – SSLv3 Não é permitido **Restrição:** Configure o mesmo valor no agente do Internet Service Monitoring, em todos os monitores e no Databridge. Padrão: 1 (SSLv3 NÃO permitido).
BridgeSSLCertificateFile	string	O caminho e o nome do arquivo do certificado SSL do Databridge digital. Padrão: `$ISMHOME/certificates/bridgeCert.pem`
BridgeSSLKeyFile	string	O caminho e o nome do arquivo de chave privado SSL do Databridge. Padrão: `$ISMHOME/certificates/bridgeKey.pem`

Tabela 163. Propriedades do Databridge relacionadas ao OpenSSL (continuação)

Nome da propriedade	Parâmetro de propriedade	Descrição
BridgeSSLKeyPassword	string	A senha usada para criptografar a chave privada SSL do Databridge. Padrão: **Tivoli**
BridgeSSLTrustStore	string	O caminho e nome de arquivo do arquivo de certificação confiável para autenticação. Isso é necessário apenas ao usar a propriedade **BridgeSSLAuthenticatePeer**. Padrão: `$ISMHOME/certificates/trust.pem` Se desejar configurar a autenticação SSL entre um monitor e o Databridge, ou entre o Databridge e o agente, configure `BridgeSSLAuthenticatePeer` como 1 e reinicie o Databridge. Essa ação autentica os certificados do servidor. É possível armazenar certificados no `SSLTrustStoreFile` e no `SSLTrustStorePath`. Padrões: • `SSLTrustStoreFile`, `$ISMHOME/certificates/trust.pem` • `SSLTrustStorePath`, `$ISMHOME/certificates/` Para incluir novos certificados, conclua uma das etapas a seguir: • Inclua um certificado no final da lista no arquivo de texto `SSLTrustStoreFile` • Inclua um novo certificado no diretório `SSLTrustStorePath` e execute o comando OpenSSL **`c_rehash certificate_dir`** para executar hash nos certificados
SSLTrustStoreFile	string	Essa propriedade é usada pelos monitores seguros e pelo Databridge. Consulte Tabela 160 na página 438, para obter mais informações.
SSLTrustStorePath	string	Essa propriedade é usada pelos monitores seguros e pelo Databridge. Consulte Tabela 160 na página 438, para obter mais informações.

Tabela 163. Propriedades do Databridge relacionadas ao OpenSSL (continuação)		
Nome da propriedade	**Parâmetro de propriedade**	**Descrição**
BridgeSSLAuthenticatePeer	0|1	Especifica se o Databridge deve realizar autenticação cruzada com outros componentes do Internet Service Monitoring. 0 – desativado 1 – ativado Se um monitor entrar em contato com o Databridge, ele deverá ser autenticado com o Databridge e o Databridge deverá ser autenticado com o monitor. Se o agente do Internet Service Monitoring entrar em contato com o Databridge, ele deverá ser autenticado com o Databridge e o Databridge deverá ser autenticado com o agente. Os certificados para o Databridge são armazenados no BridgeSSLTrustStore. Padrão: 0 - desativado

Propriedades do agente Internet Service Monitoring

O agente de Monitoramento de Serviço da Internet tem seu próprio arquivo de propriedades, que contém um conjunto de configurações e propriedades de segurança. O arquivo de propriedades do agente não se comunica com os monitores, mas ele se comunica com o Databridge, portanto, as configurações de segurança no arquivo `.props` do agente gerenciam a comunicação entre o agente e o Databridge.

Configurando o agente nos sistemas Windows

É possível configurar o agente em sistemas Windows usando a janela **IBM Performance Management**.

Procedimento

Configure o agente de Monitoramento de Serviço da Internet Agent no sistema do usuário, conforme a seguir.

Para configurar manualmente o agente do Monitoramento de Serviço da Internet em sistemas de usuário:

1. No painel do **IBM Performance Management**, clique em **Configuração do Sistema** > **Configuração do Agente** listado sob **Configuração do Sistema**.
2. Clique na guia **ISM** para abrir o painel do Internet Service Monitoring Agent.

Configurando o Databridge

A configuração do Databridge envolve definir propriedades para o Databridge que controlem sua operação, como a conexão dos módulos do componente e os monitores de serviços da Internet.

Operação e configuração
O Databridge e seus módulos de componente são configurados por meio dos arquivos de propriedades.

As propriedades determinam a operação do Databridge e seus módulos de componente que envia resultados de teste para o IBM Cloud Application Performance Management para relatório no painel do Monitoramento de Serviço da Internet Agent.

Configurando o Databridge
O Databridge deve ser configurado para receber dados dos Monitores de Serviço da Internet e encaminhar esses dados para seus módulos de componentes para processamento adicional.

A tabela a seguir lista os arquivos associados ao Databridge. O **Arquivo de propriedades**, **Arquivo Store And Forward** e **Arquivo de Log** são descritos com mais detalhes nas seções adequadas.

Tabela 164. Arquivos de Databridge e seu Local

Arquivo Databridge	Localização ou nome
Arquivo Executável	`$ISHOME/platform/arch/bin/nco_m_bridge`
Arquivo de Propriedades	`$ISHOME/etc/props/bridge.props`
Arquivo Store and Forward	o Nome e o local estão especificados pelas propriedades no arquivo`bridge.props`. O nome e o local padrão são `$ISHOME/var/sm_bridge.saf`
Arquivo de log	`$ISHOME/log/bridge.log`
Arquivo de Log de Erros	`$ISHOME/log/bridge.err`

Arquivo Store And Forward
Se o Databridge não for capaz de encaminhar os dados ao Netcool/OMNIbus, ele armazenará todos os dados que normalmente enviaria em um arquivo Store And Forward (SAF). Quando o Netcool/OMNIbus se torna disponível novamente, ele processa todos os eventos armazenados no arquivo SAF.

As propriedades QFile e QSize no arquivo de propriedades do Databridge determinam o nome, o local e a operação do processamento de armazenamento e encaminhamento.

Arquivo de log
O Databridge envia mensagens diariamente sobre suas operações a um arquivo de log de mensagens. Por padrão, o nome desse arquivo é `$ISHOME/log/bridge.log`. Ele é atualizado às 12 meia-noite. As propriedades MsgDailyLog e MsgTimeLog do Databridge controlam a operação de criação de log de mensagens.

Iniciando o Databridge
Iniciando o Databridge usando o console de Serviços do Windows.

Procedimento

Nota: Se o módulo ObjectServer estiver conectado ao Databridge, certifique-se de que o sistema de destino está sendo executado antes de iniciar o Databridge. Se algum dos módulos Databridge falhar ao inicializar corretamente, o Databridge não será iniciado.

1. Na área de trabalho do Windows, clique em **Iniciar** > **Ferramentas Administrativas** > **Serviços**.
2. Na lista de serviços, selecione o serviço denominado NCO BRIDGE Internet Service Monitor e clique em **Iniciar** a partir do menu.

Conectando Módulos
O arquivo de propriedades do Databridge define os módulos para fazer a conexão com o Databridge.

Sobre Esta Tarefa
Cada par de propriedades do Módulo n `SharedLib` e do Módulo n `PropFile` define a conexão para um módulo. Os módulos são carregados na ordem de definição, iniciando no Module0.

Procedimento

1. Para conectar módulos individuais ao Databridge:
   a) No arquivo de propriedades Databridge, identifique o próximo par de propriedades do Módulo n `SharedLib` e Módulo n `PropFile` disponível.
   b) Configure o Módulo n `SharedLib` para o nome da biblioteca compartilhada do módulo (sua implementação binária).
   c) Configure o Módulo n `PropFile` para o caminho completo do arquivo de propriedades do módulo.

Nesse exemplo, as linhas 1 e 2 conectam o módulo ObjectServer, as linhas 3 e 4 conectam o módulo Datalog, as linhas 5 e 6 conectam o módulo IBM Application Performance Management (`pipe`). O módulo Datalog não possui um arquivo de propriedades, portanto, a entrada para o arquivo de propriedades possui o valor `""`.

2. Para desativar um módulo:
   a) Configure a propriedade do Módulo n `SharedLib` correspondente como `"NONE"` e a propriedade do Módulo n `PropFile` `PropFile` para `""`. Todos os outros módulos que possuem um valor maior que n também são ignorados.

Conectando Monitores
Os monitores de serviço da Internet são conectados ao Databridge sobre TCP. Cada monitor possui um conjunto de propriedades que configura a conexão com o Databridge.

Sobre Esta Tarefa
Para conectar um monitor com o Databridge, configure o valor da propriedade `BridgePort` definida no arquivo de propriedades do monitor para o valor da propriedade `SocketPort` definida no arquivo de propriedades Databridge. O valor padrão de cada propriedade `BridgePort` do monitor e a propriedade `SocketPort` do Databridge é `9510`.

O Databridge suporta a criptografia SSL dos resultados de teste que ele recebe dos monitores. Para criptografar os resultados de teste de um monitor, configure os valores das propriedades `BridgeSSL` definidas no arquivo de propriedades do monitor com os valores das propriedades `BridgeSSL` definidas no arquivo de propriedades Databridge. Para criptografar os resultados de teste todos os monitores, todos estes monitores devem ter as mesmas propriedades `BridgeSSL`.

Configurando o Módulo Databridge
O Databridge direciona resultados de teste para o Monitoramento de Serviço da Internet Agent. O agente de monitoramento converte esses dados para o formato necessário e os distribui para o IBM Application Performance Management Server. Configure o módulo Databridge e o agente de monitoramento de serviço da Internet por meio de seus respectivos arquivos de propriedades.

Configure a operação do Databridge modificando os valores de propriedade definidos no arquivo de propriedades do módulo.

O arquivo de propriedades do módulo é denominado `pipe_module.props`. Esse arquivo está localizado no diretório `$ISHOME/etc/props/`.

A tabela a seguir lista as propriedades disponíveis para o módulo. Se as mudanças forem feitas nas propriedades, reinicie o Databridge para que as mudanças entrem em vigor.

Tabela 165. Propriedades do Módulo Databridge

Nome da propriedade	Type	Descrição
`TEMAHOST`	string	Nome do host que executa o agente de monitoramento. Padrão: `localhost`
`TEMAPORT`	integer	Número da porta usado pelo host. Padrão: `9520`

Configure a operação do agente de monitoramento de serviço da Internet modificando os valores de propriedade definidos no arquivo de propriedades do agente de monitoramento.

O arquivo de propriedades do agente de monitoramento é chamado de `kisagent.props`. Esse arquivo está localizado no diretório `$ISMHOME/etc/props/`.

A tabela a seguir lista as propriedades disponíveis para o agente de monitoramento.

Tabela 166. Propriedades do agente de monitoramento		
Nome da propriedade	**Type**	**Descrição**
TEMAPORT	integer	Número da porta usado pelo host. Esse deve ser o mesmo que o número de porta da propriedade TEMAPORT listado no arquivo de propriedades do módulo. Padrão: 9520
ObsoleteDuration	integer	O tempo, em segundos, após o qual os dados que não foram atualizados são excluídos da memória do agente de monitoramento. Os dados podem não ser atualizados quando, por exemplo, um elemento de perfil tiver sido interrompido ou uma falha de rede tiver ocorrido. **Nota:** Não configure o tempo ObsoleteDuration com um valor menor que o intervalo de pesquisa, pois isso resulta em perda de dados entre intervalos de pesquisa. Padrão: 900
AggDuration	integer	O tempo, em segundos, após o qual o agente de monitoramento impede que os dados sejam agregados e relatados no painel do agente. Qualquer dado que seja mais antigo do que o tempo especificado será excluído da memória do agente de monitoramento. Os dados antigos são calculados comparando o intervalo entre os horários de início e atual até o tempo de duração agregado. Se o intervalo for maior que o tempo de duração agregado, 10 por cento dos dados antigos serão removidos e o horário de início será aumentado em 1/10 do intervalo. O agente de monitoramento calcula isso a cada 5 minutos. Padrão: 3600
ManageServices	0|1	Inicia e para todos os monitores e o Databridge quando o agente do Internet Service Monitoring é iniciado ou interrompido. 1 é ativado e 0 é desativado. Padrão: 1

A conexão entre o agente de monitoramento de serviço da Internet e o módulo Databridge é criada quando você instala o Monitoramento de Serviço da Internet.

Ativando o Netcool/OMNIbus

Siga estas etapas para permitir que o Tivoli Netcool/OMNIbus envie os eventos do agente de Monitoramento de Serviço da Internet para o Netcool/OMNIbus.

Antes de Iniciar

Assegure-se de ter instalado o IBM Tivoli Netcool/OMNIbus.

Procedimento

Conclua as etapas a seguir para ativar o Netcool/OMNIbus:

1. Pare o agente de Monitoramento de Serviço da Internet usando o comando a seguir:

   ```
   $CANDLEHOME/bin/ism-agent.sh stop
   ```

2. Abra o arquivo `bridge.props` colocado no caminho `$ISMHOME/etc/props` e atualize-o com o seguinte fragmento de código:

   ```
   Module0SharedLib : "libSMModulePipe"
   Module0PropFile : "$ISMHOME/etc/props/pipe_module.props"
   Module1SharedLib : "libSMModuleObjectServer"
   Module1PropFile : "$ISMHOME/etc/props/objectserver.props"
   ```

3. Modifique a permissão do diretório `8.1.0` colocado no caminho `$ISMHOME/objectserver` da seguinte forma:

   ```
   cd  $ISMHOME/objectserver/
   chmod -R 777 8.1.0
   ```

   Nota: Modifique a permissão de todos os arquivos no diretório `8.1.0` usando o comando `chmod -R 777 <file-name>`. Em que `<file-name>` é o nome do arquivo dentro do diretório `8.1.0`.

4. Modifique o arquivo `omni.dat` colocado no caminho `$ISMHOME/objectserver/8.1.0/etc` para configurar o endereço do servidor Netcool/OMNIbus.
5. Execute `nco_igen` no seguinte local:

   ```
   cd $ISMHOME/objectserver/8.1.0/bin
   ./nco_igen
   ```

6. Inicie o agente de Monitoramento de Serviço da Internet usando o seguinte comando:

   ```
   $CANDLEHOME/bin/ism-agent.sh start
   ```

7. Verifique se o agente de Monitoramento de Serviço da Internet, Databridge e todos os monitores estão em estado de execução.

   Para verificar o status do Databridge e monitores, execute o seguinte comando:

   ```
   ps -aef|grep -i nco_*
   ```

   Para verificar o status do agente de Monitoramento de Serviço da Internet, execute o seguinte comando:

   ```
   ps -aef|grep -i kis
   ```

8. Use a interface com o usuário do IBM Tivoli Netcool/OMNIbus para verificar se o Databridge envia os dados para o servidor Netcool/OMNIbus.

   Os dados devem ser exibidos para o agente de Monitoramento de Serviço da Internet na interface com o usuário do IBM Application Performance Management.

Configurando o monitoramento do J2SE

Para coletar dados de diagnóstico e de monitoramento de recursos de aplicativos Java no local sendo monitorados, deve-se configurar o coletor de dados J2SE.

Antes de Iniciar

Instale um dos tempos de execução Java suportados:

- Oracle Java Platform Standard Edition 7 (Java SE Development Kit 7)

  Lembre-se: Esse Java Runtime não suporta a imagem do coletor de dados J2SE configurada com o protocolo HTTPS.
- Oracle Java Platform Standard Edition 7 (Java SE Runtime Environment 7)

Lembre-se: Esse Java Runtime não suporta a imagem do coletor de dados J2SE configurada com o protocolo HTTPS.

- Oracle Java Platform Standard Edition 8 (Java SE Development Kit 8)
- Oracle Java Platform Standard Edition 8 (Java SE Runtime Environment 8)
- IBM SDK, Java Technology Edition, Versão 7
- IBM SDK, Java Technology Edition, Versão 8

Importante: Para Windows Server 2016, instale o JDK 8, atualização 131 (Java SE Development Kit 8u131), ou Java SE Development Kit 7, atualização 80 (JDK 7u80).

Para obter mais informações sobre requisitos do sistema, consulte Relatórios de compatibilidade de produto de software para o coletor de dados J2SE.

Sobre Esta Tarefa

É possível configurar o coletor de dados J2SE em sistemas Windows, Linux e AIX.

As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões de coletor de dados e agente e sobre o que há de novo em cada versão, consulte "Histórico de Mudanças" na página 50.

Procedimento

1. Copie os seguintes arquivos do instalador do APM para um diretório:

   Importante: O caminho do diretório não deve ter nenhum espaço.

   - Windows Copie o arquivo `gdc.zip` do instalador do APM para um diretório e extraia-o.
   - Linux AIX Copie o arquivo `gdc-apd.tar.gz` do instalador do APM para um diretório e extraia-o.
   - Linux AIX Forneça permissões de leitura/gravação e execução ao usuário para a pasta `j2se_dc`. A permissão de execução é fornecida para executar scripts e arquivos JAR na pasta. Permissão de leitura/gravação é fornecida, já que os arquivos de diagnósticos de detalhamento são gerados nesta pasta.
2. Na linha de comandos, acesse *DCHOME*`\.gdc\<toolkit_version>\bin`

   Em que *toolkit_verion* é

   - Para a V8.1.4.0 e anterior, *toolkit_verion* é 7.3.0.5.0.
   - Para a V8.1.4.0.1 e mais recente, *toolkit_verion* é 7.3.0.14.0.
3. Execute o seguinte comando:

   Windows `config.bat`

   Linux AIX `config.sh`
4. Quando solicitado, especifique o caminho para o Java Home e pressione **Enter**.
   Por exemplo,

   Windows `C:\Program Files\jre7`

   Linux AIX `/opt/ibm/java`
5. Conclua as etapas a seguir para a versão do agente que você usa:

   - Para V8.1.4.0.2 e anterior, conclua as seguintes etapas:

     a. Quando solicitado, insira o nome completo (nome qualificado) da classe principal do aplicativo e pressione **Enter**. A classe principal é o ponto de entrada do aplicativo que precisa ser monitorado. Exemplo: `testapp.TemperatureConveter`

     b. Quando solicitado, insira um nome de alias de aplicativo distinto e pressione **Enter**. O nome inserido aqui é usado para criar o nome da instância no painel do APM.

Windows O arquivo `dcstartup.bat` é gerado no seguinte local: *DCHOME*`\.gdc\`*toolkit_verion*`\runtime\j2se`*application_alias*`.`*hostname*`.`*application_alias*. Esse arquivo é o script para executar seu aplicativo juntamente com o coletor de dados.

Linux AIX O arquivo `dcstartup.sh` é gerado no seguinte local: *DCHOME*`/.gdc/`*toolkit_verion*`/runtime/j2se`*application_alias*`.`*hostname*`.`*application_alias*. Esse arquivo é o script para executar seu aplicativo juntamente com o coletor de dados.

- Para a V8.1.4.0.3 para V8.1.4.0.5, conclua as etapas a seguir

  a. Quando solicitado, insira o diretório inicial do aplicativo Java. Por exemplo, `/root/J2seApp/`

  b. Selecione um aplicativo Java da lista fornecida e clique em Sair.

  – `com.ibm.SampleApplication`
  – `com.ibm.DBApplication`
  – `com.ibm.SpringBootApplication`

  Selecione qualquer aplicativo que seja fornecido na lista ou forneça 0 para selecionar qualquer aplicativo que não esteja na lista.

  1) Se você fornecer 0, insira o `nome completo` da classe principal de qualquer aplicativo. Por exemplo, `com.ibm.testApp.Main`
  2) Se você selecionar qualquer opção da lista fornecida, o nome do alias será criado com base no nome da classe. Se o nome do alias exceder o limite de caractere, forneça o nome do alias dentro do limite de caractere.

     Importante: O limite máximo de caractere para o nome do alias é calculado de forma que `alias_name + host_name` não exceda 24 caracteres.

  c. Selecione a opção para ativar ou desativar o Rastreamento de Transação. O valor padrão é *Yes*.

  d. Selecione a opção para ativar ou desativar a coleta de dados de Diagnósticos. O valor padrão é *Yes*.

  1) Se você selecionar *Yes*, selecione a opção para o modo Rastreio de Método. O valor padrão é *No*.

  e. Se você selecionar uma opção da lista que é fornecida na Etapa b, copie o script de inicialização `<DCHOME>/j2se_dc/.gdc/`*toolkit_version*`/runtime/j2se<application_alias>.<hostname>.<application_alias>` para o local de sua escolha.

- Para a V8.1.4.0.6 e mais recente, conclua as etapas a seguir:

  a. Quando solicitado, insira o diretório inicial do aplicativo Java. Por exemplo, `/root/J2seApp/`

  b. Selecione o tipo de aplicativo que você deseja monitorar.

  – Aplicação Java
  – Servidor Jetty

  c. Se você selecionar o tipo de aplicativo como *Java Application*, siga as etapas mencionadas na seção V8.1.4.0.3 a V8.1.4.0.5 da Etapa 5.

  d. Se você selecionar o tipo de aplicativo como *Jetty Server*, siga estas etapas:

  1) Insira o diretório inicial do Jetty. Por exemplo, `/home/jetty/jetty-distribution-9.4.12.v20180830`
  2) Insira o nome do alias. Se o nome do alias exceder o limite de caractere, forneça o nome do alias dentro do limite de caractere.

     Importante: Se você selecionar o tipo de aplicativo como *Java Application* e qualquer opção da lista na Etapa b da seção V8.1.4.0.3 a V8.1.4.0.5, copie o script de inicialização `<DCHOME>/j2se_dc/.gdc/toolkit_version/runtime/`

j2se<application_alias>.<hostname>.<application_alias> no local de sua escolha.

e. Se o tipo selecionado for *Jetty Server*, o `dcstartup.bat/dcstartup.sh` será copiado para o diretório Jetty Home fornecido.

- Para V8.1.4.0.7, conclua as seguintes etapas:
  - Se você configurar o coletor de dados J2SE usando o Open JDK versão 9 ou posterior e ao inserir o caminho para o Java Home, um aviso será exibido com o conteúdo da seguinte forma:

Aviso:

```
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by jnr.posix.JavaLibCHelper
(file:/root/testopen/preconf-13march/j2se_dc/.gdc/7.3.0.14.0/
bin/lib/jython.jar)to method sun.nio.ch.SelChImpl.getFD()
WARNING: Please consider reporting this to the maintainers of
jnr.posix.JavaLibCHelper
WARNING: Use --illegal-access=warn to enable warnings of next
illegal reflective access operations
WARNING: All illegal access operations will be denied in next
release Mar 15, 2019 11:35:06 AM
org.python.netty.util.internal.PlatformDependent <clinit>
INFO: Your platform does not provide complete lowlevel API for
accessing direct buffers reliably.
Unless explicitly requested, heap buffer is always preferred
to avoid potential system unstability.
```

No entanto, o coletor de dados J2SE funcionará corretamente e você poderá ignorar esse aviso.

Para a V8.1.4.0.2 e versões anteriores, siga a etapa 6 para modificar o arquivo Windows `dcstartup.bat` ou Linux AIX `dcstartup.sh`.

6. Para modificar o arquivo Windows `dcstartup.bat` ou Linux AIX `dcstartup.sh`, conclua as seguintes etapas:
   - Se as classes do aplicativo e os arquivos JAR forem empacotados em um único arquivo JAR, conclua as seguintes etapas:
     a. Abra o seguinte arquivo:
        - Windows `dcstartup.bat`
        - Linux AIX `dcstartup.sh`
     b. Substitua `-cp .:$classpath:$Classpath $ITCAM_JVM_OPTS` *`full name of the main class`* por `$ITCAM_JVM_OPTS -jar` *`Application jar file`* e salve o arquivo.
   - Se o aplicativo estiver usando vários arquivos JAR, conclua as seguintes etapas:
     a. Abra o seguinte arquivo:
        - Windows `dcstartup.bat`
        - Linux AIX `dcstartup.sh`
     b. Configure a variável *CLASSPATH* para os arquivos JAR.
     c. Substitua `-cp .:$classpath:$Classpath $ITCAM_JVM_OPTS` *`full name of the main class`* por `-cp .:$classpath:$Classpath $ITCAM_JVM_OPTS -jar` *`Application jar file`* e salve o arquivo.

        O arquivo JAR do aplicativo deve conter a classe de aplicativo principal.

   Nota: Para modificar o arquivo Windows `dcstartup.bat` ou Linux AIX `dcstartup.sh` da V8.1.4.0.3 para a V8.1.4.0.5 e V8.1.4.0.6 para a mais recente (se o tipo de Aplicativo estiver selecionado como *Java Application*), siga a etapa 7.
7. Conclua as etapas a seguir quando o aplicativo estiver usando vários arquivos JAR.
   a) Abra o seguinte arquivo:

- Windows `dcstartup.bat`
- Linux AIX `dcstartup.sh`

b) Configure a variável *CLASSPATH* para os arquivos JAR.

c) Para V8.1.4.0.7, se você configurar o coletor de dados J2SE com Java 9 ou 10 e usar a conexão SSL para conectividade do APM, os dados de Rastreamento de Transação não serão exibidos. Para resolver o problema, é possível incluir a sinalização **--add-modules java.xml.bind** na última linha do arquivo `dcstartup.bat` ou `dcstartup.sh`.

Por exemplo,

- Se o Aplicativo for um arquivo jar, atualize a última linha da seguinte forma:

```
PathToJava --add-modules java.xml.bind --add-opens=

jdk.management/com.sun.management.internal=

ALL-UNNAMED -jar $Classpath $ITCAM_JVM_OPTS AppJarName.jar
```

- Se o Aplicativo não estiver empacotado em um arquivo jar, atualize a última linha da seguinte forma:

```
PathToJava --add-modules java.xml.bind --add-opens=

jdk.management/com.sun.management.internal=ALL-UNNAMED -cp
.:$classpath:$Classpath $ITCAM_JVM_OPTS FullyQualifiedClassName
```

8. Para ativar o monitoramento de diagnósticos detalhados, edite o `custom_request.xml` com as classes e os métodos específicos do J2SE que deseja monitorar. É possível fazer isso de duas maneiras: processo manual e processo automatizado.

Para preencher automaticamente o `custom_request.xml` com classes e métodos específicos do aplicativo J2SE:

a) Acesse o diretório <DCHOME>/j2se_dc/.gdc/7.3.0.14.0/runtime/ j2se<application_alias>.<hostname>.<application_alias>/ e abra o arquivo `dc.properties`.

b) Ative a propriedade `is.auto.update.custom_requests.xml` configurando seu valor como *true* e salve o arquivo.

c) Execute os comandos da etapa 9.

d) Pare o coletor de dados após 10 ou 15 minutos.

e) Verifique se o DCHOME>/j2se_dc/.gdc/7.3.0.14.0/runtime/ j2se<application_alias>.<hostname>.<application_alias>/custom/ `custom_requests.xml` está preenchido com as classes e os métodos customizados.

f) Remova as entradas indesejadas e abra o arquivo `dc.properties` novamente.

g) Desative a propriedade `is.auto.update.custom_requests.xml` configurando seu valor *false* e salve o arquivo.

h) Execute os comandos da etapa 9.

Nota: Se algum dos métodos customizados do aplicativo não for descoberto automaticamente, será necessário incluir os métodos customizados manualmente.

Para manual manualmente o `custom_request.xml`:

a) Acesse <DCHOME>/j2se_dc/.gdc/7.3.0.14.0/runtime/ j2se<application_alias>.<hostname>.<application_alias>/custom/ `custom_requests.xml` e edite `custom_request.xml`.

Por exemplo,

```
<edgeRequest>

<requestName>truncateDb</requestName>
```

```
<Matches>testApp.JDBC.DBManager</Matches>
<type>application</type>
<methodName>truncateDb</methodName>
</edgeRequest>
```

b) Inclua as classes e os métodos específicos do aplicativo.

9. Execute o seguinte comando:

   Windows `dcstartup.bat`

   Linux AIX `dcstartup.sh`

   Nota: Se o tipo de aplicativo selecionado for *Jetty Server*, execute o `dcstartup.bat/dcstartup.sh` presente no diretório Inicial da Jetty.

   O aplicativo J2SE é iniciado junto com o coletor de dados configurado.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo coletor de dados nos painéis. Para obter informações sobre como usar o console, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Verificando o status da coleta de dados de Rastreamento de Transação e de Diagnósticos

Para a V8.1.0.3 e mais recente, na página de configuração do agente, é possível verificar o status dos dados de rastreamento de transação e de diagnósticos.

Sobre Esta Tarefa

É possível verificar o status da coleta de dados de rastreio de transação e de diagnósticos com a ajuda de dois comandos. Consulte o procedimento para saber sobre esses comandos.

Procedimento

1. Use o comando **`config status`**.
   a) Abra o diretório bin. Emita o comando

      Linux AIX **`cd <DCHOME>/j2se_dc/.gdc/toolkit_version/bin/`**

      Windows **`cd <DCHOME>\j2se_dc\.gdc\toolkit_version\bin\`**

      Em que *toolkit_version* é

      - Para a V8.1.4.0 e anterior, *toolkit_verion* é 7.3.0.5.0.
      - Para a V8.1.4.0.1 e mais recente, *toolkit_verion* é 7.3.0.14.0.

   b) Insira o seguinte comando para verificar o status

      Linux AIX **`config.sh status`**

      Windows **`config.bat status`**

   c) Selecione os Aplicativos Java com o nome do alias que são identificados da lista para verificar seu status, ou selecione sair.

      1) ddperf
      2) Main
      3) Sair

2. Use o comando **`config status <application_alias_name>`**.
   a) Insira o seguinte comando para abrir um diretório

Linux AIX **cd <DCHOME>/j2se_dc/.gdc/7.3.0.14.0/bin/**

Windows **cd <DCHOME>\j2se_dc\.gdc\7.3.0.14.0\bin**

b) Insira o seguinte comando para verificar o status

Linux AIX **config.sh status <application_alias_name>**

Windows **config.bat status <application_alias_name>**

Mudando o status da coleta de dados de Rastreamento de Transação e de Diagnósticos

Para a V8.1.0.3 e mais recente, na página de configuração do agente, é possível mudar o status dos dados de rastreamento de transação e de diagnósticos.

Sobre Esta Tarefa

É possível mudar o status da coleta de dados de rastreio de transação e de diagnósticos com a ajuda do prompt de comandos. Consulte o procedimento a seguir para saber mais sobre esses comandos.

Procedimento

1. Abra o diretório bin e execute o seguinte comando:

   Linux AIX **cd <DCHOME>/j2se_dc/.gdc/toolkit_version/bin/**

   Windows **cd <DCHOME>\j2se_dc\.gdc\toolkit_version\bin**

   Em que *toolkit_version* é

   - Para a V8.1.4.0 e anterior, *toolkit_verion* é 7.3.0.5.0.
   - Para a V8.1.4.0.1 e mais recente, *toolkit_verion* é 7.3.0.14.0.
2. Para verificar o status, insira o seguinte comando:

   Linux AIX **config.sh <application_alias_name>**

   Windows **config.bat <application_alias_name>**
3. Quando solicitado a selecionar a opção para ativar ou desativar o Rastreamento de Transação. O padrão é `Sim`.
4. Quando solicitado a selecionar a opção para ativar ou desativar a coleta de dados de Diagnósticos. O padrão é `Sim`.

   a) Se Sim, selecione a opção para ativar/desativar o Rastreio de método. O padrão é `NO`.

Configurando o monitoramento do JBoss

O Monitoring Agent for JBoss monitora os recursos de servidores de aplicativos JBoss e a plataforma do JBoss Enterprise Application. Use os painéis fornecidos com o agente JBoss para identificar os aplicativos mais lentos, as solicitações mais lentas, gargalos do conjunto de encadeamentos, problemas de memória heap da JVM e de coleta de lixo, as sessões mais ocupadas e outros gargalos no servidor de aplicativos JBoss.

Antes de Iniciar

- Estas instruções são para a liberação mais atual do agente, exceto conforme indicado.
- Certifique-se de que os requisitos do sistema para o agente JBoss sejam atendidos em seu ambiente. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o agente JBoss.
- Antes de configurar o agente JBoss, primeiro o servidor JBoss deve ser configurado concluindo as tarefas a seguir.

  1. “Ativar conexões do servidor JMX MBean” na página 458.

2. “Incluir um usuário de gerenciamento do servidor JBoss” na página 459.
3. “Ativando Web/HTTP Statistic Collection” na página 460. Este procedimento destina-se ao JBoss EAP versão 7.x e WildFly versões 8.x, 9.x e 10.x.

Sobre Esta Tarefa

O Nome do sistema gerenciado inclui o nome da instância que você especifica, por exemplo, *instance_name*:*host_name*:*pc*, em que *pc* é seu código de produto de dois caracteres. O Nome do sistema gerenciado é limitado a 32 caracteres.

O nome da instância que você especifica é limitado a 28 caracteres, menos o comprimento do nome do host. Por exemplo, se especificar `JBoss` como seu nome de instância, seu nome do sistema gerenciado será `JBoss:hostname:JE`.

Nota: Se você especificar um longo nome de instância, o nome do Sistema gerenciado é truncado e o código do agente não é exibido corretamente.

O agente JBoss é um agente de múltiplas instâncias. Deve-se criar uma instância de agente para cada servidor JBoss monitorado, e iniciar cada instância de agente manualmente.

O recurso de rastreamento de transações está disponível para o agente JBoss na oferta do Cloud APM, Advanced.

- Para ativar o rastreamento de transações para uma nova instância de agente, conclua a etapa 1 ou a etapa 2 deste procedimento e, em seguida, siga o procedimento para “Configure o coletor de dados de rastreamento de transações do agente JBoss” na página 468.
- Para ativar o rastreamento de transações para uma instância de agente que já está configurado para monitoramento básico, siga o procedimento para o “Configure o coletor de dados de rastreamento de transações do agente JBoss” na página 468.
- Para desativar o rastreamento de transações para uma instância de agente, siga o procedimento para o “Desativar o coletor de dados de rastreamento de transações do agente JBoss” na página 470.
- Para desinstalar o rastreamento de transações para todas as instâncias de agente e remover o kit de ferramentas de rastreamento de transações, siga o procedimento para o “Desinstalar todos os rastreamentos de transações do agente JBoss” na página 471.

Procedimento

1. Configure o agente em sistemas Windows usando a janela **IBM Performance Management** ou usando o arquivo de resposta silencioso.
   - “Configurando o agente nos sistemas Windows” na página 462.
   - “Configurando o agente usando o arquivo silencioso de resposta” na página 465.
2. Configure o agente em sistemas Linux executando o script de linha de comandos e respondendo aos prompts ou usando o arquivo de resposta silencioso.
   - “Configurando o agente respondendo aos prompts” na página 464.
   - “Configurando o agente usando o arquivo silencioso de resposta” na página 465.
3. Opcional: Configure o rastreamento de transação configurando instâncias de agente individuais para fornecer dados de rastreamento de transação e configurando seu Application Performance Dashboard para exibir dados de rastreamento de transação.
   a) Siga o procedimento para o “Configure o coletor de dados de rastreamento de transações do agente JBoss” na página 468.
   b) Ative os dados de rastreamento de transação no Application Performance Dashboard para o agente JBoss.
      1) A partir da barra de navegação, clique em **Configuração do Sistema** > **Configuração do Agente**. A página **Configuração do Agente** é exibida.
      2) Selecione a guia **JBoss**.

3) Selecione as caixas de seleção para as instâncias de agente do servidor JBoss que você deseja monitorar e execute uma das seguintes ações da lista **Ações**:

- Para ativar o rastreamento de transações, clique em **Configurar rastreamento de transações** > **Ativado**. O status na coluna **Rastreamento de Transações** é atualizado para *Enabled*.
- Para desativar o rastreamento de transação, clique em **Configurar Rastreamento de Transação** > **Desativado**. O status na coluna **Rastreamento de Transações** é atualizado para *Disabled*.

c) Visualize os painéis de dados de rastreamento de transações do agente JBoss, incluindo a instância do agente JBoss em um aplicativo em seu Application Performance Dashboard.

Para obter mais informações sobre como usar o editor de Aplicativos, consulte Gerenciando aplicativos.

d) Assegure-se de que as contas de usuário sejam designadas a uma função que inclua a permissão Painel de Diagnóstico para ter acesso aos seguintes botões do Application Dashboard de rastreamento de transação do agente JBoss.
Caso contrário, esses botões serão desativados para esse usuário no Application Dashboard.

1) O botão de drill-down **Diagnosticar** no widget **5 Tempos de resposta mais lentos**.
2) O botão **Solicitações em andamento** no widget **Aplicativos**.

Nota: O recurso de rastreamento de transações está disponível para o agente JBoss na oferta do Cloud APM, Advanced. Para o agente JBoss com capacidade de monitoramento de recurso básico, que está na oferta do Cloud APM, Base, ignore esta etapa.

O que Fazer Depois

No Console do Cloud APM, acesse seu Application Performance Dashboard para visualizar os dados que foram coletados. Para obter informações adicionais sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Se você não conseguir visualizar os dados nos painéis do agente, primeiro verifique os logs de conexão do servidor e, em seguida, os logs do provedor de dados. Os caminhos padrão para estes logs são conforme a seguir.

- Linux `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Para obter ajuda com a resolução de problemas, consulte o Fórum do Cloud Application Performance Management.

Ativar conexões do servidor JMX MBean

Antes de o agente JBoss reunir dados do servidor JBoss, as conexões do servidor Java Management Extensions (JMX) MBean devem ser ativadas.

Procedimento

Siga as etapas para a liberação e versão do servidor JBoss.

- Configure EAP 5,2.

  Faça uma cópia de backup do arquivo `run.conf` e, em seguida, inclua as seguintes linhas nele:

```
JAVA_OPTS="$JAVA_OPTS -Djboss.platform.mbeanserver"
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote"
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.ssl=false"
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.authenticate=false"
JAVA_OPTS="$JAVA_OPTS -Dcom.sun.management.jmxremote.port=1090"
JAVA_OPTS="$JAVA_OPTS -Djavax.management.builder.initial=
                      org.jboss.system.server.jmx.MBeanServerBuilderImpl"
```

- Configure AS 6.x.

Especifique o endereço de ligação como um parâmetro ao iniciar o servidor JBoss.

– Linux *jboss_server_home*/bin/run.sh **-b** Ip_address

– Windows *jboss_server_home*\bin\run.bat **-b** <Ip_address>

em que *jboss_server_home* é o diretório de instalação do servidor JBoss.

Por exemplo, se o endereço de ligação for 10.77.9.250:

/apps/wildfly-9.0.2.Final/bin/run.sh **-b** 10.77.9.250

- Configure todas as outras versões suportadas.

  Os servidores JBoss e WildFly são instalados com suas portas JMX desativadas para gerenciamento remoto, por padrão. Deve-se mudar a configuração do servidor JBoss para permitir o gerenciamento remoto. Deve-se editar o *jboss_server_home*/standalone/configuration/standalone.xml para permitir o gerenciamento remoto.

  a) Faça uma cópia de backup do arquivo *jboss_server_home*/standalone/configuration/standalone.xml.

  Em que *jboss_server_home* é o diretório de instalação do servidor JBoss.

  b) Permitir configuração remota.

  Procure urn:jboss:domain:jmx e, em sua seção de subsistema, certifique-se de que a entrada remoting-connector tenha use-management-endpoint="true".

  Resultado de exemplo.

```
<subsystem xmlns="urn:jboss:domain:jmx:1.3">
            <expose-resolved-model/>
            <expose-expression-model/>
            <remoting-connector use-management-endpoint="true"/>
</subsystem>
```

  c) Permitir conexões remotas.

  Localize onde as interfaces são definidas e substitua 127.0.0.1 (loopback) pelo IP externo no servidor para ligação. Não faça a ligação com 0.0.0.0.

  Exemplo antes da substituição.

```
  <interfaces>
        <interface name="management">
            <inet-address value="${jboss.bind.address.management:127.0.0.1}"/>
        </interface>
        <interface name="public">
            <inet-address value="${jboss.bind.address:127.0.0.1}"/>
        </interface>
  ...
```

  Exemplo após a substituição se o endereço IP externo for 192.168.101.1.

```
  <interfaces>
        <interface name="management">
            <inet-address value="${jboss.bind.address.management:192.168.101.1}"/>
        </interface>
        <interface name="public">
            <inet-address value="${jboss.bind.address:192.168.101.1}"/>
        </interface>
  ...
```

Incluir um usuário de gerenciamento do servidor JBoss

Antes de o agente JBoss reunir dados do servidor JBoss, um usuário de gerenciamento deve ser incluído, se não existir um.

Procedimento

Use o script JBoss **add-user** para incluir um usuário de gerenciamento.

1. Acesse o diretório binário ou `bin` no diretório de instalação do servidor JBoss.
2. Execute o script **add-user**.
   - Linux **./add-user.sh**
   - Windows **add-user.bat**
3. Siga os prompts para gerar um usuário de gerenciamento.

Exemplo

```
root@jboss-wf10-rh7:/apps/wildfly-10.0.0.Final/bin
] ./add-user.sh

Que tipo de usuário que você deseja incluir?
 a) Usuário de gerenciamento (mgmt-users.properties)
 b) Usuário do aplicativo (application-users.properties)
(a): a

Insira os detalhes do novo usuário a ser incluído.
Usando a região 'ManagementRealm' como descoberta dos arquivos de propriedades existentes.
Nome do usuário: MyAdmin
As recomendações de senha estão listadas abaixo. Para modificar essas restrições, edite o
arquivo de configuração
add-user.properties.
 - A senha deve ser diferente do nome do usuário
 - A senha não deve ser um dos seguintes valores restritos {root, admin, administrator}
 - A senha deve conter pelo menos 8 caracteres, 1 caractere alfabético, 1 dígito
1 símbolo não alfanumérico
Password:
Inserir novamente a senha:
A quais grupos você deseja que esse usuário pertença? (Insira uma lista separada por vírgula ou
deixe em branco
para none)[  ]:
Sobre incluir o usuário 'MyAdmin' para a região 'ManagementRealm'
Isso está correto yes/no? yes
Incluído usuário 'MyAdmin' no arquivo '/apps/wildfly-10.0.0.Final/standalone/configuration/mgmt-
users.properties'
Incluído usuário 'MyAdmin' no arquivo '/apps/wildfly-10.0.0.Final/domain/configuration/mgmt-
users.properties'
Incluído usuário 'MyAdmin' com grupos no arquivo
          '/apps/wildfly-10.0.0.Final/standalone/configuration/mgmt-groups.properties'
Incluído usuário 'MyAdmin' com grupos no arquivo
          '/apps/wildfly-10.0.0.Final/domain/configuration/mgmt-groups.properties'
Esse novo usuário será usado para um processo AS para se conectar a outro processo AS?
por exemplo, para um controlador host escravo que se conecta ao principal ou para uma conexão
remota do servidor para
chamadas EJB do servidor.
yes/no? no
```

Ativando Web/HTTP Statistic Collection

Antes que o agente JBoss possa reunir métricas da web do servidor JBoss e outras métricas do subsistema, a coleta de estatísticas deverá ser ativada para cada subsistema. Este procedimento destina-se ao JBoss EAP versão 7.x e WildFly versões 8.x, 9.x e 10.x.

Procedimento

O atributo **statistics-enabled** de vários subsistemas JBoss controla a coleta de estatísticas. Essa configuração pode ser visualizada e atualizada usando a interface da linha de comandos do JBoss.

Nota: Este procedimento destina-se ao JBoss EAP versão 7.x e WildFly versões 8.x, 9.x e 10.x.

1. Acesse o diretório binário ou `bin` no diretório de instalação do servidor JBoss.
2. Inicie a interface da linha de comandos do JBoss.
   - Linux **./jboss-cli.sh --connect** [**--controller**=*IP*:*port*]
   - Windows **jboss-cli.bat --connect** [**--controller**=*IP*:*port*]

   em que *IP* é o endereço IP do servidor JBoss e *port* é a porta do servidor JBoss. Por exemplo, `192.168.10.20:9990`.

Dica: Se a tentativa de conexão resultar no erro, "`Falha ao se conectar ao controlador: o controlador não está disponível no localhost:9990: java.net.ConnectException: WFLYPRT0053: não foi possível se conectar a http-remoting://localhost:9990. A conexão falhou: WFLYPRT0053: não foi possível conectar-se a http-remoting://localhost:9990. A conexão falhou: conexão recusada`", use o parâmetro **`--controller`**.

Esse erro indica que o servidor de gerenciamento não está atendendo no endereço IP do host local (127.0.0.1) e é configurado para atender no endereço IP do computador.

3. Execute os seguintes comandos para visualizar o estado atual de cada atributo statistics-enabled do subsistema:

   Nota: Se o JBoss estiver em execução no Modo de Domínio, cada comando deverá ser prefixado com o perfil associado e esses comandos deverão ser executados para cada perfil monitorado. Por exemplo: `/profile=full/subsystem=ejb3:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`ejb3`**`:read-attribute(name=enable-statistics)`

   `/subsystem=`**`transactions`**`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`undertow`**`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`webservices`**`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`datasources/data-source`**`=`*`Data_Source_Name`*`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`datasources/data-source`**`=`*`Data_Source_Name`*`/`**`statistics=pool`**`:read-attribute(name=statistics-enabled)`

   `/subsystem=`**`datasources/data-source`**`=`*`Data_Source_Name`*`/`**`statistics=jdbc`**`:read-attribute(name=statistics-enabled)`

   em que *Data_Source_Name* é o nome de uma origem de dados que está configurada para uso com o JBoss.

   Nota: As origens de dados podem ser listadas usando o comando `/subsystem=datasources:read-resource`.

   Resultado de exemplo quando as estatísticas não estão ativadas:

```
{
    "outcome" => "success",
    "result" => false
}
```

4. Execute o seguinte comando para mudar o valor de cada atributo statistics-enabled do subsistema para *true*:

   `/subsystem=`**`ejb3`**`:write-attribute(name=enable-statistics, value=true)`

   `/subsystem=`**`transactions`**`:write-attribute(name=statistics-enabled,value=true)`

   `/subsystem=`**`undertow`**`:write-attribute(name=statistics-enabled,value=true)`

   `/subsystem=`**`webservices`**`:write-attribute(name=statistics-enabled,value=true)`

   `/subsystem=`**`datasources/data-source`**`=`*`Data_Source_Name`*`:write-attribute(name=statistics-enabled,value=true)`

   `/subsystem=`**`datasources/data-source`**`=`*`Data_Source_Name`*`/`**`statistics=pool`**`:write-attribute(name=statistics-enabled,value=true)`

   `/subsystem=`**`datasources/data-source`**`=`*`Data_Source_Name`*`/`**`statistics=jdbc`**`:write-attribute(name=statistics-enabled,value=true)`

   Resultado de exemplo quando você ativar as estatísticas para um subsistema:

```
{
    "outcome" => "success",
    "response-headers" => {
        "operation-requires-reload" => true,
        "process-state" => "reload-required"
    }
}
```

5. Saia da interface da linha de comandos do JBoss.
6. Reinicie o servidor JBoss.

   Nota: Todos os agentes JBoss em execução atualmente com o rastreamento de transações ativado devem ser reiniciados.

Configurando o agente nos sistemas Windows

É possível configurar o agente JBoss em sistemas operacionais Windows usando a janela IBM Cloud Application Performance Management. Após fazer a atualização dos valores de configuração, deve-se iniciar o agente para salvar os valores atualizados.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **Agentes de Monitoramento IBM** > **IBM Cloud Application Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito no modelo **Monitoring Agent for JBoss** e, em seguida, clique em **Configurar agente**.

   Lembre-se: Depois de configurar uma instância de agente pela primeira vez, a opção **Configurar agente** é desativada. Para configurar a instância de agente novamente, clique nela com o botão direito e clique em **Reconfigurar**.
3. Insira um nome de instância exclusivo e, em seguida, clique em **OK**. Use apenas letras, numerais Arábicos, o caractere sublinhado e o caractere de menos no nome da instância.
   Por exemplo, `jboss01`.

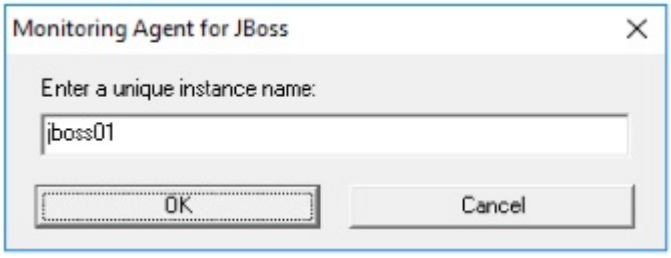


Figura 17. A janela para inserir um nome exclusivo da instância.

4. Insira as configurações do Servidor JBoss, em seguida, clique em **Avançar**.

   Consulte Tabela 167 na página 467 para obter uma explicação de cada um dos parâmetros de configuração.

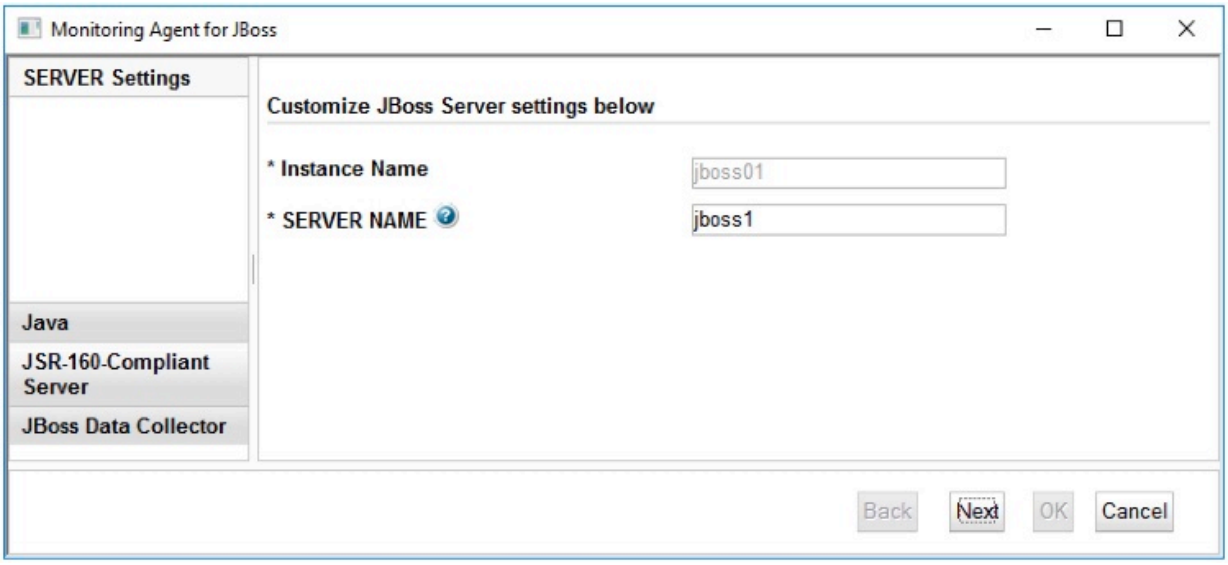


Figura 18. A janela para parâmetros de configuração para o servidor JBoss

5. Insira as configurações Java, em seguida, clique em **Avançar**.

   Consulte Tabela 167 na página 467 para obter uma explicação de cada um dos parâmetros de configuração.

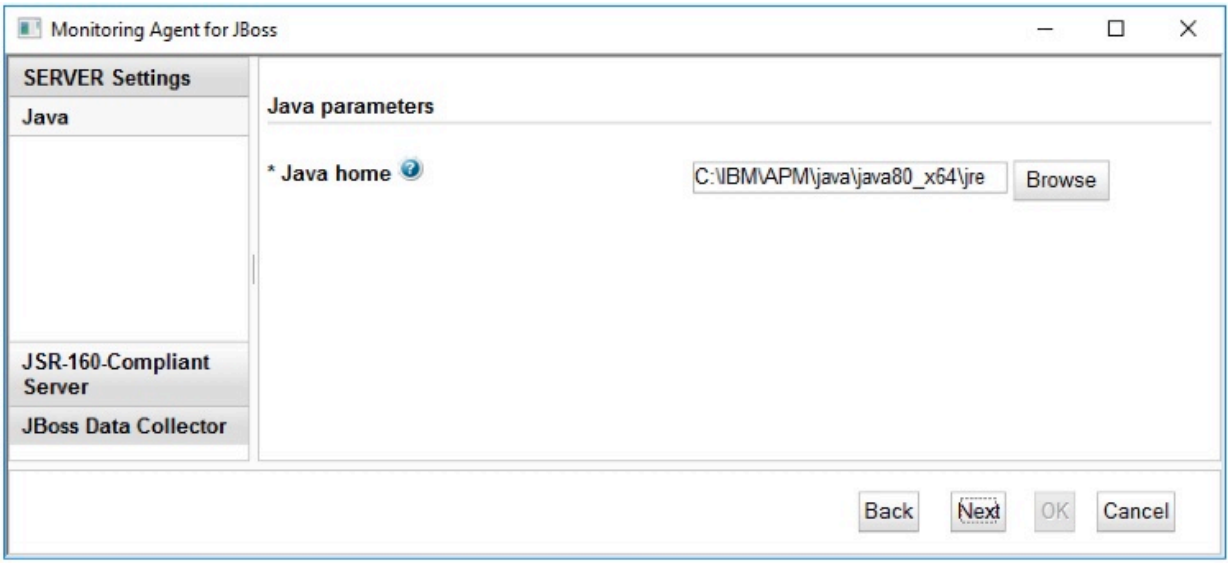


Figura 19. A janela para especificar configurações Java.

6. Insira as configurações JMX, em seguida, clique em **Avançar**.

   Consulte Tabela 167 na página 467 para obter uma explicação de cada um dos parâmetros de configuração.

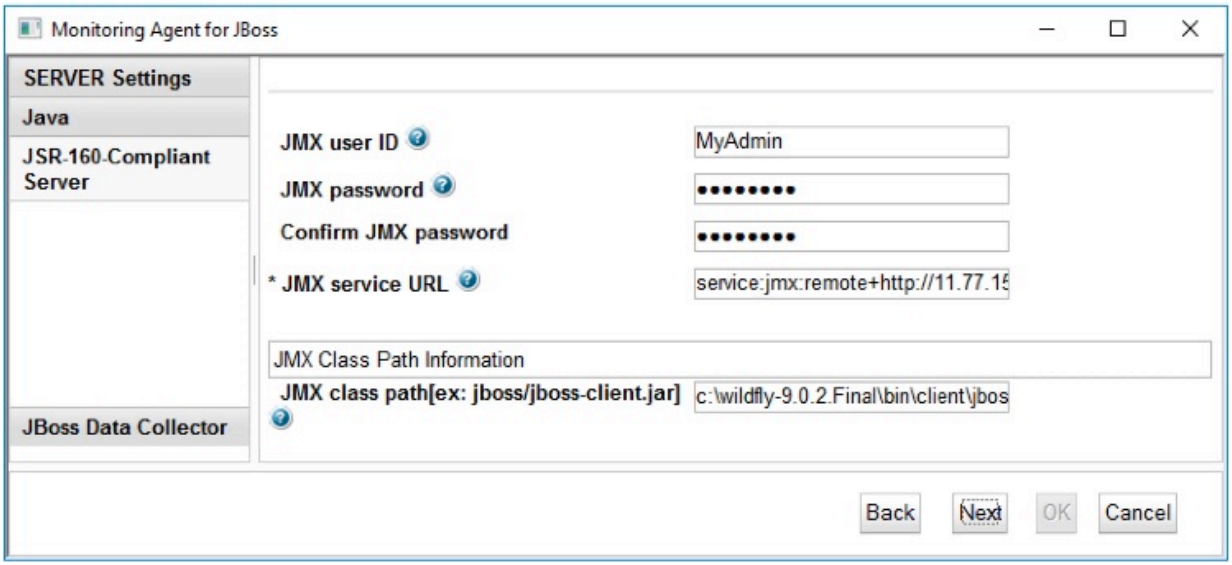


Figura 20. A janela para especificar configurações JMX.

7. Visualize as configurações do coletor de dados do agente JBoss.

   Deixe **`DC Runtime Directory`** em branco durante a configuração inicial do agente. Consulte Tabela 167 na página 467 para obter uma explicação de cada um dos parâmetros de configuração.

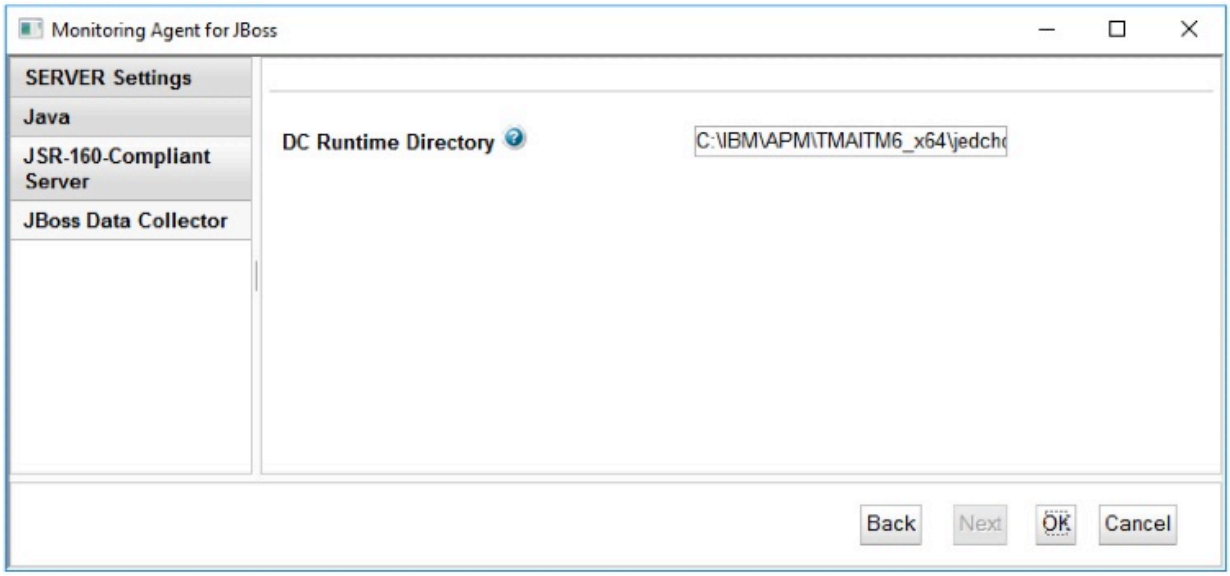


Figura 21. A janela para especificar configurações do coletor de dados do agente JBoss

8. Clique em **OK** para completar a configuração do agente.
9. Na janela IBM Cloud Application Performance Management, clique com o botão direito na instância configurada e, em seguida, clique em **Iniciar**.

Configurando o agente respondendo aos prompts

Após a instalação do agente JBoss, deve-se configurá-lo antes de iniciar o agente. Se o agente JBoss estiver instalado em um computador local Linux ou UNIX, é possível seguir essas instruções para configurá-lo interativamente através de prompts da linha de comandos.

Sobre Esta Tarefa

Lembre-se: Se estiver reconfigurando uma instância do agente configurada, o valor que é definido na última configuração será exibido para cada configuração. Se desejar limpar um valor existente, pressione a tecla Espaço quando a configuração for exibida.

Procedimento

1. Na linha de comandos, execute o seguinte comando:

   ```
   install_dir/bin/jboss-agent.sh config
   instance_name
   ```

   em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome que você deseja fornecer para a instância de agente.

   Exemplo

   ```
   /opt/ibm/apm/agent/bin/jboss-agent.sh config example-inst01
   ```

2. Responda aos prompts para configurar valores de configuração para o agente.

   Consulte "Parâmetros de Configuração para o agente JBoss" na página 466 para obter uma explicação de cada um dos parâmetros de configuração.

3. Execute o comando a seguir para iniciar o agente:

   ```
   install_dir/bin/jboss-agent.sh start
   instance_name
   ```

   em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome da instância de agente.

   Exemplo

   ```
   /opt/ibm/apm/agent/bin/jboss-agent.sh start example-inst01
   ```

Configurando o agente usando o arquivo silencioso de resposta

O arquivo de resposta silencioso contém os parâmetros de configuração do agente. É possível editar o arquivo de resposta silencioso para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

O arquivo silencioso de resposta contém os parâmetros de configuração do agente com valores padrão que são definidos para alguns parâmetros. É possível editar o arquivo silencioso de resposta para especificar os valores diferentes para os parâmetros de configuração.

Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

- Para configurar o agente JBoss no modo silencioso, conclua as seguintes etapas:
  a) Em um editor de texto, abra o arquivo `jboss_silent_config.txt` que está disponível no seguinte caminho:
  – Linux AIX *install_dir*`/samples/jboss_silent_config.txt`

    Exemplo, `/opt/ibm/apm/agent/samples/jboss_silent_config.txt`
  – Windows *install_dir*`\samples\jboss_silent_config.txt`

    em que *install_dir* é o caminho no qual o agente está instalado.

    O padrão *install_dir* caminhos são listados aqui:
  – Linux `/opt/ibm/apm/agent`
  – Windows `C:\IBM\APM\TMAITM6_x64`

Exemplo

Linux AIX
```
/opt/ibm/apm/agent/samples/jboss_silent_config.txt
```

Windows
```
C:\IBM\APM \samples\jboss_silent_config.txt
```

b) No arquivo `jboss_silent_config.txt`, especifique valores para todos os parâmetros obrigatórios. Também é possível modificar os valores padrão de outros parâmetros.

Consulte "Parâmetros de Configuração para o agente JBoss" na página 466 para obter uma explicação de cada um dos parâmetros de configuração.

c) Salve e feche o arquivo `jboss_silent_config.txt` e execute o seguinte comando:

– Linux AIX *install_dir*/bin/jboss-agent.sh config **instance_name** *install_dir*/samples/jboss_silent_config.txt

– Windows *install_dir*\bin\jboss-agent.bat config **instance_name** *install_dir* \samples\jboss_silent_config.txt

em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome da instância de agente.

O padrão *install_dir* caminhos são listados aqui:

– Linux `/opt/ibm/apm/agent`

– Windows `C:\IBM\APM\TMAITM6_x64`

Importante: Assegure que você inclua o caminho absoluto no arquivo silencioso de resposta. Caso contrário, os dados do agente não serão mostrados nos painéis.

Exemplo

Linux AIX
```
/opt/ibm/apm/agent/bin/jboss-agent.sh config example-inst01
/opt/ibm/apm/agent/samples/jboss_silent_config.txt
```

Windows
```
C:\IBM\APM \bin\jboss-agent.bat config example-inst01 C:\IBM\APM \samples
\jboss_silent_config.txt
```

d) Execute o comando a seguir para iniciar o agente:

– Linux AIX *install_dir*/bin/jboss-agent.sh start **instance_name**

– Windows *install_dir*\bin\jboss-agent.bat start **instance_name**

em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome da instância de agente.

O padrão *install_dir* caminhos são listados aqui:

– Linux `/opt/ibm/apm/agent`

– Windows `C:\IBM\APM\TMAITM6_x64`

Exemplo

Linux AIX
```
/opt/ibm/apm/agent/bin/jboss-agent.sh start example-inst01
```

Windows
```
C:\IBM\APM \bin\jboss-agent.bat start example-inst01
```

Parâmetros de Configuração para o agente JBoss

Os parâmetros de configuração para o agente JBoss são exibidos em uma tabela.

1. Configurações do agente JBoss - Configurações do ambiente do agente JBoss.

2. Tabela 168 na página 467 - URLs de serviço JMX de exemplo.

Tabela 167. Configurações do agente JBoss

Nome de parâmetro	Descrição	Nome do parâmetro do arquivo de configuração silenciosa
Nome do servidor	Forneça um nome para identificar o Servidor JBoss/WildFly.	**KJE_SERVER**
Diretório inicial Java	O caminho para onde o Java está instalado.	**JAVA_HOME**
ID do usuário JMX	O ID do usuário para conectar-se ao servidor MBean.	**KQZ_JMX_JSR160_JSR160_USER_ID**
Senha JMX	Senha	**KQZ_JMX_JSR160_JSR160_PASSWORD**
URL de serviço do JMX	A URL de serviço para conectar-se ao servidor MBean. Consulte Tabela 168 na página 467 para obter exemplos.	**KQZ_JMX_JSR160_JSR160_SERVICE_URL**
Caminho de classe JMX	Os arquivos JAR que são procurados para localizar uma classe ou recurso. Localize e insira o caminho para o arquivo `jboss-client.jar` de seu servidor JBoss. Exemplo para um servidor JBoss EAP 6, `/opt/EAP-6.3.0/jboss-eap-6.3/bin/client/jboss-client.jar`.	**KQZ_JMX_JSR160_JSR160_JAR_FILES**
DC Runtime Directory	**Nota:** Este parâmetro é apenas para o agente JBoss com o recurso de rastreamento de transações, que está na oferta do Cloud APM, Advanced. Para o agente JBoss com o recurso de monitoramento de recurso básico, que está na oferta do Cloud APM, Base, ignore esse parâmetro. O caminho completo para o diretório de tempo de execução do coletor de dados JBoss é configurado pelo script **`simpleConfig`**. Deixe este parâmetro em branco durante a configuração inicial do agente.	**KQZ_DC_RUNTIME_DIR**

Tabela 168. URLs de serviço JMX

Versão do servidor JBoss	URL de serviço JMX com a porta padrão[1]
WildFly 8, 9 e 10 JBoss EAP 7	`service:jmx:remote+http://ip:9990` `service:jmx:remote+https://ip:9994`
JBoss EAP 6 JBoss AS 7	`service:jmx:remoting-jmx://ip:9999`
JBoss EAP 5.2 JBoss AS 6.1	`service:jmx:rmi:///jndi/rmi://ip:1090/jmxrmi`

[1] A porta é baseada na porta na entrada do arquivo de configuração do JBoss `<socket-binding name="management-native" interface="management" port="${jboss.management.native.port:NNNN}"/>`. Se a porta foi mudada do valor padrão, ajuste-a de acordo com o número da porta no arquivo de configuração.

Configure o coletor de dados de rastreamento de transações do agente JBoss

O recurso de rastreamento de transações do agente JBoss requer mudanças no arquivo de configurações do ambiente da instância de agente, no arquivo de inicialização do servidor JBoss e no parâmetro de configuração do agente do Diretório de tempo de execução do DC. Um script é fornecido para ajudá-lo a fazer as mudanças.

Antes de Iniciar

Linux Assegure que o limite de recurso para o arquivo aberto seja maior do que 5.000 para que o kit de ferramentas de rastreamento da transação funcione corretamente.

- Exiba a configuração de limite do arquivo aberto atual. **`ulimit -n`**
- Exemplo: configurar o limite do arquivo aberto como 5.056. **`ulimit -n 5056`**

Execute Configurando a Etapa do agente JBoss "1" na página 457 ou "2" na página 457 antes de seguir este procedimento.

O agente JBoss deve ser instalado localmente para o servidor JBoss que é monitorado com o recurso de rastreamento de transações.

A conta do usuário que executa esse script deve ter permissão de gravação para os diretórios e arquivos a seguir:

1. O diretório *JBOSS_HOME*.
2. O diretório e arquivos *JBOSS_HOME*`/bin`.
3. O arquivo *JBOSS_HOME*`/modules/system/layers/base/org/jboss/as/server/main/module.xml`.
4. O diretório *install_dir*`/config`.
5. O arquivo *install_dir*`/config/`*hostname*`_je_`*instance_name*`.cfg`.

em que

JBOSS_HOME
Diretório de instalação do servidor JBoss.

install_dir
Caminho onde o agente está instalado. O caminho padrão é:

- Linux `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

nome_do_host
O nome do computador host no qual o agente está instalado.

instance_name
Nome da instância de agente que é designado no tópico do método de configuração do agente:

- Configurando o agente em sistemas Windows, etapa "3" na página 462
- Configurando o agente respondendo aos prompts, etapa "1" na página 465
- Configurando o agente usando o arquivo de resposta silencioso, etapa "3" na página 466

Procedimento

Execute o script **`simpleConfig`**.

1. Efetue login no servidor JBoss com o agente JBoss instalado.

2. Vá para o diretório de instalação do agente.
   - Linux *install_dir*
   - Windows *install_dir*\TMAITM6_x64

   em que *install_dir* é o caminho no qual o agente está instalado.

   O padrão *install_dir* caminhos são listados aqui:
   - Linux /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64
3. Mude o diretório para jedchome / 7.3.0.13.0/bin.
4. Execute o script de configuração.
   - Linux ./simpleConfig.sh
   - Windows simpleConfig.bat
5. Siga os prompts para inserir parâmetros para seu ambiente.
   a) Insira o *instance_name* do agente JBoss escolhido para a instância de agente.
   b) Insira o diretório de instalação do servidor JBoss.
      Se a variável de ambiente *JBOSS_HOME* estiver configurada, seu valor será oferecido como o valor padrão.

   em que

   JBOSS_HOME
   O diretório de instalação do servidor JBoss.

   instance_name
   O nome da instância de agente que é designado no tópico do método de configuração do agente:
   - Configurando o agente em sistemas Windows, etapa "3" na página 462
   - Configurando o agente respondendo aos prompts, etapa "1" na página 465
   - Configurando o agente usando o arquivo de resposta silencioso, etapa "3" na página 466

   install_dir
   É o caminho no qual o agente está instalado. O caminho padrão é:
   - Linux /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64
6. Reinicie o servidor JBoss e o agente se eles estiverem em execução.

Resultados

Arquivos do servidor JBoss que são mudados durante a configuração do rastreamento de transações:

- *JBOSS_HOME*/bin/standalone.conf

  Esse arquivo é atualizado com as definições de configuração necessárias para o recurso de rastreamento de transações. Os marcadores de configuração são inseridos no arquivo para uso quando você desativar o recurso de rastreamento de transações. Um arquivo de backup é salvo no diretório *JBOSS_HOME*/bak antes de incluir ou remover as mudanças no recurso de rastreamento de transações.
- *JBOSS_HOME*/modules/system/layers/base/org/jboss/as/server/main/module.xml

  Esse arquivo é atualizado com uma dependência do módulo Java EE API. Os marcadores de configuração são inseridos no arquivo para uso quando você desativar o recurso de rastreamento de transações. Um arquivo de backup é salvo no diretório *JBOSS_HOME*/bak antes de incluir ou remover as mudanças no recurso de rastreamento de transações.

Arquivos do agente que são mudados durante a configuração de rastreamento de transações:

- Arquivo de configuração da instância de agente
  - Linux *install_dir*/config/*hostname*_je_*instance_name*.cfg
  - Windows *install_dir*\TMAITM6_x64*hostname*_JE_*instance_name*.cfg
- Arquivo de configurações do ambiente do agente
  - Linux *install_dir*/config/je_*instance_name*.environment
  - Windows *install_dir*\TMAITM6_x64\KJEENV_*instance_name*

em que

JBOSS_HOME
Diretório de instalação do servidor JBoss.

install_dir
Caminho onde o agente está instalado. O caminho padrão é:

- Linux /opt/ibm/apm/agent
- Windows C:\IBM\APM\TMAITM6_x64

nome_do_host
O nome do computador host no qual o agente está instalado.

instance_name
Nome da instância de agente que é designado no tópico do método de configuração do agente:

- Configurando o agente em sistemas Windows, etapa "3" na página 462
- Configurando o agente respondendo aos prompts, etapa "1" na página 465
- Configurando o agente usando o arquivo de resposta silencioso, etapa "3" na página 466

Desativar o coletor de dados de rastreamento de transações do agente JBoss
O recurso de rastreamento de transações do agente JBoss requer mudanças no arquivo de configurações do ambiente da instância de agente, no arquivo de inicialização do servidor JBoss e no parâmetro de configuração do agente do Diretório de tempo de execução do DC. Um script é fornecido para remover essas mudanças para uma instância de agente com o rastreamento de transações ativado.

Antes de Iniciar

Assegure-se de que o servidor JBoss e o agente JBoss estejam encerrados.

A conta do usuário que executa esse script deve ter permissão de gravação para os diretórios e arquivos a seguir:

1. O diretório *JBOSS_HOME*
2. O diretório *JBOSS_HOME*/bin e os arquivos
3. O arquivo *JBOSS_HOME*/modules/system/layers/base/org/jboss/as/server/main/module.xml
4. O diretório *install_dir*/config
5. O arquivo *install_dir*/config/*hostname*_je_*instance_name*.cfg

Procedimento

Execute o script **simpleConfig** com a opção **remove**.

1. Efetue login no servidor JBoss com o agente JBoss instalado.
2. Vá para o diretório de instalação do agente.
   - Linux *install_dir*
   - Windows *install_dir*\TMAITM6_x64
3. Mude o diretório para jedchome / 7.3.0.13.0/bin.

4. Execute o **simpleconfig** com a opção **remove**.
   - Linux `./simpleConfig.sh` **remove** *instance_name*
   - Windows `simpleConfig.bat` **remove** *instance_name*
5. Inicie o servidor JBoss e o agente.

Em que:

JBOSS_HOME
O diretório de instalação do servidor JBoss

nome_do_host
O nome do computador host no qual o agente está instalado

instance_name
O nome da instância de agente que é designado no tópico do método de configuração do agente:
- Configurando o agente em sistemas Windows, etapa "3" na página 462
- Configurando o agente respondendo aos prompts, etapa "1" na página 465
- Configurando o agente usando o arquivo de resposta silencioso, etapa "3" na página 466

install_dir
É o caminho no qual o agente está instalado. O caminho padrão é:
- Linux `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

architecture
O identificador de arquitetura do sistema IBM Application Performance Management ou Cloud APM. Por exemplo, lx8266 representa o Linux Intel v2.6 (64 bits). Para obter uma lista completa dos códigos de arquitetura, consulte o arquivo *install_dir*`/registry/archdsc.tbl`.

Desinstalar todos os rastreamentos de transações do agente JBoss
O recurso de rastreamento de transações do agente JBoss pode ser desinstalado. Um script é fornecido para remover todas as instâncias do agente com o rastreamento de transações ativado e também remover o kit ferramentas de rastreamento de transações.

Antes de Iniciar

Assegure-se de que o servidor JBoss e todas as instâncias do agente JBoss estejam encerrados.

A conta do usuário que executa esse script deve ter permissão de gravação para os diretórios e arquivos a seguir:

1. O diretório *JBOSS_HOME*.
2. O diretório e arquivos *JBOSS_HOME*`/bin`.
3. O arquivo *JBOSS_HOME*`/modules/system/layers/base/org/jboss/as/server/main/module.xml`.
4. O diretório *install_dir*`/config`.
5. O arquivo *install_dir*`/config/`*hostname*`_je_`*instance_name*`.cfg`.

Procedimento

Execute o script **simpleConfig** com a opção **uninstall**.

1. Efetue login no servidor JBoss com o agente JBoss instalado.
2. Vá para o diretório de instalação do agente.
   - Linux *install_dir*`/`*architecture*`/je/bin`. Por exemplo: `/opt/ibm/apm/agent/lx8266/je/bin` ou `/opt/ibm/apm/agent/lx8266/je/bin`
   - Windows *install_dir*\TMAITM6_x64

3. Mude o diretório para `jedchome / 7.3.0.13.0/bin`.
4. Execute o **simpleConfig** com a opção **uninstall**.
   - Linux `./simpleConfig.sh` **uninstall**
   - Windows `simpleConfig.bat` **uninstall**
5. Inicie o servidor JBoss e todas as instâncias de agente.

Em que:

JBOSS_HOME
O diretório de instalação do servidor JBoss.

nome_do_host
O nome do computador host no qual o agente está instalado.

instance_name
O nome da instância de agente que é designado no tópico do método de configuração do agente:

- Configurando o agente em sistemas Windows, etapa "3" na página 462
- Configurando o agente respondendo aos prompts, etapa "1" na página 465
- Configurando o agente usando o arquivo de resposta silencioso, etapa "3" na página 466

install_dir
É o caminho no qual o agente está instalado. O caminho padrão é:

- Linux `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

architecture
O identificador de arquitetura do sistema IBM Application Performance Management ou Cloud APM. Por exemplo, lx8266 representa o Linux Intel v2.6 (64 bits). Para obter uma lista completa dos códigos de arquitetura, consulte o arquivo *install_dir*`/registry/archdsc.tbl`.

Configurando o monitoramento do Linux KVM

Você deve configurar o Monitoring Agent for Linux KVM para coletar dados dos servidores Red Hat Enterprise Virtualization Hypervisor (RHEVH) e Red Hat Enterprise Virtualization Manager (RHEVM). Depois de instalar o agente em um servidor ou máquina virtual, você deve criar a primeira instância e iniciar o agente manualmente.

Antes de Iniciar
Revise os pré-requisitos de hardware e de software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o agente do Linux KVM.

Sobre Esta Tarefa
O agente do Linux KVM é um agente multi-instância e multiconexão. Multi-instância significa que é possível criar várias instâncias e cada instância pode estabelecer várias conexões com um ou mais servidores RHEVM ou RHEVH.

Lembre-se: Use diferentes instâncias para monitorar servidores RHEVM ou RHEVH.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte o "Histórico de Mudanças" na página 50.

É possível usar o mesmo script de configuração para configurar instâncias para os servidores RHEVH e RHEVM:

- Para configurar uma conexão com o servidor RHEVM, conclua as etapas mencionadas no tópico "Configurando uma conexão com o servidor RHEVM".
- Para configurar uma conexão com o servidor RHEVH, conclua as etapas mencionadas no tópico "Configurando uma conexão com o servidor RHEVH".

Criando um usuário e concedendo as permissões necessárias

Antes de configurar o agente do Linux KVM, você deve criar um usuário e conceder permissões necessárias ao usuário para monitorar os servidores RHEVM e RHEVH.

Procedimento

1. Abra o portal **Red Hat Enterprise Virtualization Manager Web Administration** .
2. Clique em **Configurar**.
3. Na janela **Configuração**, selecione **Funções**.
   a) Para criar uma função, clique em **Novo**.
   b) Na janela **Nova Função**, inclua o nome da função e selecione **Administrador** como o tipo de conta.
   c) Certifique-se de que as caixas de seleção na área de janela **Caixas de seleção para permitir ação** não estejam selecionadas e clique em **OK**.
4. Na janela **Configuração**, selecione **Permissão do sistema**.
   a) Para conceder uma permissão de usuário, clique em **Incluir**.
   b) Na janela **Incluir permissão do sistema para usuário**, selecione o usuário a quem deseja conceder a permissão.
   c) Na lista **Designar função ao usuário**, selecione a função criada e clique em **OK**.

O que Fazer Depois

Conclua a configuração do agente:

- “Configurando uma conexão com o servidor RHEVH” na página 479
- “Configurando uma conexão com o servidor RHEVM” na página 477

Configurando Protocolos

O agente usa diferentes protocolos para se conectar ao servidor RHEVH. É possível configurar qualquer um desses protocolos: SSH, TLS ou TCP.

Sobre Esta Tarefa

O agente do Linux KVM se conecta remotamente a cada hypervisor usando a ferramenta **`virsh`** que gerencia suas máquinas virtuais QEMU-KVM e coleta métricas. A API `libvirt` no ambiente do agente usa vários diferentes protocolos de transporte remoto. Para obter a lista de protocolos suportados, consulte a Página de suporte remoto.

Configurando o protocolo SSH

É possível configurar o protocolo SSH para monitorar remotamente um host.

Sobre Esta Tarefa

Suposição: o agente do Linux KVM é instalado no host A. Você deseja monitorar remotamente o hypervisor no host B.

Procedimento

1. Efetue login no host A com o mesmo ID do usuário que executa o processo do agente do Linux KVM, por exemplo, o ID do usuário raiz.

   Dica: Certifique-se de que saiba o ID no host B que aceita a conexão SSH e o ID do usuário raiz no host A.

2. Gere as chaves **id_rsa** e **id_rsa.pub** no host A usando o utilitário *ssh-keygen*.
   As chaves são salvas no seguinte local: `~/.ssh: $ ssh-keygen -t rsa`.
3. Copie as chaves autorizadas do host B:

   $ scp Id on host B@name or IP address of host B:~/.ssh/authorized_keys ~/.ssh/authorized_keys_from_B
4. Conecte a chave pública para o host A à extremidade das chaves autorizadas para o host B:

   cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys_from_B
5. Copie as chaves autorizadas de volta para o host B:

   $ scp ~/.ssh/authorized_keys_from_B Id on host B@name or IP address of host B:~/.ssh/authorizede_keys

   Lembre-se: Se você estiver monitorando vários hosts, repita as etapas "3" na página 474, "4" na página 474 e "5" na página 474 para cada host.
6. Remova as chaves autorizadas que foram copiadas no host B:

   ~/.ssh/authorized_keys_from_B
7. Inclua o seguinte comando no perfil **~/.bash_** do ID atual no host A:

   $ eval `ssh-agent`

   Lembre-se: Certifique-se de usar o acento grave (`) que está localizado abaixo do til (~) em teclados dos EUA, em vez das aspas simples (').
8. Inclua a identidade no host A e insira a senha que foi usada durante a criação do ID:

   $ ssh-add ~/.ssh/id_rsa
9. Execute o seguinte comando se você receber a mensagem `Não foi possível abrir uma conexão com o agente de autenticação`:

   exec ssh-agent bash

   Dica: É possível substituir o bash pelo shell que você está usando e, em seguida, execute o seguinte comando novamente:

   $ ssh-add ~/.ssh/id_rsa
10. Teste o protocolo SSH para assegurar que ele se conecta do host A ao host B sem inserir a senha SSH:

    Dica: Se estiver monitorando vários hosts, use o seguinte comando para testar a conexão para cada host:

    $ ssh Id on host B@name or IP address of host B
11. Para verificar a conexão, execute o seguinte comando:

    virsh -c qemu+ssh://Id on host B@name or IP address of host B:port/system

    Se você não mudou a porta SSH padrão, omita a seção **:port** do comando.

    Importante: Se o comando **virsh** for bem-sucedido, o agente do Linux KVM se conectará ao hypervisor.
12. Deve-se reiniciar o host A antes de reiniciar o agente do Linux KVM no host A. Para reiniciar, execute o comando **ssh-add** novamente e especifique a senha todas as vezes.

    Dica: É possível usar cadeias chaves de SSH para evitar inserir a senha novamente.

Configurando o protocolo TLS
É possível configurar o protocolo TLS para monitorar um host remotamente.

Sobre Esta Tarefa
Suposição: o agente do Linux KVM é instalado no host A. Você deseja monitorar remotamente o hypervisor no host B.

Procedimento

1. Para criar uma chave de autoridade de certificação (CA) e um certificado em seu hypervisor, conclua as seguintes etapas:
   a) Efetue login no host B.
   b) Crie um diretório temporário e mude o caminho para esse diretório temporário:

      ```
      mkdir cert_files
      cd cert_files
      ```

   c) Crie uma chave RSA de 2048 bits:

      ```
      openssl genrsa -out cakey.pem 2048
      ```

   d) Crie um certificado autoassinado para sua CA local:

      ```
      openssl req -new -x509 -days 1095 -key cakey.pem -out \
      cacert.pem -sha256 -subj "/C=US/L=Austin/O=IBM/CN=my CA"
      ```

   e) Verifique seu certificado de CA:

      ```
      openssl x509 -noout -text -in cacert.pem
      ```

2. Para criar as chaves e certificados do cliente e do servidor em seu hypervisor, conclua as seguintes etapas:
   a) Crie as chaves:

      ```
      openssl genrsa -out serverkey.pem 2048
      openssl genrsa -out clientkey.pem 2048
      ```

   b) Crie uma solicitação de assinatura de certificado para o servidor:

      Lembre-se: Mude o endereço kvmhost.company.org, que é usado na solicitação de certificado do servidor, para o nome completo do domínio do host do hypervisor.

      ```
      openssl req -new -key serverkey.pem -out serverkey.csr \
      -subj "/C=US/O=IBM/CN=kvmhost.company.org"
      ```

   c) Crie um pedido de assinatura de certificado para o cliente:

      ```
      openssl req -new -key clientkey.pem -out clientkey.csr \
      -subj "/C=US/O=IBM/OU=virtualization/CN=root"
      ```

   d) Crie certificados do cliente e do servidor:

      ```
      openssl x509 -req -days 365 -in clientkey.csr -CA cacert.pem \
      -CAkey cakey.pem -set_serial 1 -out clientcert.pem
      openssl x509 -req -days 365 -in serverkey.csr -CA cacert.pem \
      -CAkey cakey.pem -set_serial 94345 -out servercert.pem
      ```

   e) Verifique as chaves:

      ```
      openssl rsa -noout -text -in clientkey.pem
      openssl rsa -noout -text -in serverkey.pem
      ```

   f) Verifique os certificados:

      ```
      openssl x509 -noout -text -in clientcert.pem
      openssl x509 -noout -text -in servercert.pem
      ```

3. Para distribuir as chaves e certificados no servidor host, conclua as seguintes etapas:
   a) Copie o arquivo `cacert.pem` do certificado de CA para esse diretório: `/etc/pki/CA`

      ```
      cp cacert.pem /etc/pki/CA/cacert.pem
      ```

   b) Crie o diretório `/etc/pki/libvirt` e copie o arquivo de certificado do servidor `servercert.pem` para o diretório `/etc/pki/libvirt`. Certifique-se de que somente o usuário raiz pode acessar a chave privada.

mkdir /etc/pki/libvirt

cp servercert.pem /etc/pki/libvirt/.

chmod -R o-rwx /etc/pki/libvirt

Lembre-se: Se as chaves ou certificados são nomeados incorretamente ou copiados para os diretórios errados, a autorização falha.

c) Crie o diretório `/etc/pki/libvirt/private` e copie o arquivo-chave do servidor `serverkey.pem` para o diretório `/etc/pki/libvirt/private`. Certifique-se de que somente o usuário raiz pode acessar a chave privada.

mkdir /etc/pki/libvirt/private

cp serverkey.pem /etc/pki/libvirt/private/.

chmod -R o-rwx /etc/pki/libvirt/private

Lembre-se: Se as chaves ou certificados são nomeados incorretamente ou copiados para os diretórios errados, a autorização falha.

d) Verifique se os arquivos estão posicionados corretamente:

find /etc/pki/CA/*|xargs ls -l

ls -lR /etc/pki/libvirt

ls -lR /etc/pki/libvirt/private

Lembre-se: Se as chaves ou certificados são nomeados incorretamente ou copiados para os diretórios errados, a autorização falha.

4. Para distribuir chaves e certificados para clientes ou estações de gerenciamento, conclua as seguintes etapas:

a) Efetue login no host A.

b) Copie o `cacert.pem` do certificado de CA do host para o diretório `/etc/pki/CA` no host A sem mudar o nome do arquivo.

scp kvmhost.company.org:/tmp/cacert.pem /etc/pki/CA/

c) Copie o arquivo `clientcert.pem` do certificado de cliente para o diretório `/etc/pki/libvirt` do host B. Use os nomes de arquivos padrão e certifique-se de que somente o usuário raiz pode acessar a chave privada.

mkdir /etc/pki/libvirt/

scp kvmhost.company.org:/tmp/clientcert.pem /etc/pki/libvirt/.

chmod -R o-rwx /etc/pki/libvirt

Lembre-se: Se as chaves ou certificados são nomeados incorretamente ou copiados para os diretórios errados, a autorização falha.

d) Copie o `clientkey.pem` da chave do cliente para o diretório `/etc/pki/libvirt/private` do host. Use os nomes de arquivos padrão e certifique-se de que somente o usuário raiz pode acessar a chave privada.

mkdir /etc/pki/libvirt/private

scp kvmhost.company.org:/tmp/clientkey.pem /etc/pki/libvirt/private/.

chmod -R o-rwx /etc/pki/libvirt/private

Lembre-se: Se as chaves ou certificados são nomeados incorretamente ou copiados para os diretórios errados, a autorização falha.

e) Verifique se os arquivos estão posicionados corretamente:

ls -lR /etc/pki/libvirt

ls -lR /etc/pki/libvirt/private

5. Para editar a configuração do daemon `libvirtd`, conclua as seguintes etapas:
   a) Efetue login no host B.
   b) Faça uma cópia do arquivo `/etc/sysconfig/libvirtd` e do arquivo `/etc/libvirt/libvirtd.conf`.
   c) Edite o arquivo `/etc/sysconfig/libvirtd` e certifique-se de que o parâmetro **`--listen`** seja transmitido para o daemon `libvirtd`. Esta etapa assegura que o daemon `libvirtd` está atendendo conexões de rede.
   d) Edite o arquivo `/etc/libvirt/libvirtd.conf` e configure um conjunto de assuntos permitidos com a diretiva **`tls_allowed_dn_list`** no arquivo `libvirtd.conf`.

      Importante: Os campos no assunto devem estar na mesma ordem usada para criar o certificado.
   e) Reinicie o serviço do daemon `libvirtd` para que as alterações tenham efeito:

      `/etc/init.d/libvirtd restart`
6. Para mudar a configuração de firewall, acesse a configuração de nível de segurança e inclua a porta TCP 16514 como uma porta confiável.
7. Para verificar se o gerenciamento remoto está funcionando, execute o seguinte comando no host A:

   `virsh -c qemu+tls://kvmhost.company.org/system list --all`

Configurando o protocolo TCP
Use o protocolo TCP somente para teste.

Sobre Esta Tarefa
Suposição: o agente do Linux KVM é instalado no host A. Você deseja monitorar remotamente o hypervisor no host B.

Procedimento

1. Efetue login no host B.
2. Edite o arquivo `/etc/libvirt/libvirtd.conf` e certifique-se de que o parâmetro **`listen_tcp`** esteja ativado e o valor do parâmetro **`tcp_port`** esteja configurado como o valor padrão de 16509.
3. Edite o arquivo `/etc/libvirt/libvirtd.conf` para configurar o parâmetro **`auth_tcp`** como "none". Essa etapa instrui o TCP a não autenticar a conexão.
4. Reinicie o daemon **`libvirt`** no host B no modo de atendimento executando-o com a sinalização **`--listen`** ou editando o arquivo `/etc/sysconfig/libvirtd` e removendo o comentário da linha `LIBVIRTD_ARGS="--listen"`.
5. Para verificar a conexão, execute o seguinte comando:

   `virsh -c qemu+tcp://kvmhost.company.org:port/system`

   Se você não mudou a porta TCP padrão, omita a seção **`:port`** do comando.

   Importante: Se o comando **`virsh`** for bem-sucedido, o agente do Linux KVM se conectará ao hypervisor.

O que Fazer Depois
Configure o agente concluindo as etapas descritas em "Configurando uma conexão com o servidor RHEVH" na página 479.

Configurando uma conexão com o servidor RHEVM

Para configurar uma conexão com o servidor RHEVM, você deve executar o script e responder aos prompts.

Antes de Iniciar

1. Faça download do certificado de segurança que está disponível no seguinte caminho:

```
https://RHEVM-HOST:RHEVM-PORT/ca.crt
```

Em que

RHEVM-HOST
O nome do host.

RHEVM-PORT
A porta usada em seu ambiente RHEVM.

2. Use o utilitário *keytool* para importar o arquivo de certificado de segurança para gerar um arquivo keystore local:

   keytool -import -alias ALIAS -file CERTIFICATE_FILE -keystore KEYSTORE_FILE

   Exemplo **keytool -import -alias RHEVM36vmwt9 -file hjs495-vmw-t-9.cer -keystore RHEVM36KeyStore**

   Em que

   ALIAS
   Uma referência exclusiva para cada certificado que é incluído no armazenamento confiável do certificado do agente, por exemplo, um alias apropriado para o certificado de *datasource.example.com* é *datasource*.

   CERTIFICATE_FILE
   O caminho completo e nome do arquivo para o certificado de origem de dados que está sendo incluído no armazenamento confiável.

   KEYSTORE_FILE
   O nome do arquivo keystore que você deseja especificar.

   Dica: O utilitário *keytool* está disponível com o Java Runtime Environment (JRE). O arquivo keystore é armazenado no mesmo local de onde você executa o comando.

3. Certifique-se de que o usuário, que se conecta ao RHEVM, seja um administrador com a função SuperUser. É possível usar um ID do usuário existente com essa função, ou criar um novo ID do usuário, concluindo as etapas mencionadas em "Criando um usuário e concedendo as permissões necessárias" na página 473.

Procedimento

1. Na linha de comandos, execute o seguinte comando:

   install_dir/bin/linux_kvm-agent.sh config instance_name

   Exemplo **/opt/ibm/apm/agent/bin/linux_kvm-agent.sh config instance_name**

   Em que

   instance_name
   É o nome a ser atribuído à instância.

   install_dir
   É o caminho no qual o agente está instalado.

2. Responda aos prompts e especifique valores para os parâmetros de configuração.

   Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração para conectar-se ao servidor RHEVM" na página 479.

3. Execute o comando a seguir para iniciar o agente:

   install_dir/bin/linux_kvm-agent.sh start instance_name

   Exemplo **/opt/ibm/apm/agent/bin/linux_kvm-agent.sh start instance_name**

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.

Configurando uma conexão com o servidor RHEVH

Para configurar uma conexão com o servidor RHEVH, você deve executar o script e responder aos prompts.

Antes de Iniciar

- Certifique-se de que o usuário, que se conecta ao RHEVM, seja um usuário raiz. É possível usar um ID do usuário existente ou criar um novo ID do usuário concluindo as etapas mencionadas em "Criando um usuário e concedendo as permissões necessárias" na página 473.
- Configure o protocolo que você deseja usar para conectar-se ao servidor RHEVH concluindo as etapas descritas em "Configurando Protocolos" na página 473.

Procedimento

1. Na linha de comandos, execute o seguinte comando:

   `install_dir/bin/linux_kvm-agent.sh config instance_name`

   Exemplo **`/opt/ibm/apm/agent/bin/linux_kvm-agent.sh config instance_name`**

   Em que

   instance_name
   É o nome a ser atribuído à instância.

   install_dir
   É o caminho no qual o agente está instalado.
2. Responda aos prompts e especifique valores para os parâmetros de configuração.

   Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração para conectar-se ao servidor RHEVH" na página 481.
3. Execute o comando a seguir para iniciar o agente:

   `install_dir/bin/linux_kvm-agent.sh start instance_name`

   Exemplo **`/opt/ibm/apm/agent/bin/linux_kvm-agent.sh start instance_name`**

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.

Parâmetros de configuração para conectar-se ao servidor RHEVM

É possível modificar os valores padrão de parâmetros de configuração que são usados para conectar o agente ao servidor RHEVM.

A tabela a seguir contém descrições detalhadas dos parâmetros de configuração.

Tabela 169. Nomes e descrições dos parâmetros de configuração para conexão com o servidor RHEVM		
Nome de parâmetro	**Descrição**	**Campo obrigatório**
Editar configurações do Monitoring Agent for Linux KVM	Indica que é possível começar a editar os valores padrão dos parâmetros de configuração. Insira `1 (Sim)`, que também é o valor padrão, para continuar.	Sim
Número Máximo de Arquivos de Log do Provedor de Dados	O número máximo de arquivos de log que o provedor de dados cria antes de sobrescrever os arquivos de log anteriores. O valor padrão é 10.	Sim
Tamanho Máximo em KB de Cada Log do Provedor de Dados	O tamanho máximo em KB que um provedor de dados deve atingir antes de o provedor de dados criar um novo arquivo de log. O valor padrão são 5190 KB.	Sim
Nível de Detalhe no Log do Provedor de Dados	O nível de detalhes que pode ser incluído no arquivo de log criado pelo provedor de dados. O valor padrão é 4 (Informativo). Os seguintes valores são válidos: • 1 = Desativado: nenhuma mensagem é registrada. • 2 = Grave: somente erros são registrados. • 3 = Aviso: todos os erros e mensagens que são registrados no nível Grave e erros potenciais que podem resultar em comportamento indesejado. • 4 = Informativo: todos os erros e mensagens que são registrados no nível de Aviso e as mensagens informativas de alto nível que descrevem o estado do provedor de dados quando ele é processado. • 5 = Bom: todos os erros e mensagens que são registrados no nível Informativo e mensagens informativas de baixo nível que descrevem o estado do provedor de dados quando ele é processado. • 6 = Melhor: todos os erros e mensagens que são registrados no nível Bom, além de mensagens informativas altamente detalhadas, como informações de criação de perfil de desempenho e dados de depuração. Selecionar essa opção pode afetar de maneira adversa o desempenho do agente de monitoramento. Esta configuração é destinada somente como uma ferramenta para determinação de problema juntamente com a equipe de suporte IBM. • 7 = Excelente: todos os erros e mensagens que são registrados no nível Bom e as mensagens informativas mais detalhadas que incluem mensagens de programação de baixo nível e dados. Escolher essa opção pode afetar, de maneira adversa, o desempenho do agente de monitoramento. Esta configuração é destinada somente como uma ferramenta para determinação de problema juntamente com a equipe de suporte IBM. • 8 = Todos: todos os erros e mensagens são registrados.	Sim
Editar configurações do Hypervisor	Indica se você deseja editar os parâmetros para uma conexão com o servidor RHEVH. Insira `5 (Avançar)` porque você está configurando uma conexão com o servidor RHEVM. O valor padrão é `5 (Avançar)`.	Sim

Tabela 169. Nomes e descrições dos parâmetros de configuração para conexão com o servidor RHEVM (continuação)		
Nome de parâmetro	**Descrição**	**Campo obrigatório**
Editar configurações de Detalhes da conexão do RHEVM	Indica se você deseja editar os parâmetros para uma conexão com o servidor RHEVM. Insira `1 (Incluir)` para continuar. O valor padrão é `5 (Avançar)`. **Importante:** Depois de especificar valores para todos os parâmetros de configuração, é solicitado novamente que indique se deseja continuar a editar os parâmetros. Insira `5 (Sair)`.	Sim
ID de RHEVM	O nome do usuário exclusivo, que é especificado para o RHEVM ao qual você se conecta.	Sim
Host	O nome do host ou endereço IP da origem de dados que é usada para conectar-se ao servidor RHEVM.	Sim
Usuário	O nome do usuário da origem de dados com privilégios suficientes para conectar-se ao servidor RHEVM.	Sim
Senha	A senha do nome de usuário que você usa para se conectar ao servidor RHEVM.	Sim
Digitar a Senha Novamente	A mesma senha que foi especificada no campo **Senha**.	Sim
Porta	O número da porta que é usada para se conectar ao servidor RHEVM.	Sim
Domínio	O domínio ao qual o usuário pertence.	Sim
KeyStorePath	O caminho do arquivo e o nome do arquivo keystore local que você criou usando o o comando **keytool**.	Sim

Parâmetros de configuração para conectar-se ao servidor RHEVH

É possível modificar os valores padrão de parâmetros de configuração que são usados para conectar o agente com o servidor RHEVH.

A tabela a seguir contém descrições detalhadas dos parâmetros de configuração.

Tabela 170. Nomes e descrições dos parâmetros de configuração para conexão com o hypervisor		
Nome de parâmetro	**Descrição**	**Campo obrigatório**
Editar configurações do Monitoring Agent for Linux KVM	Indica que é possível começar a editar os valores padrão dos parâmetros de configuração. Insira `1 (Sim)`, que também é o valor padrão, para continuar.	Sim
Número Máximo de Arquivos de Log do Provedor de Dados	O número máximo de arquivos de log que o provedor de dados cria antes de sobrescrever os arquivos de log anteriores. O valor padrão é 10.	Sim
Tamanho Máximo em KB de Cada Log do Provedor de Dados	O tamanho máximo em KB que um provedor de dados deve atingir antes de o provedor de dados criar um novo arquivo de log. O valor padrão são 5190 KB.	Sim

Tabela 170. Nomes e descrições dos parâmetros de configuração para conexão com o hypervisor (continuação)

Nome de parâmetro	Descrição	Campo obrigatório
Nível de Detalhe no Log do Provedor de Dados	O nível de detalhes que pode ser incluído no arquivo de log criado pelo provedor de dados. O valor padrão é 4 (Informativo). Os seguintes valores são válidos: • 1 = Desativado: nenhuma mensagem é registrada. • 2 = Grave: somente erros são registrados. • 3 = Aviso: todos os erros e mensagens que são registrados no nível Grave e erros potenciais que podem resultar em comportamento indesejado. • 4 = Informativo: todos os erros e mensagens que são registrados no nível de Aviso e as mensagens informativas de alto nível que descrevem o estado do provedor de dados quando ele é processado. • 5 = Bom: todos os erros e mensagens que são registrados no nível Informativo e mensagens informativas de baixo nível que descrevem o estado do provedor de dados quando ele é processado. • 6 = Melhor: todos os erros e mensagens que são registrados no nível Bom, além de mensagens informativas altamente detalhadas, como informações de criação de perfil de desempenho e dados de depuração. Selecionar essa opção pode afetar de maneira adversa o desempenho do agente de monitoramento. Esta configuração é destinada somente como uma ferramenta para determinação de problema juntamente com a equipe de suporte IBM. • 7 = Excelente: todos os erros e mensagens que são registrados no nível Bom e as mensagens informativas mais detalhadas que incluem mensagens de programação de baixo nível e dados. Selecionar essa opção pode afetar negativamente o desempenho do agente de monitoramento. Esta configuração é destinada somente como uma ferramenta para determinação de problema juntamente com a equipe de suporte IBM. • 8 = Todos: todos os erros e mensagens são registrados.	Sim
Editar configurações do Hypervisor	Indica se você deseja editar os parâmetros para uma conexão do Hypervisor. Insira `1 (Incluir)`. O valor padrão é `5 (Avançar)`.	Sim
ID do Hypervisor	O nome do usuário exclusivo, que é especificado para o RHEVH ao qual você se conecta.	Sim
Host	O nome do host ou endereço IP da origem de dados que é usada para conectar-se ao servidor RHEVH.	Sim
Usuário	Um nome do usuário da origem de dados com privilégios suficientes para conectar-se ao servidor RHEVM.	Sim

Tabela 170. Nomes e descrições dos parâmetros de configuração para conexão com o hypervisor (continuação)		
Nome de parâmetro	**Descrição**	**Campo obrigatório**
Transporte Remoto	O protocolo que é usado pela API `libvirt` local para conectar-se às APIs remotas `libvirt`. O valor padrão é 1. Os seguintes valores são válidos: • 1 = SSH • 2 = TLS • 3 = TCP (Descriptografado - não recomendado para uso de produção)	Sim
Porta	A porta que é usada pelo protocolo de transporte para conectar-se à API `libvirt`. O valor padrão é 22. **Importante:** Essa porta será necessária somente se as portas padrão tiverem sido mudadas (22 para SSH, 16514 para TLS, 16509 para TCP).	Sim
Domínio	O domínio ao qual o usuário pertence.	Sim
Tipo de Instância de Conexão	Indica se a API local `libvirt` se conecta ao driver do sistema privilegiado ou ao driver da sessão não privilegiado por usuário. O valor padrão é 1. Os seguintes valores são válidos: • 1 = system • 2 = session	Sim
Editar configurações de Detalhes da conexão do RHEVM	Indica se você deseja editar os parâmetros para uma conexão com o servidor RHEVM. Insira `1 (Incluir)` para continuar. O valor padrão é `5 (Avançar)`. **Importante:** Depois de especificar valores para todos os parâmetros de configuração, é solicitado novamente que indique se deseja continuar a editar os parâmetros. Insira `5 (Avançar)`.	Sim

Configurando o monitoramento do MariaDB

Deve-se configurar o MariaDB agent para que o agente possa coletar dados para monitorar a disponibilidade e o desempenho dos recursos do servidor MariaDB. Consulte os seguintes pré-requisitos para configurar o agente MariaDB para monitoramento remoto e local.

Antes de Iniciar

Assegure-se de que os requisitos do sistema para o MariaDB agent sejam atendidos em seu ambiente. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o MariaDB agent.

Sobre Esta Tarefa

O agente do MariaDB é um agente de instância única. Deve-se configurar o agente manualmente após sua instalação. É possível configurar o agente nos sistemas operacionais Windows e Linux. O agente requer um nome de instância e as credenciais do usuário do servidor MariaDB para configurá-lo. O nome do sistema gerenciado inclui o nome da instância especificada, por exemplo *instance_name*:*host_name*:*pc*, em que *pc* é o código de produto de dois caracteres. O nome do sistema gerenciado pode conter até 32 caracteres. O nome da instância especificado pode conter até 28

caracteres, excluindo o comprimento do seu nome de host. Por exemplo, se você especificar `MariaDB` como o nome da sua instância, o nome do sistema gerenciado será `MariaDB:hostname:MJ`.

Importante: Se você especificar um nome de instância longo, o nome do sistema gerenciado será truncado e o código do agente não será exibido.

Configurando o agente nos sistemas Windows

É possível configurar o agente em sistemas operacionais Windows usando a janela IBM Cloud Application Performance Management. Depois de atualizar os valores de configuração, inicie o agente para aplicar os valores atualizados.

Procedimento

Para configurar o agente em sistemas operacionais Windows, conclua as etapas a seguir:

1. Clique em **Iniciar>Todos os Programas>IBM Monitoring Agents>IBM Performance Management**.
2. Na janela **IBM Performance Management**, conclua estas etapas:
   a) Dê um clique duplo no modelo **Monitoring Agent for MariaDB**.
   b) Na janela **Monitoring Agent for MariaDB**, especifique um nome de instância e clique em **OK**.
3. Na janela **Monitoring Agent for MariaDB**, conclua estas etapas:
   a) No campo **Endereço IP**, insira o endereço IP do servidor MariaDB que você deseja monitorar remotamente. Se o agente estiver instalado em um servidor a ser monitorado, retenha o valor padrão.
   b) No campo **Nome do usuário JDBC**, insira o nome de um usuário do servidor MariaDB. O valor padrão é raiz.
   c) No campo **Senha de JDBC**, digite a senha de um usuário JDBC.
   d) No campo **Confirmar senha de JDBC**, digite a senha novamente.
   e) No campo **Arquivo Jar JDBC**, clique em **Procurar** e localize o diretório que contém o arquivo Java do conector MariaDB e selecione-o.
   f) Clique em **Avançar**.
   g) No campo **Número de porta JDBC**, especifique o número da porta do servidor JDBC.
   O número da porta padrão é 3306.
   h) Na lista **Nível de rastreio Java**, selecione um nível de rastreio para Java.
   O valor padrão é `Error`.
   i) Clique em **OK**.
   A instância é exibida na janela **IBM Performance Management**.
4. Clique com o botão direito na instância **Monitoring Agent for MariaDB** e clique em **Iniciar**.

   Lembre-se: Para configurar o agente novamente, conclua estas etapas na janela **IBM Performance Management**:

   a. Pare a instância do agente que você deseja configurar.
   b. Clique com o botão direito na instância **Monitoring Agent for MariaDB** e clique em **Reconfigurar**.
   c. Repita as etapas 3 e 4.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações adicionais sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o agente nos sistemas Linux

É possível executar o script de configuração e responder aos prompts para configurar o agente em sistemas operacionais Linux.

Procedimento

Para configurar o agente em sistemas operacionais Linux, conclua as etapas a seguir:

1. Na linha de comandos, execute o comando a seguir:

   ```
   install_dir/bin/mariadb-agent.sh config instance_name
   ```

   Em que *instance_name* é o nome a ser fornecido para a instância e *install_dir* é o diretório de instalação do MariaDB agent.
2. Quando for solicitado a inserir um valor para os parâmetros a seguir, pressione **Enter** para aceitar o valor padrão ou especifique um valor diferente e pressione **Enter**.
   - Endereço IP
   - Nome de usuário JDBC
   - senha JDBC
   - Redigitar senha JDBC
   - arquivo JAR JDBC
   - Número da porta JDBC (O número da porta padrão é 3306.)
   - Nível de rastreio Java (O valor padrão é `Error`.)

   Para obter informações adicionais sobre os parâmetros de configuração, consulte "Configurando o agente usando o arquivo de resposta silencioso" na página 578.
3. Execute o comando a seguir para iniciar o agente:

   ```
   install_dir/bin/mariadb-agent.sh start instance_name
   ```

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações adicionais sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o agente usando o arquivo de resposta silencioso

O arquivo de resposta silencioso contém os parâmetros de configuração do agente. É possível editar o arquivo de resposta silencioso para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

É possível usar o arquivo de resposta silencioso para configurar o MariaDB agent nos sistemas Linux e Windows. Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

Para configurar o agente usando o arquivo de resposta silencioso, conclua as etapas a seguir:

Lembre-se: Este procedimento considera o seguinte caminho padrão onde o agente está instalado:
Windows `C:\IBM\APM`
Linux `opt/ibm/apm/agent`
Se o agente estiver instalado em um caminho diferente, substitua o caminho nas instruções. Além disso, edite o parâmetro **AGENT_HOME** no arquivo de resposta silencioso para especificar o caminho no qual o agente está instalado.

1. Em um editor de texto, abra o arquivo de resposta que está disponível no caminho a seguir:

   Linux *install_dir*`/samples/mariadb_silent_config.txt`

Windows *install_dir*\samples\mariadb_silent_config.txt

Em que *install_dir* é o diretório de instalação do MariaDB agent

2. No arquivo de resposta, especifique um valor para os parâmetros a seguir:
   - Para o parâmetro **Server Name**, especifique o endereço IP de um servidor MariaDB que você deseja monitorar remotamente. Caso contrário, retenha o valor padrão como `localhost`.
   - Para o parâmetro **JDBC user name**, retenha o valor de username padrão de `root` ou especifique o nome de um usuário com privilégios para visualizar as tabelas INFORMATION_SCHEMA.
   - Para o parâmetro **JDBC password**, insira a senha de usuário JDBC.
   - Para o parâmetro **JDBC Jar File**, mantenha o caminho padrão se esse caminho para o conector do MariaDB para o arquivo jar Java estiver correto. Caso contrário, insira o caminho correto. O conector está disponível no caminho padrão a seguir:

     Linux `/usr/share/java/mariadb-connector-java.jar`

     Windows `C:\Program Files (x86)\MariaDB\mariadb-connector-java.jar`
   - Para o parâmetro **JDBC port number**, mantenha o número da porta padrão de 3306 ou especifique um número de porta diferente.
   - Para o parâmetro **Java trace level**, mantenha o valor padrão de `Error` ou especifique um nível diferente de acordo com as instruções de suporte IBM.
3. Salve e feche o arquivo de resposta e execute o seguinte comando para atualizar definições de configuração do agente:

   Linux *install_dir*/bin/mariadb-agent.sh config *instance_name install_dir*/samples/mariadb_silent_config.txt

   Windows *install_dir*\BIN\mariadb-agent.bat config *instance_name install_dir* \samples\mariadb_silent_config.txt

   Em que *instance_name* é o nome a ser fornecido para a instância e *install_dir* é o diretório de instalação do MariaDB agent.

   Importante: Certifique-se de incluir o caminho absoluto para o arquivo de resposta silencioso. Caso contrário, os paineis não exibirão dados do agente.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações adicionais sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o monitoramento do Microsoft Active Directory

O Monitoring Agent for Microsoft Active Directory é configurado e iniciado automaticamente após a instalação.

Antes de Iniciar

Revise os pré-requisitos de hardware e de software, consulte Agente do Software Product Compatibility Reports for Microsoft Active Directory

Para visualizar dados para todos os atributos no painel, conclua as tarefas a seguir:

- "Executando o Microsoft Active Directory agent como um usuário administrador" na página 487
- "Configurando as variáveis de ambiente local" na página 487

Sobre Esta Tarefa

As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte “Histórico de Mudanças” na página 50.

Executando o Microsoft Active Directory agent como um usuário administrador

Deve-se ter direitos administrativos para executar o Microsoft Active Directory agent.

Sobre Esta Tarefa

Todos os conjuntos de dados estão disponíveis para os usuários que são membros do Grupo de administradores. Nesta tarefa, você cria um usuário, designa direitos de administrador ao usuário e altera a conta do usuário para o agente para esse usuário.

Procedimento

1. Clique em **Iniciar** > **Todos os programas** > **Ferramentas administrativas** > **Usuários e computadores do Active Directory**.
2. Para expandir o domínio em que você deseja criar o usuário, clique no sinal de mais (+) ao lado do nome de um domínio.
3. Clique com o botão direito em **Usuários** e, em seguida, clique em **Novo** > **Usuário**.
4. Para criar um novo usuário, abra o assistente de **Novo objeto - usuário**.

   Por padrão, um novo usuário é um membro do grupo Usuários do domínio.
5. Clique com o botão direito no novo usuário que é criado no grupo Usuários do domínio e clique em **Propriedades**. A janela **Propriedades do nome de usuário** é exibida. O nome de usuário é o nome do novo usuário.
6. Na janela **Propriedades de nome de usuário**, conclua as etapas a seguir:
   a) Clique na guia **Membro de**. Na área **Membro de**, inclua o Grupo de administradores.
   b) Clique em **Aplicar** e, em seguida, clique em **OK**.
7. Clique em **Iniciar** > **Executar** e, em seguida, digite `services.msc`.
8. Na janela **Serviços**, conclua as etapas a seguir:
   a) Clique com o botão direito em **Serviço Agente de Monitoramento para o Active Directory**, e clique em **Propriedades**.
   b) Na janela **Propriedades do Agente de Monitoramento para o Active Directory** , na guia **Logon**, clique em **Esta conta**. Insira as credenciais do usuário.
   c) Clique em **Aplicar** e, em seguida, clique em **OK**.
9. Reinicie o serviço do agente.

Configurando as variáveis de ambiente local

Você deve especificar valores para as variáveis de ambiente para visualizar os dados de replicação de Sysvol no painel. Como opção, também é possível atualizar o valor do intervalo de cache para ativar ou desativar o armazenamento em cache.

Procedimento

1. Na janela **IBM Performance Management**, no menu **Ações**, clique em **Avançado** > **Editar arquivo ENV**.
2. No arquivo K3ZENV, altere os valores das variáveis de ambiente a seguir.

   ADO_CACHE_INTERVAL
   Determina se deve iniciar ou parar o armazenamento em cache e é usado para configurar um valor para o intervalo de cache. O intervalo de cache é a duração em segundos entre duas coletas de

dados consecutivas. É possível especificar qualquer valor de número inteiro positivo para o intervalo de cache iniciar o armazenamento em cache. É possível especificar o valor zero para o intervalo de cache parar o armazenamento em cache. Por padrão, o armazenamento em cache é iniciado e o valor do intervalo de cache é configurado como 1200.

ADO_SYSVOL_FORCE_REPLICATION_FLAG
Determina se a replicação de força que é iniciada pelo agente está ativada ou desativada. O valor padrão dessa variável é TRUE. Para desativar replicação forçada, altere o valor desta variável para FALSE.

ADO_SYSVOL_REPLICATION_TEST_INTERVAL
Determina o intervalo de tempo em minutos entre dois testes de replicação do Sysvol. O valor padrão dessa variável é `0` minutos. Para concluir o teste de replicação do Sysvol, certifique-se de que o valor dessa variável seja maior do que zero.

ADO_SYSVOL_REPLICATION_TEST_VERIFICATION_INTERVAL
Determina a quantia de tempo em minutos que o agente espera para verificar os resultados da replicação do Sysvol após ele concluir o teste de replicação do Sysvol.

O valor da variável de intervalo **ADO_SYSVOL_REPLICATION_TEST_INTERVAL** deve ser maior do que o valor da variável **ADO_SYSVOL_REPLICATION_TEST_VERIFICATION_INTERVAL**. É possível usar os valores a seguir para essas variáveis:

ADO_SYSVOL_REPLICATION_TEST_INTERVAL: `1440`
ADO_SYSVOL_REPLICATION_TEST_VERIFICATION_INTERVAL: `30`

Após designar valores válidos para as duas variáveis de ambiente, o agente Active Directory cria um arquivo na pasta compartilhada Sysvol do sistema gerenciado e inicializa replicação de Sysvol forçada. Essa replicação forçada é inicializada a partir do sistema gerenciado para as pastas compartilhadas Sysvol dos parceiros de replicação de Sysvol. Após verificar os resultados do teste de replicação, o agente remove os arquivos que são criados e replicados a partir do sistema gerenciado e de parceiros de replicação de Sysvol.

3. Opcional: No arquivo K3ZENV, inclua a variável ambiental **APM_ATTRIBUTES_ENABLE_COLLECTION** e configure seu valor como `Sim` para visualizar dados para os seguintes conjuntos de dados na guia **Detalhes do atributo**.
   - Serviços
   - Réplica
   - Serviço de Replicação de Arquivo
   - Unidade organizacional movida ou excluída
   - LDAP
   - Security Accounts Manager
   - DFS
   - Catálogo de Endereços
   - Log de Eventos
   - Objetos de Configuração de Senha

   Lembre-se: Se desejar desativar a coleta de dados para esses conjuntos de dados, configure o valor para a variável de ambiente **APM_ATTRIBUTES_ENABLE_COLLECTION** como `Não`.
4. Reinicie o Microsoft Active Directory agent.

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte “Iniciando o Console do Cloud APM” na página 975.

Executando o Microsoft Active Directory agent como um usuário não administrador

É possível executar o Agente Log File como um usuário não administrador.

Sobre Esta Tarefa

É possível executar o agente de monitoramento para o Active Directory como um usuário não administrador; no entanto, atributos Topologia de Confiança e atributos Replicação de Sysvol podem não estar disponíveis. Esses atributos estão disponíveis apenas para usuários do domínio.

Para visualizar os atributos Topologia de Confiança, um usuário não administrador deve ter as seguintes permissões de registro:

- Conceder acesso total ao diretório `HKEY_LOCAL_MACHINE\SOFTWARE\Candle`.
- Conceder acesso de leitura ao diretório `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT \CurrentVersion\Perflib`.

Para visualizar os atributos Replicação de Sysvol, um usuário não administrador deve ter acesso total à pasta `Sysvol` em todos os controladores de domínio em um domínio.

Importante: Quando o Microsoft Active Directory agent está em execução como um usuário não administrador, alguns serviços do grupo de atributos Serviços mostram valores para os atributos Estado Atual e Tipo de Início como Desconhecido na Interface com o Usuário do APM.

A tabela a seguir contém os grupos de atributos para o agente Active Directory que exibem dados para usuários do domínio e usuários de monitoramento de desempenho.

Tabela 171. Grupos de atributos para usuários do domínio e usuários de monitoramento de desempenho

Direito de usuário	**Grupo de atributos**
Usuários de Domínio	• Informações do Conjunto RID • Serviços • Logs de Evento • DNS • Detalhes DNS ADIntegrated • DNS ADIntegrated • DHCP • Trust • Objetos de Política de Grupo • Objetos Perdidos e Achados • Serviço de Diretório de Troca • Objetos de Conflito de Replicação • Atributo LDAP • Servidor de Diretórios Raiz • Contêineres • Parceiro de Replicação • Disponibilidade do Controlador de Domínio • Latência do Parceiro de Replicação • Topologia de Floresta

Tabela 171. Grupos de atributos para usuários do domínio e usuários de monitoramento de desempenho (continuação)	
Direito de usuário	**Grupo de atributos**
Usuários do domínio e usuários de monitoramento de desempenho	Todos os grupos de atributos que são mencionados para os usuários do domínio e os seguintes grupos de atributos extras: • Catálogo de Endereços • Réplica • Serviços de Diretório • Knowledge Consistency Checker • Key Distribution Center do Kerberos • protocolo LDAP • Autoridade de Segurança Local • Name Service Provider • Security Accounts Manager • Serviço de Replicação de Arquivo • Replicação do Sistema de Arquivo Distribuído • Conexões de Replicação de DFS • Pastas Replicadas de DFS • Volume de Serviço de DFS • Desempenho do Controlador de Domínio • Servidor de Acesso Remoto • Servidor de acesso direto • Atributos de Netlogon

Nota: Além disso, os seguintes grupos de atributos exibem dados para usuários que são membros do grupo *Administradores*:

- Informações do Banco de Dados do Active Directory
- Unidade Organizacional Movida ou Excluída
- Objetos de Configuração de Senha

Para obter informações, consulte "Configurando o monitoramento do Microsoft Active Directory" na página 486

Procedimento

1. Clique em **Iniciar>Programas>Ferramentas administrativas>Usuários e computadores do Active Directory**.
2. Expanda o domínio no qual você deseja criar o usuário clicando no sinal de mais (+) próximo do nome de um domínio.
3. Clique com o botão direito em **Usuários** e, em seguida, clique em **Novo>Usuário**.
4. Crie um novo usuário usando o assistente **Novo objeto - Usuário**. Por padrão, um novo usuário é um membro do grupo **Usuários do domínio**.
5. Clique com o botão direito no novo usuário criado no grupo *Usuários do Domínio* e clique em **Propriedades**. A janela **Propriedades do nome do usuário** se abre, em que *nome do usuário* é o nome do novo usuário. Conclua as seguintes etapas na janela **Propriedades do nome do usuário**:
   a) Clique na guia **Membro de**. Na área **Membro de**, inclua o grupo **Usuários do Monitor de Desempenho**.

b) Clique em **Aplicar** e, em seguida, clique em **OK**.

6. Acesse o diretório `Candle_Home`. O caminho padrão é `C:\IBM\APM`.
7. Clique com o botão direito na pasta APM e clique em **Propriedades**. A janela **Propriedades do APM** se abre. Conclua as seguintes etapas na janela **Propriedades do APM**.
   a) Na guia **Segurança**, clique em **Editar**.
   b) Clique em **Incluir** para incluir o novo usuário e conceder acesso total a este usuário.
   c) Clique em **Aplicar** e, em seguida, clique em **OK**.
8. Clique em **Iniciar > Executar** e, em seguida, digite `services.msc`. A janela **Serviços** é aberta. Conclua as seguintes etapas na janela **Serviços**:
   a) Clique com o botão direito no serviço **Agente de Monitoramento** para Active Directory e clique em **Propriedades**.
   b) Na janela **Propriedades do Active Directory**, na guia **Efetuar logon**, clique em **Esta conta**. Insira as credenciais do usuário.
   c) Clique em **Aplicar** e, em seguida, clique em **OK**.
9. Reinicie o serviço do agente.

Configurando serviços de domínio para o grupo de atributos AD_Services_Status

É possível configurar os Serviços de Domínio do MS Active Directory no `Services.properties` para serem usados ou excluídos
ao determinar o `Server Status`. O grupo de atributos `AD_Services_Status` e sua situação são aplicáveis ao
Windows Server 2012 e posterior.

Sobre Esta Tarefa

O arquivo `Services.properties` contém os seguintes Serviços de Domínio do MS Active Directory padrão e sua configuração.
True indica que o serviço será considerado durante a determinação do valor de Status do Servidor.
False indica que o serviço não será considerado durante a determinado do valor de Status do Servidor.

Tabela 172. Serviços de Domínio do MS Active Directory e a definição de configuração.

Serviços de Domínio do MS Active Directory	**Configuração Padrão**
Replicação DFS	verdadeiro
Remote Procedure Call (RPC)	false
Cliente DNS	verdadeiro
Servidor DNS	verdadeiro
Cliente de Política de Grupo	false
Sistema de Mensagens do Intersite	verdadeiro
Key Distribution Center do Kerberos	verdadeiro
NetLogon	verdadeiro
Horário do Windows	verdadeiro
Cliente DHCP	false
Serviços da Web do Active Directory	false
Active Directory Federation Services	false

Nota: A reinicialização do agente é necessária para ativar a coleta de dados para o grupo de atributos `AD_Services_Status` no Windows Server 2012 e posterior.

Procedimento

1. Pare o agente.
2. Localize o arquivo `Services.properties` para modificação, se houver.
   Para agentes de 32 bits, o arquivo `Services.properties` está localizado em *CANDLE_HOME* `\TMAITM6\`.
   Para agentes de 64 bits, o arquivo `Services.properties` está localizado em *CANDLE_HOME* `\TMAITM6_x64\`.
   O *CANDLE_HOME* é o diretório de instalação do agente.
3. Se quiser que os Serviços de Domínio sejam considerados durante a determinação do Status do Servidor, configure seu valor para true.
   Se quiser que os Serviços de Domínio sejam excluídos durante a determinação do Status do Servidor, configure seu valor para false.
   Salve e feche o arquivo.
4. Inicie o agente.

Atualizando o Microsoft Active Directory agent

É possível fazer upgrade do agente MS Active Directory para a versão mais recente.

Antes de Iniciar

Assegure-se de que o arquivo `installAPMAgents.bat` fornecido no instalador da liberação mais recente esteja disponível na máquina na qual o agente está instalado.

Sobre Esta Tarefa

Para fazer upgrade do agente para a versão mais recente, conclua o procedimento a seguir.

Procedimento

1. Efetue logon na máquina na qual o agente está instalado.
2. Ative um prompt de comandos e execute o arquivo `installAPMAgents.bat` originário do instalador da liberação mais recente.
3. Insira o diretório de instalação no qual o agente existente reside e pressione Enter.
4. O prompt de comandos mostra a versão do agente base e a versão do agente de destino a ser atualizada. Pressione Enter para continuar.
5. Quando o upgrade do agente for bem-sucedido, a versão atualizada será mostrada na janela **IBM Performance Management**.
6. Na janela **IBM Performance Management**, clique com o botão direito no agente e selecione **Reconfigurar** no menu suspenso.
7. Para refletir a versão do agente atualizado no **Application Performance Dashboard**, efetue logon no servidor APM e reinicie os componentes do servidor APM usando os comandos a seguir.
   a. **`apm stop_all`**
   b. **`apm start_all`**
8. Na janela **IBM Performance Management**, clique com o botão direito no agente e selecione **Reciclar** no menu suspenso.

Resultados

O agente atualizado é refletido no **Painel de Desempenho do Aplicativo**.

Nota: Ele pode levar 30 minutos ou mais para mostrar o agente atualizado no **Painel de Desempenho do Aplicativo**.

Configurando o monitoramento do Microsoft Cluster Server

Você deve configurar o Monitoring Agent for Microsoft Cluster Server para que o agente possa coletar os dados do servidor de cluster. Use o arquivo de resposta silencioso para configurar o agente.

Antes de Iniciar

Assegure-se de concluir as tarefas a seguir:

- Crie um grupo de recursos vazio para o agente.
- Crie um recurso de cluster de serviços genéricos no grupo de recursos do agente nos sistemas Windows Server 2008, 2012, 2016 e 2019.
- Certifique-se de que o usuário, que se conecta ao ambiente ou aplicativo do Microsoft Cluster Server tenha privilégios de administrador. Use um usuário existente com privilégios de administrador, ou crie um novo usuário. Designe privilégios de administrador ao novo usuário, incluindo o novo usuário no grupo Administradores.

  Lembre-se: Para configurar o Microsoft Cluster Server agent, é possível usar um usuário local ou de domínio, desde que o usuário tenha privilégios de administrador.

Revise os pré-requisitos de hardware e de software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Microsoft Cluster Server agent.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte o “Histórico de Mudanças” na página 50.

Sobre Esta Tarefa

O Microsoft Cluster Server agent é um agente de instância única. Você deve instalar e configurar o agente manualmente da mesma maneira em cada nó no cluster. Para configurar o agente, consulte “Configurando o agente usando o arquivo silencioso de resposta” na página 494.

Criando um recurso de cluster de serviços genéricos nos sistemas Windows Server 2008, 2012, 2016 e 2019

Você deve incluir o serviço do agente do cluster como um recurso para que o agente possa monitorar o servidor de cluster.

Antes de Iniciar

Assegure que o agente seja interrompido em cada nó no cluster.

Procedimento

Para criar um recurso de cluster de serviço genérico, conclua as etapas a seguir:

1. Abra o **Gerenciador de Cluster Failover** em qualquer um dos nós do cluster.
2. Execute uma das seguintes etapas:
   - Para Windows Server 2008:

     Na área de janela de navegação, clique com o botão direito em **Serviços e aplicativos** e, em seguida, clique em **Mais ações** > **Criar serviço ou aplicativo vazio**. O novo serviço é exibido na lista de serviços e aplicativos. Renomeie o serviço recém-criado.
   - Para o Windows Server 2012:

     Na área de janela de navegação, clique com o botão direito em **Funções** e, em seguida, clique em **Mais ações** > **Criar funções**. O novo serviço é exibido na lista de funções.

- Para Windows Server 2016 e 2019:

  Na área de janela de navegação, clique com o botão direito em **Funções** e, em seguida, clique em **Configurar funções**. O novo serviço é exibido.

3. Clique com o botão direito no novo serviço e clique em **Incluir Recursos** > **Serviço Genérico**.
4. Na janela **Assistente de Novo Recurso**, selecione **Monitoring Agent for Microsoft Cluster Server** e clique em **Avançar**.
5. Clique em **Avançar** nas janelas subsequentes até aparecer o botão **Concluir**.
6. Clique em **Concluir**.

   O serviço do agente é incluído como um recurso.
7. Clique com o botão direito no recurso **Monitoring Agent for Microsoft Cluster Server** e clique em **Colocar Recurso em modo Online**.

Resultados
O agente é iniciado no nó preferencial.

Configurando o agente usando o arquivo silencioso de resposta

O arquivo silencioso de resposta contém os parâmetros de configuração do Microsoft Cluster Server agent com valores padrão definidos para alguns parâmetros. É possível editar o arquivo silencioso de resposta para configurar o agente com diferentes valores para os parâmetros de configuração.

Antes de Iniciar

Crie um arquivo de resposta que contenha os parâmetros de configuração que você deseja modificar. Se você deseja modificar os parâmetros de configuração padrão, edite o arquivo de resposta.

Sobre Esta Tarefa
É possível configurar o agente usando o arquivo silencioso de resposta.

Procedimento

1. Abra o arquivo de resposta silencioso que está disponível neste caminho: *install_dir*\samples\microsoft_cluster_server_silent_config.txt
2. Para a variável de ambiente **CTIRA_HOSTNAME**, especifique o nome do cluster como um valor.
3. Em cada nó do cluster, execute o comando a seguir: **install_dir\BIN\microsoft_cluster_server-agent.bat config install_dir\samples\microsoft_cluster_server_silent_config.txt**

O que Fazer Depois
Mude a conta do usuário do usuário local para o usuário do domínio.

Mudando a conta do usuário

Depois de configurar o Microsoft Cluster Server agent, é possível mudar a conta do usuário do usuário local para o usuário do domínio.

Sobre Esta Tarefa
Por padrão, o agente é executado sob a conta de usuário local. O agente deve ser executado no usuário do domínio para que o agente possa monitorar todos os nós no cluster a partir de um único nó.

Procedimento

Para mudar a conta do usuário, conclua as etapas a seguir:

1. Abra a janela **IBM Performance Management** .
2. Clique com o botão direito no agente e clique em **Mudar Inicialização**.

3. Insira as credenciais de login de domínio.
4. Abra o **Gerenciador de Cluster Failover** em um dos nós, e inicie o serviço de cluster.

Resultados
O agente é iniciado no nó.

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como utilizar o console do Performance Management, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o monitoramento do Microsoft Exchange

Configure o Monitoring Agent for Microsoft Exchange Server para monitorar a disponibilidade e o desempenho de Exchange Servers.

Antes de Iniciar
Antes de configurar o agente, execute as seguintes tarefas:

- "Criando usuários" na página 495
- "Designando direitos de administrador para o usuário do Exchange Server" na página 498
- "Tornando o usuário do Exchange Server um administrador local" na página 500
- "Configurando o Exchange Server para alcance" na página 501
- "Configurando o agente para execução no usuário do domínio" na página 502
- Revise os pré-requisitos de hardware e software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Microsoft Exchange Server agent.

Sobre Esta Tarefa

As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte "Histórico de Mudanças" na página 50.

É possível iniciar o Microsoft Exchange Server agent após o agente ser instalado. No entanto, a configuração manual será necessária para visualizar os dados para todos os atributos do agente.

- Para configurar o agente localmente, consulte "Configurando o agente localmente" na página 503.
- Para configurar o agente usando o arquivo de resposta silencioso, consulte "Configurando o agente usando o arquivo de resposta silencioso" na página 507.

Criando usuários

É possível criar um usuário para o agente no Exchange Server manualmente ou executando o utilitário *Novo Usuário*. Crie o usuário em cada Exchange Server que você deseja monitorar.

Antes de Iniciar
Instale o Microsoft Exchange Server agent. Para criar um usuário, você deve ser um administrador de domínio com plenos direitos de administrador no Microsoft Exchange Server.

Sobre Esta Tarefa

Use um dos seguintes procedimentos para criar usuários:

- "Criando usuários no Exchange Server 2007 e 2010" na página 496

- "Criando usuários no Exchange Server 2013" na página 497
- "Criando usuários executando o utilitário Novo Usuário" na página 497

Criando usuários no Exchange Server 2007 e 2010
Você deve criar um usuário para o agente no Exchange Server 2007 e 2010 para que o agente possa se comunicar com o Exchange Server a ser monitorado.

Procedimento

Para criar um usuário, execute as seguintes etapas:

1. Clique em **Iniciar > Programas > Microsoft Exchange Server 2007 > Console de Gerenciamento do Exchange**. A janela **Console de Gerenciamento do Exchange** é aberta.
2. Na árvore Console, clique em **Caixa de Correio na Configuração do Destinatário**.
3. Na área de janela de Ação, clique em **Nova Caixa de Correio**. O assistente Nova Caixa de Correio é aberto.
4. Na página **Introdução**, clique em **Caixa de Correio do Usuário**.
5. Na página **Tipo de Usuário**, clique em **Novo Usuário**.
6. Na página **Informações sobre o Usuário**, especifique as seguintes informações:

   Unidade organizacional
   Por padrão, é exibido o contêiner de usuários no Active Directory. Clique em **Procurar** para alterar a unidade organizacional padrão.

   Nome
   Digite o nome do usuário.

   Iniciais
   Digite as iniciais do usuário.

   Sobrenome
   Digite o sobrenome do usuário.

   Nome
   Por padrão, o nome, as iniciais e o sobrenome do usuário são exibidos neste campo. É possível modificar o nome.

   Nome de logon do usuário (Nome do principal do usuário)
   Digite o nome que o usuário deve usar para efetuar logon na caixa de correio.

   Nome de logon do usuário (pré-Windows 2000 ou anterior)
   Digite o nome de usuário compatível com o Microsoft Windows 2000 Server ou anterior.

   Senha
   Digite a senha que o usuário deve usar para efetuar logon na caixa de correio.

   Confirmar senha
   Digite novamente a senha inserida no campo **Senha**.

   O usuário deve alterar a senha no próximo logon
   Marque essa caixa de seleção se desejar que o usuário reconfigure a senha.
7. Na página **Configurações da Caixa de Correio**, especifique as seguintes informações:

   Alias
   Por padrão, o valor para esse campo é idêntico ao valor especificado no campo **Nome de logon do usuário (Nome do Principal do Usuário)**.

   Banco de dados da caixa de correio
   Clique em **Procurar** para abrir a janela **Selecionar Banco de Dados da Caixa de Correio**. Selecione o banco de dados da caixa de correio a ser utilizado e clique em **OK**.

   Política da caixa de correio da pasta gerenciada
   Marque essa caixa de seleção para especificar uma política de gerenciamento de registros do sistema de mensagens (MRM). Clique em **Procurar** para selecionar a política de caixa de correio de MRM a ser associada a esta caixa de correio.

Política de caixa de correio do Exchange ActiveSync
Marque essa caixa de seleção para especificar uma política de caixa de correio do Exchange ActiveSync. Clique em **Navegar** para selecionar a política de caixa de correio do Exchange ActiveSync a ser associada a esta caixa de correio.

8. Na página **Nova Caixa de Correio**, revise o resumo da configuração. Clique em **Novo** para criar uma caixa de correio. Na página **Conclusão**, a seção Resumo mostra se a caixa de correio foi criada.
9. Clique em **Concluir**.

O que Fazer Depois

Designe direitos de administrador para o usuário do Exchange que foi criado.

Criando usuários no Exchange Server 2013
Você deve criar um usuário para o agente no Exchange Server 2013 para que o agente possa se comunicar e autenticar com o Exchange Server a ser monitorado.

Procedimento

Para criar um usuário no Exchange Server 2013, execute as seguintes etapas:

1. Efetue login no Exchange Admin Center com credenciais de administrador.
2. Na página do **Exchange Admin Center**, clique em **destinatários** e em **caixas de e-mail**.
3. Clique na seta para baixo ao lado do sinal de mais (+) localizado sob a opção **caixas de correio** e, em seguida, clique em **Caixa de correio do usuário**.
4. Na página "Caixa de correio do novo usuário", clique em **Novo usuário** e especifique valores para os outros campos.
5. Clique em **Salvar**.

O que Fazer Depois

Designe direitos de administrador para o usuário do Exchange que foi criado.

Criando usuários executando o utilitário Novo Usuário
É possível executar o utilitário Novo Usuário para criar usuários no Exchange Server 2007 ou posterior. O usuário criado por meio da execução desse utilitário possui todas as permissões necessárias para executar o agente. Esse utilitário é instalado ao instalar o agente.

Antes de Iniciar
Certifique-se de que o agente esteja instalado. Para executar o utilitário Novo Usuário, você deve ser um administrador de domínio com plenos direitos de administrador no Exchange Server.

Sobre Esta Tarefa
Ao executar esse utilitário, o usuário é criado no grupo Usuários do Active Directory e possui as seguintes permissões:

- No Exchange Server 2007:
  - Administrador local
  - Usuários de área de trabalho remota
  - Administrador do destinatário do Exchange
- No Exchange Server 2010 ou posterior:
  - Administrador local
  - Usuários de área de trabalho remota
  - Exchange Servers ou Gerenciamento de pastas públicas.

Procedimento

Para executar o utilitário Novo Usuário, execute as seguintes etapas:

1. Dê um clique duplo no arquivo `kexnewuser.exe`, disponível no seguinte local:
   install_dir\TMAITM6_x64 Em que *install_dir* é o caminho onde o agente está instalado.
2. Na janela **Novo Usuário**, execute as seguintes etapas:
   a) Insira o **nome** e o **sobrenome** do usuário.

      Restrição: O comprimento do nome e do sobrenome não deve exceder 28 caracteres.

   b) No campo **Nome de Logon do Usuário**, insira o nome que o usuário deve digitar sempre que efetuar login.

      Restrição: O comprimento do nome de logon do usuário não deve exceder 256 caracteres.

   c) No campo **Senha**, insira sua senha.

   d) No campo **Confirmar Senha**, insira a senha novamente.

   e) Selecione **O usuário deve alterar a senha no próximo logon** se desejar que a senha especificada seja reconfigurada na próxima vez que o usuário efetuar logon.

   f) Clique em **Avançar**.

   Os valores de configuração especificados são validados e são exibidas mensagens de erro para os valores incorretos.
3. Na lista de bancos de dados da caixa de correio, selecione o banco de dados necessário e clique em **Avançar**.

   É exibido um resumo dos valores de configuração.
4. Clique em **Concluir**.

Resultados

As configurações são salvas e o usuário é criado.

Designando direitos de administrador para o usuário do Exchange Server

O usuário criado para o Microsoft Exchange Server agent deve ser um administrador de domínio com direitos de administrador totais no Microsoft Exchange Server. Os direitos de administrador são necessários para acessar os componentes do Microsoft Exchange Server agent.

Antes de Iniciar

Crie um usuário do Exchange Server cuja caixa de correio esteja no Exchange Server que está sendo monitorado.

Sobre Esta Tarefa

Use um dos procedimentos a seguir para designar direitos de administrador para o usuário:

- "Designando direitos de administrador no Exchange Server 2007" na página 498
- "Designando direitos de administrador no Exchange Server 2010" na página 499
- "Designando direitos de administrador no Exchange Server 2013" na página 499
- "Designando direitos de administrador no Exchange Server 2016" na página 499

Designando direitos de administrador no Exchange Server 2007

É necessário designar direitos de Administrador de Destinatários do Exchange ao usuário no Exchange Server 2007.

Procedimento

1. Clique em **Iniciar > Programas > Microsoft Exchange Server 2007 > Console de Gerenciamento do Exchange**. A janela **Console de Gerenciamento do Exchange** é aberta.
2. Na árvore Console, clique em **Configuração de Organização**.

3. Na área de janela Ação, clique em **Incluir Administrador do Exchange**.
4. Na página **Incluir Administrador do Exchange**, clique em **Procurar**. Selecione o novo usuário criado e, em seguida, selecione a função **Administrador de Destinatários do Exchange**.
5. Clique em **Incluir**.
6. Na página **Conclusão**, clique em **Concluir**.

Designando direitos de administrador no Exchange Server 2010
Deve-se designar direitos de Servidores Exchange ou de Gerenciamento de Pasta Pública ao usuário no Exchange Server 2010.

Procedure

1. Efetue logon no servidor Exchange com privilégios de administrador.
2. Clique em **Iniciar > Ferramentas Administrativas > Server Manager.**
3. Expanda **Ferramentas**.
4. Clique em **Usuários e computadores do Active Directory**.
5. Expanda o **Domínio**, clique em **Grupos de segurança do Microsoft Exchange**.
6. Clique com o botão direito do mouse em **Exchange Servers ou Gerenciamento de Pasta Pública** e clique em **Propriedades**.
7. Na janela **Propriedades dos servidores Exchange ou Propriedades do gerenciamento de pasta pública**, acesse **Membros** e clique em **Incluir**.
8. Na lista de usuários, selecione o usuário a ser incluído no grupo e clique em **OK**.
9. Clique em **OK**.

Designando direitos de administrador no Exchange Server 2013
É necessário designar direitos do Exchange Servers ou Public Folder Management ao usuário no Exchange Server 2013.

Procedure

1. Efetue logon no servidor Exchange com privilégios de administrador.
2. Clique em **Iniciar > Ferramentas Administrativas > Server Manager.**
3. Expanda **Ferramentas**.
4. Clique em **Usuários e computadores do Active Directory**.
5. Expanda o **Domínio**, clique em **Grupos de segurança do Microsoft Exchange**.
6. Clique com o botão direito do mouse em **Exchange Servers ou Gerenciamento de Pasta Pública** e clique em **Propriedades**.
7. Na janela **Propriedades dos servidores Exchange ou Propriedades do gerenciamento de pasta pública**, acesse **Membros** e clique em **Incluir**.
8. Na lista de usuários, selecione o usuário a ser incluído no grupo e clique em **OK**.
9. Clique em **OK**.

Designando direitos de administrador no Exchange Server 2016
É necessário designar direitos do Exchange Servers ou Public Folder Management ao usuário no Exchange Server 2016.

Procedure

1. Efetue logon no servidor Exchange com privilégios de administrador.
2. Clique em **Iniciar > Ferramentas Administrativas > Server Manager.**
3. Expanda **Ferramentas**.
4. Clique em **Usuários e computadores do Active Directory**.
5. Expanda o **Domínio**, clique em **Grupos de segurança do Microsoft Exchange**.

6. Clique com o botão direito do mouse em **Exchange Servers ou Gerenciamento de Pasta Pública** e clique em **Propriedades**.
7. Na janela **Propriedades dos servidores Exchange ou Propriedades do gerenciamento de pasta pública**, acesse **Membros** e clique em **Incluir**.
8. Na lista de usuários, selecione o usuário a ser incluído no grupo e clique em **OK**.
9. Clique em **OK**.

What to do next
Torne o usuário um administrador local do computador no qual o Exchange Server está instalado.

Tornando o usuário do Exchange Server um administrador local

Para acessar os dados do Exchange Server, o usuário criado para o Microsoft Exchange Server agent deve ser um administrador local do computador no qual o Exchange Server está instalado.

Antes de Iniciar
Crie um usuário do Exchange Server.

Sobre Esta Tarefa
Use um dos seguintes procedimentos para tornar o usuário um administrador local:

- "Tornando o usuário um administrador local no computador Windows 2003" na página 500
- "Tornando o usuário um administrador local no computador Windows 2008" na página 500
- "Tornando o usuário um administrador local no computador Windows 2012" na página 501
- "Tornando o usuário um administrador local no computador Windows 2016" na página 501

Tornando o usuário um administrador local no computador Windows 2003
É necessário tornar o usuário que foi criado para o Exchange Server um administrador local do computador que é executado no sistema operacional Windows 2003 e no qual o Exchange Server está instalado.

Procedimento

1. Clique com o botão direito em **Meu Computador** na área de trabalho do computador e clique em **Gerenciar**.
2. Expanda **Usuários e Grupos Locais**.
3. Clique em **Grupos**.
4. Dê um clique duplo em **Administradores** para exibir a janela **Propriedades de Administradores**.
5. Clique em **Incluir**.
6. Selecione **Diretório Completo** na lista **Procurar**.
7. Selecione o nome do usuário criado e clique em **Incluir**.
8. Clique em **OK**.
9. Clique em **OK**.

Tornando o usuário um administrador local no computador Windows 2008
É necessário tornar o usuário que foi criado para o Exchange Server um administrador local do computador que é executado no sistema operacional Windows Server 2008 e no qual o Exchange Server está instalado.

Procedimento

1. Clique em **Iniciar > Ferramentas Administrativas > Gerenciador do Servidor**.
2. Na área de janela de navegação, expanda **Configuração**.
3. Dê um clique duplo em **Usuários e Grupos Locais**.

4. Clique em **Grupos**.
5. Clique com o botão direito no grupo a ser incluído na conta do usuário e, em seguida, clique em **Incluir no Grupo**.
6. Clique em **Incluir** e digite o nome da conta do usuário.
7. Clique em **Verificar Nomes** e clique em **OK**.

Tornando o usuário um administrador local no computador Windows 2012
É necessário tornar o usuário que foi criado para o Exchange Server um administrador local do computador que é executado no sistema operacional Windows Server 2012 e no qual o Exchange Server está instalado.

Procedimento

1. Clique em **Iniciar> Server Manager**.
2. Na página **Painel do Server Manager**, clique em **Ferramentas > Gerenciamento de computadores**.
3. Na área de janela de navegação da página **Gerenciamento de computadores**, expanda **Usuários e grupos locais** e, e seguida, clique em **Usuários**.
4. Na lista de usuários, clique com o botão direito no usuário ao qual deseja designar direitos de administrador e clique em **Propriedades**.
5. Clique na guia **Membro de** e clique em **Incluir**.
6. Na página **Selecionar Grupo**, digite `Administradores` e, em seguida, clique em **OK**.
7. Clique em **Aplicar** e em **OK**.

Tornando o usuário um administrador local no computador Windows 2016
Você deve tornar o usuário criado para o Exchange Server um administrador local do computador executado no sistema operacional Windows Server 2016 e onde o Exchange Server está instalado.

Procedimento

1. Clique em **Iniciar> Server Manager**.
2. Na página **Painel do Server Manager**, clique em **Ferramentas > Gerenciamento de computadores**.
3. Na área de janela de navegação da página **Gerenciamento de computadores**, expanda **Usuários e grupos locais** e, e seguida, clique em **Usuários**.
4. Na lista de usuários, clique com o botão direito no usuário ao qual deseja designar direitos de administrador e clique em **Propriedades**.
5. Clique na guia **Membro de** e clique em **Incluir**.
6. Na página **Selecionar Grupo**, digite `Administradores` e, em seguida, clique em **OK**.
7. Clique em **Aplicar** e em **OK**.

Configurando o Exchange Server para alcance

Para verificar o alcance, o Microsoft Exchange Server agent envia uma mensagem de email para o servidor e mede a quantidade de tempo necessária para receber uma mensagem automatizada. Antes de iniciar o agente, é necessário configurar o Exchange Server para responder mensagens de email automaticamente.

Antes de Iniciar
Antes de configurar o Exchange Server, certifique-se de que as seguintes tarefas estejam concluídas:

- Seja criada uma caixa de correio para o usuário no Exchange Server a ser monitorado.
- O usuário criado para o agente seja um usuário do domínio.
- Os servidores na organização do Microsoft Exchange sejam configurados para fluxo de correio entre os servidores.

Procedimento

Execute as etapas a seguir para cada Exchange Server cujo alcance você deseja verificar:

1. Efetue login no Microsoft Outlook, especificando as credenciais do usuário criado.
2. Clique em **Avançar** na janela **Inicialização**.
3. Selecione **Sim** e clique em **Avançar**.
4. No campo **Microsoft Exchange Server**, digite o nome do Exchange Server.
5. No campo **Caixa de Correio**, digite o nome do usuário criado.
6. Clique em **Concluir**.
7. Clique em **OK**.
8. Clique em **Ferramentas > Regras e Alertas > Nova Regra**.
9. Selecione **Iniciar a partir de uma regra em branco**.
10. Selecione **Verificar mensagens assim que chegarem** e clique em **Avançar**.
11. Selecione as seguintes opções:
    - **Onde está meu nome na caixa Para:**
    - **Com palavras específicas no assunto ou corpo**
12. Na **Etapa 2** na janela, clique em **Palavras específicas**.
13. No campo **Especificar palavras ou frases para procurar no assunto ou corpo**, digite `VERIFICAÇÃO DE DISPONIBILIDADE`.
14. Clique em **Incluir**.
15. Clique em **OK** e, em seguida, clique em **Avançar**.
16. Selecione **Fazer com que o servidor responda usando uma mensagem específica** e clique em **uma mensagem específica**.
17. No editor de mensagens de email, digite o seguinte texto no campo de assunto da mensagem:
    `CHECK RECEIVED: MAILBOX AVAILABLE.`
18. Feche o editor de mensagem de email e clique em **Sim** para salvar essas mudanças.
19. Clique em **Avançar**.
20. Quando for questionado sobre exceções, não especifique nenhuma restrição.
21. Clique em **Avançar**.
22. Clique em **Concluir** e, em seguida, clique em **OK**.

O que Fazer Depois

Configure o Microsoft Exchange Server agent.

Configurando o agente para execução no usuário do domínio

Por padrão, o Microsoft Exchange Server agent é configurado para ser executado no usuário local. O agente deve ser executado no usuário do domínio criado.

Antes de Iniciar

Certifique-se de que:

- O usuário criado seja um usuário do domínio com direitos de administrador local.
- O usuário tenha direitos de administrador no servidor em que o agente está instalado.

Sobre Esta Tarefa

Ao ser executado no usuário de domínio, o agente pode monitorar todos os componentes do Exchange Server.

Procedimento

Para alterar o usuário no qual o agente é executado, conclua as seguintes etapas:

1. Execute o seguinte comando para verificar qual ID do usuário está sendo usado para iniciar o agente.
   `install_dir\InstallITM\KinCinfo.exe -r`
2. Se o agente de monitoramento foi iniciado com um ID do usuário que não pertence ao grupo Administradores, pare o agente.
3. Abra a janela **Gerenciar Serviços de Monitoramento**.
4. Clique com o botão direito na instância de agente e clique em **Alterar Inicialização**.
5. Especifique o ID do usuário completo como `<Domain\Userid>` e, em seguida, especifique a senha.
6. Inicie o agente de monitoramento.

Configurando o agente localmente

É possível configurar o agente localmente usando a janela IBM Cloud Application Performance Management.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito em **Monitoring Agent for Microsoft Exchange Server** e clique em **Configurar Agente**.

   Atenção: Clique em **Reconfigurar** se **Configurar Agente** estiver desativado.
3. Na janela **Monitoring Agent for Microsoft Exchange Server: Configuração Avançada do Agente**, clique em **OK**.
4. Na janela **Configuração do Agente**, execute as seguintes etapas:
   a) Clique na guia **Propriedades do Exchange Server** e especifique valores para os parâmetros de configuração. Ao clicar em **OK**, os valores especificados são validados.
   b) Clique na guia **Monitoramento de Serviços do Exchange** e especifique valores para os parâmetros de configuração. Ao clicar em **OK**, os valores especificados são validados.
   c) Clique na guia **Propriedades de Configuração Avançadas** e especifique valores para os parâmetros de configuração. Ao clicar em **OK**, os valores especificados são validados.

   Para obter informações sobre os parâmetros de configuração em cada guia da **Configuração do Agente**, consulte os seguintes tópicos:

   - “Parâmetros de configuração para as propriedades do Exchange Server” na página 503
   - “Parâmetros de configuração para serviços do Exchange” na página 505
   - “Parâmetros de configuração para alcance” na página 505

   Para obter informações sobre a validação dos valores de configuração, consulte “Validação de valores de configuração” na página 507.
5. Recicle o agente

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte “Iniciando o Console do Cloud APM” na página 975.

Restrição: No painel do Cloud APM, somente as instâncias de um dos tipos de componente do Exchange (Microsoft Exchange Server ou Microsoft Exchange Server 2013) são exibidas em Meus componentes.

Parâmetros de configuração para as propriedades do Exchange Server

Na guia **Propriedades do Exchange Server** da janela **Configuração do Agente**, é possível configurar as propriedades do Exchange Server, como nome do servidor, nome de domínio e nome do usuário.

A tabela a seguir contém descrições detalhadas das definições de configuração na guia **Propriedades do Servidor Exchange** tab.

Tabela 173. Nomes e descrições das definições de configuração na guia Propriedades do Exchange Server

Nome do parâmetro	Descrição	Campo obrigatório	Exemplos
Nome do Exchange Server	O nome do Exchange Server. Durante a instalação do Exchange Server, o nome padrão do Exchange Server é o nome do host do Servidor do Windows. Se você alterar o nome padrão do Exchange Server, será necessário usar o nome alterado ao configurar o agente do Exchange Server. **Lembre-se:** Em ambientes em cluster e distribuídos, especifique o nome do Servidor da Caixa de Correio para o Exchange Server 2007.	Sim **Importante:** Não especifique valores se o agente estiver instalado em um servidor que possui um cluster de cópia único com mais de dois nós.	Se o nome do Exchange Server for `popcorn`, insira `popcorn` no campo **Nome do Exchange Server**.
Nome do Domínio do Exchange	O nome do domínio no qual o Exchange Server está instalado.	Sim	Se o Exchange Server estiver no domínio `LAB.XYZ.com`, insira o nome que precede o primeiro ponto, por exemplo, `LAB`.
Nome do Usuário do Exchange	O nome do usuário que está configurado para acessar o Exchange Server. **Lembre-se:** O usuário deve possuir uma caixa de correio no mesmo Exchange Server.	Sim	
Senha do Usuário do Exchange	A senha do usuário que está configurado para acessar o Exchange Server.	Sim	
Confirmar Senha	A mesma senha especificada para o usuário do Exchange Server.	Sim	
Nome do Perfil MAPI do Exchange	Os perfis MAPI são as definições de configuração primárias necessárias para acessar o Exchange Server. Esse campo é desativado se você estiver usando um Microsoft Exchange Server agent de 64 bits para monitorar o Exchange Server 2007 ou posterior.	Não	
Configuração em cluster	Marque essa caixa de seleção se desejar configurar o Microsoft Exchange Server agent em um ambiente em cluster.	Não aplicável	
Nome do Servidor de Cluster	O nome do Servidor de Cluster. Esse campo é ativado ao marcar a caixa de seleção **Configuração em cluster**.	Sim, se o campo estiver ativado.	`SCCCluster`

Tabela 173. Nomes e descrições das definições de configuração na guia Propriedades do Exchange Server (continuação)

Nome do parâmetro	Descrição	Campo obrigatório	Exemplos
ID do Subsistema do Exchange	O nome do nó do Servidor de Cluster. Esse campo é ativado ao marcar a caixa de seleção **Configuração em cluster**.	Sim, se o campo estiver ativado.	`node1`
Diretório de Dados Históricos do Agente Exchange	O local no disco no qual os dados históricos são armazenados. Esse campo é ativado ao marcar a caixa de seleção **Configuração em cluster**.	Sim, se o campo estiver ativado.	`c:\history`

Parâmetros de configuração para serviços do Exchange
Na guia **Monitoramento de Serviços do Exchange** da janela **Configuração do Agente**, é possível selecionar os serviços do Exchange para saber o status do Exchange Server.

A tabela a seguir contém descrições detalhadas das definições de configuração na guia **Monitoramento de Serviços do Exchange**.

Tabela 174. Nomes e descrições das definições de configuração na guia Monitoramento de Serviços do Exchange

Nome de parâmetro	Descrição	Campo obrigatório
Serviços do Exchange	Selecione os serviços do Exchange da lista disponível de serviços e clique na seta para mover os serviços selecionados para a lista **Serviços Configurados para o Status do Servidor** para que o Microsoft Exchange Server agent possa monitorá-los. **Lembre-se:** A lista de serviços disponíveis muda de acordo com a versão do Exchange Server e com as funções que estão instaladas.	Não aplicável
Serviços Configurados para o Status de Servidor	Os serviços que já estão disponíveis nessa lista determinam o status do Exchange Server. Esses serviços são obrigatórios e não podem ser movidos da lista **Serviços Configurados para o Status do Servidor** para a lista **Serviços do Exchange**. É possível incluir mais serviços na lista **Serviços Configurados para o Status do Servidor** movendo os serviços da lista **Serviços do Exchange**. É possível mover esses serviços adicionais de volta para a lista **Serviços do Exchange**.	Não aplicável

Parâmetros de configuração para alcance
Na guia **Propriedades de Configuração Avançadas** da janela **Configuração do Agente**, é possível configurar os parâmetros que estão relacionados ao alcance, como endereço de email de destino e intervalo de alcance.

A tabela a seguir contém descrições detalhadas das definições de configuração na guia **Propriedades de Configuração Avançadas**.

Tabela 175. Nomes e descrições das definições de configuração na guia Propriedades de Configuração Avançadas

Nome de parâmetro	Descrição	Campo obrigatório
Ativar Monitoramento de Alcance da Caixa de Correio	Marque essa caixa de seleção se desejar que o agente capture os dados das métricas de alcance.	Não aplicável
Endereço de Email de Destino	Um endereço de email para verificar o alcance. Quando houver vários endereços de email, separe-os com ponto e vírgula (;). **Restrição:** O número total de caracteres nesse campo não deve exceder 1023.	Sim, se o campo estiver ativado.
Intervalo de Transmissão de Email (segundos)	O tempo de espera (em segundos) do agente do Exchange Server entre o envio de emails.	Sim, se o campo estiver ativado.
Tempo Limite de Transmissão de Emails (segundos)	O intervalo (em segundos) durante o qual o agente aguarda uma resposta para o email que foi enviado para testar se o Servidor de Caixa de Correio está acessível.	Não
Ativar Monitoramento de Detalhes da Caixa de Correio	Marque essa caixa de seleção para coletar dados para as métricas de detalhes da caixa de correio.	Não aplicável
Horário de Início da Coleta de Detalhes da Caixa de Correio	O horário (no formato hh:mm:ss) em que as métricas dos detalhes da caixa de correio são coletadas.	Não
Intervalo de Coleta dos Detalhes da Caixa de Correio (segundos)	O intervalo (em segundos) entre as coleções de métricas de detalhes da caixa de correio.	Não
Horário da Coleta de Logs de Eventos (minutos)	O período (em minutos) em que o agente coleta registros de eventos.	Não
Número Máximo de Eventos	A contagem máxima para a coleta de registros de eventos. A coleta de registros de eventos é interrompida quando o número de registros de eventos coletados excede a contagem máxima.	Não
Intervalo de Coleta (segundos)	O intervalo (em segundos) entre os ciclos do agente.	Não
Intervalo de Topologia do Exchange (segundos)	O intervalo (em segundos) entre as coletas de informações detalhadas sobre a topologia.	Não

Tabela 175. Nomes e descrições das definições de configuração na guia Propriedades de Configuração Avançadas (continuação)		
Nome de parâmetro	**Descrição**	**Campo obrigatório**
Intervalo de Coleta de Rastreamento de Mensagens (horas)	O intervalo (em horas) durante o qual os logs de rastreamento de mensagens são coletados. **Restrição:** O valor do intervalo deve estar na faixa de 1 a 12. Caso seja especificado um valor de intervalo superior a 12, o valor será salvo como 12. Se você inserir um valor inválido que contenha letras ou caracteres especiais, o valor será salvo como 0, o que indica que a coleta de rastreamento de mensagens está desativada. Esse campo será desativado se alguma das seguintes condições for verdadeira: • A função Servidor de Caixa de Correio ou a função Transporte de Hub não estiver instalada no Exchange Server. • O recurso de rastreamento de mensagens estiver desativado no Exchange Server.	Não

Validação de valores de configuração
Os valores que você especifica enquanto configura o agente são validados. A validação garante a especificação de valores para todos os parâmetros obrigatórios e garante que certas condições sejam atendidas, como direitos de administrador local para o usuário.

A tabela a seguir mostra os testes de validação que são executados nos valores de configuração especificados.

Tabela 176. Testes de validação	
Teste de validação	**Verifica se**
Nome do Exchange Server	O nome do Servidor de Caixa de Correio do usuário corresponde ao nome do Exchange Server especificado.
Direitos do Exchange Server	O usuário possui os direitos necessários do Exchange Server. No Exchange Server 2007, o usuário deve ter direitos de administrador do destinatário e no Exchange Server 2010 ou posterior, o usuário deve ter direitos de gerenciamento de destinatário.
Administrador Local	O usuário possui direitos de administrador local.
Logon do Serviço do Agente	O serviço do agente está configurado para ser executado com a conta de usuário especificada.

Se um ou mais testes de validação falharem, será gerada uma mensagem de erro. É necessário especificar valores para todos os parâmetros obrigatórios. Caso contrário, não é possível salvar os valores configurados.

Configurando o agente usando o arquivo de resposta silencioso

O arquivo de resposta silencioso contém parâmetros de configuração do agente com valores padrão definidos para alguns parâmetros. É possível editar o arquivo de resposta silencioso para configurar o agente com diferentes valores para os parâmetros de configuração.

Sobre Esta Tarefa
Após você atualizar os valores de configuração no arquivo de resposta silencioso, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

1. Abra o arquivo `msex_silent_config.txt` que está localizado em *`install_dir`*`\samples` e especifique os valores para todos os parâmetros obrigatórios.
   Também é possível modificar os valores padrão de outros parâmetros.
2. Execute o seguinte comando:
   `install_dir\BIN\msexch-agent.bat config install_dir\samples \msex_silent_config.txt`

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Restrição: No painel do Cloud APM, somente as instâncias de um dos tipos de componente do Exchange (Microsoft Exchange Server ou Microsoft Exchange Server 2013) são exibidas em Meus componentes.

Configurando variáveis de ambiente locais para o agente

Você pode configurar as variáveis de ambiente local para o Microsoft Exchange Server agent para ativar ou desativar o evento de regulagem de eventos duplicados.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **Agentes de Monitoramento IBM** > **IBM Cloud Application Performance Management**.
2. Na janela **IBM Performance Management**, no menu **Ações**, clique em **Avançado** > **Editar arquivo ENV**.
3. No arquivo KEXENV, mude os valores das seguintes variáveis de ambiente:

   `EX_EVENT_THROTTLE_ENABLE`
   Essa variável permite regular eventos duplicados. O valor padrão é `False`. Para ativar a regulagem de eventos para evitar o acionamento de situações para eventos duplicados, configure o valor dessa variável como True.

   `EX_EVENT_THROTTLE_DURATION`
   Essa variável fornece a duração (em minutos) para a regulagem de eventos. O valor padrão é `0` minutos.

Configurando o monitoramento do Microsoft Hyper-V

Ao instalar o Monitoring Agent for Microsoft Hyper-V Server, o agente é configurado automaticamente e iniciado com as definições de configuração padrão. Use o arquivo de resposta silencioso para modificar as definições de configuração padrão.

Antes de Iniciar

- Revise os pré-requisitos de hardware e de software. Para obter informações de requisito do sistema atualizadas, consulte Software Product Compatibility Reports (SPCR) para o Microsoft Hyper-V Server agent.
- Crie um arquivo de resposta que contenha os parâmetros de configuração que você deseja modificar.

- Para visualizar os dados da máquina virtual na página Máquina Virtual, assegure-se de instalar o componente de integração e o agente de S.O. em cada máquina virtual. Para máquinas virtuais executadas no sistema Linux, assegure-se de executar as seguintes tarefas:
  - Faça upgrade do sistema Linux.
  - Instale o pacote `hypervkvpd` ou `hyperv-daemons rpm` atualizado na máquina virtual.

Sobre Esta Tarefa

É possível configurar o agente quando o agente está em execução ou interrompido. O agente permanece no mesmo estado após a configuração. Por exemplo, se o agente está em execução, ele permanece no estado em execução após a configuração.

Importante: Para a liberação 8.1.3 do Performance Management, a janela de configuração do agente é removida, pois não é obrigatória. A janela de configuração do agente está disponível para 8.1.2 ou versões anteriores do Performance Management.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte o “Histórico de Mudanças” na página 50.

Procedimento

Para configurar o agente, execute as seguintes etapas:

1. Abra o arquivo `microsoft_hyper-v_server_silent_config.txt` que está em *`install_dir`*`\samples` e especifique os valores para todos os parâmetros obrigatórios.

   Também é possível modificar os valores padrão de outros parâmetros.
2. Abra o prompt de comandos e insira o seguinte comando:

   `install_dir\BIN\microsoft_hyper-v_server-agent.bat config install_dir \samples\microsoft_hyper-v_server_silent_config.txt`

   O arquivo de resposta contém os seguintes parâmetros:

   - KHV_DIRECTOR_PORT
   - KHV_DIRECTOR_SERVER

   Lembre-se: A configuração do agente é organizada nos seguintes grupos:

   Configuração do IBM Systems Director (IBM_DIRECTOR_CONFIGURATION)
   Os elementos de configuração definidos nesse grupo estão sempre presentes na configuração do agente. Esse grupo define informações que se aplicam a todo o agente.

   Número da Porta do IBM Systems Director Server (KHV_DIRECTOR_PORT)
   O número da porta do IBM Systems Director Server. O valor padrão é none.

   Nome do Host do IBM Systems Director Server (KHV_DIRECTOR_SERVER)
   O nome do host ou endereço IP do IBM Systems Director Server que está gerenciando o ambiente. O valor padrão é none.
3. Inicie o agente se ele estiver no estado pausado.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte “Iniciando o Console do Cloud APM” na página 975.

Fornecendo Política de segurança local para executar o Monitoring Agent for Microsoft Hyper-V Server no Windows por um usuário não administrador

As políticas de segurança local estão disponíveis para executar o Monitoring Agent for Microsoft Hyper-V Server no Windows por um usuário não administrador.

Sobre Esta Tarefa

Uma combinação das duas seguintes políticas de segurança local funciona para executar o Microsoft Hyper-V Server agent no Windows por um usuário não administrador. Para o Microsoft Hyper-V Server agent iniciar ou parar, configurar e verificar dados, use essas duas políticas.

- Depurar programas
- Efetuar logon como um serviço

Além disso, os seguintes grupos de atributos precisam de direitos de administrador para obter dados no portal APM:

- Disponibilidade
- Migração
- Cluster WO Mig VM
- Migração de Armazenamento de VM

Siga o procedimento que é fornecido para avaliar as permissões de Segurança local para um usuário não administrador.

Procedimento

1. Instale o agente Microsoft Hyper-V Server como um administrador local.
2. Inclua o usuário não administrador no diretório `install_dir` e forneça as seguintes permissões para ele:
   a) Forneça acesso total ao registro `HKEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring`.
   b) Forneça acesso de leitura ao usuário não administrador no registro `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`.
   c) Forneça acesso total ao usuário não administrador no diretório `install_dir`.
3. Acesse o menu **Iniciar** e execute o comando **`secpol.msc`** para abrir as Políticas de segurança local.
4. Para incluir um usuário não administrador nas políticas, consulte "Concedendo permissões de Política de Segurança Local" na página 510.
5. Para incluir um usuário não administrador no grupo Usuários administradores do Hyper-V, consulte "Incluindo um usuário não administrador no grupo de usuários administradores do Hyper-V" na página 512.
6. Para incluir um usuário não administrador no grupo Usuários do Monitor de Desempenho, consulte "Incluindo um usuário não administrador no grupo de usuários do Performance Business Monitor" na página 512.
7. Para modificar a permissão de segurança DCOM para um usuário não administrador, consulte "Modificando permissões DCOM" na página 511.
8. Reinicie o Microsoft Hyper-V Server agent e verifique os dados no portal APM.

Concedendo permissões de Política de Segurança Local

Para iniciar, parar, configurar e verificar dados para o Microsoft Hyper-V Server agent, é preciso conceder permissões a essas duas políticas de segurança local: Depurar programas e Efetuar logon como serviço.

Concedendo a permissão Depurar programas

Sobre Esta Tarefa

Para conceder a permissão Depurar Programas, conclua o procedimento a seguir.

Procedimento

1. Clique em **Iniciar > Painel de Controle > Ferramentas Administrativas > Política de Segurança Local**. A janela **Configurações de Segurança Local** é aberta.

2. Expanda **Políticas Locais** e clique em **Designação de Direitos do Usuário**. A lista de aberturas de políticas.
3. Dê um clique duplo na política **Depurar programas**. A janela **Propriedades dos programas de depuração** é aberta.
4. Clique em **Incluir Usuário ou Grupo**. A janela **Selecionar Usuários ou Grupos** é exibida.
5. No campo **Inserir os nomes de objetos a serem selecionados**, insira o nome da conta do usuário a quem você deseja designar permissões e, em seguida, clique em **OK**.
6. Clique em **Aplicar** e, em seguida, clique em **OK**.

Concedendo a permissão Efetuar logon como serviço

Sobre Esta Tarefa

Para conceder a permissão Efetuar Logon como Serviço, conclua o procedimento a seguir.

Procedimento

1. Clique em **Iniciar > Ferramentas Administrativas > Política de Segurança Local**. A janela **Configurações de Segurança Local** é aberta.
2. Expanda **Políticas Locais** e clique em **Designação de Direitos do Usuário**. A lista de aberturas de políticas.
3. Dê um clique duplo na política **Efetuar logon como serviço**. A janela **Efetuar logon como propriedades de serviço** é aberta.
4. Clique em **Incluir Usuário ou Grupo**. A janela **Selecionar Usuários ou Grupos** é exibida.
5. No campo **Inserir os nomes de objetos a serem selecionados**, insira o nome da conta do usuário a quem você deseja designar permissões e, em seguida, clique em **OK**.
6. Clique em **Aplicar** e, em seguida, clique em **OK**.

Modificando permissões DCOM

É preciso modificar permissões DCOM para executar o Microsoft Hyper-V Server agent com o acesso do usuário não administrador.

Sobre Esta Tarefa

Para modificar permissões DCOM, verifique se o usuário tem as permissões apropriadas para iniciar o servidor DCOM. Para modificar permissões, conclua o procedimento a seguir.

Procedimento

1. Usando o comando **Regedit**, acesse o valor de registro `HKCR\Clsid\*clsid value`.

   Nota: Ao configurar o agente com um usuário não administrador, o valor CLSID é exibido no visualizador de eventos com o ID de evento 10016.
2. Na área de janela Editor de Registro, dê um clique duplo em **Padrão**.
3. Na caixa de diálogo **Editar sequência**, copie a sequência de dados de valor.
4. Clique em **Iniciar > Painel de Controle > Ferramentas de Administração > Serviços de Componente**.
5. Na janela **Serviços de Componente**, expanda **Serviços de Componente > Computadores > Meu Computador** e clique duas vezes em **DCOM**.
6. Na área de janela de configuração do DCOM, localize a sequência copiada (nome do programa), clique com o botão direito no nome do programa e clique em **Propriedades**.
7. Na janela **Propriedades**, selecione a guia **Segurança**.
8. Na caixa de grupo **Permissões de lançamento e ativação**, selecione **Customizar** e, em seguida, clique em **Editar**. A janela **Permissões de lançamento e ativação** é aberta.
9. Clique em **Incluir**, insira um usuário não administrador na lista de permissões e clique em **OK**.

10. Selecione a caixa de seleção **Permitir** para Lançamento local e Ativação local e, em seguida, clique em **OK**.

Incluindo um usuário não administrador no grupo de usuários administradores do Hyper-V

É preciso incluir um usuário não administrador no grupo de usuários administradores do Hyper-V para obter dados no portal APM.

Sobre Esta Tarefa

Para incluir um usuário não administrador no grupo de usuários administradores do Hyper-V, conclua o procedimento a seguir.

Procedimento

1. Clique em **Iniciar > Painel de Controle > Ferramentas de Administração > Gerenciamento de Computadores**. A janela **Gerenciamento de Computadores** é aberta.
2. Clique em **Ferramentas do Sistema > Usuários e Grupos Locais > Grupos**. A lista de grupos é aberta.
3. Dê um clique duplo no grupo **Administradores do Hyper-V**. A janela **Propriedades de administradores do Hyper-V** é aberta.
4. Clique em **Incluir**. A janela **Selecionar Usuários ou Grupos** é exibida.
5. No campo **Inserir os nomes de objetos a serem selecionados**, insira o nome da conta do usuário a quem você deseja designar permissões e, em seguida, clique em **OK**.
6. Clique em **Aplicar** e, em seguida, clique em **OK**.

Incluindo um usuário não administrador no grupo de usuários do Performance Business Monitor

É preciso incluir um usuário não administrador no grupo de usuários do Performance Monitor para obter dados no portal APM.

Sobre Esta Tarefa

Para incluir um usuário não administrador no grupo de usuários do Performance Business Monitor, conclua o procedimento a seguir.

Procedimento

1. Clique em **Iniciar > Painel de Controle > Ferramentas de Administração > Gerenciamento de Computadores**. A janela **Gerenciamento de Computadores** é aberta.
2. Clique em **Ferramentas do Sistema > Usuários e Grupos Locais > Grupos**. A lista de grupos é aberta.
3. Dê um clique duplo no grupo **Usuários do Performance Monitor**. A janela **Propriedades dos Usuários do Performance Business Monitor** é aberta.
4. Clique em **Incluir**. A janela **Selecionar Usuários ou Grupos** é exibida.
5. No campo **Inserir os nomes de objetos a serem selecionados**, insira o nome da conta do usuário a quem você deseja designar permissões e, em seguida, clique em **OK**.
6. Clique em **Aplicar** e, em seguida, clique em **OK**.

Configurando o monitoramento do Microsoft IIS

Quando você instala o Monitoring Agent for Microsoft Internet Information Services, o agente é configurado automaticamente e começa com as definições de configuração padrão.

Antes de Iniciar

- Revise os pré-requisitos de hardware e de software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Microsoft IIS agent.
- Certifique-se de que o usuário, que se conecta ao ambiente ou aplicativo do Microsoft Internet Information Server, tenha privilégios de administrador. Use um usuário existente com privilégios de administrador, ou crie um novo usuário. Designe privilégios de administrador ao novo usuário, incluindo o novo usuário no grupo Administradores.

  Lembre-se: Para configurar o Microsoft IIS agent, é possível usar um usuário local ou de domínio, desde que o usuário tenha privilégios de administrador.

Sobre Esta Tarefa

É possível configurar o agente quando o agente está em execução ou interrompido. O agente permanece no mesmo estado após a configuração. Por exemplo, se o agente está em execução, ele permanece no estado em execução após a configuração.

Para configurar o agente, é possível usar a janela **IBM Performance Management** ou o arquivo de resposta silencioso.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte o “Histórico de Mudanças” na página 50.

O que Fazer Depois

Depois de configurar o agente, você pode alterar a conta do usuário do usuário local para o usuário do domínio. Para saber as etapas para mudar a conta do usuário, consulte “Mudando a conta do usuário” na página 515.

Configurando o agente nos sistemas Windows

É possível configurar Microsoft IIS agent em sistemas operacionais Windows usando a janela **IBM Performance Management**. Após fazer a atualização dos valores de configuração, deve-se iniciar o agente para salvar os valores atualizados.

Sobre Esta Tarefa

É possível configurar o agente quando o agente está em execução ou interrompido. O agente permanece no mesmo estado após a configuração. Por exemplo, se o agente está em execução, ele permanece no estado em execução após a configuração.

O Microsoft IIS agent fornece valores padrão para alguns parâmetros. É possível especificar diferentes valores para esses parâmetros.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito em **Monitoring Agent for Microsoft Internet Information Services** e clique em **Reconfigurar**.
3. Na janela Monitoring Agent for Microsoft Internet Information Services, conclua as seguintes etapas:
   a) Na guia **Configuração do Log de Erro HTTP**, especifique um local para salvar o arquivo de log e clique em **Avançar**.

      Nota: Por padrão, esse arquivo de log é salvo no seguinte local: `C:\WINDOWS\system32\LogFiles\HTTPERR`. O administrador pode mudar o local do arquivo de log.

b) Na guia **Configuração do Log do Site**, especifique um local para salvar o arquivo de log e clique em **OK**.

Nota: Por padrão, esse arquivo de log é salvo no seguinte local: `C:\inetpub\logs\LogFiles`. O administrador pode mudar o local do arquivo de log.

4. Na janela **Reinicialização do Monitoring Agent for Microsoft IIS**, clique em **Sim**.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.

Configurando o agente usando o arquivo de resposta silencioso

Quando você instala o Microsoft IIS agent, o agente é configurado automaticamente e começa com as definições de configuração padrão. Use o arquivo de resposta silencioso para modificar as definições de configuração padrão.

Antes de Iniciar

Crie um arquivo de resposta que contenha os parâmetros de configuração que você deseja modificar. Se você deseja modificar os parâmetros de configuração padrão, edite o arquivo de resposta.

Sobre Esta Tarefa

É possível configurar o agente quando o agente está em execução ou interrompido. O agente permanece no mesmo estado após a configuração. Por exemplo, se o agente está em execução, ele permanece no estado em execução após a configuração.

Procedimento

Para configurar o Microsoft IIS agent, execute as seguintes etapas:

1. Na linha de comandos, mude o caminho para o diretório que contém o arquivo `msiis-agent.bat`.
2. Insira o seguinte comando: **`msiis-agent.bat config`** *absolute path to the response file*.

   O arquivo de resposta contém os seguintes parâmetros:

   KQ7_SITE_LOG_FILE
   C:\inetpub\logs\LogFiles

   KQ7_HTTP_ERROR_LOG_FILE
   C:\WINDOWS\system32\LogFiles\HTTPERR

   Lembre-se: A configuração do agente é organizada nos seguintes grupos:

   Configuração de Log do Site (SITE_LOG)
   Este grupo contém os parâmetros de configuração relacionados ao arquivo de log do site (KQ7_SITE_LOG_FILE). Um administrador pode especificar um local para salvar o arquivo de log. Por padrão, esse arquivo de log é salvo no seguinte local: `C:\inetpub\logs\LogFiles`

   Configuração do Log de Erros HTTP (HTTP_ERROR_LOG)
   Este grupo contém os parâmetros de configuração relacionados ao arquivo do log de erros HTTP (KQ7_HTTP_ERROR_LOG_FILE). Um administrador pode especificar um local para salvar o arquivo de log. Por padrão, esse arquivo de log é salvo no seguinte local: `C:\WINDOWS\system32\LogFiles\HTTPERR`
3. Se o agente estiver no estado pausado, inicie o agente.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.

Mudando a conta do usuário

Depois de configurar o Microsoft IIS agent, é possível mudar a conta do usuário do usuário local para o usuário do domínio.

Sobre Esta Tarefa

Por padrão, o Microsoft IIS agent é executado na conta do usuário local.

Procedimento

1. Execute o seguinte comando para verificar qual ID do usuário está sendo usado para iniciar o agente:

   ```
   install_dir\InstallITM\KinCinfo.exe -r
   ```
2. Se o agente de monitoramento foi iniciado com um ID do usuário que não pertence ao grupo Administradores, pare o agente.
3. Abra a janela **Gerenciar Serviços de Monitoramento**.
4. Clique com o botão direito na instância de agente e clique em **Alterar Inicialização**.
5. Especifique o ID do usuário completo como <Domain\User ID> e, em seguida, especifique a senha.
6. Inicie o Microsoft IIS agent.

Configurando o monitoramento do Skype for Business Server (anteriormente conhecido como Microsoft Lync Server)

Ao instalar o Monitoring Agent for Skype for Business Server (anteriormente conhecido como MS Lync Server), o agente estará no estado desconfigurado. Para iniciar o agente, é necessário configurá-lo.

Antes de Iniciar

- Revise os pré-requisitos de hardware e software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Agente Skype for Business Server.
- Certifique-se de que o usuário usado para executar o Agente Skype for Business Server seja um usuário do domínio com privilégios de administrador e tenha acesso a todos os servidores remotos que estão listados na topologia do Lync ou do Skype for Business Server. Use um usuário do domínio existente com privilégios de administrador, ou crie um novo usuário do domínio e designe privilégios de administrador ao novo usuário do domínio.

Sobre Esta Tarefa

É possível configurar o agente quando o agente está em execução ou interrompido. O agente permanece no mesmo estado após a configuração. Por exemplo, se o agente está em execução, ele permanece no estado em execução após a configuração.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte o "Histórico de Mudanças" na página 50.

Para configurar o agente, é possível usar a janela **IBM Performance Management** ou o arquivo de resposta silencioso.

O que Fazer Depois
Depois de configurar o agente, é possível mudar a conta do usuário do usuário local para o usuário do domínio. Para saber as etapas para mudar a conta do usuário, consulte "Mudando a conta do usuário" na página 518.

Permissões e direitos de acesso para um usuário não administrador

É possível executar o agente de monitoramento para o Agente Skype for Business Server como um usuário não administrador; no entanto, algumas funções estão inacessíveis.

Permissões de registro

Para criar um usuário não administrador, crie um novo usuário (não administrador) e configure permissões de registro para o novo usuário conforme a seguir.

- Acesso total ao KEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring
- Acesso total ao diretório CANDLE_HOME

O usuário não administrador deve ser um membro dos Usuários do Monitor de Desempenho e dos Usuários de Log de Desempenho. Se você definir essas permissões para um usuário não administrador, dados serão exibidos para todos os grupos de atributos baseados no Perfmon.

Para visualizar dados de grupos de atributos coletados do banco de dados

Se desejar visualizar dados para grupos de atributos que são coletados do banco de dados, você deve configurar as seguintes permissões para o usuário não administrador.

- A conta do usuário não administrador que é usada para executar o Agente Skype for Business Server deve ter a permissão Depurar programa para incluir um depurador em qualquer processo.

  Por padrão, a permissão Depurar programa é designada apenas ao administrador e a contas do Sistema local. Para conceder a permissão Depurar programa, você deve concluir as seguintes etapas no Lync ou Skype for Business Server:

  1. Clique em **Iniciar > Ferramentas Administrativas > Política de Segurança Local**. A janela **Definições de segurança local** é aberta.
  2. Expanda **Políticas Locais** e clique em **Designação de Direitos de Usuário**. A lista de direitos de usuário é aberta.
  3. Dê um clique duplo na **Política Depurar programas**. A janela **Propriedades dos programas de depuração** é aberta.
  4. Clique em **Incluir Usuário ou Grupo**. A janela **Selecionar Usuários ou Grupos** é exibida.
  5. No campo Inserir os nomes de objetos a serem selecionados, insira o nome da conta do usuário para quem você deseja designar permissões e, em seguida, clique em **OK**.
  6. Clique em **OK**.
- Conceda a permissão Efetuar logon como serviço

  Para conceder a permissão Efetuar logon como serviço, você deve concluir as seguintes etapas no Lync ou no Skype for Business Server:

  1. Clique em **Iniciar > Ferramentas Administrativas > Política de Segurança Local**. A janela **Definições de segurança local** é aberta.
  2. Expanda **Políticas Locais** e clique em **Designação de Direitos de Usuário**. A lista de direitos de usuário é aberta.
  3. Dê um clique duplo na política **Efetuar logon** como serviço. A janela **Efetuar logon como propriedades de serviço** é aberta.
  4. Clique em **Incluir Usuário ou Grupo**. A janela **Selecionar Usuários ou Grupos** é exibida.
  5. No campo Inserir os nomes de objetos a serem selecionados, insira o nome da conta do usuário para quem você deseja designar permissões e, em seguida, clique em **OK**.

6. Clique em **OK**.

O grupo de atributos Disponibilidade mostra dados para usuários que são membros do grupo de Administradores.

Configurando o agente nos sistemas Windows

É possível configurar o Agente Skype for Business Server (anteriormente conhecido como agente MS Lync Server) em sistemas operacionais Windows usando a janela **IBM Performance Management**. Após fazer a atualização dos valores de configuração, deve-se iniciar o agente para salvar os valores atualizados.

Sobre Esta Tarefa

É possível configurar o agente quando o agente está em execução ou interrompido. O agente permanece no mesmo estado após a configuração. Por exemplo, se o agente está em execução, ele permanece no estado em execução após a configuração.

O Agente Skype for Business Server fornece valores padrão para alguns parâmetros. É possível especificar diferentes valores para esses parâmetros.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito em **Monitoring Agent for Skype for Business Server** e, em seguida, clique em **Configurar agente**.
3. Na janela Monitoring Agent for Skype for Business Server, conclua as seguintes etapas:
   a) Na guia **Configuração de SQL para Topologia do Skype for Business**, para se conectar ao Microsoft Lync Server ou ao Skype for Business Server Central Management Store, especifique valores para os parâmetros de configuração e, em seguida, clique em **Avançar**.

      Nota: É possível ignorar esta guia, já que Configuração SQL para a topologia do Skype for Business não é aplicável para o IBM Cloud Application Performance Management.

      Importante: A configuração de transação sintética é opcional. Se você requerer dados da transação sintética, especifique os parâmetros de configuração nas guias **Informações de Configuração** e **Configuração do Planejador**.
   b) Na guia **Credenciais de Login do Administrador**, especifique as credenciais do administrador e, em seguida, clique em **Avançar**.
   c) Na guia **Informações de Configuração**, para executar comandos para as transações sintéticas, especifique valores para os parâmetros de configuração e, em seguida, clique em **Avançar**.
   d) Na guia **Configuração do Planejador**, para planejar as transações sintéticas, especifique valores para os parâmetros de configuração e, em seguida, clique em **Avançar**.
   e) Na guia **Configuração de SQL Server para Função de monitoramento do Skype for Business** , para se conectar à função de monitoramento do Microsoft Lync Server ou do Skype for Business Server, especifique valores para os parâmetros de configuração e, em seguida, clique em **Avançar**.

   Para obter informações sobre os parâmetros de configuração, consulte “Parâmetros de configuração para o agente” na página 519.
4. Na janela **IBM Performance Management**, clique com o botão direito em **Monitoring Agent for Skype for Business Server** e, em seguida, clique em **Iniciar**.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte “Iniciando o Console do Cloud APM” na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.

Configurando o agente usando o arquivo de resposta silencioso

Ao instalar o Agente Skype for Business Server (anteriormente conhecido como agente MS Lync Server), o agente estará no estado desconfigurado. Para iniciar o agente, é necessário configurá-lo.
O arquivo de resposta silencioso contém parâmetros de configuração do agente com valores padrão definidos para alguns parâmetros. É possível editar o arquivo de resposta silencioso para especificar os valores diferentes para os parâmetros de configuração.

Antes de Iniciar

Crie um arquivo de resposta que contenha os parâmetros de configuração que você deseja modificar. Se você deseja modificar os parâmetros de configuração padrão, edite o arquivo de resposta.

Sobre Esta Tarefa

É possível configurar o agente quando o agente está em execução ou interrompido. O agente permanece no mesmo estado após a configuração. Por exemplo, se o agente está em execução, ele permanece no estado em execução após a configuração.

Procedimento

Para configurar o Agente Skype for Business Server, execute as seguintes etapas:

1. Abra o prompt de comandos.
2. Mude o caminho para o diretório que contém o arquivo `skype_for_business_server-agent.bat`.
3. Insira o comando **`skype_for_business_server-agent.bat config`** *absolute path to the response file*.

   Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração para o agente" na página 519.
4. Inicie o agente se ele estiver no estado pausado.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.

Mudando a conta do usuário

Depois de configurar o Agente Skype for Business Server, é possível mudar a conta do usuário do usuário local para o usuário do domínio.

Sobre Esta Tarefa

Por padrão, o Agente Skype for Business Server é executado na conta do usuário local. Quando o agente for executado no usuário do domínio, o agente poderá coletar dados dos servidores remotos.

Procedimento

1. Execute o seguinte comando para verificar qual ID do usuário está sendo usado para iniciar o agente:

   `install_dir\InstallITM\KinCinfo.exe -r`
2. Se o agente de monitoramento foi iniciado com um ID do usuário que não pertence ao grupo Administradores, pare o agente.
3. Abra a janela **Gerenciar Serviços de Monitoramento**.
4. Clique com o botão direito na instância de agente e clique em **Alterar Inicialização**.
5. Especifique o ID do usuário completo como <Domain\User ID> e, em seguida, especifique a senha.
6. Inicie o Agente Skype for Business Server.

Parâmetros de configuração para o agente

Ao configurar o Agente Skype for Business Server (anteriormente conhecido como agente MS Lync Server), é possível mudar os valores padrão dos parâmetros de configuração, como o nome do servidor de banco de dados, o nome da instância do banco de dados, o nome do banco de dados e outros parâmetros.

A tabela a seguir contém descrições dos parâmetros de configuração para o Agente Skype for Business Server.

Nota: Fora de todos os campos, o campo Pool FQDN é obrigatório na tabela a seguir.

Tabela 177. Nomes e descrições dos parâmetros de configuração para o agente

Nome do parâmetro	Descrição
Nome do Servidor de Banco de Dados (por exemplo, PS6877)	• Guia **Configuração de SQL para Topologia do Skype for Business**: O nome do servidor de banco de dados no qual o Lync ou Skype for Business Server Central Management Store está instalado. • Guia **Configuração de SQL Server para Função de Monitoramento do Skype for Business**: O nome do servidor de banco de dados no qual a função de monitoramento está instalada.
Nome da Instância do Banco de Dados	• Guia **Configuração de SQL para Topologia do Skype for Business**: A instância padrão. • Guia **Configuração de SQL Server para Função de Monitoramento do Skype for Business**: O nome da instância de banco de dados onde a função de monitoramento está instalada.
Nome do banco de dados	O nome do banco de dados.
ID do Usuário de Banco de Dados	O ID do usuário do banco de dados. Esse usuário deve ter acesso à instância necessária do Microsoft SQL Server. Este usuário não precisa ser um usuário do Active Directory.
Senha do Banco de Dados	A senha do banco de dados no qual a função de monitoramento está instalada.
Nome do usuário (Exemplo: skype \administrator)	O ID do usuário do administrador. Este usuário deve ser um usuário do domínio com privilégios de administrador e acesso a todos os servidores remotos que estão listados na topologia do Lync ou do Skype for Business Server. As credenciais desse usuário também são usadas no recurso Transação Sintética. Portanto, esse usuário deve estar autorizado a criar o Planejamento do Windows no Planejador de Tarefas e executar Comandos de Transação Sintética.
Senha	A senha de login do administrador.
Confirmar Senha do Domínio	Insira a mesma senha especificada no campo Senha do Domínio.
FQDN do Conjunto	O nome completo do domínio (FQDN) do Conjunto de Skype para o qual os comandos sintéticos são executados.
Local Geográfico	A localização geográfica do sistema de produção.

Tabela 177. Nomes e descrições dos parâmetros de configuração para o agente (continuação)	
Nome do parâmetro	**Descrição**
Users1 de teste (por exemplo, user1@skype.com)	O primeiro Nome do usuário, que pode ser usado ao executar cmdlets de Transação sintética. O formato para nome do usuário é SAMAccountName@domain.com. Não forneça o Endereço Sip.
Test User1 PWD	A senha do Test User1.
Confirme o Test User1 PWD	Insira a mesma senha que você especificou no campo **Test User1 PWD**.
User2 de teste (por exemplo, user2@skype.com)	O segundo Nome do usuário, que pode ser usado ao executar cmdlets de Transação sintética. O formato para nome do usuário é SAMAccountName@domain.com. Não forneça o Endereço Sip.
Senha do Usuário2 de Teste	A senha do Test User2.
Confirme o Test User2 PWD	Insira a mesma senha que você especificou no campo **Test User2 PWD**.
Usar valores de configuração do agente	Mantenha esse campo ativado se você desejar executar comandos sintéticos usando todos os campos fornecidos no painel de configuração. Desative para usar valores configurados por New-CsHealthMonitoringConfiguration. Se desativado, o valor de **Pool FQDN** será usado como identidade para Get-CsHealthMonitoringConfiguration. Certifique-se de fornecer credenciais de usuário de teste válidas para executar o comando **Test-CsMcxP2PIM**.
Frequência	A frequência do utilitário planejado que busca dados de transações sintéticas. A frequência pode ter os valores a seguir: • Diário (DAY_FREQUENCY) • Semanal (WEEK_FREQUENCY) • Mensal (MONTHLY_FREQUENCY)
Hora da Coleção	A parte da hora do registro de data e hora, no formato do relógio de 24 horas, que você seleciona para planejar o utilitário.
Minuto da Coleção	A parte dos minutos do registro de data e hora que você seleciona para planejar o utilitário.
Data de Início (AAAA-MM-DD)	O horário em que o planejador é ativado.
Data de Encerramento (AAAA-MM-DD)	O horário em que o planejador é desativado.

Configurando o monitoramento do Microsoft .NET

O Monitoring Agent for Microsoft .NET monitora aplicativos .NET. O agente inicia automaticamente após a instalação para coletar dados de monitoramento de recursos. No entanto, para coletar dados de rastreamento de transações e diagnósticos, você deve concluir algumas tarefas de configuração.

Antes de Iniciar
Revise os pré-requisitos de hardware e software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Microsoft .NET agent.

Sobre Esta Tarefa
Após a instalação do agente, conclua as seguintes tarefas de configuração para que o agente possa coletar dados de rastreamento de transações e diagnósticos:

1. Registrando o coletor de dados
   O coletor de dados é um componente do Microsoft .NET agent. Ele coleta os dados de rastreamento de transações e diagnósticos e transmite os dados para o Microsoft .NET agent. Você deve registrar o coletor de dados para coletar esses dados. Para obter detalhes, consulte "Registrando o coletor de dados" na página 522.
2. Configurando a coleta de dados de rastreamento de transação e diagnósticos
   Depois de registrar o coletor de dados, ative a coleta de dados de rastreamento de transações e diagnósticos no Console do Cloud APM. Também é possível ativar a coleta de dados diagnósticos usando o comando **configdc**. Para obter detalhes, consulte "Ativando a coleta de dados de rastreamento de transações e diagnósticos" na página 525 e "Ativando a coleta de dados diagnósticos usando o comando configdc" na página 526.
3. Ativando as atualizações de configuração
   Se você ativar a coleta de dados diagnósticos usando o comando **configdc**, deverá ativar a configuração para que as atualizações sejam salvas no arquivo de configuração. Para obter informações adicionais sobre como ativar as mudanças na configuração, consulte "Ativando as atualizações de configuração" na página 527.
4. Ajustando o desempenho do coletor de dados
   Pode ser necessário concluir algumas tarefas para otimizar o desempenho do coletor de dados. Para obter detalhes, consulte "Ajuste de desempenho do coletor de dados" na página 528.

Coexistência de agente
Em um ambiente de coexistência do agente, é possível visualizar dados de rastreamento de transação do Console do Cloud APM ou do Tivoli® Enterprise Portal. Para obter informações sobre como ativar a coleta de dados para o rastreamento de transação no ambiente de coexistência do agente, consulte "Ativando o rastreamento de transação no ambiente de coexistência de agentes" na página 526.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Versão do Agente. Para acessar a documentação para liberações anteriores do agente, consulte a tabela a seguir:

Tabela 178. Documentação e versões do agente

Versão do Microsoft .NET agent	Documentação
8.1.3.2	IBM Cloud Application Performance Management
8.1.3 e 8.1.2	IBM Performance Management 8.1.3

O link abre um tópico do Knowledge Center no local.

Permissões para executar um agente usando uma conta local ou de domínio

Somente um usuário local ou de domínio que seja membro do grupo Administradores possui permissões para executar o Microsoft .NET agent. Este tópico fornece condições que devem ser atendidas se o usuário local ou do domínio não for um membro do grupo Administradores.

O usuário deve ter as seguintes permissões para a unidade do sistema e a unidade de instalação do agente

1. Ler
2. Gravar

3. Execução
4. Modificar

O usuário deve ter a permissão a seguir para a chave de registro HKEY_LOCAL_MACHINE

- Ler

O usuário deve ser membro dos seguintes grupos no servidor monitorado

1. usuários
2. IIS_IUSRS
3. Usuários do Performance Monitor
4. Usuários de Log de Desempenho

Nota: No entanto, é recomendável executar o Microsoft .NET agent com um usuário local ou de domínio que seja membro do grupo de Administradores locais.

Registrando o coletor de dados

Você deve registrar o coletor de dados para coletar dados de rastreamento de transações e diagnósticos. Para coletar os dados de monitoramento de recurso, nenhuma configuração específica é necessária.

Sobre Esta Tarefa

Registre os seguintes componentes do coletor de dados, dependendo da transação, de diagnósticos, ou de ambos os tipos de dados que você deseja que sejam coletados pelo coletor de dados:

Tabela 179. Componentes do coletor de dados e suas funções

Nome do Componente	**Monitores**
httpmodule	Transações ASP.NET e coleta o tempo de resposta e o tempo de CPU da solicitação
gerenciador de perfis	Transações ADO.NET e coleta dados de método, de rastreio de pilha e de contexto de solicitação para diagnósticos
isapi	Transações ASP.NET e coleta o tempo de resposta e o tempo de CPU da solicitação
soap	Transações de serviço ASMX ou WCF e tempo de resposta de serviços WCF

Lembre-se:

- Use `isapi32` para filtrar aplicativos de 32 bits em um Microsoft IIS Server de 64 bits.
- Registre todos os componentes para rastrear todas as transações e visualizar a topologia de transação completa.

Procedimento

1. No servidor no qual o agente está instalado, execute o seguinte comando como um administrador:

```
cd install_dir\qe\bin
configdc.exe registerdc [all|isapi|isapi32|profiler|httpmodule|soap]
```

Lembre-se:

- Ao executar o comando **`configdc.exe registerdc`** sem especificar nenhum componente para registrar, somente httpmodule é registrado.

- Para registrar todos os componentes, execute o comando **configdc.exe registerdc all**.
- Para registrar qualquer um dos componentes juntos, execute esse comando: **configdc.exe registerdc** *component_name component_name*. Por exemplo, **configdc.exe registerdc** httpmodule profiler

2. Reinicie os aplicativos .NET.

O que Fazer Depois
Depois de registrar o coletor de dados, você deve ativar a coleta de dados para rastreamento de transação e diagnósticos. Para obter informações sobre como ativar a coleta de dados, consulte "Ativando a coleta de dados de rastreamento de transações e diagnósticos" na página 525.

Se deseja parar o monitoramento de aplicativos .NET, cancele o registro do coletor de dados. Repita as etapas especificadas usando o comando **configdc.exe unregisterdc** para cancelar o registro de todos os componentes do coletor de dados.

Usando o módulo de Tempo de Resposta do IIS do agente .NET

Da liberação 8.1.4.0.2 em diante, o agente .NET inclui o "módulo de Tempo de Resposta do IIS ", que trabalha com o agente de Tempo de Resposta para mostrar dados de transações do usuário final para o servidor IIS.

Ativando o módulo de Tempo de Resposta
É preciso ativar o módulo de Tempo de Resposta antes de usá-lo.

Procedimento

Conclua as seguintes etapas para ativar o módulo de Tempo de Resposta:

1. Abra o prompt de comandos no modo de administrador.
2. Para parar o IIS, execute o seguinte comando:

   ```
   iisreset /stop
   ```
3. Acesse o diretório `install_dir\qe\bin` no prompt de comandos.
4. Para registrar o módulo de Tempo de Resposta para IIS, execute o seguinte comando:

   ```
   configdc registerdc rtmodule
   ```
5. Para iniciar o IIS, execute o seguinte comando:

   ```
   iisreset /start
   ```

Resultados
O módulo de Tempo de Resposta está ativado.

Configurando o agente de Tempo de Resposta para trabalhar com o módulo de Tempo de Resposta do IIS do agente .NET
É preciso configurar o agente de Tempo de Resposta para trabalhar com o módulo de Tempo de Resposta do IIS do agente .NET.

Antes de Iniciar
Instale o agente de Tempo de Resposta (versão 8.1.4); Para obter mais informações, consulte Capítulo 6, "Instalando os agentes", na página 117.

Procedimento

Conclua as seguintes etapas para configurar o agente de Tempo de Resposta para trabalhar com o módulo de Tempo de Resposta do IIS do Agente .NET:

1. Abra um editor de texto no modo de administrador.
2. Abra o seguinte arquivo no editor de texto:

config_dir\TMAITM6_x64*host_name*_T5.config

em que *config_dir* é o início do APM e *host_name* é o nome do servidor.

3. Atualize a seguinte propriedade:

   { KT5DISABLEANALYZER=YES } { KT5ENABLEWEBPLUGIN=YES }

4. Inclua a seguinte propriedade na seção SECTION=analyzerconfig [ ]:

   {KT5WEBPLUGINIPCNAME=KFC1}

5. Reinicie o agente de Tempo de Resposta.
6. Efetue login no console do Performance Management para verificar os dados coletados pelo agente nos painéis. Para obter informações sobre como utilizar o console do Performance Management, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando a injeção de JavaScript para o módulo de Tempo de Resposta do IIS
Deve-se configurar a Injeção do JavaScript (JS) para trabalhar com o módulo de Tempo de Resposta do Internet Information Services (IIS) do agente .NET.

Procedimento

Para configurar a Injeção de JS para trabalhar com o módulo de Tempo de Resposta do IIS do agente .NET, siga estas etapas:

1. Abra um editor de texto no modo de administrador.
2. Abra o seguinte arquivo no editor de texto:

   <APM_HOME>\qe\config\dotNetDcConfig.properties.inactive

3. Para ativar a Injeção de JS para o módulo de Tempo de Resposta, configure a propriedade **RTModule.JSInjection.Enabled** como **true**.
4. Para desativar a Injeção de JS para o módulo de Tempo de Resposta, configure a propriedade **RTModule.JSInjection.Enabled** como **false**.
5. Abra o prompt de comandos no modo de administrador e acesse o diretório <APM_HOME>\qe\bin.
6. Execute os seguintes comandos:
   - configdc activateconfig
   - iisreset

Desativando o Módulo de Tempo de Resposta do IIS
É possível desativar o módulo de Tempo de Resposta do IIS quando você não desejar ver dados de transações do usuário final para o servidor IIS.

Procedimento

Conclua as seguintes etapas para desativar o módulo de tempo de resposta do IIS:

1. Abra o prompt de comandos no modo de administrador.
2. Para parar o IIS, execute o seguinte comando:

   iisreset /stop

3. Acesse o diretório *install_dir*\qe\bin no prompt de comandos.
4. Para cancelar o registro do módulo de Tempo de Resposta para IIS, conclua as seguintes etapas:
   - Para cancelar o registro do módulo de tempo de resposta para IIS, execute o seguinte comando:

     configdc unregisterdc rtmodule

   - Para cancelar o registro de todos os componentes do coletor de dados, incluindo o módulo de Tempo de Resposta, execute o seguinte comando:

     configdc unregisterdc all

5. Para iniciar o IIS, execute o seguinte comando:

```
iisreset /start
```

Resultados
O módulo de tempo de resposta do IIS é desativado.

Limitações do módulo de Tempo de Resposta do IIS
As limitações do módulo de Tempo de Resposta do IIS estão listadas aqui.

- As informações sobre o usuário não são rastreadas pelo módulo de Tempo de Resposta do IIS e o nome do usuário aparece atualmente como "Desconhecido".

Ativando a coleta de dados de rastreamento de transações e diagnósticos

Na página **Configuração do agente**, é possível ativar ou desativar a coleta de dados de rastreamento de transações e diagnósticos.

Antes de Iniciar
Certifique-se de que tenha registrado o coletor de dados. Para obter detalhes, consulte “Registrando o coletor de dados” na página 522.

Procedimento

Conclua as seguintes etapas para configurar a coleta de dados para cada sistema gerenciado.

1. Efetue login no Console do Cloud APM.
2. A partir da barra de navegação, clique em **Configuração do Sistema** > **Configuração do Agente**.
   A página **Configuração do Agente** é exibida.
3. Clique na guia **MS .NET**.
4. Selecione as caixas de seleção dos sistemas gerenciados para os quais você deseja configurar a coleta de dados e conclua qualquer uma das seguintes ações da lista **Ações**.
   - Para ativar o rastreamento de transações, clique em **Configurar rastreamento de transações** > **Ativado**. O status na coluna **Rastreamento da Transação** é atualizado para Ativado para cada sistema gerenciado selecionado.
   - Para ativar a coleta de dados diagnósticos, selecione **Configurar modo de diagnóstico** e clique no nível que deseja configurar. O status na coluna **Modo de diagnóstico** é atualizado para exibir o nível especificado para cada sistema gerenciado selecionado.
     - Nível 1: O módulo HTTP coleta os dados de resumo de solicitação e de instância de solicitação.
     - Nível 2: O módulo HTTP coleta os resumo de solicitação e dados de instância de solicitação. O gerenciador de perfis coleta os dados de método e dados de rastreio de pilha.
   - Para desativar o rastreamento de transação, clique em **Configurar Rastreamento de Transação** > **Desativado**. O status na coluna **Rastreamento de Transação** é atualizado para Desativado para cada sistema gerenciado selecionado.
   - Para desativar a coleta de dados diagnósticos, clique em **Configurar Modo de Diagnóstico** > **Desativado**. O status na coluna **Modo de Diagnóstico** é atualizado para Desativado para cada sistema gerenciado selecionado.

Resultados
A coleta de dados é configurada para cada sistema gerenciado.

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados de rastreamento de transação e diagnósticos que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte “Iniciando o Console do Cloud APM” na página 975.

Ativando a coleta de dados diagnósticos usando o comando configdc

Também é possível ativar ou desativar a coleta de dados diagnósticos usando o comando **configdc**. Esse processo é opcional.

Antes de Iniciar

- Certifique-se de que tenha registrado o coletor de dados. Para obter detalhes, consulte "Registrando o coletor de dados" na página 522.
- Assegure-se de que você tenha concluído o processo no "Ativando a coleta de dados de rastreamento de transações e diagnósticos" na página 525.
- Assegure-se de que o arquivo `qe_custom.properties` seja processado pelo servidor APM no `<APM_Home>\localconfig\qe` e tenha as seguintes propriedades:
  - transaction_tracking=ENABLED
  - diagnostic_mode=LEVEL2

Procedimento

1. Execute o seguinte comando:

   ```
   cd install_dir\qe\bin configdc deepdivedc -tracelevel trace_level
   ```

   Em que

   install_dir
   O diretório de instalação do Microsoft .NET agent.

   trace_level
   O nível de rastreio que indica a quantidade de dados diagnósticos que o .NET Data Collector coleta. Especifique um dos valores a seguir:

   0
   A coleta de dados diagnósticos é desativada.

   1
   A coleta de dados diagnósticos é ativada. O módulo HTTP coleta o resumo de solicitação e dados de instância de solicitação.

   2
   A coleta de dados diagnósticos é ativada. O módulo HTTP coleta o resumo de solicitação e dados de instância de solicitação. O gerenciador de perfis coleta dados de métodos e dados de rastreio de pilha.

   Dica: Ao configurar o nível de rastreio usando o comando **`configdc.exe deepdivedc -tracelevel`**, o valor do parâmetro `bci_dc.diagnose.level` é configurado no arquivo `dotNetDcConfig.properties`.
2. Ative as mudanças na configuração.

   Para obter informações sobre a ativação de mudanças, consulte "Ativando as atualizações de configuração" na página 527.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar dados diagnósticos que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Ativando o rastreamento de transação no ambiente de coexistência de agentes

Em um ambiente coexistente do agente, é possível configurar o coletor de dados para coletar e transmitir os dados de rastreamento de transação para o Tivoli Enterprise Portal, que é um componente do IBM Tivoli Monitoring.

Antes de Iniciar
Deve-se instalar o Microsoft .NET agent, entregue como parte do Cloud APM, e remover ou cancelar o registro do componente .NET Data Collector, que é entregue com ITCAM for Microsoft Applications. Utilize o comando **configdc.exe unregisterdc** para cancelar o registro de todos os módulos do coletor de dados.

Procedimento

Para configurar o coletor de dados para coletar e transmitir os dados de rastreamento de transação para o Tivoli Enterprise Portal, conclua as seguintes etapas:

1. Vá para o diretório *install_dir*\localconfig\qe, em que *install_dir* é o diretório de instalação do Microsoft .NET agent. O caminho padrão é C:\IBM\APM.
2. Abra o arquivo qe_default.properties e configure o valor do parâmetro **transaction_tracking** para ENABLED.
3. Salve e feche o arquivo qe_default.properties.
4. Vá para o diretório *install_dir*\qe\config.
5. Abra o arquivo dotNetDcConfig.properties.inactive em um editor de texto.
6. Configure os parâmetros **TTDC.enabled** e **TTAS.enabled** como a seguir:

```
TTDC.enabled=true
TTAS.enabled=true
```

7. Para configurar a conexão para o Transaction Collector, configure os valores dos parâmetros **TTAS.Host** e **TTAS.Port** para o endereço IP e número de porta do Transaction Collector.
8. Execute o seguinte comando para ativar as mudanças:

```
install_dir\qe\bin\configdc.exe activateconfig
```

9. Reinicie o aplicativo .NET para que as mudanças entrem em vigor.

Resultados
Agora, os dados de rastreamento de transação podem ser coletados e exibidos no Tivoli Enterprise Portal.

O que Fazer Depois

Para desativar o rastreamento de transação para um .NET Data Collector, repita o procedimento e use os seguintes valores de configuração:

- No arquivo qe_default.properties, configure transaction_tracking=DISABLED.
- No arquivo dotNetDcConfig.properties.inactive, configure TTDC.enabled=false e TTAS.enabled=false.

Ativando as atualizações de configuração

Deve-se ativar as atualizações que são feitas nas definições de configuração usando o comando configdc. A ativação assegura que suas atualizações sejam salvas no arquivo dotNetConfig.properties.

Sobre Esta Tarefa
Ao atualizar as definições de configuração usando o comando **configdc**, os valores de parâmetro são atualizados no arquivo dotNetConfig.properties. No entanto, se esse arquivo estiver sendo usado e não puder ser modificado, as atualizações de definição de configuração serão salvas no arquivo dotNetDcConfig.properties.inactive. Você deve ativar a configuração para que as atualizações sejam salvas no arquivo dotNetConfig.properties.

Procedimento

1. Acesse o seguinte caminho:

install_dir\qe\bin
Em que *install_dir* é o diretório de instalação do Microsoft .NET agent.

2. Execute o seguinte comando:
   `configdc activateConfig`

O que Fazer Depois

Se as transações do Internet Information Service (IIS) forem monitoradas e a configuração do coletor de dados estiver atualizada, reinicie o IIS para ativar a configuração.

Se os serviços da web ASMX ou WCF forem monitorados e a configuração do coletor de dados for atualizada, reinicie o processo que hospeda o serviço da web.

Ajuste de desempenho do coletor de dados

Ao configurar o coletor de dados para coletar os dados de rastreamento de transação e diagnósticos, o desempenho do coletor de dados é afetado. Para melhorar o desempenho, é possível concluir algumas tarefas de ajuste de desempenho.

Pode ser necessário concluir as seguintes tarefas para melhorar o desempenho do coletor de dados:

- Filtre as interfaces ADO.NET que você deseja monitorar.
- Faça amostragem dos dados de rastreamento de transação e diagnósticos.
- Configure a criação de logs de rastreio.

Especificando interfaces ADO.NET para monitoramento

Você pode especificar as interfaces do cliente ADO.NET que deseja ativar para o rastreamento de transação.

Antes de Iniciar

Se desejar visualizar as interfaces ADO.NET que são suportadas pelo .NET Data Collector, consulte Funções de namespaces suportadas pelo coletor de dados.

Para visualizar os valores de configuração do .NET Data Collector, consulte o arquivo `dotNetDcConfig.properties` no diretório *install_dir*\qe\config, em que *install_dir* é o diretório de instalação do Microsoft .NET agent.

Sobre Esta Tarefa

Por padrão, todas as interfaces ADO.NET suportadas são ativadas para rastreamento de transação durante a instalação do agente. Para especificar as interfaces que o coletor de dados deve monitorar, ative ou desative o monitoramento para interfaces específicas.

Se você desativar o monitoramento de uma interface, as configurações de qualquer filtro de domínio de aplicativo associado permanecem no arquivo de configuração do coletor de dados. O filtro será retido quando a interface for ativada novamente.

Procedimento

- Para ativar o monitoramento de uma interface ADO.NET, conclua estas etapas:
  a) No diretório *install_dir*\qe\bin, execute o seguinte comando:

  ```
  configdc enableMonitor all | adsi | db2 | ldap | odbc | oledb | oracle | sql
  | http | web
  [-appdomain appdomain filter list]
  ```

  b) Ative as mudanças na configuração.

  Para obter informações sobre a ativação de mudanças, consulte “Ativando as atualizações de configuração” na página 527.
- Para desativar o monitoramento de uma interface ADO.NET, conclua estas etapas:

a) No diretório *install_dir*\qe\bin, execute o seguinte comando:

```
configdc disableMonitor all | adsi | db2 | ldap | odbc | oledb | oracle | sql
| http | web
```

b) Ative as mudanças na configuração.

Para obter informações sobre a ativação de mudanças, consulte "Ativando as atualizações de configuração" na página 527.

Amostragem de rastreamento de transações e dados diagnósticos

Se o desempenho do sistema for afetado devido a coleta de dados de rastreamento de transação ou diagnósticos, é possível ativar a amostragem dos dados coletados para melhorar o desempenho.

Sobre Esta Tarefa

Quando o desempenho do sistema sofre devido à coleta de dados de rastreamento de transação e diagnósticos, é possível configurar o coletor de dados para periodicamente coletar dados por amostragem. Quando a amostragem está ativada, o coletor de dados não coleta dados para cada solicitação, mas em intervalos de várias solicitações. É possível mudar a taxa de amostragem dinamicamente, de acordo com o uso da CPU do processo DotNetProfilerService.

CUIDADO: No entanto, a amostragem pode salvar dados de amostra de recursos do sistema que podem não ser eficientes para diagnosticar problemas. Após a amostragem de dados ser ativada, a topologia de rastreamento de transação pode ser interrompida ou perdida. Portanto, ative a amostragem de dados somente quando o desempenho for seriamente afetado.

Procedimento

Para ativar a amostragem na coleta de dados de rastreamento e diagnóstico de transação, conclua as seguintes etapas:

1. Acesse o diretório a seguir:
   install_dir\qe\config
   Em que *install_dir* é o diretório de instalação do Microsoft .NET agent.
2. Em um editor de texto, abra o arquivo `dotNetDcConfig.properties.inactive`.
3. Configure os parâmetros a seguir no arquivo:

   bci_dc.sampling.Enabled
   Especifica se o coletor de dados coleta periodicamente os dados de rastreamento e diagnóstico de transação. Os valores válidos são `true` e `false`.

   bci_dc.sampling.base
   Especifica a base para a amostragem de dados. Um valor válido é um número positivo. Por exemplo, se você configurar o valor do parâmetro **`bci_dc.sampling.base`** para 10, o coletor de dados coletará os dados de rastreamento e diagnóstico de transação a cada 10 solicitações. A taxa de amostragem é 1 de 10 solicitações. O coletor de dados coleta dados para a 1ª, 11ª, 21ª, 31ª e outras solicitações.

   bci_dc.dynamic.sampling
   Especifica se a taxa de amostragem é constante ou dinâmica. Os valores válidos são on e `off`. Ao configurar o valor do parâmetro **`bci_dc.dynamic.sampling`** para on, a taxa de amostragem será dinamicamente ajustada de acordo com o valor do parâmetro **`bci_dc.dynamic.max_cpu_usage`**.

   bci_dc.dynamic.max_cpu_usage
   Especifica o limite de uso de CPU para o processo DotNetProfilerService. Se o uso da CPU do processo DotNetProfilerService for maior que 110% do valor especificado, a taxa de amostragem será diminuída. Se o uso de CPU for menor que 90% do valor especificado, a taxa de amostragem será aumentada. Um valor válido está no intervalo de 1 a 100.
4. Salve e feche o arquivo `dotNetDcConfig.properties.inactive`.
5. Execute o seguinte comando para ativar as mudanças:

```
install_dir\qe\bin\configdc.exe activateconfig
```

6. Reinicie o aplicativo .NET para que a mudança entre em vigor.

Ativando a criação de logs de rastreio para o coletor de dados
É possível ativar a geração de logs de rastreio para o coletor de dados. É possível usar esses logs de rastreio para resolver problemas que podem ocorrer com a coleta de dados de rastreamento de transações e diagnósticos.

Sobre Esta Tarefa

Para coletar logs para transações ASP.NET, transações ADO.NET e dados diagnósticos, ative os logs de rastreio para os componentes httpmodule, profiler e isapi do coletor de dados. Para coletar logs para transações ASMX e WCF, ative logs de rastreio para o componente soap do coletor de dados.

Importante: O desempenho do coletor de dados pode ser afetado quando a criação de logs de rastreio é ativada. Portanto, desative a criação de logs de rastreio após a coleta dos logs de rastreio necessários.

Procedimento

1. No servidor em que o agente está instalado, navegue para o seguinte caminho:
   install_dir\qe\bin
   Em que *install_dir* é o diretório de instalação do Microsoft .NET agent.
2. Conclua ambos ou qualquer um dos seguintes procedimentos, dependendo dos logs de rastreio que você deseja ativar:
   - Para ativar os logs de rastreio para httpmodule, gerenciador de perfis, componentes soap e módulo de tempo de resposta, conclua as etapas a seguir:
     a. Execute o seguinte comando:
        configdc logging -tracing on
     b. Reinicie os aplicativos IIS e .NET.
   - Para ativar os logs de rastreio para o mecanismo BCI, conclua as etapas a seguir:
     a. Navegue para o seguinte caminho:
        <APM_HOME>\qe\config
     b. Em um editor de texto, abra o arquivo dotNetDcConfig.properties.inactive.
     c. Para a propriedade **bci_dc.trace.logging**, especifique o valor como on.
     d. Execute o seguinte comando:
        configdc activateconfig
     e. Reinicie o IIS.

O que Fazer Depois
Para desativar os logs de rastreio, faça o seguinte:

- Para desativar os logs de rastreio para httpmodule, gerenciador de perfis, componentes soap e módulo de tempo de resposta:
  – Execute o seguinte comando:
    configdc logging -tracing off
  – Reinicie os aplicativos IIS e .NET.
- Para desativar logs de rastreio para o mecanismo BCI:
  – Acesse o seguinte caminho:
    <APM_HOME>\qe\config
  – Em um editor de texto, abra o arquivo dotNetDcConfig.properties.inactive.
  – Para a propriedade **bci_dc.trace.logging**, especifique o valor como off.

- Execute o seguinte comando:
  configdc activateconfig
- Reinicie os aplicativos IIS e .NET.

Configurando o monitoramento do Microsoft Office 365

Você deve configurar o Microsoft Office 365 agent para monitorar a disponibilidade e desempenho de assinaturas do Microsoft Office 365 da organização.

Antes de Iniciar

- Revise os pré-requisitos de hardware e software.
- Para coletar dados para usuários do Office 365, os seguintes módulos devem ser instalados no cliente Windows onde o agente está instalado:
  - PowerShell 3.0 ou mais recente
  - Microsoft Online Services Sign-In Assistant PowerShell
  - SharePoint Online Management Shell
  - DotNetFrameworkVersion 4.5.2 ou mais recente

  Um usuário, que configura o agente, deve ter privilégios administrativos junto com privilégios para ativar a política de execução remota do PowerShell.
- Para monitorar transações sintéticas do Skype, conclua as seguintes tarefas:
  - Instale o cliente Skype 2013 no cliente Windows onde o usuário deseja executar transações sintéticas para o Skype.
  - Configure o dispositivo de vídeo padrão para Lync e Skype como um filtro de áudio/vídeo virtual.
- Certifique-se de que o usuário, que inicia o Microsoft Office 365, tenha privilégios de administrador. Use um usuário existente com privilégios de administrador ou crie um novo usuário. Designe privilégios de administrador ao novo usuário, incluindo o novo usuário no grupo Administradores.

Revise os pré-requisitos de hardware e de software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Microsoft Office 365 agent.

Sobre Esta Tarefa

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Microsoft Office 365 agent. Para acessar a documentação para a V1.0.0, consulte o Knowledge Center do IBM Cloud Application Performance Management.

É possível iniciar o Microsoft Office 365 agent após o agente ser instalado. No entanto, a configuração manual será necessária para visualizar os dados para todos os atributos do agente.

Para configurar o agente, é possível usar a janela IBM Cloud Application Performance Management ou o arquivo silencioso de resposta.

Verificando o alcance de usuários configurados

Para verificar o alcance, o Microsoft Office 365 agent envia um e-mail para os usuários configurados e mede a quantidade de tempo para receber uma resposta automatizada. Antes de iniciar o agente, você deve configurar todos os usuários, que são definidos na configuração de alcance da caixa de correio do agente Office 365 para responderem automaticamente aos e-mails.

Antes de Iniciar

Antes de configurar os usuários do Exchange Online para alcance, certifique-se de que as seguintes tarefas estejam concluídas:

- É criada uma caixa de correio para cada usuário no Exchange Online que você deseja monitorar.
- O usuário criado para o agente é um usuário global do Office 365.

Procedimento

Conclua as seguintes etapas para cada conta do usuário do Exchange Online para a qual você deseja verificar o alcance:

1. Efetue login no Microsoft Outlook, especificando as credenciais do usuário criado.
2. Clique em **Ferramentas > Regras e Alertas > Nova Regra**.
3. Na janela **Assistente de regras**, em **Iniciar a partir de uma regra em branco**, clique em **Aplicar regra nas mensagens que recebo** e clique em **Avançar**.
4. Selecione as seguintes opções:
   - **De pessoas ou grupo público**
   - **Com palavras específicas no assunto**
5. Na **Etapa 2** na janela, clique em **pessoas ou grupo público**.
6. Na janela **Endereço de regra**, selecione o usuário (administrador global) do qual as mensagens devem ser recebidas e clique em **Avançar**.
7. Na **Etapa 2** na janela, clique em **Palavras específicas**.
8. No campo **Especificar palavras ou frases para procurar no assunto ou corpo**, digite `Testar alcance`.
9. Clique em **Incluir**.
10. Clique em **OK** e, em seguida, clique em **Avançar**.
11. Selecione **Fazer com que o servidor responda usando uma mensagem específica** e clique em **uma mensagem específica**.
12. No editor de mensagens de email, digite o seguinte texto no campo de assunto da mensagem: `Testar alcance`.
13. Na lista **Para**, inclua o administrador global.
14. Feche o editor de mensagem de email e clique em **Sim** para salvar essas mudanças.
15. Clique em **Concluir**.
16. Clique em **Aplicar** e, em seguida, clique em **OK**.

O que Fazer Depois

Configure o Microsoft Office 365 agent.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Configurando o agente nos sistemas Windows

É possível configurar o Microsoft Office 365 agent em sistemas operacionais Windows usando a janela IBM Cloud Application Performance Management. Após fazer a atualização dos valores de configuração, deve-se iniciar o agente para salvar os valores atualizados.

Sobre Esta Tarefa

É possível configurar o agente quando o agente está em execução ou interrompido. O agente permanece no mesmo estado após a configuração. Por exemplo, se o agente está em execução, ele permanece no estado em execução após a configuração.

O Microsoft Office 365 agent fornece valores padrão para alguns parâmetros. É possível especificar diferentes valores para esses parâmetros.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.

2. Na janela **IBM Performance Management**, clique com o botão direito em **Monitoring Agent for Microsoft Office 365** e clique em **Configurar agente**.
3. Na janela **Monitoring Agent for Microsoft Office 365**, conclua as seguintes etapas:
   a) Na guia **Detalhes de assinatura do Office365**, insira o nome do usuário e a senha do administrador global do Office 365 e clique em **Avançar**.
   b) Na guia **Transação sintética**, insira a lista de endereços de e-mail que são delimitados por ponto e vírgula no campo **Endereço de e-mail de alcance**.
   c) Para ativar a coleta de dados de métricas do Skype QoS, selecione a caixa de seleção **Skype QoS** e clique em **Avançar**.
   d) Na guia **Monitoramento de uso da caixa de correio e do OneDrive**, selecione a duração para o intervalo de coleta em horas da lista **Intervalo de coleta** e clique em **Avançar**.
4. Na janela **Monitoring Agent for Microsoft Office 365**, clique em **Sim**.

O que Fazer Depois

- Configure os utilitários de transação sintética do Skype para monitorar as transações sintéticas do Skype QoS. Para obter informações adicionais sobre como monitorar o Skype QoS, consulte "Monitorando o Skype QoS" na página 534.
- Mude a conta do usuário do usuário local para o usuário do domínio. Para obter detalhes, consulte "Mudando a conta do usuário" na página 534.
- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.
- Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Configurando o agente usando o arquivo silencioso de resposta

Quando instalar o Microsoft Office 365 agent, o agente deve ser configurado e iniciado manualmente depois de fornecer as definições de configuração. Use o arquivo de resposta silencioso para definir as configurações customizadas.

Antes de Iniciar

Edite o arquivo de resposta para modificar as seguintes definições de configuração padrão:

KMO_USER_NAME
O nome do usuário do administrador global do Office 365.

KMO_PASSWORD
A senha do administrador global do Office 365.

KMO_MAIL_ADDRESSES1
Uma lista de endereços de e-mail a serem direcionados para verificar o alcance da caixa de correio. A lista de endereços de e-mail deve ser delimitada usando pontos e vírgulas.

KMO_SKYPE
Esse parâmetro é usado para ativar a coleta de transações sintéticas do Skype QoS.

KMO_DATA_COLLECTION_DURATION
A duração (em horas) para a qual o agente espera antes de buscar dados de uso na caixa de correio e no OneDrive.

O arquivo de resposta está disponível no seguinte local:
`<CANDLEHOME>\samples`

Sobre Esta Tarefa

É possível configurar o agente quando o agente está em execução ou interrompido. O agente permanece no mesmo estado após a configuração. Por exemplo, se o agente está em execução, ele permanece no estado em execução após a configuração.

Procedimento

Para configurar o Microsoft Office 365 agent, execute as seguintes etapas:

1. No prompt de comandos, mude o caminho para o diretório que contém o arquivo `microsoft_office365-agent.bat`.
2. Insira o seguinte comando: `microsoft_office365-agent.bat` *absolute path to the response file*.

   O arquivo de resposta contém os seguintes parâmetros:
3. Se o agente estiver no estado pausado, inicie o agente.

O que Fazer Depois

- Configure os utilitários de transação sintética do Skype para monitorar as transações sintéticas do Skype QoS. Para obter informações adicionais sobre como monitorar o Skype QoS, consulte "Monitorando o Skype QoS" na página 534.
- Mude a conta do usuário do usuário local para o usuário do domínio. Para obter detalhes, consulte "Mudando a conta do usuário" na página 534.
- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.
- Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Mudando a conta do usuário

Depois de configurar o Microsoft Office 365 agent, mude a conta do usuário do usuário local para o usuário do domínio.

Sobre Esta Tarefa

Por padrão, o Microsoft Office 365 agent é executado sob a conta de usuário local.

Procedimento

1. Execute o comando a seguir para verificar qual ID de usuário está sendo usado para iniciar o agente:

   `install_dir\InstallITM\KinCinfo.exe -r`
2. Se o agente de monitoramento foi iniciado com um ID do usuário que não pertence ao grupo Administradores, pare o agente.
3. Abra a janela **Gerenciar Serviços de Monitoramento**.
4. Na janela **Gerenciar serviços de monitoramento**, clique com o botão direito na instância de agente e clique em **Mudar inicialização**.
5. Especifique o ID do usuário completo como <Domain\User ID> e, em seguida, especifique a senha.
6. Inicie o Microsoft Office 365 agent.

Monitorando o Skype QoS

Para monitorar o Skype QoS, um usuário deve configurar os utilitários de transação sintética do Skype, `kmoskypecaller.exe` e `Kmoskypereceiver.exe` no cliente Windows em que o agente está instalado ou em um ambiente distribuído em que o cliente Skype for Business está configurado.

Antes de Iniciar

Para executar transações sintéticas, você deve atualizar o nome do responsável pela chamada do Skype e o nome do receptor do Skype no arquivo <CANDLEHOME>
`\tmaitm6_x64\kmoskypecallerlist.properties` no seguinte formato:
`skype caller = skype receiver`
Por exemplo, john@xyz.com = alan@xyz.com
É possível incluir vários receptores de chamada do Skype para um único responsável pela chamada do Skype no seguinte formato:

skype caller = list of skype receiver
Por exemplo, john@xyz.com = alam@xyz.com;bill@xyz.com;chuk@xyz.com

Lembre-se: Se não desejar executar transações sintéticas mas desejar monitorar o Skype QoS para usuários em tempo real, a atualização do arquivo <CANDLEHOME>\TMAITM6_x64\kmoskypecallerlist.properties não é necessária.

Sobre Esta Tarefa

Quando o Microsoft Office 365 agent estiver configurado e iniciado, os seguintes arquivos e pastas serão criados em <CANDLEHOME>\TMAITM6_x64\:

- kmoskypecaller.properties
- kmoskypecallerlist.properties
- KMOSynthTransSkype.zip
- KMOSkypeTransReceiver.zip

Além disso, o arquivo kmoskypecaller.properties é atualizado com o IP e porta do servidor que são usados para comunicação entre o agente e o utilitário kmoskypecaller.

Procedimento

Para configurar o responsável pela chamada do Skype e os receptores do Skype e iniciar transações sintéticas, como mensagem instantânea, chamadas de áudio e vídeo e sessões de compartilhamento de aplicativo, conclua as seguintes etapas:

1. Inicie o agente Office 365.
2. Copie o arquivo KMOSynthTransSkype.zip do cliente do agente para o cliente Windows de onde a chamada do Skype deve ser iniciada.
3. Extraia o arquivo KMOSynthTransSkype.zip.
4. Copie o arquivo kmoskypecaller.properties do cliente do agente para a pasta extraída KMOSynthTransSkype no cliente Windows de onde a chamada do Skype deve ser iniciada.
5. Copie o arquivo KMOSkypeTransReceiver.zip do cliente do agente em todos os clientes Windows onde as chamadas do Skype devem ser recebidas.
6. Extraia o arquivo KMOSkypeTransReceiver.zip em todos os clientes Windows em que as chamadas do Skype devem ser recebidas, e execute KMOSkypeTransReceiver.exe para começar a receber mensagens.
7. Para iniciar as transações sintéticas, execute o arquivo KMOSynthTransSkype.exe, que está disponível na pasta extraída KMOSynthTransSkype no cliente Windows. O agente Office 365 começaria a receber os dados de monitoramento do skype do cliente responsável pela chamada.

Resultados

O agente inicia o monitoramento do Skype QoS.

Configurando as variáveis de ambiente local

É possível configurar as variáveis de ambiente local para alterar o comportamento do Microsoft Office 365 agent.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **Agentes de Monitoramento IBM** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, no menu **Ações**, clique em **Avançado > Editar Arquivo ENV**.
3. No arquivo da variável de ambiente, insira os valores para as variáveis de ambiente.

Para obter informações sobre as variáveis de ambiente que podem ser configuradas, consulte "variáveis de ambiente local" na página 536.

variáveis de ambiente local
É possível alterar o comportamento do Microsoft Office 365 agent, configurando as variáveis de ambiente local.

Variáveis para definir o método de coleta de dados para o agente

Para configurar o método para coleta de dados do agente, use as seguintes variáveis de ambiente:

- **CDP_DP_INITIAL_COLLECTION_DELAY**: Use esta variável para configurar o intervalo de tempo (em segundos) após o qual o conjunto de encadeamentos começa sua coleta de dados.
- **KMO_MAILBOX_REACHABILITY_INTERVAL**: Use esta variável para configurar o intervalo de coleta de dados (em minutos) para o grupo de atributos de alcance da caixa de correio.
- **KMO_SKYPE_REPORT_INTERVAL**: Use esta variável para configurar o intervalo de coleta de dados (em horas) para o recurso de estatísticas de uso do Skype for Business.
- **KMO_SERVICE_API_INTERVAL**: Use esta variável para configurar o intervalo de coleta de dados (em minutos) para o recurso de funcionamento de serviço do Office 365.
- **KMO_NETWORK_CONNECTION_INTERVAL**: Use esta variável para configurar o intervalo de coleta de dados (em minutos) para o recurso de conectividade da Internet.
- **KMO_NETWORK_PERFORMANCE_INTERVAL**: Use esta variável para configurar o intervalo de coleta de dados (em minutos) para o recurso de desempenho de rede de serviços do Office 365.
- **KMO_SITE_CONNECTION_INTERVAL**: Use esta variável para configurar o intervalo de coleta de dados (em minutos) para o recurso de conectividade do Office 365.
- **KMO_SPSITE_COLLECTION_INTERVAL**: Use esta variável para configurar o intervalo de coleta de dados (em minutos) para o recurso de detalhes dos Sites do SharePoint.
- **KMO_UASGE_STATS_INTERVAL**: Use esta variável para configurar o intervalo de coleta de dados (em horas) para o recurso de estatísticas de uso e do usuário de Serviços do Office 365.
- **KMO_TENANT_INTERVAL**: Use esta variável para configurar o intervalo de coleta de dados (em minutos) para o recurso de detalhes do locatário do Office 365.
- **KMO_ONEDRIVE_CONNECTIVITY_INTERVAL**: Use esta variável para configurar o intervalo de coleta de dados (em minutos) para o recurso de conectividade OneDrive do Office 365.
- **KMO_TENANT_DOMAIN**: Use esta variável para configurar o nome de domínio do locatário.

Configurando o Microsoft SharePoint Server de monitoramento

Ao instalar o Monitoring Agent para Microsoft SharePoint Server, o agente é configurado automaticamente e iniciado com as definições de configuração padrão. Use o arquivo de resposta silencioso para modificar as definições de configuração padrão.

Antes de Iniciar

Assegure-se de concluir as tarefas a seguir:

- Certifique-se de que o usuário que se conecta ao ambiente ou aplicativo do Microsoft SharePoint Server tenha privilégios de administrador. Use um usuário existente com privilégios de administrador, ou crie um novo usuário. Designe privilégios de administrador ao novo usuário, incluindo o novo usuário no grupo Administradores.

  Lembre-se: Para configurar o Microsoft SharePoint Server agent, é possível usar um usuário local ou de domínio, desde que o usuário tenha privilégios de administrador.
- Edite o arquivo de resposta e modifique os parâmetros de configuração padrão.

  O arquivo de resposta contém os seguintes parâmetros:

KQP_DB_User
O ID do usuário do banco de dados.

KQP_DB_Password
A senha do banco de dados.

Revise os pré-requisitos de hardware e de software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Microsoft SharePoint Server agent.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Versão do Agente. Para acessar a documentação para liberações anteriores do agente, consulte a tabela a seguir:

Tabela 180. Documentação e versões do agente

Versão do Microsoft SharePoint Server agent	Documentação
06.31.09.00, 06.31.10.00	IBM Cloud Application Performance Management
06.31.09.00	IBM Performance Management 8.1.3 **Nota:** O link abre um tópico do Knowledge Center no local.
06.31.07.00	IBM Performance Management 8.1.2 **Nota:** O link abre um tópico do Knowledge Center no local.

Procedimento

Para configurar o Microsoft SharePoint Server agent, execute as seguintes etapas:

1. Abra o prompt de comandos.
2. Mude o caminho até o diretório que contém o arquivo `ms_sharepoint_server-agent.bat`.
3. Insira o comando a seguir: **`ms_sharepoint_server-agent.bat config`** *caminho absoluto para o arquivo de resposta*
4. Se o agente estiver no estado pausado, inicie o agente.

O que Fazer Depois
Depois de configurar o agente, você pode alterar a conta do usuário do usuário local para o usuário do domínio. Para saber as etapas para mudar a conta do usuário, consulte "Mudando a conta do usuário" na página 537.

Mudando a conta do usuário

Depois de configurar o Microsoft SharePoint Server agent, é possível mudar a conta do usuário do usuário local para o usuário do domínio.

Sobre Esta Tarefa
Com o usuário do domínio, o agente pode monitorar todos os componentes do Microsoft SharePoint Server agent.

Procedimento

Para mudar a conta do usuário, conclua as etapas a seguir:

1. Execute o seguinte comando para verificar qual ID do usuário está sendo usado para iniciar o agente.
   `install_dir\InstallITM\KinCinfo.exe -r`

2. Se o agente de monitoramento foi iniciado com um ID do usuário que não pertence ao grupo Administradores, pare o agente.
3. Abra a janela **Gerenciar Serviços de Monitoramento**.
4. Clique com o botão direito na instância de agente e clique em **Alterar Inicialização**.
5. Especifique o ID do usuário completo como <Domain\Userid> e, em seguida, especifique a senha.
6. Inicie o agente de monitoramento.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Executando o Monitoring Agent para Microsoft SharePoint Server por um usuário não administrador

Políticas de segurança local estão disponíveis para executar um Monitoring Agent para Microsoft SharePoint Server por um usuário não administrador.

Sobre Esta Tarefa

Uma combinação das duas seguintes políticas de segurança local funciona para executar o Microsoft SharePoint Server agent por um usuário não administrador.

1. Programas de depuração.
2. Efetuar logon como serviço.

Siga o procedimento que é fornecido para avaliar as permissões de Segurança local para um usuário não administrador.

Procedimento

1. Acesse o TEMA e mude a inicialização do Microsoft SharePoint Server agent com um usuário não administrador.
2. Inclua um usuário não administrador no diretório HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office Server da chave de registro e conceda a ele acesso de leitura.
3. Inclua um usuário não administrador na chave de registro HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions e conceda a ele acesso de leitura.
4. Inclua manualmente um usuário não administrador na chave de registro HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server Extensions\16.0\Secure\ e conceda a ele acesso de leitura.
5. Inclua um usuário não administrador no diretório HKEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring da chave de registro e conceda a ele permissões completas.
6. Inclua um usuário não administrador no diretório HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib da Chave de registro e conceda a ele acesso de leitura.
7. Inclua um usuário não administrador na pasta de instalação do SharePoint Agent (pasta Candle, por exemplo, C:\IBM\APM) e conceda a ele permissões completas.
8. Execute o comando **secpol.msc** em **startmenu** para abrir a **Política de segurança local**.
9. Inclua um usuário não administrador na Política de segurança local. Consulte "Permissões de Política de segurança local" na página 539
10. Inclua um usuário não administrador no grupo de usuários de Login do SQL Server. O usuário deve ter permissões de função sysadmin do SQL Server no SQL Server.
11. Reinicie o Microsoft SharePoint Server agent.
12. Verifique o status do Microsoft SharePoint Server agent e verifique os dados no portal do APM.
13. Os seguintes grupos de atributos mostram dados para usuários que são membros do grupo de Administradores.

a) Disponibilidade

b) Serviço da Web

Permissões de Política de segurança local

As políticas de segurança local estão disponíveis para executar um Microsoft SharePoint Server agent por um usuário não administrador. Essas políticas ajudam a iniciar ou parar, configurar ou executar a verificação de dados do agente. As duas seguintes políticas de segurança local funcionam para executar o Microsoft SharePoint Server agent por um usuário não administrador.

Concedendo a permissão Efetuar logon como serviço
É possível conceder a permissão Efetuar logon como serviço.

Sobre Esta Tarefa
Para conceder a permissão Efetuar logon como serviço, siga o procedimento em Microsoft SharePoint Server agent, conforme descrito aqui.

Procedimento

1. Clique em **Iniciar** > **Ferramentas administrativas** > **Política de segurança local**. A janela **Configurações de Segurança Local** é aberta.
2. Na área de janela de navegação, expanda **Política local** e clique em **Designação de direitos do usuário**. A lista de direitos de usuário é aberta.
3. Dê um clique duplo na política **Efetuar logon como serviço**. A janela **Efetuar logon como propriedades de serviço** é aberta.
4. Clique em **Incluir Usuário ou Grupo**. A janela **Selecionar Usuários ou Grupos** é exibida.
5. No campo **Inserir os nomes de objetos a serem selecionados**, insira o nome da conta do usuário a quem você deseja designar permissões e, em seguida, clique em **OK**.
6. Clique em **OK**.

Concedendo a permissão Programas de depuração
É possível conceder a permissão Depurar programas.

Sobre Esta Tarefa
Para conceder a permissão Depurar programas, siga o procedimento em Microsoft SharePoint Server agent, conforme descrito aqui:

Procedimento

1. Clique em **Iniciar** > **Ferramentas administrativas** > **Política de segurança local**. A janela **Configurações de Segurança Local** é aberta.
2. Expanda **Política local** e clique em **Designação de direitos do usuário**. A lista de direitos de usuário é aberta.
3. Dê um clique duplo na política **Programas de depuração**. A janela **Propriedades dos programas de depuração** é aberta.
4. Clique em **Incluir Usuário ou Grupo**. A janela **Selecionar Usuários ou Grupos** é exibida.
5. No campo Inserir os nomes de objetos a serem selecionados, insira o nome da conta do usuário para quem você deseja designar permissões e, em seguida, clique em **OK**.
6. Clique em **OK**.

Configurando o monitoramento do Microsoft SQL Server

Configure o Monitoring Agent for Microsoft SQL Server para que o agente possa coletar dados do aplicativo que está sendo monitorado.

Antes de Iniciar

Revise os pré-requisitos de hardware e software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Microsoft SQL Server agent.

É possível instalar e configurar o Microsoft SQL Server agent localmente usando a interface de prompt de comandos. Assegure-se de que o agente esteja instalado no servidor que está sendo monitorado.

Sobre Esta Tarefa

As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte “Histórico de Mudanças” na página 50.

O Microsoft SQL Server agent é um agente de múltiplas instâncias; você deve configurar e iniciar cada instância do agente manualmente.

- Para configurar o agente, conclua as tarefas a seguir:
  - Crie um usuário e conceda as permissões necessárias
  - Selecione os bancos de dados para monitoramento
  - Configure as variáveis de ambiente locais
- Para executar o agente em um ambiente em cluster, conclua as etapas descritas no tópico "Executando o agente em um ambiente em cluster".

Criando um usuário e concedendo permissões

No Microsoft SQL Server, deve-se criar um usuário sob o qual o agente é executado e conceder permissões ao usuário para monitorar o Microsoft SQL Server. O processo de conceder permissões é o mesmo para o Microsoft SQL Server 2005 ou mais recente.

Antes de Iniciar

Instale o Microsoft SQL Server agent. Para criar um usuário e conceder permissões ao usuário, deve-se ser um administrador de banco de dados com a função de autorização sysdamin.

Sobre Esta Tarefa

Use o procedimento a seguir para determinar se um usuário do SQL Server existente possui permissões suficientes para monitorar o Microsoft SQL Server:

- Windows “Verificando as permissões de um usuário do SQL Server existente” na página 540

Use um dos procedimentos a seguir para criar um usuário:

- Windows “Criando um ID do usuário do SQL Server com autenticação do Windows” na página 541
- Linux Windows “Criando um ID do usuário do SQL Server com autenticação do SQL Server” na página 542

Use o procedimento a seguir para conceder permissões:

- Windows “Concedendo permissões mínimas para coleta de dados” na página 543
- Windows “Concedendo permissão para a chave de registro Perflib para coletar dados para alguns conjuntos de dados” na página 544

Verificando as permissões de um usuário do SQL Server existente

Windows É possível executar a ferramenta de utilitário **koqVerifyPerminssions.exe** para verificar se um usuário do SQL Server existente possui permissões suficientes relacionadas aos bancos de dados do SQL Server.

Sobre Esta Tarefa
A ferramenta do utilitário **koqVerifyPerminssions.exe** retorna a mensagem PASS se o usuário tem a função **sysadmin** ou as permissões mínimas necessárias. O resultado da verificação detalhada é registrado em koqVerifyPermissions_log.

A seguir está uma lista das permissões mínimas:

- As permissões para o servidor devem incluir **Visualizar o estado do servidor**, **Visualizar qualquer banco de dados** e **Visualizar qualquer definição**.

  Essas permissões de nível do servidor são obrigatórias.
- Para todos os bancos de dados do sistema e para os bancos de dados definidos pelo usuário para monitoramento, a associação de função do banco de dados deve incluir **public** e **db_owner**.

  A permissão **db_owner** é necessária para coletar dados para os conjuntos de dados a seguir:
  - Conjunto de dados de Detalhes do servidor
  - Conjunto de dados de Detalhes do banco de dados
  - Conjunto de dados de Espelhamento de banco de dados
  - Conjunto de dados de Resumo do servidor
  - Conjunto de dados de Resumo da tarefa
- Para o banco de dados **msdb**, a associação de função do banco de dados deve incluir **db_datareader**, **SQLAgentReaderRole** e **SQLAgentUserRole**. Essas permissões são necessárias para o conjunto de dados Detalhes da tarefa.

Procedimento

1. Ative o prompt de comandos e mude para o seguinte diretório de utilitários.
   - Para agentes de 64 bits, *Agent_home* \TMAITM6_x64
   - Para agentes de 32 bits, *Agent_home* \TMAITM6

   em que *Agent_home* é o diretório de instalação do agente.
2. Execute o **koqVerifyPerminssions.exe**, fornecendo os parâmetros:

   ```
   koqVerifyPermissions.exe -S Instance_name -U Username -P
   Password
   ```

   Em que:
   - *Instance_name* é o nome da instância do SQL Server.
   - *Username* é o nome do usuário que é verificado pela ferramenta do utilitário.
   - *Password* é a senha do usuário. Esse parâmetro será necessário se *username* for fornecido.

   Nota: Se *username* e *password* não forem fornecidos, o usuário padrão que está com logon efetuado no sistema será usado. Exemplo: NT AUTHORITY\SYSTEM.

Resultados
O resultado de verificação detalhado está disponível no koqVerifyPermissions_log no diretório a seguir:

- Para agentes de 64 bits, *Agent_home* \TMAITM6_x64\logs
- Para agentes de 32 bits, *Agent_home* \TMAITM6\logs

Em que *Agent_home* é o diretório de instalação do agente.

Criando um ID do usuário do SQL Server com autenticação do Windows
Windows Crie um novo usuário com a autenticação do Windows e designe as funções e permissões necessárias para o usuário.

Procedimento

Para criar um usuário, execute as seguintes etapas:

1. No **SQL Server Management Studio**, abra o **Object Explorer**.
2. Clique em ***Server_instance_name*** > **Segurança** > **Logins**.
3. Clique com o botão direito em **Logins** e selecione **Novo login**.
4. Na página **Geral**, no campo **Nome de login**, digite o nome de um usuário do Windows.
5. Selecione **Autenticação do Windows**.
6. Dependendo da função e permissões que você deseja designar a esse usuário, conclua uma das tarefas a seguir:
   - Na página Funções do servidor, designe a função *sysadmin* ao novo ID de login.
   - Se você não deseja designar a função *sysadmin* ao usuário, conceda permissões mínimas ao usuário concluindo as etapas que estão mencionadas em "Concedendo permissões mínimas para coleta de dados" na página 543.

   Importante: Por padrão, a função *pública* é designada ao novo ID de login.
7. Clique em **OK**.

Resultados

Um usuário é criado com a função padrão *pública* e as permissões que você designou e é exibido na lista de **Logins**.

Criando um ID do usuário do SQL Server com autenticação do SQL Server

Linux Windows Crie um novo usuário com a autenticação do SQL Server e designe as funções e permissões necessárias para o usuário.

Procedimento

Para criar um usuário, execute as seguintes etapas:

1. No **SQL Server Management Studio**, abra o **Object Explorer**.
2. Clique em ***Server_instance_name*** > **Segurança** > **Logins**.
3. Clique com o botão direito em **Logins** e selecione **Novo login**.
4. Na página **Geral** , no campo **Nome de login**, digite o nome para um novo usuário.
5. Selecione **Autenticação do SQL Server**.
6. No campo **Senha**, digite uma senha para o usuário.
7. No campo **Confirmar senha**, digite novamente a senha inserida no campo **Senha**.
8. Dependendo da função e permissões que você deseja designar a esse usuário, conclua uma das tarefas a seguir:
   - Na página Funções do servidor, designe a função *sysadmin* ao novo ID de login.
   - Se você não deseja designar a função *sysadmin* ao usuário, conceda permissões mínimas ao usuário concluindo as etapas que estão mencionadas em "Concedendo permissões mínimas para coleta de dados" na página 543.

   Importante: Por padrão, a função *pública* é designada ao novo ID de login.
9. Clique em **OK**.

Resultados

Um usuário é criado com a função padrão *pública* e as permissões que você designou e é exibido na lista de **Logins**.

Concedendo permissões mínimas para coleta de dados

Windows Além da função **public** padrão, é possível designar a função **sysadmin** a um usuário ou conceder as permissões mínimas a um usuário para que o agente possa coletar dados para conjuntos de dados.

Sobre Esta Tarefa

É possível conceder as permissões por meio da interface com o usuário ou da ferramenta do utilitário **permissions.cmd**.

Procedimento

- Para conceder as permissões mínimas para o usuário por meio da interface com o usuário, conclua estas etapas:
  a) Abra a página **Funções do servidor** e verifique se a caixa de seleção **public** está marcada.
  b) Abra a página **Mapeamento de usuário** e, em seguida, marque as caixas de seleção a seguir de todos os bancos de dados do sistema e os bancos de dados definidos pelo usuário que você deseja monitorar:
     – **Public**
     – **db_owner**

     Para o banco de dados **msdb**, marque as seguintes caixas de seleção adicionais:
     – **db_datareader**
     – **SQLAgentReaderRole**
     – **SQLAgentUserRole**
  c) Abra a página **Securables** e, em seguida, marque as caixas de seleção a seguir para a instância do servidor que você está monitorando:
     – banco de dados de visualização
     – definição de visualização
     – estado de servidor de visualização
- Para conceder as permissões mínimas para o usuário usando a ferramenta de utilitário **permissions.cmd**, conclua o seguinte:
  a) Ative o Windows Explorer e navegue para o diretório da ferramenta do utilitário *Agent_grant_perm_dir*:
     – Para o agente de 64 bits, o *Agent_grant_perm_dir* é *Agent_home*\TMAITM6_x64\scripts\KOQ\GrantPermission.
     – Para o agente de 32 bits, o *Agent_grant_perm_dir* é *Agent_home*\TMAITM6\scripts\KOQ\GrantPermission.
     – *Agent_home* é o diretório de instalação do agente.

     Atenção: A ferramenta de utilitário **permissions.cmd** concede **db_owner** em todos os bancos de dados por padrão. Para excluir determinados bancos de dados, deve-se incluir nomes de banco de dados no arquivo *Agent_grant_perm_dir*\exclude_database.txt. Os nomes do banco de dados devem ser separados pelo alias de símbolo **@**.

     Dica: Por exemplo, se você deseja excluir os bancos de dados **MyDatabase1** e **MyDatabase2**, inclua a entrada a seguir no arquivo exclude_database.txt:

     ```
     MyDatabase1 @MyDatabase2
     ```
  b) Dê um clique duplo em **permissions.cmd** para ativar a ferramenta de utilitário.
  c) Insira os valores de parâmetro desejados quando solicitado:

Tabela 181. Parâmetros	
Parâmetros	**Descrição**
Nome do SQL Server ou nome da instância do SQL Server	Insira o nome do SQL Server ou o nome da instância do SQL Server de destino que deseja para conceder permissões para o usuário.
O nome de logon do usuário do SQL Server existente	Insira o nome do usuário cujas permissões serão alteradas.
Opções de permissão: **1** Permissão de concessão de **db_owner** **2** Conceder permissões **db_datareader**, **SQLAgentReaderRole** e **SQLAgentUserRole** **3** Conceda todas as permissões necessárias	Insira **1** ou **2** ou **3** de acordo com seu requisito.
O usuário para conceder permissões: **1** O usuário que está atualmente com logon efetuado no sistema **2** Outro usuário	Insira **1** ou **2** . Se **2** for selecionado, insira o nome do usuário de destino quando solicitado. **Nota:** Os usuários devem ter acesso para conceder permissões a outros usuários.

O que Fazer Depois
Configure o agente.

Concedendo permissão para a chave de registro Perflib para coletar dados para alguns conjuntos de dados

Windows Para coletar dados para alguns conjuntos de dados, é preciso conceder aos usuários o acesso de leitura à chave de registro Perflib.

Sobre Esta Tarefa

É preciso conceder esta permissão ao usuário do Windows com a qual os serviços do agente são configurados. Existem muitos conjuntos de dados que são afetados na ausência de permissões Perflib, como o Detalhe do Banco de dados MS SQL, MS SQL Memory Manager, Resumo do tipo de recurso de bloqueio do MS SQL, Resumo de tarefa do MS SQL, Resumo de transações do MS SQL Server, Resumo do MS SQL Server, etc.

Procedimento

Para conceder permissão para a chave de registro Perflib, conclua estas etapas:

1. Para abrir o Editor de Registro, clique em **Iniciar** > **Executar** > **Regedit.exe** e pressione **Enter**.
2. Acesse a chave de registro `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT \CurrentVersion\Perflib`.
3. Clique com o botão direito na chave **Perflib** e clique em **Permissões**.
4. Clique em **Incluir**, insira o nome do usuário do Windows com o qual o agente está instalado e configurado e, em seguida, clique em **OK**.
5. Clique no usuário que foi incluído.
6. Permita acesso de leitura ao usuário selecionando a caixa de seleção.
7. Clique em **Aplicar** e, em seguida, clique em **OK**.

variáveis de ambiente local

É possível alterar o comportamento do Microsoft SQL Server agent, configurando as variáveis de ambiente local.

Variáveis para verificar a disponibilidade do serviço do SQL Server

Para verificar a disponibilidade do serviço do SQL Server, use as variáveis de ambiente a seguir:

- **COLL_MSSQL_RETRY_INTERVAL:** Esta variável fornece o intervalo de novas tentativas (em minutos) para verificar o status de serviço do SQL Server. Se o valor for menor ou igual a zero, então, a variável assume o valor padrão de 1 minuto.
- **COLL_MSSQL_RETRY_CNT**: esta variável fornece o número de novas tentativas que o agente SQL server faz para verificar se o serviço do SQL server está iniciado ou não. Se o serviço do SQL Server não for iniciado após o número de novas tentativas especificadas nessa variável, o coletor irá parar de funcionar. Se o valor da variável for menor ou igual a zero, a variável usará o valor padrão de 3.

Variáveis para monitorar o arquivo do log de erros do SQL server

Para monitorar o conjunto de dados Detalhes do Evento de Erro do MS SQL, use as variáveis de ambiente a seguir:

- **COLL_ERRORLOG_STARTUP_MAX_TIME**: esta variável fornece o intervalo de tempo (T) para coleta de erros antes do início do agente. O valor padrão é `0` minutos. Esta variável pode assumir os valores a seguir:

  T = 0
  O agente inicia o monitoramento do arquivo do log de erros a partir do momento em que o agente é iniciado ou é reiniciado. O agente não lê os erros que foram registrados no arquivo do log de erros antes do agente ter sido iniciado.

  T = 1
  O agente monitora o arquivo do log de erros de acordo com seguintes valores que estão configurados para a variável **COLL_ERRORLOG_STARTUP_MAX_EVENT_ROW**, que é representado por R:

  - Se R < 0, o agente inicia o monitoramento do arquivo do log de erros a partir do momento em que o agente é iniciado ou é reiniciado.
  - Se R = 1, o agente monitora todos os erros que são registrados no arquivo do log de erros.
  - Se R > 1 e o agente for instalado pela primeira vez, o agente monitora o arquivo do log de erros até que R erros sejam monitorados. Se R > 1 e o agente for reiniciado, o agente monitora todos os R erros perdidos anteriormente.

  T > 1
  O agente monitora todos os erros anteriores que foram registrados até T minutos a partir do momento em que o agente for iniciado ou reiniciado. O monitoramento do agente também depende dos valores a seguir que foram configurados para a variável **COLL_ERRORLOG_STARTUP_MAX_EVENT_ROW**:

  - Se R ≤ 0, o agente inicia o monitoramento do arquivo de log de erros a partir do momento em que o agente é iniciado ou o agente é reiniciado.
  - Se R = 1, o agente monitora o arquivo do log de erros para todos os erros que são registrados até T minutos.
  - Se R > 1, o agente não monitorará mais de R erros que são registrados nos últimos T minutos.
- **COLL_ERRORLOG_STARTUP_MAX_EVENT_ROW**: esta variável fornece o número máximo de erros que deve ser processado quando o agente é iniciado. O valor padrão é `0`. É possível designar os valores a seguir para esta variável:

R = 0
O agente inicia o monitoramento do arquivo do log de erros a partir do momento em que o agente é iniciado ou reiniciado. O agente não lê erros que foram criados no arquivo do log de erros antes do agente ter sido iniciado.

R = 1
O agente monitora os erros que foram registrados nos últimos T minutos a partir do momento em que o agente for iniciado ou reiniciado.

R > 1
O agente monitora R erros registrados nos últimos T minutos.

- **COLL_ERRORLOG_MAX_EVENT_ROW**: Esta variável fornece o número de linhas de erro. O valor padrão é 50. É possível designar os valores a seguir para esta variável:

  X = 0
  O agente não exibe os logs de erros.

  X > 0
  O agente exibe as X linhas de erros.

- **COLL_ERRORLOG_RECYCLE_WAIT**: essa variável fornece o intervalo de tempo (em segundos) durante o qual o Microsoft SQL Server agent espera antes de coletar dados do grupo de atributos Detalhe do Evento de Erro do MS SQL quando a situação nesse grupo de atributos for acionada. É possível designar um valor a essa variável no intervalo de 1 a 30. Se o valor dessa variável for menor que zero, a variável usará o valor padrão de zero (segundos). Se o valor dessa variável for maior que 30, a variável usará o valor padrão de 30 (segundos).

Variável para configuração do intervalo de tempo limite de consulta

Para configurar o intervalo de tempo limite de consulta para o agente SQL Server, use as seguintes variáveis de ambiente:

- **QUERY_TIMEOUT**: Esta variável de ambiente define a quantidade máxima de tempo (em segundos) que o agente SQL Server espera para receber uma resposta para uma consulta que é enviada ao SQL Server. O valor para esta variável deve ser menor do que 45 segundos. Entretanto, se você configurar o valor para esta variável como 0 segundos, o agente do SQL Server aguardará indefinidamente para receber uma resposta do SQL Server. Se o agente do SQL Server acessa muitos bancos de dados bloqueados, o valor designado para essa variável deve estar no intervalo de 10 - 20 segundos. Se a consulta não for processada dentro do intervalo de tempo limite configurado, o agente do SQL server ignora a consulta que atingiu o tempo limite e move para a próxima consulta na fila. O agente não exibe dados para a consulta que atingiu o tempo limite.
- **QUERY_THREAD_TIMEOUT**: Esta variável de ambiente define a quantidade máxima de tempo (em segundos) que o agente SQL Server espera para receber uma resposta para uma consulta que é enviada ao SQL Server. Esta variável de ambiente é aplicável a alguns grupos de atributos que usam a coleta encadeada. Por exemplo, KOQDBD, KOQTBLD, KOQDEVD, etc. O valor dessa variável não tem nenhum limite diferente da variável QUERY_TIMEOUT. Caso contrário, funcionará de forma semelhante à variável QUERY_TIMEOUT.

Variável para visualização de informações sobre tarefas ativadas

Para visualizar as informações sobre as tarefas ativadas no conjunto de dados de Detalhe de tarefa do MS SQL, use a variável de ambiente **COLL_JOB_DISABLED**. Se você configurar o valor dessa variável como 1, o Microsoft SQL Server agent não exibe informações sobre tarefas desativadas. Se você não especificar essa variável, é possível visualizar informações sobre tarefas ativadas e desativadas.

Variável para limitar as linhas no conjunto de dados Detalhes do Grupo de Arquivos do MS SQL

Para limitar o número de linhas que o serviço do coletor busca para o conjunto de dados Detalhes do Grupo de Arquivos do MS SQL, use a variável de ambiente **COLL_KOQFGRPD_MAX_ROW**. Essa variável de ambiente define o número máximo de linhas que um serviço do coletor busca para o conjunto de dados Detalhes do Grupo de Arquivos. Se você não especificar um valor para essa variável, o serviço do coletor

buscará 10.000 linhas para o conjunto de dados Detalhes do Grupo de Arquivos. Use esta variável de ambiente para modificar o limite padrão do máximo de linhas no arquivo `koqcoll.ctl`. Conclua as etapas a seguir para modificar o limite padrão:

1. Especifique o número máximo de linhas para KOQFGRPD no arquivo `koqcoll.ctl`.
2. Inclua a variável de ambiente **COLL_KOQFGRPD_MAX_ROW** e assegure-se de que o valor para essa variável seja igual ao valor que você especificou no arquivo `koqcoll.ctl`.

Se o valor no arquivo `koqcoll.ctl` for menor que o valor especificado na variável de ambiente **COLL_KOQFGRPD_MAX_ROW**, o valor no arquivo `koqcoll.ctl` será tratado como o valor para o número máximo de linhas.

Se o valor no arquivo `koqcoll.ctl` for maior que o valor especificado na variável de ambiente **COLL_KOQFGRPD_MAX_ROW**, o valor na variável de ambiente **COLL_KOQFGRPD_MAX_ROW** é tratado como o valor para o número máximo de linhas.

Variáveis para aprimorar a coleção para o conjunto de dados Detalhes do Grupo de Arquivos do MS SQL

Use a variável **COLL_DBD_FRENAME_RETRY_CNT** para especificar o número de tentativas que podem ser feitas para mover o arquivo `%COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID%_ %COLL_SERVERID%__FGRP_TEMP` para o arquivo `%COLL_HOME%_tmp_%COLL_VERSION%_ %COLL_SERVERID%_%COLL_SERVERID%__FGRP_PREV`.

Se você não especificar um valor para essa variável, o Microsoft SQL Server agent fará três tentativas de mover o arquivo.

Variável para limitar as linhas no conjunto de dados Detalhes do Dispositivo do MS SQL

Para limitar o número de linhas que o serviço do coletor busca para o conjunto de dados Detalhes do Dispositivo do MS SQL, use a variável de ambiente **COLL_KOQDEVD_MAX_ROW**. Essa variável de ambiente define o número máximo de linhas que um serviço do coletor busca para o conjunto de dados Detalhes do Dispositivo. Se você não especificar um valor para essa variável, o serviço do coletor buscará 10.000 linhas para o conjunto de dados Detalhes do Dispositivo. Use esta variável de ambiente para modificar o limite padrão do máximo de linhas no arquivo `koqcoll.ctl`. Conclua as etapas a seguir para modificar o limite padrão:

1. Especifique o número máximo de linhas para KOQDEVD no arquivo `koqcoll.ctl`.
2. Inclua a variável de ambiente **COLL_KOQDEVD_MAX_ROW** e assegure-se de que o valor para essa variável seja igual ao valor que você especificou no arquivo `koqcoll.ctl`.

Se o valor no arquivo `koqcoll.ctl` for menor que o valor especificado na variável de ambiente **COLL_KOQDEVD_MAX_ROW**, o valor no arquivo `koqcoll.ctl` será tratado como o valor para o número máximo de linhas.

Se o valor no arquivo `koqcoll.ctl` for maior que o valor especificado na variável de ambiente **COLL_KOQDEVD_MAX_ROW**, o valor na variável de ambiente **COLL_KOQDEVD_MAX_ROW** é tratado como o valor para o número máximo de linhas.

Variáveis para aprimorar a coleção para o conjunto de dados Detalhes do Dispositivo do MS SQL

Para aprimorar a coleção do conjunto de dados Detalhes do Dispositivo do MS SQL, use as variáveis de ambiente a seguir:

- **COLL_KOQDEVD_INTERVAL**: Esta variável de ambiente permite especificar um intervalo de tempo (em minutos) entre duas coleções consecutivas do conjunto de dados Detalhes do Dispositivo do MS SQL.

  Nota: Por padrão, a coleta de dados para o conjunto de dados Detalhes do Dispositivo é baseada em demanda. Use a variável **COLL_KOQDEVD_INTERVAL** para iniciar uma coleção baseada em encadeamento para o conjunto de dados Detalhes do Dispositivo e para configurar o intervalo de tempo entre duas coleções encadeadas.

- **COLL_DBD_FRENAME_RETRY_CNT**: Use esta variável de ambiente para especificar o número de tentativas que podem ser feitas para mover o arquivo %COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID%_%COLL_SERVERID%__DEVD_TEMP para o arquivo %COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID%_%COLL_SERVERID%__DEVD_PREV.

Se você não especificar um valor para essa variável, o Microsoft SQL Server agent fará uma tentativa de mover o arquivo.

Variáveis para aprimorar a coleção para o conjunto de dados Detalhes do Banco de Dados do MS SQL

Para aprimorar a coleção do conjunto de dados Detalhes do Banco de Dados do MS SQL, use as variáveis de ambiente a seguir:

- **COLL_KOQDBD_INTERVAL**: Use esta variável de ambiente para especificar um intervalo de tempo (em minutos) entre duas coletas consecutivas baseadas em encadeamento do conjunto de Dados Detalhe do Banco de Dados MS SQL. Se você não especificar um valor para esta variável ou se o intervalo de tempo especificado for menor que 3 minutos, o Microsoft SQL Server agent será padronizado para um intervalo de 3 minutos. Nesse caso, a coleta está demorando mais ou os dados são vistos frequentemente como NOT_COLLECTED, é possível verificar o tempo de coleta consultando o log `Database Detail Collection completed in %d seconds` e configurar o valor da variável para um valor que seja maior que o tempo de coleta especificado no log.
- **COLL_DBD_FRENAME_RETRY_CNT**: Use esta variável de ambiente para especificar o número de tentativas que podem ser feitas para mover o arquivo %COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID%_%COLL_SERVERID%__DBD_TEMP para o arquivo %COLL_HOME%_tmp_%COLL_VERSION%_%COLL_SERVERID%_%COLL_SERVERID%__DBD_PREV.

Se você não especificar um valor para essa variável, o Microsoft SQL Server agent fará uma tentativa de mover o arquivo.

Variáveis para aprimorar a coleção para o conjunto de dados Detalhes da Auditoria do MS SQL

Para aprimorar a coleção do conjunto de dados Detalhes da Auditoria do MS SQL, use as variáveis de ambiente a seguir:

- **COLL_AUDIT_TYPE**: Use esta variável para ativar ou desativar o monitoramento de logs específicos. O valor padrão da variável é [AL][FL][SL]. Por padrão, o agente monitora todos os três tipos de logs que incluem os logs de aplicativo, arquivos de auditoria e os logs de segurança. O valor da variável inclui um código de dois caracteres para cada tipo de log:
  - [AL] para logs do aplicativo
  - [FL] para arquivos de auditoria
  - [SL] para logs de segurança

  É possível alterar o valor da variável para desativar o monitoramento de um tipo de log específico. Por exemplo, se especificar o valor da variável como [AL][SL], os arquivos de auditoria não serão monitorados. Se nenhum valor for especificado para a variável, os detalhes de auditoria não serão monitorados.
- **COLL_AUDIT_DURATION**: Use esta variável para relatar os eventos de auditoria que ocorreram durante o intervalo de tempo especificado nesta variável. Por exemplo, se você configurar essa variável para 7, os eventos de auditoria que ocorreram somente nas últimas sete horas serão relatados pelo conjunto de dados Detalhes da Auditoria. O valor padrão da variável **COLL_AUDIT_DURATION** é `24 hours`.
- **COLL_AUDIT_COLLECTION_INTERVAL**: A coleção encadeada no conjunto de dados Detalhes da Auditoria fornece especificações de todos bancos de dados presentes na instância do SQL Server. Use essa variável para configurar o intervalo para essa coleção encadeada. Por exemplo, se configurar essa variável para 7, um novo conjunto de especificações de banco de dados será extraído da instância do SQL server após cada 7 horas. O valor padrão da variável **COLL_AUDIT_COLLECTION_INTERVAL** é 24.

Variáveis para aprimorar a coleção para o conjunto de dados Detalhes do Processo do MS SQL

Para aprimorar a coleção do conjunto de dados Detalhes do Processo do MS SQL, use a variável **COLL_PROC_BLOCK_INTERVAL** com os valores a seguir:

- Se **COLL_PROC_BLOCK_INTERVAL =** `0`, a coleção para o atributo Duração do Processo de Bloqueio e atributo Duração do Recurso de Bloqueio será desativada.
- Se **COLL_PROC_BLOCK_INTERVAL =** *x*, o intervalo entre as duas coletas de dados consecutivas para os atributos Duração do Processo de Bloqueio e Duração do Recurso de Bloqueio será *x* minutos.

Se a variável **COLL_PROC_BLOCK_INTERVAL** não estiver configurada no diretório `CANDLE_HOME`, o intervalo entre as duas coletas de dados consecutivas será três minutos.

Variável para Excluir os Objetos Bloqueados da Coleta de Dados

Se as consultas enviadas para as áreas de trabalho Detalhes do Banco de dados, Detalhes do Grupo de Arquivos, Espelhamento do Banco de Dados e Detalhes de Dispositivo demorarem para executar, use a variável **COLL_DBCC_NO_LOCK** para executar uma consulta com o valor `WITH (NOLOCK)`. Essa variável faz com que a consulta não espere na fila quando um objeto no qual a consulta é executada estiver bloqueado.

Variável para configurar os critérios de classificação para as linhas retornadas pelo conjunto de dados Detalhes da Tabela

As linhas que são retornadas pelo conjunto de dados Detalhes da Tabela são classificadas em ordem decrescente, dependendo do valor configurado para a variável **COLL_TBLD_SORTBY**. O valor padrão para a variável **COLL_TBLD_SORTBY** é FRAG (percentual de fragmentação). Os valores válidos são: ROWS (número de linhas em tabelas), SPACE (espaço usado pela tabela) e OPTSAGE (a idade das estatísticas do otimizador da tabela).

Variável para aprimorar a coleção para os conjuntos de dados Detalhes do Problema e Resumo do Problema do MS SQL

- **COLL_ALERT_SEV**: Use esta variável para configurar o nível de severidade das mensagens de erro exibidas nos conjuntos de dados Detalhes do Problema e Resumo do Problema. Mensagens de erro, que têm um nível de severidade igual a ou maior que o valor mencionado nesta variável, são exibidas nos conjuntos de dados Detalhes do Problema e Resumo do Problema. Por exemplo, se configurar o valor dessa variável para `10`, as mensagens de erro com nível de severidade 10 ou superior serão exibidas nos conjuntos de dados Detalhes do Problema e Resumo do Problema. Se você não especificar um valor para essa variável, as mensagens de erro, que têm um nível de severidade igual a ou maior que 17, serão exibidas nos conjuntos de dados Detalhes do Problema e Resumo do Problema.
- **COLL_SINCE_ERRORLOG_RECY**: Use esta variável para monitorar somente os erros de severidade alta no atual arquivo `ERRORLOG`. Se você não especificar um valor para essa variável, o valor da variável será `0`, o que significa que para coletar os dados, o conjunto de dados Resumo do Problema também considera os erros de alta severidade que são lidos do arquivo `ERRORLOG` anterior. Para monitorar somente os erros de alta severidade no atual arquivo `ERRORLOG`, configure o valor dessa variável para `1`.

Variáveis para configurar o intervalo de tempo limite

Para configurar o intervalo de tempo limite para Microsoft SQL Server agent, é possível usar as variáveis de ambiente a seguir:

- **WAIT_TIMEOUT**: Use essa variável para configurar o intervalo de tempo limite de espera para Microsoft SQL Server agent. Se algum conjunto de dados levar mais de 45 segundos para coletar dados, o agente pode ser interrompido ou situações podem ser acionadas incorretamente. Verifique o log para os conjuntos de dados que levarem mais de 45 segundos para coletar dados e use a variável **WAIT_TIMEOUT** para aumentar o tempo de espera entre o processo do agente e o processo do coletor.
- **COLL_DB_TIMEOUT**: Use essa variável para definir o intervalo de espera (em segundos) para qualquer solicitação, como executar uma consulta na conexão do SQL Server existente, ser concluída antes de

retornar ao aplicativo. Se configurar esse valor para 0, não haverá tempo limite. Se você não especificar um valor para essa variável, o agente esperará 15 segundos antes de retornar ao aplicativo.

Variáveis para configurar as propriedades dos arquivos de log do coletor

Para configurar as propriedades dos arquivos de log do coletor, é possível usar as variáveis de ambiente a seguir:

- **COLL_WRAPLINES**: Use essa variável para especificar o número máximo de linhas em um arquivo `col.out`. O valor padrão para essa variável é 90.000 linhas (cerca de 2 MB).
- **COLL_NUMOUTBAK**: Use essa variável para especificar o número de cópias de backup dos arquivos de log do coletor que você deseja criar. Por padrão, cinco cópias de backup do arquivo de log do coletor são criadas. O arquivo de backup é denominado `*.out`. Quando esse arquivo de backup está cheio, o arquivo é renomeado para `*.ou1` e os logs mais recentes são gravados no arquivo `*.out`. Dessa maneira, para cinco arquivos de backup, os logs mais antigos estão disponíveis no arquivo `*.ou5` e os logs mais recentes estão disponíveis no arquivo `*.out`.

  É possível criar mais de cinco cópias de backup dos arquivos de log do coletor especificando um dos valores a seguir na variável **COLL_NUMOUTBAK**:

  – Para menos de dez arquivos de backup, especifique o número de arquivos de backup que deseja criar na variável **COLL_NUMOUTBAK**. Por exemplo, se especificar 9 na variável **COLL_NUMOUTBAK**, nove arquivos de backup serão criados.

  – Para mais de nove e menos de 1000 arquivos de backup, na variável **COLL_NUMOUTBAK**, especifique o número de arquivos de backup precedidos por um hífen. Por exemplo, se especificar `-352` na variável **COLL_NUMOUTBAK**, 352 arquivos de backup serão criados.
- **COLL_DEBUG**: use essa variável para ativar o rastreio integral do coletor configurando o valor dessa variável para ddddddddddd (10 vezes a letra "d").

Variável para exclusão de arquivos temporários

COLL_TMPFILE_DEL_INTERVAL: use esta variável para especificar o intervalo (em minutos) após o qual os arquivos temporários KOQ_<timestamp> devem ser excluídos. Se você não especificar um valor para essa variável, o valor da variável será 0, o que significa que arquivos temporários deverão ser excluídos imediatamente.

Variável para mudar o driver usado pelo agente MS SQL Server

Para mudar o driver usado pelo Microsoft SQL Server agent, use a variável de ambiente **KOQ_ODBC_DRIVER**. Esta variável especifica o driver que o Microsoft SQL Server agent usa para se conectar ao SQL Server. Se você não especificar um valor para esta variável, o agente usará o ODBC SQL Server Driver como um driver padrão.

Nota: Ao especificar o driver Microsoft SQL Server, certifique-se de que o nome do driver esteja correto e que o driver esteja listado na opção de drivers na origem de dados (ODBC).

Variável para conectar-se a um banco de dados SQL Server ativado para AlwaysOn

KOQ_APPLICATION_INTENT: use essa variável para especificar a opção de conexão durante a conexão com o SQL Server.
Detalhes da opção **KOQ_APPLICATION_INTENT**:

- **Readonly**: a conexão é aberta com **ApplicationIntent** como *readonly*.
- **Readwrite**: a conexão é aberta com **ApplicationIntent** como *readwrite*.
  Quando ele estiver configurado como Readwrite, o agente Microsoft SQL Server não executará nenhuma operação de gravação com a conexão.

Se essa variável não for configurada, a conexão será estabelecida sem a propriedade **ApplicationIntent**.

Nota: O driver é especificado pela variável de ambiente **KOQ_ODBC_DRIVER**. Se essa variável não for configurada, o driver SQL Server padrão será usado.
Se o driver não suportar **ApplicationIntent**, a conexão será aberta sem a propriedade **ApplicationIntent**.

Parâmetros de configuração do agente

Deve-se fornecer os parâmetros de configuração obrigatórios do agente.

Sobre Esta Tarefa

A tabela a seguir contém os detalhes dos parâmetros de configuração. Revise os parâmetros e determine o valor de cada parâmetro.

Nome do parâmetro	Descrição	Valor Padrão	Campo Obrigatório
Nome do Usuário	O nome do usuário ou login usado para estabelecer uma conexão entre o agente e o SQL Server	N/D	Sim
Senha	Senha do usuário ou login	NA	Sim
Versão do banco de dados	Versão do banco de dados do SQL Server a ser monitorado	NA	Sim
Diretório Inicial do Servidor de Banco de Dados	Caminho Inicial do Banco de Dados do SQL Server	NA	Sim
Caminho do arquivo do log de erros	Local onde o arquivo do log de erros do Server está presente	NA	Sim

Configurando o Agente em Sistemas Windows

É possível usar a janela do IBM® Cloud Application Performance Management para configurar o agente em sistemas Windows.

Antes de Iniciar

Antes de configurar o agente, execute as seguintes tarefas:

- Crie um usuário e conceda as permissões necessárias
- Revise as variáveis de ambiente locais

Sobre Esta Tarefa

O Microsoft SQL Server agent é um agente de múltiplas instâncias; você deve configurar e iniciar cada instância do agente manualmente.

- Para configurar o agente, conclua as tarefas a seguir:

– Selecione os bancos de dados para monitoramento
– Configure as variáveis de ambiente locais

Selecionando os bancos de dados para monitoramento
É possível selecionar o banco de dados que você deseja monitorar usando a janela **Configurar agentes de banco de dados**.

Procedimento

1. Abra a janela **IBM Performance Management** .
2. Na janela **IBM Performance Management**, clique na coluna **Tarefa/Subsistema**, clique com o botão direito em **Modelo** e, em seguida, **Configurar Usando Padrões**.
3. Na janela **Configurar Agentes de Banco de Dados**, selecione o servidor de banco de dados que você deseja monitorar a partir dos **Servidores de Banco de Dados Disponíveis** e mova-o para a lista **Servidor para Monitorar**.
4. Na janela **Propriedades do Servidor de Banco de Dados**, os valores para os campos a seguir são preenchidos automaticamente:
   - Nome do servidor
   - Versão do banco de dados
   - Diretório inicial
   - Arquivo do log de erros

   Os campos a seguir na janela **Propriedades de servidor de base de dados** são opcionais:
   - Autenticação do Windows
   - Suportar conexões com o banco de dados de longa duração
   - Parâmetros estendidos
   - Monitorar Todos os Bancos de Dados
   - Frequência de dia(s)
   - Frequência semanal
   - Frequência mensal
   - Horário de início da coleção
   - Coleção contínua de detalhe da tabela

   Para obter informações adicionais sobre os parâmetros de configuração na janela **Propriedades do servidor de banco de dados**, consulte “Parâmetros de configuração para as propriedades do Servidor de Banco de Dados” na página 553.
5. Se você não selecionar o campo **Autenticação do Windows**, insira seu ID do usuário e senha nos campos **Efetuar login** e **Senha** usando somente caracteres ASCII.
6. No campo **Parâmetros Estendidos**, insira o nome do conjunto de dados para desativar a coleta de dados e, em seguida, clique em **OK**.

   Exemplo:
   - Insira `koqtbld` para desativar a coleta de dados para o conjunto de dados Detalhes da Tabela.
   - Insira `koqdbd` para desativar a coleta de dados para o conjunto de dados do Detalhes do Banco de Dados.
   - Insira `koqtbld, koqdbd` para desativar a coleta de dados para os conjuntos de dados Detalhes da Tabela e Detalhes do Banco de Dados.
7. Se você não marcar a caixa de seleção **Monitorar Todos os Bancos de Dados**, especifique a lista de bancos de dados para os quais você deseja ativar ou desativar o monitoramento no campo da área do grupo **Bancos de Dados**.

Lembre-se: Se você marcar a caixa de seleção **Monitorar Todos os Bancos de Dados** e especificar os bancos de dados na área do grupo **Bancos de Dados**, a configuração da caixa de seleção **Monitorar Todos os Bancos de Dados** terá precedência.

8. Especifique a frequência para a coleta do conjunto de dados Detalhes da Tabela do MS SQL. Os possíveis valores são diário, semanal ou mensal.
9. Selecione a caixa de seleção **Coleção contínua de detalhes da tabela** para ativar a coleção contínua do conjunto de dados de Detalhe da tabela do MS SQL. Se você marcar a caixa de seleção **Coleta contínua de detalhes da tabela**, insira um valor no campo **Intervalo entre duas coletas contínuas (em minutos)**.
10. Na janela **Configurar Agentes de Banco de Dados**, clique em **OK** e inicie o agente.

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.

Parâmetros de configuração para as propriedades do Servidor de Banco de Dados
Na janela **Propriedades do Servidor de Banco de Dados**, é possível configurar as propriedades do Servidor de Banco de Dados, tais como o nome do servidor, a versão do banco de dados e o diretório inicial.

A tabela a seguir contém descrições detalhadas das definições de configuração na janela **Propriedades do Servidor de Banco de Dados**.

*Tabela 182. Nomes e descrições de definições de configuração na janela **Propriedades do Servidor de Banco de Dados***

Nome de parâmetro	Descrição	Campo obrigatório	Exemplos
Nome do servidor	O nome da instância Microsoft SQL Server que deve ser monitorada. Use MSSQLSERVER como o nome da instância para a instância padrão. O nome deve ser curto o suficiente para caber no nome total do sistema gerenciado, que deve ter 2 - 32 caracteres de comprimento.	Sim	Se a instância do Microsoft SQL Server monitorada for a instância padrão do Microsoft SQL Server, insira `MSSQLSERVER` nesse campo. Se a instância do Microsoft SQL Server monitorada for uma instância denominada, em que o nome da instância é `mysqlserver` e o nome do host é `popcorn`, insira `mysqlserver` nesse campo.

*Tabela 182. Nomes e descrições de definições de configuração na janela **Propriedades do Servidor de Banco de Dados** (continuação)*

Nome de parâmetro	Descrição	Campo obrigatório	Exemplos
Efetuar Login	O ID do usuário do Microsoft SQL Server a ser usado para se conectar ao Microsoft SQL Server. O ID do usuário é necessário somente quando o parâmetro **`Autenticação do Windows`** é configurado para `False`. Use somente caracteres ASCII para o ID do usuário. Ao configurar o Microsoft SQL Server agent especificando um ID de login no campo **Login**, o agente usa esse ID de login para se conectar ao Microsoft SQL Server. **Importante:** Ao configurar o agente, se você selecionar a caixa de seleção **Autenticação do Windows** e especificar um ID de login no campo **Login**, o agente dará preferência à autenticação do Windows.	Não	
Senha	A senha para o ID do usuário do Microsoft SQL Server. A senha é necessária apenas quando o parâmetro **`Windows Authentication`** é configurado como `False`. Use somente caracteres ASCII para a senha.	Não	
Versão do banco de dados	A versão da instância do SQL server.	Sim	As versões do banco de dados para a instância do SQL server são as seguintes: • Microsoft SQL Server 2014 - 12.0.2000.8 • Microsoft SQL Server 2012 - 11.0.2100.60 • Microsoft SQL Server 2008 R2 - 10.50.1600.1 • Microsoft SQL Server 2008 - 10.0.1600.22 • Microsoft SQL Server 2005 - 9.0.1399.06

*Tabela 182. Nomes e descrições de definições de configuração na janela **Propriedades do Servidor de Banco de Dados** (continuação)*

Nome de parâmetro	Descrição	Campo obrigatório	Exemplos
Diretório inicial	O diretório de instalação do SQL server.	Sim	O caminho do diretório inicial padrão para a instância do Microsoft SQL Server 2005 padrão é `C:\Arquivos de Programas\Microsoft SQL Server\MSSQL`. Uma instância do Microsoft SQL Server 2005 nomeada possui um caminho de diretório inicial padrão no formato `C:\Program Files\Microsoft SQL Server\MSSQL$`*nome_da_instância*, em que *nome_da_instância* é o nome da instância do Microsoft SQL Server.
Arquivo do log de erros	O local e nome completos do log de erro do SQL Server.	Sim	O caminho do log de erro padrão para a instância do Microsoft SQL Server 2005 padrão é `C:\Program Files\Microsoft SQL Server\MSSQL\LOG\ERRORLOG`. Uma instância do Microsoft SQL Server 2005 nomeada tem o caminho de log de erro padrão no formato `C:\Program Files\Microsoft SQL Server\MSSQL$`*nome_da_instância*`\LOG\ERRORLOG`, em que *nome_da_instância* é o nome da instância do Microsoft SQL Server.

*Tabela 182. Nomes e descrições de definições de configuração na janela **Propriedades do Servidor de Banco de Dados** (continuação)*

Nome de parâmetro	Descrição	Campo obrigatório	Exemplos
Windows Autenticação	Autenticação do Windows é uma conta do Windows com a qual os serviços do agente são configurados, e é a opção de configuração padrão. Se você selecionar a caixa de seleção **Autenticação do Windows**, as credenciais do Windows serão usadas para autenticação. Quando o Microsoft SQL Server agent for configurado com a Autenticação do Windows, a **Conta do sistema local** ou **Esta conta** será usada pelos serviços do agente para efetuar logon no Microsoft SQL Server. • Se os serviços do agente estiverem configurados para usar a **Conta do sistema local** para efetuar logon, o agente usará o ID do usuário NT AUTHORITY\SYSTEM para acessar o Microsoft SQL Server. • Se os serviços do agente estiverem configurados para usar **Essa conta** para efetuar logon, o agente usará o respectivo ID do usuário para acessar o Microsoft SQL Server. **Lembre-se:** Se você não marcar a caixa de seleção **Autenticação do Windows**, deve-se especificar valores para os parâmetros **Login** e **Senha**. Se você não especificar esses parâmetros e clicar em **OK** na janela **Propriedades do Servidor de Banco de Dados**, uma mensagem de erro será exibida em uma janela pop-up e a configuração do agente não será concluída. **Importante:** Se você configurar o agente selecionando a caixa de seleção **Autenticação do Windows** e especificando um ID de login no campo **Login**, o agente dará preferência à autenticação do Windows.	Não	
Suportar conexões com o banco de dados de longa duração	Ativa ou desativa conexões com o banco de dados de longa duração. Os conjuntos de dados a seguir não usam conexões de banco de dados de longa duração: • Texto do MS SQL • Detalhes do Grupo de Arquivos do MS SQL • Resumo do Servidor MS SQL	Não	

*Tabela 182. Nomes e descrições de definições de configuração na janela **Propriedades do Servidor de Banco de Dados** (continuação)*

Nome de parâmetro	Descrição	Campo obrigatório	Exemplos
Parâmetros estendidos	Desativa a coleta de dados de qualquer grupo de atributos.	Não	Exemplo: Para desativar a coleta de dados para o conjunto de dados Detalhes da tabela, insira `koqtbld` no campo **Parâmetros estendidos**. Para desativar a coleta de dados para o conjunto de dados Detalhes do banco de dados, insira `koqdbd` no campo **Parâmetros estendidos**. Para desativar a coleta de dados para os conjuntos de dados Detalhes da tabela e Detalhes do banco de dados, insira `koqtbld,koqdbd` no campo **Parâmetros estendidos**.

*Tabela 182. Nomes e descrições de definições de configuração na janela **Propriedades do Servidor de Banco de Dados** (continuação)*

Nome de parâmetro	Descrição	Campo obrigatório	Exemplos

Banco de Dados	Para selecionar os bancos de dados para monitoramento, especifique um valor para esse parâmetro. Para ativar o monitoramento de todos os bancos de dados disponíveis na instância do SQL Server, marque a caixa de seleção **Monitorar Todos os Bancos de Dados** na área do grupo **Bancos de Dados**. A caixa de seleção **Monitorar Todos os Bancos de Dados** é selecionada por padrão.
	
	Para ativar ou desativar o monitoramento de bancos de dados específicos, limpe a caixa de seleção **Monitorar Todos os Bancos de Dados**.
	• Para monitorar bancos de dados específicos, selecione **Incluir** da lista e, em seguida, especifique os nomes dos bancos de dados no campo de texto próximo da lista.
	• Para excluir bancos de dados específicos do monitoramento, selecione **Excluir** da lista e, em seguida, especifique os nomes dos bancos de dados no campo de texto próximo da lista.
	Use o campo de texto para filtrar os bancos de dados que deseja monitorar.
	Para especificar um filtro de banco de dados, você deve primeiro selecionar um separador. Um separador é um caractere que distingue um nome de banco de dados ou expressão de banco de dados de outro nome ou expressão.
	Quando você estiver selecionando um separador, assegure que os nomes e expressões de banco de dados não contenham o caractere que você escolher como separador. Você não deve usar os caracteres curinga que são normalmente usados na consulta T-SQL (por exemplo, %, _, [ ], ^, -) se eles forem usados nos nomes ou expressões de banco de dados.
	Quando estiver especificando o filtro do banco de dados:
	• Nomes de banco de dados devem iniciar com um separador.
	• A expressão do banco de dados deve iniciar com 2 separadores.
	A expressão do banco de dados é uma expressão válida que pode ser usada na parte `LIKE` da consulta `T-SQL`. No entanto, não é possível usar a cláusula `T-SQL ESCAPE` quando você estiver especificando a expressão do banco de dados. Os conjuntos de dados a seguir são afetados pelo filtro de banco de dados: Detalhes do Banco de Dados, Resumo do Banco de Dados, Detalhes do Dispositivo, Detalhes da Tabela, Resumo da Tabela, Detalhes do Grupo de Arquivos, Detalhes
		Não	Exemplos de filtros:
			Caso 1: `% usage`
			Por exemplo:
			`@@%m%`
			Saída: Todos os bancos de dados que têm o caractere m em seus nomes são filtrados.
			Caso 2: `_ usage`
			Por exemplo:
			`@@____`
			Saída: Todos os bancos de dados que têm quatro caracteres de comprimento são filtrados.
			Caso 3: `[] usage`
			Por exemplo:
			`@@[m]___`
			Saída: Todos os bancos de dados que têm quatro caracteres de comprimento e cujos nomes iniciam com o caractere m são filtrados.
			Caso 4: `[^] usage`
			Por exemplo:
			`@@[^m]%`
			Saída: todos os bancos de dados (de qualquer comprimento), exceto aqueles cujos nomes iniciam com o caractere *m*, serão filtrados.

*Tabela 182. Nomes e descrições de definições de configuração na janela **Propriedades do Servidor de Banco de Dados** (continuação)*

Nome de parâmetro	Descrição	Campo obrigatório	Exemplos

Banco de Dados (continuação)	**Lembre-se:**
	• Se você não marcar a caixa de seleção **Monitorar Todos os Bancos de Dados**, deve-se especificar a lista de bancos de dados para os quais deseja ativar ou desativar o monitoramento no campo de texto que está presente na área do grupo **Bancos de Dados**. Se você clicar em **OK** na janela **Propriedades do Servidor de Banco de Dados** sem marcar a caixa de seleção **Monitorar Todos os Bancos de Dados** e especificando a lista de bancos de dados, uma mensagem de erro será exibida em uma janela pop-up e a configuração do agente não será concluída.
	• Se você marcar a caixa de seleção **Monitorar Todos os Bancos de Dados** e também especificar os bancos de dados para monitorar no campo de texto presente na área do grupo **Bancos de Dados**, a prioridade será dada ao valor da caixa de seleção **Monitorar Todos os Bancos de Dados**. A lista de bancos de dados especificada no campo de texto é ignorada.
			Caso 5: Entrada errada
			Por exemplo:
			`@%m%`
			Saída: Nenhum dos bancos de dados é filtrado.
			Caso 6: Padrão
			Exemplo: o campo está em branco (nenhuma consulta é digitada)
			Saída: Todos os bancos de dados são filtrados.
			Caso 7: Padrões mistos
			Por exemplo:
			`@@[m-t]_d%`
			Saída: Todos os bancos de dados (de qualquer comprimento) cujos nomes iniciam com os caracteres, m, n, o, p, q, r, s, t, seguidos por qualquer caractere, com o caractere d no terceiro lugar são filtrados.

Frequência de dia(s)	Use este recurso para definir a frequência da coleta de dados dos atributos Table Detail. Os valores podem ser de zero a 31.	Não	
Frequência semanal	Use esse recurso para especificar um dia específico para a coleta de dados para os atributos Detalhes da Tabela. Os valores podem ser de zero a sete.	Não	
Frequência mensal	Use este recurso para definir a coleta de dados dos atributos Table Detail em um dia particular do mês. Os valores possíveis são 1, 2, 3 e assim por diante.	Não	
Horário de início da coleção	O horário de início da coleção pode ser inserido no formato HH:MM. Os valores possíveis para horas são de zero a 23. O valor padrão é zero. Os valores possíveis para minutos são de zero a 59. O valor padrão é zero.	Não	

*Tabela 182. Nomes e descrições de definições de configuração na janela **Propriedades do Servidor de Banco de Dados** (continuação)*			
Nome de parâmetro	**Descrição**	**Campo obrigatório**	**Exemplos**
Coleção contínua de detalhe da tabela	Use esse recurso para a coleção de segundo plano contínua dos dados de Detalhes da Tabela. A caixa de seleção **Coleção Contínua de Detalhes da Tabela** é selecionada por padrão.	Não	
Intervalo entre Duas Coleções Contínuas (em min.)	Especifique o intervalo de tempo entre duas coleções em minutos. O tempo de intervalo mínimo é 3 minutos. É possível selecionar o **Intervalo Entre Duas Coleções Contínuas (em minutos)** ou é possível usar Planejamento para especificar coleção contínua do conjunto de dados Detalhes da tabela. Se você selecionar o **Intervalo Entre Duas Coleções Contínuas (em minutos)** será necessário especificar o intervalo de tempo para a coleção. Se você usar Planejamento para especificar a coleção do conjunto de dados Detalhes da tabela, o intervalo de tempo mínimo será de um dia. O intervalo padrão entre duas coleções contínuas é 3 minutos.	Não	

O agente coleta os dados no intervalo de tempo para o qual a coleta de dados ocorre frequentemente. Por exemplo, se você especificar todas as frequências (diária, semanal e mensal) para coletar dados, o agente iniciará a coleta de dados de acordo com as condições a seguir:

- Se a frequência em dia(s) ≤ 7, as configurações de frequência em dia(s) serão selecionadas e as configurações de frequência semanal e mensal serão ignoradas.
- Se frequência em dia(s) > 7, as configurações de frequência semanal serão selecionadas e as configurações de frequência em dia(s) e mensal serão ignoradas.

Lembre-se: Se a caixa de seleção **Coleta contínua de detalhes da tabela** for selecionada, o agente coletará os dados no intervalo mencionado no campo **Intervalo entre duas coletas contínuas (em min.)** e não de acordo com as frequências diária, semanal ou mensal.

Configurando variáveis de ambiente local em sistemas Windows
É possível configurar as variáveis de ambiente local para alterar o comportamento do Microsoft SQL Server agent.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **Agentes de Monitoramento IBM** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, no menu **Ações** , clique em **Avançado > Editar Variáveis**.
3. Na janela Monitoring Agent for Microsoft SQL Server: **Substituir Configurações de Variável Local**, clique em **Incluir**.
4. Na janela **Incluir substituição de configuração do ambiente**, insira a variável e o valor correspondente.

   Nota: Consulte "variáveis de ambiente local" na página 545 para obter a lista completa de variáveis de ambiente configuráveis.

Executando Como um Usuário Não Administrador
É possível executar o agente de monitoramento para o Microsoft SQL Server como um usuário não administrador.

Sobre Esta Tarefa
O Microsoft SQL Server agent pode ser executado como um usuário não administrador do grupo Usuários do Domínio.

Procedimento

1. Inicie o aplicativo Windows Active Directory Users and Computers e crie um usuário do domínio.
   - Certifique-se de que o novo usuário seja membro do Grupo *Usuários do Domínio*
   - Certifique-se de que o SQL Server seja membro do *Computadores do domínio*.
2. Inclua o usuário do domínio recentemente criado no grupo de usuários *Login do SQL Server*. O usuário do domínio deve ter a permissão de função **sysadmin** do SQL Server no SQL Server ou as permissões que são mencionadas em https://www.ibm.com/support/knowledgecenter/SSMKFH/com.ibm.apmaas.doc/install/sql_config_agent_grant_permission_sqlserver.htm.
3. Efetue logon no SQL Server como o administrador de domínio.
4. Conceda permissão **Modificar** a cada unidade que o Microsoft SQL Server agent acessa. Conclua os procedimentos a seguir para propagar a permissão para todos os subdiretórios:
   a) Vá para **Meu Computador**.
   b) Clique com o botão direito do mouse na **unidade**.
   c) Clique na guia **Segurança**.
   d) Adicione o usuário recentemente criado.
   e) Conceda permissão **Modificar** ao usuário recém-criado.
   f) Clique em **OK**. Esse procedimento leva alguns minutos para aplicar a permissão a todos os subdiretórios.
5. Usando o Registro do Windows, conceda acesso de leitura a HKEY_LOCAL_MACHINE e propague as configurações. Conclua as etapas a seguir para propagar as configurações:
   a) Clique com o botão direito do mouse no diretório HKEY_LOCAL_MACHINE e selecione **Permissões**.
   b) Adicione o usuário recentemente criado.
   c) Selecione o usuário recentemente criado.
   d) Selecione a caixa de opção **Permitir Leitura**.
   e) Clique em **OK**. Esse procedimento leva alguns minutos para propagar as configurações para a árvore HKEY_LOCAL_MACHINE inteira.
6. Usando o Registro do Windows, conceda as permissões de registro específicas do agente, de acordo com a seguinte lista.
   - Se você instalou um agente de 32 bits em um sistema operacional de 32 bits, conceda acesso total ao diretório KEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring e, em seguida, propague as configurações.
   - Se você instalou um agente de 32 bits em um sistema operacional de 64 bits, conceda acesso total ao diretório HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Candle e, então, propague as configurações.
   - Se você instalou um agente de 64 bits em um sistema operacional de 64 bits, conceda acesso total ao diretório KEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring e, em seguida, propague as configurações.

   Conclua as etapas a seguir para propagar as configurações:
   a) Clique com o botão direito no diretório para o qual você tem acesso total e selecione **Permissões**.

b) Adicione o usuário recentemente criado.

c) Selecione o usuário recentemente criado.

d) Selecione a caixa de opção **Permitir Controle Integral**.

e) Clique em **OK**. Esse procedimento leva alguns minutos para propagar as configurações para a árvore KEY_LOCAL_MACHINE\SOFTWARE\IBMMonitoring inteira.

7. Inclua um Usuário do Domínio no novo grupo **Usuários do Monitor de Desempenho**.
8. Verifique se os Usuários do Domínio são membros do grupo *Usuários*.
9. Conceda as seguintes permissões ao diretório do Windows para execução como um usuário não administrador:

   - Se um agente de 32 bits está instalado em um sistema operacional de 32 bits, conceda acesso de leitura e gravação ao diretório OS_installation_drive:\Windows\system32
   - Se um agente de 32 bits está instalado em um sistema operacional de 64 bits, conceda acesso de leitura e gravação ao diretório OS_installation_drive:\Windows\SysWOW64

   Nota: Permissões para o diretório do Windows não são necessárias para Windows Server 2008, Windows Server 2008 R2 e Windows Server 2012, Windows Server 2012 R2, Windows Server 2016.
10. Conceda permissão **Modificar** ao arquivo de dados e ao arquivo de log do SQL Server:

    - O caminho padrão do arquivo de dados do SQL Server é *SQLServer_root_dir*\DATA, em que *SQLServer_root_dir* é o diretório raiz da instância do SQL Server. Por exemplo, se o diretório raiz da instância do SQL Server for C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL, o caminho do arquivo de dados será C:\Program Files\Microsoft SQL Server \MSSQL.1\MSSQL\DATA.
    - O caminho padrão do arquivo de log do SQL Server é *SQLServer_root_dir*\LOG, em que *SQLServer_root_dir* é o diretório raiz da instância do SQL Server. Por exemplo, se o diretório raiz da instância do SQL Server for C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL, o caminho de arquivo de log seráC:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL \LOG.
11. Conceda permissões totais ao diretório Candle_Home. O caminho padrão é C:\IBM\ITM.
12. Aplique permissões de segurança local, consulte "Permissões de Política de segurança local" na página 562.
13. Reinicie o SQL Server para assegurar que as permissões de segurança local sejam aplicadas de forma efetiva.
14. Alter as configurações de logon para os serviços do agente do SQL Server para o usuário não administrador ao concluir as seguintes etapas:

    a) Clique em **Iniciar > Ferramentas Administrativas > Serviços**.

    b) Clique com o botão direito do mouse em **Monitoring Agent For SQL Server *instance_name*** e clique em **Propriedades**. A janela **Propriedades do serviço SQL** é aberta.

    c) Clique na guia **Efetuar Logon**.

    d) Clique em **Esta Conta** e digite o nome do usuário.

    e) Nos campos **Senha** e **Confirmar Senha**, insira a senha e clique em **OK**.

    f) Repita das etapas b à e para o **Monitoring Agent for SQL Server Collector *instance_name***, em que *instance_name* é o nome da instância do SQL Server Microsoft.

Permissões de Política de segurança local

A política de segurança local administra o sistema e sua política de segurança. Ela desempenha um papel importante para manter seguros o agente e o sistema no qual o agente está instalado. Essa política funciona concedendo direitos e permissões de acesso a usuários. Para o Microsoft SQL Server agent, certifique-se de que o usuário tenha as seguintes permissões para aderir à política de permissão de segurança local.

Efetuar logon como permissão de Serviço

Sobre Esta Tarefa

Para conceder a permissão Efetuar Logon como Serviço, conclua as etapas a seguir.

Procedimento

1. Clique em **Iniciar > Ferramentas Administrativas > Política de Segurança Local**. A janela **Configurações de segurança local** é aberta
2. Clique em **Políticas Locais** para expandir a lista.
3. Clique em **Designação de direitos do usuário**. A lista de direitos de usuário é aberta.
4. Dê um clique duplo na política **Efetuar logon como serviço**. A janela **Efetuar logon como propriedades de serviço** é aberta.
5. Clique em **Incluir Usuário ou Grupo**. A janela **Selecionar Usuários ou Grupos** é exibida.
6. No campo **Inserir Nomes de Objetos para Selecionar**, insira o nome da conta do usuário para quem você deseja designar permissões e, em seguida, clique em **OK**.
7. Clique em **OK**.

Permissão Depurar programas

Sobre Esta Tarefa

Para conceder a permissão do programa de depuração, conclua o procedimento a seguir no Microsoft SQL Server agent.

Procedimento

1. Clique em **Iniciar > Ferramentas Administrativas > Política de Segurança Local**. A janela **Configurações de Segurança Local** é aberta.
2. Clique em **Políticas Locais** para expandir a lista.
3. Clique em **Designação de Direitos de Usuário**. A lista de direitos de usuário é aberta.
4. Dê um clique duplo na política **Programas de depuração**. A janela **Propriedades dos programas de depuração** é aberta.
5. Clique em **Incluir Usuário ou Grupo**. A janela **Selecionar Usuários ou Grupos** é exibida.
6. No campo **Inserir nomes de objeto para selecionar**, insira o nome da conta do usuário para a qual deseja designar permissões e clique em **OK**.
7. Clique em **OK**.

Personificar um cliente após a autenticação

Sobre Esta Tarefa

Para conceder a permissão Personificar um cliente após autenticação, conclua o procedimento a seguir no Microsoft SQL Server agent.

Procedimento

1. Clique em **Iniciar > Ferramentas Administrativas > Política de Segurança Local**. A janela **Configurações de Segurança Local** é aberta.
2. Clique em **Políticas Locais** para expandir a lista.
3. Clique em **Designação de Direitos de Usuário**. A lista de direitos de usuário é aberta.
4. Dê um clique duplo na política **Personificar um cliente após a autenticação**. A janela **Personificar um cliente após a autenticação - Propriedades** se abre.
5. Clique em **Incluir Usuário ou Grupo**. A janela **Selecionar Usuários ou Grupos** é exibida.
6. No campo **Inserir os nomes de objetos a serem selecionados**, insira o nome da conta do usuário a quem você deseja designar permissões e, em seguida, clique em **OK**.

7. Clique em **OK**.

Configurando o agente nos sistemas Linux

Para configurar o agente em sistemas operacionais Linux, deve-se executar o script e responder aos prompts.

Antes de Iniciar

Antes de configurar o agente, execute as seguintes tarefas:

- Revise as variáveis de ambiente locais

Sobre Esta Tarefa

O Microsoft SQL Server agent é um agente de múltiplas instâncias; você deve configurar e iniciar cada instância do agente manualmente.

Procedimento

1. Na linha de comandos, mude o caminho para o diretório de instalação do agente.
   Por exemplo:
   ```
   cd /opt/ibm/apm/agent/bin
   ```
2. Execute o comando a seguir em que *instance_name* é o nome que você deseja fornecer à instância:
   ```
   ./mssql-agent.sh config instance_name
   ```
3. Quando o prompt de comandos exibe a mensagem a seguir, digite 1 e insira:
   `Edit 'Monitoring Agent for MSSQL setting? [1=Yes, 2=No]`
4. Especifique valores para os parâmetros de configuração quando solicitado.
   Para obter informações sobre os parâmetros de configuração, consulte Parâmetros de Configuração do Agente.
5. Execute o comando a seguir para iniciar o agente:
   ```
   ./mssql-agent.sh start instance_name
   ```
6. Execute o comando a seguir para parar o agente:
   ```
   ./mssql-agent.sh stop instance_name
   ```

Configurando variáveis de ambiente local em sistemas Linux

É possível configurar variáveis de ambiente local para mudar o comportamento do Microsoft SQL Server agent em sistemas Linux.

Procedimento

1. Ative um gerenciador de arquivos de sistema ou terminal e altere o diretório para o diretório de instalação do agente:
   Por exemplo:
   ```
   /opt/ibm/apm/agent
   ```
2. Execute o comando a seguir para parar o agente:
   ```
   ./mssql-agent.sh stop instance_name
   ```
   Em que *instance_name* é o nome da instância do agente.
3. Abra o arquivo `.oq.environment` que existe no seguinte diretório de configuração:
   Por exemplo:

```
install_dir/config
```

Em que *install_dir* é o diretório de instalação do agente.

4. Inclua as variáveis de ambiente necessárias no final do arquivo `.oq.environment` seguindo o formato do par nome-valor.

   `export VARIABLE_NAME=VARIABLE_VALUE`

   Por exemplo:

   ```
   export KOQ_ODBC_DRIVER=ODBC Driver 17 for SQL Server
   ```

   Nota:

   - Consulte "variáveis de ambiente local" na página 545 para obter a lista completa de variáveis de ambiente configuráveis.
   - As variáveis customizadas incluídas não são preservadas após a atualização do agente.
5. Salve o arquivo.
6. Inicie o agente a partir do diretório de instalação do agente:

   ```
   cd /opt/ibm/apm/agent/bin
   ```

   ```
   ./mssql-agent.sh start instance_name
   ```

Configurando o agente usando o arquivo de resposta silencioso

É possível usar o arquivo de resposta silencioso para configurar o agente ou várias instâncias do agente.

Antes de Iniciar

Para configurar várias instâncias do agente, certifique-se de que os detalhes de configuração de todas as instâncias do agente sejam especificados no arquivo de resposta silencioso.

Sobre Esta Tarefa

Execute o script de configuração para alterar as definições de configuração. É possível editar o arquivo de resposta silencioso antes de executar o script de configuração.

Procedimento

Para configurar o agente, execute as seguintes etapas:

1. Ative um editor de texto e abra o arquivo de resposta silencioso que está disponível no seguinte local:
   - Windows *install_dir*\samples/mssql_silent_config.txt
   - Linux *install_dir*/samples/mssql_silent_config.txt

   Em que *install_dir* é o diretório de instalação do agente.

   Por exemplo:

   - Windows `C:\IBM\APM\samples\mssql_silent_config.txt`
   - Linux `/opt/ibm/apm/agent/samples/mssql_silent_config.txt`

   Nota: Para obter informações sobre os parâmetros de configuração do agente, consulte "Parâmetros de configuração do agente " na página 551.
2. Ative um prompt de comandos e mude o diretório para o seguinte:
   - Windows

     ```
     cd install_dir\bin
     ```

- Linux

```
cd install_dir/bin
```

3. Execute o seguinte comando:
   - Windows

```
mssql-agent.bat config install_dir\samples\mssql_silent_config.txt
```

   - Linux

```
mssql-agent.sh config  instance_name install_dir/samples/mssql_silent_config.txt
```

4. Inicie o agente.
   - Windows Na janela **IBM Performance Management**, clique com o botão direito na instância do agente que você criou e clique em Iniciar.
   - Linux Execute o seguinte comando:

```
cd /opt/ibm/apm/agent/bin
```

```
./mssql-agent.sh start instance_name
```

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.

Executando o agente em um ambiente em cluster

Windows É possível configurar o Microsoft SQL Server agent em um ambiente em cluster. Várias instâncias do Microsoft SQL Server e do Microsoft SQL Server agent podem ser executadas em um único nó.

Depois de instalar e configurar o Microsoft SQL Server agent, conclua as tarefas a seguir para executar o agente em um ambiente em cluster:

- Inclua variáveis de ambiente
- Mude o tipo de inicialização do serviço do agente e do serviço do coletor
- Inclua o agente e o coletor no ambiente em cluster

Você pode configurar um ambiente em cluster para as versões a seguir do Microsoft SQL Server:

- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016

Importante: Em sistemas Windows, o agente deve ser instalado no mesmo diretório no qual o agente do sistema operacional está instalado. Instale o agente no disco do sistema de nós de cada nó do cluster.

Incluindo Variáveis de Ambiente
As variáveis de ambiente que são usadas pelos agentes instalados em cada nó do cluster devem ser configuradas.

Sobre Esta Tarefa
Devem-se especificar valores para as seguintes variáveis de ambiente:

- *CTIRA_HOSTNAME*: esta variável é usada para configurar cada instância do Microsoft SQL Server agent. O valor dessa variável limita-se a 31 caracteres e é comum para todos os agentes de monitoramento. Configure o valor dessa variável como o nome do cluster para navegar para todos os agentes de monitoramento desse cluster no Application Performance Dashboard.
- *CTIRA_NODETYPE*: esta variável é usada para identificar o agente. Por padrão, o valor dessa variável é configurado como **MSS** para o Microsoft SQL Server agent.
- *CTIRA_SUBSYSTEMID*: esta variável é usada para distinguir as várias instâncias do Microsoft SQL Server agent. Por padrão, o valor dessa variável é configurado como **Microsoft SQL Virtual Server** para o Microsoft SQL Server agent.
- *COLL_HOME*: esta variável é usada para coletar dados e armazenar arquivos de log para grupos de atributos que usam arquivos de configuração em um local compartilhado. Configure o valor da variável como *X*:\shared-location, em que *X* é uma unidade compartilhada acessível para os nós do cluster. Por exemplo, configure o valor da variável *COLL_HOME* ao determinar as definições de configuração para o grupo de atributos Detalhes da tabela do MS SQL ou o grupo de atributos Detalhes de eventos de erro do MS SQL.
- *CTIRA_HIST_DIR*: essa variável é usada para especificar o caminho para o diretório do disco compartilhado. Se o histórico do Microsoft SQL Server agent for configurado para ser armazenado no agente de monitoramento, cada instância do agente deve ser configurada com uma variável *CTIRA_HIST_DIR* comum, que faz referência ao diretório do disco compartilhado.

  Lembre-se: Se o histórico for armazenado no Servidor Cloud APM, não será necessário especificar um valor para a variável *CTIRA_HIST_DIR*. Armazenar o histórico no Servidor Cloud APM aumenta a carga nesse servidor.

Para incluir essas variáveis, consulte as etapas que são descritas em "Configurando variáveis de ambiente local em sistemas Windows" na página 560.

O que Fazer Depois
Altere o tipo de inicialização do serviço do agente e do serviço do coletor para **Manual**, concluindo as etapas que são descritas em "Alterando o tipo de inicialização do serviço do agente e do serviço do coletor" na página 567.

Alterando o tipo de inicialização do serviço do agente e do serviço do coletor
Por padrão, o tipo de inicialização do serviço do agente e do serviço do coletor é **Automático**. Altere o tipo de inicialização do serviço do agente e do serviço do coletor para **Manual**, para que o recurso de cluster possa controlar a inicialização e a interrupção do agente de monitoramento

Procedimento

Para alterar o tipo de inicialização do serviço do agente, conclua as seguintes etapas:

1. Clique em **Iniciar** > **Executar**, digite o comando `services.msc` e clique em **OK**.
2. Clique com o botão direito do mouse no agente e clique em **Propriedades**.
3. Na janela **Propriedades do Monitoring Agent for Microsoft SQL Server**, na lista **Tipo de inicialização**, selecione **Manual**, clique em **Aplicar** e, em seguida, em **OK**.

O que Fazer Depois

- Use o mesmo procedimento para alterar o tipo de inicialização do serviço do coletor para **Manual**.
- Inclua o agente e o coletor no ambiente em cluster, concluindo as etapas que são descritas em "Incluindo o agente e o coletor no ambiente em cluster " na página 567.

Incluindo o agente e o coletor no ambiente em cluster
O agente e o coletor devem ser incluídos no ambiente em cluster.

Procedimento

1. Clique em **Iniciar > Painel de Controle > Ferramentas Administrativas > Gerenciamento de Cluster de Failover**.
2. Expanda **Gerenciamento de Cluster de Failover**.
3. Expanda **Serviços e Aplicativos** e clique com o botão direito do mouse na instância SQL que deseja configurar.
4. Clique em **Incluir um Recurso > Serviço Genérico**. O Assistente Novo Recurso é aberto.
5. Na página Selecionar serviço, selecione o nome do serviço e, em seguida, clique em **Avançar**.

   Exemplos de nomes de Serviços do Windows:

   - `Monitoring Agent for Microsoft SQL Server: SQLTEST#INSTANCE1`
   - `Monitoring Agent for Microsoft SQL Server: Collector SQLTEST#INSTANCE1`
   - `Monitoring Agent for Microsoft SQL Server: SQLTEST2#INSTANCE2`
   - `Monitoring Agent for Microsoft SQL Server: Collector SQLTEST2#INSTANCE2`
6. Na página Confirmação, verifique os detalhes e, em seguida, clique em **Avançar**.
7. Na página Resumo, clique em **Concluir**. O Microsoft SQL Server agent agora está incluído.

   Lembre-se: Use as mesmas etapas para incluir o coletor no ambiente em cluster.
8. Para deixar o agente on-line, clique com o botão direito no agente e clique em **Deixar este recurso on-line**.
9. Para deixar o coletor on-line, clique com o botão direito no coletor e clique em **Deixar este recurso on-line**.

Resultados
O Microsoft SQL Server agent agora está em execução em um ambiente em cluster.

Lembre-se: Se você quiser configurar o agente novamente, deverá primeiro deixar o agente e o coletor off-line ou editar as variáveis do agente no nó no qual o agente e o coletor são executados. Ao concluir a configuração do agente, deixe o agente e o coletor novamente on-line.

Configurando o agente usando o utilitário de cluster

Windows É possível usar o utilitário de cluster para incluir várias instâncias do Microsoft SQL Server agent em um grupo de clusters em um ambiente em cluster.

O utilitário de cluster inclui automaticamente o serviço do agente e o serviço do coletor de cada instância do Microsoft SQL Server agent como um recurso de serviço genérico no grupo de clusters. É possível usar o utilitário de cluster para concluir as seguintes tarefas:

- Incluindo uma Instância do Agente SQL Server no Cluster
- Atualizando uma Instância do Agente SQL Server Existente em um Cluster
- Removendo uma Instância do Agente SQL Server de um Cluster

Pré-requisitos para Usar o Utilitário do Cluster
Você deve assegurar que seu ambiente do sistema atenda aos pré-requisitos para executar o utilitário do cluster.

Certifique-se de que os seguintes pré-requisitos sejam atendidos:

- Execute o utilitário de cluster em um computador que tenha pelo menos um grupo no ambiente em cluster.
- Inicie o serviço de registro remoto para todos os nós no cluster.
- Você deve ter a autorização de gerenciador do cluster para acessar o utilitário de cluster.
- O nome do serviço do agente e do coletor deve ser o mesmo em todos os nós do cluster.

Por exemplo, se o nome do serviço do agente for Monitoring Agent for Microsoft SQL Server: SQLTEST#INSTANCE1 e o nome do coletor for Monitoring Agent for Microsoft SQL Server: Coletor SQLTEST#INSTANCE1, o mesmo nome do serviço deve estar presente em todos os nós do cluster.

Incluindo uma instância do Microsoft SQL Server agent no cluster
É possível usar o utilitário de cluster para incluir uma instância do Microsoft SQL Server agent em um grupo de clusters em um ambiente em cluster.

Procedimento

1. Para executar o utilitário, conclua uma das seguintes etapas:
   - Para um agente de 64 bits, acesse o diretório *candle_home*\TMAITM6_x64.
   - Para um agente de 32 bits, acesse o diretório *candle_home*\TMAITM6.
2. Para executar o Utilitário de Cluster, clique duas vezes em KoqClusterUtility.exe.
3. Na área **Instâncias do agente SQL Server disponíveis**, selecione uma instância do Microsoft SQL Server agent e clique em **Incluir**.
4. Na janela **Selecionar nome do grupo de cluster**, selecione um grupo de cluster.
   O grupo de clusters selecionado deve ser a instância do SQL Server que é monitorada pelo Microsoft SQL Server agent.
5. Na janela **Selecionar caminho para local compartilhado**, navegue para o caminho onde os logs do agente e do coletor estão armazenados.
   Se não o caminho não for selecionado, por padrão, o local CANDLEHOME/TMAITM6(_x64)/logs será selecionado para armazenar o agente e os logs do coletor.
6. Para incluir a instância do Microsoft SQL Server agent no ambiente em cluster, clique em **OK**.
   Os logs de atividade do utilitário de cluster serão exibidos na área de janela **Histórico**.

Atualizando uma instância existente do Microsoft SQL Server agent em um cluster
É possível usar o utilitário de cluster para atualizar o local em que os logs do agente e do coletor são armazenados para uma instância do SQL Server em um cluster.

Procedimento

1. Para atualizar uma instância existente do Microsoft SQL Server agent, abra a janela **Utilitário de Cluster**.
2. Na área **Instâncias do agente SQL Server configuradas**, selecione uma instância do Microsoft SQL Server agent e clique em **Atualizar**.
3. Na janela **Configurar Caminho para Local Compartilhado**, navegue para o caminho onde os logs do agente e do coletor estão armazenados.
   Se você não selecionar o caminho, os logs do agente e do coletor serão armazenados no local que foi configurado ao incluir a instância do Microsoft SQL Server agent em um cluster.
4. Clique em **OK**.
   Os logs de atividade do utilitário de cluster serão exibidos na área de janela **Histórico**.

Removendo uma instância do Microsoft SQL Server agent de um cluster
É possível usar o utilitário de cluster para remover uma instância do Microsoft SQL Server agent de um grupo de clusters.

Procedimento

1. Abra a janela **Utilitário de Cluster**.
2. Na área **Instâncias do agente SQL Server configuradas**, selecione uma instância do Microsoft SQL Server agent e clique em **Remover**.
3. Na caixa de diálogo **Confirmar ação**, clique em **Sim** para excluir a instância do Microsoft SQL Server agent do cluster.

Os logs de atividade do utilitário de cluster serão exibidos na área de janela **Histórico**.

Configurando várias intercalações para o arquivo ERRORLOG

O Microsoft SQL Server agent versão 06.31.17.00 ou mais recente para o Application Performance Management versão 8.1.4.0.4 suporta múltiplas ordenações no arquivo ERRORLOG. Agora é possível configurar o agente para analisar mais de uma ordenação no arquivo ERRORLOG para o grupo de atributos **Detalhe do problema**. Observe que as múltiplas ordenações no arquivo ERRORLOG não são aplicáveis ao grupo de atributos **Detalhe do evento de erro**.

Antes de Iniciar

Para configurar múltiplas ordenações do agente, certifique-se de que o agente esteja instalado.

Sobre Esta Tarefa

A intercalação padrão é Inglês. Para outros idiomas do SQL Server, o agente analisará o arquivo ERRORLOG com base nas ordenações no arquivo de configuração `koqErrConfig.ini`. Portanto, deve-se incluir as ordenações que estão em uso no arquivo `koqErrConfig.ini`.

Procedimento

Para configurar múltiplas ordenações para o agente, conclua as etapas a seguir:

1. Vá para o diretório do agente *agent_directory*.

   Windows

   - Para o agente de 64 bits, *agent_directory* é *Agent_home*\TMAITM6_x64.
   - Para o agente de 32 bits, *agent_directory* é *Agent_home*\TMAITM6.

   Linux

   - Para agente de 64 bits, o *agent_directory* é *Agent_home*/TMAITM6_x64.

   Em que *Agent_home* é o diretório de instalação do agente.
2. Abra o arquivo de configuração `koqErrConfig.ini` :
3. Mova para o término do arquivo para incluir as novas ordenações.

   Por exemplo, para ativar a ordenação para francês, inclua as configurações de ordenação a seguir no formato do par **`name-value`** no término do arquivo `koqErrConfig.ini`.

   ```
   [French]
   Error = Erreur :
   Severity = Gravité :
   State = État :
   ```

   Nota: A lista de amostra de ordenações está disponível em *agent_directory* `\koqErrConfigSample.ini`.

   Em que Windows

   - Para o agente de 64 bits, *agent_directory* é *Agent_home*\TMAITM6_x64.
   - Para o agente de 32 bits, *agent_directory* é *Agent_home*\TMAITM6.

   Linux

   - Para agente de 64 bits, o *agent_directory* é *Agent_home*/TMAITM6_x64.

   Em que *Agent_home* é o diretório de instalação do agente.

   Se a ordenação de destino não estiver disponível em `koqErrConfigSample.ini`, será possível determinar os valores da palavra-chave de ordenação a partir do arquivo ERRORLOG.
   Obedeça aa seguinte formato de ordenação ao configurar as definições de ordenação no `koqErrConfig.ini`.

```
[ Section_name ]
Error = Error_value
Severity = Severity_value
Estado =  State_value
```

Where

- *Section_name* é o nome da ordenação do SQL Server. Assegure-se de que o nome da ordenação seja colocado entre um colchete de abertura "**[**" e um colchete de fechamento "**]**".
- *Error_value* é a palavra-chave de erro correspondente localizada no arquivo ERRORLOG de sua ordenação de destino.
- *Severity_value* é a palavra-chave de severidade correspondente localizada no arquivo ERRORLOG de sua ordenação de destino.
- *State_value* é a palavra-chave do estado correspondente localizada no arquivo ERRORLOG de sua ordenação de destino.

Importante: Os valores de palavra-chave devem ser iguais aos valores de palavra-chave localizados no arquivo ERRORLOG, incluindo os caracteres especiais.

4. Salve o arquivo de configuração `koqErrConfig.ini`.

   A reinicialização do agente não é necessária.

   Se o arquivo de configuração `koqErrConfig.ini` não estiver disponível ou se o arquivo de configuração `koqErrConfig.ini` estiver vazio, o arquivo ERRORLOG mostrará a ordenação padrão como mensagem de erro em inglês com um nível de severidade mais alto que o nível de severidade padrão, se houver.

   Se o arquivo de configuração `koqErrConfig.ini` estiver definido corretamente, o arquivo ERRORLOG mostrará as mensagens de erro correspondentes com um nível de severidade mais alto que o nível de severidade padrão, se houver.

   O nível de severidade padrão é 17.

   Atenção: Como as mudanças feitas no arquivo `koqErrConfig.ini` não são preservadas durante o upgrade do agente, deve-se fazer um backup antes de executar o upgrade do agente.

O que Fazer Depois
Verifique o widget **Alerta Errorlog** ou o grupo de atributos **Detalhes do problema** no painel do Application Performance Management como resultado das configurações de ordenação.

Configurando o monitoramento do MongoDB

O Monitoring Agent for MongoDB requer um nome de instância. Deve-se configurar e iniciar manualmente a instância de agente. O Agente MongoDB suporta monitoramento local e também o remoto. Consulte os seguintes pré-requisitos para configurar o Agente MongoDB para monitoramento remoto e local.

Antes de Iniciar

- Revise os pré-requisitos de hardware e software. Para obter as informações de requisitos do sistema atualizadas, consulte o Software Product Compatibility Reports (SPCR) para o Agente MongoDB.
- Certifique-se de que o usuário, que configura o Agente MongoDB, tenha as funções necessárias para coletar dados para todos os atributos.
  - Para configurar o agente no banco de dados MongoDB versão 2.4 e versão 2.6, as funções clusterAdmin, readAnyDatabase e dbAdminAnyDatabase devem ser designadas ao usuário
  - Para configurar o agente no banco de dados MongoDB versões 3.x e 4.x, as funções clusterMonitor, readAnyDatabase e dbAdminAnyDatabase devem ser designadas ao usuário

Para saber sobre os grupos de atributos para os quais essas funções de usuário são necessárias, consulte Tabela 183 na página 572.

- Use um usuário existente ou crie um usuário no banco de dados admin.

  Importante: Antes de criar um usuário e de conceder as funções necessárias a ele, você deve conectar-se ao banco de dados MongoDB e mudar o banco de dados para o banco de dados admin. Se o processo mongod ou mongos estiver em execução no modo de autenticação, insira as credenciais necessárias para conectar-se ao banco de dados MongoDB.

  1. Execute o seguinte comando para conectar-se ao banco de dados MongoDB:

     `mongo IP:port`

     Where

     – *IP* é o endereço IP do processo mongod ou mongos
     – *port* é o número da porta do processo mongod ou mongos
  2. Mude o banco de dados para o banco de dados admin:

     `use admin`
  3. Execute um dos seguintes comandos para incluir um usuário no banco de dados admin MongoDB e designar as funções necessárias ao usuário:

     – Para o banco de dados MongoDB versão 2.4, execute o seguinte comando:

       ```
       db.addUser({ user: "username", pwd: "password", roles: [ 'clusterAdmin',
       'readAnyDatabase', 'dbAdminAnyDatabase' ] })
       ```

     – Para o banco de dados MongoDB versão 2.6, execute o seguinte comando:

       ```
       db.createUser({user: "username", pwd: "password", roles:
       [ 'clusterAdmin', 'readAnyDatabase', 'dbAdminAnyDatabase' ] })
       ```

     – Para o banco de dados MongoDB versões 3.x e 4.x, execute o seguinte comando:

       ```
       db.createUser({user: "username", pwd: "password", roles:
       [ 'clusterMonitor', 'readAnyDatabase', 'dbAdminAnyDatabase' ] })
       ```
  4. Execute o seguinte comando para verificar se o usuário foi incluído no banco de dados admin:

     `db.auth("username", "password")`

     O código de retorno **1** indica que o usuário foi incluído, enquanto o código de retorno **0** indica que a inclusão do usuário falhou.

A tabela a seguir contém informações sobre as funções de usuário e os atributos para os quais essas funções de usuário são necessárias:

Tabela 183. Grupos de atributos e suas funções de usuário necessárias

Atribuições	**Versão do banco de dados MongoDB**	**Grupos de atributos**
dbAdminAnyDatabase	2.x, 3.x e 4.x	Tempos de resposta
readAnyDatabase	2.x, 3.x e 4.x	• Listagem de mongod • Informações gerais compartilhadas • Armazenamento de coleção • Nomes do Banco de Dados • Detalhes do Shard • Detalhes do armazenamento de coleta

Tabela 183. Grupos de atributos e suas funções de usuário necessárias (continuação)

Atribuições	Versão do banco de dados MongoDB	Grupos de atributos
clusterAdmin	2.x, 3.x e 4.x	• Informações de instância do Mongo • Informações de E/S de instância do Mongo • Cópia de MII para APMUI One • Cópia de MII para APMUI Two • Bloqueio de BD de instância do Mongo • Trava • Bloqueios do MongoDB • Detalhes de WiredTiger • Detalhes de MMAPv1
clusterMonitor	2.x, 3.x e 4.x	• Informações de instância do Mongo • Informações de E/S de instância do Mongo • Cópia de MII para APMUI One • Cópia de MII para APMUI Two • Bloqueio de BD de instância do Mongo • Trava • Bloqueios do MongoDB • Detalhes de WiredTiger • Detalhes de MMAPv1

- Para monitoramento remoto do servidor MongoDB, consulte os dois pré-requisitos
  1. Como o Agente MongoDB requer o shell mongo para coletar informações remotamente do servidor MongoDB, o sistema no qual o Agente MongoDB está instalado e configurado deve ter uma instância do servidor MongoDB. O shell mongo do servidor MongoDB na máquina do agente é usado para conexão com o servidor MongoDB remoto para monitoramento.
  2. No arquivo `/etc/hosts` do sistema que hospeda o agente, há uma entrada da máquina remota.

Sobre Esta Tarefa

O nome do sistema gerenciado inclui o nome da instância que você especifica. Por exemplo, é possível especificar o nome da instância como *instance_name*:*host_name*:*pc*, em que *pc* é o código de produto de dois caracteres de seu agente. O nome do sistema gerenciado pode conter até 32 caracteres. O nome da instância pode conter até 28 caracteres, excluindo o comprimento do nome do host. Por exemplo, se você especificar `Mongo2` como o nome da instância, o nome do sistema gerenciado será `Mongo2:hostname:KJ`.

Importante: Se você especificar um nome de instância longo, o nome do sistema gerenciado é truncado e o código do agente não é completamente exibido.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu

ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte o “Histórico de Mudanças” na página 50.

Lembre-se:

- Para o agente coletar dados com êxito, inicie o agente com o superusuário (raiz), ou use o mesmo ID do usuário para iniciar o agente e o processo mongod.
- Em um ambiente onde o MongoDB é executado como um cluster, certifique-se de instalar o agente no mesmo computador em que o processo do roteador está sendo executado. Configure o agente no mesmo computador com o endereço IP e número da porta desse computador e a configuração **TYPE** como 1.
- Em um ambiente em que MongoDB é executado como um cluster no modo de autenticação, assegure-se de incluir o mesmo ID do usuário com os direitos necessários em todos os shards no cluster.

É possível configurar o agente usando as configurações padrão, editando o arquivo silencioso de resposta ou respondendo aos prompts.

Configurando o agente com configurações padrão

Para um ambiente típico, use as definições padrão para configurar o agente. Quando as configurações padrão forem usadas para a configuração do agente, o agente não será executado no modo de autenticação.

Procedimento

1. Execute o seguinte comando:
   install_dir/bin/mongodb-agent.sh config *instance_name install_dir*/samples/mongodb_silent_config.txt

   Where

   - *instance_name* é o nome especificado para a instância do aplicativo exclusiva.
   - *install_dir* é o diretório de instalação do Agente MongoDB.

   O diretório de instalação padrão é /opt/ibm/apm/agent.
2. Execute o comando a seguir para iniciar o agente:
   install_dir/bin/mongodb-agent.sh start *instance_name*

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte “Iniciando o Console do Cloud APM” na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.

Configurando o agente usando o arquivo de resposta silencioso

O arquivo de resposta silencioso contém parâmetros de configuração do agente com valores padrão definidos para alguns parâmetros. É possível editar o arquivo de resposta silencioso para especificar valores diferentes para os parâmetros de configuração e configurar o agente.

Antes de Iniciar

Para executar o banco de dados MongoDB no modo de autenticação, certifique-se de configurar o agente com um usuário que tem as funções clusterAdmin, readAnyDatabase e dbAdminAnyDatabase no banco de dados MongoDB.

Procedimento

1. Em um editor de texto, abra o arquivo de resposta silencioso que está disponível no seguinte caminho:
   install_dir/samples/mongodb_silent_config.txt.

2. Para o parâmetro **TYPE**, insira um dos seguintes valores:
   - 1 para um cluster
   - 2 para uma configuração de replicação
   - 3 para uma instância independente

   Por padrão, o agente monitora um cluster.
3. Para o parâmetro **PORT**, especifique o número da porta do roteador para um cluster MongoDB ou uma instância mongod do conjunto de replicação de MongoDB que está sendo monitorado.

   Lembre-se: Se você não especificar nenhum número de porta, o agente descobrirá automaticamente o número da porta do processo MongoDB apropriado que está ativo na interface padrão. Se nenhum processo MongoDB estiver ativo na interface padrão, o agente selecionará o número da porta do processo MongoDB adequado que está ativo na interface secundária.
4. Para o parâmetro **HOST**, especifique o endereço IP do sistema host MongoDB.

   Lembre-se: Se você não especificar nenhum endereço IP, o agente detectará automaticamente o endereço IP do processo MongoDB adequado que está ativo na interface padrão. Se nenhum processo MongoDB estiver ativo na interface padrão, o agente detectará o endereço IP do processo MongoDB adequado que está ativo na interface secundária.
5. Para o parâmetro **AUTHENTICATION**, especifique YES para indicar que mongoDB está executando no modo de autenticação. O valor padrão é N0, que indica que o agente não está em execução no modo de autenticação.

   Lembre-se: Quando o banco de dados MongoDB estiver em execução no modo de autenticação, o Agente MongoDB ou qualquer cliente MongoDB não poderá conectar-se ao banco de dados MongoDB sem credenciais. Para conectar-se ao banco de dados que é executado no modo de autenticação, especifique YES para o parâmetro **AUTHENTICATION**.

   Se você especificar YES, conclua as etapas a seguir:

   a) Para o parâmetro **User Name**, especifique um nome de usuário para o roteador ou instância mongod. Assegure-se de que o mínimo de funções seja designado ao usuário. Para obter informações sobre as funções do usuário, consulte Tabela 183 na página 572.

   b) Para o parâmetro **Senha**, especifique a senha.
6. Salve e feche o arquivo `mongodb_silent_config.txt` e execute o comando a seguir:
   `install_dir/bin/mongodb-agent.sh config instance_name install_dir/samples/mongodb_silent_config.txt`

   Where
   - *instance_name* é o nome especificado para a instância.
   - *install_dir* é o diretório de instalação do Agente MongoDB.
7. Execute o comando a seguir para iniciar o agente:
   `install_dir/bin/mongodb-agent.sh start instance_name`

   Importante: Se você fizer upgrade do agente para a V1.0.0.9 ou mais recente e desejar executar o agente no modo de autenticação, deverá configurar o agente novamente para fornecer um nome do usuário e uma senha. Para coletar dados, é preciso parar e reiniciar o agente após a configuração.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.

Configurando o agente respondendo aos prompts

Para configurar o agente com configurações customizadas, é possível especificar valores para os parâmetros de configuração, quando solicitado, enquanto o script estiver sendo executado.

Procedimento

1. Execute o seguinte comando:
   install_dir/bin/mongodb-agent.sh config *instance_name*

   Where

   - *instance_name* é o nome especificado para a instância.
   - *install_dir* é o diretório de instalação do Agente MongoDB.
2. Quando for solicitado que forneça um valor para o parâmetro **TYPE**, pressione Enter para aceitar o valor padrão ou especifique um dos seguintes valores e, em seguida, pressione Enter:

   - 1 para um cluster
   - 2 para uma configuração de replicação
   - 3 para uma instância independente

   Por padrão, o agente monitora um cluster.
3. Quando for solicitado que forneça um valor para o parâmetro **PORT**, pressione Enter para aceitar o valor padrão, ou especifique o número da porta do roteador para um cluster MongoDB ou uma instância mongod do conjunto de replicação MongoDB que está sendo monitorado e, em seguida, pressione Enter.

   Lembre-se: Se você não especificar nenhum número de porta, o agente descobrirá automaticamente o número da porta do processo MongoDB apropriado que está ativo na interface padrão. Se nenhum processo MongoDB estiver ativo na interface padrão, o agente selecionará o número da porta do processo MongoDB adequado que está ativo na interface secundária.
4. Quando for solicitado que forneça um valor para o parâmetro **HOST**, pressione Enter para aceitar o valor padrão, ou especifique o endereço IP do sistema host MongoDB e, em seguida, pressione Enter.

   Lembre-se: Se você não especificar nenhum endereço IP, o agente detectará automaticamente o endereço IP do processo MongoDB adequado que está ativo na interface padrão. Se nenhum processo MongoDB estiver ativo na interface padrão, o agente detectará o endereço IP do processo MongoDB adequado que está ativo na interface secundária.
5. Quando for solicitado que forneça um valor para o parâmetro **AUTHENTICATION**, pressione Enter para aceitar o valor padrão, ou especifique se o agente está em execução no modo de autenticação.

   O valor padrão é NO, que indica que o agente não está em execução no modo de autenticação. Especifique YES para indicar que o mongoDB está em execução no modo de autenticação.

   Lembre-se: Quando o banco de dados MongoDB estiver em execução no modo de autenticação, o Agente MongoDB ou qualquer cliente MongoDB não poderá conectar-se ao banco de dados MongoDB sem credenciais. Para conectar-se ao banco de dados que é executado no modo de autenticação, especifique YES para o parâmetro **AUTHENTICATION**.

   Se você especificar YES, conclua as etapas a seguir:

   a) Para o parâmetro **User Name**, especifique um nome de usuário para o roteador ou instância mongod. Assegure-se de que o mínimo de funções seja designado ao usuário. Para obter informações sobre as funções do usuário, consulte Tabela 183 na página 572.

   b) Para o parâmetro **Senha**, especifique a senha.
6. Execute o comando a seguir para iniciar o agente:
   install_dir/bin/mongodb-agent.sh start *instance_name*

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.

Configurando o monitoramento do MySQL

O Monitoring Agent for MySQL requer um nome de instância e as credenciais do usuário do servidor MySQL. É possível mudar as definições de configuração depois de criar a primeira instância de agente.

Antes de Iniciar

- Certifique-se de que um usuário seja criado no banco de dados MySQL para executar o agente. O usuário não requer nenhum privilégio específico no banco de dados MySQL que está sendo monitorado.
- Revise os pré-requisitos de hardware e software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Agente MySQL.

Sobre Esta Tarefa

As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte "Histórico de Mudanças" na página 50.

O nome do sistema gerenciado inclui o nome da instância especificada, por exemplo *instance_name*:*host_name*:*pc*, em que *pc* é o código de produto de dois caracteres. O nome do sistema gerenciado pode conter até 32 caracteres. O nome da instância que você especifica pode conter até 28 caracteres, excluindo o comprimento do nome do host. Por exemplo, se você especificar `MySQL2` como o nome da instância, o seu nome do sistema gerenciado será `MySQL2:hostname:SE`.

Importante: Se você especificar um nome de instância longo, o nome do sistema gerenciado é truncado e o código do agente não é completamente exibido.

Configurando o Agente em Sistemas Windows

Você pode utilizar o IBM Cloud Application Performance Management janela para configurar o agente em sistemas Windows.

Procedimento

1. Clique em **Iniciar > Todos os Programas > Agentes IBM Monitoring > IBM Performance Management**.
2. Na janela **IBM Performance Management**, conclua estas etapas:
   a) Dê um clique duplo no modelo **Monitoring Agent for MySQL**.
   b) Na janela **Monitoring Agent for MySQL**, especifique um nome de instância e clique em **OK**.
3. Na janela **Monitoring Agent for MySQL**, conclua estas etapas:
   a) No campo **Endereço IP**, insira o endereço IP de um servidor MySQL que você deseja monitorar remotamente. Se o agente estiver instalado no servidor a ser monitorado, retenha o valor padrão.
   b) No campo **Nome do usuário do JDBC**, insira o nome de um usuário do servidor MySQL. O valor padrão é raiz.
   c) No campo **Senha de JDBC**, digite a senha de um usuário JDBC.
   d) No campo **Confirmar senha de JDBC**, digite a senha novamente.
   e) No campo **Arquivo Jar JDBC**, clique em **Procurar** e localize o diretório que contém o arquivo Java do conector MySQL e selecione-o.
   f) Clique em **Avançar**.
   g) No campo **Número de porta JDBC**, especifique o número da porta do servidor JDBC.
   O número da porta padrão é 3306.
   h) Na lista **Nível de rastreio de Java**, selecione um nível de rastreio para Java.
   O valor padrão é `Error`.

i) Clique em **OK**.

A instância é exibida na janela **IBM Performance Management**.

4. Clique com o botão direito na instância **Monitoring Agent for MySQL** e clique em **Iniciar**.

   Lembre-se: Para configurar o agente novamente, conclua estas etapas na janela **IBM Performance Management**:

   a. Pare a instância do agente que você deseja configurar.

   b. Clique com o botão direito na instância **Monitoring Agent for MySQL** e clique em **Reconfigurar**.

   c. Repita as etapas 3 e 4.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o agente nos sistemas Linux

Execute o script de configuração para configurar o agente nos sistemas Linux.

Procedimento

1. Execute o seguinte comando:

   ```
   install_dir/bin/mysql-agent.sh config instance_name
   ```

   Em que *instance_name* é o nome a ser fornecido para a instância e *install_dir* é o diretório de instalação do Agente MySQL.

2. Quando for solicitado para inserir um valor para os parâmetros a seguir, pressione Enter para aceitar o valor padrão, ou especifique um valor diferente e pressione enter.

   - Endereço IP
   - nome de usuário JDBC
   - senha JDBC
   - Digite a senha JDBC novamente
   - Arquivo JAR JDBC
   - Número da porta JDBC (O número da porta padrão é 3306.)
   - Nível de rastreio Java (O valor padrão é `Error`.)

   Para obter informações sobre os parâmetros de configuração, consulte "Configurando o agente usando o arquivo de resposta silencioso" na página 578.

3. Execute o seguinte comando para iniciar o agente.

   ```
   install_dir/bin/mysql-agent.sh start instance_name
   ```

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o agente usando o arquivo de resposta silencioso

Use o arquivo de resposta silencioso para configurar o agente sem responder aos prompts ao executar o script de configuração. É possível usar o arquivo de resposta silencioso para configurar o agente nos sistemas Windows e Linux.

Sobre Esta Tarefa

O arquivo de resposta silencioso contém os parâmetros de configuração. É possível editar os valores de parâmetros no arquivo de resposta e executar o script de configuração para criar uma instância do agente e atualizar os valores de configuração.

Procedimento

1. Em um editor de texto, abra o arquivo de resposta que está disponível no caminho a seguir:

   Linux *install_dir*/samples/mysql_silent_config.txt

   Windows *install_dir*\samples\mysql_silent_config.txt

   Em que *install_dir* é o diretório de instalação do Agente MySQL.
2. No arquivo de resposta, especifique um valor para os parâmetros a seguir:
   - Para o parâmetro **Server Name**, especifique o endereço IP de um servidor MySQL que você deseja monitorar remotamente. Caso contrário, retenha o valor padrão como `localhost`.
   - Para o parâmetro **Nome do usuário JDBC**, retenha o valor do nome do usuário padrão de `root` ou especifique o nome de um usuário com privilégios para visualizar as tabelas INFORMATION_SCHEMA.
   - Para o parâmetro **JDBC password**, insira uma senha de usuário JDBC.
   - Para o parâmetro **JDBC Jar File**, mantenha o caminho padrão se esse caminho para o conector MySQL para o arquivo jar Java estiver correto. Caso contrário, insira o caminho correto. O conector está disponível no caminho padrão a seguir:

     Linux `/usr/share/java/mysql-connector-java.jar`

     Windows `C:\Program Files (x86)\MySQL\Connector J 5.1.26\mysql-connector-java-5.1.26-bin.jar`
   - Para o parâmetro **JDBC port number**, mantenha o número da porta padrão de 3306 ou especifique um número de porta diferente.
   - Para o parâmetro **Java trace level**, mantenha o valor padrão de `Error` ou especifique um nível diferente de acordo com as instruções de suporte IBM.
3. Salve e feche o arquivo de resposta e execute o seguinte comando para atualizar definições de configuração do agente:

   Linux *install_dir*/bin/mysql-agent.sh config *instance_name install_dir*/samples/mysql_silent_config.txt

   Windows *install_dir*\BIN\mysql-agent.bat config *instance_name install_dir* \samples\mysql_silent_config.txt

   Em que *instance_name* é o nome a ser fornecido para a instância e *install_dir* é o diretório de instalação do Agente MySQL.

   Importante: Certifique-se de incluir o caminho absoluto no arquivo de resposta silenciosa. Caso contrário, nenhum dado do agente será exibido nos painéis.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o monitoramento do NetApp Storage

O Monitoring Agent for NetApp Storage monitora os sistemas de armazenamento NetApp usando o NetApp OnCommand Unified Manager, o OnCommand API Services e o OnCommand Performance Manager.

Antes de Iniciar

- Revise os pré-requisitos de hardware e software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Agente NetApp Storage.
- Certifique-se de que os seguintes componentes estejam instalados em sua máquina:
  - OnCommand Unified Manager
  - OnCommand Performance Manager
  - OnCommand API Services

  Para obter informações sobre como instalar esses componentes, consulte a documentação do NetApp.
- Certifique-se de que as versões do OnCommand API Services, do OnCommand Unified Manager e do OnCommand Performance Manager sejam compatíveis. Por exemplo, para configurar o OnCommand API Services V1.0, emparelhe o OnCommand Unified Manager V6.2, V6.1 ou V6.0 com o OnCommand Performance Manager V1.1. Para versões do produto compatíveis, consulte o Interoperability Matrix Tool.
- Certifique-se de que o usuário, que se conecta ao OnCommand Unified Manager, tenha o privilégio GlobalRead para o sistema de armazenamento NetApp que está sendo monitorado. Use um ID do usuário existente com esse privilégio ou crie um novo ID do usuário. Para obter informações sobre como criar o ID do usuário em seu sistema de armazenamento NetApp, consulte a documentação do NetApp.
- Certifique-se de que o usuário, que é usado para configurar o OnCommand API Services, sejam um administrador ou um monitor. Esses tipos de usuário têm permissões padrão para executar a API rest.
- Faça download do arquivo JAR do NetApp Manageability SDK (`manageontap.jar`) no website do NetApp e instale o arquivo no diretório `lib` do agente de monitoramento, concluindo as etapas mencionadas em "Fazendo download e instalando o arquivo JAR NetApp Manageability SDK" na página 580.

Sobre Esta Tarefa

O Agente NetApp Storage é um agente de múltiplas instâncias. Deve-se criar a primeira instância e iniciar o agente manualmente.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte o "Histórico de Mudanças" na página 50.

- Para configurar o agente em sistemas Windows, é possível usar a janela **IBM Performance Management** ou o arquivo silencioso de resposta.
- Para configurar o agente em sistemas Linux, é possível executar o script e responder aos prompts, ou usar o arquivo silencioso de resposta.

Fazendo download e instalando o arquivo JAR NetApp Manageability SDK

O Agente NetApp Storage requer o arquivo JAR do NetApp Manageability SDK para se comunicar com um servidor NetApp OCUM.

Sobre Esta Tarefa

Depois de instalar o Agente NetApp Storage, faça download do arquivo JAR do NetApp Manageability SDK (`manageontap.jar`) no website do NetApp e instale o arquivo no diretório `lib` do agente de monitoramento.

Procedimento

1. Faça download do arquivo compactado que contém o arquivo JAR no seguinte website: http://communities.netapp.com/docs/DOC-1152.
2. Extraia esse arquivo compactado e copie o arquivo `manageontap.jar` para os seguintes locais:
   - Para sistemas Windows de 32 bits, copie o arquivo em *install_dir*`/tmaitm6`
   - Para sistema Windows de 64 bits, copie o arquivo em *install_dir*`/tmaitm6_x64`
   - Para sistemas Linux de 32 bits, copie o arquivo para *install_dir*`/li6263/nu/lib`
   - Para sistemas Linux x86-64 de 64 bits, copie o arquivo para *install_dir*`/lx8266/nu/lib`
   - Para sistemas zLinux de 64 bits, copie o arquivo para *install_dir*`/ls3266/nu/lib`

O que Fazer Depois
Conclua a configuração do agente.

Configurando o agente nos sistemas Windows

É possível configurar o agente em sistemas operacionais Windows usando a janela **IBM Performance Management**. Após fazer a atualização dos valores de configuração, deve-se iniciar o agente para salvar os valores atualizados.

Sobre Esta Tarefa

O Agente NetApp Storage fornece valores padrão para alguns parâmetros. É possível especificar diferentes valores para esses parâmetros.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito em **Monitoring Agent for NetApp Storage** e, em seguida, clique em **Configurar agente**.

   Lembre-se: Após você configurar o agente pela primeira vez, a opção **Configurar Agente** é desativada. Para configurar o agente novamente, clique em **Reconfigurar**.
3. Na janela Monitoring Agent for NetApp Storage, conclua as seguintes etapas:
   a) Insira um nome exclusivo para a instância do Agente NetApp Storage e clique em **OK**.
   b) Na guia **Provedor de Dados**, especifique valores para os parâmetros de configuração e clique em **Avançar**.
   c) Na guia **OnCommand Unified Manager**, especifique valores para os parâmetros de configuração e, em seguida, clique em **Avançar**.
   d) Na guia **OnCommand API Service**, especifique valores para os parâmetros de configuração e, em seguida, clique em **OK**.

   Para obter informações sobre os parâmetros de configuração em cada guia da janela Monitoring Agent for NetApp Storage, consulte os seguintes tópicos:

   - "Parâmetros de configuração para o provedor de dados" na página 584
   - "Parâmetros de configuração para o OnCommand Unified Manager" na página 585
   - "Parâmetros de configuração para o Serviço de API OnCommand" na página 586

4. Na janela **IBM Performance Management**, clique com o botão direito em **Monitoring Agent for NetApp Storage** e, em seguida, clique em **Iniciar**.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.

Configurando o agente usando o arquivo silencioso de resposta

O arquivo de resposta silencioso contém os parâmetros de configuração do agente. É possível editar o arquivo de resposta silencioso para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

O arquivo silencioso de resposta contém os parâmetros de configuração do agente com valores padrão que são definidos para alguns parâmetros. É possível editar o arquivo silencioso de resposta para especificar os valores diferentes para os parâmetros de configuração.

Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

- Para configurar o Agente NetApp Storage no modo silencioso, conclua as seguintes etapas:
  a) Em um editor de texto, abra o arquivo `netapp_storage_silent_config.txt` que está disponível no seguinte caminho:
     – Linux *install_dir*`/samples/netapp_storage_silent_config.txt`

       Exemplo `/opt/ibm/apm/agent/samples/netapp_storage_silent_config.txt`
     – Windows *install_dir*`\samples\netapp_storage_silent_config.txt`

       Exemplo `C:\IBM\APM\samples\netapp_storage_silent_config.txt`
  b) No arquivo `netapp_storage_silent_config.txt`, especifique valores para todos os parâmetros obrigatórios. Também é possível modificar os valores padrão de outros parâmetros.

     Para obter informações sobre os parâmetros de configuração, consulte os tópicos a seguir:
     – "Parâmetros de configuração para o provedor de dados" na página 584
     – "Parâmetros de configuração para o OnCommand Unified Manager" na página 585
     – "Parâmetros de configuração para o Serviço de API OnCommand" na página 586
  c) Salve e feche o arquivo `netapp_storage_silent_config.txt` e execute o seguinte comando:
     – Linux *install_dir*`/bin/netapp_storage-agent.sh config` *instance_name* *install_dir*`/samples/netapp_storage_silent_config.txt`

       Exemplo **`/opt/ibm/apm/agent/bin/netapp_storage-agent.sh config instance_name /opt/ibm/apm/agent/samples/ netapp_storage_silent_config.txt`**
     – Windows *install_dir*`\bin\netapp_storage-agent.bat config` *instance_name* *install_dir*`\samples\netapp_storage_silent_config.txt`

       Exemplo **`C:\IBM\APM\bin\netapp_storage-agent.bat config instance_name C:\IBM\APM\samples\netapp_storage_silent_config.txt`**

       Em que

instance_name
O nome que você deseja fornecer para a instância.

install_dir
Caminho onde o agente está instalado.

Importante: Assegure que você inclua o caminho absoluto no arquivo silencioso de resposta. Caso contrário, os dados do agente não serão mostrados nos painéis.

d) Execute o comando a seguir para iniciar o agente:

– Linux *install_dir*/bin/netapp_storage-agent.sh start *instance_name*

Exemplo **/opt/ibm/apm/agent/bin/netapp_storage-agent.sh start instance_name**

– Windows *install_dir*\bin\netapp_storage-agent.bat start *instance_name*

Exemplo **C:\IBM\APM\bin\netapp_storage-agent.bat start instance_name**

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.

Configurando o agente respondendo aos prompts

Para configurar o agente em sistemas Linux, deve-se executar o script e responder aos prompts.

Procedimento

1. Na linha de comandos, digite o seguinte comando:

   install_dir/bin/netapp_storage-agent.sh config *instance_name*

   Exemplo **/opt/ibm/apm/agent/bin/netapp_storage-agent.sh config instance_name**

   Em que

   instance_name
   O nome que você deseja fornecer para a instância.

   install_dir
   Caminho onde o agente está instalado.
2. Responda aos prompts consultando os seguintes tópicos:
   - "Parâmetros de configuração para o provedor de dados" na página 584
   - "Parâmetros de configuração para o OnCommand Unified Manager" na página 585
   - "Parâmetros de configuração para o Serviço de API OnCommand" na página 586
3. Execute o comando a seguir para iniciar o agente:

   install_dir/bin/netapp_storage-agent.sh start *instance_name*

   Exemplo **/opt/ibm/apm/agent/bin/netapp_storage-agent.sh start instance_name**

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.

Parâmetros de configuração para o provedor de dados

Quando você configura o Agente NetApp Storage, pode mudar os valores padrão dos parâmetros para o provedor de dados, como o número máximo de arquivos de log do provedor de dados, o tamanho máximo do arquivo de log e o nível de detalhes incluídos no arquivo de log.

A tabela a seguir contém descrições detalhadas dos parâmetros de configuração para o provedor de dados.

Tabela 184. Nomes e descrições dos parâmetros de configuração para o provedor de dados

Nome de parâmetro	Descrição	Campo obrigatório
Nome da instância (**KNU_INSTANCE_NAME**)	O nome da instância. **Restrição:** O campo Nome da instância exibe o nome da instância especificada ao configurar o agente pela primeira vez. Ao configurar o agente novamente, não é possível mudar o nome da instância do agente.	Sim
Número máximo de arquivos de log do provedor de dados (**KNU_LOG_FILE_MAX_COUNT**)	O número máximo de arquivos de log que o provedor de dados cria antes de sobrescrever os arquivos de log anteriores. O valor padrão é 10.	Sim
Tamanho máximo, em KB, de cada log do provedor de dados (**KNU_LOG_FILE_MAX_SIZE**)	O tamanho máximo em KB que um provedor de dados deve atingir antes de o provedor de dados criar um novo arquivo de log. O valor padrão são 5190 KB.	Sim

Tabela 184. Nomes e descrições dos parâmetros de configuração para o provedor de dados (continuação)		
Nome de parâmetro	**Descrição**	**Campo obrigatório**
Nível de detalhe no log do provedor de dados (**KNU_LOG_LEVEL**)	O nível de detalhes que pode ser incluído no arquivo de log criado pelo provedor de dados. O valor padrão é 4 (Informativo). Os seguintes valores são válidos: • 1 (Desativado): nenhuma mensagem é registrada. • 2 (Grave): somente erros são registrados. • 3 (Aviso): todos os erros e mensagens que são registrados no nível Grave e erros potenciais que podem resultar em comportamento indesejado. • 4 (Informativo): todos os erros e mensagens que são registrados no nível de Aviso e as mensagens informativas de alto nível que descrevem o estado do provedor de dados quando ele é processado. • 5 (Bom): todos os erros e mensagens que são registrados no nível Informativo e mensagens informativas de baixo nível que descrevem o estado do provedor de dados quando ele é processado. • 6 (Melhor): todos os erros e mensagens que são registrados no nível Bom, além de mensagens informativas altamente detalhadas, como informações de criação de perfil de desempenho e dados de depuração. Selecionar essa opção pode afetar de maneira adversa o desempenho do agente de monitoramento. Esta configuração é destinada apenas como uma ferramenta para determinação de problema em conjunto com a equipe de suporte IBM. • 7 (Excelente): todos os erros e mensagens que são registrados no nível Bom e as mensagens informativas mais detalhadas que incluem mensagens de programação de baixo nível e dados. Escolher essa opção pode afetar, de maneira adversa, o desempenho do agente de monitoramento. Esta configuração é destinada apenas como uma ferramenta para determinação de problema em conjunto com a equipe de suporte IBM. • 8 (Todos): todos os erros e mensagens são registrados.	Sim

Parâmetros de configuração para o OnCommand Unified Manager

Ao configurar o Agente NetApp Storage, é possível mudar os valores padrão dos parâmetros para o OnCommand Unified Manager (OCUM), como o endereço IP do servidor OCUM, nome do usuário e senha.

A tabela a seguir contém descrições detalhadas dos parâmetros de configuração para a origem de dados.

Tabela 185. Nomes e descrições dos parâmetros de configuração para o OnCommand Unified Manager		
Nome de parâmetro	**Descrição**	**Campo obrigatório**
Servidor (**KNU_DATASOURCE_HOST_ADDRESS**)	O nome do host ou endereço IP do servidor NetApp OCUM a ser monitorado.	Sim

Tabela 185. Nomes e descrições dos parâmetros de configuração para o OnCommand Unified Manager (continuação)		
Nome de parâmetro	**Descrição**	**Campo obrigatório**
Usuário (**KNU_DATASOURCE_USERNAME**)	Um nome de usuário no servidor NetApp OCUM com privilégios suficientes para coletar dados. O valor padrão é admin.	Sim
Senha (**KNU_DATASOURCE_PASSWORD**)	A senha do usuário especificada no parâmetro **User**.	Sim
Confirmar Senha	A mesma senha que foi especificada no parâmetro **Enter Password**.	Sim
Protocolo (**KNU_DATASOURCE_PROTOCOL**)	O protocolo a ser usado para comunicação com o servidor NetApp OCUM. O valor padrão é HTTPS.	Sim

Parâmetros de configuração para o Serviço de API OnCommand

Ao configurar o Agente NetApp Storage, é possível mudar os valores padrão dos parâmetros para o Serviço de API OnCommand, como o endereço do host, nome do usuário e senha.

A tabela a seguir contém descrições detalhadas dos parâmetros de configuração para a origem de dados.

Tabela 186. Nomes e descrições dos parâmetros de configuração para o Serviço da API OnCommand		
Nome de parâmetro	**Descrição**	**Campo obrigatório**
Endereço do host (**KNU_API_SERVICES_HOST_ADDRESS**)	O nome do host ou endereço IP do serviço da API OnCommand.	Sim
Usuário (**KNU_API_SERVICES_USERNAME**)	Um nome do usuário com privilégios suficientes para conectar-se ao serviço da API OnCommand. O valor padrão é admin.	Sim
Senha (**KNU_API_SERVICES_PASSWORD**)	A senha do usuário especificada no parâmetro **User**.	
Confirmar Senha	A mesma senha que foi especificada no parâmetro **Enter Password**.	Sim

Configurando o monitoramento do Node.js

É possível usar o agente do Node.js ou o coletor de dados Node.js independente para monitorar seus aplicativos Node.js. Se quiser uma função de rastreamento de transação e um processo de instalação mais simples, use o coletor de dados Node.js.

Antes de Iniciar

- As orientações aqui são para a liberação mais atual desse agente e coletor de dados. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte “Histórico de Mudanças” na página 50.

- Certifique-se de que os requisitos do sistema para o Agente Node.js ou Coletor de dados Node.js sejam atendidos em seu ambiente.
  - Para obter informações atualizadas sobre o requisito do sistema do Agente Node.js, consulte Software Product Compatibility Reports (SPCR) para o Agente Node.js.
  - Para obter informações atualizadas sobre o requisito do sistema do Coletor de dados Node.js, consulte Software Product Compatibility Reports (SPCR) para o Coletor de dados Node.js.

Sobre Esta Tarefa

O procedimento a seguir é um roteiro para configurar o Monitoring Agent for Node.js e o coletor de dados Node.js independente, que inclui etapas obrigatórias e opcionais.

- Para monitorar aplicativos no local, é possível configurar o Coletor de dados Node.js independente ou o Agente Node.js. Se desejar ativar o rastreamento de transação para seus aplicativos Node.js, configure o coletor de dados independente.
- Para monitorar o IBM Cloud (antigo Bluemix) ou aplicativos Kubernetes, configure o Coletor de dados Node.js independente.

Conclua as etapas a seguir, de acordo com suas necessidades.

Procedimento

- Configure o Agente Node.js para monitorar os aplicativos no local.
  a) Inclua um coletor de dados do agente nos aplicativos Node.js para que o agente funcione corretamente. Consulte “Configurando o Agente Node.js” na página 587.
  b) Opcional: Para mudar o comportamento de monitoramento de seu agente, consulte Configurando o coletor de dados do Agente Node.js.
  c) Opcional: Para configurar a coleta e exibição de dados diagnósticos, consulte Configurando o coletor de dados diagnósticos.
- Configure o Coletor de dados Node.js para monitorar os aplicativos IBM Cloud.
  a) Para configurar o Coletor de dados Node.js, consulte “Configurando o Coletor de dados Node.js independente para aplicativos IBM Cloud(antigo Bluemix)” na página 593.
  b) Para mudar o comportamento do Coletor de dados Node.js independente, consulte “Customizando o coletor de dados Node.js independente para aplicativos IBM Cloud” na página 595.
- Configure o Coletor de dados Node.js independente para monitorar aplicativos no local.
  a) Para configurar o Coletor de dados Node.js, consulte “Configurando o Coletor de dados Node.js para aplicativos no local” na página 598.
  b) Para mudar o comportamento do Coletor de dados Node.js independente, consulte “Customizando o Coletor de dados Node.js para aplicativos no local” na página 600.
- Configure o Coletor de dados Node.js independente para monitorar aplicativos no Kubernetes.
  a) Para configurar o Coletor de dados Node.js, consulte “Configurando o Coletor de dados Node.js independente para aplicativos Kubernetes” na página 604.
  b) Para mudar o comportamento do Coletor de dados Node.js independente, consulte “Customizando o coletor de dados Node.js independente para aplicativos Kubernetes” na página 605.

Configurando o Agente Node.js

Deve-se incluir um coletor de dados do agente para o seu aplicativo Node.js e reiniciá-lo antes que o agente possa iniciar o monitoramento de seu aplicativo.

Antes de Iniciar

Antes de redefinir as configurações do agente na mesma versão, use as etapas a seguir para limpar os arquivos do coletor de dados que foram criados pela configuração anterior:

1. Acesse o diretório *install_dir*/lx8266/nj/bin.

2. Execute o comando `./uninstall.sh` para remover arquivos do coletor de dados existentes.

Sobre Esta Tarefa

O agente Node.js é um agente de instância única. Ele registra os subnós para cada aplicativo Node.js monitorado. O subnó está na seguinte estrutura:

`NJ:hostname_port:NJA`

Dica: Se um aplicativo Node.js atende em vários números de porta, o número da porta mais baixo será utilizado.

Deve-se incluir um coletor de dados do agente para o seu aplicativo Node.js e reiniciar seu aplicativo antes que o agente possa iniciar o monitoramento de seu aplicativo. Os coletores de dados do agente coletam dados que são encaminhados para o agente Node.js. Atualmente, os coletores de dados do agente a seguir são fornecidos:

- O coletor de dados de recurso coleta dados de monitoramento de recurso de seus aplicativos Node.js.
- O coletor de dados diagnósticos coleta dados diagnósticos e dados de monitoramento de recurso de seus aplicativos Node.js.
- O coletor de dados de rastreio de método coleta rastreios de método, dados diagnósticos e dados de monitoramento de recurso de seus aplicativos Node.js.

Procedimento

1. Certifique-se de que o ID do usuário usado para executar o servidor de aplicativos tenha permissão completa para o diretório `install_dir` do agente.
2. Acesse o diretório *`install_dir`*`/bin` e execute o seguinte comando:

   ```
   ./nodejs-agent.sh config
   ```

3. Siga os prompts para especificar valores para as seguintes opções de configuração:

   KNJ_NODEJS_RUNTIME_BIN_LOCATION
   O diretório para a pasta `bin` do tempo de execução do Node.js. O diretório padrão é `/usr/local/bin`.

   KNJ_NPM_RUNTIME_BIN_LOCATION
   O diretório para a pasta `bin` executando o comando **npm**. O diretório padrão é `/usr/local/bin`.

   KNJ_NPM_LIB_LOCATION
   O diretório para a pasta `lib` do diretório de instalação global do pacote npm. O diretório padrão é `/usr/local/lib`. Por exemplo, se você instalar o pacote npm executando o comando `npm install -g`, o pacote será instalado em */nodejs_home*`/lib/node_modules` e o **KNJ_NPM_LIB_LOCATION** será */nodejs_home*`/lib`.

   CP_PORT
   A porta na qual o agente recebe dados de clientes do soquete. Um valor `0` indica que uma porta efêmera será usada. O valor padrão é `63336`.

   Nota: Não use o número da porta que já está em uso em seu sistema. Para verificar se a porta já está em uso, execute o comando `netstat -apn | grep` *`port_number`*.

4. Inicie o agente executando o seguinte comando:

   ```
   ./nodejs-agent.sh start
   ```

5. Verifique se o Agente Node.js foi iniciado com sucesso. A pasta *`KNJ_NPM_LIB_LOCATION`*`/node_modules/ibmapm` será gerada se o agente for iniciado com sucesso.
6. Com base em sua oferta e em seus requisitos, insira uma das seguintes entradas no arquivo `.js` de seu aplicativo Node.js para configurar os coletores de dados do agente:

Nota: Somente uma entrada pode ser incluída em seu aplicativo Node.js para ativar as capacidades do coletor de dados do agente. Além disso, se você ativar capacidades que não estão incluídas na oferta, pode ocorrer sobrecarga desnecessária, o que diminui a eficiência de execução do aplicativo.

- Se você tiver somente capacidades de monitoramento de recursos, é possível incluir o coletor de dados de recurso. Para incluí-lo, insira a seguinte linha no início do arquivo de aplicativo Node.js:

  ```
  require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm');
  ```

  Se o valor de **KNJ_NPM_LIB_LOCATION** em seu ambiente for `/usr/local/lib`, a linha será

  ```
  require('/usr/local/lib/node_modules/ibmapm');
  ```

- Se você tiver diagnósticos além das capacidades de monitoramento no nível de recurso, será possível optar por incluir um dos coletores de dados do agente a seguir:
  - Para incluir o coletor de dados de rastreio de método, insira a seguinte linha no início do arquivo de aplicativo Node.js:

    ```
    require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm/methodtrace.js');
    ```

  - Para incluir o coletor de dados diagnósticos, insira a seguinte linha no início do arquivo de aplicativo Node.js:

    ```
    require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm/deepdive.js');
    ```

  - Para incluir o coletor de dados de monitoramento de recurso, insira a seguinte linha no início do arquivo de aplicativo Node.js:

    ```
    require('KNJ_NPM_LIB_LOCATION/node_modules/ibmapm');
    ```

  Para garantir melhor desempenho, inclua o coletor de dados de rastreio de método somente para propósitos de depuração.

Nota: O código dos plug-ins muda a partir do Cloud APM, março de 2017. Se você fizer upgrade de seu agente de versões anteriores, deverá atualizar o código de coletores de dados existentes em seus aplicativos para que a capacidade de monitoramento funcione corretamente.

7. Reinicie o aplicativo Node.js para ativar o coletor de dados do agente.

Resultados
Você configurou com sucesso o Agente Node.js.

O que Fazer Depois

- Agora é possível verificar se os dados do Agente Node.js são exibidos no console do Cloud APM. Para obter instruções sobre como iniciar o console do Cloud APM, consulte Iniciando o console do Cloud APM. Para obter informações sobre o uso do Editor de aplicativos, consulte Gerenciando aplicativos.

  Importante: Para incluir seu aplicativo no Console do Cloud APM, escolha **Node.js** no editor de aplicativos.
- É possível mudar o comportamento do tempo de execução dos coletores de dados do agente Node.js. Para obter mais informações, consulte Configurando o coletor de dados do agente Node.js.
- É possível ativar a coleta de dados diagnósticos e exibir configurando o coletor de dados diagnósticos. Para obter mais informações, consulte Configurando o coletor de dados diagnósticos.

Configurando o coletor de dados do Agente Node.js
É possível mudar o comportamento de cada coletor de dados do agente Node.js mudando sua configuração de tempo de execução em seu arquivo de configuração.

Arquivo de configuração do Runtime

O código do coletor de dados Node.js está no seguinte diretório:

KNJ_NPM_LIB_LOCATION/node_modules/ibmapm

em que *KNJ_NPM_LIB_LOCATION* é o diretório para a pasta lib do diretório de instalação global do pacote npm. O diretório padrão é /usr/local/lib.

Também há um arquivo de configuração de tempo de execução para cada coletor de dados do agente na mesma pasta. O coletor de dados do agente lê o arquivo de configuração a cada minuto.

Dica: O arquivo de configuração de tempo de execução é nomeado no seguinte formato:

plugin_*application port number*_conf.json

Ao mudar o conteúdo do arquivo de configuração, o comportamento do coletor de dados do agente associado também muda. Há dois tipos de informações no arquivo de configuração que podem ser mudados:

- Regras de filtragem da URL
- coletor de dados do agente parâmetros de criação de log

Regras de filtragem da URL

É possível mudar as regras de filtragem da URL no arquivo de configuração de tempo de execução. Expressões regulares são usadas para mapear o nome do caminho da URL para um nome do caminho customizado do usuário. É possível mapear a URL para um nome do caminho customizado para atender os seguintes requisitos:

- Agregar URLs com caminhos semelhantes. Por exemplo, você tem os seguintes caminhos de URL:

  ```
  /demo/poll/1
  /demo/poll/2
  /demo/poll/3
  ...
  ```

  No servidor da web, as solicitações para esses caminhos são provavelmente atendidas por uma rotina comum, de modo que é possível agregar os caminhos para um tipo de URL único usando o filtro no exemplo a seguir.

  ```
  "filters":
  [
      {
          "pattern": "/demo/poll/.+",
          "to": "/demo/poll/"
      }
  ```

  Esse filtro faz com que todas as solicitações para caminhos de URL, como "/demo/poll/xxx", sejam mapeadas para um tipo de caminho de URL de "/demo/poll". O tempo de resposta para todas as solicitações para caminhos de URL desse tipo tem então sua média calculada para um valor único. A agregação feita dessa forma pode ajudar a utilização mais eficiente dos recursos disponíveis.
- Ignorando caminhos de URL para arquivos estáticos ou filtrando determinados tipos de solicitações. Por exemplo, se uma página da web inclui imagens que geram solicitações separadas de download do servidor, pode não ser interessante ver os tempos de resposta para esses tipos de solicitações.

  Para filtrar um tipo de solicitação, configure o valor "to" para vazio como no formato do seguinte exemplo:

  ```
  "filters":
  [
      {
          "pattern": "GET /css/.+\\.css$",
          "to": ""
      }
  ```

  Esse filtro faz as solicitações para obter um arquivo .css serem ignoradas. Como resultado, é possível usar os recursos disponíveis de forma mais eficiente nas solicitações que precisam ser monitoradas.

No arquivo de configuração, as regras de filtragem de URL são fornecidas em uma matriz JSON chamada `filters`:

```
"filters":
[
    {
        "pattern": ".+\\.png$",
        "to": ""
    },
    {
        "pattern": ".+\\.jpg$",
        "to": ""
    },
    {
        "pattern": "GET /js/.+\\.js$",
        "to": ""
    },
    {
        "pattern": "GET /css/.+\\.css$",
        "to": ""
    }
]
```

Cada membro na matriz é uma regra de filtragem. Quando uma solicitação de HTTP é recebida pelo coletor de dados do agente, o coletor de dados do agente extrai o nome do caminho da URL da solicitação e o compara com cada `"pattern"`. Se o nome do caminho não corresponder a `"pattern"`, o nome do caminho da URL original será mantido e usado para medições.

Parâmetro de log do coletor de dados do agente

É possível mudar o comportamento de criação de log modificando o parâmetro no arquivo de configuração `config.properties` no diretório *KNJ_NPM_LIB_LOCATION*`/node_modules/ibmapm/etc`. O parâmetro de criação de log a seguir é fornecido para você mudar:

O nível de log
A entrada no arquivo de configuração para o nível de log é `KNJ_LOG_LEVEL=info`, o que significa que as informações de resumo sobre as ações são impressas no log. É possível configurar o nível de log mudando o valor de `KNJ_LOG_LEVEL`. O valor padrão é `info` e o log é impresso na saída padrão.

Os cinco valores de nível de log a seguir são suportados:

desligado
Os logs não são impressos.

error
As informações são registradas somente em uma condição de erro.

informações
As informações serão registradas quando o coletor de dados Agente Node.js estiver executando normalmente. Os dados brutos de monitoramento que são enviados para o agente também são registrados.

debug
A depuração, as informações e as informações de erro são impressas no log, por exemplo, dados coletados, dados que são enviados para o servidor e resposta do servidor.

Todos
Todas as informações são impressas no log.

Configurando o coletor de dados diagnósticos do Agente Node.js

O suporte para coleta de dados diagnósticos está desativado por padrão. Se você tiver recursos diagnósticos, deve-se configurar e ajustar a coleção de dados para aplicativos Node.js específicos.

Procedimento

- Para modificar as configurações do coletor de dados de um aplicativo específico que está em execução:

1. Navegue para o diretório *KNJ_NPM_LIB_LOCATION*/node_modules/ibmapm, e abra o arquivo plugin_*port*_conf.json em um editor de texto.

   Dica: Para obter informações sobre *KNJ_NPM_LIB_LOCATION*, consulte a descrição de parâmetro do "KNJ_NPM_LIB_LOCATION" na página 588

2. Use a tabela a seguir para obter informações sobre como modificar as configurações do coletor de dados:

Tabela 187. Configurações do coletor de dados

Categoria de dados diagnósticos	Descrição	Propriedade	Ação
Delta de tempo mínimo para relatório de rastreio de pilha	Especifica o limite de tempo de resposta para coletar o rastreio de pilha de uma solicitação ou uma chamada de método. Se o tempo de resposta de uma solicitação ou chamada de método exceder esse valor, o coletor de dados coletará seu rastreio de pilha.	minClockStack	Configure como um valor em milissegundos
Delta de tempo mínimo para solicitações de relatório	Especifica o limite de tempo de resposta para coletar o rastreio de método de uma instância de solicitação. Se o tempo de resposta de uma instância de solicitação exceder esse limite, o coletor de dados coletará seu rastreio de método.	minClockTrace	Configure como um valor em milissegundos
Número máximo de eventos por arquivo	Especifica o número máximo de eventos a serem registrados em um arquivo .jso. O arquivo .jso registra os dados diagnósticos para esses eventos.	eventsPerFile	Configure como um número máximo de valor dos eventos

Tabela 187. Configurações do coletor de dados (continuação)			
Categoria de dados diagnósticos	**Descrição**	**Propriedade**	**Ação**
Quantia máxima de tempo a ser relatada a um arquivo	Especifica a quantidade máxima de tempo para o arquivo `.jso` registrar dados diagnósticos	`fileCommitTime`	Configure como o tempo máximo em segundos
Número máximo de arquivos a serem mantidos antes que os mais antigos sejam excluídos	Especifica o número máximo de arquivos `.jso` a serem mantidos antes de os mais antigos serem excluídos.	`maxFiles`	Configure como o número máximo de arquivos
Período de amostragem de solicitação	Especifica o período de amostragem para solicitações.	`sampling`	Configure como o período de amostragem desejado. O valor padrão é `10`. Um valor de `10` significa que o agente coleta uma de cada 10 solicitações.

- Opcional: Configure a variável de ambiente *SECURITY_OFF* se desejar que o coletor de dados de diagnósticos colete informações confidenciais do usuário, como cookies, contextos de solicitação de HTTP e contexto de solicitações do banco de dados. Essas informações não são coletadas por padrão.

  Tenha cuidado ao configurar esta variável, porque ela pode causar o vazamento de informações.

  Linux Por exemplo, para configurar esta variável de ambiente, emita o seguinte comando:

  ```
  export SECURITY_OFF=true
  ```

Resultados

A configuração do coletor de dados diagnósticos será alterada para o aplicativo em execução que você especificou ou para todos os aplicativos.

Configurando o Coletor de dados Node.js independente para aplicativos IBM Cloud(antigo Bluemix)

Para coletar informações sobre aplicativos Node.js no IBM Cloud, deve-se configurar o Coletor de dados Node.js.

Antes de Iniciar

1. Certifique-se de que o aplicativo Node.js possa ser executado localmente com sucesso. O Coletor de dados Node.js independente pode monitorar os fix packs Node.js V8.0.0 e futuros, fix packs V10.0.0 e futuros e fix packs V12.0.0 e futuros.
2. Faça download do pacote coletor de dados no IBM Marketplacewebsite do . Para obter instruções detalhadas, consulte “Fazendo download de seus agentes e coletores de dados” na página 101.

Procedimento

1. Extraia os arquivos do pacote do coletor de dados. O pacote `nodejs_datacollector_8.1.4.0.6.tgz` é incluído no diretório extraído.
2. Extraia o arquivo `nodejs_datacollector_8.1.4.0.6.tgz`, por exemplo, executando o seguinte comando:

```
tar -zxf nodejs_datacollector_8.1.4.0.6.tgz
```

3. Extraia o arquivo `ibmapm.tgz` na pasta `nodejs_dc` executando o comando a seguir:

```
tar -zxf nodejs_dc/ibmapm.tgz
```

   Você obterá uma pasta `ibmapm`.

4. Copie a pasta `ibmapm` extraída do pacote coletor de dados para o diretório inicial de seu aplicativo, por exemplo, executando o seguinte comando:

```
cp –r directory_to_the_ibmapm_folder  home_directory_of_your_Node.js_application
```

   Dica: O diretório inicial de seu aplicativo Node.js é determinado pelo comando usado para iniciar o aplicativo Node.js e o diretório que contém o arquivo principal. Se você usar o comando **node app.js** para iniciar seu aplicativo Node.js e o arquivo principal `app.js` estiver no diretório `/root/nodejs_app`, `/root/nodejs_app` é o diretório inicial de seu aplicativo.

5. No arquivo `package.json` de seu aplicativo Node.js, inclua a seguinte linha para a seção de dependências:

```
 “ibmapm": "./ibmapm"
```

   Lembre-se: Não se esqueça da vírgula no final de cada linha no arquivo, exceto a última, e mantenha o arquivo `package.json` em boa forma.

   Por exemplo:

```
 "dependencies": {
    "ibmapm": "./ibmapm",
    "cors": "^2.5.2",
    "helmet": "^1.3.0",
    "loopback": "^2.22.0",
    "loopback-boot": "^2.6.5",
    "loopback-datasource-juggler": "^2.39.0",
    "serve-favicon": "^2.0.1",
    "strong-error-handler": "^1.0.1"
  }
```

6. Inclua a linha a seguir no início do arquivo principal de seu aplicativo Node.js:

```
require('ibmapm');
```

   Se você iniciar seu aplicativo executando o comando **node app.js**, `app.js` será o arquivo principal de seu aplicativo.

7. No diretório que contém o arquivo `manifest.yml` de seu aplicativo Node.js, efetue login no IBM Cloud e, em seguida, execute o seguinte comando:

```
cf push
```

   Dica: Para obter um arquivo `manifest.yml` de amostra, consulte “Arquivo manifest.yml de amostra” na página 186.

Resultados

O coletor de dados é configurado e está conectado ao Servidor Cloud APM.

O que Fazer Depois

É possível verificar se os dados de monitoramento de seu aplicativo IBM Cloud são exibidos no Console do Cloud APM. Para obter instruções sobre como iniciar o Console do Cloud APM, consulte Iniciando o console do Cloud APM. Para obter informações sobre o uso do Editor de aplicativos, consulte Gerenciando aplicativos.

Lembre-se: Para incluir o aplicativo no Console do Cloud APM, escolha **Tempo de Execução de Node.js** no editor de aplicativos.

Customizando o coletor de dados Node.js independente para aplicativos IBM Cloud

É possível incluir variáveis de ambiente na interface com o usuário do IBM Cloud para customizar o monitoramento de seu aplicativo IBM Cloud.

Variáveis de ambiente definidas pelo usuário para o coletor de dados Node.js

É possível usar as informações na tabela a seguir para customizar o monitoramento de Node.js no IBM Cloud.

Tabela 188. Variáveis de ambiente definidas pelo usuário suportadas para monitoramento de Node.js no IBM Cloud

Nome de variável	Importância	Valor	Descrição
KNJ_SAMPLING	Opcional	Contagem de solicitações de amostragem	O número de solicitações com base no qual uma amostra é obtida. O valor padrão é `10`, que significa que uma entre 10 solicitações é monitorada. Se você não configurar essa variável, o valor padrão `10` será usado.
KNJ_MIN_CLOCK_TRACE	Opcional	Limite de tempo de resposta para coletar rastreio de método, em milissegundos	Se o tempo de resposta de uma instância de solicitação exceder o valor dessa variável, o coletor de dados coletará seu rastreio de método. O valor padrão é `0`. Se você não configurar essa variável, o valor padrão `0` será usado.
KNJ_MIN_CLOCK_STACK	Opcional	Limite de tempo de resposta para coletar o rastreio de pilha, em milissegundos	Se o tempo de resposta de uma instância de solicitação exceder o valor dessa variável, o coletor de dados coletará seu rastreio de pilha. O valor padrão é `0`. Se você não configurar essa variável, o valor padrão `0` será usado.
KNJ_ENABLE_METHODTRACE	Opcional	• `Verdadeiro` • `False`	Ativa ou desativa o rastreio de método. • Se você configurar esta variável como true, o rastreio de método para solicitações será desativado. • Se você configurar esse valor como false, o rastreio de método para solicitações será ativado. Esse é o valor padrão. Se você não configurar essa variável, o valor padrão `False` será usado e o rastreio de método para solicitações será ativado.

Tabela 188. Variáveis de ambiente definidas pelo usuário suportadas para monitoramento de Node.js no IBM Cloud (continuação)

Nome de variável	Importância	Valor	Descrição
KNJ_ENABLE_DEEPDIVE	Opcional	• `Verdadeiro` • `False`	Se você configurar essa variável como true, os dados diagnósticos serão enviados para o servidor. Por padrão, esse valor é configurado como false, o que significa que os dados diagnósticos não são enviados para o servidor.
KNJ_ENABLE_TT	Opcional	• `verdadeiro` • `false`	Ativa ou desativa o rastreamento de transações do AAR. • Se você configurar essa variável para true, o rastreamento de transações do AAR será ativado. • Se você configurar essa variável para false, o rastreamento de transações do AAR será desativado. Por padrão, esse valor não é configurado, o que significa que o rastreamento de transações é desativado.
KNJ_AAR_BATCH_FREQ	Opcional	Intervalo no qual os dados do AAR são enviados, em segundos	Especifica o intervalo no qual os dados do AAR estão em lote e são enviados para o servidor, em segundos. O valor padrão é 60, o que significa que os dados do AAR estão em lote e são enviados para o servidor a cada minuto. **Nota:** Essa variável funciona com KNJ_AAR_BATCH_COUNT para determinar quando os dados do AAR estão em lote e são enviados para o servidor. Quando a condição configurada por uma das duas variáveis for atendida, os dados do AAR estarão em lote e serão enviados. Quando as solicitações que os dados do AAR contêm atingirem o número máximo, por exemplo, 100, em um intervalo mais curto do que for configurado, os dados ainda estarão em lote e enviados imediatamente.

Tabela 188. Variáveis de ambiente definidas pelo usuário suportadas para monitoramento de Node.js no IBM Cloud (continuação)

Nome de variável	Importância	Valor	Descrição
KNJ_AAR_BATCH_COUNT	Opcional	Número máximo de solicitações que um lote de dados do AAR contém	Especifica o número máximo de solicitações que um lote de dados do AAR pode conter antes que seja enviado para o servidor. O valor padrão é 100, o que significa que quando o número de solicitações que um lote de dados do AAR contém atingir 100, esse lote de dados do AAR será enviado ao servidor.
KNJ_LOG_LEVEL	Opcional	O nível de informações que são impressas no log	Controla o nível de informações que são impressas no log. Os níveis a seguir são fornecidos: **desligado** Os logs não são impressos. **error** As informações são registradas somente em uma condição de erro. **informações** As informações são registradas quando o coletor de dados do agente Node.js está executando normalmente. Os dados brutos de monitoramento que são enviados para o agente também são registrados. **debug** As informações de depuração, informação e de erro são impressas no log, por exemplo, dados coletados, dados que são enviados para o servidor e resposta do servidor. **Todos** Todas as informações são impressas no log. Por padrão, o nível de log é `info`, que significa que as informações de resumo sobre as ações do coletor de dados estão impressas no log. Os logs são impressos na saída padrão.

Tabela 188. Variáveis de ambiente definidas pelo usuário suportadas para monitoramento de Node.js no IBM Cloud (continuação)

Nome de variável	Importância	Valor	Descrição
SECURITY_OFF	Opcional	• `verdadeiro` • `false`	Ativa ou desativa a coleta de informações confidenciais do usuário, como cookies, contexto de solicitação de HTTP e contexto de solicitação do banco de dados. • Se você configurar esta variável como true, as informações confidenciais do usuário serão coletadas. • Se você configurar esta variável como false, as informações confidenciais do usuário não serão coletadas. Esse é o valor padrão. Se você não especificar esta variável, o valor padrão de `false` será usado e as informações confidenciais do usuário não serão coletadas.

Desconfigurando o Coletor de dados Node.js para aplicativos IBM Cloud
Se você não precisa monitorar seu ambiente do Node.js ou se deseja fazer upgrade do Coletor de dados Node.js, deve-se primeiro desfazer as configurações anteriores para o Coletor de dados Node.js independente.

Procedimento

1. Remova a linha `require('ibmapm');` do arquivo principal do aplicativo.

   Dica: Se você iniciar seu aplicativo executando o comando **node app.js**, `app.js` será o arquivo principal de seu aplicativo.
2. Remova as seguintes dependências do arquivo `package.json`.

   ```
   “ibmapm": "./ibmapm"
   ```

   Lembre-se: Não remova as dependências de que seu aplicativo precisa.
3. Exclua a pasta `ibmapm` do diretório inicial de seu aplicativo.

Resultados
Você tem desconfigurado com sucesso o Coletor de dados Node.js.

O que Fazer Depois
Depois de desconfigurar o coletor de dados, o Console do Cloud APM continua a exibir o coletor de dados em quaisquer aplicativos nos quais você incluiu o coletor de dados. O Console do Cloud APM mostrará que nenhum dado está disponível para o aplicativo e não indicará que o coletor de dados está off-line. Para obter informações sobre como remover o coletor de dados de aplicativos e de grupos de recursos, consulte “Removendo coletores de dados do Console do Cloud APM” na página 186.

Configurando o Coletor de dados Node.js para aplicativos no local

Se você instalou o aplicativo Node.js em um ambiente local, será necessário configurar o Coletor de dados Node.js para coletar informações sobre o aplicativo Node.js.

Antes de Iniciar

1. Certifique-se de que o aplicativo Node.js possa ser executado localmente com sucesso. O Coletor de dados Node.js independente pode monitorar os fix packs Node.js V8.0.0 e futuros, fix packs V10.0.0 e futuros e fix packs V12.0.0 e futuros.
2. Faça download do pacote coletor de dados no website do IBM Marketplace. Para obter instruções detalhadas, consulte “Fazendo download de seus agentes e coletores de dados” na página 101.

Procedimento

1. Extraia os arquivos do pacote do coletor de dados. O pacote `nodejs_datacollector_8.1.4.0.6.tgz` é incluído no diretório extraído.
2. Determine o diretório inicial de seu aplicativo.
   - Para aplicativos Node.js típicos, se você usar o comando **`node app.js`** para iniciar o aplicativo Node.js e o arquivo principal `app.js` estiver no diretório `/root/nodejs_app`, `/root/nodejs_app` será o diretório inicial de seu aplicativo.
   - Para membros coletivos no ambiente do IBM API Connect, execute o comando **`wlpn-server list`** para exibir a lista de todos seus membros coletivos na mesma máquina. O diretório inicial de seu membro coletivo está no seguinte formato:

     ```
     user_directory/collective-member_name/package
     ```

     Por exemplo, se você receber `/root/wlpn/rock-8345a96-148538-1/package` como uma saída de comando, `/root/wlpn` será o diretório do usuário e `rock-8345a96-148538-1` será o nome do membro coletivo.
   - Para aplicativos do Portal do Desenvolvedor no ambiente do IBM API Connect, é possível executar o comando **`ps -ef | grep node`** para localizar o diretório inicial. Se você receber a seguinte saída de comando, por exemplo, o diretório inicial será `/home/admin/bgsync` e o arquivo principal de seu aplicativo será `rest_server.js`:

     ```
     admin 19085 1 0 Jun25?  00:06:53 /usr/local/bin/node /home/admin/bgsync/
     rest_server.js
     ```
3. No diretório inicial de seu aplicativo, execute o seguinte comando para extrair arquivos do pacote do coletor de dados:

   ```
   tar -zxf nodejs_datacollector_8.1.4.0.6.tgz
   ```
4. Extraia o arquivo `ibmapm.tgz` na pasta `nodejs_dc` executando o comando a seguir:

   ```
   tar -zxf nodejs_dc/ibmapm.tgz
   ```

   Você obterá uma pasta `ibmapm`.
5. Execute o seguinte comando para instalar o coletor de dados em seu aplicativo:

   ```
   npm install ./ibmapm
   ```
6. Inclua a linha a seguir no início do arquivo principal de seu aplicativo Node.js:

   ```
   require('ibmapm');
   ```
   - Se você iniciar seu aplicativo executando o comando **`node app.js`**, `app.js` será o arquivo principal de seu aplicativo.
   - Para membros coletivos no ambiente do IBM API Connect, o arquivo principal é definido no arquivo `package.json` no diretório inicial ou em suas subpastas. Por padrão, o arquivo principal é *`home_directory`*`/server/server.js`, em que *`home_directory`* é o diretório inicial para seu membro coletivo.

- Para aplicativos do Portal do Desenvolvedor no ambiente do IBM API Connect, é possível executar o comando **ps -ef | grep node** para localizar o arquivo principal. Se você receber a seguinte saída de comando, o arquivo principal de seu aplicativo será `rest_server.js`.

```
admin 19085 1 0 Jun25?  00:06:53 /usr/local/bin/node /home/admin/bgsync/
rest_server.js
```

7. Reinicie a aplicação.

   Dica:

   - Para reiniciar o membro coletivo, execute o comando `wlpn-server stop` *`collective_member_name`*. O membro coletivo é reiniciado automaticamente após a execução desse comando. Se ele não iniciar, execute o comando `wlpn-server start` *`collective_member_name`* para reiniciá-lo manualmente.
   - Para reiniciar seus aplicativos do Portal do Desenvolvedor, primeiro execute o comando `/etc/init.d/restservice stop` para parar o aplicativo e, em seguida, execute o comando `/etc/init.d/restservice start` para iniciá-lo.

Resultados
O coletor de dados é configurado e está conectado ao Servidor Cloud APM.

O que Fazer Depois

- É possível verificar se os dados de monitoramento de seu aplicativo são exibidos no Console do Cloud APM. Para obter instruções sobre como iniciar o Console do Cloud APM, consulte Iniciando o console do Cloud APM. Para obter informações sobre o uso do Editor de aplicativos, consulte Gerenciando aplicativos.
- Para visualizar informações de topologia para o ambiente do API Connect, ative o rastreamento de transação. Para obter mais instruções, consulte a descrição da variável *KNJ_ENABLE_TT* em “Customizando o Coletor de dados Node.js para aplicativos no local” na página 600.

Lembre-se: Para incluir o aplicativo no Console do Cloud APM, escolha **Tempo de Execução de Node.js** no editor de aplicativos.

Customizando o Coletor de dados Node.js para aplicativos no local
Ao modificar arquivos no pacote coletor de dados, é possível configurar as variáveis de ambiente para customizar o monitoramento do aplicativo Node.js.

É possível configurar as variáveis customizando as variáveis de ambiente ou editando o arquivo `config.properties`. É possível localizar o arquivo `config.properties` na pasta `ibmapm/etc` na qual o coletor de dados Node.js está instalado.

Tabela 189. Variáveis suportadas

Nome de variável	Importância	Valor	Descrição
KNJ_SAMPLING	Opcional	Contagem de solicitações de amostragem	O número de solicitações com base no qual uma amostra é obtida. O valor padrão é 10, que significa que uma entre 10 solicitações é monitorada. Se você não configurar essa variável, o valor padrão 10 será usado.

Tabela 189. Variáveis suportadas (continuação)

Nome de variável	Importância	Valor	Descrição
KNJ_MIN_CLOCK_TRACE	Opcional	Limite de tempo de resposta para coletar rastreio de método, em milissegundos	Se o tempo de resposta de uma instância de solicitação exceder o valor dessa variável, o coletor de dados coletará seu rastreio de método. O valor padrão é `0`. Se você não configurar essa variável, o valor padrão `0` será usado.
KNJ_MIN_CLOCK_STACK	Opcional	Limite de tempo de resposta para coletar o rastreio de pilha, em milissegundos	Se o tempo de resposta de uma instância de solicitação exceder o valor dessa variável, o coletor de dados coletará seu rastreio de pilha. O valor padrão é `0`. Se você não configurar essa variável, o valor padrão `0` será usado.
KNJ_ENABLE_METHODTRACE	Opcional	• `Verdadeiro` • `False`	Ativa ou desativa o rastreio de método. • Se você configurar esta variável como true, o rastreio de método para solicitações será desativado. • Se você configurar esse valor como false, o rastreio de método para solicitações será ativado. Esse é o valor padrão. Se você não configurar essa variável, o valor padrão `False` será usado e o rastreio de método para solicitações será ativado.
KNJ_ENABLE_DEEPDIVE	Opcional	• `Verdadeiro` • `False`	Se você configurar essa variável como true, os dados diagnósticos serão enviados para o servidor. Por padrão, esse valor é configurado como false, o que significa que dados diagnósticos não são enviados para o servidor.

Tabela 189. Variáveis suportadas (continuação)

Nome de variável	Importância	Valor	Descrição
KNJ_ENABLE_TT	Opcional	• `verdadeiro` • `false`	Ativa ou desativa o rastreamento de transações do AAR. • Se você configurar essa variável para true, o rastreamento de transações do AAR será ativado. • Se você configurar essa variável para false, o rastreamento de transações do AAR será desativado. Por padrão, esse valor não é configurado, o que significa que o rastreamento de transações é desativado.
KNJ_AAR_BATCH_FREQ	Opcional	Intervalo no qual os dados do AAR são enviados, em segundos	Especifica o intervalo no qual os dados do AAR estão em lote e são enviados para o servidor, em segundos. O valor padrão é 60, o que significa que os dados do AAR estão em lote e são enviados para o servidor a cada minuto. **Nota:** Essa variável funciona com KNJ_AAR_BATCH_COUNT para determinar quando os dados do AAR estão em lote e são enviados para o servidor. Quando a condição configurada por uma das duas variáveis for atendida, os dados do AAR estarão em lote e serão enviados. Quando as solicitações que os dados do AAR contêm atingirem o número máximo, por exemplo, 100, em um intervalo mais curto do que for configurado, os dados ainda estarão em lote e enviados imediatamente.
KNJ_AAR_BATCH_COUNT	Opcional	Número máximo de solicitações que um lote de dados do AAR contém	Especifica o número máximo de solicitações que um lote de dados do AAR pode conter antes que seja enviado para o servidor. O valor padrão é 100, o que significa que quando o número de solicitações que um lote de dados do AAR contém atingir 100, esse lote de dados do AAR será enviado ao servidor.

Tabela 189. Variáveis suportadas (continuação)

Nome de variável	Importância	Valor	Descrição
KNJ_LOG_LEVEL	Opcional	O nível de informações que são impressas no log	Controla o nível de informações que são impressas no log. Os níveis a seguir são fornecidos: **desligado** Os logs não são impressos. **error** As informações são registradas somente em uma condição de erro. **informações** As informações são registradas quando o coletor de dados do agente Node.js está executando normalmente. Os dados brutos de monitoramento que são enviados para o agente também são registrados. **debug** As informações de depuração, informação e de erro são impressas no log, por exemplo, dados coletados, dados que são enviados para o servidor e resposta do servidor. **Todos** Todas as informações são impressas no log. Por padrão, o nível de log é `info`, que significa que as informações de resumo sobre as ações do coletor de dados estão impressas no log. Os logs são impressos na saída padrão.
SECURITY_OFF	Opcional	• `verdadeiro` • `false`	Ativa ou desativa a coleta de informações confidenciais do usuário, como cookies, contexto de solicitação de HTTP e contexto de solicitação do banco de dados. • Se você configurar esta variável como true, as informações confidenciais do usuário serão coletadas. • Se você configurar esta variável como false, as informações confidenciais do usuário não serão coletadas. Esse é o valor padrão. Se você não especificar esta variável, o valor padrão de `false` será usado e as informações confidenciais do usuário não serão coletadas.

Desconfigurando o Coletor de dados Node.js para aplicativos no local

Se você não precisa monitorar seu ambiente do Node.js ou se deseja fazer upgrade do Coletor de dados Node.js, deve-se primeiro desfazer as configurações anteriores para o Coletor de dados Node.js independente.

Procedimento

1. Remova a linha `require('ibmapm');` do arquivo principal do aplicativo.

   Dica: Se você iniciar seu aplicativo executando o comando **node app.js**, `app.js` será o arquivo principal de seu aplicativo.
2. Remova "`ibmapm": "./ibmapm"` da seção de dependências no arquivo `package.json` do seu aplicativo Node.js.
3. Exclua a pasta `node_modules` do diretório inicial de seu aplicativo.
4. Execute o comando `npm install` para instalar dependências de aplicativo.

Resultados

Você tem desconfigurado com sucesso o Coletor de dados Node.js.

O que Fazer Depois

Depois de desconfigurar o coletor de dados, o Console do Cloud APM continua a exibir o coletor de dados em quaisquer aplicativos nos quais você incluiu o coletor de dados. O Console do Cloud APM mostrará que nenhum dado está disponível para o aplicativo e não indicará que o coletor de dados está off-line. Para obter informações sobre como remover o coletor de dados de aplicativos e de grupos de recursos, consulte "Removendo coletores de dados do Console do Cloud APM" na página 186.

Configurando o Coletor de dados Node.js independente para aplicativos Kubernetes

Se você instalou o aplicativo Node.js no Kubernetes, é possível configurar o Coletor de dados Node.js para coletar informações sobre o aplicativo Node.js.

Antes de Iniciar

1. Certifique-se de que o aplicativo Node.js possa ser executado com sucesso. O Coletor de dados Node.js independente pode monitorar os fix packs Node.js V8.0.0 e futuros, fix packs V10.0.0 e futuros e fix packs V12.0.0 e futuros.
2. Faça download do pacote coletor de dados no website do IBM Marketplace. Para obter instruções detalhadas, consulte "Fazendo download de seus agentes e coletores de dados" na página 101.

Procedimento

1. Extraia os arquivos do pacote do coletor de dados. O pacote `nodejs_datacollector_8.1.4.0.6.tgz` é incluído no diretório extraído.
2. Extraia o arquivo `nodejs_datacollector_8.1.4.0.6.tgz`, por exemplo, executando o seguinte comando:

   ```
   tar -zxf nodejs_datacollector_8.1.4.0.6.tgz
   ```
3. Extraia o arquivo `ibmapm.tgz` na pasta `nodejs_dc` executando o comando a seguir:

   ```
   tar -zxf nodejs_dc/ibmapm.tgz
   ```

   Você obterá uma pasta `ibmapm`.
4. No arquivo `package.json` de seu aplicativo Node.js, inclua a seguinte linha para a seção de dependências:

   ```
   "ibmapm": "./ibmapm"
   ```

Lembre-se: Não se esqueça da vírgula no final de cada linha no arquivo, exceto a última, e mantenha o arquivo `package.json` em boa forma.

5. Inclua a linha a seguir no início do arquivo principal de seu aplicativo Node.js:

```
require('./ibmapm');
```

   Se você iniciar seu aplicativo executando o comando **node app.js**, `app.js` será o arquivo principal de seu aplicativo.

6. Reconstrua a imagem do Docker.

   Nota: Se você executar o aplicativo Node.js em outros ambientes do Docker, por exemplo, serviços Docker Swarm ou AWS Docker, será necessário executar o Docker nas etapas.

O que Fazer Depois

Se quiser customizar o monitoramento, você pode incluir variáveis de ambiente no arquivo yaml de implementação. Para obter detalhes, consulte "Customizando o coletor de dados Node.js independente para aplicativos Kubernetes" na página 605.

Customizando o coletor de dados Node.js independente para aplicativos Kubernetes

É possível incluir variáveis de ambiente no arquivo yaml de implementação para customizar o monitoramento para o aplicativo Kubernetes.

Variáveis de ambiente definidas pelo usuário para o coletor de dados Node.js

É possível usar as informações na tabela a seguir para customizar o monitoramento do Node.js no Kubernetes.

Tabela 190. Variáveis de ambiente definidas pelo usuário suportadas para o monitoramento do Node.js no Kubernetes

Nome de variável	Importância	Valor	Descrição
KNJ_SAMPLING	Opcional	Contagem de solicitações de amostragem	O número de solicitações com base no qual uma amostra é obtida. O valor padrão é `10`, que significa que uma entre 10 solicitações é monitorada. Se você não configurar essa variável, o valor padrão `10` será usado.
KNJ_MIN_CLOCK_TRACE	Opcional	Limite de tempo de resposta para coletar rastreio de método, em milissegundos	Se o tempo de resposta de uma instância de solicitação exceder o valor dessa variável, o coletor de dados coletará seu rastreio de método. O valor padrão é `0`. Se você não configurar essa variável, o valor padrão `0` será usado.
KNJ_MIN_CLOCK_STACK	Opcional	Limite de tempo de resposta para coletar o rastreio de pilha, em milissegundos	Se o tempo de resposta de uma instância de solicitação exceder o valor dessa variável, o coletor de dados coletará seu rastreio de pilha. O valor padrão é `0`. Se você não configurar essa variável, o valor padrão `0` será usado.

Tabela 190. Variáveis de ambiente definidas pelo usuário suportadas para o monitoramento do Node.js no Kubernetes (continuação)

Nome de variável	Importância	Valor	Descrição
KNJ_ENABLE_METHODTRACE	Opcional	• `Verdadeiro` • `False`	Ativa ou desativa o rastreio de método. • Se você configurar esta variável como true, o rastreio de método para solicitações será desativado. • Se você configurar esse valor como false, o rastreio de método para solicitações será ativado. Esse é o valor padrão. Se você não configurar essa variável, o valor padrão `False` será usado e o rastreio de método para solicitações será ativado.
KNJ_ENABLE_DEEPDIVE	Opcional	• `Verdadeiro` • `False`	Se você configurar essa variável como true, os dados diagnósticos serão enviados para o servidor. Por padrão, esse valor é configurado como false, o que significa que os dados diagnósticos não são enviados para o servidor.
KNJ_ENABLE_TT	Opcional	• `verdadeiro` • `false`	Ativa ou desativa o rastreamento de transações do AAR. • Se você configurar essa variável para true, o rastreamento de transações do AAR será ativado. • Se você configurar essa variável para false, o rastreamento de transações do AAR será desativado. Por padrão, esse valor não é configurado, o que significa que o rastreamento de transações é desativado.

Tabela 190. Variáveis de ambiente definidas pelo usuário suportadas para o monitoramento do Node.js no Kubernetes (continuação)

Nome de variável	Importância	Valor	Descrição
KNJ_AAR_BATCH_FREQ	Opcional	Intervalo no qual os dados do AAR são enviados, em segundos	Especifica o intervalo no qual os dados do AAR estão em lote e são enviados para o servidor, em segundos. O valor padrão é 60, o que significa que os dados do AAR estão em lote e são enviados para o servidor a cada minuto. **Nota:** Essa variável funciona com KNJ_AAR_BATCH_COUNT para determinar quando os dados do AAR estão em lote e são enviados para o servidor. Quando a condição configurada por uma das duas variáveis for atendida, os dados do AAR estarão em lote e serão enviados. Quando as solicitações que os dados do AAR contêm atingirem o número máximo, por exemplo, 100, em um intervalo mais curto do que for configurado, os dados ainda estarão em lote e enviados imediatamente.
KNJ_AAR_BATCH_COUNT	Opcional	Número máximo de solicitações que um lote de dados do AAR contém	Especifica o número máximo de solicitações que um lote de dados do AAR pode conter antes que seja enviado para o servidor. O valor padrão é 100, o que significa que quando o número de solicitações que um lote de dados do AAR contém atingir 100, esse lote de dados do AAR será enviado ao servidor.

Tabela 190. Variáveis de ambiente definidas pelo usuário suportadas para o monitoramento do Node.js no Kubernetes (continuação)

Nome de variável	Importância	Valor	Descrição
KNJ_LOG_LEVEL	Opcional	O nível de informações que são impressas no log	Controla o nível de informações que são impressas no log. Os níveis a seguir são fornecidos: **desligado** Os logs não são impressos. **error** As informações são registradas somente em uma condição de erro. **informações** As informações são registradas quando o coletor de dados do agente Node.js está executando normalmente. Os dados brutos de monitoramento que são enviados para o agente também são registrados. **debug** As informações de depuração, informação e de erro são impressas no log, por exemplo, dados coletados, dados que são enviados para o servidor e resposta do servidor. **Todos** Todas as informações são impressas no log. Por padrão, o nível de log é `info`, que significa que as informações de resumo sobre as ações do coletor de dados estão impressas no log. Os logs são impressos na saída padrão.

Tabela 190. Variáveis de ambiente definidas pelo usuário suportadas para o monitoramento do Node.js no Kubernetes (continuação)

Nome de variável	Importância	Valor	Descrição
SECURITY_OFF	Opcional	• `verdadeiro` • `false`	Ativa ou desativa a coleta de informações confidenciais do usuário, como cookies, contexto de solicitação de HTTP e contexto de solicitação do banco de dados. • Se você configurar esta variável como true, as informações confidenciais do usuário serão coletadas. • Se você configurar esta variável como false, as informações confidenciais do usuário não serão coletadas. Esse é o valor padrão. Se você não especificar esta variável, o valor padrão de `false` será usado e as informações confidenciais do usuário não serão coletadas.

Exemplo de arquivo yaml

```
spec:
      contêineres:
      - name: testapp
        image: mycluster.icp:8500/default/testapp:v1
        imagePullPolicy: Always
        ports:
        - containerPort: 3000
          protocol: TCP
        env:
        - name: KNJ_LOG_LEVEL
          value: "debug"
        - name: KNJ_ENABLE_TT
          value: "true"
        - name: KNJ_ENABLE_DEEPDIVE
          value: "true"
```

Desconfigurando o Coletor de dados Node.js independente para aplicativos Kubernetes
Se você não precisa monitorar seu ambiente do Node.js ou se deseja fazer upgrade do Coletor de dados Node.js, deve-se primeiro desfazer as configurações anteriores para o Coletor de dados Node.js independente.

Procedimento

1. Remova a linha `require('ibmapm');` do arquivo principal do aplicativo.

   Dica: Se você iniciar seu aplicativo executando o comando **node app.js**, `app.js` será o arquivo principal de seu aplicativo.
2. Remova as seguintes dependências do arquivo `package.json`.

   ```
   "ibmapm": "./ibmapm"
   ```

   Lembre-se: Não remova as dependências de que seu aplicativo precisa.

Resultados
Você tem desconfigurado com sucesso o Coletor de dados Node.js.

O que Fazer Depois
Depois de desconfigurar o coletor de dados, o Console do Cloud APM continua a exibir o coletor de dados em quaisquer aplicativos nos quais você incluiu o coletor de dados. O Console do Cloud APM mostrará que nenhum dado está disponível para o aplicativo e não indicará que o coletor de dados está off-line. Para obter informações sobre como remover o coletor de dados de aplicativos e de grupos de recursos, consulte "Removendo coletores de dados do Console do Cloud APM" na página 186.

Configurando o monitoramento do OpenStack

Deve-se configurar o Monitoring Agent for OpenStack antes que o agente possa monitorar automaticamente o ambiente do OpenStack agent.

Procedimento

1. Configure o agente respondendo aos prompts. Para obter instruções, veja "Configurando o OpenStack agent" na página 610.
2. Se deseja coletar informações relacionadas ao processo, configure o coletor de dados para o OpenStack agent. Para obter instruções, veja "Ativando a coleta de informações relacionadas ao processo e conexões SSH" na página 612.
3. Insira valores de configuração para que o agente opere. Para obter instruções, veja "Incluindo os valores de configuração" na página 613.

Configurando o OpenStack agent

Para um ambiente típico, se você desejar que o OpenStack agent monitore automaticamente o ambiente do OpenStack, deverá configurar o agente primeiro.

Antes de Iniciar
Certifique-se de que tenha instalado todos os softwares necessários, conforme descrito em Pré-instalação em sistemas Linux.

Procedimento

Você tem duas opções para configurar o OpenStack agent em um sistema Linux:

- Para configurar o agente executando o script e respondendo a prompts, consulte "Configuração interativa" na página 610.
- Para configurar o agente editando o arquivo de resposta silencioso e executando o script sem nenhuma interação, consulte "Configuração silenciosa" na página 611.

Configuração interativa

Procedimento

1. Para configurar o agente, execute o comando a seguir:

   ```
   install_dir/bin/openstack-agent.sh config instance_name
   ```

   em que *install_dir* é o diretório de instalação do OpenStack agent. O diretório de instalação padrão é `/opt/ibm/apm/agent`.
2. Quando solicitado a `Inserir o nome da instância`, especifique um nome da instância.

   Importante: O OpenStack agent é um agente de várias instâncias e requer um nome da instância para cada instância do agente. O nome da instância especificado é incluído no nome do sistema gerenciado `instance_name:host_name:sg`. O comprimento do nome da instância especificado é limitado a 28 caracteres menos o comprimento do seu nome do host. Por exemplo, se especificar 0S1 como seu nome da instância, seu nome do sistema gerenciado é `0S1:hostname:SG`.

3. Quando solicitado a `Editar o Monitoring Agent for OpenStack`, pressione `Enter` para continuar.
4. Quando solicitado a `Editar informações de autenticação do ambiente do OpenStack`, forneça as informações a seguir:

```
OpenStack authentication url (default is: http://localhost:identity/v3):
Nome do usuário do OpenStack (o padrão é: admin):
Insira a senha do OpenStack (o padrão é: ):
Digite novamente: senha do OpenStack (o padrão é: ):
Nome do locatário do OpenStack (o padrão é: admin):
```

5. Quando solicitado pelo `Local Executável do Python`, especifique o local executável do Python, por exemplo, `/usr/bin/python`.

   É possível localizar o caminho completo executando o comando a seguir em seu ambiente:

```
which python
```

6. Quando solicitado pelo `Número da porta`, aceite o valor padrão ou especifique um número da porta.

   Esta porta é usada para monitorar a comunicação interna entre o coletor de dados do OpenStack agent e o OpenStack agent, ambos instalados somente em um servidor local. O agente atende nessa porta para dados do coletor de dados. O valor padrão de 0 indica que uma porta efêmera é usada quando o agente inicia. Em um servidor com regras de segurança rígidas sobre portas, é possível configurar uma porta específica para o agente usar. Esta porta é para uso interno pelo agente e não está relacionada ao ambiente OpenStack.
7. Edite o arquivo `/etc/hosts` no sistema para incluir o mapeamento do host para cada nó monitorado.

Configuração silenciosa

Procedimento

1. Abra o arquivo `sg_silent_config.txt` em um editor de texto. O arquivo está no diretório *`install_dir`*`/samples`, em que *install_dir* é o diretório de instalação do OpenStack agent.
2. Edite o arquivo de configuração `sg_silent_config.txt` para o OpenStack agent.
3. Especifique os valores para os parâmetros identificados no arquivo. O arquivo de resposta contém comentários que definem os parâmetros disponíveis e os valores a serem especificados.
4. Salve o arquivo e saia.
5. Edite o arquivo `/etc/hosts` no sistema para incluir o mapeamento do host para cada nó monitorado.
6. No diretório *`install_dir`*`/samples`, execute o comando a seguir para configurar o agente:

```
install_dir/bin/openstack-agent.sh config instance_name path_to_response_file
```

   em que *install_dir* é o nome da instância a ser configurada e *path_to_responsefile* é o caminho completo do arquivo de resposta silencioso. Especifique um caminho absoluto para este arquivo.

   Por exemplo, se o arquivo de resposta estiver no diretório padrão, execute o comando a seguir.

```
/opt/ibm/apm/agent/bin/openstack-agent.sh config instance_name
/opt/ibm/apm/agent/samples/sg_silent_config.txt
```

Resultados
O agente é configurado.

O que Fazer Depois

- Após finalizar a configuração do agente, é possível iniciar a instância de agente executando o comando:

```
install_dir/bin/openstack-agent.sh start instance_name
```

  em que *instance_name* é o nome da instância de agente a ser configurada.

- Para conectar o OpenStack agent a um ambiente OpenStack habilitado para SSL, especifique o diretório do certificado SSL de seu servidor OpenStack configurando a variável a seguir:

  ```
  OS_cert_path=directory of the certificate.crt file
  ```

  A variável OS_cert_path está na seção OS_authentication_info no arquivo ksg_dc_*instance_name*.cfg.
- Se desejar coletar informações relacionadas ao processo, configure o coletor de dados para o OpenStack agent concluindo as etapas em "Ativando a coleta de informações relacionadas ao processo e conexões SSH" na página 612.
- Se você deseja mudar o nível de rastreio do agente para propósitos de resolução de problemas, edite o valor da variável **KBB_RAS1** no arquivo *install_dir*/config/sg.environment de acordo com as instruções no arquivo.

Ativando a coleta de informações relacionadas ao processo e conexões SSH

Se desejar coletar informações relacionadas ao processo, configure o coletor de dados do agente para o OpenStack agent e configure conexões SSH com o servidor de componente do OpenStack de destino.

Sobre Esta Tarefa

Deve-se configurar uma conexão SSH para coletar informações do processo antes de iniciar o OpenStack agent. Para configurar a conexão, utilize a ferramenta de assistência **ksg_setup_key.sh** ou **ksg_ssh_setup.py** fornecida pelo produto e descrita no procedimento a seguir.

Se estiver familiarizado com a configuração de conexões de SSH, também será possível utilizar os comandos Linux **ssh-keygen** e **ssh-copy-id** para configurar a conexão

Procedimento

1. Acesse o diretório *install_dir*/config, em que *install_dir* é o diretório de instalação do agente.
2. Edite o arquivo ksg_dc_*instance_name*.cfg, onde *instance_name* é o nome especificado para este instância de agente.

   O arquivo é criado após a instância de agente iniciar. Se o arquivo não existir, copie *install_dir*/lx8266/sg/bin/ksg_dc.cfg para o diretório *install_dir*/config e mude o nome do arquivo para ksg_dc_*instance_name*.cfg.

   Por exemplo, se o nome da instância for OS1, mude o nome para ksg_dc_OS1.cfg.
3. No arquivo ksg_dc_*instance_name*.cfg, configure o valor do parâmetro **collect_process_information** para YES.
4. Na seção **OS_process_collection**, especifique o valor para o parâmetro **ssh_user_host** com os usuários e os nomes de host ou os endereços IP dos servidores de componente do OpenStack, de acordo com o formato do seguinte exemplo:

   ```
   ssh_user_host=root@9.112.250.248,user1@hostname
   ```
5. Salve as definições.
6. Para que as configurações entrem em vigor, reinicie a instância de agente executando os comandos a seguir:

   ```
   install_dir/bin/openstack-agent.sh stop instance_name
   install_dir/bin/openstack-agent.sh start instance_name
   ```
7. Configure as conexões de SSH com o servidor de componentes de destino usando uma das formas a seguir:
   - Configure as conexões uma a uma usando o script ksg_setup_key.sh: acesse o diretório *install_dir*/lx8266/sg/bin e execute o script ksg_setup_key.sh com o nome ou IP do host e o usuário para criar as conexões SSH com servidores de componentes que estejam

especificados na Etapa 4. Se seguir o exemplo dado na Etapa 4, você deve executar o script duas vezes para configurar a conexão uma a uma:

```
./ksg_setup_key.sh 9.112.250.248 root
./ksg_setup_key.sh hostname user1
```

Nota: Você deve fornecer as senhas ao executar os scripts pela primeira vez. Não é necessário fornecer a senha novamente.

- Configure as conexões uma a uma ou em uma tarefa em lote usando a ferramenta `ksg_ssh_setup.py` que é fornecida pelo OpenStack agent em *`install_dir`*`/lx8266/sg/bin`. Você deve instalar a biblioteca Python pexpect antes de poder usar esta ferramenta.
  - Para configurar conexões de SSH uma a uma, execute o comando:

    ```
    python ksg_ssh_setup.py -single
    ```

    Este comando ajuda a configurar a conexão de SSH para o servidor de destinos remotos. Você deve fornecer as seguintes informações:

    ```
    Insira o nome do host ou endereço IP da máquina de destino remoto: (Digite 'END' para
    encerrar a entrada.)
    Insira a conta para acessar a máquina remota (por ex., raiz):
    Insira a senha do usuário acima:
    ```

  - Para configurar conexões de SSH em uma tarefa em lote, execute o comando:

    ```
    python ksg_ssh_setup.py -ssh SSH_file
    ```

    onde *SSH_file* é o arquivo que contém as informações do servidor de destino, usuário e senha. Você deve criar o arquivo de acordo com o arquivo `ksg_dc_ssh_list.txt` no mesmo diretório que a ferramenta Python, e especificar as informações de host e usuário no arquivo de acordo com o formato dos exemplos:

    ```
    hostname root passw0rd
    9.112.250.248 user1 passw0rd
    ```

Nota: Deve-se configurar as conexões novamente somente quando o nome de usuário ou a senha para o servidor de destino mudar. Não será necessário configurar as conexões novamente após reiniciar o agente ou mudar a configuração do agente.

Resultados

O coletor de dados é configurado e as conexões de SSH são configuradas adequadamente. Agora, é possível efetuar login no console do Cloud APM e usar o Editor de aplicativos para incluir a instância do OpenStack agent no Painel de Desempenho do Aplicativo. Ao incluir a instância de agente, escolha **Ambiente do OpenStack** na lista de componentes ao incluir a instância de agente.

O que Fazer Depois

- Ao clicar em **Resumo do Terminal da API por Tipo de Serviço** > **Detalhes do Terminal da API**, você vê uma mensagem `Nenhum dado disponível` nos widgets de grupo **Histórico de Tempos de Falha de Detecção da API** e **Histórico de Percentual da Falha de Detecção da API**. Clique em um terminal da API mostrado em **Detalhes do Terminal da API** e será possível visualizar dados de monitoramento nos dois widgets de grupo.
- Ao clicar em **Resumo do Processo por Componente** > **Detalhes do Processo** ou em **Status de Conexão do Servidor SSH** > **Detalhes do Processo**, você vê uma mensagem `Nenhum dado disponível` nos widgets de grupo **Histórico de Uso da CPU do Processo** e **Histórico de Uso de Memória do Processo**. Clique em um processo mostrado em **Detalhes do Processo** e você poderá visualizar dados de monitoramento nos dois widgets de grupo.

Incluindo os valores de configuração

Para a configuração local e remota, você fornece os valores de configuração para que o agente opere.

Ao usar o modo interativo para configurar o agente, um painel será exibido para que você possa inserir cada valor. Quando existir um valor padrão, esse valor é pré-inserido no campo. Se um campo representar uma senha, dois campos de entrada serão exibidos. Você deve digitar o mesmo valor em cada campo. Os valores digitados não são exibidos, o que ajuda a manter a segurança desses valores.

Ao usar o modo silencioso para configurar o agente, é possível editar o *response_file* no diretório *install_dir*/samples para incluir os valores de configuração. Após salvar as mudanças, siga as instruções na Etapa "6" na página 611 e execute o comando a seguir para que as mudanças entrem em vigor:

```
install_dir/bin/openstack-agent.sh start instance_name
```

em que *instance_name* é o nome da instância de agente a ser configurada.

Após a conclusão da configuração, é possível localizar os valores configurados no arquivo .cfg da instância do agente, por exemplo, *hostname*_sg_*instance_name*.cfg.

A configuração deste agente está organizada nos seguintes grupos:

Informações sobre a autenticação do ambiente OpenStack (OPENSTACK_CONNECTION)
As informações sobre autenticação do ambiente do OpenStack

Os elementos de configuração definidos neste grupo estão sempre presentes na configuração do agente.

Esse grupo define informações que se aplicam a todo o agente.

URL de autenticação do OpenStack (KSG_OPENSTACK_AUTH_URL)
A auth_url do ambiente do OpenStack

O tipo é de cadeia.

Este valor é requerido.

Valor padrão: http://localhost:identity/v3

Senha do OpenStack (KSG_OPENSTACK_PASSWORD)
A senha de usuário administrador

O tipo é password.

Este valor é requerido.

Valor padrão: None

Nome do locatário do OpenStack (KSG_OPENSTACK_TENANT_NAME)
O nome do locatário do OpenStack, também conhecido como o nome do projeto

O tipo é de cadeia.

Este valor é requerido.

Valor padrão: admin

Nome do usuário do OpenStack (KSG_OPENSTACK_USERNAME)
O usuário administrador para efetuar login no ambiente do OpenStack

O tipo é de cadeia.

Este valor é requerido.

Valor padrão: admin

Python (KSG_PYTHON)
Localização executável do Python

Os elementos de configuração definidos neste grupo estão sempre presentes na configuração do agente.

Esse grupo define informações que se aplicam a todo o agente.

Local executável do Python (KSG_PYTHON_LOCATION)
O executável do python que será usado para executar o coletor de dados do agente do OpenStack. É possível localizar o caminho completo executando o comando a seguir em seu terminal: "which python".

O tipo é de cadeia.

Este valor é requerido.

Valor padrão: None

Soquete (KSG_SOCKET)
Origem de Dados do Soquete

Os elementos de configuração definidos nesse grupo estão sempre presentes na configuração do agente.

Esse grupo define informações que se aplicam a todo o agente.

Número da Porta (CP_PORT)
A porta que o agente usará para atender dados dos clientes do soquete. Um valor igual a 0 indica que uma porta efêmera será usada. Esta porta NÃO corresponde a nenhuma porta usada pelo seu aplicativo. Esta porta é para uso interno do agente.

O tipo é numérico.

This value is optional.

Valor-padrão: 0

Configurando o monitoramento do Banco de Dados Oracle

O Monitoring Agent for Oracle Database fornece capacidades de monitoramento para a disponibilidade, desempenho e uso de recursos do banco de dados Oracle. É possível configurar mais de uma instância do Agente Oracle Database para monitorar diferentes bancos de dados Oracle. A capacidade de monitoramento remoto também é fornecida por esse agente.

Antes de Iniciar

- Antes de configurar o Agente Oracle Database, deve-se conceder privilégios para a conta do usuário do Oracle que é usada pelo Agente Oracle Database. Para obter informações adicionais sobre privilégios, consulte Concedendo privilégios ao usuário do agente do Banco de dados Oracle.
- Se você estiver monitorando um banco de dados Oracle remotamente, o agente deverá ser instalado em um computador com o software do banco de dados Oracle ou com o Oracle Instant Client instalado.

Sobre Esta Tarefa

Estas instruções são para a liberação mais atual do agente, exceto conforme indicado. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Versão do Agente.

Para monitoramento do desempenho do banco de dados Oracle geral, o Agente Oracle Database fornece monitoramento para disponibilidade, desempenho, uso de recurso e atividades do banco de dados Oracle, por exemplo:

- Disponibilidade de instâncias no banco de dados Oracle monitorado.
- Informações de recursos, como memória, caches, segmentos, limitação de recurso, espaço de tabela, desfazer (retroceder), métrica do sistema e estatísticas do sistema.
- Informações de atividade, como estatísticas do sistema operacional, sessões, contenção e log de alerta.

O Agente Oracle Database é um agente de múltiplas instâncias. Você deve criar a primeira instância e iniciar o agente manualmente. Além disso, cada instância do agente pode monitorar vários bancos de dados.

O nome do sistema gerenciado para o Agente Oracle Database inclui um nome de conexão do banco de dados que você especifica, um nome da instância do agente que você especifica e o nome do host do computador no qual o agente está instalado. Por exemplo, `pc:connection_name-instance_name-host_name:SUB`, em que *pc* é seu código de produto de dois caracteres e *SUB* é o tipo de banco de dados (os valores possíveis são RDB, ASM ou DG). O Nome do sistema gerenciado é limitado a 32 caracteres. O nome da instância que você especifica é limitado a 23 caracteres, menos o comprimento do seu nome do host e da conexão com o banco de dados. Por exemplo, se você especificar **dbconn** como o nome da conexão com seu banco de dados, **Oracle02** como o nome da instância de agente e se seu nome do host for *Prod204a*, o nome do sistema gerenciado será `RZ:dbconn-oracle02-Prod204a:RDB`. Este exemplo usa 22 dos 23 caracteres disponíveis para o nome de conexão com o banco de dados, nome da instância do agente e nome do host.

- Se você especificar um longo nome de instância, o nome do Sistema gerenciado é truncado e o código do agente não é exibido corretamente.
- O comprimento das variáveis *connection_name*, *instance_name* e *hostname_name* é truncado quando elas excedem 23 caracteres.
- Para evitar um nome do subnó truncado, altere a convenção de nomenclatura do subnó configurando as variáveis de ambiente a seguir: **KRZ_SUBNODE_INCLUDING_AGENTNAME**, **KRZ_SUBNODE_INCLUDING_HOSTNAME** e **KRZ_MAX_SUBNODE_ID_LENGTH**.
- Se você configurar **KRZ_SUBNODE_INCLUDING_AGENTNAME** como `NO`, a parte de ID do subnó não incluirá o nome da instância do agente. Por exemplo,
  - Nome do subnó padrão: *DBConnection-Instance-Hostname*
  - Nome do subnó com a variável de ambiente configurada para `NO`: *DBConnection-Hostname*
- Se você configurar **KRZ_SUBNODE_INCLUDING_HOSTNAME** para `NO`, a parte do ID do subnó do nome do subnó não inclui o nome do host. For example,
  - Nome do subnó padrão: *DBConnection-Instance-Hostname*
  - Nome do subnó com a variável de ambiente configurada para `NO`: *DBConnection-Instance*

Procedimento

1. Para configurar o agente em sistemas Windows, é possível usar a janela **IBM Performance Management** ou o arquivo de resposta silencioso.
   - "Configurando o agente nos sistemas Windows" na página 617.
   - "Configurando o agente usando o arquivo silencioso de resposta" na página 625.
2. Para configurar o agente em sistemas Linux e UNIX, é possível executar o script e responder aos prompts ou usar o arquivo de resposta silencioso.
   - "Configurando o agente respondendo aos prompts" na página 621.
   - "Configurando o agente usando o arquivo silencioso de resposta" na página 625.

O que Fazer Depois

Somente para a configuração avançada, o administrador de banco de dados Oracle deve permitir que o usuário Oracle execute o script `krzgrant.sql` para acessar o banco de dados, veja Executando o script krzgrant.sql.

No Console do Cloud APM, acesse seu Application Performance Dashboard para visualizar os dados que foram coletados. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Se você não conseguir visualizar os dados nos painéis do agente, primeiro verifique os logs de conexão do servidor e, em seguida, os logs do provedor de dados. Os caminhos padrão para esses logs são os seguintes:

- Linux AIX `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Para obter ajuda com a resolução de problemas, consulte o Fórum do Cloud Application Performance Management.

Configurando o agente nos sistemas Windows

É possível configurar o agente em sistemas operacionais Windows usando a janela **IBM Performance Management**. Após você atualizar os valores de configuração, inicie o agente para salvar os valores atualizados.

Procedimento

1. Clique em **Iniciar** > **Todos os programas** > **Agentes do IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito no modelo **Monitoring Agent for Oracle Database** e, em seguida, clique em **Configurar agente**.

   Lembre-se: Depois de configurar uma instância de agente pela primeira vez, a opção **Configurar agente** é desativada. Para configurar a instância de agente novamente, clique nela com o botão direito e clique em **Reconfigurar**.
3. Na janela Monitoring Agent for Oracle Database, conclua as seguintes etapas:
   a) Insira um nome de instância exclusivo para a instância do Monitoring Agent for Oracle Database e clique em **OK**.
4. Na área de janela Configuração do Banco de Dados Padrão da janela **Configurar ITCAM Extended Agent for Oracle Database**, execute as etapas a seguir:
   a) Insira o **Nome do usuário padrão**. Este é o ID do usuário do banco de dados padrão para conexões com o banco de dados.

      Esse ID do usuário é o ID que o agente usa para acessar a instância de banco de dados monitorada. Esse ID do usuário deve ter privilégios selecionados nas visualizações de desempenho dinâmico e nas tabelas que são necessários para o agente.
   b) Insira a **Senha padrão**. Esta é a senha que está associada ao ID do usuário do banco de dados padrão especificado.
   c) Se a versão do agente do Oracle for 8.0, execute esta etapa.
      1) Insira o **Oracle JDBC Jar File**. Este é o caminho completo para o arquivo JAR do driver JDBC do Oracle usado para se comunicar com o banco de dados Oracle. O driver do Oracle Java Database Connectivity (JDBC) que suporta as versões do banco de dados Oracle monitoradas pelo agente do Oracle deve estar disponível no computador agente.
   d) Se a versão do agente do Oracle for 6.3.1.10, execute estas etapas.
      1) Se o Agente Oracle Database estiver instalado no servidor de banco de dados Oracle que é monitorado, selecione **Usar bibliotecas no Oracle Home** e insira o **Diretório Oracle Home**. Opcionalmente para monitoramento local, a configuração Diretório inicial do Oracle pode ficar em branco e a variável de ambiente do sistema *ORACLE_HOME* é usada.
      2) Se o Agente Oracle Database for remoto a partir do servidor de banco de dados Oracle que é monitorado, selecione **Usar bibliotecas no Oracle Instant Client** e insira o **Diretório de Instalação do Oracle Instant Client**.
   e) Se precisar configurar opções de configuração avançadas, marque **Mostrar opções avançadas**; caso contrário, continue com a etapa 5.
   f) Os Diretórios de Arquivos de Configuração de Rede podem ser deixados em branco e o diretório padrão é usado. Se a versão do agente Oracle for 6.3.1.10, é possível inserir vários diretórios de arquivo de configuração de rede usando um ponto e vírgula (;) para separar os diretórios. Para o agente do Oracle versão 8.0, somente um diretório é suportado.

      Essa configuração contém o arquivo ou arquivos de configuração de rede do banco de dados Oracle. O diretório é definido pela variável de ambiente *TNS_ADMIN* para cada instância do banco de dados Oracle. O diretório padrão é %ORACLE_HOME%\NETWORK\ADMIN. Se este item não estiver

configurado, o diretório padrão será usado. Para desativar o uso do diretório padrão, configure a variável de ambiente do agente a seguir para false: KRZ_LOAD_ORACLE_NET=false.

g) Deixe o Nome do arquivo de definição de SQL customizado em branco. Não é utilizado.

h) Escolha se o listener dinâmico padrão será configurado nesta estação de trabalho.

O listener dinâmico padrão é (PROTOCOL=TCP)(HOST=localhost)(PORT=1521). Se o listener dinâmico padrão estiver configurado nesta estação de trabalho, configure esse valor como Yes.

i) Clique em **Avançar**.

5. Na área de janela **Configuração da Instância** da janela **Configurar ITCAM Extended Agent for Oracle Database**, execute as etapas a seguir:

Esse é o local onde as instâncias reais de conexão com o banco de dados estão definidas. É preciso incluir pelo menos uma. Esse também é o local onde você edita e exclui instâncias de conexão com o banco de dados. Se múltiplas configurações de instância de conexão com o banco de dados existirem, use a opção **Conexões com o banco de dados** para escolher a instância que será editada ou excluída.

a) Pressione **Novo** na seção **Conexões com o banco de dados**.

b) Insira um **Nome de conexão com o banco de dados** como um alias para a conexão com o banco de dados.

Esse alias pode ser qualquer coisa escolhida para representar a conexão com o banco de dados com as restrições a seguir. Somente letras, numerais arábicos, o caractere sublinhado e o caractere menos podem ser usados no nome da conexão. O comprimento máximo do nome de uma conexão é 25 caracteres.

c) Escolha um **Tipo de conexão**

1) (Opcional) Básico

O tipo de conexão padrão e mais comum é o **Básico**. Se você estiver inseguro sobre qual tipo de conexão precisa, sugere-se que escolha esse tipo de conexão.

a) Selecione o tipo de conexão **Básico** quando o banco de dados monitorado de destino for uma única instância, como uma instância do sistema de arquivos padrão ou uma única instância do ASM.

b) Insira o Nome do host como o nome do host ou endereço IP para o banco de dados.

c) Insira o número da Porta usado pelo banco de dados.

d) Selecione **Nome do serviço** ou **SID**.

i. Quando o **Nome do Serviço** for selecionado, insira o nome do serviço que seja uma representação lógica de um banco de dados, uma sequência que é o nome do serviço de banco de dados global.

Um nome do serviço é uma representação lógica de um banco de dados, que é a maneira que um banco de dados é apresentado aos clientes. Um banco de dados pode ser apresentado como vários serviços e um serviço pode ser implementado como várias instâncias de banco de dados. O nome do serviço é uma sequência que é o nome do banco de dados global, ou seja, um nome composto pelo nome do banco de dados e o nome do domínio, inseridos durante a instalação ou a criação do banco de dados. Se não tiver certeza de qual é o nome do banco de dados global, é possível obtê-lo do valor do parâmetro SERVICE_NAMES no arquivo de parâmetro de inicialização.

ii. Quando **SID** é selecionado, insira o Identificador do Sistema Oracle que identifica uma instância específica de um banco de dados em execução.

Este é o Identificador do sistema Oracle que identifica uma instância específica de um banco de dados.

Continue com a etapa 5d.

2) (Opcional) TNS

a) Selecione o tipo de conexão **TNS** se a variável de ambiente do sistema *ORACLE_HOME* estiver configurada e o alias TNS para o banco de dados monitorado de destino for definido no arquivo `$ORACLE_HOME/network/admin/tnsnames.ora`.

b) Insira o nome do **`alias TNS`**.

Continue com a etapa 5d.

3) (Opcional) Avançado

a) Selecione o tipo de conexão **Avançada** quando houver mais de uma instância do Oracle em vários nós físicos para o banco de dados monitorado de destino. Por exemplo, um ASM com o banco de dados Real Applications Cluster (RAC).

b) Insira a **`Sequência de conexões do Oracle`**.

Este atributo suporta todos os métodos de nomenclatura de rede Oracle conforme a seguir:

- Sequência URL do SQL Connect do formato:`//host:port/service name`. Por exemplo, `//dlsun242:1521/bjava21`.
- Par de valor de palavra-chave do Oracle Net. Por exemplo,

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=dlsun242) (PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=bjava21)))
```

- Entradas **TNSNAMES**, como **inst1,** com a variável de ambiente *TNS_ADMIN* ou *ORACLE_HOME* configurada e os arquivos de configuração configurados.

Continue com a etapa 5d.

d) Marque **Usar um nome do usuário e senha diferentes** para que essa conexão use credenciais diferentes das credenciais padrão configuradas na etapa 4a e etapa 4b. Caso contrário, continue com a etapa 5g.

e) Insira o **`Nome de usuário do banco de dados`** para essa conexão.

Esse ID do usuário é o ID que o agente usa para acessar a instância de banco de dados monitorada. Esse ID do usuário deve ter privilégios selecionados nas visualizações de desempenho dinâmico e nas tabelas que são necessários para o agente.

f) Insira a **`Senha do banco de dados`**. A senha que está associada ao ID do usuário do banco de dados especificado.

g) Selecione uma **Função** que corresponda às permissões concedidas às credenciais de conexão com o banco de dados.

A função é o conjunto de privilégios a serem associados à conexão. Para um usuário que foi concedido o privilégio do sistema SYSDBA, especifique uma função que inclui esse privilégio. Para instâncias ASM, use a função **SYSDBA** ou **SYSASM**.

h) Marque **Mostrar opções de monitoramento de log remoto** se você monitorar logs de alerta remotos do Oracle a partir dessa instância de agente, caso contrário, continue na etapa 5k.

i) Digite um caminho ou use **Procurar** para selecionar os **`Caminhos do arquivo de log de alerta do Oracle`**.

Os caminhos de arquivo absolutos de arquivos de log de alerta mapeados para instâncias de banco de dados remoto nesta conexão com o banco de dados. O agente monitora logs de alerta por meio da leitura desses arquivos. Geralmente localizado em `$ORACLE_BASE/diag/rdbms/`*`DB_NAME`*`/`*`SID`*`/trace/alert_`*`SID`*`.log`. Por exemplo, se *DB_NAME* e *SID* forem db11g e *ORACLE_BASE* for `/home/dbowner/app/oracle`, o log de alerta estaria localizado em `/home/dbowner/app/oracle/diag/rdbms/db11g/db11g/trace/alert_db11g.log`.

Windows Se o Agente Oracle Database for executado e ler os arquivos de log de alerta por meio da rede, o caminho de arquivo remoto deverá seguir a convenção universal de nomenclatura para sistemas Windows. Por exemplo, `\\tivx015\path\alert_orcl.log`.

Windows

Importante: Insira o caminho e o nome do arquivo de log de alerta juntos. Um driver de rede mapeado não é suportado para o caminho de log de alerta.

Linux AIX Se o Agente Oracle Database estiver em um servidor remoto, será necessário um sistema de arquivos montado localmente para monitorar seus logs de alerta remotos.

Windows Diversos arquivos são separados por ponto e vírgula (;).

Linux AIX Diversos arquivos são separados por dois pontos (:).

Cada arquivo é correspondido a uma instância de banco de dados usando o padrão de nome do arquivo `alert_`*`instance`*`.log` ou, se ele não for correspondido, será ignorado.

Os arquivos de log de alerta da instância de banco de dados local são descobertos automaticamente.

j) Selecione ou insira o **Conjunto de caracteres do arquivo de log de alerta do Oracle**. Esta é a página de códigos dos arquivos de log de alerta mapeados.

Se esse parâmetro estiver em branco, a configuração do código de idioma atual do sistema será usada, por exemplo:

- ISO8859_1, codificação ISO 8859-1 da Europa Ocidental
- UTF-8, Codificação UTF-8 de Unicode
- GB18030, Codificação GB18030 de chinês simplificado
- CP950, Codificação de chinês tradicional
- EUC_JP, Codificação de japonês
- EUC_KR, Codificação de coreano

Para obter a lista integral de todas as páginas de códigos suportadas, consulte Páginas de códigos suportadas pelo ICU.

k) Clique em **Aplicar** para salvar essas configurações da instância de conexão com o banco de dados na seção **Conexões com o banco de dados**.

l) (Opcional) Teste a nova conexão com o banco de dados.

1) Selecione a nova conexão com o banco de dados na seção **Conexões com o banco de dados**.

2) Clique em **Conexão de Teste**.

3) Observe os resultados na janela de resultados **Testar conexão**.

- **Resultado do teste** de exemplo bem-sucedido:

```
Testando conexão config1 ...
Com Êxito
```

- **Resultado do teste** de exemplo malsucedido:

```
Testando conexão config1 ...
KBB_RAS1_LOG; Configure MAXFILES como 1
ORA-12514: TNS:listener atualmente não sabe sobre o serviço solicitado no descritor de
conexão
Falha
```

m) Clique em **Avançar**.

6. Leia as informações na área de janela **Resumo** da janela **Configurar ITCAM Extended Agent for Oracle Database**, em seguida, clique em **OK** para concluir a configuração da instância do agente.
7. Na janela **IBM Performance Management**, clique com o botão direito em **Monitoring Agent for Oracle Database** e, em seguida, clique em **Iniciar**.

O que Fazer Depois

- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte “Iniciando o Console do Cloud APM” na página 975.

Configurando o agente respondendo aos prompts

Para configurar o agente nos sistemas operacionais Linux e UNIX, execute o script de configuração da linha de comandos e responda aos seus prompts.

Procedimento

1. Abra o diretório *install_dir*/bin, em que *install_dir* é o diretório de instalação do Agente Oracle Database.
2. (Opcional) Para listar os nomes de todas as instâncias do agente configuradas existentes, execute o seguinte comando: **./cinfo -o rz**.
3. Para configurar o Agente Oracle Database, execute o seguinte comando: **./oracle_database-agent.sh config** *instance_name*.
4. Quando solicitado a Editar configurações do 'Monitoring Agent for Oracle Database' , pressione **Enter**. O valor padrão é Yes.
5. Para inserir as informações de Configuração do Banco de Dados Padrão, execute as etapas a seguir:

   Nota: A seção Configuração do Banco de Dados Padrão não é a configuração da instância de conexão com o banco de dados. É uma seção de modelo para configurar o que é usado como os valores padrão ao incluir as configurações reais da instância de conexão com o banco de dados, que começam na etapa 6.

   a) Quando for solicitado o Nome do usuário padrão, digite o ID do usuário do banco de dados padrão para conexões com o banco de dados e pressione **Enter**.

   Esse ID do usuário é o ID que o agente usa para acessar a instância de banco de dados monitorada. Esse ID do usuário deve ter privilégios selecionados nas visualizações de desempenho dinâmico e nas tabelas que são necessários para o agente.

   b) Quando for solicitado a Inserir senha padrão, digite a senha que está associada ao ID do usuário do banco de dados padrão especificado e pressione **Enter**. Em seguida, se solicitado, confirme a senha.

   c) Se a versão do agente do Oracle for 8.0, execute esta etapa.

      1) Insira o **Oracle JDBC Jar File**. Este é o caminho completo para o arquivo JAR do driver JDBC do Oracle usado para se comunicar com o banco de dados Oracle. O driver do Oracle Java Database Connectivity (JDBC) que suporta as versões do banco de dados Oracle monitoradas pelo agente do Oracle deve estar disponível no computador agente.

   d) Se a versão do agente do Oracle for 6.3.1.10, execute estas etapas.

      1) Quando for solicitado o Diretório Oracle Home, se o Agente Oracle Database estiver instalado no servidor de banco de dados Oracle monitorado, digite o diretório Oracle home e pressione **Enter**. Se o Agente Oracle Database não estiver instalado no servidor de banco de dados Oracle que será monitorado, deixe essa configuração em branco, pressione **Enter** e execute a próxima etapa. Se desejar limpar o valor para o diretório Diretório inicial do Oracle, pressione a barra de espaço e, em seguida, pressione **Enter**.

         Nota: Opcionalmente para monitoramento local, o Diretório inicial do Oracle e o Diretório de instalação do Oracle Instant Client podem ficar em branco e a variável de ambiente do sistema *ORACLE_HOME* é usada.

      2) Se o Agente Oracle Database for remoto a partir do servidor de banco de dados Oracle monitorado, digite o diretório Diretório de Instalação do Oracle Instant Client e pressione **Enter**. Se você configurar o Diretório Oracle Home na etapa “5.d.i” na página 621, esse valor será ignorado.

   e) Os Diretórios de Arquivos de Configuração de Rede podem ser deixados em branco e o diretório padrão é usado. Se a versão do agente Oracle for 6.3.1.10, é possível inserir vários diretórios de arquivo de configuração de rede usando Windows ";" ou Linux AIX ":" para separar os diretórios. Para o agente do Oracle versão 8.0, somente um diretório é suportado. Pressione **Enter**.

Essa configuração contém o arquivo ou arquivos de configuração de rede do banco de dados Oracle. O diretório é definido pela variável de ambiente *TNS_ADMIN* para cada instância do banco de dados Oracle. O diretório padrão é Linux AIX `$ORACLE_HOME/network/admin` ou Windows `%ORACLE_HOME%\NETWORK\ADMIN`. Se este item não estiver configurado, o diretório padrão será usado. Para desativar o uso do diretório padrão, configure a variável de ambiente do agente a seguir para false: `KRZ_LOAD_ORACLE_NET=false`.

f) Escolha se o listener dinâmico padrão será configurado nesta estação de trabalho e pressione **Enter**.

O listener dinâmico padrão é `(PROTOCOL=TCP)(HOST=localhost)(PORT=1521)`. Se o listener dinâmico padrão estiver configurado nesta estação de trabalho, configure esse valor como True.

g) Deixe o `Nome do arquivo de definição de SQL customizado` em branco. Não é utilizado.

6. Você é solicitado a `Editar configurações de 'Conexão com o banco de dados'` depois de ver a seguinte saída na tela:

```
Configuração da instância:
Resumo:
Conexão com o banco de dados:
```

Nota: Esta etapa é onde as instâncias reais de conexão com o banco de dados estão definidas. É preciso incluir pelo menos uma. Esse também é o local onde você edita e exclui instâncias de conexão com o banco de dados. Se múltiplas configurações da instância de conexão com o banco de dados existirem, use a opção `Avançar` para ignorar as instâncias que não precisam ser editadas ou excluídas, até que você chegue na instância que precisa editar ou excluir.

7. Para incluir uma nova conexão com o banco de dados, digite 1 e pressione **Enter**.
8. Para inserir as informações de conexão com o banco de dados, execute as etapas a seguir:

a) Quando for solicitado o `Nome da conexão com o banco de dados`, digite um alias para a conexão com o banco de dados e pressione **Enter**.

Esse alias pode ser qualquer coisa escolhida para representar a conexão com o banco de dados com as restrições a seguir. Somente letras, numerais arábicos, o caractere sublinhado e o caractere menos podem ser usados no nome da conexão. O comprimento máximo do nome de uma conexão é 25 caracteres.

b) Quando for solicitado o `Tipo de conexão`, selecione um dos seguintes tipos de conexão:

1) (Opcional) Básico

O tipo de conexão padrão e mais comum é o **Básico**. Se você estiver inseguro sobre qual tipo de conexão precisa, sugere-se que escolha esse tipo de conexão.

a) Selecione o tipo de conexão **Básica** se o banco de dados monitorado de destino for uma única instância, como uma instância do sistema de arquivos padrão ou uma única instância do ASM.

b) Quando solicitado para `Hostname`, digite o nome do host ou o endereço IP para o banco de dados Oracle e pressione **Enter**.

c) Quando for solicitada a `Porta`, digite o número da porta e pressione **Enter**.

d) Insira uma das duas próximas configurações. `Nome do serviço` ou `SID`.

i. (Opcional) Quando for solicitado o `Nome do serviço`, digite o nome do serviço que é uma representação lógica de um banco de dados, uma sequência que é o nome do serviço de banco de dados global, pressione **Enter** e continue com a etapa 8c.

Um nome do serviço é uma representação lógica de um banco de dados, que é a maneira que um banco de dados é apresentado aos clientes. Um banco de dados pode ser apresentado como vários serviços e um serviço pode ser implementado como várias instâncias de banco de dados. O nome do serviço é uma sequência que é o nome do banco de dados global, ou seja, um nome composto pelo nome do banco de dados e o nome do domínio, inseridos durante a instalação ou a criação do banco de dados. Se não tiver certeza de qual é o nome do banco de dados global, é possível obtê-lo do valor do

parâmetro SERVICE_NAMES no arquivo de parâmetro de inicialização. Esse parâmetro poderá ser deixado em branco se você configurar o SID na etapa "8.b.i.4.b" na página 623.

ii. (Opcional) Quando for solicitado do SID, digite o Identificador do sistema Oracle que identifica uma instância específica de um banco de dados em execução, pressione **Enter** e continue com a etapa 8c.

Esse parâmetro é o Oracle System Identifier que identifica uma instância específica de um banco de dados. Se o Nome do Serviço foi definido na etapa "8.b.i.4.a" na página 622, será possível deixar este item em branco.

2) (Opcional) TNS

a) Selecione o tipo de conexão **TNS** quando a variável de ambiente do sistema *ORACLE_HOME* estiver configurada e o alias TNS para o banco de dados monitorado de destino estiver definido no arquivo $ORACLE_HOME/network/admin/tnsnames.ora.

b) Digite o nome do alias TNS, pressione **Enter** e continue com a etapa 8c.

3) (Opcional) Avançado

a) Selecione o tipo de conexão **Avançada** quando houver mais de uma instância do Oracle em vários nós físicos para o banco de dados monitorado de destino. Por exemplo, um ASM com o banco de dados Real Applications Cluster (RAC).

b) Digite a sequência de conexões do Oracle, pressione **Enter** e continue com a etapa 8c.

Este atributo suporta todos os métodos de nomenclatura de rede Oracle conforme a seguir:

- Sequência URL do SQL Connect do formato://host:port/service name. Por exemplo, //dlsun242:1521/bjava21.
- Par de valor de palavra-chave do Oracle Net. Por exemplo,

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=dlsun242) (PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=bjava21)))
```

- Entradas **TNSNAMES**, como **inst1,** com a variável de ambiente *TNS_ADMIN* ou *ORACLE_HOME* configurada e os arquivos de configuração configurados.

Nota: A descrição mostrada durante a configuração da linha de comandos pode ter uma barra invertida antes de dois-pontos (\:) e antes de símbolos de sinal de igual (\=). Não digite barras invertidas na sequência de conexões. Elas são exibidas na descrição para escapar o comportamento normal de interpretação do sinal de igual como parte de um comando, e em vez disso, interpretá-las meramente como texto.

c) Continue com a etapa 8c.

c) Quando for solicitado o Nome de usuário do banco de dados, digite o ID do usuário do banco de dados para a conexão e pressione **Enter**.

Para instâncias do sistema de arquivos padrão, esse ID do usuário deve ter privilégios de seleção nas visualizações de desempenho dinâmico e nas tabelas necessárias para o agente.

Para instâncias ASM, use uma conta com a função **SYSDBA** ou **SYSASM**. Por exemplo, a conta sys.

d) Quando for solicitado a Inserir a senha do banco de dados, digite a senha que está associada ao ID do usuário do banco de dados especificado.

e) Quando solicitado para a Função, escolha a função que corresponda às permissões concedidas ao ID do usuário especificado, e pressione **Enter**.

A função é o conjunto de privilégios a serem associados à conexão. Para um usuário que foi concedido o privilégio do sistema SYSDBA, especifique uma função que inclui esse privilégio.

Para instâncias ASM, use a função **SYSDBA** ou **SYSASM**.

f) Quando forem solicitados os `Caminhos do arquivo de log de alerta do Oracle (incluindo o nome do arquivo de log de alerta)`, digite os caminhos do log de alerta e pressione **Enter**.

Este parâmetro destina-se a todos os caminhos de arquivos absolutos de arquivos de log de alerta mapeados para instâncias de banco de dados remoto nessa conexão com o banco de dados. O agente monitora logs de alerta por meio da leitura desses arquivos. Geralmente localizado em `$ORACLE_BASE/diag/rdbms/`*`DB_NAME`*`/`*`SID`*`/trace/alert_`*`SID`*`.log`. Por exemplo, se *DB_NAME* e *SID* forem db11g e *ORACLE_BASE* for `/home/dbowner/app/oracle`, o log de alerta estaria localizado em `/home/dbowner/app/oracle/diag/rdbms/db11g/db11g/trace/alert_db11g.log`.

Windows Se o Agente Oracle Database for executado e ler os arquivos de log de alerta na rede, o caminho de arquivo remoto deverá seguir a convenção universal de nomenclatura para sistemas Windows. Por exemplo, `\\tivx015\path\alert_orcl.log`.

Importante: Insira o caminho e o nome do arquivo de log de alerta juntos. Um driver de rede mapeado não é suportado para o caminho de log de alerta.

Linux AIX Se o Agente Oracle Database for executado, é necessário que haja um sistema de arquivos montado localmente para os logs de alerta remotos.

Windows Diversos arquivos são separados por ponto e vírgula (;).

Linux AIX Diversos arquivos são separados por dois pontos (:).

Cada arquivo é correspondido a uma instância de banco de dados usando o padrão de nome do arquivo `alert_`*`instance`*`.log` ou, se ele não for correspondido, será ignorado.

Os arquivos de log de alerta da instância de banco de dados local podem ser descobertos automaticamente.

g) Quando for solicitado o **`Conjunto de caracteres do arquivo de log de alerta do Oracle`**, digite a página de códigos dos arquivos de log de alerta mapeados e pressione **Enter**.

Se esse parâmetro estiver em branco, a configuração do código de idioma atual do sistema será usada, por exemplo:

- ISO8859_1, codificação ISO 8859-1 da Europa Ocidental
- UTF-8, Codificação UTF-8 de Unicode
- GB18030, Codificação GB18030 de chinês simplificado
- CP950, Codificação de chinês tradicional
- EUC_JP, Codificação de japonês
- EUC_KR, Codificação de coreano

Para obter a lista integral de todas as páginas de códigos suportadas, consulte Páginas de códigos suportadas pelo ICU.

9. Quando solicitado novamente para `Editar configurações de 'Conexão com o Banco de Dados'`, você verá o nome da conexão com o banco de dados que configurar na etapa 8a. É possível editá-la novamente ou excluí-la. Se você tiver mais de uma instância de conexão com o banco de dados que já esteja configurada, use **Avançar** para percorrê-las.
10. (Opcional) Para incluir outra conexão com o banco de dados para monitorar várias instâncias de banco de dados com essa instância de agente, digite 1, pressione **Enter** e retorne à Etapa 8.
11. Quando tiver concluído a modificação das conexões com o banco de dados, digite 5 e pressione **Enter** para sair do processo de configuração.
12. Para iniciar o agente, insira:
`install_dir``/bin/oracle_database-agent.sh start `*`instance_name`*.

O que Fazer Depois

- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o agente usando o arquivo silencioso de resposta

O arquivo de resposta silencioso contém os parâmetros de configuração do agente. É possível editar o arquivo de resposta silencioso para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

O arquivo silencioso de resposta contém os parâmetros de configuração do agente com valores padrão que são definidos para alguns parâmetros. É possível editar o arquivo silencioso de resposta para especificar os valores diferentes para os parâmetros de configuração.

Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

1. Abra o arquivo `oracle_silent_config.txt` em um editor de texto:
   - Linux AIX *install_dir*`/samples/oracle_database_silent_config.txt`.
   - Windows *install_dir*`\samples\oracle_database_silent_config.txt`
2. Para **Nome do usuário padrão**, digite o nome do usuário do banco de dados padrão para conexões com o banco de dados que são criadas para essa instância do agente. Por exemplo, **KRZ_CONN_USERID=**`user1`.

   Nota: Esse usuário deve ter privilégios suficientes para concluir as tarefas que este agente executa enquanto estiver conectado ao banco de dados, como consultar tabelas.
3. Para **Senha padrão**, deve-se inserir a senha que está associada ao usuário do banco de dados padrão especificado. Por exemplo, **KRZ_CONN_PASSWORD=**Senha.
4. Se a versão do agente do Oracle for 8.0, execute esta etapa.
   a) Insira o **Oracle JDBC Jar File**. Este é o caminho completo para o arquivo JAR do driver JDBC do Oracle usado para se comunicar com o banco de dados Oracle.

      O driver do Oracle Java Database Connectivity (JDBC) que suporta as versões do banco de dados Oracle monitoradas pelo agente do Oracle deve estar disponível no computador agente.
5. Se a versão do agente do Oracle for 6.3.1.10, execute estas etapas.
   a) Se o Agente Oracle Database estiver instalado no servidor de banco de dados Oracle monitorado, digite o diretório `Oracle home`. Por exemplo, **KRZ_ORACLE_HOME=**`home_path`.

      Nota: Para parâmetros opcionais como esse, remova o símbolo hash (#) à esquerda para usá-los.

      Se o Agente Oracle Database não estiver instalado no servidor de banco de dados Oracle que será monitorado, deixe essa configuração em branco e conclua a próxima etapa.

      Nota: Opcionalmente, para monitoramento local, o `Oracle Home Directory` e o `Oracle Instant Client Installation Directory` podem ser deixados em branco (comentados usando um símbolo hash (#) na primeira posição da linha de parâmetro no arquivo de texto de configuração silenciosa) e a variável de ambiente do sistema *ORACLE_HOME* é usada.
   b) Se o Agente Oracle Database for remoto a partir do servidor de banco de dados Oracle monitorado, digite o diretório `Oracle Instant Client Installation Directory`. Se você inserir o diretório `Diretório inicial do Oracle` na etapa anterior, esse valor será ignorado.

- Windows Defina o caminho de pasta completo do diretório **Oracle Home** que contém os arquivos de biblioteca da Oracle Call Interface (OCI). Se o caminho completo do arquivo oci.dll for C:\instantclient_10_2\oci.dll, deve-se definir este caminho C:\instantclient_10_2. Por exemplo, **KRZ_INSTANT_CLIENT_LIBPATH=**C:\instantclient_10_2
- AIX Defina o caminho de pasta completo do diretório **Oracle Home** que contém os arquivos de biblioteca da Oracle Call Interface (OCI). Se o caminho completo do arquivo libocci.so.10.1 for /home/tivoli/oci/libocci.so.10.1, deve-se definir este caminho /home/tivoli/oci. Por exemplo, **KRZ_INSTANT_CLIENT_LIBPATH=**/home/tivoli/oci

6. Os Diretórios de Arquivos de Configuração de Rede podem ser deixados em branco e o diretório padrão é usado. O Agente Oracle Database usa esse caminho de arquivo para obter o arquivo tnsnames.ora. Esse diretório é definido pela variável de ambiente *TNS_ADMIN* para cada instância do banco de dados Oracle. O diretório padrão é Linux AIX $ORACLE_HOME/network/admin ou Windows %ORACLE_HOME%\NETWORK\ADMIN. Se você inserir essa configuração com múltiplos diretórios de arquivo de configuração de rede, use Windows ";" ou Linux AIX ":" para separar os diretórios.

   Se você estiver monitorando bancos de dados Oracle remotamente, será possível copiar arquivos de configuração de rede do sistema remoto para o sistema onde o agente está instalado. Além disso, é possível mesclar o conteúdo de arquivos de configuração de rede no sistema remoto com os arquivos de configuração de rede no sistema em que o agente está instalado.
7. Para **Dynamic listener**, verifique se o listener dinâmico padrão está configurado. O listener dinâmico padrão é (PROTOCOL=TCP)(HOST=localhost)(PORT=1521). Se o listener dinâmico padrão estiver configurado, configure esse valor como TRUE conforme mostrado aqui; **KRZ_DYNAMIC_LISTENER=**TRUE.

   Os valores válidos são TRUE e FALSE.
8. Deixe o Nome do arquivo de definição de SQL customizado em branco. Não é utilizado.
9. Começando aqui, as instâncias de conexão com o banco de dados reais são definidas. É preciso incluir pelo menos uma. As entradas para uma instância são fornecidas no oracle_silent_config.txt com o nome da instância *config1*. Se você mudar o nome da instância, certifique-se de mudar todas as referências.

   Esse alias pode ser qualquer coisa escolhida para representar a conexão com o banco de dados com as restrições a seguir. Somente letras, numerais arábicos, o caractere sublinhado e o caractere menos podem ser usados no nome da conexão. O comprimento máximo do nome de uma conexão é 25 caracteres.
10. Para **Tipo de conexão**, especifique um dos tipos de conexão a seguir: **Básico**, **TNS** ou **Avançado**. Por exemplo, **KRZ_CONN_TYPE.config1=**Basic.
11. Para o tipo de conexão selecionado na etapa anterior, especifique os parâmetros necessários:

    Basic

    - Para **Hostname**, especifique o nome do host ou o endereço IP do banco de dados Oracle, por exemplo: **KRZ_CONN_HOST.config1=** hostname.
    - Para **Port**, especifique a porta do Listener para o banco de dados Oracle, por exemplo: **#KRZ_CONN_PORT.config1=** 1521.
    - Para **Nome do serviço**, especifique a representação lógica do banco de dados usando uma sequência para o nome do banco de dados global, por exemplo: **KRZ_CONN_SERVICE.config1=** orcl.

      Importante: Se você não definir o Nome do serviço, deverá especificar o Oracle System Identifier (SID).

      Para o **Oracle System Identifier (SID)**, especifique um SID que identifica uma instância específica de um banco de dados em execução, por exemplo: **KRZ_CONN_SID.config1=** sid.

TNS

Para **Alias TNS**, especifique o nome do alias de rede do arquivo `tnsnames.ora`. Por exemplo, **KRZ_CONN_TNS.config1=** `tnsalias`.

Avançada

Para a **Sequência de conexões Oracle**, especifique a sequência de conexões do banco de dados para OCI. Por exemplo, **KRZ_CONN_STR.config1=** `//host:port/service`

Essa sequência suporta todos os métodos de nomenclatura do Oracle Net, conforme mostrado aqui.

- Para uma sequência URL de SQL Connect:

```
//host:[port][/service name]
```

- Para um par de valores de palavra-chave do Oracle Net:

```
"(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=dlsun242) (PORT=1521))
(CONNECT_DATA=(SERVICE_NAME=bjava21)))"
```

Essa sequência também suporta entradas **TNSNAMES**, por exemplo, **inst1** em que a variável de ambiente *TNS_ADMIN* ou *ORACLE_HOME* é configurada e os arquivos de configuração são configurados.

Importante: Esse atributo se aplica somente ao tipo de conexão avançada.

12. Para **Database Username**, é possível especificar o nome do usuário do banco de dados para a conexão, por exemplo: **KRZ_CONN_USERID=**`UserID`.

    Esse usuário deve ter privilégios suficientes para concluir as tarefas que o agente requer enquanto ele estiver conectado ao banco de dados, por exemplo, criar, editar e excluir tabelas.

    Se esse campo estiver vazio, o agente usa o nome de usuário padrão na seção de configuração do banco de dados padrão. Se **Database Username** não foi configurado, o nome de usuário padrão será usado para essa conexão.

13. Para **Database Password**, é possível especificar a senha associada ao usuário de banco de dados especificado, por exemplo: **KRZ_CONN_PASSWORD=**`Password`.

    Se esse campo estiver vazio, o agente usará a senha padrão na seção de configuração do banco de dados padrão. Se **Database Password** não tiver sido configurado, a senha padrão será usada para essa conexão.

14. Para **Role**, é possível especificar o conjunto de privilégios que estão associados à conexão, por exemplo: **KRZ_CONN_MODE.config1=**`DEFAULT`.

    Os valores válidos incluem *SYSDBA*, *SYSOPER*, *SYSASM*, e *DEFAULT*.

    Para um usuário que tenha concedido o privilégio do sistema *SYSDBA*, é possível especificar uma conexão que inclua esse privilégio. Se esse item não estiver definido, é possível designar a função *DEFAULT* para o usuário.

15. Para **Oracle Alert Log File Paths**, quando o nome do arquivo de log de alerta é incluído, você pode especificar o caminho de arquivo absoluto dos arquivos de log de alerta mapeados para as instâncias de banco de dados remoto Neste banco de dados Conexão . Por exemplo, **KRZ_LOG_PATHS.config1=**`AlertLogPath`.

    Windows Use um ponto e vírgula (;) para separar os diversos arquivos.

    Linux AIX Use dois pontos (:) para separar os diversos arquivos.

    Cada arquivo é correspondido a uma instância de banco de dados pelo padrão de nome de arquivo `alert_`*`instance`*`.log`. De forma alternativa, ele será ignorado, se não for correspondido.

    Os arquivos de `local database instance alert log` são descobertos automaticamente.

    Se **Oracle Alert Log File Paths** não foi configurado, o `Log de Alerta` não está disponível.

16. Para **Oracle Alert Log File Charset**, é possível especificar a página de código dos arquivos de log de alerta mapeados. Por exemplo, **KRZ_LOG_CHARSET.config1=** `CharSet`

    Se esse campo estiver vazio, a configuração do código de idioma atual do sistema será utilizada, conforme mostrado aqui:

    ```
    ISO8859_1: ISO 8859-1 Western European encoding
    UTF-8: UTF-8 encoding of Unicode
    GB18030: Simplified Chinese GB18030 encoding
    CP950: Traditional Chinese encoding
    EUC_JP: Japanese encoding
    ```

17. Salve e feche o arquivo `oracle_database_silent_config.txt`. Em seguida, insira: *`install_dir`*`/bin/oracle_database-agent.sh config` *`instance_name install_dir`*`/samples/oracle_database_silent_config.txt`
    em que *`instance_name`* é o nome que você deseja fornecer para a instância.
18. Para iniciar o agente, insira: *`install_dir`*`/bin/oracle_database-agent.sh start` *`instance_name`*.

O que Fazer Depois

- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Concedendo privilégios ao usuário do agente do Banco de Dados Oracle

Após instalar o agente, deve-se conceder privilégios à conta do usuário do Oracle que é usada pelo Agente Oracle Database.

É possível conceder privilégios para os usuários a seguir:

- Usuários da instância do sistema de arquivos padrão (não ASM)
- Usuários não de SYS da instância do ASM com RAC

Concedendo privilégios aos usuários para instâncias do sistema de arquivos padrão
Para instâncias do sistema de arquivos padrão, o ID do usuário do Oracle que o Agente Oracle Database usa deve ter privilégios de seleção nas visualizações de desempenho dinâmico, tabelas e visualizações de dicionário de dados que são necessários para o agente. Ele também deve ter outro objeto do Oracle e privilégios do sistema que são necessários para executar alguns comandos do banco de dados.

Procedimento

1. (Opcional) Se um ID do usuário do banco de dados Oracle não existir, crie esse ID usando recursos do Oracle e executando o seguinte comando: `criar usuário` *`UserName`* `identificado por` *`Password`*
2. Conceda privilégios de seleção para as visualizações de desempenho dinâmico, tabelas e visualizações de dicionário de dados para o ID do usuário Oracle criado por meio da execução do script **krzgrant.sql** que é fornecido com o Agente Oracle Database. Esta etapa deve ser executada antes que o agente seja configurado. Para obter instruções sobre como customizar e executar o script **krzgrant.sql**, consulte "Customizando o script krzgrant.sql" na página 629 e "Executando o script krzgrant.sql" na página 629.

   Nota: Os privilégios de seleção para as visualizações de desempenho dinâmico, tabelas e visualizações de dicionário de dados dependem dos recursos do banco de dados Oracle em ambientes de aplicativos específicos. É possível conceder privilégios autorizados do Oracle para o ID do usuário de banco de dados Oracle somente para as visualizações de desempenho dinâmico, tabelas e visualizações de dicionário de dados utilizadas pelo Agente Oracle Database.
3. Conceda outros privilégios de objeto e privilégios de sistema Oracle ao ID do usuário Oracle que o Agente Oracle Database usa usando recursos do Oracle.

Customizando o script krzgrant.sql

Se você não desejar permitir privilégios de seleção autorizados do Oracle em algumas visualizações de desempenho dinâmico, tabelas e visualizações de dicionário de dados no script **krzgrant.sql**, poderá customizar o script **krzgrant.sql** antes de executá-lo.

Nota: A instância de agente verifica todos os privilégios padrão no script **krzgrant.sql** e relata um evento de agente com uma falta de privilégios quando o agente for iniciado. É possível desativar a verificação de privilégio usando a configuração de variável a seguir: KRZ_CHECK_ORACLE_PRIVILEGE=FALSE. A etapa de conexão de teste da configuração da GUI verifica todos os privilégios do Oracle definidos no arquivo `krzgrant.sql`. Se você confirmar que o usuário do Oracle tem os privilégios corretos, ignore se a verificação de privilégios falhar na etapa conexão de teste.

Edite o arquivo `krzgrant.sql` em um editor de texto simples para remover ou incluir o prefixo '--' no início de instruções de concessão para ignorar a execução de concessão para as tabelas ou visualizações Oracle não autorizadas.

Por exemplo, altere as linhas a seguir:

```
    execute immediate 'grant select on DBA_HIST_SNAPSHOT to '||userName;
    execute immediate 'grant select on DBA_HIST_SQLSTAT to '||userName;
    execute immediate 'grant select on DBA_HIST_SQLTEXT to '||userName;
    execute immediate 'grant select on DBA_HIST_SQL_PLAN to '||userName;
    execute immediate 'grant select on DBA_HIST_SYSMETRIC_SUMMARY to '||userName;
```

para estas linhas:

```
--    execute immediate 'grant select on DBA_HIST_SNAPSHOT to '||userName;
--    execute immediate 'grant select on DBA_HIST_SQLSTAT to '||userName;
--    execute immediate 'grant select on DBA_HIST_SQLTEXT to '||userName;
--    execute immediate 'grant select on DBA_HIST_SQL_PLAN to '||userName;
--    execute immediate 'grant select on DBA_HIST_SYSMETRIC_SUMMARY to '||userName;
```

Concedendo privilégios a usuários não SYS para instâncias ASM

Deve-se conectar as instâncias ASM que estão usando as funções SYSDBA e SYSASM para os usuários. Se você não quiser usar a conta SYS para se conectar a instâncias ASM, crie uma conta do usuário e conceda as funções SYSDBA e SYSASM à conta.

Procedimento

1. Execute os comandos a seguir para criar uma conta do usuário e conceder funções:
   - Efetue login no banco de dados do ASM com a função SYSASM para criar um novo usuário para um agente e conceder a função SYSDBA ou a função SYSASM:
     a. `create user UserName identified by Password`
     b. `grant sysdba to UserName`

     or

     `grant sysasm to UserName`
2. Ao criar a conexão do ASM na janela de configuração, especifique o *UserName* do usuário e a função SYSDBA ou SYSASM.

   Nota: Se você escolher a função SYSASM para acessar o banco de dados ASM, deverá configurar a instância de agente usando o início do Oracle ou o cliente instantâneo do Oracle para conectar-se ao banco de dados Oracle.

Executando o script krzgrant.sql

Antes de Iniciar

- Se você não executar o script **krzgrant.sql**, um evento será criado na área de trabalho de eventos do agente.

- Para concluir o procedimento de instalação, consulte Capítulo 6, “Instalando os agentes”, na página 117.

Após a instalação, é possível localizar o script **krzgrant.sql** no diretório a seguir:

- Windows *install_dir*\TMAITM6_X64
- Linux AIX *install_dir*/*architecture*/rz/bin

em que:

install_dir
Diretório de instalação para o Agente Oracle Database.

architecture
O identificador de arquitetura do sistema IBM Application Performance Management ou Cloud APM. Por exemplo, lx8266 representa o Linux Intel v2.6 (64 bits). Para obter uma lista completa dos códigos de arquitetura, consulte o arquivo *install_dir*/registry/archdsc.tbl.

O script **krzgrant.sql** tem o uso a seguir: krzgrant.sql *user_ID temporary_directory*

em que:

user_ID
O ID do usuário do Oracle. Esse ID do usuário deve ser criado antes de executar esse arquivo SQL. Exemplo de valor: *tivoli*.

temporary_directory
O nome do diretório temporário que contém o arquivo de saída krzagent.log do script **krzgrant.sql**. Esse diretório deve existir antes que esse script SQL seja executado. Valor de exemplo:install_dir/tmp.

Você deve ter a função de autorização do administrador de banco de dados (DBA) do Oracle e permissão de gravação para o diretório temporário para executar o procedimento a seguir.

Procedimento

1. Na linha de comandos, execute os comandos para configurar variáveis de ambiente.
   - Windows

     ```
     SET ORACLE_SID= sid
     SET ORACLE_HOME= home
     ```

   - Linux AIX

     ```
     ORACLE_SID = sid
     export ORACLE_SID
     ORACLE_HOME = home
     export ORACLE_HOME
     ```

   em que:

   sid
   Identificador do sistema Oracle, que faz distinção entre maiúsculas e minúsculas.

   home
   Diretório inicial para a instância Oracle monitorada.
2. Na mesma janela de linha de comandos em que você configura variáveis de ambiente, inicie o Oracle SQL PLus ou uma ferramenta alternativa que você usa para emitir instruções SQL.
3. Efetue logon no banco de dados Oracle como um usuário que tenha privilégios de DBA do Oracle.
4. Acesse o diretório que contém o script **krzgrant.sql** e execute o comando a seguir para conceder privilégios de seleção:

   ```
   @krzgrant.sql user_ID temporary_directory
   ```

A saída é registrada no arquivo `krzagent.log` no diretório temporário. Esse log registra as visualizações e tabelas nas quais o Agente Oracle Database tem privilégios selecionados concedidos.

Após os privilégios serem concedidos com sucesso, é possível configurar e iniciar o Agente Oracle Database.

Configurando o monitoramento do S.O.

Os agentes do Monitoring Agent for Linux OS, do Monitoring Agent for UNIX OS e do Monitoring Agent for Windows OS são configurados automaticamente. É possível configurar o monitoramento de arquivo de log para os agentes de S.O. para que seja possível monitorar arquivos de log do aplicativo. É possível executar os agentes de S.O. como um usuário não raiz. Além disso, há algumas opções de configuração para o agente de S.O. Linux.

Executando os agentes de S.O. como um usuário não raiz

É possível executar o Monitoring Agent for Windows OS, o Monitoring Agent for UNIX OS e o Monitoring Agent for Linux OS como um usuário não raiz.

Para executar o Windows OS agent como um usuário não raiz, consulte "Executando o Monitoring Agent for Windows OS como um usuário não raiz" na página 631.

Para executar os agentes do Monitoring Agent for UNIX OS e do Monitoring Agent for Linux OS como um usuário não raiz, consulte "Iniciando agentes como um usuário não raiz" na página 1012.

Restrição:

Ao executar como um usuário não raiz, o agente não pode acessar `/proc/pid/status` e, portanto, não pode relatar os seguintes atributos:

- -Tempo de CPU do usuário (UNIXPS.USERTIME)
- -Tempo de CPU do sistema (UNIXPS.SYSTEMTIM)
- -Tempo total de CPU (UNIXPS.TOTALTIME)
- -Contagem de encadeamentos (UNIXPS.THREADCNT)
- -Tempo de CPU do usuário filho (UNIXPS.CHILDUTIME)
- -Tempo de CPU do sistema filho (UNIXPS.CHILDSTIME)
- -Tempo total de CPU do filho (UNIXPS.CHILDTIME)
- -Tempo de CPU de espera (UNIXPS.WAITCPUTIM)
- -Terminal (UNIXPS.USERTTY)

Esses atributos não são visíveis no Console do Cloud APM, mas estão disponíveis para criar limites.

Executando o Monitoring Agent for Windows OS como um usuário não raiz

É possível executar o Windows OS agent como um usuário não raiz. No entanto, algumas funções estão indisponíveis.

Quando você executa o Windows OS agent como um usuário não raiz, algumas funções estão indisponíveis nas seguintes grupos de atributos, se eles forem de propriedade Somente pelo administrador Conta :

- Registro
- Tendência de Arquivo
- Alteração de Arquivo

A implementação remota de outros agentes não está disponível porque direitos de administrador são requeridos para instalar os novos agentes.

Para o Agent Management Services, o watchdog não pode parar ou iniciar nenhum agente que não tenha privilégios para parar ou iniciar.

Para criar um usuário não raiz, crie um novo usuário Limitado (não raiz) e configure permissões de registro para o novo usuário como no seguinte exemplo:

- Acesso total a `HKEY_LOCAL_MACHINE\SOFTWARE\Candle`
- Acesso de leitura a `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion \Perflib`

O usuário que inicia o Monitoring Agent for Windows OS – Serviço primário deve ter direitos para gerenciar o Monitoring Agent for Windows OS - Serviço Watchdog. O usuário que inicia o Monitoring Agent for Windows OS -Segurança do serviço também deve ter direitos para gerenciar quaisquer serviços que são gerenciados pelo Agente Gerenciamento de Serviços, incluindo o Monitoring Agent for Windows OS - Primário Serviço . Para conceder aos usuários autoridade para gerenciar serviços do sistema no Windows, use modelos de segurança, política de grupo ou edite o arquivo `Subinacl.exe`. Para obter mais informações, consulte a documentação da Microsoft a seguir: http://support.microsoft.com/kb/325349 (http://support.microsoft.com/kb/325349).

O exemplo a seguir mostra como conceder aos usuários a autoridade para gerenciar serviços do sistema usando modelos de segurança:

1. Clique em **Iniciar** > **Executar**, insira `mmc` na caixa Abrir e, em seguida, clique em **OK**.
2. No menu **Arquivo**, clique em **Incluir/Remover Snap-in**.
3. Clique em **Incluir** > **Configuração e análise de segurança** e, em seguida, clique em **Incluir** novamente.
4. Clique em **Fechar** e, em seguida, clique em **OK**.
5. Na árvore do console, clique com o botão direito do mouse em **Análise e Configuração de Segurança**, e, em seguida, clique em **Abrir Banco de Dados**.
6. Especifique um nome e local para o banco de dados e, em seguida, clique em **Abrir**.
7. Na caixa de diálogo **Importar modelo** exibida, clique no modelo de segurança que você deseja importar e, em seguida, clique em **Abrir**.
8. Na árvore do console, clique com o botão direito do mouse em **Análise e Configuração de Segurança**, e, em seguida, clique em **Analisar o Computador Agora**.
9. Na caixa de diálogo **Executar análise** exibida, aceite o caminho padrão para o arquivo de log exibido na caixa Caminho de arquivo do log de erros. Caso contrário, especifique o caminho que desejar. Clique em **OK**.
10. Após a análise ser concluída, configure as permissões de serviço como segue:
    a. Na árvore do console, clique em **Serviços do Sistema**.
    b. Na área de janela à direita, dê um clique duplo no serviço do Monitoring Agent for Windows OS - Primary.
    c. Selecione a caixa de seleção **Definir esta política no banco de dados** e, em seguida, clique em **Editar Segurança**.
    d. Para configurar permissões para um novo usuário ou grupo, clique em **Incluir**.
    e. Na caixa de diálogo **Selecionar usuários, computadores ou grupos**, digite o nome do usuário ou grupo para o qual você deseja configurar permissões e, em seguida, clique em **OK**. Na lista **Permissões para usuário ou grupo**, selecione a caixa de seleção **Permitir** (próxima de **Iniciar**). Permissão para parar e pausar é selecionada por padrão, para que o usuário ou grupo possa iniciar, parar ou pausar o serviço.
    f. Clique duas vezes em **OK**.
11. Repita a etapa 10 para configurar as permissões de serviço para o serviço do Monitoring Agent for Windows OS - Watchdog.
12. Para aplicar as novas configurações de segurança no computador local, clique com o botão direito do mouse em **Análise e Configuração de Segurança**, e, em seguida, clique em **Configurar o Computador Agora**.

Nota: Também é possível usar a ferramenta de linha de comandos Secedit para configurar e analisar a segurança do sistema. Para obter informações adicionais sobre Secedit, clique em **Iniciar** > **Executar**, insira `cmd` e, em seguida, clique em **OK**. No prompt de comandos, digite `secedit /?` e, em seguida, pressione **ENTER**. Ao usar esse método para aplicar configurações, todas as configurações no modelo são reaplicadas. Esse método pode substituir outras permissões de arquivo, registro ou serviço configuradas anteriormente.

O exemplo a seguir mostra como configurar o Monitoring Agent for Windows OS e os serviços do Watchdog para efetuar logon como um usuári não raiz usando o Windows Services console:

1. Clique em **Iniciar** > **Executar**, insira `services.msc` e, em seguida, clique em **OK**.
2. Selecione **Monitoring Agent for Windows OS - Primary**.
3. Clique com o botão direito em **Propriedades**.
4. Verifique o tipo de inicialização como sendo Automático.
5. Selecione a guia **Efetuar logon** e, em seguida, selecione **Efetuar logon como "Esta conta"** e forneça o ID e senha. Clique em **OK**.
6. Selecione **Monitoring Agent for Windows OS - Watchdog**.
7. Clique com o botão direito em **Propriedades**.
8. Verifique o tipo de inicialização como sendo Manual.
9. Selecione a guia **Efetuar logon** e, em seguida, selecione **Efetuar logon como "Esta conta"** e forneça o ID e senha. Clique em **OK**.

Configurando monitoramento de arquivo de log do OS Agent

Os agentes do Monitoring Agent for Linux OS, do Monitoring Agent for UNIX OS e do Monitoring Agent for Windows OS são configurados automaticamente. Entretanto, é possível configurar o monitoramento de arquivo de log para OS Agents, de modo que seja possível monitorar arquivos de log de aplicativo.

Depois que os agentes filtram os dados do log, os dados são enviados na forma de um evento de log para o Console do Cloud APM.

Incluindo ou removendo a configuração de monitoramento do arquivo de log para os agentes de S.O.
Inclua configuração de monitoramento do arquivo de log para os agentes de S.O. para que os agentes de S.O. possam filtrar dados do arquivo de log. Em seguida, subsequentemente, também é possível remover a configuração de monitoramento do arquivo de log para os agentes de S.O., se necessário.

Antes de Iniciar

Os agentes do S.O. incluem agora um arquivo de amostra regex1.conf e um arquivo regex1.fmt que é possível visualizar antes de configurar os arquivos .conf e .fmt. Os arquivos estão localizados aqui:

- No UNIX/LINUX: `<install_dir>/samples/logfile-monitoring`
- No Windows: `<install_dir\samples\logfile-monitoring`

Use um editor de texto para criar um arquivo de configuração `.conf` e um arquivo de formato `.fmt`. Para obter mais informações sobre o conteúdo desses arquivos, consulte “Arquivo de configuração” na página 638 e “arquivo de Formato ” na página 647. Você deve assegurar que salva esses arquivos no sistrema onde é acessado o console do Performance Management, para que seja possível fazer upload dos arquivos para o Servidor Cloud APM.

Sobre Esta Tarefa

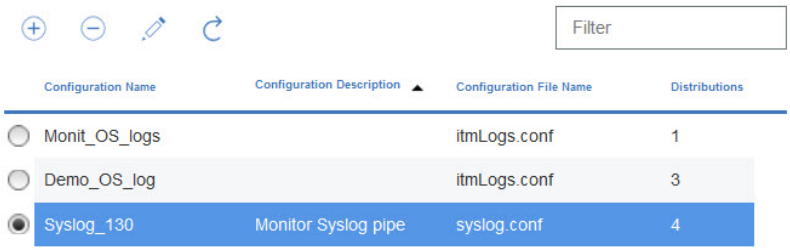
Para ativar os agentes do sistema operacional para monitorar arquivos de log, você deve fazer upload do arquivo de configuração e arquivo de formato e especificar a qual o agente de sistema operacional a configuração se aplica. O OS Agent faz download dos arquivos `.conf` e `.fmt` e o agente monitora os arquivos de log que você especifica na configuração.

Procedimento

Incluindo a configuração de monitoramento do arquivo de log para os agentes de S.O.

1. Clique em **Configuração do sistema** > **Configuração do agente**.
2. Dependendo do sistema no qual deseja monitorar os arquivos de log, clique nas guias **Sistema Operacional Unix**, **Sistema Operacional Linux** ou **Sistema Operacional Windows**.
3. Para criar uma nova configuração, clique no ícone (+) para abrir a janela **Nova Configuração de Arquivo de Log**. Insira um nome e uma descrição para a configuração.
4. Para visualizar o conteúdo dos arquivos `.conf` e `.fmt`, clique em **Visualizar**.
5. Para fazer upload da configuração usando o Servidor Cloud APM, selecione o arquivo `.conf` e o arquivo `.fmt` do mesmo sistema em que foi aberto o console do Performance Management e clique em **Concluído**.
6. Na guia OS Agent, selecione a configuração que você transferiu por upload.

   Importante: Os arquivos `.conf` e `.fmt` que são distribuídos para os agentes são renomeados para o nome de configuração que for definido.



7. Para implementar a configuração, na tabela **Lista de distribuições de configuração de log**, selecione os agentes para os quais você deseja implementar a configuração e clique em **Aplicar mudanças**.

Removendo a configuração de monitoramento do arquivo de log para os agentes do S.O.

8. Selecione o nome da configuração.
9. Desmarque os sistemas gerenciados e clique em **Aplicar mudanças**.

   Importante:

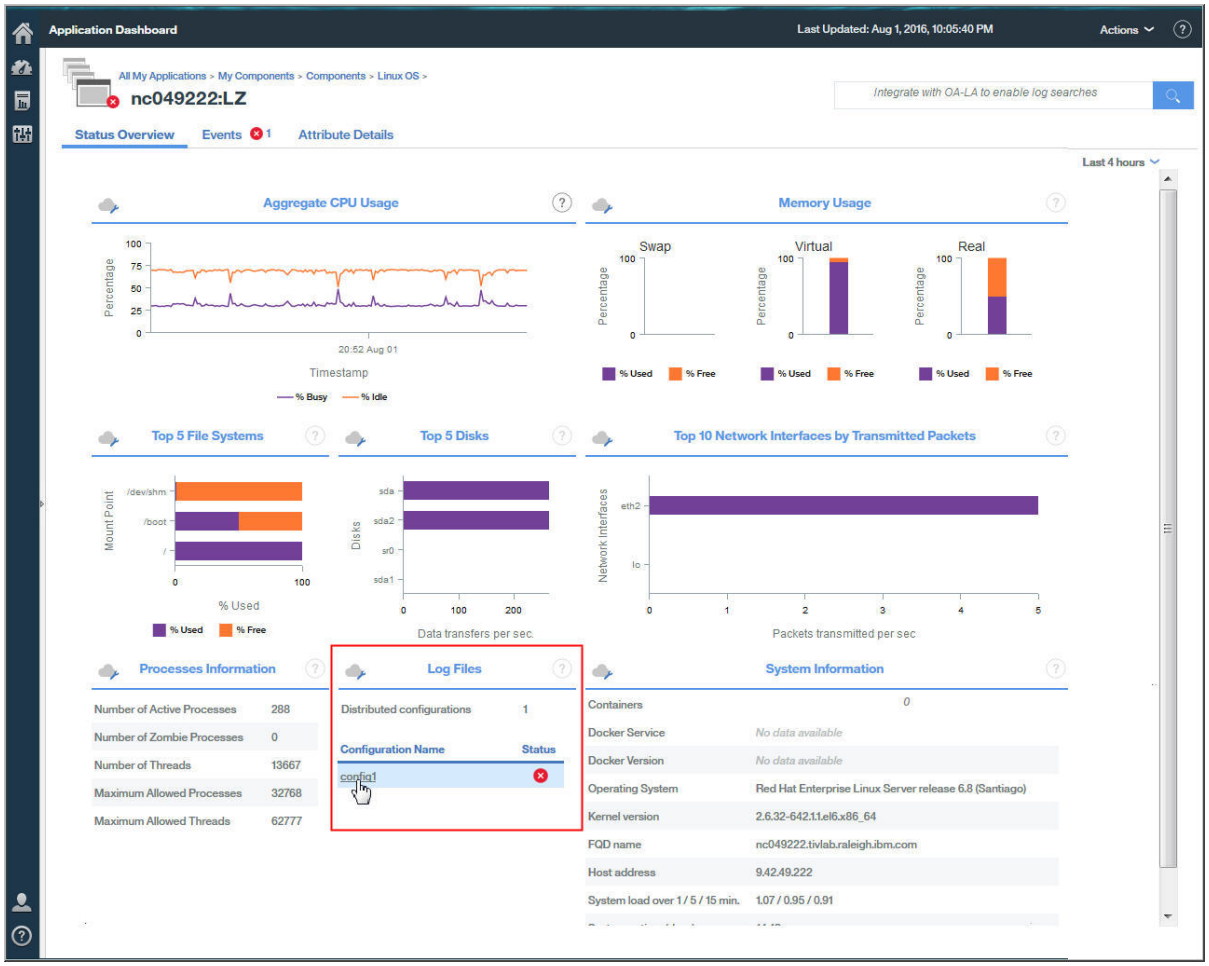
   Após remover a configuração de monitoramento de log, o recurso de monitoramento do arquivo de log continuará e permanecerá on-line até que você reinicie o agente do S.O. Os recursos de monitoramento do arquivo de log off-line são limpos após o horário especificado na opção **Atraso de remoção do sistema off-line**.

Visualizando o conteúdo do monitoramento do arquivo de log

É possível visualizar a configuração de monitoramento de arquivo de log para OS Agents implementados para monitorar arquivos de log.

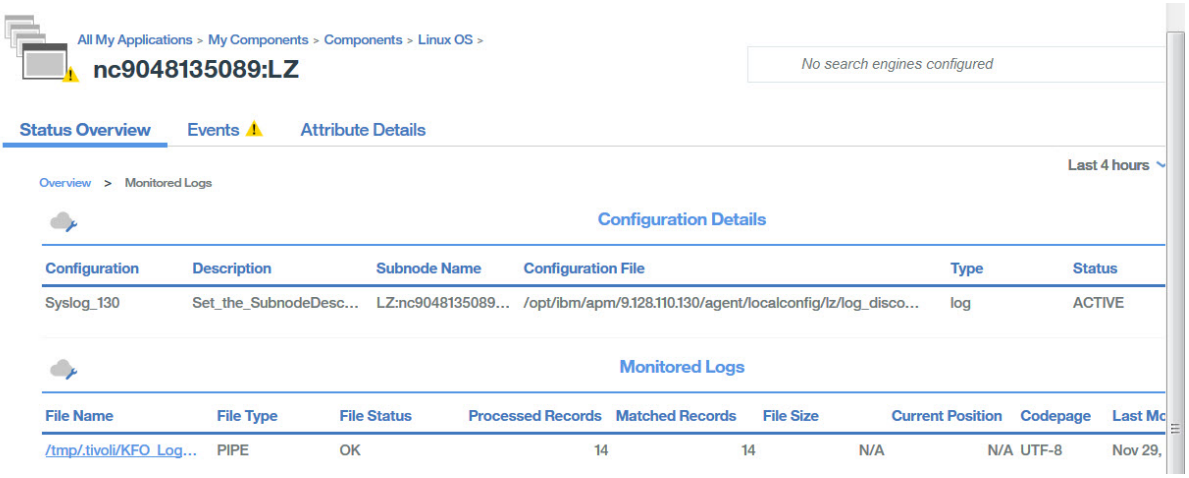
Procedimento

1. Clique em **Desempenho** > **Painel de Desempenho de Aplicativo** e selecione um aplicativo que inclua o agente de S.O. onde foi implementada a configuração de monitoramento do arquivo de log.
2. Realize drill down no painel do agente de S.O. e, no widget Arquivos de Log, clique no perfil para visualizar as configurações de monitoramento de log distribuídas e os logs monitorados.

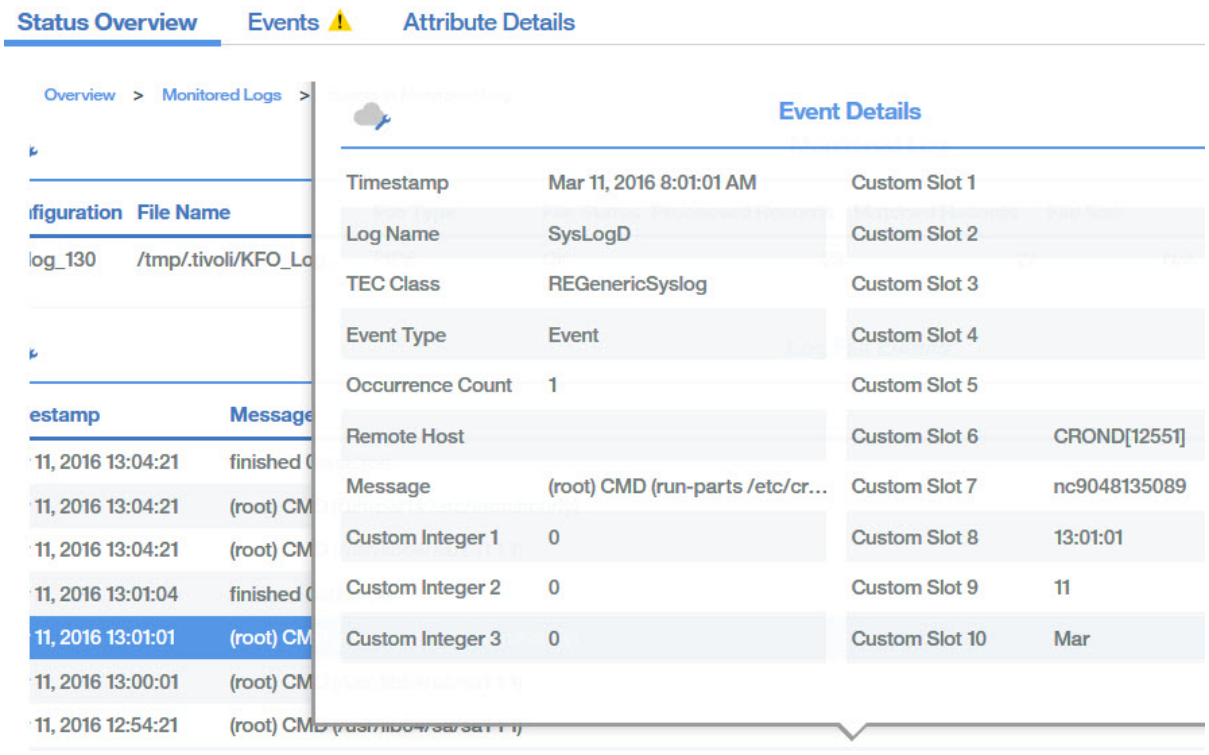


Os detalhes de configuração incluem o nome de configuração. a descrição, o subnó, o arquivo de configuração, o status e o código de erro.

3. Clique no nome do arquivo de log para visualizar todos os eventos do arquivo de log que estão associados ao arquivo de log.



4. Clique no evento para visualizar os detalhes do evento, por exemplo, todos os campos definidos no arquivo de formato.



Exibindo eventos de monitoramento de arquivo de log
Depois de configurar o agente de S.O. para monitorar os arquivos de log do aplicativo, é possível criar limites para gerar alarmes nas condições do arquivo de log das quais você deseja ser alertado.

Procedimento

1. Na Barra de Navegação, clique no ícone **Configuração do Sistema** > **Gerenciador de Limite**.
2. Selecione o S.O. de destino para **Tipo de origem de dados**.
3. Clique em Incluir para criar um novo limite.
4. Configure uma gravidade para o evento que excede esse limite.
5. Selecione o conjunto de dados para o qual criar um limite. Os seguintes conjuntos de dados são elegíveis para monitoramento de arquivo de log:
   - K*pp* Estatísticas RegEx do arquivo de log
   - K*pp* Status do arquivo de log
   - K*pp* LogfileProfileEvents
6. Clique em **Incluir** para incluir uma condição. Na caixa **Incluir condição**, selecione um atributo e um operador e, em seguida, insira um valor do limite.

   Repita esta etapa para incluir mais condições em seu limite, se necessário.
7. Na seção Designação de grupo, selecione o grupo de recursos ao qual você deseja designar seu limite.
8. Clique em **Salvar**.
9. Na barra de navegação, clique no ícone **Configuração do Sistema** > **Configuração Avançada**.
10. Na categoria **Integração da UI**, configure o valor **Ativar eventos do subnó** para ser True.
11. Clique em **Salvar**.

Resultados
Quando a condição especificada se tornar verdadeira, o evento do arquivo de log que aciona o alerta é exibido na guia Eventos.

Variáveis de ambiente de monitoramento de arquivo de log
É possível configurar variáveis de ambiente para monitoramento de arquivo de log nos arquivos do ambiente do OS Agent.

Configure as variáveis de ambiente a seguir e substitua K*PC* pelo código do OS Agent, em que *PC* é o código do agente de dois caracteres, por exemplo, klz é o código para o Linux OS Agent.

K*PC*_FCP_LOG
Esta variável está disponível no arquivo *install_dir*/config/.*pc*.environment. O valor padrão é True e você o usa para ativar ou desativar o recurso de monitoramento de log.

K*PC*_FCP_LOG_PROCESS_MAX_CPU_PCT
Esta configuração é a porcentagem máxima permitida de CPU de todo o sistema que o agente usa acima de um intervalo de 1 minuto. Os valores válidos são 5 - 100. O valor padrão é 100. Esta configuração está associada ao recurso de regulagem da CPU. Se você especificar um valor menor que 5, o valor mínimo de 5 será usado.

K*PC*_FCP_LOG_PROCESS_PRIORITY_CLASS
Esta configuração é a prioridade do planejador do sistema operacional para o processo. A é a mais baixa, C é o sistema operacional padrão e F é a prioridade mais alta. A configuração é um dos seguintes valores: A, B, C, D, E, F. Esses valores são substituídos por quaisquer valores que forem especificados no arquivo .conf.

K*PC*_FCP_LOG_SEND_EVENTS
A configuração padrão é True e é usado pelo agente do SO para enviar eventos para o Servidor Cloud APM.

K*PC*_FCP_LOG_SEND_EIF_EVENTS
A configuração padrão é True. Se essa opção for configurada para Sim o agente envia dados do evento para o Servidor Cloud APM ou para qualquer receptor EIF, como o OMNIbus EIF Análise . Se a opção estiver configurada como Não, o agente não enviará os dados do evento. A configuração desta opção é global e se aplica a todos os perfis de monitoramento.

Nota: O receptor EIF consome eventos, caso contrário, podem ocorrer problemas quando o cache do agente ficar cheio.

K*PC*_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN
Os agentes de S.O. com monitoramento de eventos do arquivo de log possuem uma limitação de subnó. Para gerenciar eventos do arquivo de log, o MSN de subnó tem a seguinte estrutura: UX:*CITRAHOSTNAME_PROFILENAME*. A limitação de tamanho máximo para o nome do subnó é de 32 caracteres. Se o nome do MSN de subnó construído for muito longo e tiver mais de 32 caracteres, ele será truncado para 32 caracteres. Esse nome corresponde à subsequência obtida do Nome do perfil.

No arquivo de configuração do agente de S.O., use as seguintes variáveis para gerenciar os nomes de perfis que são muito longos:

- Agente de S.O. UNIX: KUX_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN=true
- Agente de S.O. Linux: KLZ_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN=true
- Agente de S.O. Windows: KNT_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN=true

Por exemplo, se você tiver um agente chamado aixhost_nc123456789A, que tem 20 caracteres, CTIRAHOSTNAME=aixhost_nc123456789A terá 20 caracteres.

e você tiver dois perfis chamados:

```
ProfileLong12A (14 caracteres)
ProfileLong12B (14 caracteres)
```

os seguintes MSNs de subnó relacionados serão esperados:

```
UX:aixhost_nc123456789A_ProfileLong12A (38 caracteres)
UX:aixhost_nc123456789A_ProfileLong12B (38 caracteres)
```

No entanto, os MSNs de subnó são truncados para a limitação de 32 caracteres, por isso, os nomes resultantes são os mesmos para ambos:

```
UX:aixhost_nc123456789A_ProfileL
UX:aixhost_nc123456789A_ProfileL
```

Para truncar CTIRAHOSTNAME em vez do Nome do perfil, configure a variável *Kpc_FCP_TRUNCATE_HOSTNAME_IN_LONG_SUBNODE_MSN=true*.

Por exemplo, se *n* for o comprimento do Nome do perfil, como 14, a subsequência para o nome MSN que está relacionado a *CTIRAHOSTNAME* será truncada para 32-n-3 caracteres, portanto, a variável *CTIRAHOSTNAME* é: `aixhost_nc1234`. Portanto, os MSNs de subnó distintos são:

```
UX:aixhost_nc1234_ProfileLong12A
UX:aixhost_nc1234_ProfileLong12B
```

Arquivo de configuração
Os agentes de S.O. usam um arquivo de configuração que é lido pelo agente quando ele é iniciado. O arquivo contém opções de configuração e filtros. Você deve criar esse arquivo de configuração e configurar a instância do agente para utilizá-lo.

O arquivo de configuração é monitorado para mudanças em seu registro de data e hora a cada 60 segundos daí em diante. Se o registro de data e hora do arquivo mudar, o agente reinicializará sua configuração dinamicamente sem requerer reinicialização. Para obter mais informações, consulte “Alterando os Arquivos de Configuração e de Formato do Agente” na página 651.

O arquivo `.conf` para o agente de S.O. aceita essas opções:

página de códigos
Esse parâmetro é a página de códigos do arquivo monitorado. Use este parâmetro no arquivo de configuração quando a página de códigos do arquivo monitorado for diferente da página de códigos do sistema. Especifique a página de códigos do arquivo monitorado, por exemplo, ibm-5348_P100-1997, UTF-16 ou UTF-8.

ConfigFilesAreUTF8=Y
Este parâmetro especifica que o arquivo de configuração e arquivo de formato estão em UTF-8. Use este parâmetro se a codificação dos arquivos de configuração for UTF-8 e a página de códigos do sistema não for. O padrão é que o agente considera a codificação do sistema.

DupDetectionKeyAttributes
Uma lista separada por vírgula de atributos do Cloud APM que é usado para determinar quais eventos são duplicatas. Se todos os atributos nomeados são os mesmos em dois eventos, esses dois eventos são considerados duplicatas. Essa opção aplica-se apenas a eventos. Para obter mais informações, consulte “Filtro de eventos e resumo” na página 1017.

Nota:

1. Os nomes de atributos fazem distinção entre maiúsculas e minúsculas, portanto, é necessário inserir os nomes exatamente conforme descritos.
2. Se você não fornecer uma lista de atributos, os valores serão padronizados para `Class` e `Logname`.

ENFORCE_STRICT_TEC_COMPATIBILITY
Esse parâmetro refere-se a todos os caracteres de espaço em branco nos dados do log para assegurar que os caracteres sejam respeitados. Por exemplo, quando você usa um formato, como `"%s %s"` para extrair informações de mensagens de log, o agente de S.O. corresponde não apenas a um espaço literal, mas também a quaisquer outros caracteres de espaço em branco que estão presentes, como tabulações e retornos de linhas.

Quando esse parâmetro não está configurado, o comportamento padrão do agente de S.O. quando ele corresponde a uma sequência de formatações de estilo do Tivoli Enterprise Console é corresponder ao máximo possível de texto de entrada, enquanto processa o formato da esquerda para a direita.

Por exemplo, para a sequência de formatações `%s:%s` e a sequência de entrada `one:two:three`, o padrão do agente de S.O. designa `one.two` ao primeiro parâmetro (correspondendo ao primeiro `%s`) e designa `three` ao segundo parâmetro.

Nota:

1. Esse parâmetro não se aplica a instruções de formato que usam a sintaxe de expressão regular.
2. A configuração deste parâmetro tem um impacto no desempenho. Para dar maior controle sobre o comportamento e o desempenho de correspondência, evite configurar este parâmetro e use expressões regulares no lugar.

EventSummaryInterval
Especifica o número de segundos durante os quais o agente procura por eventos duplicados para suprimir. Configure este parâmetro como um número inteiro positivo. Essa opção aplica-se apenas a eventos. Para obter mais informações, consulte "Filtro de eventos e resumo" na página 1017.

EventFloodThreshold
Especifica quais eventos são enviados quando os eventos duplicados são detectados. Configure este parâmetro como `send_none`, `send_all`, `send_first` ou um número inteiro positivo. Essa opção aplica-se apenas a eventos. Para obter mais informações, consulte "Filtro de eventos e resumo" na página 1017.

EventMaxSize
Especifica, em bytes, o tamanho máximo de um evento gerado. Se especificado, este parâmetro é usado em dois locais:

1. O parâmetro pode ser usado pelo agente para configurar o tamanho de um buffer que seja usado para processar os eventos. Se não configurado, este buffer é padronizado com um tamanho de 16384 bytes. Se o buffer é configurado muito pequeno, os eventos são truncados e podem ser descartados.
2. O parâmetro pode ser usado pelo emissor EIF para configurar o tamanho de um buffer que seja usado para enviar os eventos para um receptor EIF, como a análise de EIF do OMNIbus. Se não configurado, este buffer é padronizado com um tamanho de 4096 bytes. Se o buffer for configurado muito pequeno, os eventos serão descartados.

FileComparisonMode
Especifica quais arquivos de log são monitorados quando mais de um arquivo corresponde a um padrão curinga. Os seguintes valores estão disponíveis:

CompareByAllMatches
Este valor é um comportamento padrão. Todos os arquivos que correspondem ao padrão de curinga especificado em `LogSources` são monitorados.

CompareByLastUpdate
Dos arquivos que correspondem ao padrão curinga especificado em `LogSources`, o arquivo com o registro de data e hora atualizado mais recentemente é monitorado.

CompareBySize
Dos dois ou mais arquivos que correspondem aos critérios de padrão de nome do arquivo, o arquivo maior é selecionado para monitoramento. Não use `CompareBySize` com diversos arquivos correspondentes que estão sendo atualizados ao mesmo tempo e aumentando os seus tamanhos de arquivo. Se o maior arquivo está sujeito à mudança frequente, o monitoramento pode reiniciar continuamente no início do arquivo recém-selecionado. Em vez disso, use `CompareBySize` para um conjunto de arquivos correspondentes onde apenas um está ativo e sendo atualizado em qualquer momento específico.

CompareByCreationTime
Dos arquivos que correspondem ao padrão curinga especificado em `LogSources`, o arquivo com o registro de data e hora criado mais recentemente é monitorado. Esse valor possui as seguintes restrições:

- O valor é aplicável apenas a sistemas operacionais Windows, porque os sistemas operacionais UNIX e Linux não armazenam um horário de criação verdadeiro para arquivos.
- O valor não é suportado para arquivos remotos que são monitorados usando o Protocolo de Transferência de Arquivos de Shell Seguro (SSH).

Dica: Os valores `CompareByLastUpdate`, `CompareBySize` e `CompareByCreationTime` podem ser utilizados para arquivos de log de rolagem. `CompareByLastUpdate` geralmente é usado para esses arquivos.

FQDomain
Especifica como e se o agente configura um nome de domínio:

- Se configurado como `yes`, o agente determina o nome de domínio do sistema.
- Se configurado como `não`, o agente não configura um nome de domínio. O atributo `fqhostname` tem uma sequência em branco designada.
- Se configurado para que ele não contenha um valor `yes` ou `no`, o nome de domínio é aceito como o valor e ele é anexado ao nome do host.

Para obter mais informações, consulte "arquivo de Formato " na página 647.

IncludeEIFEventAttr
O agente inclui um atributo grande que é chamado *EIFEvent*, que é uma representação do evento que é enviado por meio do Event Integration Facility, se esse recurso estiver ativado. As informações contidas no atributo *EIFEvent* também podem ser localizadas em outros atributos. Seu tamanho grande o tornou problemático, por isso ele foi desativado por padrão. Configurando seu valor para y, reative o atributo EIFEvent.

Nota: O uso desse atributo pode fazer com que os limites falhem se você tiver grandes eventos. Um evento grande neste contexto é um evento em que o número total de bytes necessários para conter todos os valores para todos os atributos e seus nomes resulta em uma sequência maior que 3600 bytes.

LognameIsBasename
Quando configurado para y, o valor do atributo `Logname` é o nome base do arquivo de log no qual o evento foi localizado. Essa opção aplica-se apenas a eventos do Performance Management. O caminho é removido. Por exemplo, `/data/logs/mylog.log` se torna `mylog.log`. Se esse valor for definido para n, você obterá o caminho completo. No entanto, como o atributo está limitado a 64 caracteres, configurá-lo como n significa que o nome é truncado se for mais longo. Por esse motivo, o valor padrão é y. Para ver o nome do caminho completo em um atributo mais longo, é possível especificá-lo na seção de mapeamentos de um formato no arquivo `.fmt`, por exemplo, `filename FILENAME CustomSlot1`. O mapeamento preenche o slot chamado `filename` com o caminho completo do arquivo no qual o evento foi localizado e mapeia-o para `CustomSlot1`, que tem 256 caracteres.

LogSources
Especifica os arquivos de log de texto para pesquisar mensagens. O caminho completo para cada arquivo deve ser especificado e os nomes de arquivos devem ser separados por vírgulas. Dentro de cada nome de arquivo, também é possível usar um asterisco (*) para representar qualquer sequência de caracteres ou um ponto de interrogação (?) para representar um único caractere. Por exemplo, `mylog*` resulta na pesquisa de todos os arquivos de log cujos nomes iniciam com `mylog`, embora `mylog???` resulte na pesquisa de todos os arquivos de log cujos nomes consistem em `mylog` seguido por exatamente 3 caracteres. Esses caracteres curingas são suportados apenas dentro do nome de arquivo; o caminho deve ser explicitamente especificado.

Se desejar usar expressões regulares ou correspondência de padrões no caminho, consulte a descrição de RegexLogSources.

Uma origem de arquivo de log não precisa existir quando o agente é iniciado; o arquivo de log é pesquisado quando ele é criado.

NewFilePollInterval
Especifica a frequência, em segundos, com que o agente verifica novos arquivos para monitorar. Por exemplo, se um nome do arquivo especificado pelas configurações do arquivo de configuração *LogSources* ou *RegexLogSources* ainda não existir quando o agente for iniciado, ele verificará novamente a existência dos arquivos após esse intervalo.

NumEventsToCatchUp
Especifica o evento no log com o qual o agente é iniciado. Essa opção fornece alguma flexibilidade se a origem que está sendo monitorada é nova ou o agente está interrompido por um tempo estendido. Os seguintes valores são válidos:

Nota: Para arquivos de texto, valores `0` e `-1` se aplicam. Para o Log de eventos do Windows, os valores `0`, `-1` e n se aplicam.

0
Inicia com o próximo evento nos logs. Esse valor é o padrão.

-1
Quando configurado como `-1`, o agente salva seu local no arquivo que está sendo monitorado. Ele salva seu local de forma que, quando o agente for interrompido e reiniciado posteriormente, ele possa processar qualquer evento gravado no log enquanto estava interrompido. O agente, de outra forma, ignora eventos que chegam enquanto ele estava interrompido e reinicia a partir do final do arquivo. Essa configuração não se aplica a canais, ou ao monitoramento de syslog em sistemas UNIX e Linux.

n
Configure com um número inteiro positivo. Inicia com o evento *nth* a partir do evento mais atual nos logs; ou seja, inicia os eventos *n* para trás a partir do evento mais atual nos logs. Se *n* for maior que o número de eventos disponíveis, todos os eventos que estiverem disponíveis serão processados.

Nota: É possível usar o valor n apenas para o Log de Eventos do Windows. O valor n é ignorado quando `UseNewEventLogAPI` é configurado como *y*.

PollInterval
Especifica a frequência, em segundos, para pesquisar cada arquivo de log que é listado na opção `LogSources` para as novas mensagens. O valor padrão é 5 segundos.

Se você fez upgrade de um adaptador do Log de eventos do Windows de uma liberação anterior e tiver um valor configurado para `PollingInterval` no registro do Windows, deverá especificar a opção `PollInterval` no arquivo de configuração do agente com o mesmo valor usado no registro do Windows. Essa regra se aplicará apenas se você estiver substituindo um agente de S.O. do Tivoli Enterprise Console que tinha valores no registro.

ProcessPriorityClass
Especifica a prioridade do processo para o agente. É possível ajustar este valor para melhorar o desempenho do sistema se o agente processa grandes volumes de eventos e está usando muitos recursos do processador. Os possíveis valores são:

- `A` - Prioridade muito baixa
- `B` - Baixa prioridade
- `C` - Prioridade típica
- `D` - Prioridade acima da típica
- `E` - Alta prioridade
- `F` - Prioridade muito alta
- `USE_CONF_FILE_VALUE` - Use o valor especificado no arquivo de configuração. Esse valor é o padrão.

RegexLogSources
Especifica os arquivos de log de texto para pesquisar mensagens. Difere da opção LogSources, em que metacaracteres de expressão regular podem ser usados na parte do nome base do nome do arquivo e em um subdiretório do nome do arquivo. Essa diferença oferece maior flexibilidade do que a opção LogSources na descrição de diversos arquivos para monitoramento em vários diretórios.

Por exemplo, a especificação de `/var/log/mylog*` para a instrução LogSources é idêntica a usar o metacaractere ponto `(.)` seguido por um metacaractere asterisco `(*)` para formar `/var/log/mylog.*` na instrução RegexLogSources. Este tipo de qualificador resulta na pesquisa de todos os

arquivos de log no diretório `/var/log` cujos nomes base iniciam com `mylog` e são seguidos por zero ou mais caracteres. Um qualificador `/var/log/mylog.+` resulta na pesquisa de todos os arquivos de log no diretório `/var/log` cujos nomes iniciam com `mylog` e são seguidos por um ou mais caracteres.

Semelhante a LogSources, o caminho completo para cada arquivo deve ser especificado e os nomes do arquivo devem ser separados por vírgulas. No entanto, uma vírgula também é um caractere válido dentro de uma expressão regular. Para distinguir entre uma vírgula que é usada como parte de uma expressão regular e uma que é usada para separar nomes de arquivos, as vírgulas que são usadas como parte de uma expressão regular devem ser escapadas com o caractere barra invertida `(\)`.

Por exemplo, se você desejar procurar logs que correspondem a uma das seguintes expressões regulares, `/logs/.*\.log` e `/other/logs/[a-z]{0,3}\.log`, será necessário escapar a vírgula na cláusula `{0,3}` da segunda expressão para que o agente não se engane com ela para o início de uma nova expressão: `RegexLogSources=/logs/.*\.log,/other/logs/[a-z]{0\,3}\.log`

Se metacaracteres forem usados no nome do caminho, os metacaracteres poderão ser usados somente em um subdiretório do caminho. Por exemplo, é possível especificar `/var/log/[0-9\.]*/mylog.*` para ter metacaracteres em um subdiretório. O `[0-9\.]*` resulta na correspondência de qualquer subdiretório do `/var/log` que consiste unicamente em número e pontos `(.)`. O `mylog.*` resulta na correspondência de quaisquer nomes de arquivo nesses subdiretórios `/var/log` que começam com `mylog` e são seguidos por zero ou mais caracteres.

Como alguns sistemas operacionais usam a barra invertida `(\)` como um separador de diretórios, isto pode ser confundido com um metacaractere de escape de expressão regular. Devido a essa confusão, as barras devem ser sempre usadas para indicar diretórios. Por exemplo, arquivos do Windows que são especificados como `C:\temp\mylog.*` podem significar que o `\t` é um caractere de tabulação de atalho. Portanto, sempre use barras `(/)` para todos os separadores de diretórios de sistemas operacionais. Por exemplo, `C:/temp/mylog.*` representa todos os arquivos no diretório `C:/temp` que começam com `mylog`.

Se mais de um subdiretório contiver metacaracteres, uma mensagem de rastreio também será emitida. Por exemplo, `c:/[0-9\.]*/temp.files/mylog.*` tem dois subdiretórios com metacaracteres. `[0-9\.]*` é o primeiro subdiretório com metacaracteres e `temp.files` é o segundo subdiretório que usou um metacaractere de ponto `(.)`. Neste caso, o agente assume que o primeiro subdiretório com o metacaractere seja usado e os diretórios subsequentes com metacaracteres são ignorados.

SubnodeName
Um valor da sequência de caracteres que pode ser usado para substituir o nome padrão designado para um subnó de perfil de monitoramento. Por padrão, o nome do subnó designado a um perfil de monitoramento corresponde ao nome base do arquivo de configuração usado para esse perfil. Usando esta configuração, um nome de subnó diferente pode ser designado.

SubnodeDescription
Uma valor de sequência pode ser usado para designar um valor ao atributo *Descrição de Subnó* de *LFAProfiles*.

UnmatchLog
Especifica um arquivo para registrar eventos descartados que não podem ser analisados em uma classe de eventos pelo agente. Os eventos descartados podem, então, ser analisados para determinar se as modificações no arquivo de formato do agente são necessárias. Os eventos que correspondem a um padrão que utiliza *DISCARD* não aparecem no log de não correspondência porque eles não correspondam a um padrão.

Essa opção é usada em um ambiente de teste para validar os filtros no arquivo de formato. Essa opção preenche seu sistema de arquivos se você deixá-lo ativo por períodos estendidos.

Opções para o Monitoramento Remoto do Arquivo de Log Usando SSH

Além de **SshHostList**, que é uma lista, todas as opções podem ter apenas um valor, que é aplicado a todos os hosts remotos que estão especificados em **SshHostList**.

Apenas os arquivos de log de texto são suportados. O relatório de erro do AIX, syslog, e o Log de eventos do Windows não são suportados.

Dica: É possível configurar um syslog para gravar sua saída em um arquivo de log de texto e, em seguida, monitorar remotamente esse arquivo de texto com o agente de S.O.

SshAuthType
Deve ser configurado como *PASSWORD* ou *PUBLICKEY*. Se configurado como *PASSWORD*, o valor de **SshPassword** será tratado como a senha a ser usada para autenticação SSH com todos os sistemas remotos. Se configurado como *PUBLICKEY*, o valor de **SshPassword** será tratado como o passphrase que controla o acesso para o arquivo de chave privada. Se configurado como *PUBLICKEY*, **SshPrivKeyfile** e **SshPubKeyfile** também devem ser especificados.

SshHostList
Uma lista separada por vírgula de hosts remotos a ser monitorada. Todos os arquivos de log que são especificados nas instruções **LogSources** ou **RegexLogSources** são monitorados em cada host que é listado aqui. Se *localhost* for um dos nomes de host especificados, o agente monitora o mesmo conjunto de arquivos diretamente no sistema local. Quando você especifica *localhost*, SSH não é usado para acessar os arquivos no sistema local; os arquivos de log serão lidos diretamente.

SshPassword
Quando o valor de **SshAuthType** for *PASSWORD*, esse valor será a senha de conta do usuário que é especificado em **SshUserid**. É possível fornecer a senha de conta em texto não criptografado, ou fornecer uma senha que seja criptografada com o comando de CLI **itmpwdsnmp** do IBM Tivoli Monitoring. Para obter informações adicionais sobre como criptografar uma senha usando o comando **itmpwdsnmp**, consulte "Monitoramento de arquivo de log remoto: Criptografando uma senha ou um passphrase" na página 656.

Quando o valor de **SshAuthType** for *PUBLICKEY*, esse valor será o passphrase que criptografa a chave privada especificada pelo parâmetro **SshPrivKeyfile**. É possível fornecer a passphrase em texto não criptografado, ou fornecer uma passphrase que seja criptografada com o comando de CLI **itmpwdsnmp** do IBM Tivoli Monitoring. Para obter informações adicionais sobre como criptografar uma senha usando o comando **itmpwdsnmp**, consulte "Monitoramento de arquivo de log remoto: Criptografando uma senha ou um passphrase" na página 656.

Nota: Se o valor de **SshAuthType** for *PUBLICKEY*, e configurou o SSH para não solicitar um passphrase, **SshPassword** deve ser configurado como nulo. Para configurar **SshPassword** como nulo, a entrada no arquivo de configuração é:

```
SshPassword=
```

SshPort
Uma porta TCP à qual se conectar para SSH. Se não configurado, o padrão é *22*.

SshPrivKeyfile
Se **SshAuthType** estiver configurado como *PUBLICKEY*, esse valor deverá ser o caminho completo para o arquivo que contém a chave privada do usuário especificado em **SshUserid**, e **SshPubKeyfile** também deverá ser configurado. Se **SshAuthType** não estiver configurado como *PUBLICKEY*, esse valor não será necessário e será ignorado.

SshPubKeyfile
Se **SshAuthType** estiver configurado como *PUBLICKEY*, esse valor deverá ser o caminho completo para o arquivo que contém a chave pública do usuário especificado em **SshUserid**, e **SshPrivKeyfile** também deverá ser configurado. Se **SshAuthType** não estiver configurado como *PUBLICKEY*, esse valor não será necessário e será ignorado.

SshUserid
O nome do usuário nos sistemas remotos, que o agente usa para autenticação de shell seguro.

Opção que é suportada somente em sistemas UNIX e Linux

AutoInitSyslog
Se esta opção for configurada como Sim, o agente configurará automaticamente o recurso syslog para gravar um conjunto padrão de eventos em um canal que o agente monitora. Ao ativar esta configuração, é possível monitorar eventos de syslog sem manter e substituir arquivos de log. Se essa opção não estiver configurada no arquivo de configuração, será o mesmo que estar sendo configurada como Não.

Restrição: Esta opção não é suportada para monitoramento de arquivo de log remoto.

Opções que são suportadas apenas em sistemas Windows
Windows

NTEventLogMaxReadBytes
Se estiver usando a interface do Log de eventos do NT mais antiga (UseNewEventLogAPI não está configurado como y) para ler dados do log de eventos em um sistema Windows, o agente irá ler até esse número de bytes sempre que verificar se existem novos dados no log de eventos. A configuração do valor como 0 faz com que o agente tente ler todos os dados novos, como fazia em liberações anteriores. Esta atividade pode ocupar o agente por um período de tempo considerável em um sistema com vários eventos. O valor padrão é 655360. Quando configurado, o agente pode não parar exatamente no valor especificado, mas, em vez disso, no múltiplo mais próximo de um tamanho de buffer interno para esse valor.

PreFilter
Especifica como os eventos em um Log de Eventos do Windows são filtrados antes do processamento do agente. As instruções PreFilter são usadas por PreFilterMode quando os filtros determinam quais eventos são enviados de um log de eventos para o agente. Um evento corresponde a uma instrução PreFilter quando cada especificação de *attribute=value* na instrução PreFilter corresponde a um evento no log de eventos. Uma instrução PreFilter deve conter pelo menos a especificação de log e pode conter até três especificações adicionais, que são todas opcionais: ID de evento, tipo de evento e origem de eventos. A ordem dos atributos na instrução não importa.

A instrução PreFilter possui o seguinte formato básico:

```
PreFilter:Log=log_name;EventId=value; EventType=value;Source=value;
```

É possível especificar diversos valores para cada atributo, separando cada valor com uma vírgula.

Cada instrução PreFilter deve estar em uma única linha.

PreFilter não é obrigatório. Todos os eventos de log do Windows são enviados ao agente se pré-filtros não são especificados e PreFilterMode=OUT.

PreFilterMode
Esta opção aplica-se somente ao Log de Eventos do Windows. A opção especifica se os eventos de log de sistemas Windows que correspondem a uma instrução PreFilter são enviados (PreFilterMode=IN) ou ignorados (PreFilterMode=OUT). Os valores válidos são IN, in, OUT ou out. O valor padrão é OUT.

PreFilterMode é opcional; se PreFilterMode não for especificado, apenas os eventos que não correspondem a nenhuma instrução PreFilter serão enviados para o agente.

Nota: Se você configurar PreFilterMode=IN, também deverá definir as instruções PreFilter.

SpaceReplacement
Configure como TRUE por padrão para o Windows Event Log (apenasWindows Server 2008) , mas não para anterior Versões do Evento Log . Quando SpaceReplacement é TRUE, quaisquer espaços nos campos de ID de segurança, suborigem, Nível e palavras-chave das mensagens do log de eventos são substituídos por sublinhados (_). Quando o SpaceReplacement for FALSE, qualquer espaço nos campos de ID de segurança, suborigem, Nível e palavras-chave das mensagens de log de evento permanecerá inalterado. Para obter informações adicionais sobre essa opção, consulte “Log de Eventos do Windows” na página 1019.

UseNewEventLogAPI
Quando configurado como y nos sistemas Windows, utiliza a nova interface do Log de Eventos do Windows para logs de eventos. A opção é suportada apenas no Windows 2008 e posterior. A opção é necessária para acessar muitos dos novos logs de eventos que estrearam no Windows 2008 e os aplicativos que são executados nele. A opção é ignorada em versões anteriores do Windows e no UNIX e Linux. Para obter informações adicionais sobre essa opção, consulte "Log de Eventos do Windows" na página 1019.

WINEVENTLOGS
Controla quais logs de eventos do Windows são monitorados.

A instrução WINEVENTLOGS é uma lista delimitada por vírgulas sem espaços. Para obter mais informações, consulte "Log de Eventos do Windows" na página 1019.

Nota: Todos os retornos de linhas, tabulações ou novas linhas em eventos do Windows são substituídos por espaços.

Opção que é suportada somente em sistemas AIX

AIX

AIXErrptCmd
Uma sequência de caracteres de comando **errpt** (relatório de erro) que é executada pelo agente pode ser fornecida aqui. A saída do comando é alimentada no fluxo de dados de log que está sendo monitorado.

Por exemplo, o comando a seguir faz com que o agente procure a sequência *mmddhhmmaa* e a substitua pela data e hora reais na inicialização. Somente a primeira ocorrência da sequência é substituída.

```
AIXErrptCmd=errpt -c -smmddhhmmyy
```

Embora seja possível fornecer seu próprio comando `errpt`, deve-se usar a opção `-c` (modo simultâneo) para que o comando seja executado continuamente. Não é possível usar a opção `-t` ou as opções a seguir que resultam em saída detalhada: `-a`, `-A` ou `-g`.

O fluxo de dados é a saída padrão do comando `errpt`, portanto, expressões regulares no arquivo `.fmt` deverão ser gravadas para correspondência. Por exemplo, a saída de dados pode ser:

```
IDENTIFIER TIMESTAMP  T C RESOURCE_NAME  DESCRIPTION
F7FA22C9   0723182911 I O SYSJ2      UNABLE TO ALLOCATE SPACE IN FILE SYSTEM
2B4F5CAB   1006152710 U U ffdc       UNDETERMINED ERROR
2B4F5CAB   1006152610 U U ffdc       UNDETERMINED ERROR
```

Um formato de amostra que seleciona as linhas de dados, mas não o cabeçalho, é:

```
REGEX GenericErrpt
^([A-F0-9]{8}) +([0-9]{10}) ([A-Z]) ([A-Z]) (\S+) +(.*)$
Identifier $1 CustomSlot1
Timestamp  $2 CustomSlot2
T          $3 CustomSlot3
C          $4 CustomSlot4
Resource   $5 CustomSlot5
msg        $6
END
```

Para obter mais informações, consulte *Monitorando um log binário do AIX* no Guia do Usuário do IBM Agent Builder.

Opções que se aplicam somente quando os eventos estão sendo encaminhados para o EIF

Importante: Essas opções se aplicam a eventos do EIF enviados diretamente para o Operations Analytics - Log Analysis, OMNIbus ou qualquer outro receptor EIF genérico. As opções não são destinadas para uso com o Servidor Cloud APM.

BufferEvents
Especifica como o buffer de eventos é ativado. Os possíveis valores são:

- **YES** - Armazena eventos no arquivo especificado pela opção BufEvtPath (Este valor é o padrão).
- **MEMORY_ONLY** - Armazena eventos em buffer na memória.
- **NO** - Não armazena eventos nem os coloca em buffers.

BufEvtPath
Especifica o nome do caminho completo do arquivo de cache do agente. Se esse caminho não for retificado, o padrão será:

- AIX `/etc/Tivoli/tec/cache`
- Windows `\etc\Tivoli\tec\cache`

Nota: Se eventos estiverem sendo encaminhados para mais de um servidor, um valor *BufEvtPath* deverá ser especificado para cada canal de encaminhamento. Um número de índice é anexado ao nome de *BufEvtPath* para cada entrada adicional. Por exemplo, use *BufEvtPath1* para indicar o nome do caminho do arquivo de cache do agente para encaminhamento ao primeiro servidor extra. O valor que é configurado em cada *BufEvtPath* deve ser exclusivo.

BufEvtMaxSize
Especifica o tamanho máximo, em KB, do arquivo de cache do agente. O valor padrão é 64. O arquivo de cache armazena eventos em disco quando a opção *BufferEvents* está configurada como Sim. O tamanho mínimo para o arquivo é 8 KB. Os tamanhos de arquivos especificados menores que esse nível são ignorados, e um tamanho de 8 KB é usado. O valor especificado para o tamanho máximo do arquivo não tem um limite superior.

Nota: Se o arquivo de cache existir, você deverá excluir o arquivo para que mudanças de opção entrem em vigor.

NO_UTF8_CONVERSION
Especifica se o Event Integration Facility codifica dados do evento em UTF-8. Quando esta opção está configurada como YES, o EIF não codifica os dados do evento em UTF-8. Supõe-se que os dados já estejam em codificação UTF-8 quando transmitidos ao EIF. No entanto, um prefixo será incluído na sinalização para indicar que os dados estão na codificação UTF-8 (se a sinalização não existir no início nos dados do evento). O valor padrão é N0.

MaxEventQueueDepth
Este valor indica o número máximo de eventos que podem ser enfileirados para encaminhamento. Quando o limite é atingido, cada novo evento que é colocado na fila empurra o evento mais antigo da fila. Se não especificado, o valor padrão será 1000. Esta configuração se aplica a todos os canais de encaminhamento se *NumAdditionalServers* é usado.

NumAdditionalServers
Essa entrada será necessária se você desejar encaminhar eventos para mais de um Netcool/OMNIbus ObjectServer. Seu valor é usado para indicar o número de servidores para os quais os eventos são encaminhados. Os valores válidos são 1 - 8.

ServerLocation
Especifica o nome do host no qual o servidor de eventos está instalado. Especifique o nome do host ou endereço IP. Use o formato de pontos para o endereço IP. É possível especificar valores de failover, como `ServerLocation1 = 2.3.4.5,2.3.4.6.` para os locais do servidor, se você desejar. Se você especificar valores de failover para *ServerLocation*, também deverá especificar um valor *ServerPort* extra para cada *ServerLocation*.

Nota: Se eventos estão sendo encaminhados para mais de um servidor, um valor de *ServerLocation* deve ser especificado para cada servidor. Um número de índice é anexado ao nome de *ServerLocation* para cada entrada adicional. Por exemplo, use *ServerLocation1* para especificar o nome do host no qual o primeiro servidor extra está instalado.

ServerPort
Especifica o número da porta na qual o receptor de EIF recebe os eventos. A opção *ServerPort* pode conter até oito valores, que são separados por vírgulas. Se os valores de failover forem especificados para *ServerLocation*, será necessário configurar um valor *ServerPort* equivalente. ServerPort não é usada quando a opção *TransportList* é especificada.

Nota: Se eventos estão sendo encaminhados para mais de um servidor, um valor de *ServerPort* deve ser especificado para cada servidor. Um número de índice é anexado ao nome de *ServerPort* para cada entrada adicional. Por exemplo, use *ServerPort1* para especificar o número da porta na qual o receptor EIF recebe eventos para o primeiro servidor extra.

TransportList
Especifica os nomes fornecidos pelo usuário dos mecanismos de transporte, que são separados por vírgulas. Quando um mecanismo de transporte falha nos aplicativos do emissor, a API usa os mecanismos de transporte a seguir na ordem especificada na lista. Para aplicativos de recepção, a API cria e usa todos os mecanismos de transporte. O tipo de transporte e o canal para cada *type_name* devem ser especificados usando as palavras-chave Type e Channels:

***type_name*Type**

Especifica o tipo de transporte para o mecanismo de transporte especificado pela opção *TransportList*. SOCKET é o único tipo de transporte suportado.

O servidor e a porta para cada channel_name são especificados pelas opções *ServerLocation* e *ServerPort*.

***type_name*Channels**

***channel_name*Port**
Especifica o número da porta no qual o servidor atende de mecanismos de transporte recebe o canal especificado (configurado pela opção *Channel*). Quando esta palavra-chave for configurada como zero, o portmapper será usado. Esta palavra-chave é obrigatório.

***channel_name*PortMapper**
Ativa o portmapper para o canal especificado.

***channel_name*PortMapperName**
Especifica o nome do portmapper, se o portmapper estiver ativado.

***channel_name*PortMapperNumber**
Especifica o ID que é registrado pela chamada de procedimento remoto.

***channel_name*PortMapperVersion**
Especifica a versão do portmapper, se o portmapper estiver ativado.

***channel_name*ServerLocation**
Especifica o nome do servidor de eventos e a região onde o servidor para mecanismos de transporte está localizado para o canal especificado. O canal é configurado pela opção *Channel*. Esta palavra-chave é obrigatório.

O arquivo de configuração aceita opções de EIF genéricas quando usado diretamente com o OMNIbus. Essas opções operam apenas por meio de uma conexão de EIF para o OMNIbus. Elas não afetam os eventos que são enviados para o Servidor Cloud APM. Para obter mais informações sobre essas opções de EIF, consulte Palavras-chave de EIF.

arquivo de Formato
OS Agents extraem informações das mensagens de log do sistema e, depois, fazem a correspondência de diferentes mensagens de log com classes de eventos. Um arquivo de formato serve como um arquivo de consulta para corresponder mensagens de log com classes de eventos, que instrui a classe de eventos sobre o que ler, o que corresponder e como formatar os dados.

Quando o arquivo de formato é usado como um arquivo de consulta, todas as especificações de formato no arquivo são comparadas do início ao fim do arquivo. Quando duas classes correspondem ou quando uma mensagem tem várias classes correspondentes, a primeira expressão da extremidade que corresponder será usada. Se nenhuma correspondência for localizada, o evento será descartado. Um evento descartado é gravado no log sem correspondência se ele é definido no arquivo `.conf`.

A sintaxe de expressão regular usada para criar padrões para a correspondência de mensagens de log e eventos é descrita. O suporte de filtragem de expressão regular é fornecido usando as bibliotecas International Components for Unicode (ICU) para verificar se um valor de atributo examinado corresponde ao padrão especificado.

Para obter informações adicionais sobre como usar expressões regulares, consulte Regular Expressions no *Guia do Usuário do ICU*.

Especificações do Arquivo de Formato
O arquivo de formato descreve os padrões que o agente procura para corresponder eventos nos logs monitorados. O arquivo de formato consiste em uma ou mais especificações de formato.

É possível alterar o arquivo de formato enquanto uma instância do agente está em execução. O arquivo é lido pelo agente quando ele é iniciado e é monitorado em busca de mudanças em seu registro de data e hora a cada 60 segundos depois disso. Se o registro de data e hora do arquivo mudar, o agente reinicializará sua configuração dinamicamente sem requerer reinicialização. Para obter mais informações, consulte "Alterando os Arquivos de Configuração e de Formato do Agente" na página 651.

Para criar novos padrões para corresponder a um evento, use a nova sintaxe de expressão regular que consiste nas partes a seguir:

- Cabeçalho de Formato
- Expressão regular
- Mapeamentos de Slot
- Instrução End

O cabeçalho de formato contém a palavra-chave **REGEX**, que informa ao agente que você está usando uma expressão regular para corresponder ao padrão no log monitorado.

Você designa esta expressão regular para uma classe de eventos, conforme mostrado no exemplo a seguir:

```
REGEX REExample
```

Se você usar a classe de eventos predefinida especial *DISCARD* como sua classe de eventos, quaisquer registros de log correspondentes ao padrão associado serão descartados e nenhum evento será gerado para eles. Por exemplo:

```
REGEX *DISCARD*
```

Quando um padrão é correspondido, nada é gravado no log não correspondido. Os registros de status de arquivo de log que são correspondidos incluem estes eventos descartados.

Nota: É possível designar diversas definições de eventos para a mesma classe de eventos ou para classes de eventos diferentes. O nome de classe é arbitrário e você pode usá-lo para indicar o tipo de evento ou para agrupar eventos de várias maneiras.

Após o cabeçalho de formato, o conteúdo do formato consiste em uma expressão regular na primeira linha, seguida por mapeamentos. Cada mapeamento é mostrado em uma linha separada e estes mapeamentos são descritos no exemplo a seguir.

Todas as linhas que correspondem a expressões regulares são selecionadas e enviadas ao servidor de monitoramento como eventos. A expressão regular contém subexpressões. É possível usar as subexpressões para corresponder a partes específicas dessas linhas que são iguais a uma variável chamada *slot* no Event Integration Facility.

O log de monitoramento a seguir contém três linhas que talvez você queira monitorar:

```
Error:  disk failure
Error: out of memory
WARNING: incorrect login
```

Por exemplo, você gera um evento para um erro específico, como as linhas que começam com `Error` e ignora a linha que começa com `Warning`. A expressão regular deve corresponder às linhas que começam com `Error` e também incluem uma subexpressão. A subexpressão é denotada por parênteses e deve

corresponder apenas ao texto de entrada que você deseja designar ao slot *msg*. A seguinte definição de formato é uma expressão regular simples com apenas uma subexpressão:

```
REGEX REExample
Error: (.*)
msg $1
END
```

Com base nesta especificação de formato e no conjunto de dados de log precedente, o agente gera dois eventos. Ambos os eventos têm a classe de eventos `REEXample` designada. No primeiro evento, o valor de `disk failure` é designado ao slot *msg*. Além disso, no segundo evento, o valor out of memory é designado ao slot *msg*. Como a linha `Warning` não correspondeu à expressão regular, ela será ignorada e nenhum evento será gerado.

Ao designar o valor de $1 ao slot *msg*, você designa a ele o valor da primeira subexpressão.

Se você tiver um texto de log que contém os seguintes erros, talvez queira designar essas mensagens de erro à sua própria classe de eventos para ser informado imediatamente de uma falha de disco:

```
Error: disk failure on device /dev/sd0: bad sector
Error: disk failure on device /dev/sd1: temperature out of range
```

É possível incluir uma descrição do disco no qual o erro ocorreu, e mais especificamente o erro de disco no evento.

A expressão regular a seguir contém duas subexpressões que identificam estas informações:

```
REGEX DiskFailure
Error: disk failure on device (/dev/sd[0-9]):(.*)
device $1 CustomSlot1
msg $2
END
```

Você designa essas duas subexpressões a slots de eventos. Os dois eventos que são gerados contêm os seguintes valores:

```
"device=/dev/sd0" and "msg=bad sector"
"device=/dev/sd1" and "msg=temperature out of range"
```

Se você utilizar o EIF para gerar o primeiro evento, ele será exibido conforme mostrado no exemplo a seguir:

```
DiskError;device='/dev/sd0';msg='bad sector';END
```

Se o evento é enviado para o Servidor Cloud APM, o slot que é denominado *msg* é designado para o agente do Performance Management Atributo com o mesmo Nome . Mas o slot *device* não possui nenhum atributo predefinido.

Se precisar ver o valor designado a *device* diretamente no Console do Cloud APM, ou gravar limites nele, deve-se designá-lo a um atributo de Performance Management.

O agente de S.O. inclui os 13 seguintes atributos predefinidos:

- Dez atributos de tipo de sequência que variam de *CustomSlot1* a *CustomSlot10*
- Três atributos de tipo de número inteiro que variam de *CustomInteger1* a *CustomInteger3*

O uso desses nomes de atributos no arquivo de formato preenche atributos do Performance Management com o mesmo nome. O uso destes atributos não afeta o conteúdo do evento EIF enviado diretamente ao OMNIbus.

Nota: Os nomes de atributos `CustomSlot` e `CustomInteger` fazem distinção entre maiúsculas e minúsculas, portanto, deve-se inserir os nomes exatamente conforme mostrados.

Você designa um slot da definição de evento a um dos atributos do Performance Management customizados no arquivo de formato.

Você designa o slot *device* ao atributo de tipo sequência do Performance Management chamado *CustomSlot1*, conforme mostrado no exemplo a seguir:

```
REGEX DiskFailure
Error: disk failure on device (/dev/sd[0-9]):(.*)
device $1 CustomSlot1
msg $2
END
```

Quando o evento é exibido no Application Performance Dashboard, o valor designado ao slot *device* é designado ao atributo `CustomSlot1` do Performance Management. Você visualiza esse valor no Console do Cloud APM ou usa-o para definir limites. É possível designar qualquer slot na definição de evento a qualquer um dos 10 atributos de agente customizado da mesma maneira, usando "`CustomSlot`*n*", em que *n* é um número de 1 a 10, próximo à definição de slot.

Neste exemplo, a primeira subexpressão é definida especificamente como `(/dev/sd[0-9])`, mas a segunda subexpressão é geralmente definida como `(.*)`. Ao definir a expressão regular o mais especificamente possível, você melhora o desempenho. Portanto, se você inserir uma procura por um erro em um dispositivo que não corresponde à mensagem de erro específica definida aqui, o procedimento de procura parará imediatamente quando o erro não for localizado. O tempo não é desperdiçado procurando uma correspondência.

A palavra-chave *END* completa a especificação de formato. O cabeçalho de formato, a expressão comum e a palavra-chave *END* deve iniciar cada um em uma nova linha, conforme mostrado no exemplo a seguir:

```
REGEX REExample
Erro:
msg $1
END <EOL>
<EOF>
```

Nota: Para o último formato no arquivo, deve-se inserir uma nova linha após a palavra-chave `END`, conforme mostrado no exemplo. Caso contrário, você obtém um erro de análise.

CustomInteger1 a *CustomInteger3* são atributos de número inteiro customizados de 64 bits. É possível usá-los da mesma maneira que os atributos do tipo sequência `CustomSlot`. Você pode utilizar esses atributos para mapear slots individuais, ou subexpressões, a partir do arquivo de log para cada Cloud APM atributos. Como esses atributos são numéricos, é possível usar comparações aritméticas neles, como < e >, o que não é possível com os atributos de sequência.

Nota: Embora esses valores são avaliados como inteiros pelo Servidor Cloud APM, para propósitos de EIF e no arquivo de formato, eles ainda são tratados como Sequências . Por exemplo, para usar um slot de número inteiro em uma instrução PRINTF, você ainda o identifica com “%s”, não com “%d”.

O exemplo a seguir ilustra o uso de um atributo de número inteiro customizado. Suponha que uma mensagem syslog periódica do UNIX que relata a porcentagem de um sistema de arquivos que está livre seja recebida, tal como o registro de log hipotético a seguir:

```
Oct 24 11:05:10 jimmy fschecker[2165]: Filesystem /usr is 97% full.
```

É possível usar a instrução a seguir no arquivo de formato para verificar a porcentagem do sistema de arquivos que está livre:

```
REGEX FileSystemUsage
^([A-Z][a-z]{2}) ([ 0-9][0-9]) ([0-9]{2}:[0-9]{2}:[0-9]{2}) (.*?) (.*?):
Filesystem (.*?) is ([0-9]+)% full\.$
Month   $1 CustomSlot1
Date    $2 CustomSlot2
Time    $3 CustomSlot3
Host    $4 CustomSlot4
Service $5 CustomSlot5
Filesystem     $6 CustomSlot6
PctFull         $7  CustomInteger1
msg          PRINTF("%s: %s% full", Filesystem, PctFull)
END
```

Nota: Na instrução precedente, tudo entre os símbolos ^ e $ na segunda e na terceira linhas devem estar em uma única linha.

Como você pode ter outros eventos que colocam valores em *CustomInteger1*, é possível evitar confundir os diferentes tipos de eventos utilizando o valor do atributo *Class* para limitar seu efeito para o tipo correto de eventos. Por exemplo, a fórmula de limite a seguir faz com que o limite seja disparado somente quando um evento da classe de eventos *FileSystemUsage* tiver um valor maior que ou igual a 95 no *CustomInteger1*:

```
(  Class == 'FileSystemUsage' AND CustomInteger1 >= 95)
```

Um evento diferente pode então usar *CustomInteger1* para um propósito diferente e não acionar esse limite acidentalmente.

Em resumo, agora é possível gravar um limite no Performance Management que use operadores aritméticos em atributos `CustomInteger`, o que não é possível com atributos `CustomSlots`.

Nota: Se você mapear dados não de número inteiro para os atributos `CustomInteger`, o valor resultante pode ser zero ou algum valor inesperado.

Alterando os Arquivos de Configuração e de Formato do Agente
O agente de S.O. lê seus arquivos de configuração (`.conf`) e de formato (`.fmt`) quando ele é iniciado, e monitora o registro de data e hora a cada 60 segundos depois disso.

Se o registro de data e hora do arquivo de configuração ou de formato mudar, o agente inicializará sua configuração dinamicamente, sem requerer uma reinicialização. Durante a reinicialização, o monitoramento é interrompido momentaneamente. Quando o monitoramento for retomado, o agente deverá determinar a posição nos logs monitorados a partir da qual reiniciar. Como resultado, o agente se comporta da mesma maneira que uma parada e uma reinicialização completas.

Nota: A reinicialização do agente depois de uma mudança no arquivo de configuração ou de formato reconfigura as informações nos grupos de atributos `Estatísticas RegEx do arquivo de log`, `Status do arquivo de log` e `Evento do arquivo de log`.

Por padrão, o agente inicia o monitoramento a partir do final do arquivo, quando a reinicialização conclui. Esta posição inicial pode fazer com que eventos que ocorreram durante a interrupção do monitoramento sejam perdidos. Para assegurar que tais eventos sejam selecionados quando o monitoramento for retomado, use a configuração `NumEventsToCatchUp=-1`.

A configuração `NumEventsToCatchUp=-1` faz com que um arquivo de posição seja mantido. O arquivo de posição é atualizado sempre que o agente lê o arquivo de log. A atualização salva a posição do agente no arquivo de log, no caso de um agente reiniciar. A manutenção do arquivo de posição tem um pequeno impacto no desempenho, portanto, mantenha esse arquivo somente se necessário. Para obter informações adicionais sobre `NumEventsToCatchUp`, consulte “Arquivo de configuração” na página 638.

Nota: Alguns valores de configuração não estão presentes no arquivo de configuração e são configurados durante a configuração inicial. Se você alterar estes valores, deverá reiniciar o agente.

Herança
Um arquivo de formato usa a herança para derivar definições de slot a partir de uma especificação de formato definida anteriormente.

Use o relacionamento FOLLOWS para construir especificações de formato específico a partir de especificações de formato genérico usando a herança.

Primeiro, defina uma classe base e chame-a de `DiskFailure`, por exemplo, conforme mostrado aqui:

```
REGEX DiskFailure
Disk Failure on device (.*)
device $1 CustomSlot1
END
```

Esta expressão regular corresponde os erros `Disk Failure on device/dev/sd0` no log de monitoramento para que o valor `/dev/sd0` seja designado ao slot *device*.

No entanto, também é possível ver uma versão estendida desta mensagem de erro relatada no log de monitoramento.

Por exemplo, você pode ver uma mensagem de erro `Disk Failure on device /dev/sd0, error code: 13`.

Esta mensagem de erro é correspondida em um slot, conforme mostrado no exemplo a seguir:

```
REGEX DiskFailureError FOLLOWS DiskFailure
Disk Failure on device (.*), error code: ([0-9]*)
errcode $2 CustomSlot2
END
```

Agora, o evento inclui o slot *device* e o slot *errcode*. Como a classe de eventos `DiskFailure` já definiu um slot para o nome do dispositivo, permita que a subclasse herde esse slot e essa herança evita que você declare-o uma segunda vez. O slot é definido como $1, portanto, a primeira subexpressão na expressão regular é designada a esse slot.

No entanto, a classe `DiskFailureError` também define uma segunda subexpressão. É possível designar essa subexpressão a um novo slot chamado `errcode` e defini-lo como $2 para referir-se à segunda subexpressão na expressão regular. Este tipo de designação é mostrado no exemplo anterior que exibe o texto de log.

O evento agora contém o slot `device` que tem o valor `/dev/sd0` designado e o slot `errcode` que tem um valor igual a 13 designado. CustomSlot1 tem o dispositivo designado e CustomSlot2 tem o código de erro designado.

Mapeamentos de atributo customizado do Performance Management também são herdados. Para obter mais informações sobre os mapeamentos de atributo customizado do Performance Management, consulte “Especificações do Arquivo de Formato” na página 648.

Várias Linhas

Use a sintaxe multilinhas para corresponder registros que se estendem por mais de uma linha aos padrões no log que está sendo monitorado.

Especifique o caractere de nova linha `\n` como parte da expressão regular para indicar onde as quebras de linha ocorrem no log de monitoramento. Consulte este tipo de sintaxe no exemplo a seguir:

```
REGEX REMultiLine
Line1:(.*)\nLine2(.*)
msg $1
second_msg $2
END
```

Nota: Windows Especifique uma combinação de retorno de linha `\r\n` e de nova linha.

Se as mensagens de erro a seguir forem relatadas no texto do log, o evento REMultiLine será criado:

```
Line1: An error occurred
Line2: The error was "disk error"
```

O slot `msg` recebe o valor de `An error occurred` e o slot `second_msg` recebe o valor de `The error was "disk error"`.

Mapeamentos

O OS Agent usa mapeamentos para determinar a classe de eventos para uma mensagem de log do sistema. O agente determina a classe de eventos correspondendo a mensagem com um padrão no arquivo de formato.

O agente converte mensagens de log em instâncias da classe de eventos que contêm pares de atributos `name=value`. O evento é então enviado ao servidor de eventos.

O agente determina a classe de eventos para uma mensagem de log do sistema na origem. O agente determina a classe de eventos correspondendo uma mensagem de log do sistema com um padrão no

arquivo de formato. Após usar este procedimento correspondente para determinar uma classe, você deve designar valores para os atributos.

Os valores de atributo vêm de várias origens, tais como:

- Valores padrão que são fornecidos pelo agente
- Texto de log que corresponde às subexpressões específicas em expressões regulares

Uma instrução de mapa é incluída no arquivo de formato e consiste na seguinte sintaxe:

```
name    value CustomSlotn
```

Aqui, você especifica qualquer identificador para descrever o name de um slot (também conhecido como uma variável, um atributo ou identificador de valor). Em seguida, você especifica um valor para designar a este slot aplicando qualquer um dos valores que são descritos em "Especificadores de Valor" na página 653.

Use slots customizados para visualizar dados no console do Performance Management e definir limites. Ao criar limites, todos os valores de slot customizados são sequências. Os slots customizados também são necessários para que a detecção de duplicata funcione, porque é preciso identificar os slots que são usados para determinar duplicatas. Para obter mais informações sobre como filtrar eventos, consulte "Filtro de eventos e resumo" na página 1017. msg é um nome de slot especial, com seu próprio atributo na tabela de eventos. Não é necessário usar um slot customizado para msg.

É possível limitar o escopo de um slot para que ele exista apenas dentro da definição de formato. Ao definir o slot, preceda o nome do slot com um traço, por exemplo:

```
-name    value
```

Qualquer slot definido desta maneira não é incluído no evento final. No entanto, é possível referenciar o slot em outra parte na definição de formato, especificamente dentro de uma instrução PRINTF. No exemplo REGenericSyslog a seguir, o slot service não será incluído se você gerar, mas puder referenciá-lo na instrução PRINTF. Ele retém o mesmo valor que foi aplicado ao slot original quando ele foi definido sem o traço. Usando esse procedimento, é possível usar variáveis temporárias da definição de formato que não estão incluídas no evento final. Por exemplo, é possível definir uma classe de eventos, REGenericSyslog, para corresponder eventos syslog do UNIX genéricos da seguinte maneira:

```
REGEX REGenericSyslog
^([A-Z][a-z]{2}) ([ 0-9][0-9]) ([0-9]{2}:[0-9]{2}:[0-9]{2}) (.*?) (.*?): (.*)$
mês $1
date $2
time $3
host $4
-service $5
msg $6
syslog_msg PRINTF("service %s reports %s", service, msg)
END
```

Especificadores de Valor
Os mapeamentos em uma especificação de formato designam valores a atributos.

A parte do mapeamento de uma especificação de formato consiste nos tipos a seguir de especificadores de valor:

- $i
- Constante de cadeia
- Instrução PRINTF

$i

O i indica a posição de uma subexpressão em uma sequência de formatações. Cada subexpressão é numerada de 1 ao número máximo de subexpressões na sequência de formatações.

O valor de um especificador de valor $i (também conhecido como uma variável, slot ou atributo) é a parte da mensagem de log do sistema que é correspondida pela subexpressão correspondente.

No exemplo a seguir, o agente de log converte qualquer mensagem de log do recurso syslog do UNIX em um evento syslog com valores designados a ele:

```
REGEX REGenericSyslog
^([A-Z][a-z]{2}) ([ 0-9][0-9]) ([0-9]{2}:[0-9]{2}:[0-9]{2})
 (.*?) (.*?): (.*)$
month   $1
date    $2
time    $3
host    $4
service $5
msg     $6
END
```

Cada subexpressão numerada de $1 a $6 corresponde a um item entre parênteses na expressão regular.

Portanto, o evento syslog a seguir:

```
Apr  6 10:03:20 jimmy syslogd 1.4.1: restart.
```

tem os valores a seguir designados:

```
month=Apr
date=6
time=10:03:20
host=jimmy
service=syslogd 1.4.1
msg=restart.
```

Por exemplo, no evento syslog, o valor `10:03:20` corresponde ao terceiro item entre parênteses na expressão regular, portanto, o valor é designado ao valor de tempo de *$3*. De modo semelhante, o valor de `jimmy` corresponde ao quarto item entre parênteses na expressão regular, portanto, o valor é designado ao valor de host *$4*.

constante da sequência

A constante da sequência declara que o valor do atributo é a sequência especificada. Se o valor de atributo for uma constante única sem qualquer espaço, especifique-o sem colocá-lo entre aspas duplas (" "), conforme mostrado no exemplo a seguir:

```
severity WARNING
```

Caso contrário, se há espaços no valor de atributo, aspas duplas devem ser usadas conforme mostrado no exemplo a seguir:

```
component "Web Server"
```

Instrução PRINTF

A instrução PRINTF cria valores de atributos mais complexos a partir de outros valores de atributos. A instrução PRINTF consiste na palavra-chave `PRINTF` seguida por uma sequência de formatações C printf() e um ou mais nomes de atributos.

A sequência de formatações suporta apenas o especificador do componente `%s`. Os valores dos atributos que são usados na instrução PRINTF devem ser derivados de uma especificação de valor *$i* ou de uma especificação de valor de sequência constante (não é possível derivá-los de uma outra instrução PRINTF).

Use o valor dos atributos de argumento para compor uma nova sequência de constantes de acordo com a sequência de formatações. Essa nova cadeia de constantes torna-se o valor do atributo.

Com base no exemplo anterior no qual você definiu a classe base `REGenericSyslog`, e os slots *service* e *msg*, é possível definir um atributo chamado *syslog_msg* usando a palavra-chave `PRINTF`.

```
syslog_msg PRINTF("service %s reports %s", service, msg)
```

Se a mensagem de log a seguir for relatada:

```
Apr  6 10:03:20 jimmy syslogd 1.4.1: restart.
```

é editada uma nova sequência de constantes que contém os valores de atributo da sequência de formatações:

```
syslog_msg="service syslogd 1.4.1 reports restart."
```

Palavras-Chave
No arquivo de formato, use palavras-chave para designar valores que se expandem no tempo de execução.

As palavras-chave a seguir se expandem no tempo de execução:

- DEFAULT
- FILENAME
- LABEL
- REGEX

DEFAULT

Use a palavra-chave DEFAULT para designar um valor DEFAULT para um slot ou atributo específico. O OS Agent designa um valor padrão interno aos slots descritos na tabela a seguir:

Tabela 191. Slots e o Valor DEFAULT

Slots	**Descrição**
nome do host	*hostname* é o nome abreviado do host do sistema no qual o agente está em execução. Ele não inclui o nome de domínio do sistema.
origin	*origin* é o endereço IP do sistema no qual o agente está em execução.
fqhostname	*fqhostname* é o nome completo do host do sistema no qual o agente está em execução. Ele inclui o nome de domínio do sistema.
Host Remoto	Quando um evento for originado no sistema local, esse atributo ficará vazio. Se um evento for originado em um sistema remoto, *RemoteHost* conterá uma sequência no formato *user@host:port*, que indica o nome do sistema remoto no qual ocorreu o evento, e o usuário e porta nesse host que são usados para conexão.

O valor designado a *fqhostname* é influenciado pelas seguintes configurações de FQDomain (opcional) no arquivo `.conf`:

- Se você configurar FQDomain como `yes`, o próprio agente determinará o nome de domínio do sistema.
- Se você não configurar um valor para FQDomain ou se configurar o valor como no, o agente não configurará um nome de domínio, e ao atributo *fqhostname* será designada uma sequência em branco.
- Se você configurar FQDomain para que não contenha um valor `yes` ou no, o nome de domínio será aceito como o valor e será anexado ao nome do host.

No exemplo a seguir, a definição de formato contém três atributos ou slots:

- *hostname* DEFAULT

- *origin* DEFAULT
- *fqhostname* DEFAULT

Se você configurar FQDomain como yes no arquivo .conf e executá-lo em um computador com as seguintes propriedades:

- *hostname*: myhost
- *IP address*: 192.168.1.100
- *domainname*: mycompany.com

será criado um evento e aos três slots serão designados os seguintes valores:

```
"hostname=myhost", "origin=192.168.1.100", "fqhostname=myhost.mycompany.com"
```

FILENAME

A palavra-chave FILENAME indica o nome completo do arquivo (incluindo o caminho) do arquivo de log que contém a mensagem. Se você usar um único agente para monitorar vários arquivos de log e precisar identificar a origem do evento, use essa palavra-chave para preencher um atributo do evento com o nome do arquivo. Se a mensagem vier do log do sistema, o mapeamento será configurado como EventLog para agentes de S.O. Windows e SysLogD para agentes de S.O. UNIX.

Nota: O caminho inclui um atributo para esta palavra-chave.

LABEL

A palavra-chave LABEL especifica o nome do host do sistema onde o agente está em execução.

REGEX

A palavra-chave REGEX se expande para a expressão regular que corresponder à mensagem e causou o evento.

Comprimento Máximo de Mensagem
Este valor é o comprimento máximo da mensagem que o OS Agent pode receber sem truncar a mensagem.

O comprimento máximo da mensagem é diferente para o Performance Management e o Tivoli Netcool/OMNIbus.

Performance Management

Para eventos enviados para o Performance Management, o atributo msg é limitado a 2048 bytes. As mensagens com comprimento maior são truncadas.

Tivoli Netcool/OMNIbus

Para eventos enviados por meio de Probe for Tivoli EIF para Netcool/OMNIbus, o tamanho total do evento, incluindo o nome de classe e todos os slots e seus valores, não pode exceder 4096 bytes. Por exemplo, no evento EIF de amostra a seguir, ;END não conta para o limite de 4096 bytes. No entanto, todo o restante é considerado para o limite, incluindo os elementos sintáticos, como pontos e vírgulas, aspas e sinais de igual.

```
Class;attr1=value1;attr2=value2;msg='Hello, world';END
```

Monitoramento de arquivo de log remoto: Criptografando uma senha ou um passphrase
Para maior segurança, você pode criptografar as senhas e os passphrases que são transmitidos para os sistemas remotos ao usar o Monitoramento de Arquivo de Log Remoto.

Sobre Esta Tarefa
A senha e as passphrases criptografadas são armazenadas no arquivo de configuração (.conf). Para obter informações adicionais sobre o arquivo de configuração, consulte “Arquivo de configuração” na página 638.

Procedimento

- Execute o comando **itmpwdsnmp** e forneça a senha ou o passphrase que deve ser criptografado:
  - Linux AIX O comando é executado a partir do diretório de instalação do Cloud APM. O caminho da instalação padrão é `opt/ibm/apm/agent` e *install_dir* é onde o agente foi instalado.
  - Windows O caminho da instalação padrão é `C:\IBM\APM`.

  Linux Exemplo do comando, quando ele for executado em um sistema Linux:

```
$ export install_dir=/opt/ibm/apm/agent/bin
$ /opt/ibm/apm/agent/bin

Insira a sequência a ser criptografada:
mypassword

Confirmar Sequência:
mypassword

{AES256:keyfile:a}Z7BS23aupYqwlXb1Gh+weg==
$
```

  No exemplo, a saída inteira do comando `{AES256:keyfile:a}Z7BS23aupYqwlXb1Gh+weg==` é usada para configurar **SshPassword** no arquivo de configuração do agente. O prefixo `{AES256:keyfile:a}` informa ao agente que a senha está criptografada.

  Para criptografar um passphrase para um arquivo de chave privado, siga o mesmo procedimento.

Configurando script customizado do agente de S.O.

Os agentes do Monitoring Agent for Linux OS, do Monitoring Agent for UNIX OS e do Monitoring Agent for Windows OS são configurados automaticamente. Esse recurso permite que os usuários definam scripts para execução em agentes de S.O. em uma frequência determinada.

O recurso de script customizado é ativado por padrão. O administrador pode ativá-lo ou desativá-lo configurando uma nova variável de ambiente *KXX_FCP_SCRIPT*=true/false (o padrão é true) no arquivo de configuração do agente, em que XX pode ser:

- LZ para Monitoring Agent for Linux OS

- UX para Monitoring Agent for UNIX OS

- NT para Monitoring Agent for Windows OS

Os detalhes são fornecidos nas seções a seguir.

Iniciação rápida de script customizado
Inclua o script customizado para os agentes de S.O. para definir scripts para execução em agentes de S.O. em uma frequência definida.

O recurso é ativado com valores padrão assim que o agente de S.O. é iniciado. A única ação para iniciar o recurso de script é:

Crie um arquivo de propriedade sob o diretório padrão (no Linux™ ou UNIX™, é `install_dir/localconfig/product code/scripts_definitions`, no Windows™, é `install_dir\localconfig\nt\scripts_definitions`) usando como exemplo o modelo `script_property.txt` fornecido.

Somente duas propriedades são necessárias:

ATTRIBUTE_NAME
Qualquer nome usado para identificar exclusivamente a definição de script dentro do arquivo de propriedade.

SCRIPT_PATH_WITH_PARMS
O caminho completo do script com argumentos.

Não só os shell scripts, mas também o perl e outros tipos de scripts podem ser usados. Especifique o comando completo para execução na propriedade SCRIPT_PATH_WITH_PARMS.

Por exemplo, `perl C:\IBM\scripts\Custom_Scripts\date.pl`. Nesse exemplo, certifique-se de que o local do `perl` possa ser resolvido pelo agente através da variável PATH em seu ambiente. Senão, especifique o caminho completo no qual o `perl` é instalado.

Parâmetros em arquivos de ambiente do agente de S.O.
É possível configurar os parâmetros para script customizado nos arquivos de ambiente de agente de S.O.

É possível customizar o recurso de script definindo parâmetros nos arquivos de ambiente do agente de S.O.:

***install dir*/config/lz.environment**
O arquivo de ambiente para o Monitoring Agent for Linux OS.

***install dir*/config/ux.environment**
O arquivo de ambiente para o Monitoring Agent for UNIX OS.

***install dir*\TMAITM6_x64\KNTENV**
O arquivo de ambiente para o Monitoring Agent for Windows OS de 64 bits.

***install dir*\TMAITM6\KNTENV**
O arquivo de ambiente para o Monitoring Agent for Windows OS de 32 bits.

KXX_FCP_SCRIPT
O recurso de script é ativado por padrão. Para desativá-lo, configure: KXX_FCP_SCRIPT=false

Outros parâmetros podem ser definidos dentro dos arquivos de ambiente do agente com base em necessidades específicas:

KXX_FCP_SCRIPT_DEFINITIONS
O local onde arquivos de propriedade estão armazenados.

O local padrão no Linux™ ou UNIX™ é *install dir*/localconfig/*PC*/scripts_definitions; no Windows™, é *install dir*\localconfig\nt\scripts_definitions

KXX_FCP_SCRIPT_INTERVAL

O agente de S.O. usa o valor dessa variável como um intervalo de loop em segundos para verificar a execução dos scripts e envia eventos se a condição de filtro for atendida. O valor mínimo é de 30 segundos e o valor máximo é de 300 segundos. Valores inválidos são reconfigurados para o padrão. O valor-padrão é 60 segundos.

Nota: Esse parâmetro será ignorado se KXX_FCP_SCRIPT_SYNC_INTERVALS for configurado para USE_SCRIPT (consulte a definição para KXX_FCP_SCRIPT_SYNC_INTERVALS).

KXX_FCP_SCRIPT_SYNC_INTERVALS

Se o intervalo de looping do agente definido por KXX_FCP_SCRIPT_INTERVAL for maior que a frequência de execução do script, pode acontecer de os dados produzidos por alguns dos loops de execução do script serem perdidos. Para evitar esse comportamento, a frequência de execução do script pode ser sincronizada com o intervalo de looping do agente configurando KXX_FCP_SCRIPT_SYNC_INTERVALS para:

- USE_AGENT - O valor de cada frequência de execução do script é forçado a ser o máximo entre o KXX_FCP_SCRIPT_INTERVAL e o EXECUTION_FREQUENCY definido em seu arquivo de propriedade.
- USE_SCRIPT - O intervalo de loop do agente é configurado dinamicamente para o valor mínimo de frequência (EXECUTION_FREQUENCY no arquivo de propriedade) entre todos os scripts definidos. O valor configurado por KXX_FCP_SCRIPT_INTERVAL é ignorado. A frequência dos scripts permanece conforme definido nos arquivos de propriedade. Quando se configura USE_SCRIPT, o intervalo de looping do agente pode mudar cada vez que uma definição de script é incluída ou removida. Em qualquer caso, ele não pode ser menor que o valor configurado por KXX_FCP_OVERRIDE_MIN_FREQUENCY_LIMIT ou maior que 300 segundos.
- NO - Não é feita qualquer sincronização e alguns resultados de execução podem ser perdidos.

KXX_FCP_SCRIPT_DEFINITIONS_CHECK_INTERVAL

Na inicialização e em cada intervalo definido por essa variável, o agente de S.O. verifica quaisquer mudanças em scripts ou arquivos de propriedades. Observe que se o KXX_FCP_SCRIPT_DEFINITIONS_CHECK_INTERVAL for menor que o intervalo de looping do agente, ele será reconfigurado para o intervalo de looping do agente. O valor máximo permitido é o padrão, de 300 segundos.

KXX_FCP_USER

Este parâmetro só é válido em agentes de S.O. Linux™ ou UNIX™. Ele define o `user` usado para criar o processo fcp_deamon se for diferente do usuário do processo do agente de S.O.; todos os scripts são executados por esse usuário. Saiba que o proprietário do agente de S.O. deve ter a permissão correta para criar o processo fcp_daemon. No Windows™, um usuário diferente deve ser definido como login do serviço Monitoring Agent for Windows OS "FCProvider". O usuário deve ter a permissão "Controle Total" para o diretório de instalação do agente e para os diretórios do repositório de scripts. Para obter mais informações, consulte:

https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/install/install_linuxaix_agent_nonroot.html

KXX_FCP_MAX_CDP_DP_THREAD_POOL_SIZE

Define o número máximo simultâneo de scripts a serem executados. O valor máximo é 32.

KXX_FCP_MAX_DAEMON_RESTARTS

O agente de S.O. observa o fcp_daemon: se ocorrer uma saída anormal do processo, o agente de S.O. irá reiniciá-lo. O valor padrão é 4. A reinicialização é feita para KXX_FCP_MAX_DAEMON_RESTARTS (vezes por dia). O valor 0 deve ser usado para evitar reinicialização; se -1 for configurado, o agente de S.O. tentará reiniciar o fcp_daemon novamente para sempre. O contador de reinicialização é reconfigurado na reinicialização do agente de S.O.

KXX_FCP_SEND_SCRIPT_RUNTIME_EVENTS

O valor padrão é true. Se for configurado para false, o agente de S.O. parará de enviar eventos para cada linha de saída padrão de script. Nesse caso, as saídas de script ficam visíveis nas áreas de trabalho do console, mas nenhuma situação é exibida e nenhum dado histórico é coletado.

KXX_FCP_OVERRIDE_MIN_FREQUENCY_LIMIT

Usado quando KXX_FCP_SCRIPT_SYNC_INTERVALS é configurado para USE_SCRIPT. Nessa condição, ele configura o valor mínimo do intervalo de looping do agente de S.O.

O uso de valores baixos para o intervalo de looping do agente de S.O. (menor que 5 segundos) é altamente invasivo e pode impactar o desempenho do agente de S.O. Se for necessário fazer coletas de dados frequentes (por exemplo, a cada segundo), é sugerido customizar um script. O script armazena dados em cache na frequência necessária e retorna os dados coletados para o agente de S.O. em um intervalo maior (por exemplo, a cada 60 segundos).

As seguintes variáveis (CDP) do Agent Builder também podem ser usadas para controlar o comportamento do fcp_daemon:

CDP_DP_REFRESH_INTERVAL

(padrão de 60 seg.) Horário de início planejado do script global. Usado se a frequência não for transmitida no arquivo de propriedade de script.

CDP_DP_SCRIPT_TIMEOUT

(padrão de 30 seg.) Tempo máximo de execução do script global. Quando o tempo de execução de um script excede esse limite, seu Status_Code é configurado para TIMEOUT

CDP_DP_KILL_ORPHAN_SCRIPTS

(Y|N - padrão N) Comportamento global usado pelo processo fcp_daemon para scripts de tempo limite. Quando configurado para 'Y', os scripts são finalizados; caso contrário, abandonados. Esse valor será ignorado para um script específico se a chave KILL_AFTER_TIMEOUT estiver configurada no arquivo de propriedade de script.

CDP_MAXIMUM_ROW_COUNT_FOR_CPCI_DATA_RESPONSES
(padrão 1000) O valor global é incluído por motivos de desempenho para limitar o número máximo de linhas de saída retornado pelos scripts. Linhas extra após esse limite são ignoradas. Os valores permitidos são números inteiros positivos. Os valores inválidos são alterados para sem limite.

O fcp_daemon também suporta as outras variáveis de ambiente que são usadas para controlar agentes Agent Builder. Para obter uma lista completa, consulte a documentação oficial do Agent Builder aqui:

http://www-01.ibm.com/support/knowledgecenter/api/redirect/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/agentbuilder63_user.pdf

Parâmetros em arquivos de propriedade
É possível configurar os parâmetros para script customizado nos arquivos de propriedade.

O diretório KXX_FCP_SCRIPT_DEFINITIONS contém uma lista de arquivos *.properties. Cada arquivo de propriedade contém uma lista de scripts para execução com as respectivas propriedades em forma de `key=value`. As propriedades que podem ser definidas (sem distinção entre maiúsculas e minúsculas) são:

ATTRIBUTE_NAME

Obrigatório - sequência de no máximo 256 caracteres. Um nome escolhido por você que define um script específico e seus atributos. Os caracteres que podem ser usados para o nome `ATTRIBUTE NAME` podem ser alfanuméricos e somente o sublinhado pode ser utilizado como caractere especial. Se outros caracteres especiais (espaço ou em branco) forem usados, eles serão convertidos em sublinhado (_). Quando vários scripts são listados dentro do mesmo arquivo de propriedade, mais um `ATTRIBUTE_NAME` diferente deve ser definido (um para cada script). Esse deve ser o primeiro valor especificado para cada script definido e delimita o início do conjunto de propriedades para o script específico até o próximo `ATTRIBUTE_NAME`.

SCRIPT_PATH_WITH_PARMS
Obrigatório - sequência de no máximo 512 caracteres. Esse parâmetro define o caminho completo para o script com parâmetros, que são separados por um espaço em branco. Nenhum caractere especial pode ser usado no nome do caminho do script. Os valores contendo espaços em branco devem ser colocados entre aspas simples (') ou aspas duplas ("). Variáveis de ambiente podem ser transmitidas, mas só podem ser colocadas entre ${...} para todos os sistemas operacionais. As variáveis de ambiente devem estar disponíveis no contexto do processo do agente de S.O.

EXECUTION_FREQUENCY
Opcional - o valor padrão são 60 segundos. Esse parâmetro define a frequência de execução do script.

CUSTOM_NAME
Opcional - sequência de no máximo 256 caracteres. Esse parâmetro pode ser usado para uma descrição do script.

IS_ACTIVE
Opcional - true|false O valor padrão é true. Ele ativa o script. Se for false, o script não será executado.

DISABLE_USE_AGENT_SYNC
Opcional - true|false O valor padrão é false. Se for true, o `EXECUTION_FREQUENCY` do script será respeitado também se a variável global `KXX_FCP_SCRIPT_SYNC_INTERVALS` for configurada para `USE_AGENT`.

KILL_AFTER_TIMEOUT
Opcional - true|false O valor padrão é definido pela variável `CDP_DP_KILL_ORPHAN_SCRIPTS`. Quando true, o script é encerrado após o tempo limite. O tempo limite ocorre quando a execução do script é maior que o valor especificado pelo parâmetro `CDP_DP_SCRIPT_TIMEOUT` no arquivo de configuração do agente de S.O. Caso contrário, ela é ignorada. Em ambos os casos, nenhum dado é coletado. Observe que quando `KILL_AFTER_TIMEOUT` é configurado, somente o script definido no arquivo de propriedade é encerrado, e não os processos-filhos (se houver) criados pelo script. Esse recurso não é suportado pelos agentes de S.O. Solaris™ e Windows™ de 32 bits e nenhum script com tempo limite atingido é abandonado.

As linhas de saída que são retornadas por um script são analisadas.
O script retorna uma saída padrão (chamada de primeiro token). Quando o script retorna mais valores na linha de saída, eles são incluídos como mais tokens. No máximo cinco sequências, cinco números inteiros e cinco valores flutuantes seguem uma sintaxe predefinida.

OUTPUT_TYPE

STRING|INTEGER|FLOAT - Opcional - o valor padrão é sequência. Ele define o tipo do primeiro token retornado por cada linha do script; 0UTPUT_TYPE pode ser:

- STRING (padrãot) - sequências de até 2048 caracteres. Quando usado, o atributo "Standard_Output_String" de KXX_Custom_Scripts_Rtm_Smp é concluído pelo primeiro token.
- INTEGER - permite a obtenção de valores numéricos entre -9223372036854775806 e 9223372036854775806. Quando usado, o atributo "Standard_Output_Integer" do KXX_Custom_Scripts_Rtm_Smp é concluído pelo primeiro token.
- FLOAT - permite a obtenção de valores numéricos entre -92233720368547758.06 e 92233720368547758.06, com duas precisões decimais. Quando usado, o atributo "Standard_Output_Float" de KXX_Custom_Scripts_Rtm_Smp é concluído pelo primeiro token.

TOKEN_TYPES
STRING|INTEGER|FLOAT - Opcional - Define o tipo de saída de mais tokens após o primeiro. O usuário pode definir no máximo cinco sequências, cinco números inteiros e cinco valores flutuantes. É uma lista de tipos que são separados por vírgulas: <token_type>,<token_type>,... token_type pode ser vazio ou um destes (sem distinção entre maiúsculas e minúsculas):

- - STRING ou S
- - INTEGER ou I
- - FLOAT ou F
- Se *TOKEN_TYPES* estiver vazio, o token correspondente será ignorado.

  Exemplos dos mesmos layouts válidos:
- - TOKEN_TYPES=S,I,S,,,F,,F,F
- - TOKEN_TYPES=String,integer,S,,,Float,,f,FLOAT

TOKEN_LABELS
STRING - Opcional - Máximo de 16 caracteres cada rótulo. Define os rótulos dos tokens definidos em TOKEN_TYPES. Esse valor é uma lista de rótulos de token separados por vírgulas e deve corresponder aos tokens definidos por TOKEN_TYPES. Por exemplo:

- TOKEN_TYPES=S,I,S,,,F,,F,F
- TOKEN_LABELS=Cpu Name,Cpu number,Description,,,value 1,,value 2,value 3
- TOKEN_LABELS será ignorado se TOKEN_TYPES não estiver configurado.

TOKEN_SEPARATOR
Opcional - o ponto e vírgula padrão ";" configura a sequência a ser usada como um separador para dividir a linha de saída em tokens. Ele será ignorado se TOKEN_TYPES não estiver configurado. O valor vazio (em branco) é aceito como um separador e os espaços em branco múltiplos consecutivos nas linhas de saída são considerados um.

Os dois parâmetros a seguir permitem filtrar a saída de linhas de um script. Eles são aplicados pelo agente de S.O. somente ao primeiro token e devem ser usados juntos:

FILTER_VALUE
Opcional. O valor usado para comparação. Será obrigatório se FILTER_OPERATOR estiver definido. Se OUTPUT_TYPE for uma sequência, o valor do filtro deverá refletir exatamente o valor da sequência retornado pelo script que deve ser filtrado, sem quaisquer aspas adicionais (sem curingas permitidos).

FILTER_OPERATOR
Opcional. O operador usado para comparação. Obrigatório se FILTER_VALUE estiver definido. Os valores de FILTER_OPERATOR aceitos incluem:

- = (igual a)
- != (não igual a)
- > (maior que) somente para o tipo numérico
- >= (não menor que) somente para o tipo numérico
- < (menor que) somente para o tipo numérico
- <= (não maior que) somente para o tipo numérico

Exemplos de arquivo de propriedade
Exemplos de configuração de parâmetros nos arquivos de propriedade.

#Primeira definição de script: o script ex_script1.sh é iniciado a cada 150 segundos. Ele retorna valores flutuantes e somente as linhas de saída iguais a 0,5 são consideradas pelo agente.

```
ATTRIBUTE_NAME=sample1
SCRIPT_PATH_WITH_PARMS=/opt/ibm/apm/agent/localconfig/lz/scripts_definitions/ex_script1.sh
EXECUTION_FREQUENCY=150
OUTPUT_TYPE=FLOAT
FILTER_VALUE=0.5
FILTER_OPERATOR==
```

#Segunda definição de script: o script ex_script2 é iniciado a cada 60 segundos. Ele retorna valores de número inteiro e somente as linhas diferentes de 0 são consideradas pelo agente.

```
ATTRIBUTE_NAME=ex_script2
SCRIPT_PATH_WITH_PARMS=${CANDLE_HOME}/tmp/check_out.sh
EXECUTION_FREQUENCY=60
OUTPUT_TYPE=INTEGER
FILTER_VALUE=0
FILTER_OPERATOR=!=
```

#Terceira definição de script: o script ex_script3.sh é iniciado a cada 120 segundos com três parâmetros de entrada (o primeiro parâmetro de entrada é um número inteiro e o segundo e o terceiro são sequências). Ele será encerrado se for interrompido ou se o tempo de execução for maior que o valor do tempo limite.

```
ATTRIBUTE_NAME=ex_script3
SCRIPT_PATH_WITH_PARMS=/opt/scripts/ex_script3.sh 1 "second input parameter" "third input
parameter"
EXECUTION_FREQUENCY=120
OUTPUT_TYPE=STRING
KILL_AFTER_TIMEOUT=TRUE
```

#Quarta definição de script: o script cpu_mem_percentage.sh é iniciado a cada 50 segundos e retorna o cpuid como a sequência de saída padrão e dois valores flutuantes para a porcentagem de CPU Usada e Inativa e dois números inteiros para o uso de Memória e Memória Virtual. A barra vertical é usada como separador para analisar a saída. Um exemplo de linha que deve ser retornada pelo script é:

cpu2|35,5|65,5|3443|123800

```
ATTRIBUTE_NAME=cpu and mem Usage
SCRIPT_PATH_WITH_PARMS=${SCRIPT_HOME}/cpu_mem_percentage.sh
OUTPUT_TYPE=STRING
TOKEN_TYPES=F,F,I,I
TOKEN_LABELS= Idle CPU %, Used CPU %, Virt MEM used MB, MEM used MB
TOKEN_SEPARATOR=|
EXECUTION_FREQUENCY=50
```

Problemas e limitações conhecidos
Limitações e Problemas Conhecidos

- O Recurso de Script não é suportado em sistemas Windows™ 2003 de 64 bits.
- O encerramento após o tempo limite não funciona em agentes de S.O. Solaris™ e Windows™ de 32 bits.
- O fcp_daemon pode parar de executar scripts no Windows™ 32 bits se alguns scripts não forem concluídos dentro do período de tempo limite e o usuário ativou o rastreamento intensivo. Se o

fcp_daemon parar a execução dos scripts, os dados relatados no console refletirão a última vez que o script foi executado. Também é possível que o agente de S.O. pare de retornar dados. A interrupção do processo fcp_daemon permite que o agente retome a operação adequada.

- SCRIPT_NONZERO_RETURN é retornado no lugar de SCRIPT_NOT_FOUND or SCRIPT_LAUNCH_ERROR no Solaris™.
- O recurso de script não fornece globalização integral; alguns problemas podem ser encontrados no uso de caracteres nacionalizados em arquivos de propriedade ou saídas de script.
- No agente de S.O. Windows™, não há possibilidade de executar scripts que residem em uma unidade de rede mapeada.
- Quando o agente de S.O. Windows™ é atualizado, o recurso de script não é ativado por padrão. Edite KNTENV e mude `KNT_FCP_SCRIPT=FALSE` para `KNT_FCP_SCRIPT=TRUE`

Resolução de problemas de script customizado
Resolução de problemas de script customizado

A variável *KBB_RAS1* padrão se aplica ao agente de S.O. e aos processos fcp_daemon. Para aplicar uma configuração de rastreio específica somente ao fcp_daemon, use a variável *KXX_FCP_KBB_RAS1*; quando *KXX_FCP_KBB_RAS1* for configurado, o valor especificado por *KBB_RAS1* será ignorado pelo fcp_daemon.

Para rastrear as operações registradas pelos encadeamentos principais do agente de S.O. do recurso:

```
KBB_RAS1=ERROR (UNIT:factory ALL)
```

Para rastrear as consultas de script do servidor APM e os eventos enviados para o servidor, inclua as entradas:

No Monitoring Agent for Linux OS

```
(UNIT:klz34 ALL) (UNIT:klz36 ALL)
```

No Monitoring Agent for UNIX OS

```
(UNIT:kux48 ALL) (UNIT:kux50 ALL)
```

No Monitoring Agent for Windows OS

```
(UNIT:knt84 ALL) (UNIT:knt86 ALL)
```

Para visualizar os rastreios do TEMA para verificar a execução de uma situação particular, inclua as entradas:

```
(UNIT:kraavp all) (UNIT:kraapv all)
```

Para ver a execução dos scripts e como os dados dos scripts estão sendo analisados, configure:

```
KXX_FCP_KBB_RAS1=Error (UNIT:command ALL)
```

Para solucionar problemas na comunicação entre o agente e o fcp_daemon, inclua esse nível de rastreio em *KBB_RAS1* e *KXX_FCP_KBB_RAS1*:

```
(UNIT:cps_socket FLOW) (UNIT:cpci FLOW)
```

Para ver a interação entre o agente de S.O. e o fcp_daemon com detalhes, inclua em *KBB_RAS1* e *KXX_FCP_KBB_RAS1*:

```
(UNIT:cps_socket ALL) (UNIT:cpci ALL)
```

Cenário de iniciação rápida
Esta seção descreve as etapas mínimas necessárias para configurar um script customizado para um cenário de exemplo.

A seção a seguir descreve as etapas mínimas necessárias para configurar o Monitoring Agent for Linux OS para executar dois scripts customizados.

Descrições de scripts customizados

Neste exemplo, o usuário possui dois scripts sob um diretório /scripts_repo:

checkDIRsize.sh – Este script verifica o tamanho de um diretório especificado transmitido como um parâmetro de entrada. A saída é um número inteiro, como: `4594740`

cpu_mem_usage.sh – Este script verifica a porcentagem de CPU utilizada e os megabytes de Memória de Troca utilizados. A saída é retornada no formato: `cpu1|96,5|23800`

Em que o primeiro token é o ID da CPU, o segundo token é a porcentagem de CPU utilizada e o terceiro token é a memória de troca utilizada em megabytes.

A customização precisa que o Monitoring Agent for Linux OS execute esses scripts.

O recurso é ativado com valores padrão assim que o agente de S.O. é iniciado:

Crie os arquivos de propriedade `AnyName.properties` sob o diretório padrão `install dir/localconfig/lz/scripts_definitions`. Neste exemplo, crie dois arquivos de propriedade, um para cada script denominado checkDIRsize.properties e cpu_mem_usage.properties:

```
#CheckDIRsize.properties
ATTRIBUTE_NAME=OPT_DIR_SIZE
SCRIPT_PATH_WITH_PARMS=/scripts_repo/checkDIRsize.sh /opt
EXECUTION_FREQUENCY=20
OUTPUT_TYPE=INTEGER
```

```
#cpu_mem_usage.properties
ATTRIBUTE_NAME=cpu_mem_usage
SCRIPT_PATH_WITH_PARMS=/scripts_repo/cpu_mem_percentage.sh
OUTPUT_TYPE=string
TOKEN_TYPES=F,I
TOKEN_LABELS= Used CPU %, Swap MEM used MB
TOKEN_SEPARATOR=|
EXECUTION_FREQUENCY=10
```

Não é necessário reiniciar o agente de S.O. após você incluir (ou alterar) os dois arquivos de propriedade. O agente de S.O. verifica o diretório de definição de script com um intervalo de tempo especificado (valor padrão de 300 segundos). Abra o console e, sob a área de trabalho "Scripts Customizados", os detalhes e os resultados dos scripts são mostrados.

Configurando a coleta de dados do sistema de arquivos do Linux OS Agent

O Monitoring Agent for Linux OS é configurado automaticamente. No entanto, é possível configurar o comportamento para a coleta de dados do sistema de arquivos.

O Monitoring Agent for Linux OS tem o comportamento padrão para coleta de dados do sistema de arquivos.

O comportamento padrão é monitorar sistemas de arquivos somente de `/etc/fstab`. Uma variável de ambiente *KBB_SHOW_MTAB_FS* é definida no arquivo `lz.environment` para controlar o comportamento da coleta de dados do sistema de arquivos. Se desejar monitorar todos os sistemas de arquivos (listados em `/etc/fstab` e `/etc/mtab`), é possível configurar KBB_SHOW_MTAB_FS=true.

KBB_SHOW_MTAB_FS

Esta variável está disponível no arquivo *`install_dir`*`/config/`*`.lz`*`.environment`. O valor padrão é `false` e define o agente para monitorar sistemas de arquivos somente a partir do `/etc/fstab`. Se desejar monitorar todos os sistemas de arquivos (listados em `/etc/fstab` e `/etc/mtab`), mude o valor para `true`. Por exemplo, *KBB_SHOW_MTAB_FS=true*.

Configurando o monitoramento do PHP

Configure o Monitoring Agent for PHP para que o agente possa coletar dados do aplicativo PHP que está sendo monitorado.

Antes de Iniciar

1. Assegure-se de instalar o pacote php-process. Se você usar o comando `yum install` para instalar o PHP, execute o comando `yum install php-process` para instalar o pacote php-process.
2. Assegure-se de que o servidor Apache HTTPD seja iniciado antes de você configurar o agente.

   Abra o arquivo de configuração `httpd.conf` do Servidor HTTP Apache e assegure-se de que as opções `mod_status` e `ExtendedStatus On` estejam ativadas. Por exemplo:

   ```
   ExtendedStatus On
   <Location /server-status>
           SetHandler server-status
           Order deny,allow
           Allow from all
           Allow from 127.0.0.1
   </Location>
   ```

   No exemplo fornecido, para que o agente funcione corretamente, o `http://127.0.0.1/server-status` deve funcionar corretamente.

   Nota: Deve-se ter Lynx ou Links instalados no Linux para o agente para obter dados de monitoramento.

   Certifique-se de que o comando `apachectl status` funcione adequadamente no servidor Apache monitorado, sem mudanças de código no comando `apachectl`. Para que o comando `apachectl status` funcione corretamente, o Lynx deve estar instalado.

Sobre Esta Tarefa

Para evitar problemas de permissão ao configurar o agente, certifique-se de utilizar o mesmo ID de usuário raiz ou de usuário não raiz que foi utilizado para instalar o agente. Se você instalou o seu agente como um usuário selecionado e deseja configurar o agente como um usuário diferente, consulte "Configurando agentes como um usuário não raiz" na página 181. Se você instalou e configurou seu agente como um usuário selecionado e deseja iniciar o agente como um usuário diferente, consulte "Iniciando agentes como um usuário não raiz" na página 1012.

O Agente PHP é um agente de múltiplas instâncias; você deve criar a primeira instância e iniciar o agente manualmente. O Nome do sistema gerenciado inclui o nome da instância que você especifica, por exemplo, *instance_name*:*host_name*:*pc*, em que *pc* é seu código de produto de dois caracteres. O Nome do sistema gerenciado é limitado a 32 caracteres. O nome da instância que você especifica é limitado a 28 caracteres, menos o comprimento do nome do host. Por exemplo, se você especificar PHP2 como o nome da instância, o nome do sistema gerenciado será PHP2:`hostname`:PJ.

Importante: Se você especificar um longo nome de instância, o nome do Sistema gerenciado é truncado e o código do agente não é exibido corretamente.

Procedimento

- Se o seu ambiente for igual às configurações padrão, é possível usar o caminho binário de execução padrão, o caminho do arquivo `php.ini` padrão e a porta padrão para configurar o agente:

  a) Insira:
  install_dir`/bin/php-agent.sh config` *instance_name* *install_dir*`/samples/php_silent_config.txt`
  Em que *instance_name* é o nome a ser atribuído para a instância e *install_dir* é o diretório de instalação do Agente PHP. O diretório de instalação padrão é `/opt/ibm/apm/agent`.

  b) Para iniciar o agente, insira:

install_dir/bin/php-agent.sh start *instance_name*

- Para configurar o agente ao editar o arquivo de resposta silenciosa e executar o script sem nenhuma interação, conclua as seguintes etapas:
  a) Abra *install_dir*/samples/php_silent_config.txt em um editor de texto.
  b) Para **Location of PHP execution binary**, você pode especificar o diretório no qual a execução de PHP está localizada. O local padrão é /usr/local/bin.
  c) Para **Location of PHP INI file**, é possível especificar o diretório em que o arquivo php.ini está localizado. O local padrão é /etc..
  d) Para **Web server port**, você pode especificar o número da porta do servidor da web que está executando o WordPress. O padrão é 80.
  e) Para **Application DocumentRoot**, você pode especificar o DocumentRoot do aplicativo PHP WordPress. Use dois pontos para separar vários registros. Para permitir que o agente localize todos os registros para você, use o valor padrão de ALL.
  f) Salve e feche o arquivo php_silent_config.txt e, em seguida, insira:
  install_dir/bin/php-agent.sh config *instance_name install_dir*/samples/php_silent_config.txt
  Em que *instance_name* é o nome a ser atribuído para a instância e *install_dir* é o diretório de instalação do Agente PHP. O diretório de instalação padrão é /opt/ibm/apm/agent.
  g) Para iniciar o agente, insira:
  install_dir/bin/php-agent.sh start *instance_name*
- Para configurar o agente executando o script e respondendo aos prompts, conclua as seguintes etapas:
  a) Insira:
  install_dir/bin/php-agent.sh config *instance_name*
  Em que *instance_name* é o nome a ser atribuído para a instância e *install_dir* é o diretório de instalação do Agente PHP.
  b) Quando for solicitado Editar Agente de Monitoramento para configurações PHP , insira 1 para continuar.
  c) Quando for solicitado Localização da execução binária do PHP, pressione Enter para aceitar o local padrão ou especificar seu próprio local.
  d) Quando for solicitado Localização do arquivo INI do PHP, pressione Enter para aceitar o local padrão ou especificar seu próprio local.
  e) Quando for solicitado Porta do Servidor da Web, pressione Enter para aceitar a porta padrão ou especifique um número de porta diferente.
  f) Quando for solicitado para DocumentRoot do Aplicativo, pressione Enter para aceitar o padrão ou especifique o DocumentRoot do aplicativo PHP WordPress. Você pode usar dois pontos para separar vários registros.
  g) Para iniciar o agente, insira:
  install_dir/bin/php-agent.sh start *instance_name*

Resultados
O agente avalia somente o desempenho de solicitações PHP em aplicativos WordPress. Carregamento CSS e JS não são avaliados. O agente não usa argumentos de URL para identificar URLs.

O que Fazer Depois

É possível verificar os dados Agente PHP que são exibidos no Console do Cloud APM.

Você deve assegurar que o plug-in do WordPress para o agente está ativado. Para assegurar-se da ativação, conclua as seguintes etapas:

1. Em um navegador da web, insira a seguinte URL http://*hostname*:*port*/wp-admin/.
2. Acesse a página administrativa navegando para **Plugins** > **Plugins Instalados**.

3. Assegure-se de que o plug-in Agente PHP esteja ativado. O plug-in Agente PHP é listado como **WordPress Agent**. Geralmente, o plug-in já está ativado. Se ainda não estiver ativado, clique em **Ativar**.

Configurando o monitoramento do PostgreSQL

Configure o Monitoring Agent for PostgreSQL para que o agente possa coletar dados do banco de dados PostgreSQL que está sendo monitorado.

Antes de Iniciar

Você deve instalar o driver JDBC do PostgreSQL antes de instalar esse agente. O caminho para esse driver é necessário no momento da configuração do agente.

O driver JDBC tipo 4 é a nova versão e, portanto, a preferencial. O usuário pode instalar a versão 4 do subtipo JDBC de acordo com a versão JDK que o agente usa. Para o mapeamento da versão do JDBC para a versão do JDK, obtenha informações adicionais em https://jdbc.postgresql.org/download.html.

Alguns dos atributos coletados pelo agente dependem da extensão `pg_stat_statements`. Para incluir `pg_stat_statements`, primeiramente instale o pacote `postgresql-contrib`. Deve-se modificar o arquivo de configuração `postgresql.conf` para que o servidor PostgreSQL carregue a extensão `pg_stat_statements`.

1. Abra o arquivo `postgresql.conf` em um editor de texto e atualize a linha `shared_preload_libraries`:

   ```
   shared_preload_libraries = 'pg_stat_statements'
   pg_stat_statements.track_utility = false
   ```

   Essas mudanças são necessárias para monitorar as instruções SQL, exceto os comandos do utilitário.

   Nota: O status de `pg_stat_statements.track_utility` é configurado ou modificado somente por um superusuário.
2. Reinicie o servidor PostgreSQL depois de atualizar e salvar o `postgresql.conf`.
3. Execute o comando SQL a seguir usando psql, que deve ser conectado ao mesmo banco de dados que seria fornecido posteriormente na configuração do agente para conectividade JDBC:

   ```
   create extension pg_stat_statements;
   select pg_stat_statements_reset();
   ```

   Nota: O comando `create extension` e a função `pg_stat_statements_reset()` são executados somente por um superusuário.

   A visualização `pg_stat_statements` precisa ser ativada para o banco de dados específico, para obter mais detalhes, consulte https://www.postgresql.org/docs/9.6/static/pgstatstatements.html.

O arquivo `pg_hba.conf` é o arquivo de banco de dados PostgreSQL que contém configurações de autenticação. Quando o valor de parâmetro `auth-method` for configurado como `ident` no arquivo `pg_hba.conf`, o Agente PostgreSQL não poderá se conectar ao banco de dados PostgreSQL. Assegure que as configurações de autenticação para o parâmetro `auth-method` estejam corretas. Por exemplo, é possível configurar esses valores para o parâmetro `auth-method`: `md5`, `trust` ou `password`.

Revise os pré-requisitos de hardware e de software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Agente PostgreSQL.

Sobre Esta Tarefa

O Agente PostgreSQL é um agente de múltiplas instâncias; você deve criar a primeira instância e iniciar o agente manualmente. O nome do sistema gerenciado inclui o nome da instância especificada, por exemplo *instance_name*:*host_name*:*pc*, em que *pc* é o código de produto de dois caracteres. O nome do sistema gerenciado é limitado a 32 caracteres. O nome da instância que você especifica é limitado a

28 caracteres, menos o comprimento do nome do host. Por exemplo, se você especificar `PostgreSQL2` como o seu nome da instância, o nome do sistema gerenciado será `PostgreSQL2:hostname:PN`.

Importante: Se você especificar um nome de instância longo, o nome do sistema gerenciado será truncado e o código do agente não será exibido completamente.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte o "Histórico de Mudanças" na página 50.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o agente nos sistemas Windows

Você pode utilizar o Use a janela do IBM Cloud Application Performance Management para configurar o agente nos sistemas Windows.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito em **Monitoring Agent for PostgreSQL** e, em seguida, clique em **Configurar agente**.
3. No campo **Inserir um nome de instância exclusivo**, digite o nome de instância do agente e clique em **OK**.
4. Na janela **Monitoring Agent for PostgreSQL**, conclua essas etapas:
   a. No campo **Endereço IP**, insira o endereço IP de um servidor PostgreSQL que você deseja monitorar remotamente. Se o agente estiver instalado no servidor a ser monitorado, retenha o valor padrão.

      Nota:

      Para o monitoramento remoto, os dados para **CPU atual usada (%)** e **Memória física usada (MB)** não estarão disponíveis no painel. Esses widgets mostrarão **N/A** .
   b. No campo **Nome do banco de dados JDBC**, insira um nome do banco de dados para mudar o nome do banco de dados padrão de `postgres`.
   c. No campo **Nome do usuário JDBC**, insira um nome do usuário para mudar o nome padrão de `postgres`.
   d. No campo **Senha JDBC**, insira a senha de usuário JDBC.
   e. No campo **Confirmar senha JDBC**, insira novamente a senha.
   f. No campo **Número da porta JDBC**, insira um número da porta para mudar o número da porta padrão de 5432.
   g. No campo **Arquivo JAR JDBC**, insira o caminho para o conector PostgreSQL para o arquivo JAR Java e clique em **Avançar**.
   h. No campo **Nível de rastreio Java**, insira o nível de rastreio de acordo com as instruções do suporte IBM. O nível de rastreio padrão é `Erro`.
   i. Clique em **OK**. A instância de agente é exibida na janela IBM Performance Management.
5. Clicar com o botão direito na instância **Monitoring Agent for PostgreSQL** e clique em **Iniciar**.

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o console, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Configurando o agente nos sistemas Linux

Para configurar o agente em sistemas operacionais Linux, você deve executar o script e responder aos prompts.

Procedimento

1. Na linha de comandos, digite o seguinte comando:
   install_dir/bin/postgresql-agent.sh config *instance_name*
2. Quando for solicitado para editar o agente para as configurações do PostgreSQL, insira 1 para continuar.
3. Quando for solicitado para inserir um valor para os parâmetros a seguir, pressione Enter para aceitar o valor padrão ou especifique um valor diferente e pressione Enter:
   - Endereço IP

     Nota:

     Insira o endereço IP de um servidor PostgreSQL que você deseja monitorar remotamente. Se o agente estiver instalado no servidor a ser monitorado, retenha o valor padrão.

     Para o monitoramento remoto, os dados para **CPU atual usada (%)** e **Memória física usada (MB)** não estarão disponíveis no painel. Esses widgets mostrarão **N/A** .
   - nome do banco de dados JDBC
   - nome de usuário JDBC
   - senha JDBC
   - número da porta JDBC
   - arquivo JAR JDBC

   Importante: A versão do arquivo JAR JDBC deve ser igual à versão do banco de dados PostgreSQL que está sendo monitorado.
4. Quando for solicitado para inserir um valor para o parâmetro `Java trace level`, insira 2 para aceitar o valor padrão ou especifique o nível de rastreio de acordo com as instruções de suporte IBM.
5. Execute o comando a seguir para iniciar o agente:

```
install_dir/bin/postgresql-agent.sh
start instance_name
```

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Configurando o agente usando o arquivo silencioso de resposta

O arquivo silencioso de resposta contém os parâmetros de configuração do agente. É possível editar o arquivo silencioso de resposta para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa
É possível usar o arquivo silencioso de resposta para configurar o Agente PostgreSQL em sistemas Linux e Windows. Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

- Para configurar o agente editando o arquivo de resposta silencioso e executando o script sem responder aos prompts, conclua as etapas a seguir:
  1. Em um editor de texto, abra o arquivo de resposta silencioso que está disponível neste caminho: *install_dir*/samples/postgresql_silent_config.txt em que *install_dir* é o diretório de instalação do Agente PostgreSQL. O diretório de instalação padrão é /opt/ibm/apm/agent.
  2. Para editar o arquivo de configuração silencioso, conclua as etapas a seguir:
     a. Para o parâmetro **IP Address**, especifique o endereço IP de um servidor PostgreSQL que você deseja monitorar remotamente. Se o agente estiver instalado no servidor a ser monitorado, retenha o valor padrão.

        Nota:

        Para o monitoramento remoto, os dados para **CPU atual usada (%)** e **Memória física usada (MB)** não estarão disponíveis no painel. Esses widgets mostrarão **N/A** .
     b. Para o parâmetro **JDBC database name**, especifique um nome do banco de dados para mudar o nome do banco de dados padrão de postgres.
     c. Para o parâmetro **JDBC user name**, especifique um nome de usuário para mudar o nome padrão de postgres.
     d. Para o parâmetro **JDBC password**, insira a senha de usuário JDBC.
     e. Para o parâmetro **JDBC port number**, especifique um número de porta para mudar o número da porta padrão de 5432.
     f. Para o parâmetro **JDBC JAR file**, especifique o caminho para o conector PostgreSQL para o arquivo JAR Java se o caminho padrão estiver incorreto. O caminho padrão do arquivo JAR Java é:

        /opt/PostgreSQL/lib/postgresql-9.3-1100.jdbc4.jar

        Importante: A versão do arquivo JDBC JAR deve ser compatível com a versão do banco de dados PostgreSQL que está sendo monitorado.
     g. Para o parâmetro **Java trace level**, especifique o nível de rastreio de acordo com as instruções de suporte IBM. O nível de rastreio padrão é Erro.
  3. Salve e feche o arquivo de resposta silencioso e execute o comando a seguir:

     ```
     install_dir/bin/postgresql-agent.sh config
     instance_name
     install_dir/samples/postgresql_silent_config.txt
     ```

     Em que *instance_name* é o nome que você deseja fornecer para a instância.
  4. Para iniciar o agente, digite o seguinte comando:

     ```
     install_dir/bin/postgresql-agent.sh
     start instance_name
     ```

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Configurando o monitoramento de Python

Os aplicativos IBM Cloud Python e no local podem ser monitorados. Conclua as etapas de configuração correspondentes com base no tipo de aplicativo.

Sobre Esta Tarefa

Configure o Coletor de dados do Python para monitorar seus aplicativos IBM Cloud Python e no local.

Procedimento

- Configure o coletor de dados para monitorar os aplicativos IBM Cloud.
  a) Configure o coletor de dados Python para coletar e enviar dados para aplicativos IBM Cloud. Para obter instruções, veja “Configurando o coletor de dados Python para aplicativos IBM Cloud” na página 671.
  b) Opcional: Customize os recursos de monitoramento do Coletor de dados do Python. Para obter mais informações, consulte “Customizando os aplicativos Coletor de dados do Python para IBM Cloud” na página 672.
- Configure o coletor de dados para monitorar aplicativos no local.
  a) Configure o coletor de dados para coletar e enviar dados para o Servidor Cloud APM. Para obter instruções, veja “Configurando o Coletor de dados do Python para aplicativos no local” na página 677.
  b) Opcional: Customize os recursos de monitoramento do Coletor de dados do Python. Para obter mais informações, consulte “Customizando o Coletor de dados do Python para aplicativos no local” na página 678.

Configurando o coletor de dados Python para aplicativos IBM Cloud

Para coletar informações sobre aplicativos Python no IBM Cloud, deve-se configurar o coletor de dados Python.

Antes de Iniciar

1. Certifique-se de que os aplicativos Python que você deseja monitorar tenham nomes exclusivos. O Coletor de dados do Python manipula dois aplicativos diferentes com o mesmo nome de um aplicativo, o que pode fazer com que os dados exibam problemas no Console do Cloud APM.
2. Faça download do pacote coletor de dados no website do IBM Marketplace. Para obter instruções detalhadas, consulte “Fazendo download de seus agentes e coletores de dados” na página 101.

Sobre Esta Tarefa

Para configurar o coletor de dados, primeiro você implementa um servidor de pacote pypi e, em seguida, instala o coletor de dados para um aplicativo Python Django.

Procedimento

1. Extraia os arquivos do pacote do coletor de dados. O pacote `python_datacollector_8.1.4.0.tgz` é incluído no diretório extraído.
2. Extraia o pacote `python_datacollector_8.1.4.0.tgz`, por exemplo, executando o seguinte comando:

   ```
   tar -zxf python_datacollector_8.1.4.0.tgz
   ```

3. Localize o arquivo `manifest.yml` do servidor de pacote no diretório extraído e defina o domínio, o host e o nome nesse arquivo, conforme mostrado no exemplo a seguir:

```
domain: mybluemix.net
name: pythondc
host: pythondc
```

Lembre-se: Os valores *host* e *name* devem ser iguais e exclusivos.

4. No diretório `python_dc`, envie por push o aplicativo `pythondc` para o IBM Cloud executando o comando a seguir:

```
cf push
```

5. No arquivo `requirements.txt` de seu aplicativo Python, inclua as seguintes linhas:

```
cryptography==1.9.0
--extra-index-url https://<your_host_name_and_domain>/python-dc-repos/simple/
ibm_python_dc
```

6. No arquivo `settings.py` do aplicativo Python, inclua `ibm_python_dc.kpg_plugin.ResourceMiddleware` no início da seção `MIDDLEWARE_CLASSES`, por exemplo:

```
MIDDLEWARE_CLASSES = (
    "ibm_python_dc.kpg_plugin.ResourceMiddleware",
    "mezzanine.core.middleware.UpdateCacheMiddleware",
    'django.contrib.sessions.middleware.SessionMiddleware',
    'django.middleware.common.CommonMiddleware',
```

7. No diretório que contém o arquivo `manifest.yml` do aplicativo Python, execute o seguinte comando:

```
cf push
```

Dica: Para obter um arquivo `manifest.yml` de amostra, consulte "Arquivo manifest.yml de amostra" na página 186.

Resultados
O coletor de dados é configurado e está conectado ao Servidor Cloud APM.

O que Fazer Depois

É possível verificar se os dados de monitoramento de seu aplicativo IBM Cloud são exibidos no Console do Cloud APM. Para obter instruções sobre como iniciar o Console do Cloud APM, consulte Iniciando o console do Cloud APM. Para obter informações sobre o uso do Editor de aplicativos, consulte Gerenciando aplicativos.

Customizando os aplicativos Coletor de dados do Python para IBM Cloud
É possível incluir variáveis de ambiente na interface com o usuário (IU) do IBM Cloud para customizar o monitoramento de seu aplicativo IBM Cloud. Use as seguintes informações para incluir as variáveis de acordo com suas necessidades.

Variáveis de ambiente definidas pelo usuário para o Coletor de dados do Python

É possível usar as informações na tabela a seguir para customizar o monitoramento do Python no IBM Cloud.

Tabela 192. Variáveis de ambiente definidas pelo usuário suportadas para monitoramento do Python no IBM Cloud

Nome de variável	Importância	Valor	Descrição
APM_BM_GATEWAY_URL	Opcional	• https://*<server ip or hostname>*:443 • http://*<server ip or hostname>*:80	A URL de gateway do servidor no local de destino.

Tabela 192. Variáveis de ambiente definidas pelo usuário suportadas para monitoramento do Python no IBM Cloud (continuação)

Nome de variável	Importância	Valor	Descrição
APM_KEYFILE_PSWD	Opcional	Senha criptografada do arquivo-chave	A senha do arquivo-chave criptografado que é pareada com o arquivo-chave. Caso seja um usuário do Linux, você poderá usar o comando `echo -n <keyfile password> | base64` para criptografar sua senha. **Nota:** Configure essa variável somente quando tiver configurado o Gateway para usar HTTPS.
APM_KEYFILE_URL	Opcional	http://*<hosted http server>*:*<port>*/keyfile.p12	A URL para fazer download do arquivo-chave. **Nota:** Configure essa variável somente quando tiver configurado o Gateway para usar HTTPS.
KPG_ENABLE_DEEPDIVE	Opcional	• False • Verdadeiro	Ativa ou desativa a coleta de dados diagnósticos. • True: o valor padrão. Se você configurar essa variável como `True`, os dados diagnósticos serão coletados. • False: se você configurar essa variável como `False`, os dados diagnósticos não serão coletados. Se você não configurar essa variável, os dados diagnósticos serão coletados.
KPG_DD_CONFIG_FILE	Opcional	Nome do arquivo de configuração de monitoramento de diagnósticos.	Nome do arquivo de configuração de monitoramento de diagnósticos. O nome padrão do arquivo é `kpg_dd_config.xml`. **Nota:** Após customizar as configurações nesse arquivo, ele deverá ser colocado no diretório-raiz do aplicativo. Se você não configurar essa variável, o arquivo de configuração padrão `kpg_dd_config.xml` no pacote coletor de dados será usado.

Tabela 192. Variáveis de ambiente definidas pelo usuário suportadas para monitoramento do Python no IBM Cloud (continuação)

Nome de variável	Importância	Valor	Descrição
KPG_DD_APP_PATH	Opcional	Caminho para o aplicativo Python.	O caminho para o aplicativo Python ou o módulo para o qual o coletor de dados coleta dados de diagnósticos. Separe os caminhos de diferentes aplicativos e módulos Python que deseja monitorar com um ponto-e-vírgula `;`. Se você não configurar essa variável, o coletor de dados coletará dados para solicitações e os módulos usados por seu aplicativo. Os dados de solicitações na lib Python não são coletados.
KPG_DD_SECURITY_FILTER	Opcional	• Verdadeiro • False	• True: o valor padrão. Se você configurar essa variável como `True`, os valores (como as senhas) serão mascarados em instruções SQL e os parâmetros não serão exibidos no widget de grupo **Contexto de solicitação**. • False: se você configurar essa variável como `False`, os valores em instruções SQL não serão mascarados e os parâmetros serão exibidos no widget de grupo **Contexto de solicitação**. Se você não configurar essa variável, os valores (como as senhas) serão mascarados em instruções SQL e os parâmetros não serão exibidos no widget de grupo **Contexto de solicitação**.

Tabela 192. Variáveis de ambiente definidas pelo usuário suportadas para monitoramento do Python no IBM Cloud (continuação)

Nome de variável	Importância	Valor	Descrição
KPG_GC_STATS	Opcional	Verdadeiro	Todas as funções estatísticas da coleta de lixo do Python são ativadas. Configurar esse valor como `True` equivale à execução do comando a seguir: `gc.set_debug(gc.DEBUG_STATS | gc.DEBUG_COLLECTABLE | gc.DEBUG_UNCOLLECTABLE | gc.DEBUG_INSTANCES | gc.DEBUG_OBJECTS )` Para desativar KPG_GC_STATS, exclua essa variável de ambiente. Não configure-a como `False`. **Nota:** Nunca configure `KPG_SAVE_ALL=True` em seu ambiente de produção formal. É somente para o modo de depuração. Assegure-se de que haja memória suficiente designada ao aplicativo.
KPG_LOG_LEVEL	Opcional	• DEBUG • ERROR • INFO	• DEBUG: somente informações úteis sobre depuração são impressas no log, por exemplo, dados coletados, dados que são enviados para o servidor e resposta do servidor. • ERROR: somente informações sobre exceções e situações inesperadas são impressas no log. • INFO: as informações de resumo sobre o coletor de dados para o usuário saber o que ele está fazendo são impressas no log.
KPG_LOG_TOCONSOLE	Opcional	• S • Verdadeiro • Qualquer outro valor que não seja `False`	O log é impresso no console e é possível ver o log executando o comando **`cf logs <appname>`**.

Tabela 192. Variáveis de ambiente definidas pelo usuário suportadas para monitoramento do Python no IBM Cloud (continuação)

Nome de variável	Importância	Valor	Descrição
KPG_SAVE_ALL	Opcional	Verdadeiro	Todos os objetos sem referência são salvos em `gc.garbage`, e é preciso limpar `gc.garbage` a cada minuto (o coletor de dados faz a limpeza). Configurar esse valor como `True` equivale à execução do comando a seguir: `gc.set_debug(gc.SAVE_ALL)` Para desativar KPG_SAVE_ALL, exclua essa variável de ambiente. Não configure-a como `False`. **Nota:** Nunca configure `KPG_SAVE_ALL=True` em seu ambiente de produção formal. É somente para o modo de depuração. Assegure-se de que haja memória suficiente designada ao aplicativo.

Desconfigurando o Coletor de dados do Python para aplicativos IBM Cloud
Se você não precisa monitorar seu ambiente do Python ou se deseja fazer upgrade do Coletor de dados do Python, deve-se primeiro desconfigurar configurações anteriores para o Coletor de dados do Python.

Procedimento

1. Acesse o diretório inicial de seu aplicativo Python.
2. Remova as seguintes linhas do arquivo `requirements.txt` para o aplicativo:

```
--extra-index-url https://<your_host_name_and_domain>/python_dc/static/python-dc-repos/
simple/
ibm-python-dc
```

3. No arquivo `settings.py`, remova a linha a seguir da seção `MIDDLEWARE_CLASSES`:

```
ibm_python_dc.kpg_plugin.ResourceMiddleware
```

4. Execute o seguinte comando para enviar por push novamente o aplicativo para que as mudanças entrem em vigor:

```
cf push
```

Resultados
Você desconfigurou o Coletor de dados do Python com sucesso.

O que Fazer Depois
Depois de desconfigurar o coletor de dados, o Console do Cloud APM continua a exibir o coletor de dados em quaisquer aplicativos nos quais você incluiu o coletor de dados. O Console do Cloud APM mostrará que nenhum dado está disponível para o aplicativo e não indicará que o coletor de dados está off-line. Para obter informações sobre como remover o coletor de dados de aplicativos e de grupos de recursos, consulte "Removendo coletores de dados do Console do Cloud APM" na página 186.

Configurando o Coletor de dados do Python para aplicativos no local

Para coletar informações sobre aplicativos Python que são executados em seu ambiente local, deve-se configurar o Coletor de dados do Python.

Antes de Iniciar

1. Certifique-se de que os aplicativos Python que você deseja monitorar tenham nomes exclusivos. O Coletor de dados do Python manipula dois aplicativos diferentes com o mesmo nome de um aplicativo, o que pode fazer com que os dados exibam problemas no Console do Cloud APM.
2. Faça download do pacote coletor de dados no website do IBM Marketplace. Para obter instruções detalhadas, consulte “Fazendo download de seus agentes e coletores de dados” na página 101.

Sobre Esta Tarefa

O pacote do coletor de dados é um pacote pré-configurado com arquivo `global.environment` pré-configurado e um `keyfile.p12` que é copiado para a pasta `etc`. Como resultado, o coletor de dados se conecta automaticamente ao Servidor Cloud APM.

O procedimento a seguir configura o coletor de dados no aplicativo Python com configurações padrão. Para customizar a configuração do coletor de dados, use as variáveis de ambiente nos arquivos de configuração do coletor de dados. Para obter mais informações, consulte “Customizando o Coletor de dados do Python para aplicativos no local” na página 678.

Procedimento

1. Extraia os arquivos do pacote do coletor de dados. O pacote `python_datacollector_8.1.4.0.tgz` é incluído no diretório extraído.
2. Extraia arquivos do pacote coletor de dados, por exemplo, executando o seguinte comando:

   ```
   tar -zxf python_datacollector_8.1.4.0.tgz
   ```

3. A partir do diretório `python_dc`, execute o comando a seguir:

   ```
   python server.py
   ```

4. Execute o seguinte comando:

   ```
   pip install ibm_python_dc --extra-index-url http://host name or ip:8000/
   python-dc-repos/simple/ --trusted-host host name or ip
   ```

   em que *host name or ip* é o nome ou endereço IP do host para executar o repositório do coletor de dados Python.

   Importante: Use o nome ou o endereço IP para especificar o host para a URL e o host confiável neste comando. Por exemplo, se você especificar o host usando o endereço IP e o endereço IP for `9.42.36.180`, o comando será semelhante ao seguinte:

   ```
   pip install ibm_python_dc --extra-index-url http://9.42.36.180:8000/
   python-dc-repos/simple/ --trusted-host 9.42.36.180
   ```

5. No arquivo `settings.py` do aplicativo Python, inclua `ibm_python_dc.kpg_plugin.ResourceMiddleware` na seção `MIDDLEWARE_CLASSES` no formato do seguinte exemplo:

   ```
   MIDDLEWARE_CLASSES = (
       "ibm_python_dc.kpg_plugin.ResourceMiddleware",
       "mezzanine.core.middleware.UpdateCacheMiddleware",
       'django.contrib.sessions.middleware.SessionMiddleware',
       'django.middleware.common.CommonMiddleware',
   ```

Resultados

O coletor de dados é definido com as configurações padrão e conectado ao Servidor Cloud APM.

O que Fazer Depois
Agora é possível efetuar login no Servidor Cloud APM para visualizar os dados de monitoramento.

Lembre-se: Depois de incluir seu aplicativo Python no Console do Cloud APM, será possível visualizar seus dados de monitoramento no componente chamado aplicativo Python Runtime.

Para obter instruções sobre como iniciar o Servidor Cloud APM, consulte Iniciando o console do Cloud APM. Para obter informações sobre o uso do Editor de aplicativos, consulte Gerenciando aplicativos.

Customizando o Coletor de dados do Python para aplicativos no local
Ao modificar arquivos no pacote do coletor de dados, é possível configurar as variáveis de ambiente para customizar o monitoramento de seu aplicativo Python.

São fornecidos dois arquivos para customizar configurações do coletor de dados, `global.environment` e `config.properties`. Depois de mudar as configurações nesses arquivos, reinicie o aplicativo Python para que a mudança entre em vigor.

Ao modificar o arquivo `global.environment`, é possível customizar a conexão entre o coletor de dados e o Servidor Cloud APM. Se desejar usar outro Servidor Cloud APM em vez do padrão, ou se o arquivo-chave ou sua senha for mudada, modifique o Servidor Cloud APM para reconectar o coletor de dados ao Servidor Cloud APM.

Ao modificar o arquivo `config.properties`, é possível customizar os comportamentos do coletor de dados de acordo com suas necessidades, como ativar ou desativar o rastreio de método.

O arquivo de configuração `global.environment`

A Tabela 193 na página 678 mostra as variáveis de ambiente que podem ser configuradas no arquivo de configuração `global.environment` e as descrições correlacionadas. É possível localizar o arquivo `global.environment` na pasta `etc` onde o Coletor de dados do Python está instalado, por exemplo, diretório `/root/.pyenv/versions/3.5.2/lib/python3.5/site-packages/ibm_python_dc/etc`.

Tabela 193. Variáveis de ambiente suportadas no arquivo `global.environment`

Nome de variável	Importância	Valor	Descrição
APM_BM_GATEWAY_URL	Opcional	• https://<*server ip or hostname*>:443 • http://<*server ip or hostname*>:80	A URL de gateway do servidor no local de destino.
APM_KEYFILE_PSWD	Opcional	Senha do arquivo-chave	A senha do arquivo-chave que está associada ao arquivo-chave. **Nota:** Configure essa variável somente quando tiver configurado o Gateway para usar HTTPS.
APM_KEYFILE_URL	Opcional	http://<*hosted http server*>:<*port*>/keyfile.p12	A URL para fazer download do arquivo-chave. **Nota:** Configure essa variável somente quando tiver configurado o Gateway para usar HTTPS.

O arquivo `config.properties`

A Tabela 194 na página 679 mostra as variáveis de ambiente que podem ser configuradas nos arquivos de configuração `config.properties` e a descrição correlacionada. É possível localizar o arquivo `config.properties` no diretório de instalação do Coletor de dados do Python, por exemplo, diretório `/root/.pyenv/versions/3.5.2/lib/python3.5/site-packages/ibm_python_dc`.

Tabela 194. Variáveis de ambiente suportadas no arquivo `config.properties`

Nome de variável	Importância	Valor	Descrição
KPG_ENABLE_DEEPDIVE	Opcional	• False • Verdadeiro	• False: o valor padrão. Se você configurar essa variável como `False`, os dados diagnósticos não serão coletados. • True: se você configurar essa variável como `True`, os dados diagnósticos serão coletados. O nível padrão é `True`. Se você não configurar essa variável, os dados diagnósticos não serão coletados.
KPG_DD_CONFIG_FILE	Opcional	Nome do arquivo de configuração de monitoramento de diagnósticos.	Nome do arquivo de configuração de monitoramento de diagnósticos. O nome padrão do arquivo é `kpg_dd_config.xml`. **Nota:** Após customizar as configurações nesse arquivo, ele deverá ser colocado no diretório-raiz do aplicativo. Se você não configurar essa variável, o arquivo de configuração padrão `kpg_dd_config.xml` no pacote do coletor de dados será usado.
KPG_DD_APP_PATH	Opcional	Caminho para o aplicativo Python.	O caminho para o aplicativo Python ou o módulo para o qual o coletor de dados coleta dados de diagnósticos. Separe os caminhos de diferentes aplicativos e módulos Python que deseja monitorar com um ponto-e-vírgula `;`. Se você não configurar essa variável, o coletor de dados coletará dados diagnósticos para solicitações e os módulos usados por seu aplicativo. Os dados de solicitações na lib Python não serão coletados.

Tabela 194. Variáveis de ambiente suportadas no arquivo `config.properties` (continuação)

Nome de variável	Importância	Valor	Descrição
KPG_DD_SECURITY_FILTER	Opcional	• Verdadeiro • False	• True: o valor padrão. Se você configurar essa variável como `True`, os valores (como as senhas) serão mascarados em instruções SQL e os parâmetros não serão exibidos no widget de grupo **Contexto de solicitação**. • False: se você configurar essa variável como `False`, os valores em instruções SQL não serão mascarados e os parâmetros serão exibidos no widget de grupo **Contexto de solicitação**. Se você não configurar essa variável, os valores (como as senhas) serão mascarados em instruções SQL e os parâmetros não serão exibidos no widget de grupo **Contexto de solicitação**.
KPG_GC_STATS	Opcional	Verdadeiro	Todas as funções estatísticas da coleta de lixo do Python são ativadas. Configurar esse valor como `True` equivale à execução do comando a seguir: `gc.set_debug(gc.DEBUG_STATS | gc.DEBUG_COLLECTABLE | gc.DEBUG_UNCOLLECTABLE | gc.DEBUG_INSTANCES | gc.DEBUG_OBJECTS )` Para desativar KPG_GC_STATS, exclua essa variável de ambiente. Não configure-a como `False`. O valor padrão é `True`. **Nota:** Nunca configure KPG_GC_STATS=`True` em seu ambiente do produto formal. É somente para o modo de depuração. E certifique-se de que haja memória suficiente designada ao aplicativo.

Tabela 194. Variáveis de ambiente suportadas no arquivo `config.properties` (continuação)

Nome de variável	Importância	Valor	Descrição
KPG_LOG_LEVEL	Opcional	• DEBUG • ERROR • INFO	• DEBUG: somente informações úteis sobre depuração serão impressas no log, por exemplo, dados coletados, dados que são enviados para o servidor e resposta do servidor. • ERROR: somente informações sobre exceções e situações muito inesperadas serão impressas no log. • INFO: as informações de resumo sobre o coletor de dados para o usuário saber o que ele está fazendo serão impressas no log. O valor padrão é ERR0R.
KPG_LOG_TOCONSOLE	Opcional	• S • Verdadeiro • Qualquer outro valor que não seja `False`	O log será impresso no console e é possível ver o log executando o comando **`cf logs <appname>`**. O valor padrão é `True`.
KPG_SAVE_ALL	Opcional	Verdadeiro	Todos os objetos sem referência serão salvos em `gc.garbage`, e é preciso limpar `gc.garbage` a cada minuto (o coletor de dados faz essa limpeza). Configurar esse valor como `True` equivale à execução do comando a seguir: `gc.set_debug(gc.SAVE_ALL)` Para desativar KPG_SAVE_ALL, exclua essa variável de ambiente. Não configure-a como `False`. O valor padrão é `True`. **Nota:** Nunca configure `KPG_SAVE_ALL=True` em seu ambiente do produto formal. Eles serve somente para o modo de Depuração. E certifique-se de que haja memória suficiente designada ao aplicativo.
APM_GW_PROXY_CONNECTION	Opcional	http://*<server ip or hostname>*:port	O proxy HTTP ou HTTPS que o coletor de dados Python usa para enviar dados de monitoramento.

Desconfigurando o Coletor de dados do Python para aplicativos no local
Se você não precisa monitorar seu ambiente do Python ou se deseja fazer upgrade do Coletor de dados do Python, deve-se primeiro desconfigurar configurações anteriores para o Coletor de dados do Python.

Procedimento

1. Acesse o diretório inicial de seu aplicativo Python.
2. Remova as seguintes linhas do arquivo `requirements.txt` para o aplicativo:

```
--extra-index-url https://<your_host_name_and_domain>/python_dc/static/python-dc-repos/
simple/
ibm-python-dc
```

3. No arquivo `settings.py`, remova a linha a seguir da seção `MIDDLEWARE_CLASSES`:

```
ibm_python_dc.kpg_plugin.ResourceMiddleware
```

4. Execute o comando `pip uninstall ibm_python_dc` para desinstalar o Coletor de dados do Python do tempo de execução de Python.

Resultados

Você desconfigurou o Coletor de dados do Python com sucesso.

O que Fazer Depois

Depois de desconfigurar o coletor de dados, o Console do Cloud APM continua a exibir o coletor de dados em quaisquer aplicativos nos quais você incluiu o coletor de dados. O Console do Cloud APM mostrará que nenhum dado está disponível para o aplicativo e não indicará que o coletor de dados está off-line. Para obter informações sobre como remover o coletor de dados de aplicativos e de grupos de recursos, consulte “Removendo coletores de dados do Console do Cloud APM” na página 186.

Configurando o monitoramento do RabbitMQ

O Monitoring Agent for RabbitMQ monitora o funcionamento e desempenho dos recursos de cluster do RabbitMQ, como os nós, filas e canais do cluster. Você deve configurar o Agente RabbitMQ para que o agente possa coletar os dados do RabbitMQ.

Antes de Iniciar

- Revise os pré-requisitos de hardware e software.
- Certifique-se de que o usuário do RabbitMQ, que se conecta ao nó, tenha permissão de leitura e o monitoramento, administrador ou tag de gerenciamento esteja ativada para esse usuário.
- Certifique-se de que o plug-in de gerenciamento do RabbitMQ esteja ativado em todos os nós do cluster, porque se um nó do cluster falhar, o agente RabbitMQ se conectará a um nó peer que está disponível no cluster.

Revise os pré-requisitos de hardware e de software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Agente RabbitMQ.

Sobre Esta Tarefa

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte o “Histórico de Mudanças” na página 50.

O Agente RabbitMQ é um agente de múltiplas instâncias. Deve-se criar a primeira instância e iniciar o agente manualmente.

- Para configurar o agente em sistemas Windows, é possível usar a janela IBM Cloud Application Performance Management ou o arquivo silencioso de resposta.
- Para configurar o agente em sistemas Linux, é possível executar o script e responder aos prompts, ou usar o arquivo silencioso de resposta.

Configurando o agente nos sistemas Windows

Você pode utilizar o Use a janela do IBM Cloud Application Performance Management para configurar o agente nos sistemas Windows.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito em **Monitoring Agent for RabbitMQ** e, em seguida, clique em **Configurar agente**.

   Lembre-se: Após você configurar o agente pela primeira vez, a opção **Configurar Agente** é desativada. Para configurar o agente novamente, clique em **Reconfigurar**.
3. No campo **Inserir um nome de instância exclusivo**, digite o nome de instância do agente e clique em **OK**.
4. Na janela **Monitoring Agent for RabbitMQ**, especifique valores para os parâmetros de configuração e, em seguida, clique em **Avançar**.

   Para obter informações sobre os parâmetros de configuração, consulte o tópico a seguir: "Parâmetros de configuração para o agente" na página 684
5. Clique com o botão direito na instância **Monitoring Agent for RabbitMQ** e clique em **Iniciar**.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o console, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Configurando o agente nos sistemas Linux

Para configurar o agente em sistemas operacionais Linux, você deve executar o script e responder aos prompts.

Procedimento

1. Na linha de comandos, insira o seguinte comando: *install_dir*/bin/rabbitmq.sh config *instance_name*, em que *instance_name* é o nome que você deseja dar à instância:
2. Quando for solicitado para fornecer um valor para os parâmetros a seguir, pressione Enter para aceitar o valor padrão, ou especifique um valor e, em seguida, pressione Enter:
   - Endereço IP
   - Nome do Usuário
   - Senha
   - Número da Porta
   - Diretório inicial Java
   - Nível de rastreio de Java

   Para obter informações sobre os parâmetros de configuração, consulte o tópico a seguir: "Parâmetros de configuração para o agente" na página 684
3. Execute o comando a seguir para iniciar o agente:

   ```
   install_dir/bin/rabbitmq.sh start instance_name
   ```

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Configurando o agente usando o arquivo silencioso de resposta

O arquivo de resposta silencioso contém os parâmetros de configuração do agente. É possível editar o arquivo de resposta silencioso para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa
É possível usar o arquivo silencioso de resposta para configurar o Agente RabbitMQ em sistemas Linux e Windows. Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

1. Abra o arquivo de resposta silencioso que está disponível nesse caminho: *install_dir*\samples\rabbitmq_silent_config.txt
2. No arquivo rabbitmq_silent_config.txt, especifique valores para todos os parâmetros obrigatórios. Também é possível modificar os valores padrão de outros parâmetros.

   Para obter informações sobre os parâmetros de configuração, consulte o tópico a seguir: "Parâmetros de configuração para o agente" na página 684
3. Salve o arquivo de resposta e execute o comando a seguir:

   Linux AIX *install_dir*/bin/rabbitmq-agent.sh config *install_dir*/samples/rabbitmq_silent_config.txt

   Windows *install_dir*/bin/rabbitmq-agent.bat config *install_dir*/samples/rabbitmq_silent_config.txt
4. Inicie o agente:

   Linux AIX Execute o seguinte comando: *install_dir*\bin\rabbitmq-agent.sh start

   Windows Clique com o botão direito em **Monitoring Agent for RabbitMQ** e, em seguida, clique em **Iniciar**.

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Parâmetros de configuração para o agente

Quando você configura o Agente RabbitMQ, é possível mudar os valores padrão dos parâmetros, como o nome da instância e os certificados de validação SSL.

A tabela a seguir contém descrições detalhadas dos parâmetros de configuração para o Agente RabbitMQ.

Tabela 195. Nomes e descrições dos parâmetros de configuração para o Agente RabbitMQ		
Nome de parâmetro	**Descrição**	**Campo obrigatório**
Endereço IP	O endereço IP do nó no qual o aplicativo RabbitMQ está instalado.	Sim
Nome de Usuário	O nome de usuário do usuário RabbitMQ.	Sim
Senha	A senha para conectar-se à interface com o usuário de gerenciamento do RabbitMQ.	Sim
Confirmar Senha	A mesma senha inserida no campo **Senha**.	Sim
Número da Porta	O número da porta em que o plug-in de gerenciamento RabbitMQ está ativado. Use o número da porta padrão 15672, ou especifique outro número da porta.	Não
Início Java	O caminho onde o plug-in Java está instalado. Use o caminho padrão `C:\Program Files\IBM\Java50`, ou o caminho do diretório onde o plug-in Java está instalado.	Não
Nível de rastreio de Java	O nível de rastreio do provedor Java. Os valores de nível de rastreio válidos são os seguintes: • DESLIGADO • ERROR • WARN • INFO • DEBUG_MAX • TODOS	Não

Configurando o Monitoramento do Tempo de Resposta

O agente Response Time Monitoring monitora transações HTTP e HTTPS em seu servidor HTTP. As transações do usuário reais baseadas em navegador (sincronizações do navegador) também são monitoradas.

O agente Response Time Monitoring pode ser usado para visualizar os seguintes níveis de informações de monitoramento:

Monitoramento de transações HTTP e HTTPS

O monitoramento de transações HTTP está disponível automaticamente ao instalar o agente Response Time Monitoring.

Dependendo do tipo de servidor HTTP que está sendo monitorado, o monitoramento de transações HTTPS pode ficar disponível automaticamente ou talvez precise ser configurado manualmente. Para obter mais informações, consulte “Response Time MonitoringComponentes ” na página 686.

O Response Time Monitoring também monitora dados relacionados a contagens de usuários, contagem de sessões e dispositivos.

Os dados são apresentados no painel do Transações de Usuários Finais no horário local do usuário e também é usado no widget Solicitações e Tempo de Resposta.

Monitoramento real de transações do usuário final (sincronizações do navegador)

Dependendo do tipo de servidor HTTP que está sendo monitorado, os limites baseados em navegador podem ficar disponíveis automaticamente ou talvez precisem ser configurados. Para obter mais informações, consulte “Response Time MonitoringComponentes ” na página 686.

As sincronizações baseadas em navegador são possíveis com o JavaScript Injection.

Com o JavaScript Injection, é possível usar widgets adicionais e detalhes nos painéis de Transação do usuário final. O JavaScript Injection assegura que o tempo de resposta real do usuário final seja coletado no navegador. Ele monitora o desempenho de páginas HTTP e objetos integrados para paginas da web que são entregues pelo HTTP Server. Os seguintes detalhes adicionais de transação real do usuário final estão disponíveis:

- Widget Tempo total do cliente em solicitações de transação e tempo de resposta
- Widget Transações de tempo de resposta para tempo de espera do cliente nas transações - 10 principais
- Detalhamento do Tempo de Renderização

Para obter informações sobre como configurar o JavaScript injection, consulte "JavaScript Injection" na página 689

Visualizando Painéis de Transação

Visualizar dados de transação no Application Performance Dashboard.

Uma série de widgets está disponível no Application Performance Dashboard que fornecem detalhes contextuais sobre transações.

Boas solicitações têm um tempo de resposta menor que 10 segundos. *Solicitações lentas* têm um tempo de resposta maior que 10 segundos. O valor de 10 segundos usado para determinar os tempos de resposta bom e lento não é configurável. Os widgets a seguir estão disponíveis:

- Widget de grupo Pior por Usuário - 5 Principais
- Widget de grupo Pior por Dispositivo - 5 Principais
- Widget de grupo Solicitações e Tempo de Resposta
- Widget de grupo Transações-10 Principais
- Widget de grupo Solicitações de Transação e Tempo de Resposta
- Widget Em grupo de Execuções
- Widget do Grupo de Subtransações
- Widget de grupo Instâncias de transação
- Widget de Grupo Usuários por Local
- Widget de Grupo Usuários no Local Selecionado
- Widget de grupo Sessões do Usuário no Local Selecionado - 10 Principais
- Widget de grupo Solicitação de Usuário e Tempo de Resposta
- Sessões do Usuário - 10 principais widgets de grupo
- Widget de grupo Solicitação de Dispositivo e Tempo de Resposta
- Widget do grupo Sessão
- Widget de Grupo Solicitações de
- Widget de grupo Instâncias de Sessão
- Widget de grupo Instâncias de transação
- Painel Resumo de Transações de Middleware
- Painel Detalhes de Transações do Middleware
- Limites de evento para Monitoramento de transação
- Dados Agregados de Interação
- Dados de Agregação de Transações
- Status da Transação do WRT

Response Time MonitoringComponentes

A funcionalidade base do agente Response Time Monitoring é:

- monitoramento da transação HTTP
- Monitoramento de transações HTTPS
- Monitoramento de sincronizações baseadas em navegador (usando o JavaScript Injection)

Para ver descrições mais detalhadas dessa funcionalidade, consulte "Configurando o Monitoramento do Tempo de Resposta" na página 685.

Dependendo do tipo de HTTP Server que está sendo monitorado, a funcionalidade base do agente Response Time Monitoring é fornecida usando um dos seguintes componentes:

Módulo de Tempo de Resposta do IBM HTTP Server
O Módulo de Tempo de Resposta do IBM HTTP Server monitora somente o tipo de conteúdo http de: text/html, application/xml ou application/json (sem injeção de JavaScript)

Atualmente, o Módulo de Tempo de Resposta do IBM HTTP Server não pode monitorar solicitações compactadas de instrumento JavaScript.

Atualmente, a injeção de JavaScript do Módulo de Tempo de Resposta do IBM HTTP Server pode monitorar somente o tipo de conteúdo http de text/html.

Packet Analyzer
O Packet Analyzer pode monitorar somente o tipo de conteúdo de text/html. O Packet Analyzer pode monitorar solicitações compactadas gzip.

Se você estiver monitorando um IBM HTTP Server ou Apache HTTP Server no AIX ou Linux, use Módulo de Tempo de Resposta do IBM HTTP Server. É possível, mas não é recomendado, usar Packet Analyzer. O Módulo de Tempo de Resposta do IBM HTTP Server não é suportado no Windows. Use Packet Analyzer em um ambiente Windows.

Se você estiver monitorando qualquer outro servidor HTTP, use Packet Analyzer. O Packet Analyzer é suportado no Windows, Linux e AIX.

Planejando a Instalação

Planeje a instalação do agente Response Time Monitoring com base em seu sistema operacional e no tipo de servidor HTTP.

A funcionalidade base do Response Time Monitoring pode ser fornecida usando um dos seguintes componentes:

- Packet Analyzer
- Módulo de Tempo de Resposta do IBM HTTP Server

Você determina qual componente usar com base em:

- O tipo de servidor HTTP no qual o agente Response Time Monitoring está sendo instalado.
- Em qual sistema operacional o servidor HTTP está instalado.

As considerações para instalar o agente Response Time Monitoring com o Packet Analyzer são:

- O Packet Analyzer é suportado em todos os sistemas operacionais (Windows, Linux e AIX).
- O Packet Analyzer monitora transações HTTP na porta 80 para todos os sistemas operacionais.
- O monitoramento de transações HTTPS não é automático e deve ser configurado manualmente. O agente Response Time Monitoring requer acesso aos certificados SSL para que ele possa decriptografar o tráfego SSL de servidores HTTP. Para obter mais informações, consulte "Monitorando transações HTTPS" na página 706.
- O Packet Analyzer é suportado em todos os servidores HTTP, mas é recomendado somente para o Sun Java System Web Server e o Microsoft Internet Information Services.
- AIX Linux Windows Para instalar o agente Response Time Monitoring para trabalhar com o Packet Analyzer no IBM HTTP Server ou Apache HTTP Server, o servidor HTTP deve ser interrompido.

Ao instalar o agente Response Time Monitoring e o servidor HTTP ser interrompido, o Packet Analyzer é ativado automaticamente.

- AIX Linux Windows Embora o Packet Analyzer possa ser configurado para IBM HTTP Server ou Apache HTTP Server, isso não é recomendado; Módulo de Tempo de Resposta do IBM HTTP Server é recomendado.
- Windows O WinPcap 4.1.3 é necessário antes da instalação do agente Response Time Monitoring.
- Windows AIX Linux Se você instalar o agente Response Time Monitoring no Sun Java System Web Server ou Microsoft Internet Information Services, o Packet Analyzer será configurado automaticamente.

As considerações para instalar o agente Response Time Monitoring com o Módulo de Tempo de Resposta do IBM HTTP Server são:

- O Módulo de Tempo de Resposta do IBM HTTP Server é um componente do Agente do HTTP Server. Deve-se instalar o Agente do HTTP Server antes do agente do Response Time Monitoring ou instalar ao mesmo tempo. Para obter mais informações, consulte “Módulo de Tempo de Resposta do IBM HTTP Server” na página 695.
- O Módulo de Tempo de Resposta do IBM HTTP Server é suportado em todos os sistemas operacionais (Windows, Linux e AIX). O Módulo de Tempo de Resposta do IBM HTTP Server suporta o IBM HTTP Server versões 7, 8 e 9.
- Instale o agente Response Time Monitoring e o Agente do HTTP Server na mesma máquina.
- O Módulo de Tempo de Resposta do IBM HTTP Server monitora todas as portas para solicitação de HTTP e HTTPS no AIX, Linux e Windows.
- O Módulo de Tempo de Resposta do IBM HTTP Server é suportado somente para o IBM HTTP Server ou o Apache HTTP Server.
- Ambos os agentes são iniciados automaticamente, mas deve-se reiniciar o servidor HTTP.

A tabela a seguir descreve as diferentes combinações para configurar automaticamente o agente Response Time Monitoring.

Tabela 196. Cenários para configurar automaticamente o agente do Response Time Monitoring

Combinações de servidor HTTP e S.O.	**Packet Analyzer**	**Módulo de Tempo de Resposta do IBM HTTP Server**
Sun Java System Web Server ou Microsoft Internet Information Services no AIX ou no Linux	Automático	Não suportado
Sun Java System Web Server ou Microsoft Internet Information Services no Windows	Automático	Não suportado
IBM HTTP Server ou Apache HTTP Server no AIX, Linux ou Windows	Automático se o servidor HTTP for interrompido.	Automático se o servidor HTTP estiver presente e configurado

Planejando a Configuração

O monitoramento HTTP é ativado automaticamente ao instalar o agente Response Time Monitoring. Dependendo de seu ambiente, o HTTPS e JavaScript Injection talvez precisem ser configurados manualmente.

Monitoramento HTTP

O monitoramento de transações HTTP é configurado automaticamente para o Packet Analyzer e Módulo de Tempo de Resposta do IBM HTTP Server, se você seguir as diretrizes de instalação. Consulte “Planejando a Instalação ” na página 687.

Monitoramento HTTPS

O monitoramento de transações HTTPS é configurado automaticamente para o Módulo de Tempo de Resposta do IBM HTTP Server se você seguir as diretrizes de instalação. Consulte “Planejando a Instalação ” na página 687.

O monitoramento de transações HTTPS precisa ser configurado manualmente para o Packet Analyzer. Para obter mais informações, consulte “ Roteiro do Packet Analyzer” na página 704.

Sincronizações baseadas em navegador (usando o JavaScript Injection)

As sincronizações baseadas em navegador (usando o JavaScript Injection) são configuradas automaticamente para o Módulo de Tempo de Resposta do IBM HTTP Server.

As sincronizações baseadas em navegador (usando o JavaScript Injection) precisam ser configuradas manualmente para o Packet Analyzer. Para obter mais informações, consulte “ Roteiro do Packet Analyzer” na página 704.

A tabela a seguir descreve como a funcionalidade base é configurada para cada componente:

Tabela 197. Configuração de funcionalidade base

	Packet Analyzer on Sun Java System Web Server ou Microsoft Internet Information Services (Windows, Linux ou AIX)	**Módulo de Tempo de Resposta do IBM HTTP Server on IBM HTTP Server ou Apache HTTP Server (Windows, Linux ou AIX)**
monitoramento da transação HTTP	Ativado automaticamente.	Ativado automaticamente
Monitoramento de transações HTTPS	Deve ser configurado manualmente.	Ativado automaticamente
Monitoramento real de transações do usuário final (Sincronizações do navegador) usando JavaScript Instrumentation	Deve ser configurado manualmente.	Ativado automaticamente

JavaScript Injection

É possível customizar os dados que são coletados pelo agente do Response Time Monitoring para exibição nos painéis do Transações de Usuários Finais.

Para assegurar uma boa experiência do usuário para um aplicativo baseado na web, você deve monitorar o desempenho que é visto pelos usuários reais. Isso significa monitoramento no nível do navegador.

Para poder monitorar no nível do navegador, é preciso injetar Código de Monitoramento JavaScript nas páginas que você deseja monitorar. Este código então coleta dados para sincronizações do navegador específicas.

Isso é feito usando JavaScript Injection nas páginas da web e objetos que você deseja monitorar. Dependendo do tipo de servidor HTTP no qual você instalou seu agente Response Time Monitoring, existem dois métodos que podem ser usados para coletar informações de tempo de resposta de transação real do usuário final.

- Se estiver usando um IBM HTTP Server ou um servidor HTTP Apache, use o Módulo de Tempo de Resposta do IBM HTTP Server. O Módulo de Tempo de Resposta do IBM HTTP Server executa automaticamente o JavaScript Injection. O Módulo de Tempo de Resposta do IBM HTTP Server é um componente do Agente do HTTP Server. Ele é instalado e configurado como parte do Agente do HTTP Server. Para obter mais informações, consulte “Módulo de Tempo de Resposta do IBM HTTP Server” na página 695.

- Se estiver usando qualquer outro servidor HTTP suportado, use Packet Analyzer. Com o Packet Analyzer, você deve instrumentar manualmente suas páginas da web para coletar sincronizações do navegador. Para obter mais informações, consulte “Incluindo o componente de monitoramento JavaScript em seu aplicativo” na página 705.

A tabela a seguir mostra os recursos que estão disponíveis no Application Performance Dashboard se você configurar seu ambiente para o Packet Analyzer ou Módulo de Tempo de Resposta do IBM HTTP Server:

	Packet Analyzer	**Módulo de Tempo de Resposta do IBM HTTP Server**
10 Transações Principais	✓	✓
Tempo de Espera do Servidor	✓	✓
Detalhamento do Tempo de Renderização	–	✓
Subtransações AJAX	✓	✓
Dados de Sincronização de Recursos na tabela Subtransações	–	✓
Instâncias de Transação (10 Principais)	✓	✓
Topologia da Instância de Transação	✓	✓
Topologia do Aplicativo	✓	✓
Instrumentação Automática da Injeção do JavaScript	N/A	✓

Reconfigurando o Response Time Monitoring no Windows

Use o comando de configuração interativa `rt-agent` ou o utilitário IBM Cloud Application Performance Management para configurar ou reconfigurar o agente.

Antes de Iniciar

Se estiver ativando o monitoramento de transação HTTPS, certifique-se de que o Monitoring Agent for HTTP Server não esteja instalado na mesma máquina. Caso contrário, a configuração do Response Time Monitoring não mudará a configuração HTTPS para o Packet Analyzer.

Sobre Esta Tarefa

O agente Response Time Monitoring é configurado automaticamente após a instalação. Siga as diretrizes de instalação: “Planejando a Instalação ” na página 687. Talvez seja necessário reconfigurar, por exemplo, se quiser monitorar uma porta diferente ou monitorar transações HTTPS.

O diretório de instalação é chamado *install_dir*. O diretório de instalação padrão é: `C:\IBM\APM\`

Como uma alternativa para usar o comando de configuração interativa `rt-agent`, é possível configurar o agente no utilitário IBM Cloud Application Performance Management. Para obter mais informações, consulte “Usando a janela IBM Cloud Application Performance Management em sistemas Windows” na página 180.

Procedimento

Para customizar suas configurações de dados, conclua as etapas a seguir:

1. No computador no qual o agente Response Time Monitoring está instalado, pare o agente:

install_dir\BIN\rt-agent.bat stop

2. Use a configuração silenciosa para definir o agente:

```
install_dir\BIN\rt-agent.bat config install_dir\samples\rt_silent_config.txt
```

Se quiser ativar o monitoramento de transação HTTPS, remova o comentário das seguintes linhas no arquivo de configuração silenciosa. A amostra do `rt_silent_config.txt` para configurar o agente Response Time Monitoring para monitorar HTTPS no Windows deve ser semelhante a esta:

```
# Monitor HTTPS transactions
KT5MONITORHTTPSAPP=YES

# HTTPS keystore (e.g. - /tmp/keys.kdb)
KT5KEYSTORE=C:\keys\key.kdb

# HTTPS server certificate map (eg - certAlias,9.48.152.1,443;...)
KT5SERVERMAP=certalias,9.48.152.1,443

# O tráfego de rede do monitor para o NIC hospeda esse endereço IP
#KT5MONITORIP=9.48.152.1
```

3. Reinicie o agente do Response Time Monitoring para que as mudanças entrem em vigor:
install_dir\BIN\rt-agent.bat start

Resultados
Os dados da nova origem são exibidos nos painéis que estão associados ao Response Time Monitoring.

Reconfigurando o Response Time Monitoring no AIX e Linux

Use o comando de configuração `rt-agent` para configurar ou reconfigurar o agente Response Time Monitoring.

Sobre Esta Tarefa

O agente Response Time Monitoring é configurado automaticamente após a instalação. Siga as diretrizes de instalação: “Planejando a Instalação ” na página 687. Pode ser necessário reconfigurar, por exemplo, se você desejar monitorar uma porta diferente.

O diretório de instalação é referido como *install_dir*. O diretório de instalação padrão é: `/opt/ibm/apm/agent`.

Use o mesmo usuário raiz que foi usado para instalar o agente para iniciar, parar e configurar o agente.

Procedimento

Para reconfigurar, conclua as seguintes etapas:

1. No computador, no qual o agente Response Time Monitoring está instalado, pare o agente:

```
install_dir/bin/rt-agent.sh stop
```

2. Use a configuração interativa ou silenciosa:

a) Configuração interativa:

```
install_dir/bin/rt-agent.sh config
```

b) Configuração silenciosa:

```
install_dir/bin/rt-agent.sh config  install_dir/samples/rt_silent_config.txt
```

Se quiser ativar o monitoramento de transação HTTPS, remova o comentário das seguintes linhas no arquivo de configuração silenciosa. A amostra de `rt_silent_config.txt` para configurar o

agente Response Time Monitoring para monitorar HTTPS no AIX e Linux deve ser semelhante a esta:

```
# Monitor HTTPS transactions
KT5MONITORHTTPSAPP=YES

# HTTPS keystore (e.g. - /tmp/keys.kdb)
KT5KEYSTORE=/tmp/keys.kdb

# HTTPS server certificate map (eg - certAlias,9.48.152.1,443;...)
KT5SERVERMAP=certalias,9.48.152.1,443

# O tráfego de rede do monitor para o NIC hospeda esse endereço IP
#KT5MONITORIP=9.48.152.1
```

3. Reinicie o agente do Response Time Monitoring para que as mudanças entrem em vigor:
   install_dir/bin/rt-agent.sh start

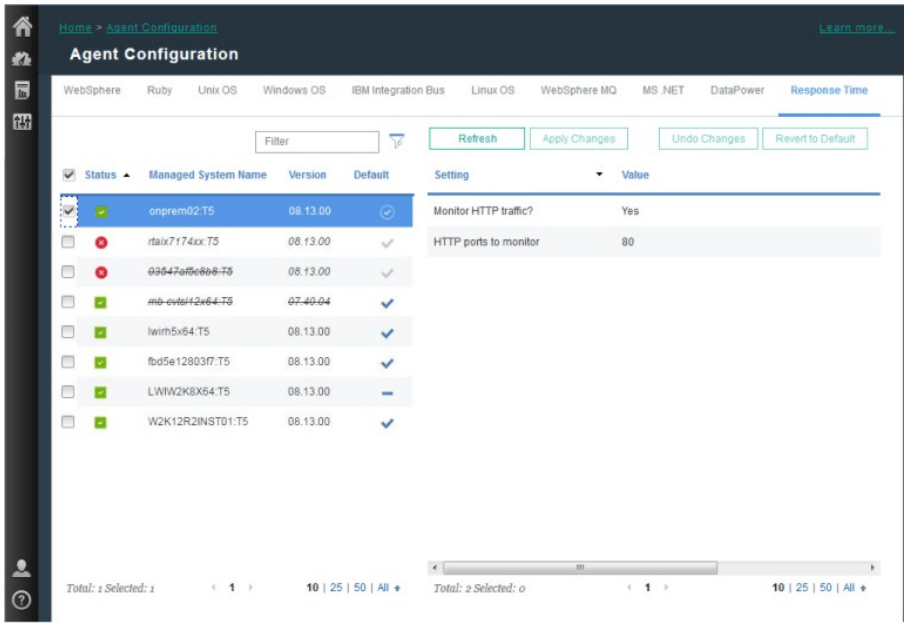
Resultados
Os dados da nova origem são exibidos nos painéis que estão associados ao Response Time Monitoring.

Configurando usando a página Configuração do agente

É possível usar a página **Configuração do agente** no Console do Cloud APM para ver quais agentes estão instalados. Quando aplicável, será possível desativar ou ativar o monitoramento de transação HTTP e configurar as portas que são monitorados pelos agentes Response Time Monitoring.

Configuração do Agente

Para acessar a página Response Time Monitoring **Configuração do agente**, no Console do Cloud APM, selecione **Configuração do sistema** > **Configuração do agente**, em seguida, selecione a guia **Tempo de resposta**.



A página **Configuração de Agente** lista os sistemas em seu ambiente no qual o Response Time Monitoring está instalado.

Para cada sistema com um agente Response Time Monitoring instalado, a página **Configuração de Agente** aparece:

- Se o sistema está on-line (visto com plano de fundo verde) ou off-line (cruz com plano de fundo vermelho).
- A versão do agente Response Time Monitoring que está instalado.

- Se a configuração central não puder determinar o tipo do agente (ou seja, se o Packet Analyzer ou Módulo de Tempo de Resposta do IBM HTTP Server estiver sendo usado para monitorar transações HTTP), somente o agente será tachado. Geralmente o tipo do agente não pode ser determinado quando o agente não está enviando seus detalhes por meio de atividade ASF.
- Se o sistema usa os valores de configuração padrão ou tem alguns valores customizados configurados.
- As portas que são monitoradas se o agente Response Time Monitoring estiver usando o Packet Analyzer para monitorar transações HTTP.

Setting	Value
Monitor HTTP traffic?	Yes
HTTP ports to monitor	80

- Se o Módulo de Tempo de Resposta do IBM HTTP Server, junto com o Agente do HTTP Server, está sendo usado para monitorar transações HTTP.

Setting	Value
Is IBM HTTP Server Response Time module enabled?	Yes

Dica: O Módulo de Tempo de Resposta do IBM HTTP Server monitora transações HTTP e HTTPS automaticamente. Nenhuma configuração adicional do agente Response Time Monitoring é necessária.

Selecione um agente para exibir suas definições de configuração. Para localizar um agente específico, insira no campo **Filtrar** uma parte ou todo o nome do sistema no qual ele está instalado.

Customizações feitas na página **Configuração de Agente** têm precedência sobre qualquer customização e sobre valores padrão.

Caso você mude de ideia sobre as configurações alteradas, clique em **Desfazer Mudanças** para reverter as últimas configurações que foram salvas ou clique em **Reverter para o padrão** para reverter para os valores padrão.

Os novos valores de configuração são enviados para Serviços de Configuração Central e agentes online são, então, automaticamente reconfigurados sem precisar serem reiniciados. Se o agente estiver offline, ele fará download das novas definições de configuração quando se tornar online. Dados de novas portas são exibidos nos painéis associados ao Response Time Monitoring quando dados são atualizados.

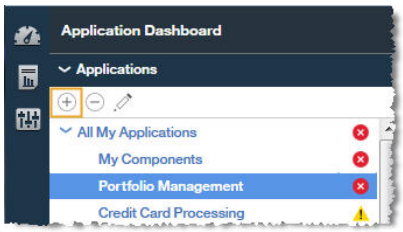
Incluindo Aplicativos

Após a instalação do agente do Response Time Monitoring, talvez seja necessário incluir no Painel de Desempenho do Aplicativo os aplicativos a serem monitorados.

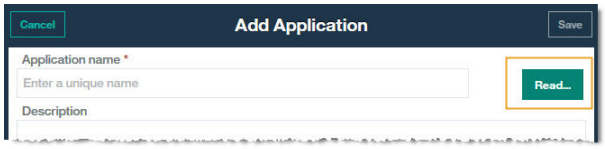
Procedimento

Para incluir aplicativos no Painel de Desempenho do Aplicativo :

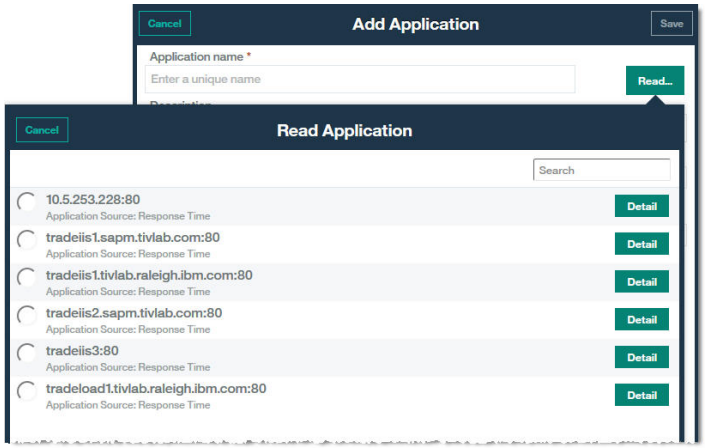
1. No Painel de Desempenho do Aplicativo , clique em **Incluir Aplicativo**.



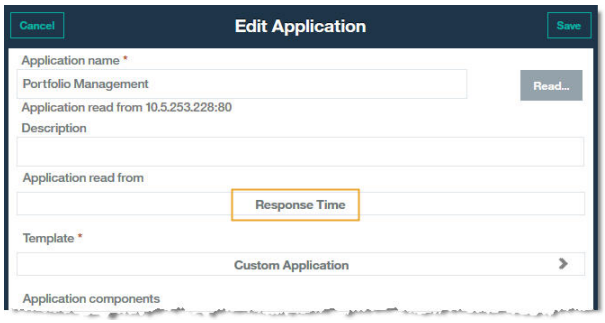
2. Selecione **Ler** para abrir uma lista de aplicativos descobertos.



3. Selecione o aplicativo que você deseja monitorar.



Tempo de Resposta é exibido como repositório de origem no campo **Ler a partir do Aplicativo**, e qualquer componente é listado em **Componentes do aplicativo**.



4. Não é necessário fazer qualquer configuração adicional para exibir aplicativos monitorados pelo agente Response Time Monitoring no Painel de Desempenho do Aplicativo . Clique em **Salvar** na janela **Incluir Aplicativo**.

Resultados

Aplicativos detectados pelo agente Response Time Monitoring são listados em **Todos os Meus Aplicativos** no Painel de Desempenho do Aplicativo .

Configurando o Módulo de Tempo de Resposta do IBM HTTP Server

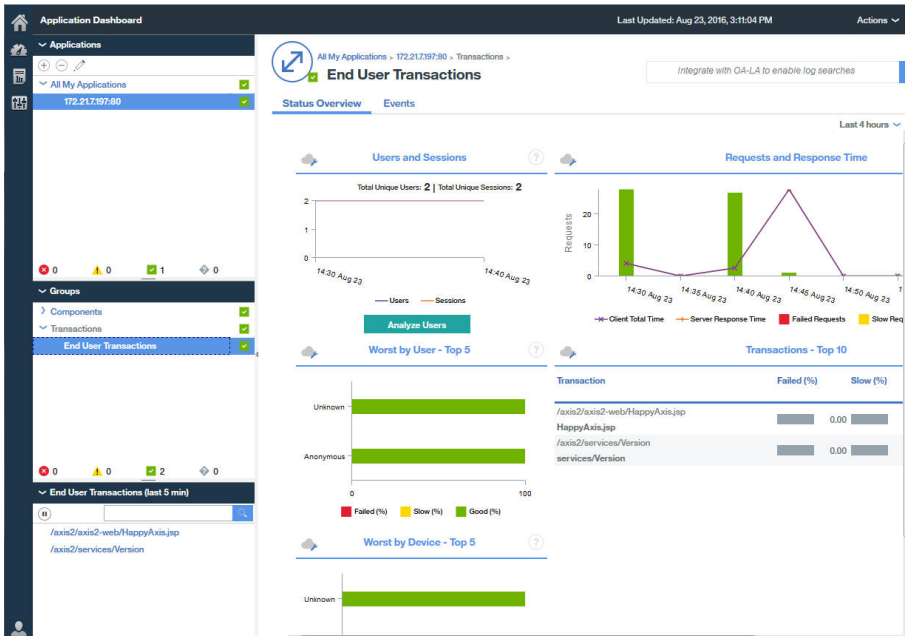
Para IBM HTTP Server e Apache HTTP Server, use o Módulo de Tempo de Resposta do IBM HTTP Server para visualizar métricas de monitoramento de tempo de resposta real do usuário final para páginas HTTP.

O Módulo de Tempo de Resposta do IBM HTTP Server é instalado e configurado como parte do Agente do HTTP Server. O Módulo de Tempo de Resposta do IBM HTTP Server funciona apenas junto com o IBM HTTP Server e o Apache HTTP Server no AIX, Linux e Windows. O Módulo de Tempo de Resposta do IBM HTTP Server monitora todas as portas para solicitações HTTP e HTTPS.

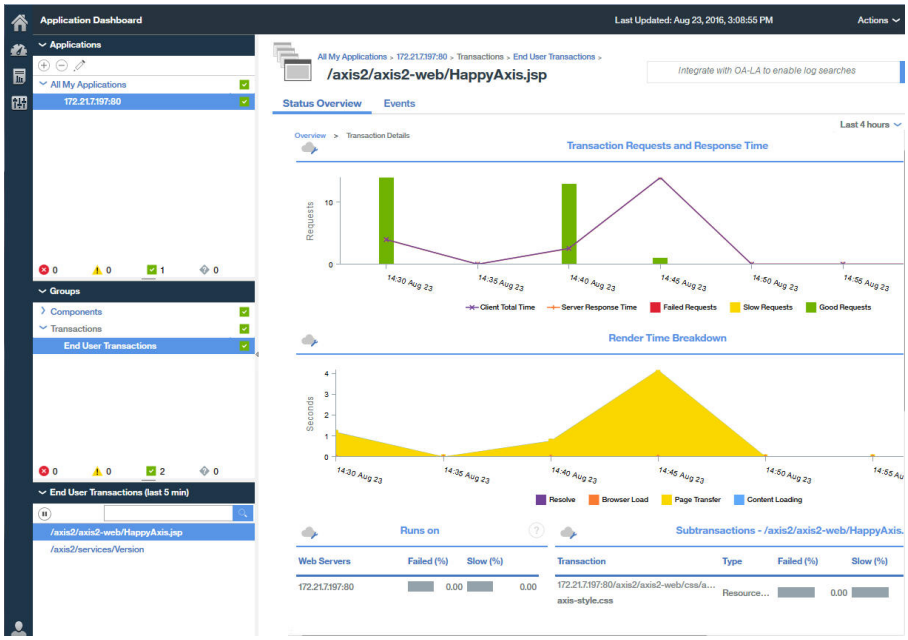
Usando JavaScript, o Módulo de Tempo de Resposta do IBM HTTP Server insere um cabeçalho em páginas da web que são entregues por um IBM HTTP Server para que o agente Response Time Monitoring possa monitorar essas páginas. Objetos integrados carregados pela página são controlados usando cookies. As informações da transação de páginas da web que são entregues pelo IBM HTTP Server ou Apache são então incluídas nos painéis do Transações de Usuários Finais.

Por exemplo:

Área de trabalho Transações do usuário final que mostra dados que são coletados do Módulo de Tempo de Resposta do IBM HTTP Server nas Transações - 10 principais:



A área de trabalho Transações do Usuário Final que mostra dados que são coletados do Módulo de Tempo de Resposta do IBM HTTP Server na tabela **Subtransações**



Módulo de Tempo de Resposta do IBM HTTP Server
O Módulo de Tempo de Resposta do IBM HTTP Server é uma parte do Agente do HTTP Server. Mas ele funciona em conjunto com o agente Response Time Monitoring para monitorar transações de aplicativo em servidores HTTP suportados.

Ao instalar o agente Response Time Monitoring para trabalhar com o Módulo de Tempo de Resposta do IBM HTTP Server, ele monitora todas as portas para solicitações HTTP e HTTPS.

O Módulo de Tempo de Resposta do IBM HTTP Server é uma parte do Agente do HTTP Server. Deve-se instalar o Agente do HTTP Server antes do agente do Response Time Monitoring ou instalar ao mesmo tempo.

O Agente do HTTP Server é composto de dois plug-ins:

1. khu_module - este é o Agente do HTTP Server. Esse plug-in é responsável por todos os painéis associados ao Agente do HTTP Server. Para obter mais informações, consulte Referência do Agente do Servidor HTTP.
2. wrt_module - esse é o Módulo de Tempo de Resposta do IBM HTTP Server.

Esses dois plug-ins são indicados no arquivo de configuração do Agente do HTTP Server. O arquivo de configuração do Agente do HTTP Server é conforme a seguir para o Apache HTTP Server:

```
khu.usr.local.apache24.conf.httpd.conf
```

O arquivo é conforme a seguir para o IBM HTTP Server:

```
khu.opt.IBM.HTTPServer.conf.httpd.conf
```

A regra de nomenclatura desse arquivo é: khu.(caminho completo do arquivo de configuração do servidor http, mude o / para .).conf

```
LoadModule khu_module

LoadModule wrt_module
```

Para que o Módulo de Tempo de Resposta do IBM HTTP Server funcione, o arquivo de configuração do servidor HTTP deve ter uma instrução include que referencie o arquivo de configuração do Agente do HTTP Server. Exemplo:

```
include /opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf
```

Essa instrução include ativa ambos os plug-ins ao mesmo tempo. Para obter mais informações, consulte “Configurando o monitoramento do Servidor HTTP” na página 266.

Instalando e Configurando o Módulo de Tempo de Resposta do IBM HTTP Server
A configuração é automática no lado do agente Response Time Monitoring. O Módulo de Tempo de Resposta do IBM HTTP Server precisa estar instalado e configurado como parte do Agente do HTTP Server. O agente Response Time Monitoring detecta automaticamente o Módulo de Tempo de Resposta do IBM HTTP Server e o ativa.

Sobre Esta Tarefa

Procedimento

1. Instale o Agente do HTTP Server que instala automaticamente o Módulo de Tempo de Resposta do IBM HTTP Server.
2. Configure o Agente do HTTP Server. Isso ativa o Módulo de Tempo de Resposta do IBM HTTP Server. Para obter mais informações, consulte “Configurando o monitoramento do Servidor HTTP” na página 266.
3. Instale o agente Agente Response Time Monitoring como root ou Administrator, dependendo de seu sistema operacional. Para obter instruções detalhadas, consulte Capítulo 6, “Instalando os agentes”, na página 117.
4. Reinicie o IBM HTTP Server. Quando o instalador do Response Time Monitoring detecta o Agente do HTTP Server, o agente Response Time Monitoring ativa o Módulo de Tempo de Resposta do IBM HTTP Server automaticamente.

Ativando o Módulo de Tempo de Resposta do IBM HTTP Server manualmente
É possível ativar o Módulo de Tempo de Resposta do IBM HTTP Server manualmente para monitorar o desempenho de páginas HTTP e objetos integrados para páginas da web que são atendidas pelo IBM HTTP Server.

Sobre Esta Tarefa
O Módulo de Tempo de Resposta do IBM HTTP Server é ativado automaticamente quando o Agente do HTTP Server é instalado e configurado. No entanto, talvez você queira ativar manualmente o Módulo de Tempo de Resposta do IBM HTTP Server.

Procedimento

Para ativar o Módulo de Tempo de Resposta do IBM HTTP Server manualmente no Linux, AIX ou Windows, conclua as seguintes etapas:

1. Linux AIX
   Para ativar o Módulo de Tempo de Resposta do IBM HTTP Server manualmente no Linux ou AIX, conclua as seguintes etapas:
   a) Pare o agente Response Time Monitoring.
      Execute:
      ```
      $AGENT_HOME/bin/rt-agent.sh stop
      ```
      em que *$AGENT_HOME* pode ser `/opt/ibm/apm/agent` em um sistema Linux ou `/opt/ibm/ccm/agent` em um sistema AIX.
   b) Execute um comando de configuração e use *$AGENT_HOME*`/samples/rt_silent_config_ihs.txt` para incluir os módulos de carregamento no arquivo de configuração do servidor da web e definir os parâmetros de configuração para o Módulo de Tempo de Resposta do IBM HTTP Server.
   c) Reinicie o agente do Response Time Monitoring.
2. Windows
   Para ativar o Módulo de Tempo de Resposta do IBM HTTP Server manualmente no Windows, conclua as seguintes etapas:
   a) Pare o agente Response Time Monitoring.
      Execute:
      ```
      AGENT_HOME/bin/rt-agent.bat stop
      ```
      em que *AGENT_HOME* pode ser `C:\IBM\APM` em um sistema Windows.
   b) Execute um comando de configuração e use *AGENT_HOME*`\samples\rt_silent_config_ihs.txt` para incluir os módulos de carregamento no arquivo de configuração do servidor da web e definir os parâmetros de configuração para o Módulo de Tempo de Resposta do IBM HTTP Server.
      Por exemplo,
      ```
      AGENT_HOME\bin\rt_agent.bat config AGENT_HOME\samples\rt_silent_config_ihs.txt
      ```
   c) Reinicie o agente do Response Time Monitoring.

Desativando o Módulo de Tempo de Resposta do IBM HTTP Server manualmente
Para desativar o Módulo de Tempo de Resposta do IBM HTTP Server e usar o Packet Analyzer novamente, reconfigure o agente e desative o monitoramento pelo Módulo de Tempo de Resposta do IBM HTTP Server.

Sobre Esta Tarefa

Use os seguintes procedimentos para desativar o Módulo de Tempo de Resposta do IBM HTTP Server.

Procedimento

Para reconfigurar o agente interativamente no Linux, AIX ou Windows, conclua as seguintes etapas:

1. Linux AIX

Para reconfigurar o agente interativamente no Linux e AIX, conclua as seguintes etapas:

a) Execute *install_dir*/bin/rt-agent.sh config
em que *install_dir* é /opt/ibm/apm/agent no Linux e AIX.

b) Reinicie o agente do Response Time Monitoring.

Como alternativa, para configurar os parâmetros manualmente:

a) Abra *install_dir*/config/*hostname*_t5.cfg em um editor de texto.
em que *install_dir* é /opt/ibm/apm/agent no Linux e AIX.

b) Configure os seguintes parâmetros:

```
KT5DISABLEANALYZER=NO
KT5ENABLEWEBPLUGIN=NO
```

c) Reinicie o agente do Response Time Monitoring.

2. Windows
Para reconfigurar o agente interativamente no Windows, conclua as seguintes etapas:

a) Configure os parâmetros relacionados manualmente, abra o *install_dir*\TMAITM6_x64*hostname*_t5.cfg em um editor de texto.
em que *install_dir* é C:\IBM\APM no Windows.

b) Configure os seguintes parâmetros:

```
KT5DISABLEANALYZER=NO
KT5ENABLEWEBPLUGIN=NO
```

c) Reinicie o agente do Response Time Monitoring.

Configuração Avançada do Módulo de Tempo de Resposta do IBM HTTP Server
Existem várias opções de configuração avançada para o Módulo de Tempo de Resposta do IBM HTTP Server.

O Módulo de Tempo de Resposta do IBM HTTP Server é configurado automaticamente, mas existem várias tarefas de avançado avançada que podem ser executadas para otimizar o desempenho e recursos.

Desativando o monitoramento da sincronização de recurso
O monitoramento de sincronização de recursos está ativado para todas as instâncias do Módulo de Tempo de Resposta do IBM HTTP Server instaladas pelo Agente do HTTP Server.

Sobre Esta Tarefa

Se desejar reduzir o número de recursos monitorados pelo Módulo de Tempo de Resposta do IBM HTTP Server ou desativar o monitoramento de sincronização de recursos para reduzir o carregamento de processamento necessário para monitorar um IBM HTTP Server específico, conclua as etapas a seguir:

Procedimento

Para editar o arquivo de configuração do Agente do HTTP Server gerado, conclua as etapas a seguir:

1. No final do arquivo de configuração do servidor HTTP (httpd.conf), anexe

```
WrtMaxPostResourcesSize
```

2. Configure um dos valores a seguir:
   - `WrtMaxPostResourcesSize -1`, para monitorar todos os recursos
   - `WrtMaxPostResourcesSize 0`, para desativar o monitoramento de recurso

- `WrtMaxPostResourcesSize n`, para monitorar um número específico de recursos, `10` por padrão. Por exemplo, configure `WrtMaxPostResourcesSize 2` para configurar no máximo dois recursos para portar para o servidor.

3. Reinicie o servidor HTTP.

Desativando a geração de Correlacionador ARM

Por padrão, a geração de Correlacionador do ARM está ativada, o que permite que o Módulo de Tempo de Resposta do IBM HTTP Server conecte-se a quaisquer servidores de backend na topologia. É possível desativar a geração de Correlacionador ARM, se necessário.

Sobre Esta Tarefa

Restrição: Se você desativar a geração de Correlacionador ARM, o Módulo de Tempo de Resposta do IBM HTTP Server não poderá ser vinculado a servidores de backend, como WebSphere Application Server. Desative a geração do Correlacionador ARM somente sob aviso do Suporte de Software IBM.

Procedimento

Para desativar a geração de Correlacionador ARM, conclua as etapas a seguir:

1. No final do arquivo de configuração do servidor HTTP (httpd.conf), anexe

```
WrtDisableArmCorr
```

2. Reinicie o Servidor HTTP

Desativando o Response Time Monitoring with Client Time (JavaScript Instrumentation)

No IBM Application Performance Management, Response Time Monitoring with Client Time (JavaScript Instrumentation) é ativada para todas as instalações em execução em todos os computadores. IBM HTTP Server

Sobre Esta Tarefa

Procedimento

Para desativar o JavaScript Injection manualmente, conclua as etapas a seguir:

1. Abra o arquivo de configuração do servidor HTTP localizado aqui: *`HTTP_Server_root`*`/conf/httpd.conf`
2. Navegue para a linha incluída para o agente de servidor HTTP e anexe a seguinte linha após ela:

```
WrtDisableJSI
```

   Por exemplo,

```
include /opt/ibm/apm/agent/tmp/khu/khu.opt.IBM.HTTPServer.conf.httpd.conf
WrtDisableJSI
```

3. Salve o arquivo `httpd.conf` e recicle o servidor HTTP.

Efetuando bypass do cookie WRTCorrelator

Quando a injeção de JavaScript está ativada para o agente do Response Time Monitoring no WebSphere Portal, os cookies, como o cookie WRTCorrelator, podem causar problemas enquanto você está usando o WebSphere Portal. Para evitar esses problemas, é possível configurar o cookie WRTCorrelator para que seja ignorado.

Procedimento

1. Se necessário, inicie o servidor `WebSphere_Portal` .
2. Efetue login no WebSphere® Integrated Solutions Console.
3. Acesse **Recursos** > **Ambiente de Recursos** > **Provedores de Ambiente de Recursos**.

4. Selecione **WP ConfigService** .
5. Em Propriedades Adicionais, selecione **Propriedades Customizadas** .
6. Clique em **Novo**.
7. Especifique o nome da propriedade, neste caso, o cookie WRTCorrelator e configure o valor da propriedade a ser ignorada.

   Para configurar o cookie WRTCorrelator a ser ignorado, digite o seguinte:

   ```
   cookie.ignore.regex =
   digest\.ignore. * | LTPAToken | LTPAToken2 | JSESSIONID | WASReqURL | WRTCorrelator
   |PD_STATEFUL.*
   ```
8. Clique em **Aplicar** e salve suas mudanças.
9. Efetue logout do WebSphere® Integrated Solutions Console.

Resultados
O cookie WRTCorrelator é configurado para que seja ignorado e problemas, como loop, são evitados.

Excluindo páginas do relatório de tempo de espera do cliente
Você pode desejar excluir determinadas páginas do relatório de tempo de espera do cliente a partir do navegador.

Sobre Esta Tarefa
É possível incluir um parâmetro no arquivo de configuração para parar o Módulo de Tempo de Resposta do IBM HTTP Server de injetar JavaScript em qualquer arquivo que corresponda aos padrões especificados. Isso, por sua vez, para o relatório de tempo de espera do cliente do navegador nessas páginas.

Procedimento

Para excluir determinadas páginas do relatório de tempo de espera do cliente no navegador, conclua as seguintes etapas:

1. Abra o arquivo a seguir em um editor de texto:

   Linux AIX *install_dir*/config/*hostname*_t5.cfg, em que *install_dir* é /opt/ibm/apm/agent

   Windows *install_dir*\TMAITM6_x64*hostname*_t5.cfg em que *install_dir* é C:\IBM\APM
2. Na seção **advconfig**, inclua

   ```
   {KT5WEBPLUGIN_JSI_EXCLUDE_URI_WITH_PATTERNS=URL_path_pattern to_exclude}
   ```

   Por exemplo,

   ```
   {KT5WEBPLUGIN_JSI_EXCLUDE_URI_WITH_PATTERNS=*/DoNotJSIMe.jsp,/absolutePath/index.jsp,/
   skipThisDir/*}
   ```

   O caminho da URL é limitado a 256 caracteres.

   Dica: Use um asterisco (*) como um prefixo ou sufixo para corresponder aos padrões. Inclua diversos valores separados por uma vírgula no parâmetro, se necessário.
3. Salve e feche *hostname*_t5.cfg.
4. Reinicie o agente Response Time Monitoring:

   ```
   rt-agent.sh stop
   rt-agent.sh start
   ```

Usando o Módulo de Tempo de Resposta do IBM HTTP Server como um usuário não raiz
Com uma configuração cautelosa, é possível usar o Módulo de Tempo de Resposta do IBM HTTP Server com um ID de usuário diferente de `root`. Lembre-se de que, se você estiver usando o Network Packet Analyzer, o usuário `root` deverá ser utilizado.

Para usar um ID de usuário diferente de `raiz`, siga estas diretrizes.

Para o agente Response Time Monitoring

Instale o agente Response Time Monitoring usando o ID do usuário com o qual irá executá-lo em um diretório com acesso de gravação.

- Para esse procedimento, o ID do usuário do agente Response Time Monitoring é *agentuser*. O diretório em que o agente está instalado é *$AGENT_HOME*.
- Se você instalar o agente Response Time Monitoring como `raiz` e, em seguida, executar o agente como um usuário diferente, não será possível criar arquivos.

Para o Módulo de Tempo de Resposta do IBM HTTP Server

`ServerRoot` deve pertencer ao mesmo ID do usuário que o usado para executar `apache start|stop`.

- Durante o `apache start`, um diretório de rastreamento do `wrt` é criado em `ServerRoot`. Portanto, o usuário precisa de permissões suficientes para criar arquivos e diretórios sob `ServerRoot`.
- Se o usuário do Módulo de Tempo de Resposta do IBM HTTP Server, *ihsuser*, for diferente do *agentuser*, ele exigirá acesso de gravação ao `$AGENT_HOME/tmp`.

  O `$AGENT_HOME/tmp` é criado durante a instalação de agentes. O *ihsuser* precisa de permissão para criar um diretório `kt5` no `$AGENT_HOME/tmp`.
- Pode haver várias versões de `ServerRoot`, cada uma administrada por usuários diferentes.

Para o agente Response Time Monitoring e o Módulo de Tempo de Resposta do IBM HTTP Server

O *agentuser* e o *ihsuser* precisam de acesso de leitura/gravação aos diretórios a seguir:

- `$AGENT_HOME/tmp/kt5`
- `ServerRoot/wrt`

Normalmente, o Módulo de Tempo de Resposta do IBM HTTP Server é iniciado primeiro e os diretórios `wrt` são criados automaticamente pelo Response Time Monitoring quando ele é iniciado pela primeira vez com acesso de leitura/gravação para todos.

O `ServerRoot/wrt` também é usado pelo `camconfig` para configuração push. O *ihsuser* cria arquivos de ID de fila compartilhada que são escolhidos pelo *agentuser*; o *agentuser* lê o ID da fila a partir do diretório e envia a configuração por push.

Se a `raiz` for usada para executar inicialmente o `apache start` e o *ihsuser* não for `raiz`, conclua as seguintes etapas:

1. Pare o agente Response Time Monitoring.
2. Usando a `raiz`, execute `apachectl stop`.
3. Exclua os seguintes diretório:
   - `$AGENT_HOME/tmp/kt5`
   - `ServerRoot/wrt`
4. Usando *ihsuser*, execute `apachectl start` para recriar os diretórios com as permissões corretas.

Para a reconfiguração da permissão do Módulo de Tempo de Resposta do IBM HTTP Server para o diretório `wrt`

É possível reconfigurar a permissão do diretório Módulo de Tempo de Resposta do IBM HTTP Server `wrt` para aumentar a segurança. A atualização envolve a inclusão de um parâmetro no arquivo de

configuração para limitar a permissão para o diretório `wrt` que foi criado pelo usuário não raiz durante a instalação do IBM HTTP Server.

Conclua este procedimento no sistema em que o Módulo de Tempo de Resposta do IBM HTTP Server está instalado para mudar a permissão do diretório `wrt` para o usuário não raiz de 777 para 700:

1. Abra o arquivo `$IHS_HOME$/conf/httpd.conf` em um editor de texto.
2. Inclua a propriedade **`WrtDisableDirPermNonRoot`** no término do arquivo:
   - Quando a propriedade é ativada, somente o ID do usuário que iniciou o httpd e que corresponde ao ID do usuário que criou o diretório é usado para criar o diretório `wrt` com a permissão 700. Todos os outros usuários têm o acesso negado para trabalhar com este diretório.
   - Quando a propriedade não está ativada, o diretório `wrt` é criado com a permissão padrão 777.
3. Reinicie o agente do Response Time Monitoring :

```
rt-agent.sh stop
rt-agent.sh.start
```

Os dados de configuração do Response Time Monitoring e alguns arquivos persistentes são armazenados no diretório `wrt`, que é usado durante o processo de comunicação e cada processo de conexão cria um arquivo de configuração wrt no diretório. Depois de incluir **`WrtDisableDirPermNonRoot`** no arquivo `httpd.conf`, somente o usuário específico limitado poderá comunicar-se com o agente de monitoramento do Response Time Monitoring com sucesso.

Usando balanceadores de carga

Se estiver usando balanceadores de carga em seu ambiente, alguma customização adicional é necessária.

Procedimento

Se estiver usando um balanceador de carga, siga estas diretrizes:

1. Desative a regravação de URL do balanceador de carga.
2. Instale um agente do Response Time Monitoring em cada servidor da web que deseja monitorar.

   Não instale o Response Time Monitoring no balanceador de carga.

O que Fazer Depois

Caso você esteja executando o agente do Response Time Monitoring atrás de um balanceador de carga, é possível configurar o balanceador de carga para encaminhar o endereço IP do cliente para otimizar o desempenho do monitoramento. Use as seguintes etapas como um exemplo:

1. No cabeçalho de HTTP, configure o endereço IP do cliente no campo **`X-Forwarded-For`**.
2. No arquivo `$AGENT_HOME/config/`*`hostname`*`_t5.cfg`, inclua `{KT5WEBPLUGIN_OVERRIDE_SOURCE_ADDR_HEADERS=X-Forwarded-For}` na seção `SECTION=advconfig`.

   Dica: Inclua diversos valores para o parâmetro se necessário. Por exemplo, `{KT5WEBPLUGIN_OVERRIDE_SOURCE_ADDR_HEADERS=x-forwarded-for, iv-remote-address}`
3. Reinicie o agente do Response Time Monitoring. Execute os seguintes comandos:

```
rt-agent.sh stop
rt-agent.sh start
```

Limitando a CPU usada para monitorar o IBM HTTP Server

Em ambientes saturados, talvez você queira limitar a porcentagem de CPU usada pela instrumentação IBM HTTP Server.

Sobre Esta Tarefa

Especifique a porcentagem da CPU que o Módulo de Tempo de Resposta do IBM HTTP Server pode usar. A porcentagem de CPU usada não é limitada por padrão. Configure a porcentagem de CPU no servidor no qual o agente está instalado.

Procedimento

Para configurar a porcentagem de CPU usada, conclua as etapas a seguir:

1. Reconfigure o agente de forma interativa ou manualmente:
   - Execute o script do agente para configurar interativamente:

     Linux AIX

     ```
     $AGENT_HOME/bin/rt-agent.sh config
     ```

     Windows

     ```
     install_dir\BIN\rt-agent.bat config
     ```

   - Abra o arquivo a seguir em um editor de texto:

     Linux AIX

     ```
     /opt/ibm/apm/agent/config/hostname_t5.cfg
     ```

     Windows

     ```
     C:\IBM\APM\TMAITM6_x64\hostname_T5.cfg
     ```

2. Na seção **advconfig**, inclua o parâmetro a seguir e configurar um valor de 0 a 100:

   ```
   KT5WEBPLUGIN_TARGET_CPU_PERCENTAGE=10
   ```

   em que o valor que você especificar é o limite de porcentagem de uso da CPU. O valor padrão igual a *0* significa que o uso da CPU não é limitado.
3. Também é possível configurar os parâmetros a seguir:

Opção	Descrição
KT5WEBPLUGINCONFIGPOSTURL	Lista de URLs correspondente a uma instalação do IBM HTTP Server. Padrão: `http://localhost/WrtUpdateConfig.dat`
KT5WEBPLUGIN_MAX_REQUESTS_PER_SECOND	Número de solicitações por segundo monitoradas por cada instalação do IBM HTTP Server. Se o número de solicitações exceder esse número, as solicitações subsequentes não serão monitoradas. Se o limite for atingido, a inserção de JavaScript para e nenhum dado é enviado para o agente do Response Time Monitoring. Padrão: `0` (sem máximo)
KT5WEBPLUGIN_CPUMAN_PERIOD_IN_SEC	O período, em segundos, no qual o uso de CPU é verificado para determinar se o destino foi excedido. Padrão: `60` segundos

Opção	Descrição
KT5WEBPLUGIN_CATCHUP_PERIOD_COUNT	Número de períodos permitidos no mesmo estado antes de a CPU ser escalada de volta. Por exemplo, usando o padrão, se o uso de CPU estiver alto e, 4 ciclos depois, permanecer alto, o uso de CPU será escalado de volta. Padrão: 3

Resultados
A porcentagem de CPU disponível para o Módulo de Tempo de Resposta do IBM HTTP Server é configurada em uma percentagem fixa.

Roteiro do Packet Analyzer

Use o Packet Analyzer para monitorar transações HTTP. É preciso configurar manualmente o monitoramento HTTPS. É necessário instrumentar manualmente suas páginas da web para coletar sincronizações do navegador.

Para determinar os ambientes nos quais é possível usar o Packet Analyzer, consulte “Response Time MonitoringComponentes ” na página 686 e “Planejando a Instalação ” na página 687.

O Analisador de Pacotes é ativado automaticamente ao instalar o agente Response Time Monitoring, mas existem diversas etapas e customizações adicionais que talvez você precise executar.

1. É possível customizar configurações do Packet Analyzer, por exemplo, o número da porta na janela Configuração do Agente. Para obter mais informações, consulte “Configurando o Packet Analyzer usando a janela Configuração do agente” na página 704.
2. Para monitorar transações HTTPS, instrumente manualmente suas páginas da web para coletar sincronizações do navegador. Para obter mais informações, consulte “Monitorando transações HTTPS” na página 706.
3. Para ativar sincronizações do navegador, inclua o componente JavaScript Injection em seu aplicativo e associe o componente de monitoramento JavaScript ao seu aplicativo, Para obter mais informações, consulte “Incluindo o componente de monitoramento JavaScript em seu aplicativo” na página 705.
4. Se estiver operando um ambiente de alta carga de transações, existem algumas etapas de ajuste avançadas que talvez você precise executar. Para obter mais informações, consulte “Configuração Avançada do Analisador de Pacotes” na página 711

Configurando o Packet Analyzer usando a janela Configuração do agente
É possível usar a janela Configuração do agente para configurar o Packet Analyzer.

Para monitorar o tráfego HTTP para um determinado sistema usando Packet Analyzer, conclua as etapas a seguir:

1. Para acessar a página do Configuração do Agente, no APM UI, selecione **Configuração do Sistema** > **Configuração do Agente** e, em seguida, selecione a guia **Tempo de Resposta**.
2. Selecione o(s) sistema(s) a ser(em) atualizado(s). Selecione vários sistemas se desejar usar as mesmas configurações de HTTP para cada um desses sistemas.

   Se os sistemas selecionados tiverem diferentes valores HTTP configurados, `Múltiplos Valores` ou `Múltiplas Listas` são exibidos em vez de valores individuais. Não é possível atualizar ao mesmo tempo sistemas com valores diferentes
3. No campo **Monitorar tráfego de HTTP?**, dê um clique duplo no valor e selecione **Sim** na lista.
4. No campo **Portas HTTP para Monitorar**, dê um clique duplo no valor e insira quaisquer portas adicionais que você deseja monitorar além da porta padrão 80 e de quaisquer outras portas já listadas.

Para parar o monitoramento de uma porta, selecione a porta que não deseja mais monitorar e clique em **Remover**.

5. Clique em **Aplicar Mudanças**.

Incluindo o componente de monitoramento JavaScript em seu aplicativo

Para ajudar a entender o desempenho das páginas da web em um navegador e os erros, o agente do Response Time Monitoring precisa estar apto a coletar dados de sincronização do navegador. Para ativar esse recurso, você deve configurar o aplicativo que deseja monitorar.

Sobre Esta Tarefa

Antes de monitorar interações em suas páginas da web, é preciso incluir o componente de monitoramento JavaScript em cada página da web para seu aplicativo. O componente de monitoramento JavaScript captura o estado de cada página da web e interações JavaScript associadas. Inclua o componente de monitoramento JavaScript no aplicativo que você deseja monitorar. O conteúdo e ações relevantes são capturados automaticamente e enviados para o Servidor Cloud APM para análise e correlação.

Procedimento

Conclua as etapas a seguir para ativar a coleta de dados de monitoramento real do usuário a partir do navegador. Estas etapas precisam ser concluídas somente uma vez, a menos que a configuração do aplicativo seja alterada.

1. Inclua o componente de monitoramento do JavaScript no aplicativo. O procedimento que você usa depende do tipo de aplicativo:
   a) Para obter uma lista de aplicativos Java EE, extraia *install_dir*/clienttime/ClientTime.war do pacote de instalação para um diretório acessível para o servidor HTTP.
   b) Para aplicativos não Java EE, como Ruby, .NET, Python e Node.js, salve o *install_dir*/clienttime/wrtInstrumentation.js do pacote de instalação em um diretório acessível para o servidor HTTP.

      Extraia o arquivo *install_dir*/clienttime/ClientTime.war em um caminho temporário. Deve-se copiar o arquivo wrtTimingTarget.dat extraído na raiz do documento. A raiz do documento é uma configuração no servidor HTTP (Apache, IIS e assim por diante). É um diretório para armazenar seus documentos. Por padrão, todas as solicitações são obtidas desse diretório, mas links simbólicos e alias podem ser usados para apontar para outros locais. Por exemplo, a raiz do documento para Apache é /opt/IBM/HTTPServer/htdocs.

      O arquivo wrtInstrumentation.js pode ser colocado em qualquer diretório. Assegure-se de atualizar a localização do caminho para o arquivo wrtInstrumentation.js no cabeçalho HTML.
2. Associe o componente de monitoramento do JavaScript com o aplicativo.

   Normalmente essa associação pode ser feita modificando um script de cabeçalho de aplicativo. Geralmente, somente um script de cabeçalho precisa ser modificado para cada componente ou aplicativo que deve ser monitorado.

   Para aplicativos Java EE e aplicativos não Java EE, inclua o seguinte JavaScript no cabeçalho do aplicativo antes de qualquer JavaScript:

   ```
   <script language="JavaScript" src="path/wrtInstrumentation.js"
   type="text/JavaScript"></script>
   ```

   em que *path* é o caminho relativo para o componente de monitoramento JavaScript

   Por exemplo:

   ```
   <script language="JavaScript" src="/ClientTime/wrtInstrumentation.js"
   type="text/JavaScript"></script>
   ```

Resultados

Páginas instrumentadas com o componente de monitoramento JavaScript são monitoradas e os dados das páginas são analisados e exibidos em painéis Transações de Usuários Finais.

Ativando a sincronização do navegador

Ao ativar o monitoramento de sincronização de recurso, o agente Response Time Monitoring processa os dados do W3C Resource Timing usando Packet Analyzer. Com essa função ativada, é possível visualizar informações detalhadas sobre o desempenho nos elementos de front-end.

Sobre Esta Tarefa

Antes de monitorar os dados de sincronização de recursos, você deve incluir o componente de monitoramento de sincronização de recursos em seu aplicativo e associar o componente de monitoramento de sincronização de recursos ao aplicativo. O componente de monitoramento de sincronização de recurso captura automaticamente o estado e as interações dos elementos front-end e envia os dados para o Servidor Cloud APM para análise. Os resultados dessa análise são exibidos no painel **Subtransações**.

Procedimento

Execute as etapas a seguir para ativar a função de monitoramento da sincronização de recursos. Execute essas etapas somente uma vez, a menos que haja mudanças na configuração do aplicativo.

1. Inclua o componente de monitoramento da sincronização de recursos no aplicativo.
   a) Extraia o arquivo *install_dir*/clienttime/wrtInstrumentation.js do pacote de instalação.
   b) Inclua o arquivo wrtInstrumentation.js no diretório do JavaScript de seu aplicativo.
2. Anexe a seguinte linha ao cabeçalho do aplicativo:

   ```
   <script> var wrt_enableResourceTiming=true; </script>
   ```

   Por exemplo,

   ```
   <script language="JavaScript" src="path/wrtInstrumentation.js"
   type="text/JavaScript"></script>
   <script> var wrt_enableResourceTiming=true; </script>
   ```

Resultados

As páginas são instrumentadas com o componente de monitoramento da sincronização de recursos. Esse componente é ativado por padrão. Os dados da sincronização de recursos nas páginas que são instrumentadas com o componente de monitoramento da sincronização de recursos são analisados e exibidos nos painéis **Subtransações**.

O que Fazer Depois

Caso deseje desativar o componente de monitoramento de sincronização de recursos, configure o parâmetro **wrt_enableResourceTiming** para false.

Monitorando transações HTTPS

O Response Time Monitoring monitora transações HTTP por padrão. Para monitorar as transações HTTPS, o Response Time Monitoring requer acesso aos Certificados SSL para que ele possa decriptografar o tráfego SSL de seus servidores da web remotos.

Antes de Iniciar

Identifique os servidores da web HTTPS a serem monitorados, incluindo seus endereços IP e portas configuradas. Por exemplo, 192.168.1.23, porta 443. Para cada servidor da web HTTPS, verifique se o

Response Time Monitoring pode ler as suas cifras. O Response Time Monitoring suporta as cifras suportadas pelo IBM Java, incluindo as cifras a seguir.

- RSA_WITH_RC4_40_MD5
- RSA_WITH_RC4_128_MD5
- RSA_WITH_RC4_128_SHA
- RSA_WITH_RC4_40_SHA
- RSA_WITH_DES40_CBC_SHA
- RSA_WITH_DESC_CBC_SHA
- RSA_WITH_3DES_EDE_CBC_SHA
- RSA_WITH_AES_128_CBC_SHA
- RSA_WITH_AES_256_CBC_SHA
- RSA_EXPORT1024_WITH_RC4_56_MD5
- RSA_EXPORT1024_WITH_RC2_CBC_56_MD5
- RSA_EXPORT1024_WITH_DES_CBC_SHA
- RSA_EXPORT1024_WITH_RC4_56_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

Restrição: Response Time Monitoring não pode decriptografar tráfego que usa Diffie-Hellman Key Exchange.

Procedimento

Para ativar o monitoramento de transação HTTPS, conclua as etapas a seguir:

1. Configure o keystore. Para obter mais informações, consulte "Configurando o keystore" na página 708.
2. Configure o agente do Response Time Monitoring, executando um dos comandos a seguir e fornecendo valores, quando solicitado:

   Exemplo:

```
Configurando o Agente de Monitoramento do Tempo de Resposta
Editar configurações do 'Agente de Monitoramento do Tempo de Resposta'? [1=Sim,2=Não](o
padrão é: 1): 1

Configuração Básica:   Especifique a configuração de monitoramento básica. Nota: o HTTP
agora é configurado centralmente usando a guia Tempo de Resposta na Configuração do Agente.

Especifica se as transações HTTPS devem ser monitoradas
Monitorar transações HTTPS [ 1=Sim, 2=Não ] (o padrão é:2): 1

Esse armazenamento de chaves contém os certificados dos websites HTTPS que estão sendo
monitorados
Keystore HTTPS (por exemplo, - /tmp/keys.kdb) (o padrão é: ): /tmp/keys.kdb

Esta tabela mapeia servidores HTTPS para os certificados adequados (por exemplo, cert1,
ip do servidor, porta do servidor; cert2, ip do servidor2, porta do servidor2);...
Mapa de certificado do servidor HTTPS (por ex., - certAlias,9.48.152.1,443;...)(o padrão
é: ):
 rótulo1,10.0.0.1,9443;rótulo1,9.185.150.71,443

Configuração Avançada:
Especificar configuração de monitoramento avançada

A placa NIC que possui o endereço IP selecionado será monitorada.
Endereço IP do NIC a ser monitorado (o padrão é: ): 10.0.0.1

Coleta de Dados e Configuração de Análise:
Especifique as informações de configuração sobre como os dados são analisados.

Configuração concluída com sucesso.
A reinicialização do agente é necessária para aplicar mudanças de configuração.
```

em que:

- Keystore HTTPS é o keystore configurado na etapa 1
- Mapa de certificado do servidor HTTPS, especifique:
  - `rótulo 1` - o rótulo chave configurado na etapa 1
  - `IP do servidor` - o endereço IP do servidor, que deve corresponder ao atributo de Origem/Destino no cabeçalho IPV4 dos pacotes
  - `porta do servidor` - número da porta do servidor, que deve corresponder ao atributo de porta de Origem/Destino no cabeçalho TCP dos pacotes

  Inclua várias entradas para várias possibilidades do IP do servidor do mesmo rótulo chave.
- Endereço IP do NIC a ser monitorado, a interface que pode ver os pacotes e é mapeada para eth0, en0, e assim por diante. O nome não precisa corresponder a qualquer atributo de IPV4 ou aos cabeçalhos de TCP dos pacotes. Se `10.0.0.1` corresponde a eth0, use `tcpdump -s0 -i eth0 ...` para ver todos os pacotes que precisam ser analisados pelo Analisador de Pacotes.

3. Reinicie o agente do Response Time Monitoring.

Configurando o keystore

Para monitorar transações HTTPS, importe chaves para o KT5Keystore para todos os servidores da web que você deseja monitorar.

Sobre Esta Tarefa

É possível exportar os certificados SSL dos servidores da web sendo monitorados e importá-los no Keystore HTTPS usando IBM Key Management (iKeyman) ou especificar o arquivo stash keystore do servidor da web (`.kdb`) no Keystore HTTPS. Ao instalar ou configurar o Response Time Monitoring, será solicitado o local do arquivo `keys.kdb`.

Se você não tiver arquivos stash de keystore (`.kdb` e `.sth`), verifique se o Provedor do CMS está ativado em sua versão Java, de forma que você possa usar o iKeyman para configurar o banco de dados de chaves:

1. Acesse o diretório *`install_dir`*`/ibm-jre/jre/lib/security`. Por exemplo:
   - Linux `/opt/ibm/apm/agent/JRE/lx8266/lib/security`
   - Windows `C:\Program Files\IBM\APM\ibm-jre\jre\lib\security`
2. No arquivo `java.security`, inclua a instrução a seguir na lista de provedores de segurança conforme mostrado; em que *number* é o último número da sequência na lista.

   ```
   security.provider.number=com.ibm.security.cmskeystore.CMSProvider
   ```

   A lista de provedores tem a seguinte aparência:

   ```
   ## List of providers and their preference orders #
   security.provider.1=com.ibm.jsse.IBMJSSEProvider
   security.provider.2=com.ibm.crypto.provider.IBMJCE
   security.provider.3=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.4=com.ibm.security.cert.IBMCertPath
   security.provider.5=com.ibm.security.cmskeystore.CMSProvider
   ...
   #
   ```

3. Salve e feche o arquivo.

Restrição: Response Time Monitoring não pode decriptografar tráfego usando Diffie-Hellman Key Exchange.

Procedimento

Para ativar o monitoramento de transação HTTPS, colete os certificados SSL dos servidores da web que deseja monitorar e importe os arquivos stash keystore e de certificado no Keystore HTTPS usando

iKeyman. O exemplo a seguir usa iKeyman para exportar os certificados de um IBM HTTP Server e para importá-los no Keystore HTTPS:

1. Instale um agente Response Time Monitoring em cada servidor da web HTTPS a ser monitorado.
2. Execute **IBM Key Management** (iKeyman) de dentro do diretório `bin` IBM Java executando um dos comandos a seguir, dependendo do seu sistema operacional.
   - AIX Linux `/opt/ibm/apm/agent/JRE/lx8266/bin/ikeyman`

     Nota: Deve-se ter X-Window no ambiente para que o iKeyman funcione corretamente.
   - Windows `c:\IBM\APM\java\java80_x64\jre\bin\ikeyman`
3. Crie um novo banco de dados de Keystore. Na caixa de diálogo **Novo**, conclua as etapas a seguir:
   a) Na lista **Tipo de banco de dados de chaves**, selecione **CMS**.

   Caso CMS não esteja disponível na lista, o Provedor CMS pode não estar ativado. Ative o Provedor CMS no arquivo de segurança Java.

   b) No campo **Nome do Arquivo**, insira o nome do Arquivo Keystore HTTPS e clique em **OK**.
   Por exemplo, `keys.kdb`.
4. Na caixa de diálogo **Prompt de Senha**, conclua as etapas a seguir:
   a) Nos campos **Senha** e **Confirmar Senha**, insira e confirme a senha para acessar o `keys.kdb`.

   Não configure um prazo de expiração, a menos que queira recriar o banco de dados de keystore e reiniciar o agente Response Time Monitoring periodicamente.

   b) Selecione **Armazenar a senha em arquivo stash?** para armazenar a senha do `keys.kdb` em um formulário criptografado em um arquivo stash, `keys.sth`.

   Nota: o agente de Tempo de Resposta suporta somente a versão 1 de senha armazenada em arquivo stash. Após o APM 8.1.4, execute o comando a seguir para armazenar a senha para keys.kdb em um arquivo stash criptografado, keys.sth.

   No Linux:

   ```
   cp keyfile.sth keyfile.sth.new-format
   ```

   ```
   cd /opt/IBM/ccm/agent/lx8266/gs/bin
   ```

   ```
   #export LD_LIBRARY_PATH=/opt/ibm/apm/agent/lx8266/gs/lib64:$LD_LIBRARY_PATH
   ```

   ```
   ./gsk8capicmd_64 -keydb -stashpw
   -db /opt/IBM/ccm/agent/keyfiles/keyfile.kdb -v1stash
   ```

   No Windows:

   ```
   copy server.sth server.sth.backup
   ```

   ```
   set PATH=c:\IBM\APM\GSK8_x64\lib64;%PATH%
   ```

   ```
   C:\IBM\APM\GSK8_x64\bin\gsk8capicmd_64 -keydb
   -stashpw -db .\server.kdb -pw passw0rd -v1stash
   ```
5. Na seção **Conteúdo do Banco de Dados de Chaves** da janela iKeyman, conclua as etapas a seguir:
   a) Selecione **Certificados Pessoais**.
   b) Clique em **Importar**.
   c) Na caixa de diálogo **Importar Chave**, na lista **Tipo de arquivo-chave**, selecione **CMS**.
   d) Navegue para o arquivo keystore e clique em **Abrir** e, em seguida, clique em **OK**.
   e) Na caixa de diálogo **Prompt de Senha**, digite a senha do keystore.
   f) Selecione uma chave na lista e clique em **OK**.

g) Na caixa de diálogo **Alterar Rótulos**, selecione o nome do rótulo da chave. No campo **Inserir novo rótulo**, especifique o nome do host do servidor e clique em **Aplicar**.

Nota: Você precisará desse valor quando configurar o Response Time Monitoring, portanto, anote-o.

h) Clique em **OK**.

6. Salve o Keystore HTTPS.

Importando Chaves dos Serviços de Informações da Internet

Para extrair chaves do Internet Information Services e importá-las para o KT5Keystore, conclua as seguintes etapas:

1. Instale um agente Response Time Monitoring em cada servidor da web HTTPS a ser monitorado.
2. Exporte um arquivo .pfx do Internet Information Services:
   a. No menu **Iniciar** do Windows, selecione **Ferramentas administrativas** > **Gerenciador de Internet Information Services (IIS)**.
   b. Selecione o servidor da web e o site cujas chaves privadas você deseja exportar, em seguida, clique com o botão direito e selecione **Propriedades** no menu de contexto.
   c. Selecione a guia **Segurança do diretório**, em seguida, selecione **Certificado do servidor** na seção **Comunicações seguras**.
   d. No **Assistente de certificado do IIS**, clique em **Avançar**.
   e. Selecione **Exportar o certificado atual para um arquivo .pfx** e clique em **Avançar**.
   f. Insira o caminho e o nome do arquivo e clique em **Avançar**.
   g. Insira uma senha de exportação para a chave e clique em **Avançar**.
   h. Clique em **Avançar** em todas as páginas subsequentes, e depois clique em **Concluir**.
3. Extraia os Certificados de Assinante e Pessoal do arquivo .pfx:
   a. Execute o **IBM Key Management** (iKeyman) a partir do diretório do IBM Java `bin` usando o comando `c:\IBM\APM\java\java80_x64\jre\bin\ikeyman`. Certifique-se de que a variável de ambiente `JAVA_HOME` esteja configurada.
   b. No Banco de dados de keystore, selecione **Arquivo** > **Abrir**.
   c. Na lista **Tipo de Banco de Dados de Chaves**, selecione **PKCS12**.
   d. Insira o nome e o caminho para o arquivo .pfx criado acima, em seguida, clique em **OK**. Quando solicitado, insira a senha, em seguida, clique em **OK**.
   e. Selecione **Conteúdo do banco de dados de chaves** > **Certificados pessoais**, em seguida, clique em **Exportar/Importar**.
   f. Selecione um tipo de ação de **Exportar chave** e um tipo de arquivo-chave de **PKCS12**. Insira um nome de arquivo e local para a chave exportada e clique em **OK**. Quando solicitado, insira uma senha de exportação, e depois clique em **OK** novamente.
   g. Se o Certificado pessoal foi assinado por uma Autoridade de certificação, selecione **Conteúdo do banco de dados de chaves** > **Certificados de assinante** e clique em **Extrair**. Selecione o tipo de arquivo padrão e digite um nome e local de arquivo para o certificado exportado, e depois clique em **OK**.
4. Extraia os arquivos `.cer` do Assinante (se necessário):
   a. Se um Certificado de Assinante foi extraído do arquivo .pfx, navegue para o diretório no qual ele foi salvo e faça uma cópia com a extensão `.cer`. Dê um clique duplo na nova cópia para abri-la usando o visualizador de Certificado do Windows.
   b. Na guia **Caminho de certificação**, é possível visualizar a cadeia de certificados de assinante. O item mais baixo na cadeia deve ser o Certificado Pessoal. Para todos os certificados acima desse, faça o seguinte:
      1) Selecione um certificado e clique em **Visualizar certificado**.

2) Selecione **Detalhes** e clique em **Copiar para Arquivo**.
3) Aceite todos os padrões no Assistente de Exportação de Certificado e insira um nome de arquivo com a extensão `.cer`.

5. Crie um novo banco de dados de Keystore. Na caixa de diálogo **Novo**, conclua as etapas a seguir:
   a. Na lista **Tipo de banco de dados de chaves**, selecione **CMS** e insira um nome de arquivo e local. Quando solicitado, digite uma senha para o novo keystore.

      Nota: Certifique-se de selecionar **Armazenar a senha em um arquivo stash**.
   b. Se Certificados de Assinante foram extraídos do arquivo .pfx, faça o seguinte:
      1) Selecione **Conteúdo do banco de dados de chaves** > **Certificados de assinante**.
      2) Para cada certificado de assinante, clique em **Incluir** e inclua o arquivo `.cer`.
   c. Selecione **Conteúdo do banco de dados de chaves** > **Certificados pessoais** e clique em **Importar**.
   d. Selecione o tipo de arquivo de chave **PKCS12**, e o nome e o local do arquivo **.p12**. Quando solicitado, digite a senha.
   e. Salve o keystore e saia do utilitário de gerenciamento de chave.
   f. Copie os arquivos `.kdb` e `.sth` para o KT5Keystore na máquina do dispositivo do Response Time Monitoring.
   g. Coloque os arquivos de banco de dados do IBM Key Management (`.kdb`) e armazene em arquivo stash (`.sth`) em um diretório seguro e certifique-se de que eles sejam legíveis apenas pelo Administrador ou `raiz` (ou o ID do usuário que foi usado para instalar o agente do Response Time Monitoring).

Configuração Avançada do Analisador de Pacotes
Existem várias opções de configuração avançada para o Analisador de Pacotes.

Depois de configurar o Analisador de Pacotes, existem várias tarefas de configuração avançada que podem ser executadas para otimizar o desempenho e recursos.

Usando balanceadores de carga
Se estiver usando balanceadores de carga em seu ambiente, alguma customização adicional é necessária.

Procedimento

Se estiver usando um balanceador de carga, siga estas diretrizes:

1. Desative a regravação de URL do balanceador de carga.
2. Instale um agente do Response Time Monitoring em cada servidor da web que deseja monitorar.

   Não instale o Response Time Monitoring no balanceador de carga.
3. Inclua o componente de monitoramento JavaScript em seu aplicativo. Para obter mais informações, consulte “Incluindo o componente de monitoramento JavaScript em seu aplicativo” na página 705.

O que Fazer Depois

Caso você esteja executando o agente do Response Time Monitoring atrás de um balanceador de carga, é possível configurar o balanceador de carga para encaminhar o endereço IP do cliente para otimizar o desempenho do monitoramento. Use as etapas a seguir como um exemplo:

1. No cabeçalho de HTTP, configure o endereço IP do cliente no campo **`X-Forwarded-For`**.
2. Configure o agente do Response Time Monitoring para usar o cabeçalho do endereço IP do cliente. Configure o cabeçalho do endereço IP do cliente no campo **`KFC_OVERRIDE_SOURCE_ADDR_HEADER`** em um dos arquivos a seguir, dependendo de seu sistema operacional:
   - AIX Linux `/opt/ibm/apm/agent/tmaitm6/wrm/kfcmenv`
   - Windows `C:\IBM\ITM\TMAITM6_x64\wrm\Analyzer\kfcmenv`

Por exemplo:

```
KFC_OVERRIDE_SOURCE_ADDR_HEADER=x-forwarded-for
```

ou se estiver usando WebSEAL:

```
KFC_OVERRIDE_SOURCE_ADDR_HEADER=iv-remote-address
```

Configurando o limite de sobrecarga da CPU

Se você estiver operando um ambiente de carga de alta transação, é possível limitar os recursos de monitoramento usados pelo agente Response Time Monitoring.

Sobre Esta Tarefa

Essa função limita o uso de CPU do agente Response Time Monitoring monitorando e relatando somente uma parte do trafego da web usando amostragem. O `limite de sobrecarga de CPU` não é configurado por padrão. Deve-se configurar o `limite de sobrecarga de CPU` no servidor onde o agente está instalado.

Procedimento

Para configurar o `limite de sobrecarga de CPU`, conclua as seguintes etapas:

1. Abra o arquivo a seguir em um editor de texto:

   Linux AIX `/opt/ibm/apm/agent/tmaitm6/wrm/kfcmenv`

   Windows `C:\IBM\ITM\TMAITM6_x64\wrm\Analyzer\kfcmenv`

2. Configure os valores para os seguintes parâmetros:

   KFC_MAX_PROTOCOL_PACKETRATE
   A taxa máxima inicial do pacote. Por exemplo, ao configurar o parâmetro como **KFC_MAX_PROTOCOL_PACKETRATE=2000**, a taxa máxima do pacote será 2.000 pacotes por segundo. Essa taxa varia de forma dinâmica, com base no valor de **KFC_CPUTHROTTLE_TARGET** e no uso atual da CPU.

   KFC_CPUTHROTTLE_TARGET
   A porcentagem do total do recurso da CPU que pode ser usada pelo processo `kfcmserver`. Por exemplo, ao configurar o parâmetro como **KFC_CPUTHROTTLE_TARGET=10.0**, o processo `kfcmserver` pode usar até 10% do total do recurso da CPU.

   Nota: O valor para o parâmetro **KFC_CPUTHROTTLE_TARGET** é a porcentagem do total do recurso da CPU que está disponível para o processo do `kfcmserver`. Por exemplo, se você tiver 4 núcleos de CPU e **KFC_CPUTHROTTLE_TARGET** estiver configurado como 10, o Monitor de Recurso em Windows mede o recurso de CPU como 400%. Como resultado, o processo `kfcmserver` pode usar até 40% do total de 400% de recursos de CPU disponíveis.

Resultados

O `limite de sobrecarga de CPU` é configurado para o agente Response Time Monitoring.

Reconfigurando o módulo Tempo de Resposta do IBM HTTP Server para o Packet Analyzer

Talvez você queira alterar seu ambiente de monitoramento do módulo Tempo de Resposta do IBM HTTP Server para o Packet Analyzer.

Procedimento

1. Desinstale o agente do servidor HTTP
   a) Edite o `/etc/httpd/conf/httpd.conf` comentando a linha do plug-in Tempo de Resposta. Por exemplo

```
#include /opt/ibm/apm/agent/tmp/khu/khu.etc.httpd.conf.httpd.conf
```

b) Desinstale o agente do servidor HTTP. Por exemplo

```
/opt/ibm/apm/agent/bin/http_server-agent.sh uninstall
```

c) Abra uma nova janela de prompt de comandos para limpar a variante do sistema antes de reconfigurar o agente de Tempo de Resposta na próxima etapa.

2. Abra o arquivo a seguir

   Linux AIX *install_dir*/config/*hostname*_t5.cfg
   Em que *install_dir* é /opt/ibm/apm/agent
   Windows *install_dir*\TMAITM6_x64*hostname*_t5.cfg
   em que *install_dir* é C:\IBM\APM

3. Defina os parâmetros como segue:

```
{ KT5DISABLEANALYZER=NO } { KT5ENABLEWEBPLUGIN=NO }
```

4. Reconfigure o agente da seguinte forma:

```
re-agent.bat config  install_dir\samples\rt_silent_config.txt
```

Customizando valores de locais de Transações do Usuário Final

É possível customizar os locais aplicados a endereços IP específicos ou a intervalos de endereços nos painéis de Transação do usuário final para seu ambiente específico.

Antes de Iniciar

Use a guia **Localização geográfica** na **Configuração do agente** para customizar valores de locais.

Use este recurso para configurar o local dos endereços IP que são exibidos no painel como **Desconhecido**. Esses endereços podem ser endereços IP internos, por exemplo, 192.168.x.x ou 10.x.x.x, ou externos que não estão resolvidos. Também é possível usar esse recurso para substituir locais incorretos para endereços IP. Por exemplo, se você souber que o endereço IP 9.1.1.1 está em Los Angeles, mas ele for mostrado como São Francisco, substitua o local e configure 9.1.1.1 para Los Angeles.

Sobre Esta Tarefa

Customize valores de locais nos painéis de Transação do usuário final fazendo upload de um arquivo CSV que contém os valores necessários. É possível localizar um arquivo CSV de amostra na guia **Localização geográfica**.

O arquivo CSV deve ter os valores a seguir como cabeçalho. Os valores podem estar em qualquer ordem e as entradas devem corresponder a essa ordem.

```
IP_ADDRESS, COUNTRY, REGION, CITY
```

Por exemplo,

```
IP_ADDRESS, COUNTRY, REGION, CITY
10.0.5.0/24, Australia, WA, Perth
10.1.0.6, Australia, VIC, Melbourne
```

É possível especificar um único endereço IPv4 ou um intervalo. Se você especificar um intervalo, certifique-se de usar um valor válido no intervalo 1-32.

Procedimento

Para customizar os valores de locais exibidos nos painéis de Transação do usuário final, conclua as etapas a seguir no Painel de desempenho do aplicativo.

1. Configure seu arquivo ou arquivos CSV com endereços IP correspondentes aos locais.
2. Fazer upload do arquivo CSV.
   a) Acesse **Configuração do agente** > **Localização geográfica**.
   b) Clique em **Fazer upload de CSV**, selecione os arquivos dos quais você deseja fazer upload e clique em **Abrir**.
      - Certifique-se de que seu arquivo CSV liste primeiro os intervalos gerais de endereços IP, antes de endereços IP mais específicos.
      - Faça upload de vários arquivos, se necessário.
      - Se os valores em um arquivo sobrepuserem os valores no outro, os valores no arquivo mais recente substituirão os valores no primeiro.
3. Expanda **Fazer upload de resultados** para verificar erros. Verifique os problemas a seguir:
   - Substitui
   - Endereços IP inválidos
   - Linhas inválidas
   - Valores com mais de 250 caracteres

Resultados
Aguarde alguns minutos e visualize seus valores customizados nos painéis de Transação do usuário final.

O que Fazer Depois

Será possível remover valores customizados se necessário. Execute uma das seguintes etapas:

- Para remover alguns dos valores customizados, selecione os endereços IP que deseja remover, clique em **Limpar entradas selecionadas** e clique em **OK** para confirmar a remoção
- Para remover todos os valores customizados, clique em **Limpar todas as entradas** e clique em **OK** para confirmar a remoção

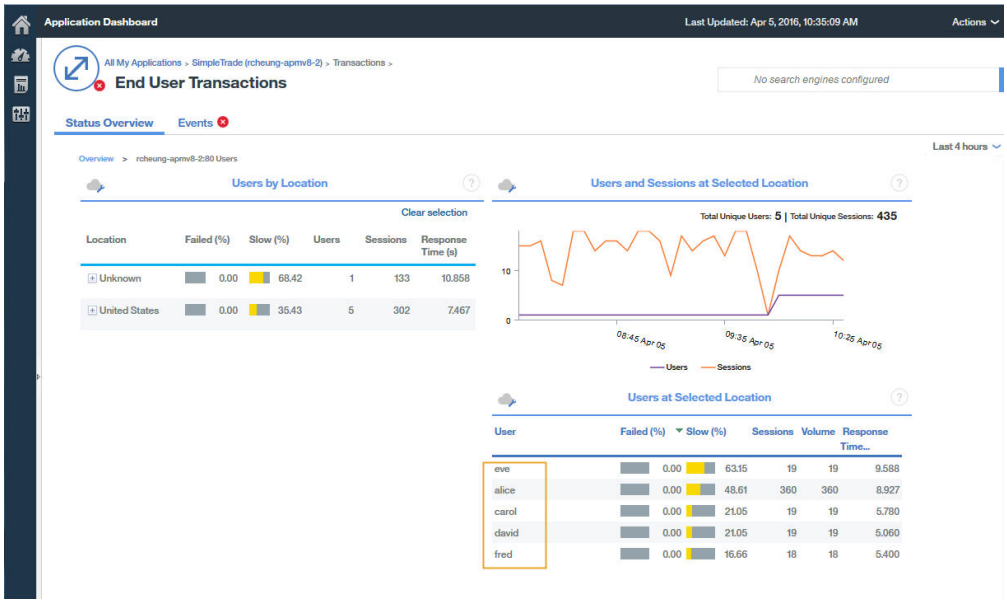
Rastreando aplicativos da web adicionais

Para rastrear aplicativos da web além daqueles rastreados por padrão, deve-se identificar e configurar métodos de rastreamento de usuário e de sessão.

Antes de Iniciar

Se seu aplicativo não é suportado pelos padrões, os painéis não conterão detalhes do usuário e da sessão, o nome do usuário será exibido como `anônimo` ou `desconhecido` e nenhuma informação de sessão estará disponível.

Se os métodos de rastreamento de usuário estiverem configurados corretamente, o ID do usuário será extraído e listado no painel **Transações do usuário final** > **Resumo do usuário** > **Usuários em locais selecionados**.



Nota: o rastreamento de usuário é baseado no rastreamento de sessão. É necessário configurar a variável de métodos de rastreamento de sessão correta primeiro, nas definições de configuração do agente de Tempo de Resposta, para os métodos de rastreamento de sessão e usuário.

Sobre Esta Tarefa

No IBM Application Performance Management V8.1.4 e posterior, é possível usar a página **Configuração do Agente** > **Tempo de Resposta** para incluir aplicativos para serem rastreados pelo Packet Analyzer ou Módulo de Tempo de Resposta do IBM HTTP Server. Os valores definidos nesta página têm precedência sobre os valores no arquivo `WRT_Defaults.xml`.

Para rastrear aplicativos adicionais, deve-se primeiro identificar os métodos e os valores de ID do usuário e de ID de sessão para o aplicativo que deseja monitorar. Por exemplo:

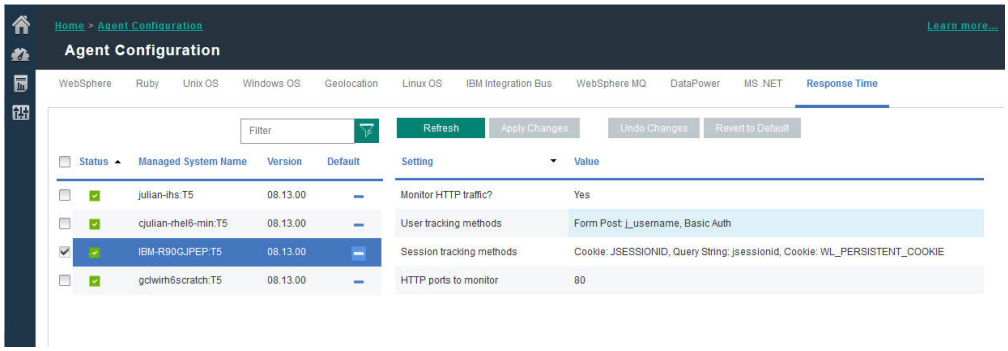
1. Abra a ferramenta do desenvolvedor para seu navegador, para que seja possível ver as solicitações para o aplicativo que deseja monitorar.
2. Selecione a última solicitação no log de rede do navegador, para que seja possível identificar sua solicitação de teste facilmente.
3. Crie uma solicitação de teste com os parâmetros que você irá reconhecer. Por exemplo, efetue login em seu website com `testuser`.
4. Selecione a solicitação de teste e observe os `Cabeçalhos`.
5. Identifique o ID de sessão no log de solicitação. O ID de sessão é geralmente especificado em `cookie`, `POST`, `request/response header` ou `query string`. Se o `cookie` já estiver definido no perfil padrão, não será necessário incluí-lo na etapa 2.
6. Identifique o ID do usuário no log de solicitação. ID do usuário pode ser especificado no conteúdo de `cookie`, `request header`, `POST` ou `query string`. Por exemplo, procure por `testuser`, que fornecerá o valor para o ID do usuário.
7. Os **Métodos de Rastreamento de Usuário** e **Métodos de Rastreamento de Sessão** devem ser atualizados com o nome do valor correto da sessão e do usuário em uso no código do aplicativo do cliente. A forma como você identifica o nome do valor da Sessão e do Nome do Usuário depende do código do aplicativo. A seguir está o valor padrão da configuração Usuário/Sessão na 8.1.4.

```
Session tracking methods=cookie\:JSESSIONID,querystring\:jsessionid,cookie\
       :WL_PERSISTENT_COOKIE
User tracking methods=formpost\:j_username,formpost\:uid,formpost\
       :ctl00%24MainContent%24uid,basicauth\:Authorization\: Basic
```

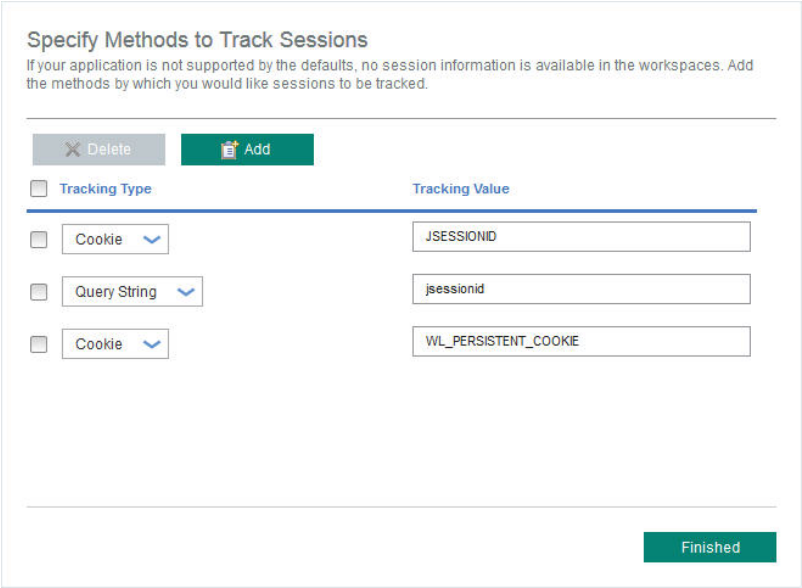
Procedimento

Após ter identificado os métodos e os valores de rastreamento de usuário e de sessão utilizados em seu aplicativo, conclua as seguintes etapas:

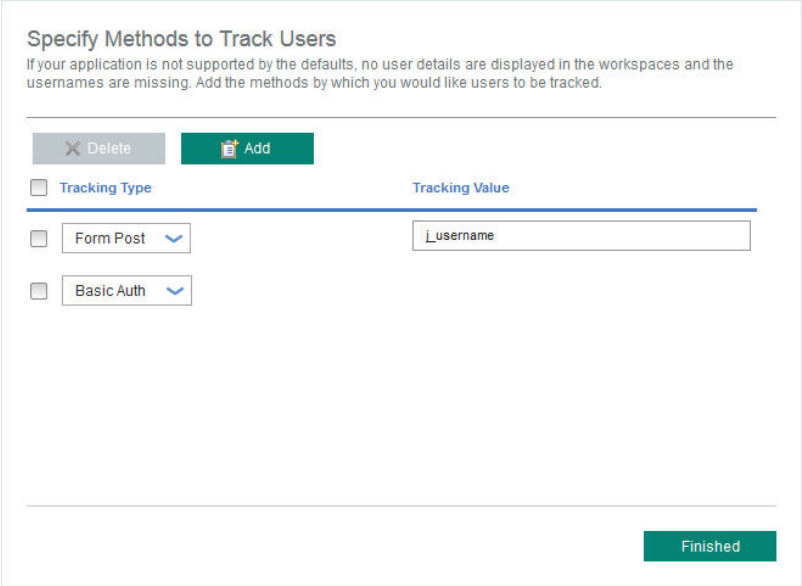
1. Acesse a página de configuração **Configuração do agente** > **Tempo de resposta**.



2. Selecione o sistema gerenciado que você deseja atualizar.
3. Se necessário, atualize os métodos de rastreamento de sessão:
   a) Clique no valor no campo **Métodos de rastreamento de sessão**.



   b) Na janela **Especificar métodos para rastrear sessões**, clique em **Incluir**.
   c) Na lista **Tipo de Rastreamento**, selecione o tipo de rastreamento. Por exemplo, `Cookie`.
   d) No campo **Valor de Rastreamento**, especifique um valor. Por exemplo, `WL_PERSISTENT_COOKIE`.
   e) Clique em **Concluído**.
4. Se necessário, atualize os métodos de rastreamento de usuário:
   a) Clique no valor no campo **Métodos de rastreamento de usuário**.



b) Na janela **Especificar métodos para rastrear usuários**, clique em **Incluir**.

c) Na lista **Tipo de Rastreamento**, selecione o tipo de rastreamento. Por exemplo, `Cabeçalho`.

d) No campo **Valor de Rastreamento**, especifique um valor. Por exemplo, `nome do usuário`.

e) Clique em **Concluído**.

5. Na página de configuração do agente, clique em **Aplicar mudanças**.

Resultados

Os aplicativos que utilizam os métodos de rastreamento recém-especificados são exibidos no Painel do aplicativo.

O que Fazer Depois

Teste se as informações de IDs e de sessões do usuário do seu aplicativo são exibidas no Painel do aplicativo.

Especificando um nome do sistema gerenciado exclusivo para o Agente Response Time Monitoring

O nome da instância do Agente Response Time Monitoring exibido no console do Cloud APM também é conhecido como o nome do sistema gerenciado (MSN). É possível usar o parâmetro de configuração do agente para especificar um MSN exclusivo para cada instância do agente.

Sobre Esta Tarefa

O nome do sistema gerenciado para o Agente Response Time Monitoring está no seguinte formato:

```
instancename:hostname:T5
```

T5 é o código do produto para o Agente Response Time Monitoring.

Procedimento

1. Pare todas as instâncias de agente existentes. Se você não tiver nenhuma instância de agente existente, avance para a próxima etapa. Para obter mais informações sobre como parar as instâncias de agente, consulte “Utilizando comandos do agente” na página 175.
2. Linux AIX Mude **`CTIRA_SUBSYSTEM_ID`** no arquivo `runagent`. Normalmente, todas as instâncias do agente em uma máquina usam o mesmo valor de nome do host.

   a) Faça uma cópia de backup do arquivo:

Linux AIX *install_dir/platform*/t5/bin/runagent

b) Edite o arquivo. Inclua *newinstancename* em sistemas Linux ou AIX.

Linux AIX **CTIRA_SUBSYSTEM_ID**=*newsubsystemid*

3. Inicie as instâncias existentes do agente.
4. Inicie o Console do Cloud APM. Modifique seus aplicativos removendo as instâncias do agente nos MSNs antigos e incluindo as novas instâncias do agente.

Configurando o monitoramento do Ruby

É possível monitorar os aplicativos IBM Cloud Ruby e no local. Para monitorar aplicativos Ruby no local, configure o Agente Ruby. Para monitorar os aplicativos IBM Cloud Ruby, configure o Coletor de dados Ruby.

Sobre Esta Tarefa

Essas direções destinam-se à liberação mais atual do agente, exceto conforme indicado.

O procedimento a seguir é um roteiro para configurar o Agente Ruby e o Coletor de dados Ruby, que inclui as etapas necessárias e opcionais. Conclua as etapas de configuração de acordo com suas necessidades.

Procedimento

- Para monitorar aplicativos Ruby no local, conclua as etapas a seguir para configurar o Agente Ruby:
  a) Configure instâncias do agente para monitorar aplicativos Ruby. Consulte Configurando o Agente Ruby para monitorar aplicativos Ruby .
  b) Instale o coletor de dados para monitorar dados para exibição no Console do Cloud APM. Consulte Instalando o coletor de dados.
  c) Opcional: Se você for um usuário do Cloud APM, Advanced, poderá concluir as seguintes tarefas de acordo com suas necessidades:
     – Para configurar o coletor de dados para coletar dados diagnósticos, consulte Configurando o coletor de dados diagnósticos.
     – Para ativar o rastreio de método para solicitações e ajustar o comprimento para o parâmetro de caminho de arquivo que é exibido no widget Rastreio de Pilha de Solicitação, consulte Ativando o rastreio de método e ajustando a exibição do caminho.
     – Para aumentar o tamanho de heap da JVM para evitar o erro de `falta de memória`, consulte Aumentando o tamanho de heap da JVM.
     – Para desativar diagnósticos, consulte Desativando ou ativando dados diagnósticos para aplicativos Ruby.
- Para monitorar os aplicativos IBM Cloud Ruby, conclua as tarefas a seguir para configurar o Coletor de dados Ruby:
  a) Configure o coletor de dados Ruby para aplicativos IBM Cloud. Para obter instruções, veja “Configurando o Coletor de dados Ruby para aplicativos IBM Cloud” na página 726.
  b) Opcional: Para mudar o comportamento do coletor de dados Ruby, consulte “Customizando os aplicativos Coletor de dados Ruby para IBM Cloud” na página 727.

Configurando o Agente Ruby

Para que o Agente Ruby monitore seus aplicativos, especifique o tempo de execução do Ruby. Como resultado, você usa o tempo de execução para reunir dados dos aplicativos Ruby e para configurar o agente.

Antes de Iniciar
Determine o servidor que você usa para iniciar aplicativos Ruby e o diretório bin qualificado para o executável Ruby ou Rake que é usado pelo agente:

1. Para determinar o servidor de aplicativos que está sendo usado, execute o seguinte comando:

   ```
   ps -ef | grep ruby
   ```

   Você vê o nome do servidor que é usado para iniciar seu aplicativo. Os possíveis nomes de servidores são listados conforme a seguir:

   - `Passageiro`
   - `Unicorn`
   - `Puma`
   - `Magro`

   Se a saída de comando não indicar os nomes de servidores que são mostrados na lista anterior, o servidor usado para iniciar o aplicativo pode ser WEBrick.

   Importante: Se você usar vários servidores da web para iniciar seus aplicativos Ruby, deverá criar uma instância de agente para cada servidor da web de aplicativo, por exemplo, uma instância para PUMA e uma para Unicorn.
2. Para determinar o diretório bin qualificado para o executável Ruby ou Rake usado pelo Agente Ruby, execute o seguinte comando:

   ```
   which ruby
   ```

Sobre Esta Tarefa
É possível repetir essa tarefa para configurar várias instâncias do agente de acordo com suas necessidades.

Procedimento

1. Para configurar o agente, execute o comando a seguir:
   install_dir`/bin/ruby-agent.sh config` *instance_name*
   em que *instance_name* é o nome que você deseja dar à instância, e *install_dir* é o diretório de instalação do Agente Ruby. O diretório de instalação padrão é `/opt/ibm/apm/agent`.

   Importante: Não especifique um nome de instância longo. O comprimento total do nome do host e do nome da instância do agente não deve exceder 28 caracteres. Se o comprimento exceder o limite, o Nome do sistema gerenciado será truncado, e o código do produto para o Agente Ruby não será exibido corretamente.

   O Nome do sistema gerenciado inclui o nome da instância especificado, por exemplo, *instance_name*`:`*host_name*`:`*pc*, em que *pc* é seu código do produto de dois caracteres para o agente. Por exemplo, se você especificar `Ruby2` como o nome da instância, o nome do sistema gerenciado será `Ruby2:hostname:KM`, em que *KM* é o código do produto de dois caracteres para o Agente Ruby.
2. Quando for solicitado a `Editar configurações do 'Monitoring Agent for Ruby'` , insira `1` para continuar.
3. Quando for solicitado o `Diretório bin completo de Rubies`, especifique o diretório binário. Por exemplo, se você usar o Ruby Version Manager (RVM), insira `/usr/local/rvm/rubies/ruby-2.0.0-p247/bin`.
4. Quando for solicitado `Detectar automaticamente a sinalização de aplicativos Ruby`, insira Y para continuar. O agente recebe os dados enviados pelo coletor de dados do agente.
5. Quando for solicitado o `Nome do processo do servidor de aplicativos`, pressione Enter para aceitar o padrão de `ruby` ou especifique o valor para o servidor usado, de acordo com a seguinte lista:

- Para servidores WEBrick, aceite o padrão ou especifique `ruby`; se o Ruby on Rails for instalado pelo Ruby Stack, especifique `.ruby.bin`.
- Para servidores Passenger, especifique `passenger`.
- Para servidores Unicorn, especifique `unicorn`.
- Para servidores Puma, especifique `puma`.
- Para servidores Thin, se os aplicativos forem iniciados executando o comando `thin start`, aceite o padrão para usar `ruby`; se os aplicativos forem iniciados executando o comando `thin start -d`, especifique `thin`; se o Ruby on Rails for instalado pelo Ruby Stack e os aplicativos forem iniciados executando o comando `thin start`, especifique `.ruby.bin`.

6. Quando for solicitada a `Origem de dados do soquete`, pressione Enter para aceitar o padrão de `0` para usar a porta efêmera.
7. Quando for solicitado a `Editar configurações do 'Aplicativo'`, insira 5 para sair da configuração.
8. Para iniciar o agente, execute o seguinte comando:
   install_dir`/bin/ruby-agent.sh start` *instance_name*

O que Fazer Depois
Instale o coletor de dados para que o Agente Ruby funcione corretamente e para que os dados sejam exibidos na UI do Cloud APM. Para obter instruções, consulte Instalando o coletor de dados

Instalando o coletor de dados
Você deve instalar o coletor de dados para o agente funcionar corretamente. Depois de instalar o coletor de dados, os dados de monitoramento são exibidos no Application Performance Dashboard.

Antes de Iniciar
Se você instalou o aplicativo Ruby on Rails em um sistema Linux usando uma conta não raiz, e planeja coletar dados diagnósticos, o usuário não raiz deverá ter acesso ao diretório inicial do coletor de dados diagnósticos. Verifique se o usuário não raiz tem acesso de leitura e gravação no diretório *install_dir*`/install-images/kkm`, em que *install_dir* é o diretório de instalação do Agente Ruby. O diretório de instalação padrão é `/opt/ibm/apm/agent`. Se necessário, forneça permissões de leitura e gravação usando o comando `chmod 777`.

Procedimento

1. Pare o seu aplicativo Ruby on Rails.
2. Opcional: Se estiver fazendo upgrade do coletor de dados Ruby para uma nova versão, primeiro você deve desinstalar o coletor de dados da versão antiga executando o seguinte comando:

   ```
   gem uninstall stacktracer
   ```

3. Instale o coletor de dados diagnósticos. Insira `gem install --local` *install_dir*`/lx8266/km/bin/stacktracer-`*version*`.gem`, em que *version* é o número da versão e *install_dir* é o diretório de instalação do Agente Ruby. O número da versão no nome do arquivo `stacktracer-`*version*`.gem` no diretório de instalação do agente indica o número da versão que precisa ser inserido aqui. O diretório de instalação padrão é `/opt/ibm/apm/agent`.

   Importante: Instale o coletor de dados como o mesmo usuário de quando for instalar e executar o aplicativo Ruby on Rails.
4. Navegue para o diretório inicial do aplicativo, abra o `Gemfile` e inclua a seguinte linha no final do arquivo: `gem 'stacktracer', '`*version*`'`
   em que *version* é o número da versão do coletor de dados. O número da versão é indicado no nome do arquivo `stacktracer-`*version*`.gem` que está no *install_dir* do Agente Ruby.
   Por exemplo, se você instalar o coletor de dados Ruby Versão 1.0 Fix Pack 8, poderá localizar um arquivo `stacktracer-01.00.08.00.gem` no diretório de instalação do agente. Em seguida, inclua a linha `gem 'stacktracer', '01.00.08.00'` em seu aplicativo para instalar o coletor de dados.

Nota: Se houver somente uma versão de `stacktracer` no ambiente, inclua a linha `gem 'stacktracer'` no final do arquivo. Não especifique o número da versão na linha.

5. No diretório inicial do aplicativo, insira `bundle install`.
6. Reinicie o seu aplicativo Ruby on Rails.

Resultados
O coletor de dados está instalado e configurado e o seu aplicativo Ruby on Rails foi iniciado.

O que Fazer Depois

- Se você não estiver com login efetuado, siga as instruções em "Iniciando o Console do Cloud APM" na página 975. Selecione **Desempenho** > **Application Performance Dashboard** para abrir o painel **Todos os Meus Aplicativos** e fazer drill down para os painéis de monitoramento de recursos e painéis de diagnósticos do Aplicativo Ruby, para observar seus aplicativos Ruby on Rails a partir do resumo do status até as instâncias de solicitações individuais.
- Para ver e modificar as configurações para o coletor de dados diagnósticos, continue com o próximo tópico, "Configurando o coletor de dados diagnósticos" na página 721.
- Para exibir dados de rastreio de método para solicitações na UI do Cloud APM, consulte Ativando o rastreio de método e ajustando a exibição do caminho.
- Quando o rastreio de método estiver ativado ou as solicitações de dados forem grandes, você pode receber erros de `falta de memória`. É possível aumentar o tamanho de heap da JVM para evitar esses erros. Consulte Aumentando o tamanho de heap da JVM.
- É possível desativar e ativar a coleta de dados diagnósticos para um ou mais aplicativos Ruby on Rails gerenciados a qualquer momento por meio do Console do Cloud APM. Consulte "Desativando ou ativando dados diagnósticos para aplicativos Ruby" na página 725. Esta função não está disponível para monitoramento de recursos.

Configurando o coletor de dados diagnósticos
Se você é um usuário do Cloud APM, Advanced, pode continuar a configurar o coletor de dados para dados diagnósticos. A coleta de dados diagnósticos é desativada por padrão no arquivo de configuração do coletor de dados.

Antes de Iniciar
Deve-se ter instalado o coletor de dados diagnósticos e suporte configurado para a coleta de dados diagnósticos, conforme descrito em "Instalando o coletor de dados" na página 720.

Sobre Esta Tarefa
O arquivo de configuração `instrumenter_settings.rb` aparece depois que o agente registra a existência de um aplicativo Ruby on Rails, configurando adequadamente o `Gemfile`. Esse arquivo de configuração pode ser modificado enquanto o agente do Ruby está em execução e as mudanças são capturadas automaticamente. Como alternativa, é possível aplicar as mudanças em todos os aplicativos Ruby on Rails que estão sendo monitorados, o que requer que os aplicativos sejam interrompidos enquanto você editar o arquivo de configuração.

Procedimento

- Para modificar as configurações do coletor de dados de um aplicativo específico que está em execução:
  1. Navegue para o diretório *`install_dir`*`/install-images/kkm/dchome/`*`appClassName`*`/config`, em que *`appClassName`* é o nome de classe do aplicativo Ruby e *`install_dir`* é o diretório de instalação do Agente Ruby. O diretório de instalação padrão é `/opt/ibm/apm/agent`.
  2. Abra `instrumenter_settings.rb` em um editor de texto.
  3. Modifique as configurações do coletor de dados:

:instrumentation_enabled
Para ativar o suporte para a coleta de dados diagnósticos, configure `:instrumentation_enabled => true`.

Para desativar o suporte para a coleta de dados diagnósticos, configure `:instrumentation_enabled => false`.

:sample_frequency
Para modificar a frequência de amostragem de solicitações, insira o número de solicitações entre amostragens.

O coletor de dados coleta dados diagnósticos somente para solicitações com amostra. Se você configurar `:sample_frequency => 10`, por exemplo, os dados são coletados para 1 em cada 10 solicitações.

:max_methods_to_instrument
Para desativar a coleta de rastreio de método ou para ativar a coleta de rastreio de método e limitar o número de métodos que são rastreados, configure o valor como zero, ou insira o número máximo de métodos para rastreio.

Para desativar a coleção de rastreios de método, configure `:max_methods_to_instrument => 0`.

Para ativar a coleção de rastreios de método, configure `:max_methods_to_instrument => 10000`. O valor poderá ser maior, mas um valor bem maior pode causar problemas de desempenho. Quando os dados do método são coletados, as chamadas para os métodos são incluídas no widget Rastreio de método do painel Rastreios de solicitação, que mostra todas as instâncias da solicitação e suas solicitações aninhadas.

:min_wallclock_to_include_in_trace
Para modificar o limite que determina se a solicitação ou o método deve ser rastreado, configure o tempo de resposta mínimo. Se você configurar `:min_wallclock_to_include_in_trace => 0.001`, por exemplo, somente as solicitações e os métodos cujos tempos de resposta são mais de 1 milissegundo serão rastreados.

Lembre-se: No painel de diagnóstico **Rastreio de solicitação**, é possível realizar drill down em uma instância de solicitação específica a partir do widget Grupo de rastreio de pilha de solicitação. Os totais de tempos de resposta para a instância podem estar incorretos devido aos filtros configurados para `:min_wallclock_to_include_in_trace` e `:min_wallclock_to_include_stacks`, que podem excluir alguns dados.

:min_wallclock_to_include_stacks
Para modificar o limite que determina se as informações de rastreio de pilha devem ser coletadas para uma solicitação ou um método, configure o tempo de resposta mínimo.

Se você configurar `:min_wallclock_to_include_stacks => 0.1`, por exemplo, as informações da rastreio de pilha são coletadas para todas as solicitações e métodos cujo tempo de resposta é mais longo do que 100 milissegundos.

:include_subclasses_of_these_modules
O painel de diagnósticos Rastreios de solicitação ajuda a identificar a sequência de chamadas para solicitações e métodos aninhados para uma instância de solicitação. O coletor de dados preventivamente filtra os métodos de classes que não estão incluídas na lista de filtros. Se as operações que você deseja rastrear não estiverem incluídas nos rastreios de pilha de método, é possível incluí-las aqui.

Para especificar os métodos para rastrear, inclua seus nomes de classes.

Considere, por exemplo, que você deseja rastrear as APIs Moped no tipo de código de Ruby a seguir:

```
session = Moped::Session.new(['ip:27017'])
session.use(:HR)
session[:profiles].insert({......})
session[:profiles].find({...}).remove
```

Inclua os nomes dos módulos dessas APIs Moped na propriedade:

```
:include_subclasses_of_these_modules => {"
ActionController" => true,
                     "ERB" => true,
                     "erb" => true,
                     "Arel" => true,
                     "Mongoid" => true,
                     "Moped" => true
                    },
```

Restrição: Os rastreios de método não incluem métodos de classes e métodos privados (métodos definidos em uma classe que têm especificados de acesso "privado" implícitos ou explícitos).

:include_sql_text
Para coletar dados de contexto para métodos, configure esta propriedade para `true`.

:num_samples_per_file
Para modificar o número máximo de solicitações rastreadas para armazenar em cada arquivo, insira um valor como `:num_samples_per_file => 1000`. Após o limite configurado aqui ser atingido, um novo arquivo será criado.

Considere configurar `:num_samples_per_file` para um valor inferior, se você ajustar a configuração de uma maneira que faça com que mais dados sejam coletados. Por exemplo, configurar `:include_subclasses_of_these_modules` para rastrear mais classes e métodos pode aumentar a coleta de dados. Configurar qualquer das propriedades a seguir para um valor inferior também pode aumentar a coleta de dados: `:sample_frequency`, `:min_wallclock_to_include_in_trace` e `:min_wallclock_to_include_stacks`.

:verbose_request_instrumentation
:verbose_class_instrumentation
:verbose_method_instrumentation
Para aumentar o nível de criação de log do coletor de dados diagnósticos, configure essas propriedades para `true`.

Dica: Se operações que você deseja especificamente para rastreio não forem incluídas nos rastreios de pilha do método, configure `:verbose_class_instrumentation => true` e verifique o log para descobrir se a classe que você deseja rastrear está instrumentada. Se não estiver instrumentada, inclua o nome da classe do nome do módulo da classe na propriedade `:include_subclasses_of_these_modules`.

4. Se você editou qualquer uma das propriedades a seguir, reinicie o aplicativo Ruby on Rails correspondente para que suas mudanças entrem em vigor:

```
:include_subclasses_of_these_modules
:max_methods_to_instrument
```

O reinício é necessário porque essas propriedades são usadas somente quando um aplicativo é ativado para determinar qual classe ou método deve ser instrumentado pelo coletor de dados Ruby.

- Para modificar as configurações do coletor de dados de todos os aplicativos Ruby on Rails, conclua estas etapas:

1. Pare qualquer aplicativo Ruby on Rails que estiver em execução no momento.
2. Remova `instrumer_settings.rb` do diretório *`install_dir`*`/install-images/kkm/dchome/`*`application_name`*`/config`.
3. Modifique as configurações do coletor de dados em *`Gem_dir`*`/gems/stacktracer-`*`version`*`/config/instrumenter_settings_template.rb` em que *version* é o número da versão, como 01.00.05.00 e *Gem_dir* é o diretório de instalação do `stacktracer-version.gem`, como `/usr/local/rvm/gems/ruby-2.1.4/`. Para obter informações adicionais, consulte a etapa “3” na página 721 no procedimento para modificar as configurações do coletor de dados de um aplicativo específico.

4. Reinicie qualquer aplicativo Ruby on Rails que estiver em execução no momento.

Resultados
A configuração do coletor de dados diagnósticos foi alterada para o aplicativo em execução que você especificou ou para todos os aplicativos.

Ativando o rastreio de método e ajustando a exibição do caminho
O IBM Cloud Application Performance Management, Advanced com dados diagnósticos permite que os usuários tenham um painel **Rastreios de solicitação**. Se dados do método forem coletados, as chamadas para os métodos são mostradas. O widget **Rastreio de método** exibe as instâncias de solicitação e suas solicitações aninhadas. É possível ativar o rastreio de método para incluir as chamadas nos métodos nas solicitações aninhadas. Também é possível ajustar a configuração do widget **Rastreio de pilha de solicitação** para mostrar mais do que o padrão de 50 caracteres de cada caminho de arquivo.

Sobre Esta Tarefa
O rastreio de método está desativado por padrão. Conclua o procedimento primeiro para ativar o rastreio de método para exibição no painel **Rastreios de solicitação**. É possível ativar o rastreio de método alterando uma configuração no arquivo de configuração.

Conclua o segundo procedimento para ajustar o número de caracteres mostrados para o caminho de arquivo no widget **Rastreio de pilha de solicitação**.

Procedimento

- Para ativar o rastreio de método, edite as configurações de `instrumenter_settings.rb`:
  a) Localize o arquivo `instrumenter_settings.rb` na instalação do Agente Ruby, por exemplo, *`install_dir`*`/install-images/kkm/dchome/`*`appClassName`*`/config` em que *`appClassName`* é o nome da classe de aplicativo Ruby e *install_dir* é o diretório de instalação do Agente Ruby. O diretório de instalação padrão é `/opt/ibm/apm/agent`.
  b) Abra `instrumenter_settings.rb` em um editor de texto.
  c) Configure a propriedade a seguir para 10000.

  ```
  max_method_to_instrument
  ```

  O valor poderá ser maior, mas um valor bem maior pode causar problemas de desempenho. (Consulte também "Aumentando o tamanho de heap da JVM" na página 725.)
  d) Reinicie os aplicativos Ruby on Rails para iniciar a coleta de dados de método.

  Para obter informações adicionais sobre todas as propriedades `instrumenter_settings.rb`, veja "Configurando o coletor de dados diagnósticos" na página 721.
- Para ajustar o tamanho de exibição do caminho do arquivo no widget **Rastreio de pilha de solicitação**, edite o arquivo `dfe.properties`:
  a) Localize o arquivo `dfe.properties` na instalação do Agente Ruby, por exemplo, *`install_dir`*`/lx8266/km/bin/dfe.properties`
  em que *install_dir* é o diretório de instalação do Agente Ruby. O diretório de instalação padrão é `/opt/ibm/apm/agent`.
  b) Abra `dfe.properties` em um editor de texto.
  c) Altere o tamanho máximo do caminho de arquivo para exibir em cada elemento de rastreio de pilha, ajustando o valor da propriedade a seguir:

  ```
  dfe.stacktrace.filepath.maxsize
  ```

  d) Reinicie o Agente Ruby.

Aumentando o tamanho de heap da JVM

Quando o rastreio de método está ativado para o painel **Rastreios de solicitação** do Ruby Diagnostics ou solicitações de dados são muito grandes, é possível aumentar o tamanho de heap da JVM para evitar erros de falta de memória.

Sobre Esta Tarefa

O Agente Ruby é um agente baseado em Java e o tamanho de heap da JVM padrão é 384 MB. Execute estas etapas para aumentar o tamanho de heap e, assim, reduzir a probabilidade da condição de falta de memória. A condição de memória insuficiente pode ocorrer a partir de solicitações de dados frequentes e quando o rastreio de método está ativado.

Procedimento

1. Localize a configuração do tamanho de heap da JVM no diretório de instalação do Agente Ruby, por exemplo, `install_dir/lx8266/km/bin/runDeepDiveClient.sh`
   Em que *install_dir* é o diretório de instalação do Agente Ruby. O diretório de instalação padrão é `/opt/ibm/apm/agent`.

   O valor padrão é `-Xmx384m`.
2. Aumente o valor, por exemplo, para 1024 MB, como mostrado em `-Xmx1024m`:
   ```
   export JAVA_OPT="-Djlog.common.dir=$CANDLEHOME/logs -DCONFIG_DIR=
   $DC_RUNTIME_DIR -Dkqe.cache.interval=60 -Xmx1024m -Dkqe.timespan=900 -
   Djlog.propertyFileDir.CYN=$CANDLEHOME/$ITM_BINARCH/$PRODUCT_CODE/bin"
   ```
3. Reinicie o Agente Ruby.

Desativando ou ativando dados diagnósticos para aplicativos Ruby

Se você tiver um IBM Cloud Application Performance Management, Advanced, poderá usar a página **Configuração do agente** no Console do Cloud APM para desativar ou ativar a coleta de dados diagnósticos a qualquer momento para um ou mais sistemas gerenciados.

Antes de Iniciar

- É necessário ter o Cloud APM, Advanced em seu ambiente.
- Você deve instalar e configurar o Monitoring Agent for Ruby em uma máquina virtual, conforme descrito em "Instalando agentes" na página 122 nos sistemas AIX ou "Instalando agentes" na página 130 nos sistemas Linux e em "Configurando o monitoramento do Ruby" na página 718.
- Instale o coletor de dados diagnósticos e configure o suporte para a coleta de diagnósticos, conforme descrito em "Instalando o coletor de dados" na página 720.

Sobre Esta Tarefa

Após a configuração do suporte para dados diagnósticos na configuração do coletor de dados, a coleta de dados diagnósticos é desativada por padrão para cada sistema gerenciado. Para exibir dados nos painéis de diagnósticos, é necessário ativar a coleta de dados diagnósticos para cada sistema gerenciado que estiver monitorando.

Execute estas etapas para ativar e desativar a coleta de dados diagnósticos para cada sistema gerenciado:

Procedimento

1. Na barra de navegação, selecione **Configuração do Sistema->Configuração do Agente**.
   A página **Configuração do Agente** é exibida.
2. Clique na guia **Ruby**.
3. Selecione as caixas de seleção dos sistemas gerenciados nos quais você deseja desativar ou ativar a coleta de dados diagnósticos.

4. Na lista **Ações**, selecione uma das opções a seguir para desativar ou ativar a coleta de dados diagnósticos para os sistemas gerenciados selecionados:
   - Selecione **Desativar coleta de dados**. O status na coluna `Coletor de dados ativado` é atualizado para `Não` para cada sistema gerenciado selecionado.
   - Selecione **Ativar coleta de dados**. O status na coluna `Coletor de dados ativado` é atualizado para `Sim` para cada sistema gerenciado selecionado.

Resultados
Você configurou a coleta de dados diagnósticos para cada um dos sistemas gerenciados selecionados.

Configurando o Coletor de dados Ruby para aplicativos IBM Cloud

Para coletar informações sobre aplicativos Ruby no IBM Cloud, deve-se configurar o Coletor de dados Ruby.

Antes de Iniciar

1. Faça download do pacote coletor de dados no website do IBM Marketplace. Para obter instruções detalhadas, consulte "Fazendo download de seus agentes e coletores de dados" na página 101.

Procedimento

1. Extraia os arquivos do pacote do coletor de dados. O pacote `ruby_datacollector_8.1.4.0.tgz` é incluído no diretório extraído.
2. Extraia os arquivos no `ruby_datacollector_8.1.4.0.tgz` executando o seguinte comando:

   ```
   tar -zxf ruby_datacollector_8.1.4.0.tgz
   ```

   Você obtém uma pasta `ibm_ruby_dc`.
3. Copie todo os conteúdo da pasta `etc` em `ibm_ruby_dc` para a pasta raiz do aplicativo Ruby executando o comando a seguir:

   ```
   cp –r directory to the etc folder  home directory of your Ruby application
   ```

   O comando a seguir extrai o coletor de dados no diretório `/opt/ibm/ccm/ibm_ruby_dc/etc` e o diretório inicial do seu aplicativo Ruby é `/root/ruby_app/`:

   ```
   cp –r /opt/ibm/ccm/ibm_ruby_dc/etc /root/ruby_app/
   ```
4. Inclua a seção a seguir no `Gemfile`, na pasta inicial do seu aplicativo Ruby:

   ```
   gem 'logger',  '>= 1.2.8'
   source 'https://maagemserver.ng.bluemix.net/' do
     gem 'ibm_resource_monitor'
     gem 'stacktracer'
   end
   ```
5. Execute o comando `bundle lock` para gerar novamente o arquivo `Gemfile.lock`.
6. No diretório que contém o arquivo `manifest.yml` do aplicativo Ruby, execute o seguinte comando:

   ```
   cf push
   ```

   Dica: Para obter um arquivo `manifest.yml` de amostra, consulte "Arquivo manifest.yml de amostra" na página 186.

Resultados
O coletor de dados é configurado e está conectado ao Servidor Cloud APM.

O que Fazer Depois

É possível verificar se os dados de monitoramento de seu aplicativo IBM Cloud são exibidos no Console do Cloud APM. Para obter instruções sobre como iniciar o Console do Cloud APM, consulte Iniciando o console do Cloud APM. Para obter informações sobre o uso do Editor de aplicativos, consulte Gerenciando aplicativos.

Customizando os aplicativos Coletor de dados Ruby para IBM Cloud

É possível incluir variáveis de ambiente na interface com o usuário (IU) do IBM Cloud para customizar o monitoramento de seu aplicativo IBM Cloud. Use as seguintes informações para incluir as variáveis de acordo com suas necessidades.

Variáveis de ambiente definidas pelo usuário para o Coletor de dados Ruby

É possível usar as informações na tabela a seguir para customizar o monitoramento do Ruby no IBM Cloud.

Tabela 198. Variáveis de ambiente definidas pelo usuário suportadas para monitoramento do Ruby no IBM Cloud

Nome de variável	Importância	Valor	Descrição
APM_BM_GATEWAY_URL	Opcional	• https://*<server ip or hostname>*:443 • http://*<server ip or hostname>*:80	A URL de gateway do servidor no local de destino.
APM_KEYFILE_PSWD	Opcional	Senha criptografada do arquivo-chave	A senha do arquivo-chave criptografado que é pareada com o arquivo-chave. Caso seja um usuário do Linux, você poderá usar o comando `echo -n <keyfile password> | base64` para criptografar sua senha. **Nota:** Configure essa variável somente quando tiver configurado o Gateway para usar HTTPS.
APM_KEYFILE_URL	Opcional	http://*<hosted http server>*:*<port>*/keyfile.p12	A URL para fazer download do arquivo-chave. **Nota:** Configure essa variável somente quando configurar o Gateway para usar HTTPS.

Tabela 198. Variáveis de ambiente definidas pelo usuário suportadas para monitoramento do Ruby no IBM Cloud (continuação)

Nome de variável	Importância	Valor	Descrição
kkm_instrumentation_enabled	Opcional	• verdadeiro • false	Ativa ou desativa a coleta de dados diagnósticos. true: se você configurar o valor como `true`, os dados diagnósticos serão coletados. false: se você configurar o valor como `false`, os dados diagnósticos não serão coletados. O valor padrão é `true`.
kkm_max_methods_to_instrument	Opcional	Número máximo de métodos que são rastreados	O número máximo de métodos que são rastreados. É possível desativar o rastreio de método configurando o valor como `0`. Por padrão, o valor é `10000` e o rastreio de método é ativado. **Nota:** É recomendável não configurar o valor como maior que 10000. Um valor muito mais alto que 10000 pode reduzir a eficiência de execução do aplicativo.
kkm_sample_frequency	Opcional	Frequência de solicitações de amostragem	O número de solicitações das quais uma solicitação de amostra é obtida, por exemplo, se você configurar o valor como `10`, os dados de monitoramento serão coletados para uma em cada 10 solicitações. O valor padrão é `10`.
kkm_min_wallclock_to_include_in_trace	Opcional	Limite de tempo de resposta para coletar rastreio de método, em segundos	Se o tempo de resposta de uma instância de solicitação exceder o valor dessa variável, o coletor de dados coletará seu rastreio de método. Se você configurar como 0,001, por exemplo, as solicitações e os métodos cujo tempo de resposta for maior que 1 milissegundo serão rastreados. O valor padrão é `0`, que significa que o rastreio de método está ativado para todas as solicitações e métodos.

Tabela 198. Variáveis de ambiente definidas pelo usuário suportadas para monitoramento do Ruby no IBM Cloud (continuação)

Nome de variável	Importância	Valor	Descrição
kkm_min_wallclock_to_include_stacks	Opcional	Limite de tempo de resposta para coletar rastreio de pilha, em segundos	Se o tempo de resposta de uma instância de solicitação exceder o valor dessa variável, o coletor de dados coletará seu rastreio de pilha. Se você configurar como 0,001, por exemplo, as solicitações e os métodos cujo tempo de resposta for maior que 1 milissegundo serão rastreados. O valor padrão é `0`, que significa que o rastreio de pilha está ativado para todas as solicitações e métodos.

Desconfigurando o Coletor de dados Ruby para aplicativos IBM Cloud
Se não precisar monitorar o ambiente Ruby ou se desejar fazer upgrade do Coletor de dados Ruby, primeiro você deve desconfigurar configurações anteriores para o Coletor de dados Ruby.

Procedimento

1. Acesse a pasta raiz do aplicativo.
2. Remova as seguintes linhas do `Gemfile` na pasta inicial de seu aplicativo Ruby:

```
gem 'logger',  '>= 1.2.8'
source 'https://maagemserver.ng.bluemix.net/' do
  gem 'ibm_resource_monitor'
  gem 'stacktracer'
end
```

3. Execute o comando `bundle lock`.
4. No diretório inicial do aplicativo, execute o seguinte comando para enviar novamente por push o aplicativo para o IBM Cloud para que as mudanças entrem em vigor.

```
cf push
```

Resultados
Você desconfigurou o Coletor de dados Ruby com sucesso.

O que Fazer Depois
Depois de desconfigurar o coletor de dados, o Console do Cloud APM continua a exibir o coletor de dados em quaisquer aplicativos nos quais você incluiu o coletor de dados. O Console do Cloud APM mostrará que nenhum dado está disponível para o aplicativo e não indicará que o coletor de dados está off-line. Para obter informações sobre como remover o coletor de dados de aplicativos e de grupos de recursos, consulte “Removendo coletores de dados do Console do Cloud APM” na página 186.

Configurando o monitoramento do SAP

Para monitorar um sistema SAP, o Monitoring Agent for SAP Applications deve se conectar a um servidor de aplicativos no sistema a ser monitorado, para que o agente possa acessar o código ABAP (Advanced Business Application Programming) que é fornecido com o produto.

Antes de Iniciar

- Revise os pré-requisitos de hardware e de software, consulte Agente do Software Product Compatibility Reports for SAP
- O agente SAP não suporta sistemas SAP não Unicode.

Sobre Esta Tarefa

O Agente SAP é um agente de múltiplas instâncias; você deve criar a primeira instância e iniciar o agente manualmente.

- Para configurar o agente em sistemas Windows, é possível usar a janela **IBM Performance Management** ou o arquivo de resposta silencioso.
  - "Configurando o agente nos sistemas Windows" na página 730
  - "Configurando o agente usando o arquivo de resposta silencioso" na página 732
- Para configurar o agente em sistemas Linux ou AIX, é possível executar o script e responder aos prompts ou usar o arquivo de resposta silencioso.
  - "Configurando o agente em sistemas Linux ou AIX" na página 731
  - "Configurando o agente usando o arquivo de resposta silencioso" na página 732

Depois de instalar o agente SAP, é possível importar o transporte Advanced Business Application Programming (ABAP) no sistema SAP, para oferecer suporte à coleta de dados no sistema SAP. Para obter mais informações, consulte "Importando o transporte do ABAP no sistema SAP" na página 737.

Depois de configurar o agente SAP, verifique a configuração do agente. Para obter mais informações, consulte "Verificando a configuração do agente" na página 745.

Depois de configurar o agente SAP, é possível incluir o número da Porta de comunicação do banco de dados necessário para conformidade OSLC (Open Source Lifecycle Collaboration). Para obter mais informações, consulte "Incluindo o número da porta de comunicação do banco de dados" na página 749.

Para excluir o transporte do ABAP a partir do sistema SAP, deve-se importar o transporte de exclusão para o sistema SAP. Para obter mais informações, consulte "Excluindo o transporte do ABAP a partir do sistema SAP" na página 744.

O novo design do CCMS é ativado por padrão. A entrada está presente na tabela de banco de dados / IBMMON/ITM_CNGF para o parâmetro isnewccmsdesign , cujo valor é configurado para YES.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte o "Histórico de Mudanças" na página 50.

Configurando o agente nos sistemas Windows

É possível configurar Agente SAP em sistemas Windows usando a janela **IBM Performance Management** para que o agente possa coletar dados do SAP Applications Server que está sendo monitorado.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique no botão direito em **Modelo** sob a coluna **Tarefa/Subsistema** e clique em **Configurar usando padrões**.

   A janela **Monitoring Agent for SAP Applications** é aberta.
3. No campo **Inserir um nome de instância exclusivo**, digite um nome de instância do agente e clique em **OK**.

Importante: O nome da instância de agente deve corresponder ao identificador do sistema (SID) de 3 dígitos do SAP Applications Server gerenciado. Por exemplo, se o SID do SAP Applications Server gerenciado for PS1, insira PS1 como o nome da instância.

4. Configure o Agente SAP no modo Application Server ou no modo Grupo de Logon.
   - Conclua as seguintes etapas para configurar o Agente SAP no modo Application Server:
     a. No campo **Modo de Conexão**, selecione **Modo Servidor de Aplicativos** e clique em **Avançar**.
     b. Na área **Especificar Informações do Servidor de Aplicativos**, especifique valores para os parâmetros de configuração e clique em **Avançar**.
     c. Na área **Especificar informações de logon no sistema SAP**, especifique valores para os parâmetros de configuração e clique em **OK**.

     Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração do agente" na página 733
   - Conclua as seguintes etapas para configurar o Agente SAP no modo Grupo de Logon:
     a. No campo **Modo de Conexão**, selecione **Modo Grupo de Logon** e clique em **Avançar**.
     b. Na área **Especificar Informações do Grupo de Logon**, especifique valores para os parâmetros de configuração e clique em **Avançar**.
     c. Na área **Especificar informações de logon no sistema SAP**, especifique valores para os parâmetros de configuração e clique em **OK**.

     Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração do agente" na página 733

   Importante: Para o modo Servidor de aplicativos, é obrigatório configurar a instância de diálogo que possui o dispatcher no sistema SAP no qual o servidor de mensagens ou o ASCS está configurado. Para o modo Grupo de logon, não é obrigatório configurar a instância de diálogo que possui o dispatcher no sistema SAP no qual o servidor de mensagens ou ASCS está configurado.
5. Na janela **IBM Performance Management**, clique com o botão direito na instância do agente criada e clique em **Iniciar**.

   Importante: Se desejar criar outra instância do Agente SAP, repita as Etapas 1 a 6. Use um identificador exclusivo do sistema para cada instância do Agente SAP que você deseja criar.

O que Fazer Depois

- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.
- Deve-se editar a situação `R3_Alert_Crit` predefinida e a situação `R3_Alert_Warn` para configurar a condição do atributo Status de Alerta como `Alert Status!= DONE` para que essas situações não sejam acionadas para alertas CCMS encerrados.

Configurando o agente em sistemas Linux ou AIX

É possível configurar o Agente SAP nos sistemas Linux ou AIX para que o agente possa coletar dados do SAP Applications Server que está sendo monitorado.

Procedimento

1. Na linha de comandos, mude o caminho para o diretório de instalação do agente.
   Exemplo: `/opt/ibm/apm/agent/bin`
2. Execute o comando a seguir em que instance_name é o nome que deseja dar à instância:

   `./sap-agent.sh config` *`instance_name`*

   Importante: O nome da instância de agente deve corresponder ao identificador do sistema (SID) de 3 dígitos do SAP Applications Server gerenciado. Por exemplo, se o SID do SAP Applications Server gerenciado for PS1, insira PS1 como o nome da instância.

3. Quando a linha de comandos exibir a mensagem a seguir, insira 1 e pressione Enter: `Edit 'Monitoring Agent for SAP Applications' setting? [1=Yes, 2=No]`
4. Configure o Agente SAP usando o modo Application Server ou o modo Grupo de Logon.
   - Conclua as seguintes etapas para configurar o Agente SAP no modo Application Server:
     a. Quando a linha de comandos exibir a seguinte mensagem, digite 1 e pressione Enter: `Connection Mode [ 1=Application Server Mode, 2=Logon Group Mode ]`
     b. Especifique valores para os parâmetros de configuração.

     Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração do agente" na página 733
   - Conclua as seguintes etapas para configurar o Agente SAP no modo Grupo de Logon:
     a. Quando a linha de comandos exibir a seguinte mensagem, digite 2 e pressione Enter: `Connection Mode [ 1=Application Server Mode, 2=Logon Group Mode ]`
     b. Especifique valores para os parâmetros de configuração.

     Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração do agente" na página 733

   Importante: Para o modo Servidor de aplicativos, é obrigatório configurar a instância de diálogo que possui o dispatcher no sistema SAP no qual o servidor de mensagens ou o ASCS está configurado. Para o modo Grupo de logon, não é obrigatório configurar a instância de diálogo que possui o dispatcher no sistema SAP no qual o servidor de mensagens ou ASCS está configurado.
5. Execute o seguinte comando para iniciar o Agente SAP:

   `./sap-agent.sh start` *`instance_name`*

   Importante: Se desejar criar outra instância do Agente SAP, repita as Etapas 1 a 5. Use um identificador exclusivo do sistema para cada instância do Agente SAP que for criada.

O que Fazer Depois

- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.
- Deve-se editar a situação `R3_Alert_Crit` predefinida e a situação `R3_Alert_Warn` para configurar a condição do atributo Status de Alerta como `Alert Status!= DONE` para que essas situações não sejam acionadas para alertas CCMS encerrados.

Configurando o agente usando o arquivo de resposta silencioso

É possível configurar Agente SAP em sistemas Windows, Linux ou AIX usando o arquivo de resposta silencioso.

Procedimento

1. Em um editor de texto, abra o arquivo `sap_silent_config.txt` que está disponível no caminho *`install_dir`*`\samples` e especifique valores para todos os parâmetros de configuração.

   Windows `C:\IBM\APM\samples`

   Linux AIX `/opt/ibm/apm/agent/samples`

   Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração do agente" na página 733
2. Na linha de comandos, mude o caminho para o diretório bin:

   Windows *`install_dir`*`\BIN`

   Linux AIX *`install_dir`*`\bin`
3. Execute o seguinte comando:

Windows `sap-agent.bat config instance_name install_dir\samples\sap_silent_config.txt`

Linux AIX `sap-agent.sh config instance_name install_dir\samples\sap_silent_config.txt`

Importante: O nome da instância de agente deve corresponder ao identificador do sistema (SID) de 3 dígitos do SAP Applications Server gerenciado. Por exemplo, se o SID do SAP Applications Server gerenciado for PS1, insira PS1 como o nome da instância.

4. Inicie o agente.

   Windows Na janela **IBM Performance Management**, clique com o botão direito na instância do agente criada e clique em **Iniciar**.

   Linux AIX Execute o seguinte comando: `./sap-agent.sh start instance_name`

   Importante: Se desejar criar outra instância do Agente SAP, repita as Etapas 1 a 4. Use um identificador exclusivo do sistema para cada instância do Agente SAP que for criada.

O que Fazer Depois

- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.
- Deve-se editar a situação `R3_Alert_Crit` predefinida e a situação `R3_Alert_Warn` para configurar a condição do atributo Status de Alerta como `Alert Status!= DONE` para que essas situações não sejam acionadas para alertas CCMS encerrados.

Parâmetros de configuração do agente

Quando você configura o Agente SAP, é possível mudar o valor padrão dos parâmetros, como o nome do host e o número do sistema SAP.

A tabela a seguir contém descrições detalhadas dos parâmetros de configuração do Agente SAP.

Tabela 199. Nomes e descrições dos parâmetros de configuração do Agente SAP

Nome de parâmetro	Descrição	Campo obrigatório	Exemplos
Nome do Host SAP (Primário)	O nome do host do servidor de aplicativos SAP ao qual o agente se conecta. Caso os servidores SAP se comuniquem por meio de uma LAN privada, os computadores que hospedam os servidores têm duas ou mais placas de rede. Para o nome do host, insira um nome pelo qual o servidor de aplicativos pode ser alcançado de sistemas externos, como o logon SAPGUI. Não use o nome do host da LAN privada. O valor padrão é o nome do host no qual o agente está instalado.	Sim	`saphost.domain.com`
Número do Sistema SAP (Primário)	O sistema SAP de dois dígitos ou número de instância usado para conexão com um servidor host SAP. O valor padrão é 00.	Sim	
Nome do Host SAP (Alternativo 1)	A segunda opção de nome de host, caso o host primário esteja indisponível.	Não	
Número do Sistema SAP (Alternativo 1)	O número do sistema para o nome do host do primeiro alternativo.	Não	

Tabela 199. Nomes e descrições dos parâmetros de configuração do Agente SAP (continuação)

Nome de parâmetro	Descrição	Campo obrigatório	Exemplos
Nome do Host SAP (Alternativo 2)	A terceira opção para o nome do host se os hosts Nome do Host SAP (Primário) e Nome do Host SAP (Alternativa 1) estiverem indisponíveis.	Não	
Número do Sistema SAP (Alternativo 2)	O número do sistema para o nome do host do segundo alternativo.	Não	
Número do Cliente SAP	O número do cliente SAP do logon de RFC para SAP. O valor padrão é 000. Se o usuário IBMMON_AGENT que é gerado por ABAP for usado, insira o número do cliente especificado na importação de transporte. Esse número é o mesmo que o número do cliente nnn sob o perfil.	Sim	
ID do Usuário do SAP	O ID de usuário SAP para o logon RFC para SAP. O valor padrão é IBMMON_AGENT, que é o ID do usuário predefinido que é criado durante a importação.	Sim	
Senha de Usuário SAP	Use a senha padrão ou especifique uma senha diferente.	Sim	
Confirmar Senha do Usuário do SAP	A senha especificada no campo **Senha do Usuário do SAP**.	Sim	

Tabela 199. Nomes e descrições dos parâmetros de configuração do Agente SAP (continuação)

Nome de parâmetro	Descrição	Campo obrigatório	Exemplos
Código de Idioma SAP	O código de idioma que indica o idioma usado pelo agente ao se conectar ao sistema SAP. A linguagem especificada determina o idioma no qual você vê informações SAP, como mensagens de alerta, mensagens de syslog e mensagens do log de tarefa. Todos os sistemas SAP são fornecidos em inglês e alemão. Se você precisar de um idioma diferente, confirme com seu administrador SAP se o idioma está instalado no sistema SAP. Se você especificar um idioma que não seja suportado, o agente não poderá se conectar ao sistema SAP. Os seguintes idiomas e códigos são suportados: • CS - Tcheco • EN - Inglês • FR - Francês • DE - Alemão • HU - Húngaro • IT - Italiano • ES - Espanhol • JA - Japonês • KO - Coreano • PL - Polonês • PT - Português • RU - Russo • ZH - Chinês • ZF - Chinês tradicional	Sim	
Rastreio RFC	A configuração de rastreio Remote Function Call (RFC) para a variável *SAPTRACE*. Ao marcar esse caixa de seleção, você ativa o rastreio RFC e o valor padrão será nenhum rastreamento RFC. Para a linha de comandos, 2 = Não executar rastreio e 1 = Executar rastreio. Como o rastreio RFC gera informações de diagnóstico extensivas, utilize-o cuidadosamente. Para obter mais informações sobre o rastreio RFC, entre em contato com o suporte IBM.	Não	
Grupo de Logon SAP	O nome do grupo de logon do SAP Server.	Sim	
Nome do Servidor de Mensagens SAP	O nome do host do servidor de mensagens SAP.	Sim	

Tabela 199. Nomes e descrições dos parâmetros de configuração do Agente SAP (continuação)			
Nome de parâmetro	**Descrição**	**Campo obrigatório**	**Exemplos**
Serviço de Mensagens SAP	O nome do serviço no qual o servidor de mensagens SAP está localizado. Inclua nomes de serviço nos arquivos de serviços do sistema operacional a seguir: • `/etc/services` • `\windows\system32\drivers\etc \services`	Sim	Você pode usar o nome do serviço de mensagens sapmsTV1 ou o número da porta de serviço de mensagem completo 3601.
Sequência de Rota SAP	Especifique uma sequência de roteador SAP se desejar acessar o servidor SAP com um roteador SAP.	Não	A sequência do roteador `/H/host/H/` deve estar no seguinte formato: `/H/ beagle/H/ brittany/H/` ou `/H/ amsaix11.tivlab. raleigh.ibm.com/W / tivoli/H/amsaix25`
SNC	Especifique se você deseja ativar ou desativar o Secure Network Communications (SNC). O valor padrão é desativado.	Sim	**sap_conn.sap_snc_ mode** =`true` ou `false`
Nível de segurança de SNC	O nível de segurança de SNC.	Sim	**sap_snc_mode1.sap _snc _qop**=*QOP value*. O valor padrão é 8.
Nome do SNC de cliente ou agente	O nome do SNC do cliente ou agente.	Sim	**sap_snc_mode1.sap _snc _client**= *Client SNC Name*
Nome de SNC do parceiro ou do SAP Server	O nome de SNC do parceiro ou SAP Server.	Sim	**sap_snc_mode1.sap _snc _server**= *Server SNC Name*
Caminho de Cryptolibrary do SAP	O caminho do SAP Cryptolibrary.	Sim	**sap_snc_mode1.sap _snc _library**= *Crypto library path*

Nome do host SAP é cortado de acordo com o limite de comprimento do Nome do Sistema Gerenciado

O `Nome do Sistema Gerenciado` de qualquer recurso publicado no console do APM é limitado a 32 caracteres. O Agente SAP suporta o corte de nomes de domínio para formar o `Nome do Sistema Gerenciado` dentro do limite.

Cenário 1

O `Nome do Sistema Gerenciado` para o subnó do tipo **Sys** possui o seguinte formato:

SID-DBHOST:**Sys**
Em que:

- O *SID* é o ID do sistema SAP.
- O *DBHOST* é o nome do host do sistema SAP.

Por exemplo:
Sabendo que *SID* é **P27** e *DBHOST* é **VPT02F90.mycorporation.co.in**, o nome completo do domínio (FQDN) do Nome do Sistema Gerenciado formado seria **P27-VPT02F90.mycorporation.co.in:Sys**.

Quando o Nome do Sistema Gerenciado tem mais de 32 caracteres, o Agente SAP corta o nome do domínio para formar o Nome do Sistema Gerenciado **P27-VPT02F90:Sys**. O Nome do Sistema Gerenciado cortado do subnó será publicado no console do APM.

Nota: Se o comprimento do Nome do Sistema Gerenciado que inclui o nome do domínio for menor que ou igual a 32 caracteres, o FQDN do Nome do Sistema Gerenciado não será cortado. O FQDN do Nome do Sistema Gerenciado é publicado no console do APM de acordo.
Quando necessário para atender ao limite de comprimento do Nome do Sistema Gerenciado, o corte do nome do domínio é aplicável a todos os tipos de subnó publicados pelo Agente SAP.

Cenário 2

O Nome do Sistema Gerenciado para o subnó da instância de agente **mySAP** tem o seguinte formato:

$SAPSYSTEMNAME-$dbhost:*$CTIRA_HOSTNAME*:**mySAP**
Em que:

- O *$SAPSYSTEMNAME* é o nome da instância de agente fornecido durante a configuração.
- O *$dbhost* é o nome do host do sistema SAP.
- O *$CTIRA_HOSTNAME* é o nome do host da máquina do agente.

Por exemplo:
Sabendo que *$SAPSYSTEMNAME* é **SA2**, *$dbhost* é **VPT02F90. mycorporation.co** e *$CTIRA_HOSTNAME* é **mysap1-v27.mycorp.co**, o nome completo do domínio (FQDN) do Nome do Sistema Gerenciado formado seria **SA2-VPT02F90.mycorporation.co.in: mysap1-v27:mySAP**.

Nota: O nome de domínio padrão do nome do host da máquina do agente é cortado e passa a ser **mysap1-v27**.

O Nome do Sistema Gerenciado tem mais de 32 caracteres. Primeiro, o Agente SAP corta o nome do domínio do nome do host do sistema SAP para formar **SA2-VPT02F90:mysap1-v27:mySAP**.
Se o Nome do Sistema Gerenciado resultante continuar excedendo 32 caracteres, o Agente SAP cortará os caracteres finais do nome do host da máquina do agente para formar o Nome do Sistema Gerenciado dentro do limite de 32 caracteres. Depois, o Nome do Sistema Gerenciado do subnó é publicado no console do APM.

Importando o transporte do ABAP no sistema SAP

É possível instalar um Agente SAP para cada sistema SAP para o qual for importada a solicitação de transporte ABAP (Advanced Business Application Programming) para oferecer suporte à coleta de dados no sistema SAP.

Antes de Iniciar

Antes de importar o transporte do ABAP no sistema SAP, assegure-se de que os pré-requisitos a seguir sejam atendidos:

- Para importar a solicitação de transporte do produto, é necessário usar o R3trans Versão 01.07.04 ou posterior, porque o Dynpro e as tabelas Exportação e Importação são incompatíveis. A operação básica do agente não é afetada pelos problemas de incompatibilidade do Dynpro ou de Exportação e Importação; somente as janelas de configuração do SAP são afetadas.

- Deve-se assegurar que o transporte do Agente SAP V7.1.1 seja importado no cliente em que a configuração MAI está disponível para monitorar o Solution Manager System. Para visualizar recursos do sistema PI, importe o transporte do Agente SAP V7.1.1 no sistema PI em um cliente em que a configuração PI esteja disponível.
- Para visualizar dados nos widgets de grupo que estão sob o subnó do SLM, execute as configurações de MAI para o PI e para o Solution Manager. Configure também o monitoramento de processos de negócios para que seja possível visualizar dados no widget de grupo Alertas do BPM. Para visualizar dados para o widget de grupo Alertas Críticos e de Prioridade Alta, faça as seguintes configurações:
  - No Solution Manager 7.1, execute a transação SOLMAN_SETUP e selecione **Monitoramento do sistema**, ative ou permita o componente de terceiro e inclua **Implementação: definição de BADI para reações de alertas** e conector de terceiro.
  - Configure o filtro de escopo como **Todos os Alertas e Métricas**.
  - Assegure-se de que o estado de Implementação seja **Ativo**.

  Para obter mais informações, consulte as Notas do Online Service System (OSS) a seguir, que incluem uma lista de níveis de pacotes de serviços do SAP necessários:
  - Nota do OSS 454321
  - Nota do OSS 330267
  - Nota do OSS 743155
- Para monitorar os sistemas SAP, o Agente SAP precisa de dados estatísticos do SAP. Nos sistemas SAP 7.0, é necessário configurar o fuso horário do sistema SAP para corresponder ao fuso horário do sistema operacional, para que as estatísticas do SAP sejam coletadas com os registros de data e hora corretos. Da mesma forma, atualize o fuso horário do sistema SAP para o Agente SAP para que o agente possa coletar dados. Para obter mais informações sobre esse problema, consulte o Note 926290 do SAP.

Sobre Esta Tarefa
Para obter informações sobre a importação do transporte SAP, consulte “Importando o transporte do SAP” na página 740.

Pré-requisitos relacionados ao Alerta MAI para importar o transporte ABAP
Deve-se verificar os pré-requisitos relacionados ao Alerta MAI antes de importar o transporte ABAP.

Definições de configuração no arquivo `transport.prop`

Ao usar o novo mecanismo de busca de Alerta MAI que inclui a busca de Alertas MAI sem configurar definições de notificação por e-mail e sem implementação BAdi, deve-se modificar a definição de configuração a seguir no arquivo `transport.prop`.

Inclua a linha SPLEVEL=X, em que X é o nível de pacote de suporte (SP) do sistema Solution Manager.

Por exemplo, se o ID do sistema for S10 e o nível do pacote de suporte for 13, inclua SPLEVEL=13.

Importante: Para o sistema SAP com o SP nível 10, ou mais recente, o valor do atributo Nome Técnico (MEA) não é preenchido no widget de grupo Alertas MAI mais recentes com a classificação 'Vermelho' no SAP Solution Manager Dashboard quando os Alertas MAI forem buscados sem a configuração da notificação por e-mail no SAP Solution Manager e sem a implementação de BAdi. O valor do atributo Nome Técnico (MEA) é preenchido no widget de grupo Alertas MAI mais recentes com a classificação 'Vermelho' no SAP Solution Manager Dashboard quando os Alertas MAI forem buscados, configurando a notificação por e-mail no SAP Solution Manager e na implementação de BAdi.

Determinação do mecanismo antigo e novo para a busca de Alertas MAI com base no nível do Pacote de Suporte (SP) do Solution Manager

Mecanismo de busca de Alerta MAI antigo
Esse mecanismo é baseado na definição de configurações de notificação por e-mail e na implementação de BAdi /IBMMON/ITM_IMPL_ALRTINBX com a interface IF_ALERT_DYN_COFIGURATION para coletar Alertas MAI e enviá-los ao Agente SAP.

Novo mecanismo de busca de Alerta MAI
Esse mecanismo é baseado na busca de Alertas MAI sem configurar definições de notificação por e-mail e sem a implementação BAdi /IBMMON/ITM_IMPL_ALRTINBX com a interface IF_ALERT_DYN_COFIGURATION.

É possível usar a tabela a seguir para entender o uso do arquivo `transport.prop` e sua dependência da configuração de definições de notificação por e-mail.

Tabela 200. Uso do arquivo transport.prop e suas dependências

Nível de SP do sistema SAP	**Configurações transport.prop**		**Configuração de definições de notificação por e-mail**	**Mecanismo de Alerta MAI a ser usado**
	MAI_ CONFIGURADO	**Solution Manager nível de SP**		
Qualquer	Não ou o arquivo não existe	Não Aplicável	Configurado ou não configurado	O subnó SLM não aparece; em vez disso, aparece o subnó SOL.
SP 6 a 9	Sim	Mencionado	Configurada	Mecanismo antigo
SP 6 a 9	Sim	Não mencionado	Configurada	Mecanismo antigo
SP 6 a 9	Sim	Não mencionado	Não Configurado	O mecanismo antigo não funciona porque a configuração de definições de notificação por e-mail é obrigatória.
SP 6 a 9	Sim	Mencionado	Não Configurado	O mecanismo antigo não funciona porque a configuração de definições de notificação por e-mail é obrigatória.
SP 10 ou mais recente	Sim	Mencionado	Configurada	Novo mecanismo
SP 10 ou mais recente	Sim	Mencionado	Não Configurado	Novo mecanismo
SP 10 ou mais recente	Sim	Não mencionado	Configurada	Mecanismo antigo

Tabela 200. Uso do arquivo transport.prop e suas dependências (continuação)				
Nível de SP do sistema SAP	**Configurações transport.prop**		**Configuração de definições de notificação por e-mail**	**Mecanismo de Alerta MAI a ser usado**
	MAI_ CONFIGURADO	**Solution Manager nível de SP**		
SP 10 ou mais recente	Sim	Não mencionado	Não Configurado	O mecanismo antigo não funciona porque a configuração de definições de notificação por e-mail é obrigatória.

Importando o transporte do SAP
O Agente SAP fornece um conjunto de rotinas Advanced Business Application Programming (ABAP) para suportar a coleta de dados no sistema SAP. Esse código ABAP é fornecido como um transporte SAP que deve ser instalado em cada sistema SAP a ser monitorado. O administrador do SAP instala o transporte.

Sobre Esta Tarefa

O perfil de autorização **ZITM_610AUTH** e a função de autorização **ZITM_610AUT** são válidos somente até a liberação 6.1. A partir da liberação 6.2 ou posterior, é utilizado o perfil de autorização **/IBMMON/ AUTH**. Para que haja proteção contra a utilização não autorizada, o código ABAP instalado no sistema SAP não é visível a partir do sistema SAP. Além disso, esse código não pode ser modificado nem gerado. É preciso acessar o website de suporte de software IBM para obter o suporte para esse código.

Além de instalar o código do ABAP, o transporte também instala elementos de texto de idioma traduzidos para fornecer suporte multicultural para elementos de texto de transporte do SAP.

Importante: Antes de importar o transporte para o sistema SAP, você não deve iniciar a instância do Agente SAP que é configurada para monitorar o sistema SAP.

Quando você importa o transporte do SAP, os usuários são implicitamente definidos no sistema SAP.

Use esse procedimento para importar o transporte do SAP para o sistema SAP.

Procedimento

1. Copie o arquivo de transporte do IBM Tivoli Monitoring dos caminhos a seguir no computador em que o agente está instalado.
   - Para o Windows: *install_dir*\TMAITM6_x64\ABAP
   - Para não Windows: *install_dir*/*intrp*/sa/ABAP, em que *intrp* deve ser **lx8266** ou **aix526**.
2. Copie os arquivos de transporte a seguir a partir dos caminhos mencionados na etapa 1 para o ambiente do SAP:
   - K711_00xxxU.ITM e R711_00xxxU.ITM

     Esses arquivos são versões Unicode do transporte. Eles contêm o código ABAP do Agente SAP e o suporte Unicode para sequências de texto para páginas de código Latim e páginas de código de byte duplo.
   - K711_00xxx_DELETE.ITM e R711_00xxx_DELETE.ITM

     Esses arquivos removem o código ABAP. O transporte DELETE não precisa ser importado, a menos que você pare o uso do produto inteiramente e deseje remover os transportes dos sistemas SAP. Consulte o “Excluindo o transporte do ABAP a partir do sistema SAP” na página 744.
3. Copie seus arquivos de transporte para o diretório de dados do Sistema de Transporte SAP conforme a seguir e não altere o nome do arquivo de transporte:

   Transporte Unicode

a. Copie o arquivo K711_00xxxU.ITM para o diretório cofiles
b. Copie o arquivo R711_00xxxU.ITM para o diretório data.

4. Para instalar o único arquivo de transporte do IBM Tivoli Monitoring no sistema SAP, selecione uma das opções de importação do arquivo a seguir:
   - Para o sistema SAP que é um nível do Solution Manager 7.1 Service Pack 6 ou posterior e tem MAI configurado, deve-se criar o arquivo transport.prop no diretório de trabalho usr/sap/SID/DVEBMGS*instancenumber*/work do sistema SAP. Se o sistema SAP for um sistema distribuído com ABAP SAP Central Services (ASCS), crie o arquivo transport.prop no diretório usr/sap/SID da Instância Central (CI). Em seguida, inclua a entrada MAI_CONFIGURED = YES nesse arquivo. Essa entrada cria uma entrada MAI_CONFIGURED = YES na tabela /IBMMON/ITM_CNFG. É possível agora importar o único arquivo de transporte do IBM Tivoli Monitoring no sistema SAP.

     Nota: Antes de importar o único arquivo de transporte do IBM Tivoli Monitoring, deve-se criar o arquivo transport.prop no diretório de trabalho usr/sap/SID/DVEBMGS*instancenumber*/work do sistema SAP e incluir a entrada MAI_CONFIGURED = YES nesse arquivo. Não se deve editar a entrada na tabela /IBMMON/ITM_CNFG.
   - Para todos os outros sistemas SAP com versão de base igual a 7.0 ou posterior e Solution Manager V7.1 sem configuração MAI, deve-se importar diretamente o único arquivo de transporte do IBM Tivoli Monitoring.
5. Execute o comando a seguir para importar o transporte do SAP:

```
tp addtobuffer ITMK711_00xxxU SID
pf=\usr\sap\trans\bin\PROFILE_NAME
```

   Em que:

   SID
   ID do sistema SAP de destino.

   PROFILE_NAME
   Nome do perfil do tp. Certifique-se de que o arquivo de parâmetro do tp atual seja especificado ao importar os arquivos de transporte do agente da linha de comandos. O arquivo de parâmetro do tp é normalmente denominado TP_DOMAIN_*SID*.PFL. Esse nome de arquivo faz distinção entre maiúsculas e minúsculas em sistemas UNIX.

   nnn
   Número do cliente de destino no qual o agente é executado e para o qual o ID do usuário, IBMMON_AGENT, o perfil de autorização e /IBMMON/AUTH, são definidos.

   Como alternativa, é possível usar a transação STMS do SAP para importar as solicitações de transporte ITMK711_00xxxU.ITM. Certifique-se de que as opções a seguir sejam selecionadas na guia **Opções de Importação** da janela **Importar Solicitação de Transporte**.

   - **Deixar Solicitação de Transporte na Fila para Importação Posterior**
   - **Importar Solicitação de Transporte Novamente**
   - **Sobrescrever Originais**
   - **Sobrescrever Objetos nos Reparos Não Confirmados**

   Para a versão Base do SAP, se a opção **Ignorar Versão de Componente Inválida** estiver ativada, assegure-se de que ela esteja selecionada.

Resultados
Dependendo de seu nível da liberação do SAP, quando você executa o comando **tp import**, pode receber o código de retorno 4, o que não indica um problema. Receber o código de retorno 4 é um resultado esperado do comando **import**.

Usuários e autorizações requeridos pelo Agente SAP
Para proteger contra o acesso não autorizado ao sistema SAP, é possível designar autorizações a um usuário que efetue login no sistema SAP. Essas autorizações definem os níveis de acesso para um usuário no sistema SAP.

Depois de importar o transporte ABAP, o agente SAP cria o ID de usuário padrão como IBMMON_AGENT no sistema SAP com a senha padrão como ITMMYSAP. Esse usuário é um usuário do sistema e o perfil de autorização /IBMMON/AUTH está associado ao usuário. O perfil /IBMMON/AUTH e o usuário IBMMON_AGENT são criados após a importação do transporte ABAP. Com o perfil /IBMMON/AUTH, o usuário IBMMON_AGENT pode acessar transações que são necessárias para ler dados de desempenho do sistema SAP. Alguns exemplos de transações que são usadas são os seguintes:

- Alertas e administração do CCMS
- Autorização para monitoramento de mensagens PI/XI
- Autorizações do Solution Manager

É possível criar qualquer outro usuário de tipo do sistema para o agente. Ao usuário deve ser designado o perfil /IBMMON/AUTH.

Para visualizar e acessar dados de componentes SAP, certifique-se de que o usuário criado para o agente tenha todas as autorizações especificadas na seguinte tabela:

Tabela 201. A Lista de Autorizações

Componentes	Objetos de autorização	Descrição da autorização
Autorizações gerais do sistema que incluem os seguintes componentes: • Instância do SAP • Sistema SAP	S_ADMI_FCD	Para acessar o sistema SAP
	S_BDS_DS -BC-SRV-KPR-BDS	Para acessar o conjunto de documentos
	S_BTCH_JOB	Para executar operações em tarefas de segundo plano
	S_CCM_RECV	Para transferir dados do repositório do sistema central
	S_C_FUNCT	Para fazer chamadas de função C kernel nos programas ABAP
	S_DATASET	Para acessar arquivos
	S_RFC	Para verificar o acesso ao RFC. O objeto de autorização S_RFC contém as duas subautorizações a seguir: • RFC1: Para fornecer as autorizações para o grupo de função RFC1. • SDIFRUNTIME: Para fornecer as autorizações para o grupo de função SDIFRUNTIME.
	S_RFCACL	Para verificar autorização para usuários de RFC
	S_RZL_ADM	Para acessar a administração do Computing Center Management System (CCMS) for R/3 System
	S_TCODE	Para verificar autorizações para iniciar as transações que estão definidas para um aplicativo
	S_TOOLS_EX	Para exibir registros de estatísticas externas em ferramentas de monitoramento
Autorizações para PI que incluem o SAP Process Integration	S_XMB_MONI	Para acessar o monitoramento de mensagens XI

Tabela 201. A Lista de Autorizações (continuação)		
Componentes	**Objetos de autorização**	**Descrição da autorização**
Autorizações para MAI que incluem o SAP Solution Manager	AI_DIAGE2E	Para restringir funções de E2E Diagnostics
	AI_LMDB_OB	Para acessar objetos Landscape Management Database (LMDB)
	SM_MOAL_TC	Para controlar o acesso à funcionalidade de alerta e monitoramento no SAP Solution Manager
	SM_WC_VIEW	Para restringir o acesso a elementos da UI específicos em centros de trabalho do Solution Manager
	S_RFC_ADM	Para controlar direitos para administrar destinos de RFC
	S_RS_AUTH	Para especificar autorizações de análise em uma função
	SM_APPTYPE	Para acessar o tipo de aplicativo Solution Manager
	SM_APP_ID	Para acessar aplicativos fornecidos em centros de trabalho

Excluindo o transporte do ABAP a partir do sistema SAP

Se você optar por remover o Agente SAP de seu sistema, deve-se importar o transporte delete para o sistema SAP. O transporte Delete exclui os objetos de dicionário e os módulos de funções do Agente SAP.

Antes de Iniciar

Antes de você excluir o transporte do sistema SAP, deve parar a instância do Agente SAP que está configurada para monitorar o sistema SAP.

Se o sistema SAP for da versão 7.20 ou posterior, antes de importar o transporte Delete, em seu perfil de transporte, inclua o seguinte parâmetro do perfil de transporte: **`tadirdeletions=true`**. Esse parâmetro do perfil de transporte está disponível no tp versão 375.57.68 e também no R3trans versão 6.14 liberação 700 ou superior. Para obter mais informações sobre como remover solicitações de transporte do sistema SAP, consulte Excluindo solicitações de transporte.

Procedimento

1. Acesse o seguinte caminho:
   - Para o Windows: *install_dir*\TMAITM6_x64\ABAP
   - Para não Windows: *install_dir*/*intrp*/sa/ABAP, em que *intrp* deve ser **`lx8266`** ou **`aix526`**.
2. Copie os arquivos de transporte para o ambiente SAP.
3. Copie os arquivos K711_00xxx_DELETE e R711_00xxx_DELETE para o diretório de dados do Sistema de Transporte do SAP, conforme a seguir:
   a) Copie o arquivo K711_00xxx_DELETE para o diretório `cofiles`.
   b) Copie o arquivo R711_00xxx_DELETE para o diretório `data`.
4. Execute o comando a seguir para importar o transporte delete:

a) **tp addtobuffer ITMK711_00xxx_DELETE SID pf=\usr\sap\trans\bin***PROFILE_NAME*

b) **tp import ITMK711_00xxx_DELETE SID client=nnn U16 pf=\usr\sap\trans\bin** *PROFILE_NAME* em que:

SID
ID do sistema SAP de destino.

PROFILE_NAME
Nome do perfil do tp.

nnn
Número do cliente de destino no qual o agente deve ser executado.

Verificando a configuração do agente

Depois de instalar o Agente SAP, você deve verificar a configuração do agente fazendo download, copiando e verificando a biblioteca do NetWeaver RFC SDK V7.20. Deve-se também verificar a configuração do Solution Manager V7.1 com MAI_Monitoring, verifique Alertas MAI e verifique a definição de configuração específica para o componente de terceiro.

Para verificar a configuração do agente, execute os seguintes procedimentos:

- "Fazendo download da biblioteca NetWeaver RFC SDK V7.20" na página 745
- "Copiando a biblioteca NetWeaver RFC SDK V7.20 na configuração do agente SAP" na página 746
- "Verificando a biblioteca NetWeaver RFC SDK V7.20" na página 746
- "Verificando a configuração do Solution Manager V7.1 com Monitoramento MAI" na página 747
- "Verificando Alertas MAI" na página 748
- "Verificando definições de configuração específicas para o componente de terceiro" na página 748

Fazendo download da biblioteca NetWeaver RFC SDK V7.20

Faça download da biblioteca NetWeaver RFC SDK V7.20 depois de concluir a instalação do agente SAP. Todos os arquivos relacionados à biblioteca NetWeaver RFC SDK V7.20 estão disponíveis para download no website do SAP.

Procedimento

1. Efetue login no SAP Marketplace, usando a seguinte URL: http://service.sap.com
2. Clique em **Portal do suporte ao SAP**.
3. Insira o nome de usuário e a senha do Service Marketplace.
4. Clique em **Downloads de software** e expanda o link **Pacotes e correções de suporte**.
5. Clique em **Procurar em nosso catálogo de downloads** e, em seguida, clique em **Componentes adicionais**.
6. Clique em **SAP NetWeaver RFC SDK** e, em seguida, clique em **SAP NetWeaver RFC SDK 7.20**.
7. Selecione o sistema operacional no qual está o agente SAP.
8. Faça download do arquivo `*.SAR` em seu computador.
9. Para extrair o arquivo SAP `Netweaver RFC SDK *.SAR`, usando o utilitário SAPCAR fornecido pelo SAP, execute o seguinte comando:
   `sapcar -xvf SAP NetWeaver RFC SDK File Name.SAR`

   Nota: É possível fazer download do utilitário SAPCAR no website do SAP.
10. Navegue para a pasta `lib` dentro da pasta extraída.

O que Fazer Depois

Copie a biblioteca NetWeaver RFC SDK V7.20 na configuração do agente SAP.

Copiando a biblioteca NetWeaver RFC SDK V7.20 na configuração do agente SAP

A biblioteca NetWeaver RFC SDK V7.20 contém arquivos que devem ser copiados manualmente no local da configuração do agente SAP.

Procedimento

1. Navegue para o diretório no qual você transferiu por download a biblioteca NetWeaver RFC SDK V7.20.
2. Copie os arquivos para o local da configuração do agente SAP.
   - Para sistemas operacionais Windows de 64 bits, você deve copiar os arquivos a seguir:
     - `icuin34.dll`
     - `libicudecnumber.dll`
     - `libsapucum.dll`
     - `icudt34.dll`
     - `icuuc34.dll`
     - `sapnwrfc.dll`

     Deve-se copiar os arquivos para o local `install_dir\TMAITM6_x64`.
   - Para sistemas operacionais diferentes do Windows, deve-se copiar os arquivos para o local `install_dir/`*`intrp`*`/sa/lib`, em que *intrp* é o código do sistema operacional (aix526, li6263, sol606). Copie os seguintes arquivos:
     - `libsapnwrfc.so`
     - `ibicudecnumber.so`
     - `ibicuuc34.a`
     - `libicui18n34.a`
     - `libicudata34.a`
     - `libsapucum.so`

O que Fazer Depois

Verifique a versão da biblioteca NetWeaver RFC SDK V7.20 que é transferida por download.

Verificando a biblioteca NetWeaver RFC SDK V7.20

Você deve verificar a versão do arquivo depois de copiar o arquivo extraído.

Procedimento

- Windows Para verificar a versão do arquivo, conclua as seguintes etapas:
  a) Clique com o botão direito em `sapnwrfc.dll` e clique em **Propriedades**.
  b) Clique na guia **Versão**.
  c) Na seção **Versão do Produto**, certifique-se de ter a versão a seguir: 720, correção 514, lista de mudanças 1448293, ou posterior.
- Linux AIX Para verificar a versão do arquivo, conclua as seguintes etapas:
  a) Acesse a pasta `lib` no arquivo `*.SAR` extraído.
  b) Execute o seguinte comando: **`strings libsapnwrfc.so | grep SAPFileVersion`**
  c) Você deverá ver a seguinte mensagem: `[root@IBMSAP2V6 lib]# strings libsapnwrfc.so | grep SAPFileVersion GetSAPFileVersion #[%]SAPFileVersion: 7200, 514, 22, 6206 .GetSAPFileVersion`

  Nota: A mensagem mostra que essa biblioteca tem a versão 720 correção 514, ou posterior.

Verificando a configuração do Solution Manager V7.1 com Monitoramento MAI

Para receber dados de Alertas MAI, verifique se o Solution Manager V7.1 está configurado corretamente.

Sobre Esta Tarefa

É possível usar o Solution Manager V7.1 com a Infraestrutura de Monitoramento e Alertas MAI para monitorar os sistemas gerenciados. O Solution Manager V7.1 monitora a si mesmo e os sistemas satélites. Cada sistema satélite tem um plug-in e agentes de diagnósticos. Agentes de diagnósticos buscam dados para os níveis de Host ou Sistema Operacional. Cada host pode ter vários agentes de diagnósticos para diferentes Solution Managers monitorando o host. A seguir são mostradas as palavras-chave usadas no Monitoramento MAI do Solution Manager:

- Métricas: Dados dos sistemas satélite.
- Alertas: Notificações baseadas em alguns cruzamentos de valores limites que podem ser configurados.
- Incidente: Alertas que são convertidos em chamados e designados a qualquer usuário.

Para verificar a configuração do Solution Manager V7.1 com o monitoramento MAI, verifique as configurações básicas, as configurações em nível global e as configurações em nível de modelo.

Procedimento

1. Para verificar as configurações básicas, insira o Código de Transação: SOLMAN_SETUP e clique em **Enter**.

   Assegure-se de que todos os LEDs estejam verdes nas guias a seguir:

   - Visão Geral
   - Configuração Básica
   - Configuração do Sistema Gerenciado

   Nota: Existem diferentes categorias de Sistemas Gerenciados, como Sistemas Técnicos, Cenários Técnicos, Host, Banco de dados, Instância, Domínio PI, Componente Técnico e Conexão. Configure esses Sistemas Gerenciados de acordo com as necessidades de negócios. Os Alertas MAI são baseados nos Sistemas Gerenciados configurados.
2. Insira o código de Transação: SE38 e clique em **Enter**.
3. Forneça o nome do programa como RTCCTOOL e execute o relatório.

   Assegure-se de que todos os LEDs estejam verdes no resultado.
4. Para verificar as configurações de nível global, insira o código de Transação: SOLMAN_WORKCENTER e clique em **Enter**.

   Assegure-se de que todos os LEDs estejam verdes nas guias a seguir:

   - Visão Geral
   - Configurar Infraestrutura
   - Pré-requisitos
   - Configurar
5. Verifique se as **Configurações Globais** para **Notificação** têm o status **Ativo**.
6. Para verificar as configurações no nível de modelo, insira o Código de Transação: SOLMAN_SETUP e clique em **Enter**.

   Em **Configurações Técnicas**, na lista **Notificações Automáticas**, assegure-se de que **Ativo** esteja selecionado.

   Nota: Para a resolução de problemas inicial, assegure-se de que as notificações por email estejam ativas.
7. Para o monitoramento de sistema MAI, verifique a configuração de End-User Experience Monitoring (EEM), usando as seguintes etapas:

   a) Insira o código de Transação: SE37 e pressione **Enter**.

   b) Insira **AI_EEM_LIST_ALL_SCENARIOS** no campo **Nome do Módulo de Função** e pressione F8.

Deve haver uma entrada para End-User Experience Monitoring (EEM).

Verificando Alertas MAI
Para assegurar-se de que o MAI do Solution Manager esteja configurado corretamente para monitorar a Caixa de Entrada de Alertas MAI, deve-se verificar se recebe Alertas MAI como resultado.

Procedimento

1. Insira o código de Transação SOLMAN_WORKCENTER e clique em **Enter**. Verifique se é possível visualizar Alertas MAI na Caixa de Entrada de Alertas MAI do Solution Manager, em Monitoramento Técnico.
2. Verifique a implementação BAdi, usando as seguintes etapas:
   a) Insira o código de Transação: SE19 e clique em **Enter**
   b) Insira /IBMMON/ITM_IMPL_ALRTINBX no campo **Implementação de Aprimoramento**.
   c) Clique em **Exibir** e verifique se a implementação BAdi está ativa na seção **Comportamento de Tempo de Execução**.
3. Verifique se o banco de dados /IBMMON/ITM_ALIX contém Alertas MAI, usando as seguintes etapas:
   a) Insira o código de Transação: SE16 e pressione **Enter**.
   b) No campo **Nome da Tabela**, insira /IBMMON/ITM_ALIX e execute-o. Assegure-se de estar recebendo Alertas MAI na tabela.
4. Insira o código de Transação: SE37 e clique em **Enter**.
5. No campo **Nome do Módulo de Função**, insira /IBMMON/ITM_MAIALRT_INX e pressione F8.
   Deve-se ver Alertas MAI como resultado.

O que Fazer Depois
Caso não seja possível visualizar Alertas MAI no banco de dados /IBMMON/ITM_ALIX, verifique as configurações no Componente de Terceiros.

Verificando definições de configuração específicas para o componente de terceiro
Se você não puder visualizar Alertas MAI, então, deverá verificar as configurações no componente de terceiro.

Procedimento

1. Verifique se o Componente de Terceiros está ativo.
2. Verifique se o **Adaptador de S.O.**, em **Implementação BAdi**, **Reação ao Alerta** está disponível. Caso a **Reação ao Alerta** não esteja disponível, remova as configurações padrão e selecione **Implementação BAdi - Reação ao Alerta**.
3. Verifique as configurações de modelo, usando as seguintes etapas:
   a) Verifique as configurações utilizadas para transferir alertas específicos para o Sistema de Terceiros, como SAP ABAP 7.0.0.
   b) Selecione **Modo Especializado**, selecione **Alertas** e, em seguida, clique em **Componente de Terceiros**.
      Assegure-se de que seja possível visualizar o nome BAdi de Reação ao Alerta.
      Nota: Assegure-se de que as notas SAP mais recentes estejam implementadas. Para o Solution Manager V7.1 Service Pack 8, verifique se as notas a seguir estão implementadas:
      - https://service.sap.com/sap/support/notes/1959978
      - https://service.sap.com/sap/support/notes/1820727
4. Caso não seja possível visualizar Alertas MAI no banco de dados /IBMMON/ITM_MAIALRT_INX, execute as seguintes etapas de configurações MAI do Solution Manager para o Componente de Terceiros:
   a) Insira o código de Transação: SOLMAN_SETUP e clique em **Enter**.

b) Em **Monitoramento Técnico**, selecione **Monitoramento do Sistema**.

c) Clique na guia **Configurar Infraestrutura** e, em seguida, clique na guia **Configurações Padrão**.

d) Clique na guia **Componentes de Terceiros** e, em seguida, clique em **Editar**.

e) Selecione **Ativo** na lista.

f) Assegure-se de que o filtro de escopo esteja configurado como **Todos os alertas, Eventos e Métricas (com Eventos Internos)** para o conector selecionado.

Nota: O Adaptador de Comandos do S.O. é um dos métodos para enviar dados por push para o conector de terceiros. Para configurar o Adaptador de Comandos do S.O., leia as definições de detalhes de configuração no Guia de Instruções do Adaptador de Comandos do S.O..

Incluindo o número da porta de comunicação do banco de dados

Um número de porta de comunicação do banco de dados é essencial para identificar com exclusividade a entidade do banco de dados nos cenários integrados. Para conseguir a colaboração entre componentes, os componentes do SCM AI incluíram OSLC (Open Source Lifecycle Collaboration). Na conformidade OSLC, é essencial identificar os componentes de colaboração exclusivamente. Portanto, o número da Porta de comunicação de banco de dados é importante.

Sobre Esta Tarefa

Quando você importa o transporte relevante do IBM Tivoli Monitoring para o Sistema SAP, a tabela de banco de dados `/IBMMON/ITM_PORT` é criada automaticamente. A tabela contém os campos de banco de dados a seguir:

- ID do sistema
- Nome do host do sistema
- Nº da porta de comunicação do BD (banco de dados)

Procedimento

Para incluir o número da Porta de comunicação do banco de dados SAP para o Agente SAP que é exigido para conformidade de OSLC, execute as etapas a seguir:

1. Acesse o Código de transação SE16 e pressione Enter.
2. No campo **Nome da tabela de banco de dados**, insira `/IBMMON/ITM_PORT` e pressione F7.
3. Quando a tela de seleção da tabela de banco de dados **/IBMMON/ITM_PORT** aparecer, pressione F8.

   A tabela de banco de dados **/IBMMON/ITM_PORT** contém os três campos do banco de dados a seguir:

   - ID do sistema
   - Nome do host do sistema
   - Nº da porta de comunicação do BD

   Nota: Os sistemas SAP que aparecem na tabela de banco de dados `/IBMMON/ITM_PORT` são para ambas as arquiteturas Java e ABAP.
4. No campo **Nº da porta de comunicação do BD**, insira o número da Porta de comunicação do banco de dados SAP relevante para o respectivo ID do sistema SAP e Nome do host do sistema SAP, e salve as mudanças.

   Nota: Se você não inserir qualquer valor no campo **Nº da porta de comunicação do DB** na tabela de banco de dados `/IBMMON/ITM_PORT`, então, por padrão, o número da porta de comunicação do DB será 0.

Instalação e Configuração Avançada do Agente SAP

Essas são instalações e configurações avançadas que são específicas do Agente SAP.

Os tópicos de instalação e configuração a seguir são descritos:

- “Módulo de Função SAP” na página 750
- “IDs do Usuário de SAP” na página 751
- Utilitários para Agente SAP
- “Conexões de SAP RFC” na página 751
- “Recurso de Conexão de Teste” na página 762
- “Configuração Avançada Opcional em SAP” na página 753
- “Relatório CEN CCMS” na página 760
- “Desinstalando o Transporte do Advanced Business Application Programming (ABAP) do Sistema SAP” na página 761

Nota: A instalação e configuração avançadas do Agente SAP contém referências ao IBM Tivoli Monitoring para que a documentação seja compatível com a UI do código de transação customizada de transporte ABAP.

Módulo de Função SAP

Quando o volume de dados é alto no servidor SAP, você pode ter problemas com determinados widgets, causando um tempo de resposta lento do servidor. Se os widgets não forem críticos, será possível desativar o módulo de função SAP associado.

Por padrão, os módulos de função Agente SAP estão ativados. Entretanto, os módulos de função a seguir são desativados por padrão:

- Serviços HTTP sob o subnó SYS (`/IBMMON/ITM_HTTP_SRVS`)
- As mensagens XML no subnó PI/XI (`/IBMMON/ITM_SXMB_MONI_NEW`)
- A comunicação Sync/Async sob o subnó PI/XI (`/IBMMON/ITM_SYN_ASYN_COMM`)
- Os detalhes de fila de entrada qRFC no subnó Sys (`/IBMMON/ITM_QIN_QDETAILS`)

Depois de desativar o módulo de função SAP, se você selecionar um widget, os dados não serão exibidos no painel do IBM Application Performance Management. Portanto, evite qualquer problema relacionado ao desempenho.

Ativando o Módulo de Função do Agente SAP

Se você desativou anteriormente o módulo de função do Agente SAP para resolver problemas de desempenho, é possível ativar o módulo de função também.

Procedimento

1. Efetue logon no sistema SAP.
2. Execute o código de transação SE16.
3. Insira o nome da tabela como `/IBMMON/ITM_CNFG`.
4. Selecione a linha a ser excluída e pressione **shift + F2** para excluir a entrada.
5. Clique em **Salvar**.

Desativando o Módulo de Função SAP

Alguns widgets podem causar uma resposta lenta do servidor SAP para que seja possível desativar o módulo de função SAP para melhorar o desempenho do servidor.

Procedimento

1. Efetue logon no sistema SAP.
2. Execute o código de transação SE16.
3. Insira o nome da tabela como `/IBMMON/ITM_CNFG`.
4. Pressione **F5** para criar uma nova entrada.
5. Insira o nome do módulo de função SAP no campo **PARM NAME**.
6. Insira Não no campo **VALUE CHAR**.

7. Clique em **Salvar**.

IDs do Usuário de SAP
Esta seção fornece informações sobre os IDs do usuário mySAP e permissões requeridas pelo Agente SAP.

Os IDs do Usuário suportam as seguintes finalidades:

- “Conexões de SAP RFC” na página 751
- “Monitorando de Agente Básico” na página 751

Conexões de SAP RFC
O Agente SAP usa conexões de Chamadas de Função Remotas (RFC) para pesquisa de Centralized Computing Center Management (CCMS) e coleção de dados de alerta CCMS. Este comportamento é específico para a arquitetura de SAP RFC.

O Agente SAP abre uma conexão RFC dedicada para o sistema SAP que é monitorado pelo agente. O sistema SAP abre, então, uma conexão interna por servidor de aplicativos para coleta de dados por meio de módulos e programas de função. Se os alertas CCMS forem coletados pelo agente, o sistema SAP abrirá uma conexão RFC adicional (interna do sistema) para cada servidor de aplicativos para esse encadeamento de coleção. Quando a coleta de dados for iniciada, uma conexão RFC para o agente será aberta. Em seguida, até o dobro do número de servidores de aplicativos SAP para as conexões RFC adicionais do sistema interno serão abertos.

Você deve assegurar que a instância que está sendo monitorada pode acomodar sessões RFC adicionais, especialmente em grandes sistemas com 10 instâncias ou mais. Quando a carga RFC antecipada para monitoramento puder afetar contrariamente o desempenho do sistema e as tolerâncias, ajuste o parâmetro do perfil SAP. Entre em contato com o Administrador SAP e consulte as Notas SAP a seguir:

- Sessões de terminal (configuração padrão: 200) 22099
- Configurações de Comunicação/Gateway/Conversação 887909 316877 384971

Monitorando de Agente Básico
O Agente SAP cria um IBMMON_AGENT no sistema SAP quando o transporte do agente é importado.

Este ID do usuário é IBMMON_AGENT com a senha padrão ITMMYSAP. Ele é pré-configurado para ser o Tipo de Comunicação somente pelo usuário e para usar o perfil de autorização /IBMMON/AUTH. Esse perfil, que é criado na hora de importação do transporte, contém o conjunto mínimo de permissões para executar o código Advanced Business Application Programming (ABAP) do agente. Além disso, este perfil aceita um conjunto de ações limitadas no sistema SAP.

Se esse nome de ID do usuário for inaceitável, por exemplo, se violar suas convenções de nomenclatura de instalação, é possível criar um ID de usuário diferente. O ID do usuário pode ser qualquer ID de usuário do SAP permitido, mas requer o conjunto completo de permissões no perfil /IBMMON/AUTH. O ID do usuário requer o Tipo de Comunicação acesso somente pelo usuário.

O ID de usuário padrão fornece autoridade suficiente apenas para os propósito a seguir:

- Monitoramento e coleta de dados
- Alertas de Closing Computing Center Management System (CCMS)
- Ativação, desativação e reconfiguração de estatísticas de gateway
- Reconfiguração das estatísticas do banco de dados Oracle

Se você optar por limitar as capacidades de ação do agente, é possível remover algumas das permissões de ação, como o fechamento de alertas CCMS.

Para acessar dados no Portal da UI do IBM Application Performance Management para componentes específicos, assegure-se de ter autorizações apropriadas. A tabela a seguir lista as autorizações que são necessárias para acessar os dados de diferentes subnós:

Tabela 202. A Lista de Autorizações

Subnós	Objetos de autorização	Descrição da autorização
Autorizações gerais do sistema que incluem os seguintes subnós: • Ins • Sys	S_ADMI_FCD	Para acessar o sistema
	S_BDS_DS -BC-SRV-KPR-BDS	Para acessar o Conjunto de Documentos
	S_BTCH_JOB	Para executar operações em tarefas de segundo plano
	S_CCM_RECV	Para transferir os dados do Repositório do Sistema Central
	S_C_FUNCT	Para fazer chamadas C nos programas ABAP
	S_DATASET	Para acessar arquivos
	S_RFC	Para verificar o acesso ao RFC. O objeto de autorização S_RFC contém as duas subautorizações a seguir: • RFC1: Para fornecer as autorizações para o grupo de função RFC1. • SDIFRUNTIME: Para fornecer as autorizações para o grupo de função SDIFRUNTIME.
	S_RFCACL	Para o usuário do RFC
	S_RZL_ADM	Para acessar o Computing Center Management System (CCMS): Administração do Sistema
	S_TCODE	Para verificar o Código de Transação no Início da Transação
	S_TOOLS_EX	Para acessar o Monitor de Desempenho de Ferramentas
Autorizações para o Solution Manager que incluem os seguintes subnós: • Lds • Sol	D_MD_DATA -DMD	Para visualizar o Conteúdo de Dados dos Dados Principais
	D_SOLMANBU	Para acessar um Tipo de Sessão do Solution Manager
	D_SOLM_ACT	Para acessar uma solução no Solution Manager
	D_SOL_VSBL	Para visualizar uma solução no Solution Manager
	S_CTS_SADM	Para visualizar Administração específica do sistema (transporte)
	S_TABU_RFC	Para visualizar Comparação e cópia do cliente: exportação de dados com RFC

Tabela 202. A Lista de Autorizações (continuação)

Subnós	Objetos de autorização	Descrição da autorização
Autorizações para PI que incluem o subnó PI	S_XMB_MONI	Para acessar o Monitoramento de Mensagens XI
Autorizações para MAI que incluem o subnó Slm	AI_DIAGE2E	Para acessar análise de ponta a ponta dos Diagnósticos de Solução
	AI_LMDB_OB	Para acessar objetos Landscape Management Database (LMDB)
	SM_MOAL_TC	Para acessar Monitoramento e Alerta
	SM_WC_VIEW	Para acessar Elementos da Interface com o Usuário do Centro de Trabalhos
	S_RFC_ADM	Para acessar opções de administração para o destino do RFC
	S_RS_AUTH	Para acessar Análise de BI na Função
	SM_APPTYPE	Para acessar o tipo de aplicativo do Solution Manager
	SM_APP_ID	Para acessar aplicativos fornecidos no Centro de Trabalhos

Usando a Administração do Usuário Central (CUA)
A Administração do Usuário Central (CUA) é usada para monitorar um sistema SAP.

Procedimento

Para usar o ID do usuário predefinido e a função de autorização para monitorar um sistema SAP configurado com Central User Administration, conclua uma das etapas a seguir:

- Instale o transporte no cliente do sistema lógico pai Central User Administration.
- Manualmente, crie o ID do usuário ou função no cliente onde deseja instalar o transporte. O ID do usuário ou função está no cliente onde o transporte está instalado (importado).
- Crie manualmente o ID do usuário ou função no cliente do sistema lógico pai do Central User Administration. Em seguida, distribua o ID do usuário ou a função para o cliente no qual o agente é executado.
- Manualmente, crie o ID do usuário ou função no cliente do sistema lógico pai Central User Administration e execute o agente nesse cliente.

Configuração Avançada Opcional em SAP
É possível configurar o Agente SAP usando funções SAP padrão do SAP ou do agente.

Use as transações fornecidas pelo agente no SAP para customizar vários comportamentos de agentes. Depois de executar a transação `/n/IBMMON/ITM_CONFIG` para acessar o menu de configuração principal no SAP, selecione uma das opções de configuração a seguir:

- “Recurso Copiar, Fazer Backup, Restaurar e Transações” na página 754
- “Copiar, Fazer Backup e Restaurar Dados Usando Transações” na página 755
- “Ferramenta de utilitário de linha de comandos” na página 755

- “Executando o utilitário de linha de comandos em um ambiente Windows” na página 756
- “Executando o utilitário de linha de comandos em um ambiente Não Windows” na página 756
- “Manutenção de alertas” na página 757
- “Selecionar Conjuntos de Monitor e Transação de Monitores” na página 758
- “Configurar o Limite de Resposta da Etapa de Diálogo do Sistema SAP” na página 758

Nota: Você deve usar como prefácio todas as transações `/IBMMON/ITM*` com `/n`.

As alterações de configuração feitas nessas transações são utilizadas imediatamente pelo Agente SAP, exceto as alterações feiras para manter grupos gerenciados. Quando a configuração de grupo gerenciado for alterada, as mudanças serão descobertas pelo Agente SAP na próxima pulsação.

Use as funções padrão SAP para concluir as configurações a seguir: “Configurar o Limite de Resposta da Etapa de Diálogo do Sistema SAP” na página 758

Recurso Copiar, Fazer Backup, Restaurar e Transações
Os recursos de cópia, backup e restauração estarão disponíveis após você efetuar logon no servidor SAP e executar a seguinte transação: `/n/IBMMON/ITM_CONFIG`.

As operações de cópia, de backup e de restauração permitem copiar, fazer backup e restaurar os dados de configuração do IBM Tivoli Monitoring.

Use recurso para selecionar a partir das funções a seguir e para salvar os dados de configuração do IBM Tivoli Monitoring:

- **Copiar**

  Use este recurso para copiar as definições de configuração do IBM Tivoli Monitoring a partir de um servidor SAP para outro servidor SAP. Por exemplo, você pode desejar copiar as definições de configuração do IBM Tivoli Monitoring do agente **a1** para a instância do servidor SAP SAP2. Este agente executa em sistema **m1** e está configurado para instância do servidor SAP SAP 1. Todas as definições de configuração do IBM Tivoli Monitoring, exceto as configurações de monitoramento da instância do servidor SAP são copiadas para o sistema SAP de destino. Você implementa o recurso de cópia usando o utilitário de linha de comandos ou a GUI do SAP.

- **Backup**

  É possível armazenar configurações específicas do agente que foram concluídas no servidor SAP, executando um backup do sistema. Use este recurso para salvar definições de configuração específicas do IBM Tivoli Monitoring no sistema SAP. Você usa a transação `/IBMMON/ITM_CONFIG` para inserir as configurações. O arquivo de backup é armazenado no diretório de trabalho no servidor SAP para o caminho a seguir: `/usr/sap//DVEBMGS/work`.

- **Restaurar**

  Use este recurso para restaurar os dados de configuração do IBM Tivoli Monitoring no servidor SAP do diretório de trabalho. É possível restaurar os dados de configuração do IBM Tivoli Monitoring no mesmo servidor SAP em que você concluiu o procedimento de backup desses dados de configuração ou outro servidor SAP. É possível restaurar os dados de configuração do IBM Tivoli Monitoring para tabelas de SAP e IBM Tivoli Monitoring específicas. Arquivos de configuração são armazenados com uma data e registro de data e hora, portanto é possível selecionar o ponto em que deseja restaurar seus arquivos.

Configurações específicas do agente incluem definições de configuração na transação `/IBMMON/ITM_CONFIG` em SAP. É possível concluir os procedimentos de configuração a seguir:

- Forneça uma amostra da frequência para alertas.
- Ative alertas específicos.
- Armazene nomes de arquivos de log.
- Gerencie definições de grupo.
- Selecione configurações de monitor e monitores.
- Selecione instâncias de SAP para propósitos de monitoramento.

Copiar, Fazer Backup e Restaurar Dados Usando Transações
Na interface com o usuário SAP, você copia, faz backup e restaura dados usando a transação `/n/IBMMON/ITM_CONFIG`.

Antes de Iniciar
Use os procedimentos de cópia, backup e restauração para copiar as definições de configuração do IBM Tivoli Monitoring de um servidor SAP para outro servidor SAP. Todas as definições de configuração IBM Tivoli Monitoring, exceto as configurações de monitoramento da instância do servidor SAP, são copiadas para o sistema SAP de destino.

Procedimento

Conclua os procedimentos a seguir para copiar, fazer backup e restaurar os dados no SAP:

- **Copiar**
  a. Insira o ID do sistema SAP de destino e o nome do arquivo existente como `source system id__<filenam>date_time`.

     A transação `/IBMMON/ITM_COPY` cria um arquivo de configuração do IBM Tivoli Monitoring no diretório de trabalho com o nome de arquivo SAP `target SAP system id__<filename>_date_time`.
  b. Clique em **Executar** para copiar os dados de configuração IBM Tivoli Monitoring para o arquivo.
  c. Clique em **Voltar** ou em **Cancelar** para retornar para a tela de configuração anterior do IBM Tivoli Monitoring.

     Os parâmetros de entrada esperados são **`Target System id`** e **`filename`** que devem ser copiados.
- **Backup**
  a. Efetue logon no servidor SAP e inicie a transação `/IBMMON/ITM_CONFIG`.
  b. Selecione **Fazer Backup**.
  c. Insira o nome do arquivo de backup.

     O nome do arquivo é armazenado como `sys_id_<filename>_date_time`.
  d. Clique em **Executar** para executar o backup e para armazenar o arquivo no Servidor de Aplicativos.

     Nota: O arquivo de backup é armazenado no diretório de trabalho do servidor de aplicativos.
  e. Clique em **Voltar** ou em **Cancelar** para retornar para a tela de configuração anterior do IBM Tivoli Monitoring.
- **Restaurar**
  a. Efetue logon no servidor SAP e inicie a transação `/IBMMON/ITM_CONFIG`.
  b. Selecione **Restaurar**.
  c. Insira o nome do arquivo a ser restaurado como `sys_id_<filename>_date_time`.
  d. Clique em **Executar** para restaurar os dados de configuração IBM Tivoli Monitoring.
  e. Clique em **Voltar** ou em **Cancelar** para retornar para a tela de configuração anterior do IBM Tivoli Monitoring.

Ferramenta de utilitário de linha de comandos
É possível usar a ferramenta de utilitário de linha de comandos para copiar, fazer backup e restaurar os dados de configuração do IBM Tivoli Monitoring no servidor SAP.

É possível executar a ferramenta de utilitário de linha de comandos no ambiente Windows e Não Windows. Consulte "Executando o utilitário de linha de comandos em um ambiente Windows" na página 756 e "Executando o utilitário de linha de comandos em um ambiente Não Windows" na página 756.

- **Copiar**

Execute o comando **backup** para copiar o arquivo de configuração do IBM Tivoli Monitoring da instância do servidor SAP sap1 do diretório do agente para sap2. Insira o nome do arquivo e sap1 como o sistema de origem do diretório do agente sap1. Em seguida, a função ABAP é chamada e copia as configurações de IBM Tivoli Monitoring deste arquivo para o arquivo de configuração IBM Tivoli Monitoring para Sap2. Agora selecione **Copy** na ferramenta do utilitário de diretório do agente sap1 e insira um nome de arquivo e sap2 como o sistema SAP de destino.

- **Backup**

  Após executar a ferramenta de utilitário de linha de comandos, selecione a opção **Backup** . Em seguida, é necessário inserir o nome do arquivo e o ID do sistema SAP. A ferramenta chama o módulo de função de SAP `/IBMMON/ITM_BACKUP`. O módulo de função lê as definições de configuração específicas do IBM Tivoli Monitoring que são armazenadas em tabelas e as armazena com um separador de linhas e colunas. Em seguida, a ferramenta de utilitário de linha de comandos lê a sequência e grava os dados em um arquivo. O nome do arquivo que é gerado tem o seguinte formato: ID>_<filename>-<date&time>. Este arquivo é armazenado no diretório em que o programa utilitário está armazenado.

- **Restaurar**

  Depois de executar a ferramenta de utilitário de linha de comandos, insira o nome do arquivo a ser restaurado e o sistema SAP de destino em que você deseja restaurar o arquivo. A ferramenta de utilitário de linha de comandos lê o arquivo no diretório do agente e chama o módulo de função SAP `/IBMMON/ITM_RESTORE`. Em seguida, a ferramenta passa as configurações de IBM Tivoli Monitoring como uma sequência. O módulo de função SAP atualiza as tabelas de IBM Tivoli Monitoring específicas e restaura as configurações de IBM Tivoli Monitoring específicas.

Executando o utilitário de linha de comandos em um ambiente Windows

É possível executar o utilitário de linha de comandos em um ambiente Windows para concluir os procedimentos de cópia, backup e restauração.

Procedimento

1. Dependendo de seu sistema operacional, conclua um dos procedimentos a seguir:
   - Para um sistema operacional de 64 bits, configure o caminho CANDLEHOME usando o comando **`set CANDLE_HOME = C:\IBM\APM`** e execute o comando **`ksacopybackuprestore.bat`** a partir do seguinte caminho: `%candle_home%\ TMAITM6x64`.
2. Para criar um arquivo de backup, conclua as etapas a seguir:
   a) Selecione **Backup** e insira o nome do arquivo e o nome do sistema SAP de origem.
   b) O arquivo de backup é criado com o seguinte formato: SYS ID>_<filename>_<date&time>.
3. Para restaurar o arquivo, conclua as etapas a seguir:
   a) Selecione **Restaurar** e insira o nome do sistema SAP de destino.
   b) Insira o nome do arquivo.
4. Para copiar o arquivo, conclua as etapas a seguir:
   a) A partir do agente de origem, selecione **Backup** e crie um arquivo de backup.
   b) Copie o arquivo de backup do diretório do agente de origem para o diretório do agente de destino.
   c) No diretório de origem, execute a ferramenta de utilitário de linha de comandos e selecione **Copiar**.
   d) Insira o nome do arquivo e o sistema SAP de destino.

Executando o utilitário de linha de comandos em um ambiente Não Windows

É possível executar o utilitário de linha de comandos em um ambiente Não Windows para concluir os procedimentos de cópia, backup e restauração.

Procedimento

1. Execute o comando **`ksacopybackuprestore.sh`** a partir do seguinte caminho: `/candle_home/<arch>/sa/shell`.
2. Para criar um arquivo de backup, conclua as etapas a seguir:

a) Selecione **Backup** e insira o nome do arquivo e o nome do sistema SAP de origem.

b) O arquivo de backup é criado com o seguinte formato: SYS ID>_<filename>_<date&time>.
O arquivo de backup é salvo neste local: `%candlehome% / arch /sa/bin`.

3. Para restaurar o arquivo, conclua as etapas a seguir:
   a) Selecione **Restaurar** e insira o nome do sistema SAP de destino.
   b) Insira o nome do arquivo.
4. Para copiar o arquivo, conclua as etapas a seguir:
   a) A partir do agente de origem, selecione **Backup** e crie um arquivo de backup.
   b) Copie o arquivo de backup do diretório do agente de origem para o diretório do agente de destino.
   c) No diretório de origem, execute a ferramenta de utilitário de linha de comandos e selecione **Copiar**.
   d) Insira o nome do arquivo e o sistema SAP de destino.

Manutenção de alertas

É possível modificar os alertas que são gerados pelo Tivoli Monitoring alterando seus status e limites.

Essa transação é utilizada para ativar ou desativas alertas gerados pelo Tivoli Monitoring e para configurar limites de aviso e críticos. Todos os alertas gerados pelo Tivoli Monitoring são mostrados com seus valores de limite e status atuais.

Ao modificar o status e os limites de alerta, os valores modificados são utilizados na próxima amostragem.

Manutenção do período de amostra padrão

O período de amostra padrão fornece informações sobre o relatório em tempo real para certos grupos de atributo.

Alguns grupos de atributos contêm data e hora implícitas para cada registro no grupo. Por exemplo, o grupo de atributos R/3_Abap_Dumps relata o tempo de criação para o dump e o grupo de atributos R/3_System_Log relata o tempo de criação para a entrada de log. Esses registros possuem um campo de data e hora. É possível obter um relatório de um histórico breve da tabela no lugar das informações mais recentes apenas. Esse intervalo é o período de tempo para a coleta de dados e é utilizado como o intervalo em tempo real ao coletar dados. A transação /IBMMON/ITM_PERIOD define um período de amostra padrão (período de tempo para relato em tempo real) para cada um desses grupos de atributos. O período de amostra identifica o comprimento do período de amostra de dados que inicia do momento atual e volta no tempo.

Manutenção do Nome do Arquivo de Log

Os arquivos de log específicos que são correspondidos apenas nas instâncias estão incluídos nos relatórios IBM Tivoli Monitoring com informações do arquivo de log.

Essa transação é usada para identificar quais arquivos de log considerar para inclusão nos relatórios do IBM Tivoli Monitoring que contêm informações de arquivo de log. Todos os arquivos de registro com um nome que corresponde aos padrões de nomes especificados nas instâncias especificadas são incluídos no relatório no próximo intervalo de coleta de dados.

Manutenção do grupo gerenciado

A transação de nomes do Grupo Gerenciado monitora e processa transações específicas no sistema SAP.

Utilize essa transação para manter as definições de Grupo Gerenciado do IBM Tivoli Monitoring. Todos os nomes de Grupos Gerenciados são passados para o Portal da UI do IBM Application Performance Management e mostrados nas Listas de Seleção do Sistema Gerenciado. No momento da coleta de dados, apenas os dados que correspondem às condições de seleção de Atributo são enviados para o agente SAP. Esses dados são mostrados nos relatórios ou usados para avaliação em situações e políticas.

Use os Grupos Gerenciados para monitorar os subconjuntos de informações no sistema SAP. Focalize apenas nas partes do sistema SAP nas quais você esteja interessado e ignore outras partes que não sejam de seu interesse. Por exemplo, se você estiver somente interessado no tempo de resposta das transações que fazem parte do Aplicativo Financeiro, crie um Grupo Gerenciado denominado Finanças. Em seguida, inclua apenas os códigos de transação Financeira. Sempre que o Financials Managed Group é processado pelo Tivoli Enterprise Portal, apenas as informações que contêm os códigos de transação especificados são consideradas ao mostrar um relatório, avaliar uma situação ou avaliar uma política.

Selecionar Conjuntos de Monitor e Transação de Monitores
Use os conjuntos de monitores e transação de monitores selecionados para editar a configuração de alertas do Centralized Computing Central Management (CCMS). Por exemplo, é possível desligar completamente a coleção de alertas de CCMS.

Essa transação é utilizada para selecionar os monitores CCMS dos quais o IBM Tivoli Monitoring recupera alertas. Por padrão, o monitor do Sistema Inteiro é selecionado na primeira vez em que esta janela é mostrada. Você pode alterar o conjunto de monitores, o monitor ou ambos, e, em seguida, salvar a configuração. Você pode selecionar um máximo de três monitores para os quais coletar alertas CCMS.

Para desativar a coleta de alertas CCMS completamente, impe as caixas de opções para todos os monitores e salve essa configuração.

O agente que já está em execução lê essa configuração e coleta alertas CCMS para os monitores selecionados. No entanto, quaisquer alertas CCMS que já foram coletados pelo agente antes de alterar a configuração dos alertas CCMS permanecem com o agente e o IBM Tivoli Monitoring.

Além de selecionar monitores e conjuntos de monitores, essa transação especifica o número de ocorrências de um tipo de alerta a ser recuperado. Além disso, ajuda a decidir se deve fechar automaticamente as ocorrências anteriores dos alertas que não são recuperados.

Configurar o Limite de Resposta da Etapa de Diálogo do Sistema SAP
É possível configurar um Limite de resposta da Etapa de diálogo para qualquer transação, executando a transação SE16.

Procedimento

1. No campo **Nome da Tabela**, digite `/IBMMON/ITM_TRSH` e, em seguida, selecione **Conteúdo da Tabela (F7)** para acessar a tabela.
2. Para visualizar as configurações de limite, selecione **Executar (F8)**. Os nomes das transações são mostrados na coluna **WORKLOAD** ; os valores dos limites são mostrados na coluna **THRESHOLD** .
3. Para incluir uma nova configuração de limite, selecione **Criar (F5)**. Digite o nome da transação no campo **WORKLOAD**. Os curingas a seguir são aceitos para o valor **WORKLOAD**:
   - * corresponde a múltiplos caracteres
   - + corresponde a qualquer caractere único
4. Digite o valor do limite, em milissegundos, no campo **THRESHOLD** . Selecione **Salvar** para salvar essa configuração. Valores de limite novos e alterados não entram em vigor imediatamente, mas entram em vigor sob uma das seguintes condições:
   - O agente é reiniciado.
   - O agente reabre a conexão RFC para o sistema SAP. Este procedimento ocorre a cada 12 pulsações, que, por padrão, é de cerca de 2 horas e 10 minutos.

Resultados
O valor digitado para a coluna **Limite** é retornado no atributo Limite de Resposta da Etapa do Diálogo do grupo de atributos R/3_Transacation_Performance.

Operações de tarefa em lote
É possível buscar todas as Tarefas em Lote em um intervalo de tempo especificado.

Procedimento

Siga as etapas após "Importando o transporte do ABAP no sistema SAP" na página 737.

Lembre-se: A Constante Crítica está configurada para todas as tarefas em lote.

1. Para buscar todas as Tarefas em Lote Ativas e Canceladas dentro de um intervalo de tempo especificado.

   Inclua a entrada a seguir na tabela /IBMMON/ITM_CNFG.

Tabela 203. /IBMMON/ITM_CNFG	
PARM_NAME	**VALUE_CHAR**
BATCH_JOBS_PERF	SIM

2. Para buscar todas as tarefas Canceladas dentro de um intervalo de tempo especificado e todas as tarefas Ativas, independentemente do intervalo de tempo.

   Inclua a entrada a seguir na tabela /IBMMON/ITM_CNFG.

Tabela 204. /IBMMON/ITM_CNFG	
PARM_NAME	**VALUE_CHAR**
BATCH_JOBS_PERF	YES_LONG_RUN

3. Para buscar todas as Tarefas em Lote em um intervalo de tempo especificado e todas as Tarefas em Lote Ativas, independentemente do intervalo de tempo.

   Inclua a entrada a seguir na tabela /IBMMON/ITM_CNFG.

Tabela 205. /IBMMON/ITM_CNFG	
PARM_NAME	**VALUE_CHAR**
BATCH_JOBS_PERF	YES_ALL

   Nota:

   - Se o parâmetro de configuração não for incluído, ele buscará todas as Tarefas em Lote dentro de um intervalo de tempo especificado sem a Constante Crítica configurada.
   - O número de linhas que são buscadas é sempre igual ao valor da Constante Crítica configurada no Código de Transação /n/IBMMON/ITM_CONFIG.

Melhorando o desempenho do Módulo de Função /IBMMON/ITM_MAIALRT_INX

É possível aprimorar o desempenho do Módulo de Função /IBMMON/ITM_MAIALRT_INX para Agente SAP.

Procedimento

Siga as etapas para melhorar o desempenho do módulo de função /IBMMON/ITM_MAIALRT_INX.

1. Efetue logon na GUI do Agente SAP.
2. Execute o código de transação SE16, insira o nome da tabela como /IBMMON/ITM_CNFG e pressione F7.
3. Pressione F5 ou clique em **Criar entradas** e inclua a entrada a seguir na tabela IBMMON/ITM_CNFG.

Tabela 206. /IBMMON/ITM_CNFG	
PARM_NAME	**VALUE_CHAR**
MAI_ALERTS_PERF	YES

   Nota:

- Se a Constante Crítica não estiver configurada no Código de Transação - /N/IBMMON/ITM_CONFIG, o valor padrão será 2500.
- Esse processo é aplicável apenas para buscar os Alertas MAI a partir do sistema SAP no qual o PERIOD_START e o PERIOD_END são iniciais.

  Lembre-se: Agora, o Módulo de Função /IBMMON/ITM_MAIALRT_INX busca o número de Alertas MAI equivalente à Constante Crítica configurada no Código de Transação - /N/IBMMON/ITM_CONFIG.
- Se essa entrada no /IBMMON/ITM_CNFG não for criada por padrão, então os 2.500 alertas MAI mais recentes serão buscados.
- O número de linhas que são buscadas é sempre igual ao valor da Constante Crítica configurada no Código de Transação /n/IBMMON/ITM_CONFIG.

Relatório CEN CCMS

O Centralized (CEN) Computing Center Management System (CCMS) é uma capacidade de monitoramento SAP.

Use esta capacidade para relatar alertas CCMS para diversos sistemas SAP para um hub de monitoramento central. Monitore o ambiente SAP a partir de um console CCMS. Os relatórios CCMS centralizados são melhor utilizados nos seguintes ambientes:

- Primeiramente, uma operação CCMS onde alertas CCMS são os únicos dados de monitoramento necessários.
- CCMS Centralized é parte do ambiente SAP.
- Grandes ambientes SAP com muitos sistemas SAP, como ISV e ISP.
- A integração do IBM Tivoli Monitoring V5.x com os adaptadores de CCMS do Agente SAP.
- Colete alertas de componentes e servidores de aplicativos SAP não-ABAP.

O Agente SAP suporta CCMS Centralizado para relatar alertas apenas. Em seguida, você coloca um Agente SAP em um sistema SAP Centralizado e visualiza os alertas CCMS para o ambiente SAP inteiro. Esse suporte é fornecido das seguintes maneiras:

- Ao relatar alertas CCMS, o agente verifica se os alertas estão associados ao sistema SAP que é monitorado diretamente pelo agente. Se o agente determinar que um alerta pertence a um sistema SAP diferente, ele assume o CCMS Centralized e cria automaticamente sistemas gerenciados R3_Group adicionais.
- O sistema gerenciado <local_SID>-All_CCMS_alerts:Grp é usado para relatar o conjunto completo de alertas de todos os sistemas SAP remotos. O valor de <local_SID> é o identificador do sistema para o sistema SAP que é monitorado diretamente. Por exemplo, se o sistema SAP local for QA1, esse nome de grupo seria QA1-All_CCMS_alerts:Grp.
- O sistema gerenciado <local_SID>-<remote_SID>_CCMS_alerts:Grp é usado para relatar todos os alertas para um sistema SAP remoto. O valor de <local_SID> é o identificador do sistema para o sistema SAP que é monitorado diretamente. O valor de <remote_SID> é o identificador do sistema para o sistema SAP remoto. Por exemplo, se o sistema SAP local for QA1 e o sistema SAP remoto for QA2, esse nome de grupo seria QA1-QA2_CCMS_alerts:Grp.
- Cada um desses sistemas gerenciados na árvore do Navegador possui o conjunto completo de widgets nele, mas apenas os widgets Alertas têm dados significativos.

O Agente SAP mantém sua definição de grupos CCMS Centralized no código de Programação de Aplicativo de Negócios Avançada (ABAP) no sistema SAP diretamente gerenciado. Pode ser necessário modificar essas definições se um sistema SAP para o qual você está recebendo alertas centralizados também está sendo monitorado diretamente por outra instância do Agente SAP. Você não deseja que os alertas sejam relatados em ambos os sistemas. Você pode limitar os relatórios de alerta centralizados da seguinte forma:

- Use a transação /IBMMON/ITM_CONFIG para Manter Grupos Gerenciados. Altere o grupo Todos Alertas CCMS. Remova o sistema remoto dessa lista editando a definição do grupo para EXCLUDE o identificador do sistema remoto.

- Use a transação /IBMMON/ITM_CONFIG para Manter Grupos Gerenciados. Exclua o grupo de alertas CCMS <remote_SID>. Por exemplo, se o sistema SAP remoto for QA2, esse nome de grupo seria alertas QA2 CCMS.

Como alternativa, é possível usar o CCMS Centralized para relatar alertas de todos os sistemas SAP, evitando relatos de alertas de cada agente instalado localmente. Utilize as seguintes etapas para definir essa configuração:

- Configure uma instância do Agente SAP para monitorar o sistema CCMS Centralized. Permita que o agente detecte e relate todos os alertas de todos os sistemas SAP remotos.
- Configure uma instância do Agente SAP para monitorar cada sistema SAP remoto. Desative a coleta de alertas e relatórios para essas instâncias de agente utilizando a transação /IBMMON/ITM_CONFIG para Selecionar Conjuntos de Monitores e Monitores. Nessa função, limpe as caixas de opções para todos os monitores e salve essa configuração.

O suporte Agente SAP para o CCMS Centralizado é usado em um ambiente de monitoramento CCMS puro para visualizar todos os alertas em um console comum. Além disso, ele pode ser usado com seu conjunto completo de funções para fornecer situações, políticas e comandos Executar Ação para os sistemas SAP remotos.

Desinstalando o Transporte do Advanced Business Application Programming (ABAP) do Sistema SAP
Se você optar por remover o Agente SAP do sistema, importe o transporte Delete para o sistema SAP. O transporte Delete exclui os objetos de dicionário e os módulos de funções do Agente SAP.

Antes de Iniciar
Se o sistema SAP for da versão 7.20 ou posterior, antes de importar o transporte Delete, em seu perfil de transporte, inclua o seguinte parâmetro do perfil de transporte: **tadirdeletions=true**. Esse parâmetro do perfil de transporte está disponível no tp versão 375.57.68 e também no R3trans versão 6.14 liberação 700 ou superior. Para obter mais informações sobre como remover solicitações de transporte do sistema SAP, consulte Excluindo solicitações de transporte.

Procedimento

1. Acesse o diretório /ABAP no CD do produto.
2. Copie os arquivos de transporte para o ambiente SAP.
3. Copie os arquivos K711_00xxx_DELETE e R711_00xxx_DELETE para o diretório de dados do Sistema de Transporte do SAP, conforme a seguir:
   a) Copie o arquivo K711_00xxx_DELETE para o diretório cofiles.
   b) Copie o arquivo R711_00xxx_DELETE para o diretório data.
4. Execute os seguintes comandos:
   a) **tp addtobuffer ITMK711_00xxx_DELETE SID pf=\usr\sap\trans\bin***PROFILE_NAME*
   b) **tp import ITMK711_00xxx_DELETE SID client=nnn U16 pf=\usr\sap\trans\bin** *PROFILE_NAME*

      Em que:

      SID
      ID do sistema SAP de destino

      PROFILE_NAME
      Nome do arquivo de perfil tp

      nnn
      Número do cliente de destino onde o agente deve ser executado

Customização da Instância do SAP
Por padrão, todas as instâncias do sistema SAP são monitoradas e mostradas no Portal da UI do IBM Application Performance Management.

Como administrador, escolha qual instância SAP deseja monitorar. Além disso, como um administrador, é possível desligar uma instância do SAP que você não deseja monitorar.

A transação customizada /IBMMON/ITM_INSTANCE se vincula à transação /IBMMON/ITM_CONFIG.

Selecione a opção **Instâncias SAP** para visualizar a instâncias disponíveis do servidor SAP. Em seguida, selecione a instância que deseja monitorar. Essas instâncias são exibidas no Portal da UI do IBM Application Performance Management. Quaisquer instâncias inativas ou limpas não são mostradas no Portal da UI do IBM Application Performance Management.

Recurso de Conexão de Teste
O recurso de Conexão de Teste permite verificar se você pode conectar o seu agente ao sistema SAP que é monitorado.

Insira os parâmetros na GUI para concluir o procedimento de conexão de teste. Se você se conectar ao sistema SAP com sucesso, uma mensagem de êxito será exibida. Como alternativa, se a conexão falhar, uma mensagem de falha será exibida.

O botão **Conexão de teste** está disponível somente na janela IBM Application Performance Management.

Ativando o Design do CCMS
O monitoramento do Computing Center Management System (CCMS) foi aprimorado para coletar registros do CCMS que estão em um estado aberto ou fechado desde o último período de amostra. É possível configurar o período de Amostra e, por padrão, ele tem um valor de 3 minutos. No entanto, você deve assegurar que os arquivos de transporte que são referenciados pelo Agente SAP e pelo transporte do Advanced Business Application Programming (ABAP) estejam na mesma versão.

Procedimento

1. Efetue logon no sistema SAP.
2. Abra a transação SE16 e inclua o nome da tabela /IBMMON/ITM_CNFG na transação.
3. Para executar o módulo de função ABAP /IBMMON/ITM_CNFG e para fornecer configurações para o programa ABAP, pressione **Enter** e, em seguida, pressione **F8**.
4. Para criar uma nova entrada na qual você incluirá novos parâmetros de configuração, pressione **F5**.
5. Para criar um novo parâmetro de configuração chamado **ISNEWCCMSDESIGN** com o valor *YES* no servidor SAP, no campo **PARM NAME**, insira ISNEWCCMSDESIGN e, no campo **VALUE CHAR**, insira YES.
6. Clique em **Salvar**.

   É possível ignorar o campo VALUE INT.

Modificando o Valor do Limite de um Alerta
É possível modificar o valor do limite **max ccms alert** que está associado a um alerta. Por padrão, o valor é 1000, o que significa que é possível visualizar 1000 alertas no IBM Application Performance Management. Os alertas mais antigos são removidos do cache

Procedimento

1. Execute uma das seguintes etapas:
   - No sistema operacional Windows, abra o arquivo <cancle home>\tmaitm6\KSAENV.
   - Em um sistema operacional não Windows, abra o arquivo <candle home>/config/sa.ini.
2. Inclua *MAX_CCMS_ALERT_THRESHOLD=< Value>* no final do arquivo.

   Nota: O valor deve ser maior que 100.

Desativando o Design do CCMS
É possível desativar o design do Computing Center Management System (CCMS).

Procedimento

1. Efetue logon no sistema SAP.
2. Abra a transação SE16 e inclua o nome da tabela `/IBMMON/ITM_CNFG` na transação.
3. Para executar o módulo de função ABAP `/IBMMON/ITM_CNFG` e para fornecer configurações para o programa ABAP, pressione **Enter** e, em seguida, pressione **F8**.
4. Para excluir a entrada existente, selecione e clique com o botão direito em **ISNEWCCMSDESIGN** e, em seguida, clique em **Excluir**.

Configurando o monitoramento do SAP HANA Database

Você deve configurar o SAP HANA Database agent para que o agente possa coletar dados do servidor de banco de dados SAP HANA que está sendo monitorado.

Antes de Iniciar

Revise os pré-requisitos de hardware e de software, consulte Agente do Software Product Compatibility Reports for SAP HANA Database

A seguir estão os pré-requisitos antes de configurar o SAP HANA Database agent

1. Assegure-se de criar usuários em todos os bancos de dados (sistema e locatário) do sistema SAP HANA com os privilégios a seguir:
   - Função: Monitoramento
   - Privilégios do sistema: Monitorar Administrador

   O nome e senha do usuário para os bancos de dados do sistema e do locatário devem ser os mesmo.
2. Quando a alternância entre a conectividade principal para a espera ocorre no sistema SAP HANA Database agent, o agente usa o nome do host de Standby Server que precisa ser resolvido no sistema do agente. Para resolver o nome do host para um endereço IP, é necessário incluir uma entrada de mapeamento no arquivo host da máquina na qual o agente está instalado.

Nota: Se você configurar o agente usando o Host Principal, insira o nome completo do host ou o endereço IP do Host Principal. Se o usuário estiver configurando o agente usando Stand by Host, insira o nome completo do host ou o endereço IP do Stand Host. Quando você configura o agente por meio do nó de Espera, o nó Principal deve estar inativo juntamente com a máquina host.

Sobre Esta Tarefa

O SAP HANA Database agent é um agente de múltiplas instâncias. Você deve criar a primeira instância e iniciar o agente manualmente.

Procedimento

- Windows Para configurar o agente em sistemas Windows, conclua as etapas a seguir:
  a) Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.
  b) Na janela **IBM Performance Management**, clique no botão direito em **Modelo** sob a coluna **Tarefa/Subsistema** e clique em **Configurar usando padrões**.
  A janela **Monitoring Agent for SAP HANA Database** é aberta.
  c) No campo **Inserir um nome de instância exclusivo**, digite um nome de instância do agente e clique em **OK**.

  Importante: O nome da instância do agente deve corresponder ao identificador do sistema de banco de dados de 3 dígitos do HANA (SID). Por exemplo, se o SID dos bancos de dados gerenciados do SAP HANA for H01, insira o H01 como o nome da instância.

d) Na janela **Monitoring Agent for SAP HANA Database**, especifique valores para os seguintes campos:

Nome da instância
O valor padrão para este campo é idêntico ao valor especificado no campo **Inserir um nome de instância exclusivo**.

Nome do servidor
O nome completo do host ou o endereço IP do servidor do SAP HANA onde o banco de dados do sistema está instalado.

Nome do banco de dados
O nome do banco de dados do SAP HANA.

Número da Porta
O número da porta SQL do serviço do servidor de índice no banco de dados do sistema do servidor de banco de dados SAP HANA.

Administrador de BD HANA
O nome do usuário para acessar o servidor de banco de dados do SAP HANA.

Senha do administrador do banco de dados HANA
A senha para acessar o servidor de banco de dados do SAP HANA.

Confirmar senha do administrador de banco de dados HANA
A senha especificada no campo **Senha de Administrador do DB HANA**.

e) Clique em **OK**.

f) Na janela **IBM Performance Management**, clique com o botão direito na instância do agente criada e clique em **Iniciar**.

- Linux AIX Para configurar um agente em sistemas Linux ou AIX, conclua as etapas a seguir:

a) Na linha de comandos, mude o caminho para o diretório de instalação do agente.
Exemplo: `/opt/ibm/apm/agent/bin`

b) Execute o comando a seguir em que instance_name é o nome que deseja dar à instância:

`./sap_hana_database-agent.sh config` *`instance_name`*

Importante: O nome da instância do agente deve corresponder ao identificador do sistema de banco de dados de 3 dígitos do HANA (SID). Se o SID do banco de dados gerenciados do SAP HANA for H01, insira H01 como o nome da instância.

c) Quando a linha de comandos exibir a mensagem a seguir, digite 1 e pressione Enter: `Edit 'Monitoring Agent for SAP HANA Database' setting? [1=Yes, 2=No]`

d) Especifique valores para os seguintes parâmetros do agente:

Nome do servidor
O nome completo do host ou o endereço IP do servidor do SAP HANA onde o banco de dados do sistema está instalado.

Nome do banco de dados
O nome do banco de dados do SAP HANA.

Número da Porta
O número da porta SQL do serviço do servidor de índice no banco de dados do sistema do servidor de banco de dados SAP HANA.

Administrador de BD HANA
O nome do usuário para acessar o servidor de banco de dados do SAP HANA.

Senha do administrador do banco de dados HANA
A senha para acessar o servidor de banco de dados do SAP HANA.

Confirmar senha do administrador de banco de dados HANA
A senha especificada no campo **Senha de Administrador do DB HANA**.

e) Execute o seguinte comando para iniciar o SAP HANA Database agent:

`./sap_hana_database-agent.sh start instance_name`

- Para configurar o agente usando o arquivo de resposta silencioso, conclua as etapas a seguir:
  a) Em um editor de texto, abra o arquivo `sap_hana_silent_config.txt` que está disponível no caminho *install_dir*`\samples` e especifique valores para todos os parâmetros.

  Windows `C:\IBM\APM\samples`

  Linux AIX `/opt/ibm/apm/agent/samples`

  b) Na linha de comandos, mude o caminho para o *install_dir*`\bin`

  c) Execute o seguinte comando:

  Windows `sap_hana_database-agent.bat config instance_name install_dir \samples\sap_hana_silent_config.txt`

  Linux AIX `sap_hana_database-agent.sh config instance_name install_dir\samples\sap_hana_silent_config.txt`

  d) Inicie o agente.

  Windows Na janela **IBM Performance Management**, clique com o botão direito na instância do agente criada e clique em **Iniciar**.

  Linux AIX Execute o comando a seguir: `./sap_hana_database-agent.sh start instance_name`

  Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte o "Histórico de Mudanças" na página 50.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o monitoramento do SAP NetWeaver Java Stack

Você deve configurar o SAP NetWeaver Java Stack para que o agente possa coletar dados de monitoramento de recursos do SAP NetWeaver Application Server que está sendo monitorado. Para monitorar dados de rastreamento de transações e diagnósticos, você deve concluir algumas tarefas de configuração.

Antes de Iniciar

Revise os pré-requisitos de hardware e de software, consulte Agente do Software Product Compatibility Reports for SAP NetWeaver Java Stack

Certifique-se de concluir as seguintes tarefas de pré-requisitos antes de configurar o agente:

- Copie os seguintes arquivos JAR para o diretório `bin`:
  - `sapj2eeclient.jar` (a API do cliente do SAP J2EE Engine que inclui o JMX Adapter)
  - `logging.jar` (a biblioteca de criação de log)
  - `com_sap_pj_jmx.jar` (a biblioteca SAP-JMX)
  - `exception.jar` (a estrutura de exceção do SAP)

  O diretório `bin` está no seguinte caminho:

  Windows `candle_home\TMAITM6_x64`

Linux `candle_home/interp/sv/bin`

Importante: Os arquivos JAR são os mesmos para todos os sistemas operacionais suportados. Esses arquivos estão disponíveis no caminho do Agente de Diagnóstico ou do Software Update Manager (SUM).

- Em Variáveis de Ambiente, inclua *<candleHome>\svdchome\<build number>\toolkit\lib\win64\ttapi* na variável de caminho.
- Designe a função NWA_READONLY ao usuário *Guest* para coletar dados de rastreamento de transações e diagnósticos.

Sobre Esta Tarefa

O SAP NetWeaver Java Stack é um agente de múltiplas instâncias. Você deve criar a primeira instância e iniciar o agente manualmente.

- Para configurar o agente em sistemas Windows, é possível usar a GUI ou o arquivo de resposta silencioso.
- Para configurar o agente em sistemas Linux ou AIX, é possível usar a linha de comandos ou o arquivo de resposta silencioso.

Para configurar a coleta de dados de rastreamento de transações e diagnósticos, conclua as seguintes tarefas:

1. Configure o coletor de dados. Para obter detalhes, consulte “Configurando o coletor de dados” na página 768.
2. Ative a coleta de dados de rastreamento de transações e diagnósticos. Para obter detalhes, consulte “Ativando a coleta de dados de rastreamento de transações e diagnósticos” na página 770.

As instruções mencionadas nesse tópico são para a liberação mais atual do agente, exceto conforme indicado. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Versão do Agente.

Configurando o agente nos sistemas Windows

É possível configurar o agente em sistemas operacionais Windows usando a janela **IBM Performance Management**.

Antes de Iniciar

Assegure-se de que os arquivos, que estão listados na seção "Antes de iniciar" do tópico “Configurando o monitoramento do SAP NetWeaver Java Stack” na página 765, estejam disponíveis no diretório `bin`.

Sobre Esta Tarefa

O SAP NetWeaver Java Stack fornece valores padrão para alguns parâmetros. É possível especificar diferentes valores para esses parâmetros.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito em **Modelo**, na coluna **Tarefa/Subsistema**, e clique em **Configurar agente**.

   A janela **Monitoring Agent for SAP NetWeaver Java Stack** é aberta.
3. No campo **Inserir um nome de instância exclusivo**, digite um nome de instância do agente e clique em **OK**.

   Importante: O nome da instância do agente deve corresponder ao identificador do sistema (SID) do SAP NetWeaver Java Stack de 3 dígitos. Por exemplo, se o SID do SAP NetWeaver Java Stack gerenciado for P14, insira P14 como o nome da instância.

4. Na janela **Monitoring Agent for SAP NetWeaver Java Stack**, especifique valores para os parâmetros de configuração e clique em **OK**.

   Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração do agente" na página 772.
5. Na janela **IBM Performance Management**, clique com o botão direito na instância do agente criada e clique em **Iniciar**.

O que Fazer Depois

- Efetue login no Console do Cloud APM para visualizar os dados de monitoramento de recursos que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte Iniciando o console do Performance Management.
- Para coletar dados de rastreamento e diagnósticos de transação, configure o coletor de dados e ative a coleta de dados para rastreamento e diagnóstico de transação.

Configurando o agente em sistemas Linux ou AIX

Para configurar o agente em sistemas Linux ou AIX, você deve executar o script e responder aos prompts.

Antes de Iniciar

Assegure-se de que os arquivos, que estão listados na seção "Antes de iniciar" do tópico "Configurando o monitoramento do SAP NetWeaver Java Stack" na página 765, estejam disponíveis no diretório `bin`.

Procedimento

1. Na linha de comandos, mude o caminho para o diretório de instalação do agente.

   Linux `/opt/ibm/apm/agent/bin`

   Linux AIX `/opt/ibm/apm/agent/bin`
2. Execute o seguinte comando:

   `./sap_netweaver_java_stack-agent.sh config` *`instance_name`*

   em que *instance_name* é o nome que você deseja dar à instância.

   Importante: O nome da instância do agente deve corresponder ao identificador do sistema (SID) do SAP NetWeaver Java Stack de 3 dígitos. Por exemplo, se o SID do SAP NetWeaver Java Stack gerenciado for P14, insira P14 como o nome da instância.
3. Quando a linha de comandos exibir a seguinte mensagem, digite 1 e pressione Enter:

   `Edit 'Monitoring Agent for SAP NetWeaver Java Stack' setting? [1=Yes, 2=No]`
4. Quando for solicitado, especifique valores para os parâmetros de configuração.

   Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração do agente" na página 772
5. Execute o comando a seguir para iniciar o agente:

   `./sap_netweaver_java_stack-agent.sh start` *`instance_name`*

O que Fazer Depois

- Efetue login no Console do Cloud APM para visualizar os dados de monitoramento de recursos que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte Iniciando o console do Performance Management.
- Para coletar dados de rastreamento e diagnósticos de transação, configure o coletor de dados e ative a coleta de dados para rastreamento e diagnóstico de transação.

Configurando o agente usando o arquivo silencioso de resposta

O arquivo de resposta silencioso contém os parâmetros de configuração do agente. É possível editar o arquivo de resposta silencioso para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Antes de Iniciar

Assegure-se de que os arquivos, que estão listados na seção "Antes de iniciar" do tópico “Configurando o monitoramento do SAP NetWeaver Java Stack” na página 765, estejam disponíveis no diretório `bin`.

Sobre Esta Tarefa

O arquivo silencioso de resposta contém parâmetros de configuração do agente com valores padrão definidos para alguns parâmetros. É possível editar o arquivo silencioso de resposta para especificar os valores diferentes para os parâmetros de configuração.

Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

1. Em um editor de texto, abra o arquivo `sap_netweaver_java_stack_silent_config.txt` que está disponível no seguinte caminho e especifique valores para os parâmetros de configuração.

   Windows `C:\IBM\APM\samples`

   Linux AIX `/opt/ibm/apm/agent/samples`

   Para obter informações sobre os parâmetros de configuração, consulte “Parâmetros de configuração do agente” na página 772
2. Na linha de comandos, mude o caminho para `install_dir\bin`
3. Execute o seguinte comando:

   Windows `sap_netweaver_java_stack-agent.bat config` *`instance_name`* `install_dir\samples\sap_netweaver_java_stack_silent_config.txt`

   Linux AIX `./sap_netweaver_java_stack-agent.sh config` *`instance_name`* `install_dir\samples\sap_netweaver_java_stack_silent_config.txt`
4. Inicie o agente.

   Windows Na janela IBM Cloud Application Performance Management, clique com o botão direito na instância de agente criada e clique em **Iniciar**. Como alternativa, também é possível executar o seguinte comando: `sap_netweaver_java_stack-agent.bat start` *`instance_name`*

   Linux AIX Execute o comando a seguir: `./sap_netweaver_java_stack-agent.sh start` *`instance_name`*

O que Fazer Depois

- Efetue login no Console do Cloud APM para visualizar os dados de monitoramento de recursos que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte Iniciando o console do Performance Management.
- Para coletar dados de rastreamento e diagnósticos de transação, configure o coletor de dados e ative a coleta de dados para rastreamento e diagnóstico de transação.

Configurando o coletor de dados

É possível usar/configurar o coletor de dados para cada instância do servidor de aplicativos que você deseja monitorar.

Antes de Iniciar

Assegure-se de que os arquivos, que estão listados na seção "Antes de iniciar" do tópico “Configurando o monitoramento do SAP NetWeaver Java Stack” na página 765, estejam disponíveis no diretório `bin`.

Procedimento

Para configurar o coletor de dados respondendo aos prompts, conclua as seguintes etapas:

1. Na linha de comandos, mude o caminho para o diretório Windows `install_dir\svdchome\build no\bin\configNW` ou Linux AIX `install_dir/svdchome/build no/bin/configNW` e execute o seguinte script:

   Windows config.bat

   Linux AIX config.sh
2. Selecione a versão do NetWeaver Server digitando o número que corresponde ao produto para o qual você deseja configurar o coletor de dados e pressione Enter.
3. Quando for solicitado o nome do usuário, insira o nome do usuário que está configurado no SAP NetWeaver Application Server with Java Stack e pressione Enter.
4. Quando for solicitada a senha, insira a senha e pressione Enter.
5. Quando for solicitado que insira novamente a senha, insira a senha novamente e pressione Enter.
6. Quando for solicitado um número da porta P4, insira o número da porta P4 da instância do SAP NetWeaver Application Server disponível no computador local e pressione Enter.

   Importante: Use essa fórmula para calcular o número da porta P4: 50000 + (número da instância*100) + 4
7. Quando for solicitado que selecione o número da instância do NetWeaver Server, insira o número que corresponde à instância que você deseja configurar e pressione Enter.

   Lembre-se: Para cada instância, é preciso configurar o coletor de dados separadamente.
8. Se for solicitada a inserção do caminho para o Java Home, use JAVA_HOME da instância SAP. Por exemplo, `E:\usr\sap\J01\J04\exe\sapjvm_6`.
9. Quando solicitado, insira 1 se desejar ativar a coleta de dados de rastreamento de transações. Caso contrário, insira 2 e pressione Enter.
10. Quando solicitado, insira 1 se desejar ativar a coleta de dados diagnósticos. Caso contrário, insira 2 e pressione Enter.

Resultados

O caminho gerado para carregar arquivos de classe.

O que Fazer Depois

1. Inclua o caminho gerado para a variável de ambiente apropriada.

   Windows *PATH*

   Linux *LD_LIBRARY_PATH* e *LIBPATH*

   AIX *LD LIBRARY PATH* e *LIB PATH*

   Lembre-se:

   Windows Inclua o caminho gerado na variável de ambiente *PATH*.

   Linux Inclua o caminho gerado no *LD_LIBRARY_PATH* e *LIBPATH* no arquivo `/home/sidadm/.cshrc` no seguinte formato.

   ```
   setenv LD_LIBRARY_PATH /path
   setenv LIBPATH /path
   ```

AIX Inclua o caminho gerado no *LD LIBRARY PATH* e no *LIB PATH* no arquivo `/etc/environment` no seguinte formato.

```
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/path
```

```
LIBPATH=$LIBPATH:/path
```

2. Reinicie as instâncias do servidor de aplicativos.
3. Ative a coleta de dados para rastreamento de transações e diagnósticos. Para obter detalhes, consulte “Ativando a coleta de dados de rastreamento de transações e diagnósticos” na página 770.

Ativando a coleta de dados de rastreamento de transações e diagnósticos

Na página **Configuração do agente**, é possível ativar ou desativar a coleta de dados para rastreamento de transação ou diagnósticos.

Antes de Iniciar

Certifique-se de que o coletor de dados esteja configurado. Para obter detalhes, consulte “Configurando o coletor de dados” na página 768.

Sobre Esta Tarefa

Ao ativar a coleta de dados de rastreamento de transações, o agente coleta dados dos seguintes componentes:

- Servlet JSP
- RemoteEJB
- JMS

Procedimento

Conclua as seguintes etapas para configurar a coleta de dados para cada instância do SAP NetWeaver Application Server.

1. Efetue login no Console do Cloud APM.
2. A partir da barra de navegação, clique em **Configuração do Sistema** > **Configuração do Agente**.
   A página **Configuração do Agente** é exibida.
3. Clique na guia **NetWeaver**.
4. Selecione as caixas de seleção para as instâncias do SAP NetWeaver Application Server para as quais você deseja configurar a coleta de dados e conclua qualquer uma das seguintes ações da lista **Ações**.
   - Para ativar o rastreamento de transações, clique em **Configurar rastreamento de transações** > **Ativado**. O status na coluna **Rastreamento de transação** é atualizado para Ativado para cada instância selecionada do SAP NetWeaver Application Server.
   - Para ativar a coleta de dados diagnósticos, selecione **Configurar modo de diagnóstico** > **Somente modo de diagnóstico ativado**. O status na coluna Modo de diagnóstico é atualizado para Ativado para cada instância selecionada do SAP NetWeaver Application Server.
   - Para ativar a coleta de dados diagnósticos e o rastreio de método, selecione **Configurar modo de diagnóstico** > **Modo de diagnóstico e Rastreio de método ativados**. O status nas colunas Modo de diagnóstico e Rastreio de método é atualizado para Ativado para cada instância selecionada do SAP NetWeaver Application Server.
   - Para desativar o rastreamento de transação, clique em **Configurar Rastreamento de Transação** > **Desativado**. O status na coluna **Rastreamento de transação** é atualizado para Desativado para cada instância selecionada do SAP NetWeaver Application Server.
   - Para desativar a coleta de dados diagnósticos, clique em **Configurar modo de diagnóstico** > **Modo de diagnóstico e Rastreio de método desativados**. O status nas colunas **Modo de diagnóstico e Rastreio de método** é atualizado para Desativado para cada instância selecionada do SAP NetWeaver Application Server.

Resultados
A coleta de dados é configurada para cada instância do SAP NetWeaver Application Server.

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados de rastreamento de transação e diagnósticos que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Removendo a configuração do coletor de dados

É possível retroceder as mudanças que foram feitas quando o coletor de dados foi configurado para uma instância do SAP Netweaver Application Server with Java Stack.

Procedimento

Para remover a configuração do coletor de dados respondendo aos prompts, conclua as seguintes etapas:

1. Na linha de comandos, mude o caminho para o diretório Windows `install_dir\svdchome*build no*\bin\configNW` ou Linux AIX `install_dir/svdchome/*build no*/bin/configNW` e execute o seguinte script:

   Windows unconfig.bat

   Linux AIX unconfig.sh

   Todas as instâncias para as quais o coletor de dados está configurado são listadas.
2. Insira o número que corresponde à instância para a qual você deseja remover a configuração do coletor de dados e pressione Enter.

   Dica: Para remover a configuração de várias instâncias do coletor de dados, insira o número que corresponde às instâncias separadas por vírgulas. Para remover a configuração do coletor de dados de todas as instâncias, é possível executar os seguintes scripts:

   Windows config.bat -a

   Linux AIX config.sh -a

O que Fazer Depois
Reinicie o SAP NetWeaver AS com instâncias de Java Stack.

Restaurando a instância do SAP NetWeaver Application Server

É possível usar o utilitário de restauração para restaurar parâmetros da JVM, se a instância do SAP NetWeaver Application Server não iniciar após a configuração do SAP NetWeaver Data Collector ou para restaurar a instância do SAP NetWeaver Application Server.

Procedimento

Para restaurar a instância do SAP NetWeaver Application Server respondendo aos prompts, conclua as seguintes etapas:

1. Na linha de comandos, mude o caminho para o diretório Windows `install_dir\svdchome\*build no*\bin\configNW` ou Linux AIX `install_dir/svdchome/*build no*/bin/configNW` e execute o seguinte script:

   Windows `restoreNW.bat`

   Linux AIX `restoreNW.sh`
2. Selecione a versão do NetWeaver Server digitando o número que corresponde ao produto para o qual você deseja restaurar os parâmetros da JVM e pressione Enter.
3. Quando for solicitado o nome do usuário, insira o nome do usuário para a instância do SAP NetWeaver Application Server e pressione Enter.

4. Quando for solicitada a senha de usuário, insira-a para a instância do SAP NetWeaver Application Server e pressione Enter.
5. Quando for solicitado um número da porta P4, insira o número da porta P4 da instância do SAP NetWeaver Application Server disponível no computador local e pressione Enter.

   Se as informações da instância não forem encontradas usando a porta P4 inserida, a mensagem `Não foi possível conectar-se ao SAP NetWeaver Server` será exibida e será solicitado que forneça o caminho para o início da instância do NetWeaver Server.

   Exemplo, `usr\sap\`*`System_Name`*`\`*`Instance_Number`*
6. Quando for solicitado que selecione o número da instância do NetWeaver Server, insira o número que corresponde à instância que você deseja restaurar e pressione Enter.

Resultados

A mensagem a seguir é exibida:

```
Restauração bem-sucedida. Reinicie a instância.
```

Parâmetros de configuração do agente

Ao configurar o SAP NetWeaver Java Stack, é possível mudar o valor padrão dos parâmetros, como SAP_NETWEAVER_P4_HOSTNAME e SAP_NETWEAVER_P4_PORT.

A tabela a seguir contém descrições detalhadas dos parâmetros de configuração do SAP NetWeaver Java Stack. Você deve especificar um valor para todos os campos porque esses campos são obrigatórios.

Tabela 207. Nomes e descrições de parâmetros de configuração

Nome de parâmetro	**Descrição**
Nome da instância	O nome da instância. O valor padrão para este campo é idêntico ao valor especificado no campo **Inserir um nome de instância exclusivo**.
SAP_NETWEAVER_P4_ NOME DO HOST	O nome do host ou endereço IP do SAP NetWeaver Application Server.
SAP_NETWEAVER_P4_ PORT	O número da porta P4 do SAP NetWeaver Application Server.
SAP_NETWEAVER_P4_ NOMEDOUSUARIO	O nome de usuário do administrador para acessar o SAP NetWeaver Application Server.
SAP_NETWEAVER_P4_ PASSWORD	A senha do administrador para acessar o SAP NetWeaver Application Server.
Confirmar SAP_NETWEAVER_P4_ PASSWORD	A senha especificada para o parâmetro **SAP_NETWEAVER_P4_PASSWORD**.

Configurando o monitoramento do Siebel

O Agente Siebel fornece um ponto central de monitoramento para os recursos do Siebel, incluindo estatísticas do Siebel, sessões do usuário, componentes, tarefas, servidor de aplicativos, Siebel Gateway Name Server, CPU do processo, uso de memória e monitoramento de eventos de log.

Antes de Iniciar

- Leia o tópico "Configurando o monitoramento do Siebel" na página 772 inteiro para determinar o que é necessário para concluir a configuração.
- Estas instruções são para a liberação mais atual do agente, exceto conforme indicado.

- Certifique-se de que os requisitos do sistema para o Agente Siebel sejam atendidos em seu ambiente. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Agente Siebel.
- Antes de configurar o Agente Siebel, você deve verificar a conta do usuário Siebel que é usada pelo Agente Siebel.

O Monitoramento de Estatísticas por Componente é desativado, por padrão. É possível ativar o Monitoramento de Estatísticas por Componente.

Sobre Esta Tarefa

O Agente Siebel é um agente de múltiplas instâncias. Deve-se criar a primeira instância e iniciar o agente manualmente.

Procedimento

1. Para configurar o agente nos sistemas Windows, é possível usar a janela do IBM Performance Management ou o arquivo de resposta silencioso.
   - "Configurando o agente nos sistemas Windows" na página 775.
   - "Configurando o agente usando o arquivo silencioso de resposta" na página 780.
2. Para configurar o agente em sistemas Linux e UNIX, é possível executar o script e responder aos prompts ou usar o arquivo de resposta silencioso.
   - "Configurando o agente respondendo aos prompts" na página 779.
   - "Configurando o agente usando o arquivo silencioso de resposta" na página 780.

O que Fazer Depois

No Console do Cloud APM, acesse as páginas do Application Performance Dashboard para visualizar os dados que foram coletados. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Se você não conseguir visualizar os dados nos painéis do agente, primeiro verifique os logs de conexão do servidor e, em seguida, os logs do provedor de dados. Os caminhos padrão para esses logs são os seguintes:

- Linux AIX `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Para obter ajuda com a resolução de problemas, consulte o Fórum do Cloud Application Performance Management.

Verificar conta do usuário do Siebel

Você deve verificar a conta do usuário que é usada para executar o agente Siebel antes de configurar o agente.

Sobre Esta Tarefa

A conta do usuário que é usada para executar o Agente Siebel deve ter permissões para executar o utilitário de linha de comandos **srvrmgr** do Siebel. Para verificar se a conta do usuário tem as permissões necessárias, execute estas etapas:

Procedimento

1. Efetue logon no computador com a conta do usuário que é usada para executar o Agente Siebel.
2. Mude o diretório para o local onde o servidor Siebel está instalado.
3. Acesse o arquivo de ambiente Siebel:

   ```
   source siebenv.sh
   ```

4. Execute o seguinte comando:

```
srvrmgr /s Siebel_server /g Siebel_gateway /e Siebel_enterprise
/u useraccount /p password
/c "list servers"
```

em que

Siebel_server
Nome do Siebel Application Server.

Siebel_gateway
Nome do servidor de nomes do gateway atualmente ativo.

Siebel_enterprise
Nome do Siebel Enterprise.

Utilizadora
Conta do usuário que você usa para efetuar logon no computador.

senha
A senha que está associada à conta do usuário.

Se a conta do usuário tiver as permissões necessárias, você verá a saída que é semelhante ao exemplo a seguir em que os campos retornados são limitados a três:

```
Connected to 1 server(s) out of a total of 1 server(s) in the enterprise

srvrmgr:s82win8> list servers show SBLSRVR_NAME, HOST_NAME, SBLSRVR_STATUS

SBLSRVR_NAME  HOST_NAME  SBLSRVR_STATUS
------------  ---------  --------------------------------
s82win8       s82win8    16.0.0.0 [23057] LANG_INDEPENDENT

1 row returned.
```

Se o comando **srvrmgr** não for executado corretamente, consulte o administrador do Siebel do servidor. Assegure de configurar as variáveis de ambiente do Siebel necessárias para a conta do usuário e que a conta do usuário tenha as permissões apropriadas para executar o comando **srvrmgr**.

Ativando Monitoramento de Estatísticas por Componente

O Monitoramento de Estatísticas por Componente é desativado, por padrão. É possível ativar o Monitoramento de Estatísticas por Componente usando a variável de ambiente KUY_ENABLE_COMP_STATS.

Antes de Iniciar

Por causa de um problema conhecido com os servidores do Siebel V8.1 e posterior, a reunião das Estatísticas de Componente do Siebel pode ter um efeito negativo no uso da memória do Siebel Gateway Server. Esse problema é abordado na nota técnica publicada pelo Oracle que é nomeada "Gateway Service on Siebel 8.1 ou 8.2 Might Consume High Memory Consumption: Recuperação (ID do Doc. 1269177.1)". Uma correção para o problema é fornecida nesse artigo. A correção é implementada no servidor Siebel.

Se o Monitoramento de Estatística por Componente for necessário no ambiente, aplique a correção do Oracle ao Gateway Servers of Siebel V8.1 e posterior, antes de ativar o Monitoramento de Estatísticas por Componente.

Sobre Esta Tarefa

Depois de aplicar a correção do Oracle, conclua as seguintes etapas para ativar o Monitoramento de Estatísticas por Componente no Agente Siebel:

Procedimento

1. Acesse o diretório de instalação do agente do Agente Siebel:

- Windows *install_dir*\TMAITM6_x64
- Linux AIX *install_dir*/config

2. Edite o arquivo de configuração do Agente Siebel para configurar KUY_ENABLE_COMP_STATS como true.
   - Windows KUYENV_*instance_name*
   - Linux AIX uy.environment

   em que *instance_name* é o nome da instância do agente Siebel.
3. Reinicie o agente.

   Importante: Para tornar esta configuração o padrão para todas as novas instâncias do agente, configure KUY_ENABLE_COMP_STATS para true nos arquivos de modelo de configuração:
   - Windows KUYENV
   - Linux AIX Esta configuração já tornou-se a padrão para novas instâncias de agentes editando uy.environment na Etapa 2.

Configurando o agente nos sistemas Windows

É possível configurar o Agente Siebel em sistemas operacionais Windows usando a janela IBM Cloud Application Performance Management. Após fazer a atualização dos valores de configuração, deve-se iniciar o agente para salvar os valores atualizados.

Procedimento

1. Clique em **Iniciar** > **Todos os programas** > **Agentes do IBM Monitoring** > **IBM Cloud Application Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito no modelo **Monitoring Agent for Siebel** e, em seguida, clique em **Configurar agente**.

   Lembre-se: Depois de configurar uma instância de agente pela primeira vez, a opção **Configurar agente** é desativada. Para configurar a instância de agente novamente, clique nela com o botão direito e clique em **Reconfigurar**.
3. Insira um nome de instância exclusivo e, em seguida, clique em **OK**. Use apenas letras, numerais Arábicos, o caractere sublinhado e o caractere de menos no nome da instância. Por exemplo: siebel01.

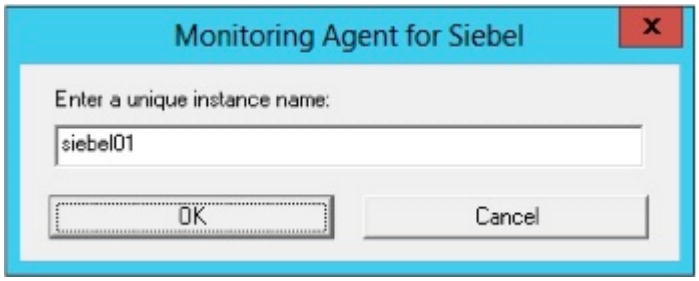


Figura 22. A janela para inserir um nome exclusivo da instância.

4. Selecione um tipo de servidor e insira valores para os campos necessários para esse tipo de servidor, em seguida, clique em **Avançar**.

   Consulte Tabela 208 na página 781 para obter uma explicação de cada um dos parâmetros de configuração.

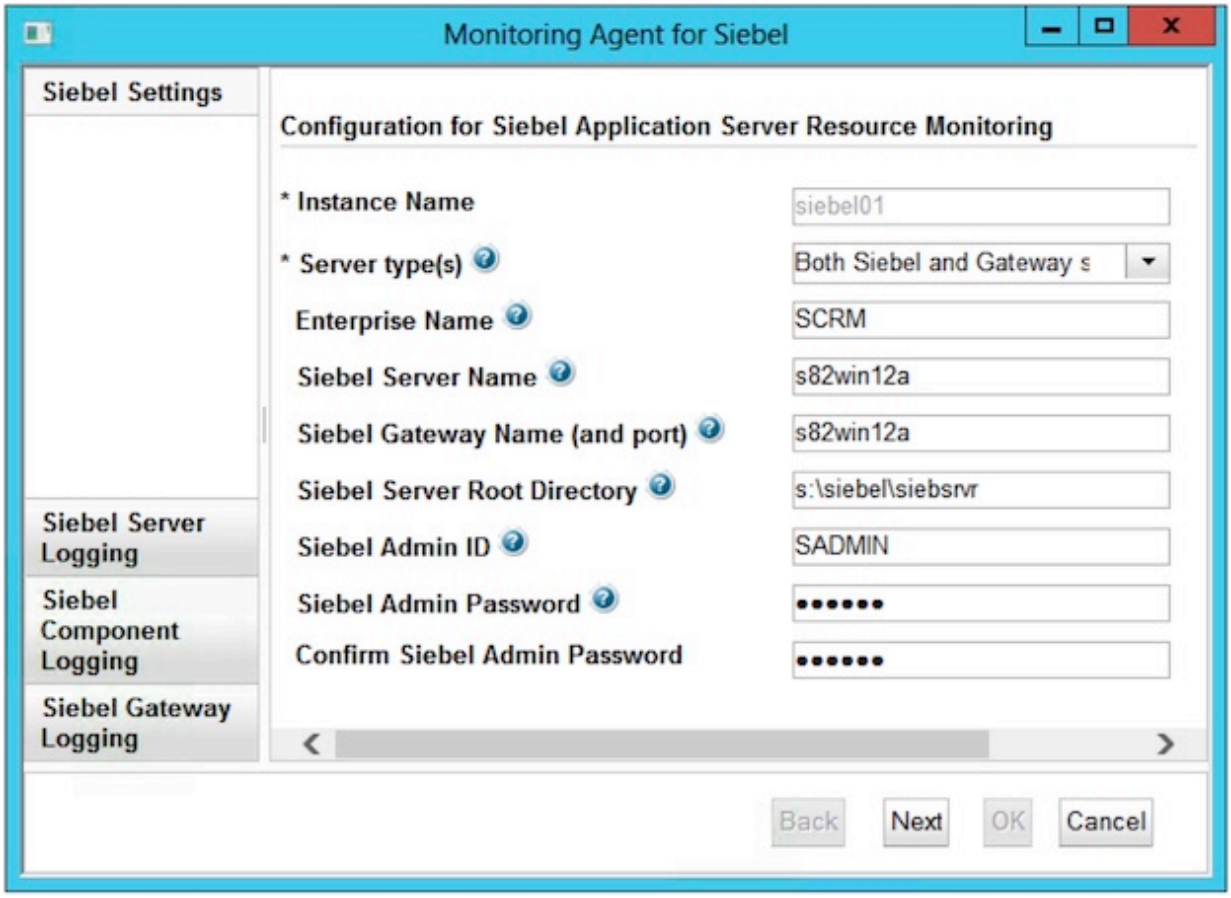


Figura 23. A janela para parâmetros de configuração para tipos de servidores Siebel que são instalados em um host Siebel

Importante: Se o Agente Siebel for instalado em um computador com o Siebel Gateway Name Server mas sem o Servidor Siebel, os dados exibidos no Application Dashboard serão aplicáveis somente ao Siebel Gateway Name Server para essa instância. Todas as outras visualizações do Agente Siebel estão vazias.

5. Opcional: Edite os valores para criação de log do servidor Siebel, em seguida, clique em **Avançar**.
   Consulte Tabela 209 na página 782 para obter uma explicação de cada um dos parâmetros de configuração.

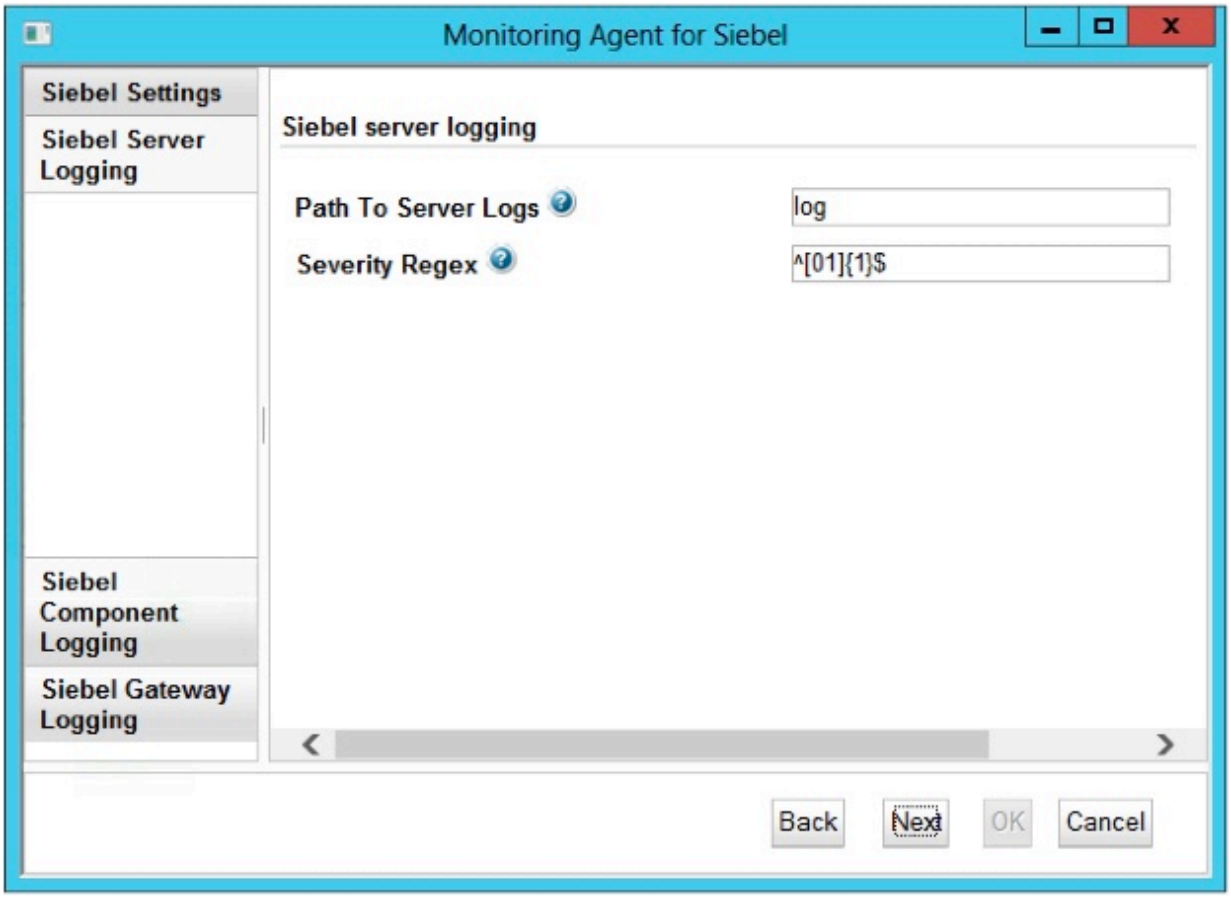


Figura 24. A janela para especificar configurações de criação de log do servidor Siebel.

6. Opcional: Edite os valores para criação de log do componente Siebel, em seguida, clique em **Avançar**. Por padrão, os logs de componentes no Tabela 212 na página 783 são monitorados pelo Agente Siebel. Para incluir até 10 logs de componentes adicionais a serem monitorados, especifique o alias do componente correspondente, por exemplo, `SCBroker`.

   Consulte Tabela 210 na página 783 para obter uma explicação de cada um dos parâmetros de configuração.

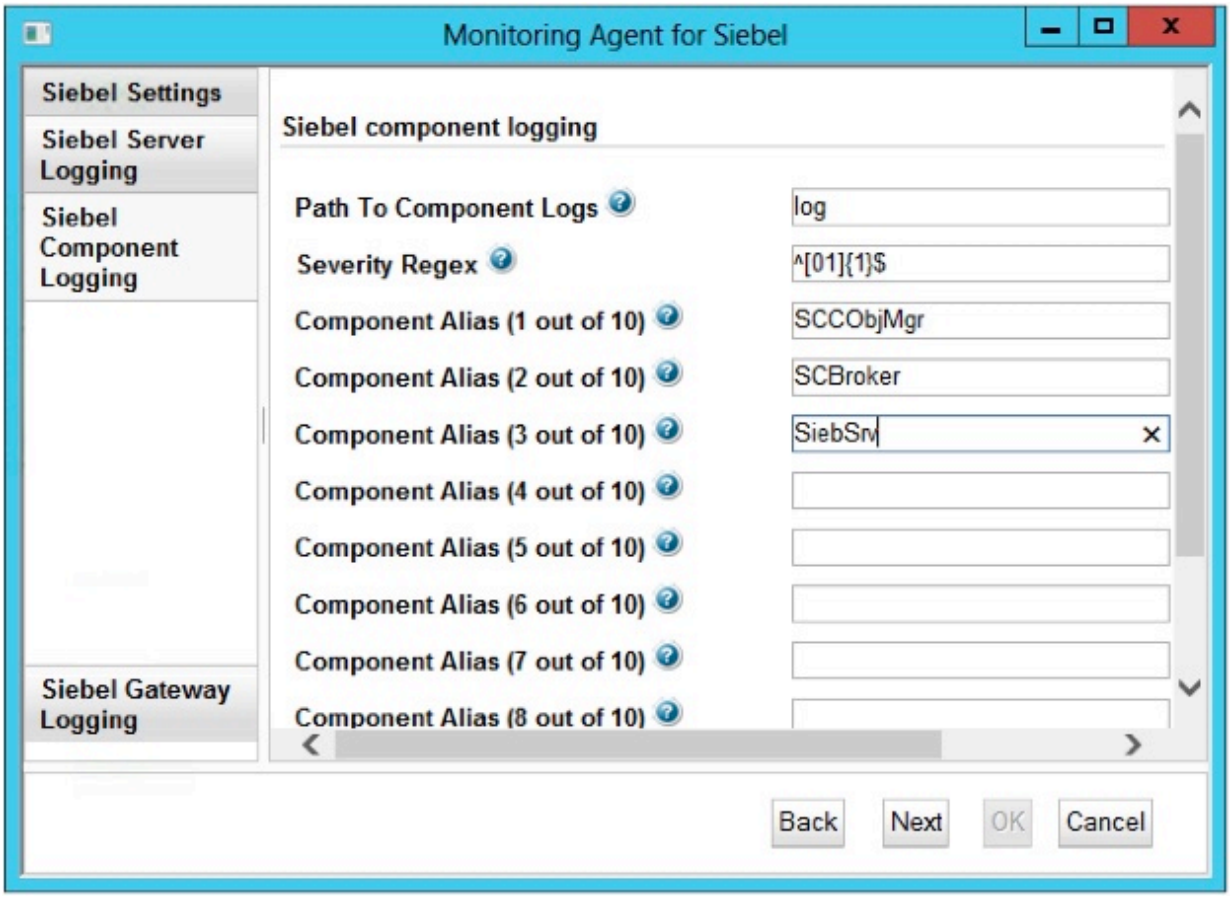


Figura 25. A janela para especificar logs do componente extras que você deseja monitorar.

7. Opcional: Edite os valores para criação de log do gateway Siebel.

   Consulte Tabela 211 na página 783 para obter uma explicação de cada um dos parâmetros de configuração.

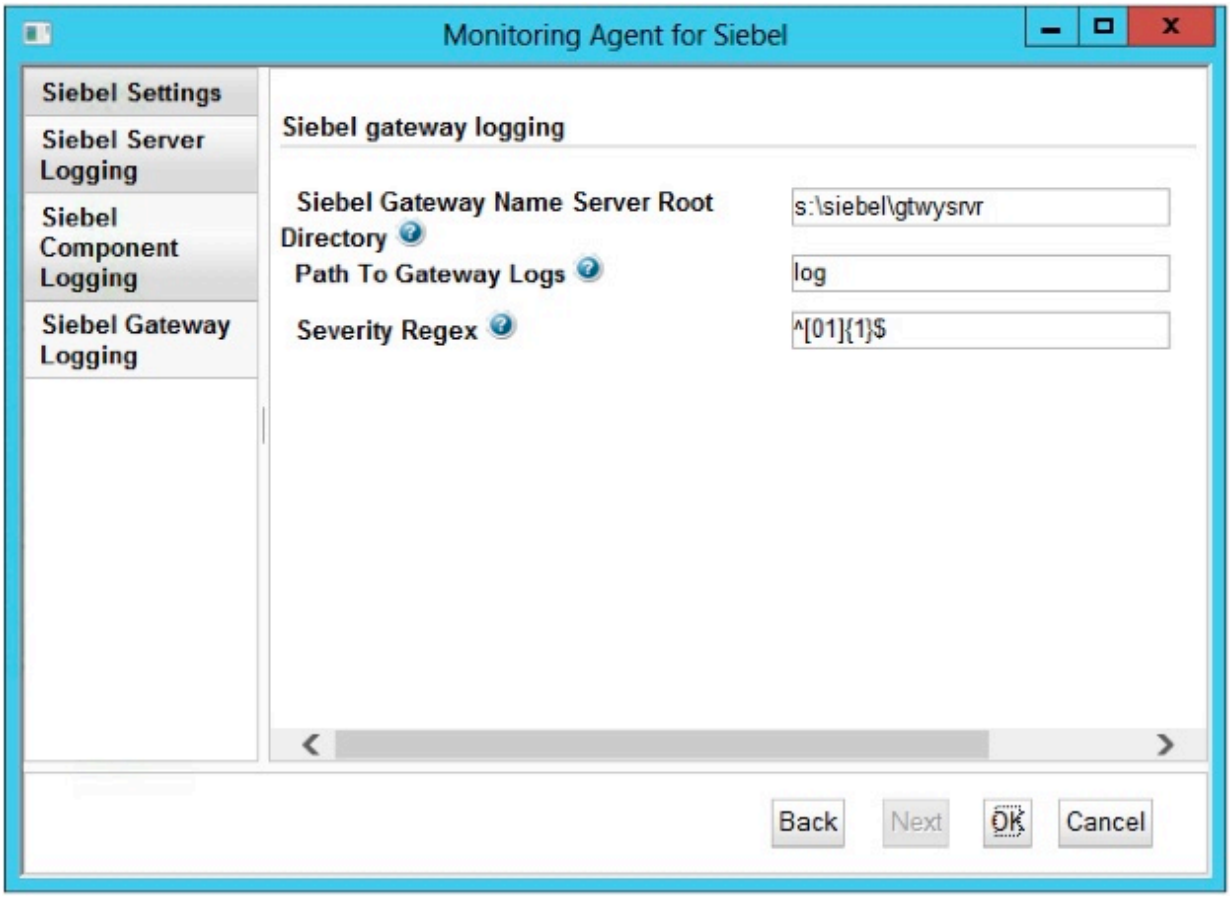


Figura 26. A janela para especificar configurações de criação de log do gateway Siebel.

8. Clique em **OK** para concluir a configuração.
9. Na janela IBM Cloud Application Performance Management, clique com o botão direito na instância configurada e, em seguida, clique em **Iniciar**.

Configurando o agente respondendo aos prompts

Após a instalação do Agente Siebel, deve-se configurá-lo antes de iniciar o agente. Se o Agente Siebel estiver instalado em um computador local Linux ou UNIX, é possível seguir essas instruções para configurá-lo interativamente através de prompts da linha de comandos.

Sobre Esta Tarefa

Lembre-se: Se estiver reconfigurando uma instância do agente configurada, o valor que é definido na última configuração será exibido para cada configuração. Se desejar limpar um valor existente, pressione a tecla Espaço quando a configuração for exibida.

Procedimento

- Siga essas etapas para configurar o Agente Siebel executando um script e respondendo aos prompts.
  a) Na linha de comandos, execute o seguinte comando:

  install_dir/bin/siebel-agent.sh config **instance_name**

  em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome que você deseja fornecer para a instância de agente.

  Exemplo

```
/opt/ibm/apm/agent/bin/siebel-agent.sh config example-inst01
```

b) Responda aos prompts para configurar valores de configuração para o agente.

Consulte "Parâmetros de Configuração para o Agente Siebel" na página 781 para obter uma explicação de cada um dos parâmetros de configuração.

c) Execute o comando a seguir para iniciar o agente:

install_dir/bin/siebel-agent.sh start **instance_name**

em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome da instância de agente.

Exemplo

```
Start example-inst01
```

Configurando o agente usando o arquivo silencioso de resposta

O arquivo de resposta silencioso contém os parâmetros de configuração do agente. É possível editar o arquivo de resposta silencioso para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

O arquivo silencioso de resposta contém os parâmetros de configuração do agente com valores padrão que são definidos para alguns parâmetros. É possível editar o arquivo silencioso de resposta para especificar os valores diferentes para os parâmetros de configuração.

Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

- Para configurar o Agente Siebel no modo silencioso, conclua as seguintes etapas:
  a) Em um editor de texto, abra o arquivo `siebel_silent_config.txt` que está disponível no seguinte caminho:
     – Linux AIX *install_dir*/samples/siebel_silent_config.txt
     – Windows *install_dir*\samples\siebel_silent_config.txt

     em que *install_dir* é o caminho no qual o agente está instalado.

     Exemplo

     – Linux AIX /opt/ibm/apm/agent/samples/siebel_silent_config.txt
     – Windows C:\IBM\APM \samples\siebel_silent_config.txt
  b) No arquivo `siebel_silent_config.txt`, especifique valores para todos os parâmetros obrigatórios. Também é possível modificar os valores padrão de outros parâmetros.

     Consulte "Parâmetros de Configuração para o Agente Siebel" na página 781 para obter uma explicação de cada um dos parâmetros de configuração.

  c) Salve e feche o arquivo `siebel_silent_config.txt` e execute o seguinte comando:
     – Linux AIX *install_dir*/bin/siebel-agent.sh config **instance_name** *install_dir*/samples/siebel_silent_config.txt
     – Windows *install_dir*\bin\siebel-agent.bat config **instance_name** *install_dir*\samples\siebel_silent_config.txt

     em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome da instância de agente.

Importante: Assegure que você inclua o caminho absoluto no arquivo silencioso de resposta. Caso contrário, os dados do agente não serão mostrados nos painéis.

Exemplo

– Linux AIX `/opt/ibm/apm/agent/bin/siebel-agent.sh config example-inst01 /opt/ibm/apm/agent/samples/siebel_silent_config.txt`

– Windows `C:\IBM\APM\bin\ siebel-agent.bat config example-inst01 C:\IBM\APM\samples\siebel_silent_config.txt`

d) Execute o comando a seguir para iniciar o agente:

– Linux AIX *`install_dir`*`/bin/siebel-agent.sh start` **`instance_name`**

– Windows *`install_dir`*`\bin\siebel-agent.bat start` **`instance_name`**

em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome da instância de agente.

Exemplo

– Linux AIX `/opt/ibm/apm/agent/bin/siebel-agent.sh start example-inst01`

– Windows `C:\IBM\APM\bin\siebel-agent.bat start example-inst01`

Parâmetros de Configuração para o Agente Siebel

Os parâmetros de configuração para o Agente Siebel são exibidos em tabelas que os agrupam de acordo com as categorias.

1. Configurações do Siebel - Configurações gerais do ambiente Siebel.
2. Criação de log do servidor Siebel - Configurações específicas para monitorar logs do servidor Siebel.
3. Criação de log do componente Siebel - Configurações específicas para monitorar uma lista customizada de logs do componente Siebel.
4. Criação de log do gateway Siebel - Configurações específicas para monitorar logs do gateway Siebel.

Tabela 208. Configurações do Siebel

Nome de parâmetro	Descrição	Necessário para a opção de tipo de servidor	Nome do parâmetro do arquivo de configuração silenciosa
Tipo(s) de Servidor	Indica os tipos de servidor instalados no computador local.	• **Somente servidor gateway** • **Apenas servidor Siebel** • **Ambos servidores Siebel e Gateway**	**KUY_SERVER_TYPE**
Nome da Empresa	O nome da empresa do Siebel.	• **Apenas servidor Siebel** • **Ambos servidores Siebel e Gateway**	**KUY_ENTERPRISE**

Tabela 208. Configurações do Siebel (continuação)

Nome de parâmetro	Descrição	Necessário para a opção de tipo de servidor	Nome do parâmetro do arquivo de configuração silenciosa
Nome do Siebel Server	O nome do Servidor Siebel a monitorar. **Nota:** Este nome não é o nome do host do servidor. É o nome do servidor que é usado ao executar o comando **srvrmgr** do Siebel.	• **Apenas servidor Siebel** • **Ambos servidores Siebel e Gateway**	**KUY_SERVER**
Nome do gateway Siebel	O Siebel Gateway Name Server para monitorar e opcionalmente a porta, por exemplo, `gtwysrvr` ou `gtwysrvr:1234`.	• **Apenas servidor Siebel** • **Ambos servidores Siebel e Gateway**	**KUY_GATEWAY**
Diretório-raiz do servidor Siebel	O diretório de instalação base para o Siebel Application Server.	• **Apenas servidor Siebel** • **Ambos servidores Siebel e Gateway**	**KUY_INSTALL_ROOT**
ID de administrador do Siebel	O ID do usuário específico do Siebel que o agente usa para autenticar-se no Siebel Enterprise ao executar o comando **srvrmgr**. Por exemplo: `SADMIN`	• **Apenas servidor Siebel** • **Ambos servidores Siebel e Gateway**	**KUY_ADMIN_ID**
Senha de administrador do Siebel	A senha do administrador do Servidor Siebel.	• **Apenas servidor Siebel** • **Ambos servidores Siebel e Gateway**	**KUY_ADMIN_PASSWORD**

Tabela 209. Configurações de criação de log do servidor Siebel

Nome de parâmetro	Descrição	Nome do parâmetro do arquivo de configuração silenciosa
Caminho para logs do servidor	O caminho relativo do "Diretório raiz do Servidor Siebel" para logs do servidor. Para desativar a captura de criação de log do servidor Siebel, insira qualquer caminho inválido. Por exemplo: `xyz`.	**KUY_SERVER_LOGGING_PATH**
Regex de gravidade	A expressão regular usada para capturar logs do servidor Siebel que correspondem a um nível de severidade. Usar o padrão de `^[01]{1}$` facilita a captura de erros nível 0 e nível 1.	**KUY_SERVER_LOGGING_SEVERITY_REGEX**

Tabela 210. Configurações de criação de log do componente Siebel		
Nome de parâmetro	**Descrição**	**Nome do parâmetro do arquivo de configuração silenciosa**
Caminho para logs do componente	O caminho relativo do "Diretório raiz do Servidor Siebel" para logs do servidor. Para desativar a captura de criação de log do servidor Siebel, insira qualquer caminho inválido. Por exemplo: `xyz`.	**KUY_COMPONENT_LOGGING_PATH**
Regex de gravidade	A expressão regular usada para capturar logs do servidor Siebel que correspondem a um nível de severidade. Usar o padrão de `^[01]{1}$` facilita a captura de erros nível 0 e nível 1.	**KUY_COMPONENT_LOGGING_SEVERITY_ REGEX**
Alias do componente (*N* de 10)	O alias do Componente para o qual monitorar um log adicional do Componente. Exemplo: `SCBroker`. em que *N* é 1 - 10 componentes opcionais.	**KUY_CUSTCOMPLOG_00** a **KUY_CUSTCOMPLOG_09**

Tabela 211. Configurações de criação de log do gateway Siebel		
Nome de parâmetro	**Descrição**	**Nome do parâmetro do arquivo de configuração silenciosa**
Diretório-raiz do Siebel Gateway Name Server	O diretório de instalação base para o Servidor de Nomes do Gateway Siebel.	**KUY_GATEWAY_ROOT**
Caminho para logs do gateway	O caminho relativo do Diretório-raiz do Siebel Gateway Name Server para logs do gateway. Para desativar a captura de criação de log do Gateway Name Server, insira qualquer caminho inválido. Por exemplo: `xyz`.	**KUY_GW_LOGGING_PATH**
Regex de gravidade	A expressão regular usada para capturar logs do servidor Siebel que correspondem a um nível de severidade. Usar o padrão de `^[01]{1}$` facilita a captura de erros nível 0 e nível 1.	**KUY_GW_LOGGING_SEVERITY_REGEX**

Logs do componente Siebel que são sempre monitorados

Os logs do componente são sempre monitorados para 10 componentes do Siebel.

Tabela 212. Os aliases e nomes dos componentes do Siebel para os quais os logs do componente são sempre monitorados.	
Alias do componente	**Nome do Componente**
SCCObjMgr	Call Center Object Manager
SMObjMgr	Marketing Object Manager

Tabela 212. Os aliases e nomes dos componentes do Siebel para os quais os logs do componente são sempre monitorados. (continuação)	
Alias do componente	**Nome do Componente**
SSEObjMgr	Sales Object Manager
CommInboundRcvr	Communications Inbound Receiver
CommOutboundMg	Communications Outbound Manager
CommSessionMgr	Communications Session Manager
WorkMon	Workflow Monitor Agent
WfProcBatchMgr	Workflow Process Batch Manager
WfProcMgr	Workflow Process Manager
SiebSrvr	Siebel Server

Configurando o monitoramento do Sterling Connect Direct

Você deve configurar o Agente Sterling Connect Direct para que o agente possa coletar dados dos servidores Connect Direct para monitorar as estatísticas de transferência de arquivos e funcionamento de servidores Connect Direct.

Antes de Iniciar

Revise os pré-requisitos de hardware e de software, consulte Software Product Compatibility Reports para o agente Sterling Connect Direct

Sobre Esta Tarefa

- Para configurar o agente em sistemas Windows, é possível usar a janela IBM Cloud Application Performance Management ou o arquivo silencioso de resposta.
- Para configurar o agente em sistemas Linux, é possível executar o script e responder aos prompts, ou usar o arquivo silencioso de resposta.

Configurando o agente nos sistemas Windows

É possível usar a janela do IBM Cloud Application Performance Management para configurar o agente em sistemas Windows.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito em **Modelo** na coluna **Tarefa/Subsistema** e clique em **Configurar agente**.
3. No campo **Inserir um nome de instância exclusivo**, digite um nome de instância do agente e clique em **OK**.

   Nota: Limite o comprimento do nome da instância de agente. Preferencialmente no intervalo de 7 a 10 caracteres.
4. Na janela **Monitoring Agent for Sterling Connect Direct**, na guia **Detalhes do Connect Direct Server**, especifique valores para os parâmetros de configuração e clique em **OK**.

   Para obter informações sobre os parâmetros de configuração, consulte “Parâmetros de configuração do agente” na página 786.
5. Clique em **Avançar**.

6. Na guia Parâmetros Java, mantenha os valores padrão e clique em **Avançar**.
7. Na guia Configuração do Cliente Java API, clique em **OK**.
8. Na janela **IBM Performance Management**, clique com o botão direito na instância de agente criada e clique em **Iniciar** para iniciar o agente.

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o console, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Configurando o agente nos sistemas Linux

Para configurar o agente em sistemas operacionais Linux, você deve executar o script e responder aos prompts.

Procedimento

1. Na linha de comandos, mude o caminho para o diretório de instalação do agente.
   Exemplo `/opt/ibm/apm/agent/bin`
2. Execute o comando **`/sterling_connect_direct-agent.sh config instance_name`**.

   Nota: O *instance_name* é o nome que você deseja dar à instância de agente.
3. A linha de comandos exibe a mensagem `Editar configuração do 'Monitoring Agent for Sterling Connect Direct'? [1=Sim, 2=Não]`.
4. Insira 1 para editar as configurações.
5. Especifique valores para os parâmetros de configuração quando solicitado. Para obter informações sobre os parâmetros de configuração, consulte "Parâmetros de configuração do agente" na página 786.
6. Execute o comando para iniciar o agente **`./sterling_connect_direct-agent.sh start instance_name`**

O que Fazer Depois
Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Obtenha mais informações sobre como usar o Console do Cloud APM em "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Configurando o agente usando o arquivo silencioso de resposta

O arquivo de resposta silencioso contém os parâmetros de configuração do agente. É possível editar o arquivo de resposta silencioso para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

É possível usar o arquivo silencioso de resposta para configurar o Monitoring Agent for Sterling Connect Direct em sistemas Linux e Windows. Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

1. Abra o arquivo de resposta silencioso presente em *`install_dir`*`/samples/sterling_connect_direct_silent_config.txt` em um editor de texto.

2. Insira o nome do servidor, nome do usuário, senha, diretório de instalação no arquivo e salve o arquivo.
3. No prompt de comandos, acesse *install_dir*/bin e execute o comando

   Linux AIX `./sterling_connect_direct-agent.sh config <Instance_name> install_dir/samples/sterling_connect_direct_silent_config.txt`.

   Windows `./sterling_connect_direct-agent.bat config <Instance_name> install_dir/samples/sterling_connect_direct_silent_config.txt`.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Forum no developerWorks.

Parâmetros de configuração do agente

Ao configurar o Monitoring Agent for Sterling Connect Direct, é possível configurar os valores para parâmetros de configuração.

A tabela a seguir contém descrições detalhadas dos parâmetros de configuração do Monitoring Agent for Sterling Connect Direct.

Tabela 213. Nomes e descrições dos parâmetros de configuração

Nome de parâmetro	Descrição	Campo obrigatório
Nome da instância	O valor padrão para esse campo é idêntico ao valor especificado no campo **Inserir um nome da instância exclusivo**.	Sim
Nome do Servidor	O nome do host ou IP do servidor Sterling Connect Direct.	Sim
Porta do servidor	A porta do servidor Sterling Connect Direct. O valor padrão para o Sterling Connect Direct é 1363.	Sim
Nome de Usuário	O nome do usuário para se conectar ao servidor Sterling Connect Direct.	Sim
Senha	A senha para se conectar ao servidor Sterling Connect Direct.	Sim
Início Java	Caminho para a pasta onde o Java está instalado.	NÃO
Nível de rastreio de Java	O nível de rastreio usado por provedores Java. O valor padrão para o Sterling Connect Direct é Erro	Sim
argumentos da JVM	Este parâmetro permite que você especifique uma lista opcional de argumentos para a JVM (Java Virtual Machine).	NÃO
Caminho da classe para jars externos	O caminho para jars requeridos pelo provedor de dados da API Java que não estão incluídos com o agente.	NÃO

Configurando o monitoramento do Sterling File Gateway

O Monitoring Agent for Sterling File Gateway monitora o aplicativo IBM Sterling File Gateway usando as APIs REST business-to-business (B2B) e o banco de dados de gateway do arquivo. Você deve configurar o Agente Sterling File Gateway para que o agente possa coletar dados das origens de dados e monitorar as estatísticas e o funcionamento do aplicativo Sterling File Gateway. É possível configurar o agente em sistemas Windows e Linux.

Antes de Iniciar

- Revise os pré-requisitos de hardware e de software; consulte Software Product Compatibility Reports para o agente Sterling File Gateway.
- Certifique-se de que as APIs REST B2B estejam instaladas no nó de gateway do arquivo. Para obter informações adicionais sobre a instalação da API REST B2B, consulte "Instalando a API REST B2B" na página 787.

Sobre Esta Tarefa

O Agente Sterling File Gateway é um agente de múltiplas instâncias. Você deve criar a primeira instância e iniciar o agente manualmente.

- Para configurar o agente em sistemas Windows, é possível usar a janela **IBM Performance Management** ou o arquivo de resposta silencioso.
- Para configurar o agente em sistemas Linux, é possível executar o script e responder aos prompts, ou usar o arquivo silencioso de resposta.

Instalando a API REST B2B

É possível instalar e configurar as APIs REST business-to-business (B2B) no nó do Sterling File Gateway. As APIs REST B2B estão disponíveis no instalador do B2B Integrator (V5.2.6.2).

Procedimento

1. Navegue para o diretório `<install_dir>/bin`.

   Em que *install_dir* é o diretório do instalador de agente para o integrador B2B.
2. Execute o seguinte comando:

   - Linux `./InstallService.sh/`*`install_dir`*`/bin/b2bAPIs_10000602.jar`

     Em que *<install_dir>* é o local onde você extraiu o conteúdo do arquivo de mídia.
   - Windows `./InstallService.cmd/`*`install_dir`*`/bin/b2bAPIs_10000602.jar`

     Em que *<install_dir>* é a pasta do instalador do B2B.

Configurando o Agente Sterling File Gateway em sistemas Windows

É possível configurar o Agente Sterling File Gateway em sistemas operacionais Windows usando a janela **IBM Cloud Application Performance Management**. Após fazer a atualização dos valores de configuração, deve-se iniciar o agente para salvar os valores atualizados.

Sobre Esta Tarefa

O Agente Sterling File Gateway fornece valores padrão para alguns parâmetros. É possível especificar diferentes valores para esses parâmetros.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito em **Monitoring Agent for Sterling File Gateway** e, em seguida, clique em **Configurar agente**.

   Lembre-se: Depois de configurar o agente pela primeira vez, a opção **Configurar agente** não estará disponível. Para configurar o agente novamente, clique em **Reconfigurar**.
3. Na janela Agente Sterling File Gateway , conclua as seguintes etapas:

   a) Insira um nome exclusivo para a instância do Agente Sterling File Gateway e clique em **OK**.

b) Na guia **Detalhes da API B2B**, especifique valores para os parâmetros de configuração e, em seguida, clique em **Avançar**.

c) Na guia **Detalhes do banco de dados**, especifique valores para os parâmetros de configuração e, em seguida, clique em **Avançar**.

d) Na guia **API Java**, especifique valores para os parâmetros de configuração e, em seguida, clique em **OK**.

Para obter informações adicionais sobre os parâmetros de configuração em cada guia da janela Agente Sterling File Gateway , consulte os seguintes tópicos:

- "Parâmetros de configuração para os detalhes da API B2B" na página 792
- "Parâmetros de configuração para detalhes do banco de dados" na página 792
- "Parâmetros de configuração para a API Java" na página 792

4. Na janela **IBM Performance Management**, clique com o botão direito em **Agente Sterling File Gateway** e, em seguida, clique em **Iniciar**.

Configurando o Agente Sterling File Gateway em sistemas Linux

É possível executar o script de configuração e responder aos prompts para configurar o Agente Sterling File Gateway nos sistemas operacionais Linux.

Procedimento

1. Acesse a linha de comandos e execute o comando **<install_dir>/bin/sterling_file_gateway-agent.sh config instance_name**.

   Em que *instance_name* é o nome que você deseja dar à instância e *install_dir* é o caminho do diretório de instalação do agente.
2. É solicitado que forneça valores para todos os parâmetros de configuração obrigatórios. É possível modificar os valores padrão de parâmetros de configuração.

   Para obter informações adicionais sobre os parâmetros de configuração, consulte os seguintes tópicos:

   - "Parâmetros de configuração para os detalhes da API B2B" na página 792
   - "Parâmetros de configuração para detalhes do banco de dados" na página 792
   - "Parâmetros de configuração para a API Java" na página 792
3. Para iniciar o agente, execute o comando **<install_dir>/bin/sterling_file_gateway-agent.sh start instance_name**.

Configurando o Agente Sterling File Gateway usando o arquivo de resposta silencioso

É possível usar o arquivo de resposta silencioso para configurar o Agente Sterling File Gateway sem responder aos prompts ao executar o script de configuração. É possível configurar o agente que usa o arquivo de resposta silencioso em sistemas Windows e Linux. O arquivo de resposta silencioso contém os parâmetros de configuração do agente. É possível editar o arquivo de resposta silencioso para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

O arquivo silencioso de resposta contém os parâmetros de configuração do agente com valores padrão que são definidos para alguns parâmetros. É possível editar o arquivo de resposta silencioso para especificar os valores diferentes para os parâmetros de configuração.

Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

- Para configurar o Agente Sterling File Gateway no modo silencioso, conclua as seguintes etapas:
  a) Em um editor de texto, abra o arquivo `sterling_file_gatway_silent_config.txt` que está disponível no seguinte caminho:
     – Linux *install_dir*/samples/sterling_file_gatway_silent_config.txt

       Exemplo **/opt/ibm/apm/agent/samples/sterling_file_gateway_silent_config.txt**
     – Windows *install_dir*\samples\sterling_file_gateway_silent_config.txt

       Exemplo **C:\IBM\APM\samples\sterling_file_gateway_silent_config.txt**
  b) No arquivo `sterling_file_gateway_silent_config.txt`, especifique valores para todos os parâmetros obrigatórios. Também é possível modificar os valores padrão de outros parâmetros.

     Para obter informações adicionais sobre os parâmetros de configuração, consulte os seguintes tópicos:
     – "Parâmetros de configuração para os detalhes da API B2B" na página 792
     – "Parâmetros de configuração para detalhes do banco de dados" na página 792
     – "Parâmetros de configuração para a API Java" na página 792
  c) Salve e feche o arquivo `sterling_file_gateway_silent_config.txt` e execute o seguinte comando:
     – Linux *install_dir*/bin/sterling_file_gateway-agent.sh config *instance_name* *install_dir*/samples/sterling_file_gateway_silent_config.txt

       Exemplo **/opt/ibm/apm/agent/bin/sterling_file_gateway-agent.sh config instance_name /opt/ibm/apm/agent/samples/sterling_file_gateway_silent_config.txt**
     – Windows *install_dir*/bin/sterling_file_gateway-agent.bat config *instance_name* *install_dir*/samples/sterling_file_gateway_silent_config.txt

       Exemplo **C:\IBM\APM\bin\sterling_file_gateway-agent.bat config instance_name C:\IBM\APM\samples\sterling_file_gateway_silent_config.txt**

       Em que *instance_name* é o nome que você deseja dar à instância e *install_dir* é o caminho onde o agente está instalado.

     Importante: Assegure que você inclua o caminho absoluto no arquivo de resposta silencioso. Caso contrário, os dados do agente não serão mostrados nos painéis.
  d) Execute o comando a seguir para iniciar o agente:
     – Linux *install_dir*/bin/sterling_file_gateway-agent.sh start *instance_name*

       Exemplo **/opt/ibm/apm/agent/bin/sterling_file_gateway-agent.sh start instance_name**
     – Windows *install_dir*\bin\sterling_file_gateway-agent.bat start *instance_name*

       Exemplo **C:\IBM\APM\bin\sterling_file_gateway-agent.bat start instance_name**

Configurando variáveis de ambiente do agente para o provedor de dados no Linux

É possível configurar as variáveis de ambiente do Agente Sterling File Gateway para o provedor de dados em sistemas operacionais Linux.

Sobre Esta Tarefa

O Agente Sterling File Gateway fornece variáveis de ambiente que podem ser configuradas para o provedor de dados.

Procedimento

1. Acesse o diretório `<install_dir>/agent/config`.
2. Abra o arquivo `.fg.environment` em um editor e edite as variáveis de ambiente.

   Para obter informações adicionais sobre as variáveis de ambiente do agente que podem ser configuradas, consulte "Variáveis de ambiente para o provedor de dados" na página 790.

Configurando variáveis de ambiente do agente para o provedor de dados no Windows

É possível configurar as variáveis de ambiente do Agente Sterling File Gateway para o provedor de dados em sistemas operacionais Windows usando a janela **IBM Performance Management**.

Sobre Esta Tarefa

O Agente Sterling File Gateway fornece variáveis de ambiente que podem ser configuradas para o provedor de dados.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > > **Agentes de Monitoramento IBM** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito na instância de agente e clique em **Avançado** > **Editar arquivo ENV** e edite os valores padrão para as variáveis de ambiente.

   Para obter informações adicionais sobre as variáveis de ambiente do agente que podem ser configuradas, consulte "Variáveis de ambiente para o provedor de dados" na página 790.

Variáveis de ambiente para o provedor de dados

Depois de configurar o Agente Sterling File Gateway , é possível modificar alguns valores de duração de limite relacionados à coleta de dados do agente. É possível especificar esses valores no arquivo de ambiente do agente.

A tabela a seguir contém uma descrição detalhada das variáveis de ambiente para o provedor de dados.

Tabela 214. Nome e descrição das variáveis de ambiente para o provedor de dados

Nome do parâmetro	Descrição
Duração da coleta para transferência de arquivos (em horas) (**KFG_FILE_ARRIVED_INTERVAL**)	A duração, em horas, na qual o agente coleta dados para transferências de arquivos. O valor padrão é 24 horas.
Intervalos de coleta para atividades de transferência de arquivos que são exibidas como um gráfico de linha (em horas) (**KFG_FILE_ACTIVITY_INTERVAL**)	A duração, em horas, na qual o agente coleta dados para atividades de transferência de arquivos. O valor padrão é 1 hora. Por exemplo, o agente coleta as atividades de transferência de arquivos que ocorreram na última hora. Esses dados são visíveis em termos de gráficos de linha na página da instância. O valor padrão é 1 hora.

Tabela 214. Nome e descrição das variáveis de ambiente para o provedor de dados (continuação)	
Nome do parâmetro	**Descrição**
Intervalo limite para parceiros inativos (em dias) (**KFG_INACTIVE_PARTNERS_INTERVAL**)	A duração de limite quando o parceiro está inativo, ou não recebeu ou fez upload de nenhum arquivo. O valor-padrão é 10 dias. Por exemplo, se algum parceiro não recebeu ou transferiu um arquivo nos últimos 10 dias, ele será exibido como "Inativo" no agente.
Número máximo de arquivos de log do provedor de dados (**KFG_LOG_FILE_MAX_COUNT**)	O número máximo de arquivos de log que o provedor de dados cria antes de sobrescrever os arquivos de log anteriores. O valor padrão é 10.
Tamanho máximo, em KB, de cada log do provedor de dados (**KFG_LOG_FILE_MAX_SIZE**)	O tamanho máximo em KB que um provedor de dados deve atingir antes de o provedor de dados criar um novo arquivo de log. O valor padrão são 5190 KB.
Nível de detalhe no log do provedor de dados (**KFG_LOG_LEVEL**)	O nível de detalhes que são incluídos no arquivo de log criado pelo provedor de dados. O valor padrão é 4 (Informativo). Os seguintes valores são válidos: • 1 (Desativado): nenhuma mensagem é registrada. • 2 (Grave): somente erros são registrados. • 3 (Aviso): Todos os erros e mensagens que são registrados no nível grave e possíveis erros que podem resultar em comportamento indesejado. • 4 (Informativo): Todos os erros e mensagens que são registrados no nível de aviso e mensagens informativas de alto nível que descrevem o estado do provedor de dados quando ele é processado. • 5 (Bom): Todos os erros e mensagens que são registrados no nível informativo e mensagens informativas de baixo nível que descrevem o estado do provedor de dados quando ele é processado. • 6 (Melhor): Todos os erros e mensagens que são registrados no nível bom, mas mensagens informativas detalhadas, como informações de criação de perfil de desempenho e dados de depuração. Selecionar essa opção pode afetar de maneira adversa o desempenho do agente de monitoramento. Esta configuração é destinada apenas como uma ferramenta para determinação de problema junto com a equipe de suporte IBM. • 7 (Excelente): Todos os erros e mensagens que são registrados no nível Bom e as mensagens informativas mais detalhadas que incluem mensagens e dados de programação de baixo nível. Selecionar essa opção pode afetar negativamente o desempenho do agente de monitoramento. Esta configuração é destinada apenas como uma ferramenta para determinação de problema junto com a equipe de suporte IBM. • 8 (Todos): todos os erros e mensagens são registrados.
Buscando eventos para todas as transferências de arquivos (**KFG_ALL_FGEVENTS**)	A sinalização para buscar eventos para todas as transferências de arquivos. Os valores válidos são `Sim` ou `Não`. O valor padrão é `Não`. Se o valor for configurado como `Não`, o agente buscará eventos para transferências de arquivos com falha para uma duração configurável do usuário. Se o valor for configurado como `Sim`, o agente buscará eventos para todas as transferências de arquivos para um duração configurável do usuário.

Parâmetros de configuração para os detalhes da API B2B

Ao configurar o Agente Sterling File Gateway , você deve especificar valores dos parâmetros de configuração para os detalhes da API business-to-business (B2B).

A tabela a seguir contém a descrição detalhada dos parâmetros de configuração para os detalhes da API B2B.

Tabela 215. Nome e descrição dos parâmetros de configuração para os detalhes da API B2B

Nome do parâmetro	**Descrição**
Nome da instância (**KFG_Instance_Name**)	O nome da instância. **Restrição:** O campo Nome da instância exibe o nome da instância especificada ao configurar o agente pela primeira vez. Ao configurar o agente novamente, não é possível mudar o nome da instância do agente.
Nome do servidor (**KFG_API_SERVICES_Node_ADDRESS**)	O nome do host ou endereço IP do serviço da API B2B.
Porta do servidor (**KFG_API_SERVICES_PORT**)	A porta da API B2B.
Nome do usuário (**KFG_API_SERVICES_USERNAME**)	Um nome do usuário para se conectar ao serviço da API B2B.
Senha (**KFG_API_SERVICES_PASSWORD**)	A senha para o nome do usuário usado para se conectar ao serviço da API B2B.

Parâmetros de configuração para detalhes do banco de dados

Ao configurar o Agente Sterling File Gateway , você deve especificar valores dos parâmetros de configuração para os detalhes do banco de dados.

A tabela a seguir contém a descrição detalhada dos parâmetros de configuração para os detalhes do banco de dados.

Tabela 216. Nome e descrição dos parâmetros de configuração para os detalhes do banco de dados

Nome do parâmetro	**Descrição**
Nome do servidor de banco de dados (**KFG_DB_Node_ADDRESS**)	O nome do host ou endereço IP do servidor de banco de dados Sterling File Gateway.
Usuário do banco de dados (**KFG_DB_USERNAME**)	O nome do usuário do banco de dados.
Senha do banco de dados (**KFG_DB_PASSWORD**)	A senha do banco de dados.
Porta do banco de dados (**KFG_DB_PORT**)	A porta do banco de dados.
Tipo de banco de dados (**KFG_DB_TYPE**)	O tipo do banco de dados.

Parâmetros de configuração para a API Java

Ao configurar o Agente Sterling File Gateway , você deve especificar valores dos parâmetros de configuração para a API Java.

A tabela a seguir contém a descrição detalhada dos parâmetros de configuração para a API Java.

Tabela 217. Nome e descrição dos parâmetros de configuração para a API Java	
Nome do parâmetro	**Descrição**
Caminho da classe para o JAR externo (**KFG_CLASSPATH**)	O caminho do arquivo JAR do driver de banco de dados que você deseja especificar para o banco de dados correspondente.

Configurando o monitoramento do Sybase Server

O Sybase agent oferece um ponto central de gerenciamento para bancos de dados distribuídos. Ela coleta as informações necessárias para administradores de bancos de dados e de sistemas examinarem o desempenho do sistema do servidor Sybase, detectar problemas antecipadamente e evitá-los. Os administradores do banco de dados e do sistema podem configurar os níveis e as sinalizações de limite necessários para acionar alertas quando o sistema atinge esses limites.
Deve-se configurar o Monitoring Agent for Sybase Server para monitorar o servidor Sybase.

Antes de Iniciar

Revise os pré-requisitos de hardware e software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Sybase agent.

Sobre Esta Tarefa

As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte “Histórico de Mudanças” na página 50.

O Sybase agent é um agente de instância múltipla, será preciso configurar e iniciar cada instância de agente manualmente.

Procedimento

1. Configure o agente de monitoramento.
   - “Configurando o agente usando a interface da linha de comandos” na página 795
   - “Configurando o agente usando o arquivo silencioso de resposta” na página 796
2. Inicie e pare o agente de monitoramento usando o comando do agente **sybase-agent**.

   Para obter mais informações sobre o **sybase-agent**, consulte *Usando comandos do agente* em https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm.
3. Conecte o agente de monitoramento ao servidor Performance Management usando o comando **agent2server**.

   Para obter mais informações sobre o **agent2server**, consulte *Usando comandos do agente* em https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm.

Concedendo permissões

Deve-se conceder permissões para o ID do usuário que é usado para monitorar o servidor Sybase.

Antes de Iniciar

Instale o Sybase agent.

Deve-se ter a função de administrador de banco de dados para conceder permissões.

Sobre Esta Tarefa

O ID do usuário que é usado pelo agente de monitoramento deve ter acesso às tabelas do Sybase e às tabelas do monitor instaladas.

É possível executar as seguintes tarefas:

- Crie um ID do usuário para o agente de monitoramento.
- Conceda permissão para o novo ID do usuário e para as tabelas do monitor instaladas.

Se você não estiver executando o Sybase agent como usuário `root`, certifique-se de que o ID do usuário pertença ao grupo `Sybase` e que tenha acesso somente leitura aos arquivos de log do Sybase.

Procedimento

1. Insira o comando para o sistema operacional que você está usando.
   - Windows

     ```
     cd  install_dir \tmaitm6\SQLLIB
     ```

   - UNIX

     ```
     cd  install_dir /misc
     ```

   Em que, *install_dir* é o diretório inicial no qual o servidor Sybase está instalado.
2. Use o comando **isql** para efetuar login no servidor Sybase como usuário `sa`.
3. Execute o comando a seguir para configurar o ID que é usado pelo agente Sybase para comunicar-se com o servidor Sybase:

   ```
   1 > sp_addlogin  user_name,  password  2 > g
   ```

   Em que:

   - *user_name* é o ID do usuário. Por padrão, ele é `tivoli`.

     Se o ID do usuário não for `tivoli`, edite o arquivo `koygrant.sql` e mude o `tivoli` para o ID do usuário correto.
   - *senha* é a senha do usuário.

   Nota:

   Local do arquivo `koygrant.sql` :

   - Windows `\opt\ibm\apm\agent\misc\`
   - UNIX `/opt/ibm/apm/agent/misc/`
4. Execute o comando a seguir para conceder permissão para as tabelas no banco de dados:

   ```
   isql -U sa -P password -S servername -i koygrant_filepathkoygrant.sql
   ```

   Em que:

   - *password* é a senha do usuário `sa`.
   - *servername* é o nome do servidor de banco de dados.
   - *koygrant_filepath* está no seguinte local:

     Nota:

     – Windows `\opt\ibm\apm\agent\misc\`

     – UNIX `/opt/ibm/apm/agent/misc/`
5. Execute o comando a seguir para criar tabelas proxy que sejam usadas para as tabelas do monitor instaladas:

```
isql -U sa -P password -S servername
     -i $SYBASE/ASE-12_5/scripts/installmontables
```

Em que:

- *password* é a senha do usuário sa.
- *servername* é o nome do servidor de banco de dados.

O que Fazer Depois

Quando as permissões forem concedidas com sucesso, será possível configurar o agente de monitoramento.

Configurando o agente usando a interface da linha de comandos

É possível configurar o Monitoring Agent for Sybase Server usando a interface da linha de comandos.

Antes de Iniciar

O Sybase agent não suporta configuração remota. Portanto, será necessário garantir que o servidor Sybase esteja instalado no mesmo host no qual o Sybase agent foi instalado.

O Sybase agent suporta somente o Sybase Server versão 15.7 e 16.0 .

O ID do usuário usado para conectar-se ao servidor de banco de dados é criado.

Sobre Esta Tarefa

O Sybase agent é um agente de instância múltipla, será preciso configurar e iniciar cada instância de agente manualmente.

Procedimento

1. Execute o comando a seguir para configurar o agente.
   - Windows

     ```
     install_dir \bin\sybase-agent.bat  instance_name
     ```

   - UNIX

     ```
     install_dir /bin/sybase-agent.sh  instance_name
     ```

   Em que:

   - *install_dir* é o diretório de instalação do agente.
   - *instance_name* é o nome da instância de servidor Sybase.
2. Quando for solicitado a fornecer valores para os seguintes parâmetros, pressione Enter para aceitar o valor padrão ou especifique um valor e pressione Enter.
   a) Para o parâmetro Home Directory, insira o caminho do diretório inicial do servidor Sybase.
      - Windows

        O exemplo de Home Directory é \opt\sybase.
      - UNIX

        O exemplo de Home Directory é /opt/sybase.

   b) Para o parâmetro ASE Directory, insira o caminho do servidor de banco de dados ASE.
      - Windows

        O exemplo de ASE Directory é \opt\sybase\ASE-12_5.

- UNIX

  O exemplo de ASE Directory é /opt/sybase/ASE-12_5.

c) Para o parâmetro Open Client Directory, insira o local de instalação do cliente aberto do Sybase.

- Windows

  O exemplo de Open Client Directory é \opt\sap\ocs-16_0.

- UNIX

  O exemplo de Open Client Directory é /opt/sap/ocs-16_0.

d) Para o parâmetro USER ID, insira o ID do usuário que é usado pelo agente de monitoramento para conectar-se ao servidor Sybase.

O USER ID padrão é tivoli.

e) Para o parâmetro PASSWORD, insira a senha do ID do usuário que é usado pelo agente de monitoramento para conectar-se ao servidor Sybase.

f) Para o parâmetro VERSION, insira a versão do servidor Sybase.

O Sybase agent suporta somente as versões 15.7 e 16.0 do servidor Sybase.

g) Para o parâmetro ERROR LOG FILE, insira o nome completo do arquivo de log de erros para o servidor Sybase.

- Windows

  O exemplo de ERROR LOG FILE é \opt\sap\ASE-16_0\install*servername*.log.

- UNIX

  O exemplo de ERROR LOG FILE é /opt/sap/ASE-16_0/install/*servername*.log.

Em que *servername* é o nome do servidor Sybase.

h) Para o parâmetro EXTENDED, insira o parâmetro estendido que é usado pelo suporte para excluir determinada execução do cursor. Opcionalmente, pressione Enter sem especificar quaisquer valores para executar todos os cursores.

As opções para o parâmetro EXTENDED são DBD2,DBD15,KOYSEGD.

- DBD2 excluirá a execução do cursor para conjuntos de dados Sybase_Database_Detail e Sybase_Database_Summary.
- DBD15 excluirá a execução do cursor para o conjunto de dados Sybase_Database_Detail.
- KOYSEGD excluirá a execução do cursor para o conjunto de dados Sybase_Segment_Detail.

O que Fazer Depois

Ao concluir a configuração, será possível iniciar o agente de monitoramento e conectá-lo ao servidor de gerenciamento de desempenho.

Para iniciar o Sybase agent, use o comando do agente sybase-agent.

Para conectar o Sybase agent ao servidor Performance Management, use o comando agent2server.

Para obter mais informações sobre os comandos sybase-agent e agent2server, consulte *Usando comandos do agente* em https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm.

Configurando o agente usando o arquivo silencioso de resposta

É possível configurar o Monitoring Agent for Sybase Server usando o arquivo de resposta silencioso.

Antes de Iniciar

O Sybase agent não suporta configuração remota. Portanto, será necessário garantir que o servidor Sybase esteja instalado no mesmo host no qual o Sybase agent foi instalado.

O Sybase agent suporta somente o Sybase Server versão 15.7 e 16.0 .

O ID do usuário usado para conectar-se ao servidor de banco de dados é criado.

Sobre Esta Tarefa

O Sybase agent é um agente de instância múltipla, será preciso configurar e iniciar cada instância de agente manualmente.

Deve-se editar o arquivo de resposta silencioso e executar o comando do agente para configurar o agente de monitoramento.

Procedimento

1. Edite o arquivo de resposta silencioso.
   - Windows

     O arquivo de resposta silencioso está em: *install_dir*\samples\sybase_silent_config.txt.
   - UNIX

     O arquivo de resposta silencioso está em: *install_dir*/samples/sybase_silent_config.txt.

   Em que *install_dir* é o diretório de instalação do agente.

   a) Para o parâmetro Home Directory, especifique o caminho do diretório inicial do servidor Sybase.
      - Windows

        O exemplo de Home Directory é \opt\sybase.
      - UNIX

        O exemplo de Home Directory é /opt/sybase.

   b) Para o parâmetro ASE Directory, especifique o caminho do servidor de banco de dados ASE.
      - Windows

        O exemplo de ASE Directory é \opt\sybase\ASE-12_5.
      - UNIX

        O exemplo de ASE Directory é /opt/sybase/ASE-12_5.

   c) Para o parâmetro Open Client Directory, especifique o local de instalação do cliente aberto do Sybase.
      - Windows

        O exemplo de Open Client Directory é \opt\sap\ocs-16_0.
      - UNIX

        O exemplo de Open Client Directory é /opt/sap/ocs-16_0.

   d) Para o parâmetro USER ID, especifique o ID do usuário que é usado pelo agente de monitoramento para conectar-se com o servidor Sybase.

      O USER ID padrão é tivoli.

   e) Para o parâmetro PASSWORD, especifique a senha do ID do usuário que é usado pelo agente de monitoramento para conectar-se ao servidor Sybase.

   f) Para o parâmetro VERSION, especifique a versão do servidor Sybase.

O Sybase agent suporta somente as versões 15.7 e 16.0 do servidor Sybase.

g) Para o parâmetro ERROR LOG FILE, especifique o nome completo do arquivo de log de erros para o servidor Sybase.

- Windows

  O exemplo de ERROR LOG FILE é \opt\sap\ASE-16_0\install*servername*.log.

- UNIX

  O exemplo de ERROR LOG FILE é /opt/sap/ASE-16_0/install/*servername*.log.

Em que *servername* é o nome do servidor Sybase.

h) Para o parâmetro EXTENDED, especifique o parâmetro estendido que é usado pelo suporte para excluir determinada execução do cursor. Opcionalmente, deixe-o em branco para executar todos os cursores.

As opções para EXTENDED são DBD2,DBD15,KOYSEGD.

- DBD2 excluirá a execução do cursor para conjuntos de dados Sybase_Database_Detail e Sybase_Database_Summary.
- DBD15 excluirá a execução do cursor para o conjunto de dados Sybase_Database_Detail.
- KOYSEGD excluirá a execução do cursor para o conjunto de dados Sybase_Segment_Detail.

2. Salve o arquivo de resposta silencioso.
3. Execute o comando do agente a seguir para configurar o agente de monitoramento.

- Windows

```
install_dir\bin\sybase-agent.bat config instance_name
 install_dir \samples\sybase_silent_config.txt
```

- UNIX

```
install_dir/bin/sybase-agent.sh config instance_name
 install_dir /samples/sybase_silent_config.txt
```

Em que:

- *install_dir* é o diretório de instalação do agente.
- *instance_name* é o nome do servidor Sybase.

O que Fazer Depois

Ao concluir a configuração, será possível iniciar o agente de monitoramento e conectá-lo ao servidor de gerenciamento de desempenho.

Para iniciar o Sybase agent, use o comando **sybase-agent**.

Para conectar o Sybase agent ao servidor Performance Management, use o comando **agent2server**.

Para obter mais informações sobre os comandos **sybase-agent** e **agent2server**, consulte *Usando comandos do agente* em https://www.ibm.com/support/knowledgecenter/SSHLNR_8.1.4/com.ibm.pm.doc/welcome.htm.

Desativando leituras sujas para consulta

O Sybase agent permite leituras sujas para sua execução de consulta por padrão para evitar bloqueios.
A variável COLL_USE_NOLOCK é usada para ativar ou desativar leitura suja da consulta.
Quando a leitura suja é ativada, a consulta é executada com nível de isolamento zero para evitar bloqueios.
Se quiser desativar as leituras sujas para a consulta do agente, é possível configurar a variável COLL_USE_NOLOCK para zero.

Antes de Iniciar

Para desativar `leituras sujas` para a consulta de agente, assegure-se de que o agente esteja instalado.

Sobre Esta Tarefa

O Sybase agent permite `leituras sujas` por padrão. Para desativar as `leituras sujas` para a consulta de agente, conclua as seguintes etapas.

Procedimento

1. Parar o agente.
2. Configure a variável `COLL_USE_NOLOCK` para zero.
   - UNIX
     a. Inclua **`COLL_USE_NOLOCK=0`** no arquivo *`CANDLEHOME`*`/config/.oy.environment`.
     b. Salve e feche o arquivo.
   - Windows
     a. Localize o arquivo de instância de agente *`CANDLEHOME`*`\TMAITM6_x64\KOYENV_`*`INSTANCENAME`*.
     b. Inclua a seguinte linha no arquivo:

        `COLL_USE_NOLOCK=0`

     c. Salve e feche o arquivo.

   O *`CANDLEHOME`* é o diretório de instalação do agente.
   O *`INSTANCENAME`* é o nome da instância do agente.
3. Inicie o agente.

Configurando o monitoramento da Reprodução Sintética

Deve-se configurar o Synthetic Playback agent para que o agente possa coletar dados sobre a disponibilidade e o desempenho de aplicativos da web internos. Esses dados são exibidos no Application Performance Dashboard.

Sobre Esta Tarefa

Configure o Synthetic Playback agent executando um script e respondendo aos prompts. Em seguida, inicie o script e verifique se ele está em execução.

Importante: Somente usuários existentes do complemento do IBM Website Monitoring on Cloud podem instalar, configurar e executar o Synthetic Playback agent. Website Monitoring foi substituído pelo IBM Cloud Availability Monitoring. Para obter mais informações, consulte “Sobre o Monitoramento de Disponibilidade” na página 1045.

Procedimento

- Para configurar o agente executando o script e respondendo aos prompts, conclua as seguintes etapas:
  a) Insira *`install_dir`*`/bin/synthetic_playback-agent.sh config`, em que *install_dir* é o diretório de instalação do Synthetic Playback agent.
  b) Quando solicitado `Editar o Agente de monitoramento para configurações de reprodução sintética`, insira 1 para continuar.
  c) Quando for solicitado que você insira o nome do datacenter para seu ponto de presença de reprodução, insira um nome que identifique a localização do agente.

Importante: Escolha um nome descritivo para seu ponto de presença de reprodução. Quando você conclui a instalação do agente, é possível selecionar a localização por nome como uma localização de reprodução de suas transações sintéticas e visualizar dados da transação a partir desse local no Application Performance Dashboard.

d) Quando você solicitado que você forneça `Parâmetros Java`, escolha `Nível de Rastreio Java`. Pressione Enter para escolher o parâmetro padrão ou insira um número de 1 a 8 para especificar o nível de rastreio.

e) Quando for solicitado que você forneça `Caminho da Classe para jars Externos`, pressione Enter para deixar em branco ou especifique a localização do jar externo.

- Para configurar o agente usando o arquivo de resposta silencioso, conclua as etapas a seguir:

  a) Em um editor de texto, abra o arquivo `synthetic_playback_silent_config.txt` que está disponível no caminho *install_dir*`/samples`.
  Por exemplo

  Linux `/opt/ibm/apm/agent/samples`

  b) No arquivo `synthetic_playback_silent_config.txt`, remova o comentário e designe valores às seguintes propriedades:

  – Para `LOCATION`, iguale esse parâmetro ao nome do seu datacenter ou um nome que descreva onde seu agente está instalado.

  – Para `JAVA_TRACE_LEVEL`, iguale este parâmetro a um dos níveis de rastreio listados, como `JAVA_TRACE_LEVEL=ERROR`.

  Salve o arquivo.

  c) Na linha de comandos, mude o caminho para *install_dir*`/bin`.

  d) Execute o seguinte comando para configurar o agente no modo silencioso:

```
synthetic_playback-agent.sh config install_dir/samples/
synthetic_playback_silent_config.txt
```

- Para iniciar o Synthetic Playback agent, insira: *install_dir*`/bin/synthetic_playback-agent.sh start`.
- Para verificar se o Synthetic Playback agent está em execução, insira: *install_dir*`/bin/synthetic_playback-agent.sh status`. Para obter mais informações, consulte Tabela 12 na página 178.

O que Fazer Depois
Para visualizar o desempenho de aplicativos da web internos, deve-se criar transações sintéticas no Gerenciador de Script Sintético. Para obter mais informações, consulte “Gerenciando transações e eventos sintéticos com o Website Monitoring” na página 1026.

Ativando o Suporte do Proxy de Envio de Dados para o Synthetic Playback agent

Ative o suporte de proxy de envio de dados para o Synthetic Playback agent para monitorar solicitações HTTP de aplicativos web internos para aplicativos web externos.

Antes de Iniciar
Assegure-se de estar executando o Synthetic Playback agent versão 01.00.05.08 ou posterior. Para verificar qual a versão do agente em execução, insira *install_dir*`/bin/cinfo -t` na linha de comandos, onde *install_dir* é o local de instalação do agente. Se você estiver executando qualquer outra versão do Synthetic Playback agent, será necessário fazer download e instalar a correção temporária 08 do IBM Cloud Application Performance Management, Private 8.1.4.0 Synthetic Playback agent a partir do IBM Fix Central (insira `Sintético` no campo **Procura** e a lista de correções temporárias do Synthetic Playback agent será exibida). Para obter instruções de instalação, consulte 8.1.4.0-IBM-IPM-SYNTHETIC-PLAYBACK-AGENT-IF0008 Readme.

Sobre Esta Tarefa

Aplicativos web internos por trás de um firewall corporativo requerem um proxy de envio de dados para acessar recursos externos da web. Configure a definição de proxy do Synthetic Playback agent para permitir que seu agente suporte o proxy de envio de dados, de modo que seja possível monitorar solicitações de HTTP de aplicativos da web internos para aplicativos da web externos.

Procedimento

- Para configurar e ativar o suporte de proxy de envio de dados para seu agente, conclua as etapas a seguir.
  a) Como usuário raiz, configure as definições de proxy executando os seguintes comandos na linha de comandos.

```
cd install_dir/agent/lx8266/sn/bin
#./set_proxy.sh
```

  Quando solicitado, insira o caminho da instalação do agente, cujo caminho padrão é `/opt/ibm/apm/agent`. Insira o número para o tipo de proxy que deseja configurar para o Synthetic Playback agent.

  Por exemplo:

```
# cd /install_dir/agent/lx8266/sn/bin/
#./set_proxy.sh
please input the agent install path, default is (/opt/ibm/apm/agent)
agent install path is:/opt/ibm/apm/agent
please input the number of proxy type:
1 system proxy
2 manual proxy
3 pac proxy
4 no proxy
```

  b) Insira *install_dir*`/bin/synthetic_playback-agent.sh start` para reiniciar seu agente.
- Linux Para desativar o suporte ao proxy de envio de dados para seu agente, execute o comando `./set_proxy.sh` novamente e selecione `4 no proxy`. Em seguida, reinicie o agente.

Configurando o monitoramento do Tomcat

É possível configurar o Monitoring Agent for Tomcat com as configurações padrão ou customizadas para monitorar os recursos de servidores de aplicativos Tomcat. O agente pode ser configurado em sistemas Windows e Linux.

Antes de Iniciar

Revise os pré-requisitos de hardware e software. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Agente Tomcat.

Sobre Esta Tarefa

O Agente Tomcat é um agente de múltiplas instâncias; você deve criar a primeira instância e iniciar o agente manualmente. O nome do sistema gerenciado inclui o nome da instância especificada, por exemplo *instance_name*`:`*host_name*`:`*pc*, em que *pc* é o código de produto de dois caracteres. O nome do sistema gerenciado é limitado a 32 caracteres. O nome da instância especificado é limitado a 28 caracteres que exclui o comprimento do nome do host. Por exemplo, se você especificar `TOMCAT2` como o nome da instância, o nome do sistema gerenciado será `TOMCAT2:hostname:OT`. Se você especificar um nome de instância longo, o nome do sistema gerenciado será truncado e o código do agente não será exibido completamente.

Para evitar problemas de permissão ao configurar o agente, certifique-se de utilizar o mesmo ID de usuário raiz ou de usuário não raiz que foi utilizado para instalar o agente. Se você instalou o seu agente como um usuário selecionado e deseja configurar o agente como um usuário diferente, consulte

"Configurando agentes como um usuário não raiz" na página 181. Se você instalou e configurou seu agente como um usuário selecionado e deseja iniciar o agente como um usuário diferente, consulte "Iniciando agentes como um usuário não raiz" na página 1012.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte o "Histórico de Mudanças" na página 50.

Configurando o Agente Tomcat com as configurações padrão

É possível usar as configurações padrão do Agente Tomcat para monitorar o servidor Tomcat. Não é preciso fornecer mais informações de configuração além do novo nome da instância.

Antes de Iniciar

Antes de configurar o agente com as configurações padrão, certifique-se de que os seguintes pré-requisitos sejam atendidos:

- O agente está instalado no diretório padrão.
- A URL do serviço JMX que usa a porta 8686.
- O servidor Tomcat é configurado sem a autorização JMX.

Sobre Esta Tarefa

Lembre-se: Ao configurar o agente com as configurações padrão, a coleta de dados diagnósticos de rastreamento de transação e de detalhamento não é ativada.

Procedimento

1. Execute o seguinte comando:
   Linux `install_dir/bin/tomcat-agent.sh config instance_name install_dir/samples/tomcat_silent_config.txt`
   Windows `install_dir\bin\tomcat-agent.bat config instance_name install_dir\samples\tomcat_silent_config.txt`
   Where
   install_dir
   O diretório de instalação do Agente Tomcat.
   instance_name
   É o nome a ser atribuído à instância.
2. Execute o comando a seguir para iniciar o agente:
   Linux `install_dir/bin/tomcat-agent.sh start instance_name`
   Windows `install_dir\bin\tomcat-agent.bat start instance_name`

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Configurando o agente nos sistemas Windows

É possível configurar o agente em sistemas operacionais Windows usando a janela **IBM Performance Management**.

Antes de Iniciar

Certifique-se de que os seguintes pré-requisitos sejam atendidos:

- O Java está instalado no Tomcat Server onde o agente está instalado.
- A versão do JDK 1.6 ou posterior é configurada no prompt do qual o instalador de agente é instalado.
- JMX Remoto está ativado para o Servidor Tomcat. Para obter detalhes, consulte Ativando o JMX Remoto.
- O Servidor Tomcat está funcionando.

Sobre Esta Tarefa

É possível configurar o agente a partir do prompt de comandos. Para obter detalhes, siga as etapas fornecidas no tópico "Configurando o Agente Tomcat em sistemas Linux" na página 806 e execute os comandos com a extensão .bat em vez da extensão .sh. O procedimento a seguir explica como configurar o agente usando o painel de configuração do agente.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito em **Monitoring Agent for Tomcat**.
3. Clique em **Configurar Agente**.

   Atenção: Se **Configurar agente** estiver indisponível, clique em **Reconfigurar**.
4. Na janela **Nome da instância**, especifique um nome exclusivo para a instância do Agente Tomcat e clique em **OK**.

   Restrição: O MSN não deve exceder 32 caracteres.
5. No campo **NOME DO SERVIDOR**, insira um nome exclusivo para identificar o Tomcat Server que está sendo monitorado.
6. Na janela **Configurações de parâmetro Java**, conclua uma das seguintes etapas:
   - Clique em **Avançar** para aceitar o local padrão onde o Java está instalado. O caminho da instalação padrão é `C:\IBM\APM\java\java80_x64\jre`.
   - No campo **Início do Java**, especifique o caminho quando o IBM Java é instalado em um caminho diferente.
7. Na janela **Servidor compatível com JSR-160**, especifique os detalhes dos seguintes parâmetros:
   a) No campo **ID do usuário do JMX**, especifique o ID do usuário que é usado para conectar-se ao servidor MBean Tomcat quando a autorização JMX estiver ativada no Tomcat.
   b) No campo **Senha JMX**, especifique a senha do usuário JMX quando a autorização JMX estiver ativada no Tomcat.
   c) No campo **URL de serviço JMX**, insira a URL que é usada para conectar-se ao servidor MBean Tomcat.

      O formato da URL é `service:jmx:rmi:///jndi/rmi://`*`host_name`*`:`*`port_number`*`/jmxrmi`. A URL padrão é válida quando o servidor é executado no host local e usa a porta 8686 como uma porta do JMX. É possível modificar o nome do host e o número da porta na URL, mantendo o mesmo formato.
   d) Na lista **Configuração do coletor de dados**, selecione Sim se desejar ativar a coleta de dados de rastreamento de transação e de detalhamento.
8. Na janela **Monitoring Agent for Tomcat**, clique com o botão direito na instância do Agente Tomcat e clique em **Iniciar**.
9. Ative a coleta de dados do Rastreamento de transação e Detalhamento e reinicie o Tomcat Server.

O que Fazer Depois

Se o Agente Tomcat estiver em execução como um serviço, após a configuração do agente no Windows, configure o Tomcat Data Collector. Para obter mais informações, consulte “Configurando o Tomcat Data Collector ” na página 805.

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte “Iniciando o Console do Cloud APM” na página 975.

Fornecendo política de segurança local para executar o Monitoring Agent for Tomcat no Windows por um usuário não administrador

As políticas de segurança local estão disponíveis para executar um Monitoring Agent for Tomcat no Windows por um usuário não administrador.

Sobre Esta Tarefa

Uma combinação das duas seguintes políticas de segurança local funciona para executar o Agente Tomcat no Windows por um usuário não administrador. Para um Agente Tomcat iniciar/parar, configurar e executar a Verificação de dados, essas duas políticas funcionam.

1. Programas de depuração.
2. Efetuar logon como serviço.

Siga o procedimento que é fornecido para avaliar as permissões de Segurança local para um usuário não administrador.

Procedimento

1. Acesse TEMA e mude a inicialização do agente Tomcat com um usuário não administrador.
2. Inclua um usuário não administrador na Pasta de instalação do Agente Tomcat e conceda permissões completas a ele.
3. Inclua um usuário não administrador na chave de registro HKEY_LOCAL_MACHINE e clique em **Permissões completas**.
4. Execute o comando **`secpol.msc`** em **startmenu** para abrir as políticas de segurança local
5. Em seguida, para incluir um usuário não administrador nas políticas, consulte “Permissões de Política de segurança local” na página 804
6. Reinicie o Agente Tomcat.
7. Verifique os status de Agentes Tomcat e verifique os dados no portal do APM.

Permissões de Política de segurança local

Concedendo a permissão Depurar programas

Sobre Esta Tarefa

Para conceder a permissão Depurar programas, siga o procedimento em Agente Tomcat, conforme descrito aqui:

Procedimento

1. Clique em **Iniciar > Ferramentas Administrativas > Política de Segurança Local**. A janela **Configurações de segurança local** é aberta
2. Expanda **Políticas Locais** e clique em **Designação de Direitos de Usuário**. A lista de direitos de usuário é aberta.
3. Dê um clique duplo na política **Programas de depuração**. A janela **Propriedades dos programas de depuração** é aberta.
4. Clique em **Incluir Usuário ou Grupo**. A janela **Selecionar Usuários ou Grupos** é exibida.

5. No campo Inserir os nomes de objetos a serem selecionados, insira o nome da conta do usuário para quem você deseja designar permissões e, em seguida, clique em **OK**.
6. Clique em **OK**.

Concedendo a permissão Efetuar logon como serviço

Sobre Esta Tarefa
Para conceder a permissão Efetuar logon como serviço, siga o procedimento em Agente Tomcat, conforme descrito aqui.

Procedimento

1. Clique em **Iniciar > Ferramentas Administrativas > Política de Segurança Local**. A janela **Configurações de segurança local** é aberta
2. Expanda **Políticas Locais** e clique em **Designação de Direitos de Usuário**. A lista de direitos de usuário é aberta.
3. Dê um clique duplo na política **Efetuar logon como serviço**. A janela **Efetuar logon como propriedades de serviço** é aberta.
4. Clique em **Incluir Usuário ou Grupo**. A janela **Selecionar Usuários ou Grupos** é exibida.
5. No campo Inserir os nomes de objetos a serem selecionados, insira o nome da conta do usuário para quem você deseja designar permissões e, em seguida, clique em **OK**.
6. Clique em **OK**.

Configurando o Tomcat Data Collector
Se o Agente Tomcat estiver em execução como um serviço, após configurar o agente no Windows, configure o Tomcat Data Collector com as instruções fornecidas aqui.

Sobre Esta Tarefa

Após configurar e iniciar a instância do Agente Tomcat, ela gera ou atualiza um arquivo `setenv.bat` no `/CANDLEHOME/setenv_<instance_name>.bat`. Esse arquivo contém parâmetros de configuração do coletor de dados necessários para configurar o Tomcat Data Collector.

Procedimento

1. Abra a janela **Propriedades do Apache Tomcat** e clique em **Java**
2. Abra `setenv_<instanceName>.bat` no local `/CANDLEHOME/setenv_<instance_name>.bat`
3. Copie o valor do parâmetro **JAVA_OPTS** do `setenv_<instance_name>.bat` mostrado no bloco:

```
agentlib:am_ibm_16=C:\IBM\APM\otdchome\7.3.0.13.0\runtime\TOMTKWIN1
-Xbootclasspath/p:C:\IBM\APM\otdchome\7.3.0.13.0\toolkit\lib\bcm-bootstrap.jar
-Djava.security.policy=C:\IBM\APM\otdchome\7.3.0.13.0\itcamdc\etc\datacollector.policy
-Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=
C:\IBM\APM\otdchome\7.3.0.13.0\runtime\TOMTKWIN1\TOM_TK_1_DCManual.txt
-Dcom.ibm.tivoli.itcam.serverHome=C:\TOMCAT_9\apache-tomcat-9.0.5\apache-tomcat-9.0.5
-Dam.home=C:\IBM\APM\otdchome\7.3.0.13.0\itcamdc
-Dcom.ibm.tivoli.itcam.toolkit.runtime.dir=C:\IBM\APM\otdchome\7.3.0.13.0\runtime
```

4. Cole esse valor na caixa de texto rotulada **Opções Java** na guia **Java** de **Propriedades do Apache Tomcat**
5. Clique em **Aplicar**
6. Acesse **Painel de Controle**, clique em **Sistema** > **Avançado** > **Variáveis de Ambiente**
7. Em **Variáveis do Sistema**, edite a variável *PATH* anexando o caminho de arquivo <OTDC_home> `\toolkit\lib\win64;<OTDC_HOME>/ toolkit\lib\win64\ttapi` e clique em **OK**

   Nota: Substitua <OTDC_home> pelo caminho real do diretório de instalação do kit de ferramentas. Por exemplo, `C:\IBM\APM\otdchome\7.3.0.13.0\toolkit\lib\win64;C:\IBM\APM \otdchome\7.3.0.13.0\toolkit\lib\win64\ttapi`
8. Clique em **NEW** para incluir uma variável *RUNTIME_DIR*.

9. Inclua **Nome da Variável** como *RUNTIME_DIR* e **Caminho da Variável** como `C:\IBM\APM\otdchome\7.3.0.13.0\runtime`. Esse caminho está disponível em `setenv_<instancename>.bat`
10. Reinicie o Windows. Certifique-se de que a inicialização do serviço Tomcat esteja configurada para Automático

Configurando o Agente Tomcat em sistemas Linux

Execute o script de configuração e responda aos prompts para configurar o Agente Tomcat em sistemas Linux.

Antes de Iniciar

- JMX Remoto está ativado para o Servidor Tomcat. Para obter detalhes, consulte Ativando o JMX Remoto.
- O Servidor Tomcat está funcionando.

Procedimento

1. Execute o seguinte comando:
   install_dir`/bin/tomcat-agent.sh config` *instance_name*
   Em que *instance_name* é o nome que você deseja fornecer para a instância.
2. Quando for solicitado que especifique um valor para SERVER, especifique um nome exclusivo para identificar o Tomcat Server que está sendo monitorado, e pressione Enter.
3. Quando for solicitado a especificar um valor para `Início Java`, pressione Enter para aceitar o local padrão onde a Java virtual machine está instalada. O local padrão é `/opt/ibm/apm/agent/JRE/lx8266/jre`. Se o agente não estiver instalado no diretório padrão, especifique *install_dir*`/JRE/lx8266/jre`.
4. Quando for solicitado a especificar um valor para `ID do usuário JMX`, especifique o ID do usuário que se conecta ao servidor MBean Tomcat. Se a autorização JMX não estiver ativada, pressione Enter.
5. Quando for solicitado a especificar um valor para Senha `JMX`, especifique a senha do usuário JMX e confirme-a. Se a autorização JMX não estiver ativada, pressione Enter.
6. Quando for solicitado a especificar um valor para `URL de serviço JMX`, pressione Enter para aceitar a URL padrão ou especifique outra URL de serviço para conectar-se ao servidor MBean Tomcat. O formato da URL é `service:jmx:rmi:///jndi/rmi://`*host_name*`:`*port_number*`/jmxrmi`. A URL padrão é válida quando o servidor é executado no host local e usa a porta 8686 como uma porta do JMX. É possível modificar o nome do host e a porta na URL, mantendo o mesmo formato.
7. Quando for solicitado que especifique um valor para `Data Collector Configuration`, especifique 1 e pressione Enter para ativar a coleta de dados de rastreamento de transação e de detalhamento.
8. Execute o comando a seguir para iniciar o agente:
   install_dir`/bin/tomcat-agent.sh start` *instance_name*
9. Ative a coleta de dados Rastreamento de transação e Detalhamento, reinicie o Tomcat Server.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte “Iniciando o Console do Cloud APM” na página 975.

Configurando o Agente Tomcat usando o arquivo silencioso de resposta

É possível usar o arquivo silencioso de resposta para configurar o Agente Tomcat sem responder aos prompts.

Procedimento

1. Em um editor de texto, abra o arquivo `tomcat_silent_config.txt` que está disponível no seguinte caminho:
   install_dir`/samples`
2. Para o parâmetro **KOT_SERVER**, especifique um nome exclusivo para identificar o Tomcat Server que está sendo monitorado.
3. Para o parâmetro **Java home**, especifique o caminho em que a Java virtual machine está instalada. O local padrão é `/opt/ibm/apm/agent/JRE/lx8266/jre`. Se o agente não estiver instalado no diretório padrão, especifique *install_dir*`/JRE/lx8266/jre`.
4. Para o parâmetro **JMX user ID**, especifique o ID do usuário que é usado para conectar-se ao servidor MBean Tomcat. Você deve especificar um valor para esse parâmetro quando a autorização JMX estiver ativada no Tomcat.
5. Para o parâmetro **JMX password** , especifique a senha do usuário JMX. Você deve especificar um valor para esse parâmetro quando a autorização JMX estiver ativada no Tomcat.
6. Para o parâmetro **JMX service URL**, especifique a URL de serviço para conectar-se ao servidor MBean Tomcat. O formato da URL é `service:jmx:rmi:///jndi/rmi://`*host_name*`:`*port_number*`/jmxrmi`. A URL padrão é válida quando o servidor é executado no host local e usa a porta 8686 como uma porta do JMX. É possível modificar o nome do host e o número da porta na URL, mantendo o mesmo formato.
7. Para o parâmetro **KOT_DCCONFIGURATION**, especifique `Yes` se desejar ativar a coleta de dados de rastreamento de transação e de detalhamento.
8. Salve e feche o arquivo `tomcat_silent_config.txt` e execute o seguinte comando para atualizar as definições de configuração do agente:
   Linux *install_dir*`/bin/tomcat-agent.sh config` *instance_name install_dir*`/samples/tomcat_silent_config.txt`
   Windows *install_dir*`/bin/tomcat-agent.bat config` *instance_name install_dir*`/samples/tomcat_silent_config.txt`
   Em que *instance_name* é o nome que você deseja dar para a instância, e *install_dir* é o diretório de instalação do Agente Tomcat.
9. Execute o comando a seguir para iniciar o agente:
   Linux *install_dir*`/bin/tomcat-agent.sh start` *instance_name*
   Windows *install_dir*`/bin/tomcat-agent.bat start` *instance_name*
10. Se ativar a coleta de dados de detalhamento e de rastreamento de transação, reinicie o Tomcat Server.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre como usar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

Ativando a coleta de dados de rastreamento de transações e diagnósticos

Na página **Configuração do agente**, é possível ativar ou desativar a coleta de dados de rastreamento de transações e diagnósticos.

Sobre Esta Tarefa

Ao ativar a coleta de dados de rastreamento de transações, o agente coleta dados dos seguintes componentes:

- Servlet JSP
- Aplicativos EJB
- JMS

Procedimento

Conclua as seguintes etapas para configurar a coleta de dados para cada sistema gerenciado.

1. Efetue login no Console do Cloud APM.
2. A partir da barra de navegação, clique em **Configuração do Sistema** > **Configuração do Agente**.
   A página **Configuração do Agente** é exibida.
3. Clique no **Tomcat** guia.
4. Selecione as caixas de seleção dos sistemas gerenciados para os quais você deseja configurar a coleta de dados e conclua qualquer uma das seguintes ações da lista **Ações**.
   - Para ativar o rastreamento de transações, clique em **Configurar rastreamento de transações** > **Ativado**. O status na coluna **Rastreamento da Transação** é atualizado para Ativado para cada sistema gerenciado selecionado.
   - Para ativar a coleta de dados diagnósticos, selecione **Configurar modo de diagnóstico** > **Somente modo de diagnóstico ativado**. O status na coluna Modo de diagnóstico é atualizado para Ativado para cada sistema gerenciado selecionado.
   - Para ativar a coleta de dados diagnósticos e o rastreio de método, selecione **Configurar modo de diagnóstico** > **Modo de diagnóstico e Rastreio de método ativados**. O status nas colunas Modo de diagnóstico e Rastreio de método é atualizado para Ativado para cada sistema gerenciado selecionado.
   - Para desativar o rastreamento de transação, clique em **Configurar Rastreamento de Transação** > **Desativado**. O status na coluna **Rastreamento de Transação** é atualizado para Desativado para cada sistema gerenciado selecionado.
   - Para desativar a coleta de dados diagnósticos, clique em **Configurar modo de diagnóstico** > **Modo de diagnóstico e Rastreio de método desativados**. O status nas colunas **Modo de diagnóstico e Rastreio de método** é atualizado para Desativado para cada sistema gerenciado selecionado.

O que Fazer Depois

Efetue login no Console do Cloud APM para visualizar os dados de rastreamento de transação e diagnósticos que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte “Iniciando o Console do Cloud APM” na página 975.

Atualizar ou mudar o servidor de aplicativos Tomcat

Para atualizar ou mudar o servidor de aplicativo Tomcat após a configuração do Agente Tomcat, siga as etapas fornecidas neste tópico. Essas etapas são comuns para ambos, o Tomcat configurado por meio do Windows e o Tomcat configurado por meio do Linux.

Procedimento

1. Pare a instância do Agente Tomcat e o Tomcat Server
2. Acesse <TOMCAT_SERVER>/bin e abra o arquivo setenv.sh no editor
3. Remova todos os parâmetros de inicialização para o Data Collector de setenv.sh. Remova as linhas a seguir do arquivo

```
export LD_LIBRARY_PATH="<CANDLE_HOME>/otdchome/7.3.0.13.0/toolkit/lib/lx8266"
export RUNTIME_DIR="<CANDLE_HOME>/otdchome/7.3.0.13.0/runtime"
export JAVA_OPTS="-agentlib:am_ibm_16=<CANDLE_HOME>/otdchome/7.3.0.13.0/runtime/
<Tomcat_Application_
Server> -
Xbootclasspath/p:<CANDLE_HOME>/otdchome/7.3.0.13.0/toolkit/lib/bcm-bootstrap.jar -
Djava.security.policy=<CANDLE_HOME>/otdchome/7.3.0.13.0/itcamdc/etc/datacollector.policy -
Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=<CANDLE_HOME>/otdchome/7.3.0.13.0/runtime/
<Tomcat_
Application_Server>/<Agent_Instance>_DCManual.txt -
Dcom.ibm.tivoli.itcam.serverHome=<TOMCAT_HOME> -
Dam.home=<CANDLE_HOME>/otdchome/7.3.0.13.0/itcamdc -
Dcom.ibm.tivoli.itcam.toolkit.runtime.dir=<CANDLE_HOME>/otdchome/7.3.0.13.0/runtime"
```

4. Salve as mudanças e inicie o Tomcat Server

5. Reconfigure o Agente Tomcat para atualizar ou mudar o Tomcat Application Server
6. Atualize ou mude somente o Tomcat Application Server e não mude nenhuma definição de configuração
7. Inicie a instância do Agente Tomcat
8. O arquivo de verificação `setenv.sh` é atualizado com o novo Tomcat Application Server em parâmetros de inicialização para o Data Collector
9. Reinicie o Tomcat Server
10. Verifique se as mudanças feitas no Tomcat Application Server são refletidas na Máquina do Agente e no no painel do IBM Cloud Application Performance Management
    - Verifique a mudança do Tomcat Application Server no local `<CANDLE_HOME>/otdchome/7.3.0.13.0/runtime/<Tomcat_Application_Server>` na máquina do agente
    - Verifique a mudança do Tomcat Application Server na página **Aggregate Transaction Topology** e o atributo *appserver* no grupo de atributos *KOT_Server* no painel IBM Cloud Application Performance Management dashboard

Configurando o monitoramento do VMware VI

Depois de instalar o Monitoring Agent for VMware VI, é preciso criar a primeira instância, e iniciar manualmente o agente para que ele possa coletar dados do VMware Virtual Infrastructure que está sendo monitorado.

Antes de Iniciar

- Revise os pré-requisitos de hardware e software.
- Crie um ID do usuário no VMware Virtual Infrastructure. O agente usa esse ID do usuário para conectar-se ao VMware vCenter para monitorar o VMware Virtual Infrastructure. Certifique-se de que tenha os privilégios "System.View" e "System.Read" em todos os servidores vCenters e ESX que estão sendo monitorados. Para obter informações sobre como criar o ID do usuário, consulte a documentação do VMware para gerenciar usuários, grupos, permissões e funções.
- Determine se o vCenter está configurado para comunicação de SSL. Se estiver configurado, você deve configurar o Agente VMware VI para usar SSL para se comunicar com o vCenter.
  - Para determinar se o vCenter usa SSL para comunicação, use a URL `https://vCenterIPaddress` para acessar o vCenter. Se for possível acessar o vCenter, isso indica que o vCenter usa SSL para se comunicar pela rede.
  - Para configurar o Agente VMware VI para usar SSL para se comunicar com o vCenter, conclua as etapas descritas em “Ativando a comunicação de SSL com origens de dados VMware VI” na página 811.
- Decida o número de instâncias do agente de que você precisa para monitorar o VMware Virtual Infrastructure. Para obter informações sobre como dimensionar as instâncias do agente de acordo com seu ambiente de monitoramento, consulte “Dimensionando e planejando a implementação do Agente VMware VI” na página 810.

Sobre Esta Tarefa

O Agente VMware VI é um agente de múltiplas instâncias. Diferente de um agente de instância única, para o qual é possível configurar o agente para monitorar e coletar dados somente para um aplicativo monitorado, o Agente VMware VI pode ter várias instâncias configuradas que se conectam a vários servidores vCenter e monitoram remotamente o VMware Virtual Infrastructure.

Os parâmetros de configuração definem as origens de dados do VMware VI que são monitoradas e definem uma conexão com o VMware vCenter, o vCenter Server Appliance ou um servidor ESX VMware individual. Para saber as versões suportadas desses aplicativos, consulte o Software Product Compatibility Reports para o Agente VMware VI.

Muitas vezes, a versão do produto e a versão do agente diferem. As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte o “Histórico de Mudanças” na página 50.

Você deve configurar manualmente o agente para visualizar dados para todos os atributos do agente.

- Para configurar o agente em sistemas operacionais Windows, é possível usar a janela **IBM Performance Management** ou o arquivo de resposta silencioso.
- Para configurar o agente em sistemas operacionais Linux, é possível executar o script e responder aos prompts, ou usar o arquivo silencioso de resposta.

Dimensionando e planejando a implementação do Agente VMware VI

O número de instâncias do agente que podem ser configuradas em um único sistema depende da disponibilidade e utilização de recursos no sistema.

A tabela a seguir categoriza o ambiente do VMware em vários tamanhos com o tamanho de heap Java necessário:

Tabela 218. Ambiente do VMware e tamanho do heap Java

Tamanho do ambiente VMware	Número de servidores ESX	Tamanho de Heap Java
Ambiente pequeno	Um servidor vCenter que gerencia até 125 servidores ESX(i) e 300 - 1500 guests.	**-Xmx2048m** (2 GB)
Ambiente médio	Um servidor vCenter que gerencia entre 125 - 250 servidores ESX(i) e 1500 - 4000 guests.	**-Xmx4096m** (4 GB)
Ambiente grande	Um servidor vCenter que gerencia entre 250 - 500 servidores ESX(i) e 4000 - 7500 guests.	**-Xmx8192m** (8 GB)
Ambientes muito grandes	Um servidor vCenter que gerencia mais de 500 servidores ESX(i) e mais de 7500 guests.	**-Xmx16384m** (16 GB)

Para aumentar o tamanho de heap para o provedor de dados Java, conclua as etapas descritas em “Aumentando o tamanho de heap Java” na página 816.

Para que as instâncias do agente monitorem o ambiente com sucesso, o servidor no qual você instala o agente deve ter recursos de memória adequados para acomodar os dados que são coletados por essas instâncias do agente. Uma única instância do Agente VMware VI requer aproximadamente 300 - 400 MB para monitorar um ambiente pequeno. Consulte as seguintes diretrizes sobre o número de instâncias do agente a serem configuradas:

- Use uma única instância para monitorar um único vCenter. Não use a mesma instância para monitorar vários vCenters.
- Em um ambiente não em cluster, use uma única instância para monitorar um máximo de 8 servidores ESX pequenos (100 - 200 máquinas virtuais em um servidor ESX). Não configure vários servidores ESX individuais na única instância do agente.
- Use várias instâncias do agente do Agente VMware VI para monitorar um ambiente que contém vários vCenters. Antes de configurar várias instâncias, certifique-se de que tenha recursos de memória adequados no sistema em que o agente é instalado.

Ativando a comunicação de SSL com origens de dados VMware VI

Antes de configurar o agente para se comunicar de forma segura com as origens de dados do VMware VI usando SSL, você deve incluir um certificado SSL da origem de dados no armazenamento confiável do certificado do agente.

Sobre Esta Tarefa

Importante: As informações a seguir aplicam-se somente se o agente estiver configurado para validar certificados SSL.

Se a validação de certificados SSL estiver desativada, o Agente VMware VI se conectará às origens de dados do VMware mesmo se seus certificados SSL estiverem expirados, não forem confiáveis ou forem inválidos. No entanto, é preciso ter cuidado ao desligar a validação de certificados SSL, pois isso não é seguro.

Se uma origem de dados VMware utiliza um certificado SSL que é assinado por uma Autoridade de Certificação comum (por exemplo, Verisign, Entrust ou Thawte), não é necessário incluir certificados no armazenamento confiável de certificados do Agente VMware VI. No entanto, se a origem de dados usar um certificado que não está assinado por uma Autoridade de Certificação comum, como é o caso por padrão, você deverá incluir o certificado no armazenamento confiável para permitir que o agente se conecte e colete dados com sucesso.

Nota:

1. O arquivo de certificado padrão do VMware é denominado `rui.crt`.
2. Para um Virtual Center, por padrão o arquivo de certificado SSL localiza-se no seguinte caminho:

   ```
   C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL
   ```
3. Para um servidor ESX, por padrão o arquivo de certificado SSL localiza-se no diretório `/etc/vmware/ssl`.

Procedimento

1. Copie o arquivo de certificado da origem de dados para o computador do agente.
2. No computador agente, substitua o arquivo de certificado em um diretório de sua escolha. Não sobrescreva os arquivos de certificado. Use um nome de arquivo exclusivo e um rótulo para cada certificado incluído.
3. Use o comando *keytool* para incluir o certificado de origem de dados no armazenamento confiável de certificados do agente:

   ```
   keytool -import -noprompt -trustcacerts -alias CertificateAlias -file
   CertificateFile -keystore Truststore -storepass TruststorePassword
   ```

   Em que

   CertificateAlias

   Referência exclusiva para cada certificado incluído no armazenamento confiável de certificados do agente, por exemplo, um alias apropriado para o certificado de *datasource.example.com* é *datasource*.

   CertificateFile

   O nome completo do caminho e do arquivo para o certificado de origem de dados do VMware a ser incluído no armazenamento confiável.

   Armazenamento Confiável

   O nome completo do caminho e arquivo para o banco de dados de certificados do Agente VMware VI. Use o seguinte nome de caminho e arquivo:

   - Windows (64 bit): *install_dir*\tmaitm6_x64\kvm.truststore

- Linux (64 bit): *install_dir*/lx8266/vm/etc/kvm.truststore

TruststorePassword

ITMVMWAREVI é a senha padrão para o armazenamento confiável do Agente VMware VI. Para alterar essa senha, consulte a documentação do Java Runtime para obter informações sobre as ferramentas a serem usadas.

Importante: Para usar o comando *keytool*, o diretório bin do Java Runtime deve estar em seu caminho. Use os seguintes comandos:

- Windows (64 bit): `set PATH=%PATH%;install_dir\java\java70_x64\jre\bin`
- Linux (64 bits): `PATH="$PATH":/opt/ibm/apm/agent/JRE/lx8266/bin`

4. Após incluir todos os certificados de origem de dados, inicie o agente de monitoramento.

O que Fazer Depois
Conclua a configuração do agente.

Configurando o agente nos sistemas Windows

É possível configurar o agente em sistemas operacionais Windows usando a janela **IBM Performance Management**. Após fazer a atualização dos valores de configuração, deve-se iniciar o agente para salvar os valores atualizados.

Sobre Esta Tarefa

O Agente VMware VI fornece valores padrão para alguns parâmetros. É possível especificar diferentes valores para esses parâmetros.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito em **Monitoring Agent for VMware VI** e, em seguida, clique em **Configurar agente**.

   Lembre-se: Após você configurar o agente pela primeira vez, a opção **Configurar Agente** é desativada. Para configurar o agente novamente, clique em **Reconfigurar**.
3. Na janela Monitoring Agent for VMware VI, conclua as seguintes etapas:
   a) Insira um nome exclusivo para a instância do Agente VMware VI e clique em **OK**.
   b) Na guia **Provedor de Dados**, especifique valores para os parâmetros de configuração e clique em **Avançar**.
   c) Na guia **Origem de Dados**, especifique valores para os parâmetros de configuração e clique em **Avançar**.

      O Agente VMware VI é um agente de origem multidados. É possível monitorar várias origens de dados a partir do mesmo agente.

      - Se desejar configurar uma nova origem de dados, clique em **Novo**.
      - Se desejar excluir uma origem de dados existente, clique em **Excluir**.

      Para obter informações sobre os parâmetros de configuração em cada guia da janela Monitoring Agent for VMware VI, consulte os seguintes tópicos:

      - Parâmetros de configuração para o provedor de dados
      - Parâmetros de configuração para origem de dados
4. Na janela **IBM Performance Management**, clique com o botão direito na instância configurada e, em seguida, clique em **Iniciar**.

O que Fazer Depois

- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

  Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.
- Se estiver monitorando um ambiente grande do VMware com mais de 500 hosts ESX, pode ser necessário aumentar o tamanho de heap para o provedor de dados Java. Para obter mais informações, consulte "Aumentando o tamanho de heap Java" na página 816.

Configurando o agente usando o arquivo de resposta silencioso

O arquivo de resposta silencioso contém os parâmetros de configuração do agente. É possível editar o arquivo de resposta silencioso para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

O arquivo silencioso de resposta contém os parâmetros de configuração do agente com valores padrão que são definidos para alguns parâmetros. É possível editar o arquivo silencioso de resposta para especificar os valores diferentes para os parâmetros de configuração.

Após você atualizar os valores de configuração no arquivo de resposta silencioso, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

- Para configurar o Agente VMware VI no modo silencioso, conclua as seguintes etapas:
  a) Em um editor de texto, abra o arquivo `vmware_vi_silent_config.txt` que está disponível no caminho a seguir:
     – Linux *install_dir*`/samples/vmware_vi_silent_config.txt`

       Exemplo `/opt/ibm/apm/agent/samples/vmware_vi_silent_config.txt`
     – Windows *install_dir*`\samples\vmware_vi_silent_config.txt`

       Exemplo `C:\IBM\APM\samples\vmware_vi_silent_config.txt`
  b) No arquivo `vmware_vi_silent_config.txt`, especifique valores para todos os parâmetros obrigatórios. Também é possível modificar os valores padrão de outros parâmetros.

     Para obter informações sobre os parâmetros de configuração, consulte os tópicos a seguir:
     – "Parâmetros de configuração para o provedor de dados" na página 816
     – "Parâmetros de configuração para a origem de dados" na página 815
  c) Salve e feche o arquivo `vmware_vi_silent_config.txt` e execute o comando a seguir:
     – Linux *install_dir*`/bin/vmware_vi-agent.sh config` *instance_name* *install_dir*`/samples/vmware_vi_silent_config.txt`

       Exemplo **`/opt/ibm/apm/agent/bin/vmware_vi-agent.sh config instance_name /opt/ibm/apm/agent/samples/vmware_vi_silent_config.txt`**
     – Windows *install_dir*`\bin\vmware_vi-agent.bat config` *instance_name* *install_dir*`\samples\vmware_vi_silent_config.txt`

       Exemplo **`C:\IBM\APM\bin\ vmware_vi-agent.bat config instance_name C:\IBM\APM\samples\vmware_vi_silent_config.txt`**

       Where

instance_name
O nome que você deseja fornecer para a instância.

install_dir
Caminho onde o agente está instalado.

Importante: Assegure que você inclua o caminho absoluto no arquivo de resposta silencioso. Caso contrário, os dados do agente não serão mostrados nos painéis.

d) Execute o comando a seguir para iniciar o agente:

– Linux *install_dir*/bin/vmware_vi-agent.sh start *instance_name*

Exemplo **/opt/ibm/apm/agent/bin/vmware_vi-agent.sh start instance_name**

– Windows *install_dir*\bin\vmware_vi-agent.bat start *instance_name*

Exemplo **C:\IBM\APM\bin\vmware_vi-agent.bat start instance_name**

O que Fazer Depois

- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

  Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.
- Se você estiver monitorando um ambiente VMware grande com mais de 500 hosts ESX, talvez seja necessário aumentar o tamanho de heap para o provedor de dados Java™. Para obter mais informações, consulte "Aumentando o tamanho de heap Java" na página 816.

Configurando o agente respondendo aos prompts

Para configurar o agente em sistemas operacionais Linux, deve-se executar o script e responder aos prompts.

Procedimento

- Para configurar o agente executando o script e respondendo aos prompts, conclua as seguintes etapas:

  a) Na linha de comandos, execute o seguinte comando:

  install_dir/bin/vmware_vi-agent.sh config *instance_name*

  Exemplo **/opt/ibm/apm/agent/bin/vmware_vi-agent.sh config instance_name**

  Em que

  instance_name
  O nome que você deseja fornecer para a instância.

  install_dir
  Caminho onde o agente está instalado.

  b) Responda aos prompts consultando os seguintes tópicos:

  – "Parâmetros de configuração para o provedor de dados" na página 816
  – "Parâmetros de configuração para a origem de dados" na página 815

  c) Execute o comando a seguir para iniciar o agente:

  install_dir/bin/vmware_vi-agent.sh start *instance_name*

  Exemplo **/opt/ibm/apm/agent/bin/vmware_vi-agent.sh start instance_name**

O que Fazer Depois

- Efetue login no Console do Cloud APM para visualizar os dados que são coletados pelo agente nos painéis. Para obter informações sobre o uso do Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975.

  Para obter ajuda com a resolução de problemas, consulte o IBM Cloud APM Fórum do nodeveloperWorks.
- Se você estiver monitorando um ambiente VMware grande com mais de 500 hosts ESX, talvez seja necessário aumentar o tamanho de heap para o provedor de dados Java™. Para obter mais informações, consulte "Aumentando o tamanho de heap Java" na página 816.

Parâmetros de configuração para a origem de dados

Quando você configura o Agente VMware VI, é possível mudar os valores padrão dos parâmetros para a origem de dados, como o endereço, o ID do usuário e a senha da origem de dados.

A tabela a seguir contém descrições detalhadas dos parâmetros de configuração para a origem de dados.

Tabela 219. Nomes e descrições dos parâmetros de configuração para a origem de dados

Nome de parâmetro	Descrição	Campo obrigatório
ID da Origem de Dados	O ID da origem de dados.	Sim
Endereço da Origem de Dados	Endereço da origem de dados. Se não quiser que o agente valide os certificados SSL, configure o valor para o nome do host ou endereço IP do VMware Virtual Center ou servidor ESX sendo monitorado. Se desejar que o agente valide certificados SSL durante o uso de SSL para se comunicar por meio da rede, configure o agente usando o Subject Alternative Name fornecido no certificado. Para visualizar o Subject Alternative Name do datacenter, conclua as etapas a seguir: 1. Abra o certificado. 2. Na janela **Certificado**, clique na guia **Detalhes**. 3. Selecione **Nome alternativo do assunto** e use o valor do Nome DNS. Por exemplo, se o valor de Nome DNS for "`ibmesx3v3vc.ITMfVS.com`", use o valor "`ibmesx3v3vc.ITMfVS.com`" para o nome do host.	Sim
Usar Conexão SSL para Origem de Dados	Indica se o agente usa uma conexão SSL para conectar-se às origens de dados do VMware Virtual Infrastructure. Especifique `Yes` se o agente usar uma conexão SSL para conectar-se às origens de dados. Caso contrário, especifique `Não`. O valor padrão é `Sim`.	Sim
ID do Usuário da Origem de Dados	O ID do usuário tem privilégios suficientes para coletar dados de monitoramento e é conhecido para a origem de dados.	Sim
Senha de Origem de Dados	A senha do ID do usuário configurada para acessar a origem de dados.	Sim
Confirmar Senha da Origem de Dados	A mesma senha que a especificada no campo **Senha da Origem de Dados**.	

Parâmetros de configuração para o provedor de dados

Quando você configura o Agente VMware VI, pode mudar os valores padrão dos parâmetros para o provedor de dados, como o número máximo de arquivos de log do provedor de dados, o tamanho máximo do arquivo de log e o nível de detalhes incluídos no arquivo de log.

A tabela a seguir contém descrições detalhadas dos parâmetros de configuração para o provedor de dados.

Tabela 220. Nomes e descrições dos parâmetros de configuração para o provedor de dados

Nome de parâmetro	Descrição	Campo obrigatório
Nome da instância	O nome da instância. **Restrição:** O campo **Nome da Instância** exibe o nome da instância que você especifica ao configurar o agente pela primeira vez. Ao configurar o agente novamente, não é possível mudar o nome da instância do agente.	Sim
Certificados SSL válidos	Indica se o agente valida certificados SSL ao usar SSL para se comunicar pela rede. Configure o valor para `Sim` se desejar que o agente valide certificados SSL ao usar SSL para se comunicar pela rede. Configure o valor para `Não` para evitar que o agente valide certificados SSL. O valor padrão é `Yes`. Para obter informações sobre como incluir um certificado SSL de origem de dados no armazenamento confiável do certificado do agente, consulte "Ativando a comunicação de SSL com origens de dados VMware VI" na página 811.	Sim
Número Máximo de Arquivos de Log do Provedor de Dados	O número máximo de arquivos de log que o provedor de dados cria antes de sobrescrever os arquivos de log anteriores. O valor padrão é 10.	Sim
Tamanho Máximo em KB de Cada Log do Provedor de Dados	O tamanho máximo em KB que um provedor de dados deve atingir antes de o provedor de dados criar um novo arquivo de log. O valor padrão são 5190 KB.	Sim
Nível de Detalhe no Log do Provedor de Dados	O nível de detalhes que pode ser incluído no arquivo de log criado pelo provedor de dados. O valor padrão é INFO. Os valores a seguir são válidos: OFF, SEVERE, WARNING, INFO, FINE, FINER, FINEST e ALL.	Sim
KEY_STORE_PASSWORD	O **KEY_STORE_PASSWORD** permite que o usuário configure o agente com a nova senha de armazenamento de chaves configurada para o agente JRE. Observe que esse armazenamento de chaves Java não possui relação com o armazenamento de chaves do vCenter. Não é obrigatório inserir a senha em cada configuração. Se esse campo for deixado em branco, o agente assumirá que a senha do armazenamento de chaves Java padrão deverá ser usada durante a utilização do agente JRE.	Não

Aumentando o tamanho de heap Java

Depois de configurar o Agente VMware VI, se estiver monitorando um grande ambiente VMware Virtual Infrastructure, pode ser necessário aumentar o tamanho de heap para o provedor de dados Java™.

Sobre Esta Tarefa

O tamanho máximo de heap padrão para o provedor de dados Java é de 256 megabytes. Você deve configurar o tamanho máximo de heap para um valor apropriado que depende do tamanho do ambiente do VMware. Para obter informações sobre os tamanhos de heap que são necessários para os vários ambientes do VMware, consulte Tabela 218 na página 810.

Importante: O sistema, no qual é instalado e configurado o Agente VMware VI, deve ter espaço de memória adequado para acomodar o tamanho de heap necessário.

Se surgir qualquer um dos seguintes problemas, pode ser necessário aumentar o tamanho de heap:

- O provedor de dados Java parar devido a um problema de `javacore` e criar um arquivo chamado `javacore.`*`date.time.number`*`.txt` no diretório `CANDLEHOME\tmaitm6_x64`.
- O arquivo `javacore.`*`date.time.number`*`.txt` contém a sequência `java/lang/OutOfMemoryError`.

Procedimento

- Windows

  Execute as etapas a seguir para configurar um valor de 1 GB como o tamanho de heap:

  1. Abra o arquivo `%CANDLE_HOME%\TMAITM6_x64\kvm_data_provider.bat`.
  2. Inclua a seguinte linha antes da linha que começa com `KVM_JVM_ARGS="%KVM_CUSTOM_JVM_ARGS...`:

     ```
     SET KVM_CUSTOM_JVM_ARGS=-Xmx1024m
     ```

  3. Reinicie o agente.

- Linux

  Execute as etapas a seguir para configurar um valor de 1 GB como tamanho de heap:

  1. Abra o arquivo `$CANDLEHOME/lx8266/vm/bin/kvm_data_provider.sh`.
  2. Inclua a linha a seguir antes da linha que começa com `KVM_JVM_ARGS="$KVM_CUSTOM_JVM_ARGS...`:

     ```
     KVM_CUSTOM_JVM_ARGS=-Xmx1024m
     ```

  3. Reinicie o agente.

Configurando o monitoramento do WebLogic

O Monitoring Agent for WebLogic fornece um ponto central de monitoramento para o funcionamento, a disponibilidade e o desempenho do ambiente do servidor WebLogic. O agente exibe um conjunto abrangente de métricas para ajudá-lo a tomar decisões informadas sobre seus recursos WebLogic, incluindo Java virtual machines (JVMs), serviço de sistema de mensagens Java (JMS), Java Database Connectivity (JDBC).

Antes de Iniciar

- Estas instruções são para a liberação mais atual do agente, exceto conforme indicado.
- Certifique-se de que os requisitos do sistema para o Agente WebLogic sejam atendidos em seu ambiente. Para obter informações atualizadas sobre requisitos do sistema, consulte o Software Product Compatibility Reports (SPCR) para o Agente WebLogic.
- Antes de você configurar o Agente WebLogic, o servidor Oracle WebLogic deve ser configurado, primeiramente, concluindo as tarefas a seguir:

  Nota: A maior parte da configuração do servidor Oracle WebLogic é feita usando o console administrativo, geralmente em `http://`*`weblogic-server`*`:7001/console`.

1. Configure um usuário de monitor no grupo de Monitores.
   a. Selecione o domínio para monitorar/editar.
   b. Selecione **Domínios de Segurança**.
   c. Selecione o seu domínio de segurança (ou crie um se não existir um).
   d. Crie um usuário que será usado para se comunicar com WebLogic sobre JMX.
   e. Inclua esse usuário no grupo de Monitores.
   f. Salve as mudanças no domínio.
2. Ative as Portas de Escuta.
   a. Selecione o domínio para monitorar/editar.
   b. Em cada servidor que deseja monitorar, clique em **Ambiente** > **Servidores** > ***Selecionar um Servidor***.
   c. Certifique-se de que a **Porta de recebimento** esteja ativada e anote seu número da porta.
   d. Se desejar ativar SSL, certifique-se de que a **Porta do listener SSL** esteja ativada e também configure uma porta para SSL.
3. Ative as Conexões do Servidor de Bean Gerenciado de JMX.
   a. Selecione o domínio que deseja monitorar/editar.
   b. Selecione **Configurar** > **Avançado**.
   c. Marque **Servidor de Bean Gerenciado de Plataforma Ativado**.
   d. Salve a alteração.
4. Ative a opção Protocolo de IIOP.
   a. Selecione o domínio que deseja monitorar/editar.
   b. Em cada servidor que você deseja monitorar, clique em **Ambiente** > **Servidores**, em seguida, selecione um servidor.
   c. Selecione a **Guia de Protocolo** > ***Selecione IIOP***.
   d. Sob a seção **Avançada**, insira o nome do usuário e senha de IIOP padrão.
   e. Salve a alteração.
5. Ative o SSL.
   a. Ativar encapsulamento HTTP.
      1) Acesse **Ambiente** > **Servidores** > ***Selecione um servidor*** > **Protocolo** > **Geral**.
      2) Marque **Ativar Tunelamento de HTTP**.
   b. Ative Porta de Escuta de SSL.
      1) Acesse **Ambiente** > **Servidores** > ***Selecionar um Servidor*** > **Configuração** > **Geral**.
      2) Configure um número da porta.

Sobre Esta Tarefa

O Agente WebLogic é um agente de várias instâncias e também um agente de vários subnós. É possível criar uma instância de agente com vários subnós – um para cada servidor WebLogic, ou é possível criar uma instância de agente para cada servidor WebLogic com um subnó para esse servidor. Ou é possível criar uma combinação de cada tipo de configuração. Depois de configurar instâncias de agente, você deve iniciar cada instância de agente manualmente.

Procedimento

1. Para configurar o agente em sistemas Windows, use a janela **IBM Performance Management** ou o arquivo de resposta silencioso com o arquivo em lote de configuração do agente.
   - "Configurando o agente nos sistemas Windows" na página 819.

- “Configurando o agente usando o arquivo silencioso de resposta” na página 823.

2. Para configurar o agente em sistemas Linux e UNIX, execute o script de configuração do agente e responda aos prompts, ou use o arquivo de resposta silencioso.
   - “Configurando o agente respondendo aos prompts” na página 822.
   - “Configurando o agente usando o arquivo silencioso de resposta” na página 823.
3. Opcional: Para configurar o rastreamento de transação, configure instâncias de agente individuais para fornecer dados de rastreamento de transação e configure o Application Performance Dashboard para exibir dados de rastreamento de transação.
   a) Siga o procedimento para “Configurando o rastreamento de transações para o Agente WebLogic” na página 826.
   b) Siga o procedimento para “Configurando o Application Performance Dashboard para exibir dados de rastreamento de transação para o Agente WebLogic” na página 832.

   Nota: O recurso de rastreamento de transações está disponível para o Agente WebLogic na oferta do Cloud APM, Advanced. Para o Agente WebLogic com capacidade de monitoramento de recurso básico, que está na oferta do Cloud APM, Base, ignore esta etapa.

O que Fazer Depois

No Console do Cloud APM, acesse seu Application Performance Dashboard para visualizar os dados que foram coletados. Para obter informações adicionais sobre como usar o Console do Cloud APM, consulte “Iniciando o Console do Cloud APM” na página 975.

Se você não conseguir visualizar os dados nos painéis do agente, primeiro verifique os logs de conexão do servidor e, em seguida, os logs do provedor de dados. Os caminhos padrão para esses logs são os seguintes:

- Linux AIX `/opt/ibm/apm/agent/logs`
- Windows `C:\IBM\APM\TMAITM6_x64\logs`

Para obter ajuda com a resolução de problemas, consulte o Fórum do Cloud Application Performance Management.

Configurando o agente nos sistemas Windows

É possível configurar o Agente WebLogic em sistemas operacionais Windows usando a janela IBM Cloud Application Performance Management. Após fazer a atualização dos valores de configuração, deve-se iniciar o agente para salvar os valores atualizados.

Procedimento

1. Clique em **Iniciar** > **Todos os Programas** > **Agentes de Monitoramento IBM** > **IBM Cloud Application Performance Management**.
2. Na janela **IBM Performance Management**, clique com o botão direito no modelo **Monitoring Agent for WebLogic** e, em seguida, clique em **Configurar agente**.

   Lembre-se: Depois de configurar uma instância de agente pela primeira vez, a opção **Configurar agente** é desativada. Para configurar a instância de agente novamente, clique nela com o botão direito e clique em **Reconfigurar**.
3. Insira um nome de instância exclusivo e, em seguida, clique em **OK**. Use apenas letras, numerais Arábicos, o caractere sublinhado e o caractere de menos no nome da instância. Por exemplo: `weblogic01`.

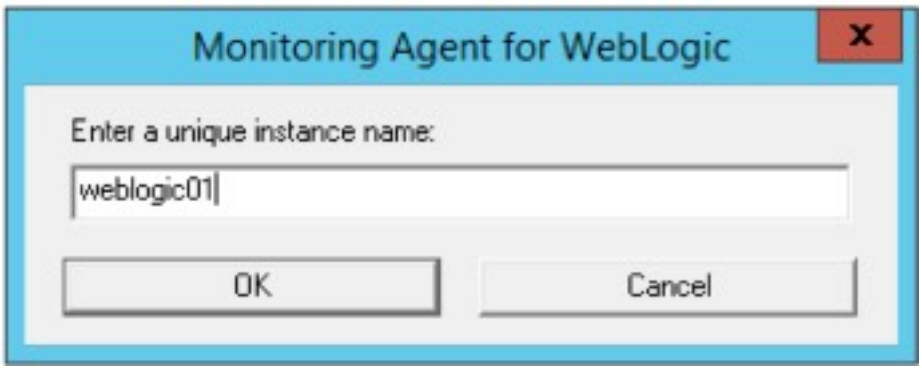


Figura 27. A Janela para Inserir um Nome da Instância Exclusivo

4. Clique em **Avançar** no painel de configuração do agente **Nome da instância**.

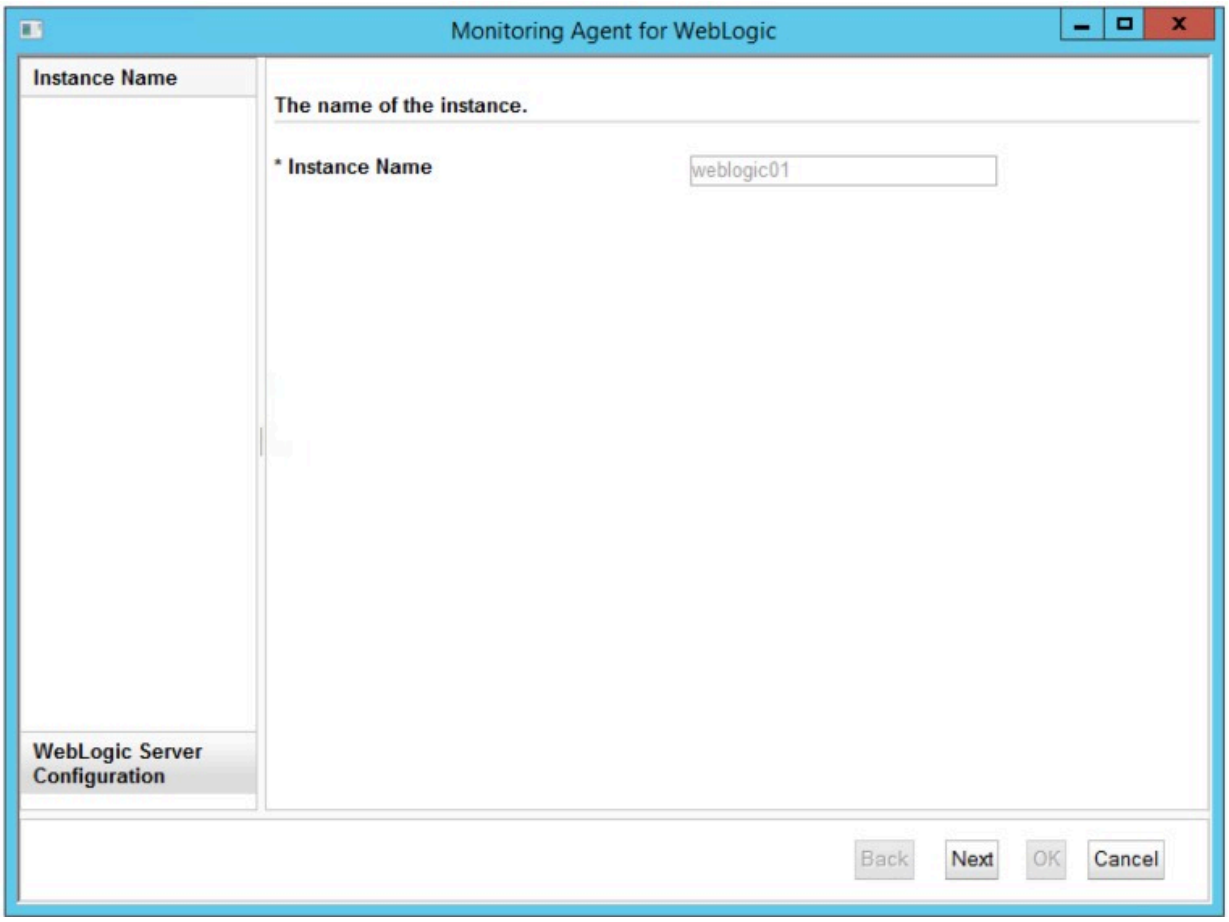


Figura 28. A janela que exibe o nome da instância de agente

5. Insira as configurações de modelo de instância **Configuração do servidor WebLogic**.

   Nota: Essa seção não é a configuração da instância de conexão do servidor WebLogic. É uma seção de modelo para configurar o que é usado como os valores padrão ao incluir as configurações reais da instância de conexão do servidor WebLogic começando na etapa 6.

   Consulte Tabela 221 na página 825 para obter uma explicação de cada um dos parâmetros de configuração.

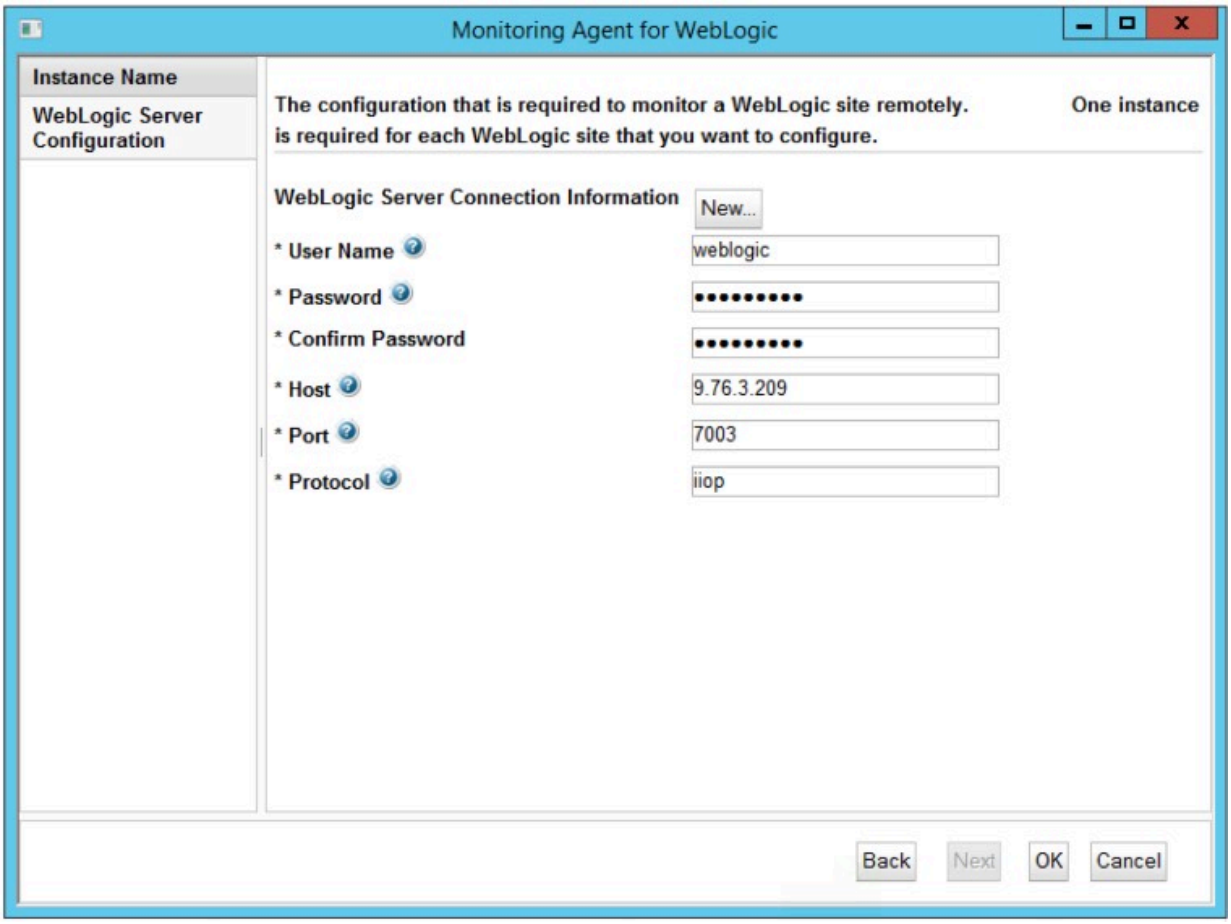


Figura 29. A janela para especificar configurações de modelo de instância de conexão do servidor WebLogic

6. Pressione **Novo** e insira configurações de instância de conexão do servidor WebLogic, em seguida, clique em **Avançar**.

   Consulte Tabela 221 na página 825 para obter uma explicação de cada um dos parâmetros de configuração.

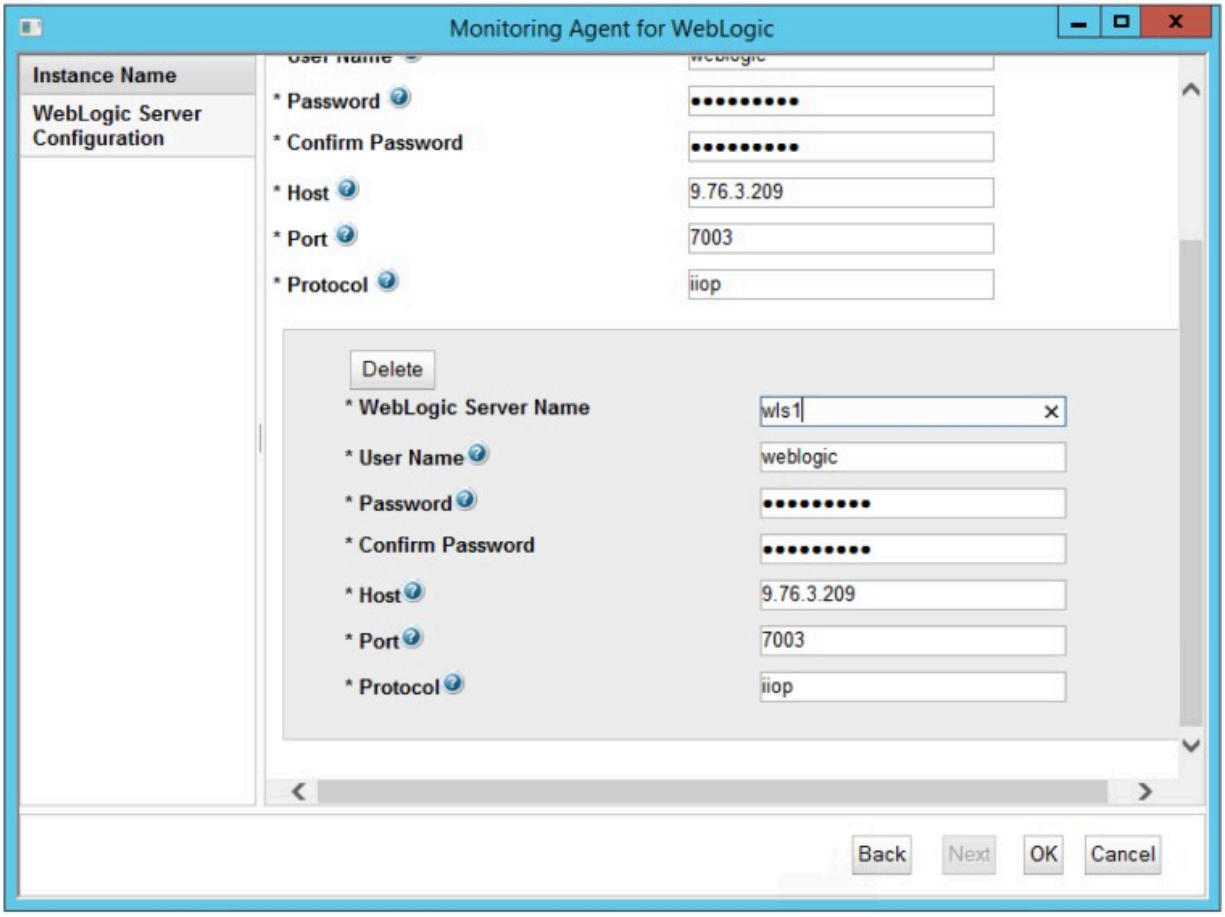


Figura 30. A janela para especificar configurações da instância de conexão do servidor WebLogic

7. Clique em **OK** para concluir a configuração.
8. Copie os arquivos de segurança do WebLogic no diretório binário do Agente WebLogic.
   a. Localize os arquivos `wlclient.jar` e `wljmxclient.jar` em `ORACLE_HOME`. Por exemplo, `C:\Oracle\Middleware\Oracle_Home\wlserver\server\lib`.
   b. Copie os arquivos da etapa "8.a" na página 822 para o diretório binário do Agente WebLogic.
      - Linux AIX *install_dir*`/bin`.
      - Windows *install_dir*`\TMAITM6_x64`

      em que *install_dir* é o caminho no qual o agente está instalado. O padrão *install_dir* caminhos são listados aqui:
      - Linux AIX `/opt/ibm/apm/agent`
      - Windows `C:\IBM\APM\TMAITM6_x64`
9. Na janela IBM Cloud Application Performance Management, clique com o botão direito na instância configurada e, em seguida, clique em **Iniciar**.

Configurando o agente respondendo aos prompts

Após a instalação do Agente WebLogic, deve-se configurá-lo antes de iniciar o agente. Se o Agente WebLogic estiver instalado em um computador local Linux ou UNIX, é possível seguir essas instruções para configurá-lo interativamente através de prompts da linha de comandos.

Sobre Esta Tarefa

Lembre-se: Se estiver reconfigurando uma instância do agente configurada, o valor que é definido na última configuração será exibido para cada configuração. Se desejar limpar um valor existente, pressione a tecla Espaço quando a configuração for exibida.

Procedimento

Siga essas etapas para configurar o Agente WebLogic executando um script e respondendo aos prompts.

1. Execute o comando a seguir.

   install_dir/bin/weblogic-agent.sh config **instance_name**

   em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome que você deseja fornecer para a instância de agente.

   Exemplo

   ```
   /opt/ibm/apm/agent/bin/weblogic-agent.sh config example-inst01
   ```

2. Responda aos prompts para configurar valores de configuração para o agente.

   Consulte "Parâmetros de Configuração para o Agente WebLogic" na página 825 para obter uma explicação de cada um dos parâmetros de configuração.

3. Copie os arquivos da biblioteca do cliente WebLogic para o diretório binário do Agente WebLogic.

   a) Localize os arquivos `wlclient.jar` e `wljmxclient.jar` em ORACLE_HOME.

   b) Copie os arquivos da etapa "3.a" na página 823 para o diretório binário do Agente WebLogic.

   install_dir/bin

   em que *install_dir* é o caminho no qual o agente está instalado.

   Exemplo

   ```
   /opt/ibm/apm/agent/bin
   ```

4. Execute o comando a seguir para iniciar o agente:

   install_dir/bin/weblogic-agent.sh start **instance_name**

   em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome da instância de agente.

   Exemplo

   ```
   Start example-inst01
   ```

Configurando o agente usando o arquivo silencioso de resposta

O arquivo silencioso de resposta contém os parâmetros de configuração do agente. É possível editar o arquivo silencioso de resposta para modificar os valores desses parâmetros e executar o script de configuração para criar uma instância e atualizar os valores de configuração do agente. Esse modo de configuração é chamado modo silencioso.

Sobre Esta Tarefa

O arquivo silencioso de resposta contém parâmetros de configuração do agente com valores padrão definidos para alguns parâmetros. É possível editar o arquivo silencioso de resposta para especificar os valores diferentes para os parâmetros de configuração.

Após você atualizar os valores de configuração no arquivo silencioso de resposta, deve executar o script de configuração para configurar o agente com esses valores atualizados.

Procedimento

Configure o Agente WebLogic no modo silencioso concluindo as etapas a seguir.

1. Em um editor de texto, abra o arquivo `weblogic_silent_config.txt` que está disponível no seguinte caminho:

   - Linux AIX *install_dir*/samples/weblogic_silent_config.txt
   - Windows *install_dir*\samples\weblogic_silent_config.txt

   em que *install_dir* é o caminho no qual o agente está instalado.

   Exemplo

   - Linux AIX /opt/ibm/apm/agent/samples/weblogic_silent_config.txt
   - Windows C:\IBM\APM\samples\weblogic_silent_config.txt

2. No arquivo `weblogic_silent_config.txt`, especifique valores para todos os parâmetros obrigatórios. Também é possível modificar os valores padrão de outros parâmetros.

   Consulte "Parâmetros de Configuração para o Agente WebLogic" na página 825 para obter uma explicação de cada um dos parâmetros de configuração.

3. Salve e feche o arquivo `weblogic_silent_config.txt` e execute o seguinte comando:

   - Linux AIX *install_dir*/bin/weblogic-agent.sh config **instance_name** *install_dir*/samples/weblogic_silent_config.txt
   - Windows *install_dir*\bin\weblogic-agent.bat config **instance_name** *install_dir*\samples\weblogic_silent_config.txt

   em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome que você deseja fornecer para a instância de agente.

   O padrão *install_dir* caminhos são listados aqui:

   - Linux AIX /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64

   Importante: Assegure que você inclua o caminho absoluto no arquivo silencioso de resposta. Caso contrário, os dados do agente não serão mostrados nos painéis.

   Exemplo

   - Linux AIX /opt/ibm/apm/agent/bin/weblogic-agent.sh config example-inst01 /opt/ibm/apm/agent/samples/weblogic_silent_config.txt
   - Windows C:\IBM\APM\bin\weblogic-agent.bat config example-inst01 C:\IBM\APM\samples\weblogic_silent_config.txt

4. Copie as bibliotecas do cliente WebLogic para o diretório binário do Agente WebLogic.

   a. Localize os arquivos `wlclient.jar` e `wljmxclient.jar` em ORACLE_HOME.

   b. Copie os arquivos da etapa "5.a" na página 824 para o diretório binário do Agente WebLogic.

   - Linux AIX *install_dir*/bin.
   - Windows *install_dir*\TMAITM6_x64

   em que *install_dir* é o caminho no qual o agente está instalado. O padrão *install_dir* caminhos são listados aqui:

   - Linux AIX /opt/ibm/apm/agent
   - Windows C:\IBM\APM\TMAITM6_x64

5. Execute o comando a seguir para iniciar o agente:

- Linux AIX *install_dir*/bin/weblogic-agent.sh start **instance_name**
- Windows *install_dir*\bin\weblogic-agent.bat start **instance_name**

em que *install_dir* é o caminho no qual o agente está instalado e *instance_name* é o nome da instância de agente.

O padrão *install_dir* caminhos são listados aqui:

- Linux AIX /opt/ibm/apm/agent
- Windows C:\IBM\APM\TMAITM6_x64

Exemplo

- Linux AIX /opt/ibm/apm/agent/bin/weblogic-agent.sh start example-inst01
- Windows C:\IBM\APM\bin\weblogic-agent.bat start example-inst01

Parâmetros de Configuração para o Agente WebLogic

Os parâmetros de configuração para o Agente WebLogic são exibidos em uma tabela.

1. Configurações do Agente WebLogic - Configurações do ambiente do agente WebLogic.

Tabela 221. Configurações do agente WebLogic

Nome de parâmetro	Descrição	Nome do parâmetro do arquivo de configuração silenciosa
Nome do Servidor WebLogic	Forneça um nome para identificar a instância de agente do servidor WebLogic. Exemplo: *wls1* **Nota:** Esse alias pode ser qualquer opção escolhida para representar a instância de agente do servidor WebLogic com as seguintes restrições. Somente letras, numerais arábicos, o caractere sublinhado e o caractere menos podem ser usados no nome da conexão. O comprimento máximo do nome de uma conexão é 25 caracteres.	Cada um dos seguintes parâmetros deve ter um sufixo de nome da instância que será o mesmo para cada parâmetro de uma instância de agente. As novas instâncias de agente devem usar um nome de instância exclusivo para seu conjunto de parâmetros. Por exemplo, uma instância de agente pode usar *.wls1* e outra instância de agente pode usar *.wls2* no lugar de *.instance_name* nos nomes de parâmetros abaixo.
Nome do Usuário	O nome do usuário usado para se autenticar com o servidor WebLogic.	**KWB_WLS_USERNAME.instance_name**
Senha	A senha usada para se autenticar com o servidor WebLogic.	**KWB_WLS_PASSWORD.instance_name**
Host	O host usado para se autenticar com o servidor WebLogic. Digite o nome completo do host ou o endereço IP do servidor WebLogic.	**KWB_WLS_HOST.instance_name**
Porta	A porta usada para se autenticar com o servidor WebLogic.	**KWB_WLS_PORT.instance_name**
Protocolo	O protocolo usado para se autenticar com o servidor WebLogic. Os protocolos suportados são *iiop* e *https*.	**KWB_WLS_PROTOCOL.instance_name**

Configurando o rastreamento de transações para o Agente WebLogic

O recurso de rastreamento de transação do Agente WebLogic requer mudanças no arquivo de configurações do ambiente de instância de agente e no arquivo de inicialização do servidor WebLogic. Um script é fornecido para ajudá-lo a fazer as mudanças.

Antes de Iniciar

Linux AIX Assegure que o limite de recurso para o arquivo aberto seja maior do que 5.000 para que o kit de ferramentas de rastreamento da transação funcione corretamente.

- Exiba a configuração de limite do arquivo aberto atual. **`ulimit -n`**
- Exemplo: configurar o limite do arquivo aberto como 5.056. **`ulimit -n 5056`**

Execute a "Configurando o monitoramento do WebLogic" na página 817 Windows etapa 1 ou a Linux AIX etapa 2 antes de seguir este procedimento.

Nota: O recurso de rastreamento de transações está disponível para o Agente WebLogic na oferta do Cloud APM, Advanced. Para o Agente WebLogic com capacidade de monitoramento de recurso básico, que está na oferta do Cloud APM, Base, ignore esta etapa.

O Agente WebLogic deve ser instalado localmente para o servidor WebLogic que é monitorado com o recurso de rastreamento de transação.

A conta do usuário que executa esse script deve ter permissão de gravação para os diretórios e arquivos a seguir:

1. O diretório *WEBLOGIC_HOME*.
2. O diretório *WEBLOGIC_HOME*/bin e arquivos.
3. O diretório *install_dir*/config.
4. O arquivo *install_dir*/config/*hostname*_wb_*instance_name*.cfg.

em que

WEBLOGIC_HOME
Diretório de instalação do servidor WebLogic.

install_dir
Caminho onde o agente está instalado. Os caminhos padrão para estes logs são conforme a seguir.

- Linux AIX `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

nome do host
Nome do computador host no qual o agente está instalado.

instance_name
Nome da instância de agente que é designado no tópico do método de configuração do agente:

- Configurando o agente em sistemas Windows, etapa "3" na página 819
- Configurando o agente respondendo aos prompts, etapa "1" na página 823
- Configurando o agente usando o arquivo de resposta silencioso, etapa "2" na página 824

Procedimento

Execute o script **`simpleConfig`**.

1. Efetue login no servidor WebLogic com o Agente WebLogic instalado.
2. Vá para o diretório de instalação do agente.

- Linux AIX *install_dir*
- Windows *install_dir*\TMAITM6_x64

em que *install_dir* é o caminho no qual o agente está instalado.

O padrão *install_dir* caminhos são listados aqui:

- Linux AIX `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

3. Mude o diretório para `wbdchome/8.1.4.0.0/bin`.
4. Execute o script de configuração.
   - Linux AIX `./simpleConfig.sh`
   - Windows `simpleConfig.bat`
5. Siga os prompts para inserir parâmetros para seu ambiente.
   a) Escolha o *instance_name* do Agente WebLogic e o subnó para configurar na lista de instâncias de agente detectadas e de combinações de subnó, em que *instance_name* é o nome da instância de agente.
   b) Digite o número do método de inicialização do servidor WebLogic.
   c) Digite o caminho da procura raiz de domínio do WebLogic.
      Este caminho é usado como a base para a qual procurar domínios do WebLogic. Se a variável de ambiente *WEBLOGIC_HOME* estiver configurada, seu valor será oferecido como o valor padrão.
   d) Digite o número do domínio do WebLogic para o servidor WebLogic para configuração.
   e) Digite o número do nome do servidor WebLogic para configuração.

Linux Configuração de exemplo com um método de inicialização do WebLogic de `WebLogic startup script`.

```
./simpleconfig.sh

Os seguintes agentes e subnós ainda não estão configurados para rastreamento de transação:

1) wlinst1 Server1
2) wlinst1 Server2

Digite o número que corresponde à instância do agente e do subnó que você deseja configurar.

Digite sua seleção aqui (Por exemplo: 1): 1

Os métodos de inicialização a seguir são suportados WebLogic:

1) Script de inicialização do WebLogic
2) WebLogic Node Manager

Digite sua seleção aqui (o padrão é 1): 1

O caminho para começar a procurar domínios WebLogic.
Raiz de procura por domínio do WebLogic (o padrão é: ): /home/wlsadmin

Os caminhos de domínio do WebLogic encontrados:

1) /home/wlsadmin/oracle/user_projects/domains/ttdd

Digite o número que corresponde ao domínio do WebLogic que contém o servidor WebLogic que
você deseja configurar.

Digite sua seleção aqui (Por exemplo: 1): 1

Os seguintes servidores WebLogic estão disponíveis para configuração:

1) AdminServer
2) Server1

Selecione um nome do servidor WebLogic (o padrão é: 2): 2
INFO: [2000] Configuração automática do arquivo de ambiente do agente bem-sucedida.
INFO: [3000] Configuração automática do script de início do WebLogic bem-sucedida.
INFO: [9000] Reinicie o agente WebLogic e o servidor WebLogic para que a configuração entre
em vigor.
```

6. Siga estas etapas se `Gerenciador de nó WebLogic` estiver selecionado como o **`WebLogic server startup method`** na etapa “5.b” na página 827. Caso contrário, prossiga para a etapa “7” na página 829.
   a) Abra o arquivo `weblogic_nodemanager_dc_opts` que é listado na mensagem de informação número 3011 do texto de saída da etapa “5” na página 827.

   Windows Saída de configuração de exemplo com um método de inicialização do WebLogic de `WebLogic Node Manager`.

   ```
   INFO: [2000] Configuração automática do arquivo de ambiente do agente bem-sucedida.
   INFO: [3010] Configuração automática do script de início do WebLogic ignorada.
   INFO: [3011] Revise C:\IBM\APM\TMAITM6_x64\wbdchome\8.1.4.0.0\runtime\ttdd_win
   \win_Server1\
   staging\weblogic_nodemanager_dc_opts.win para opções iniciais necessárias da JVM do
   WebLogic.
   INFO: [9000] Reinicie o agente WebLogic e o servidor WebLogic para que a configuração
   entre em vigor.
   ```

   b) Efetue login no console do WebLogic e selecione **Ambiente** > **Servidores**.
   c) Selecione o servidor para configurar.
   d) Selecione **Configuração** > **Iniciar Servidor** guia.
   e) Copie os argumentos de início do servidor do arquivo `weblogic_nodemanager_dc_opts` para os Argumentos do **servidor de início** do servidor no console do WebLogic e salve as mudanças.

   Os argumentos de início do servidor são todas as linhas após a linha de comentário `# Add the following lines to the server start arguments` no arquivo `weblogic_nodemanager_dc_opts`.
   f) Certifique-se de que o kit de ferramentas de rastreamento de transação esteja no caminho da biblioteca compartilhada no tempo de execução.

   Escolha um método.

   - Atualize o script de início Node Manager.

     Nota: Todos os servidores WebLogic iniciados pelo Node Manager têm esse caminho da biblioteca configurado com as bibliotecas do arquivo de objeto do kit de ferramentas de rastreamento de transação incluídas.

     1) Abra o arquivo `weblogic_nodemanager_dc_opts` que é listado na mensagem de informação número 3011 do texto de saída da etapa “5” na página 827.
     2) Configure o caminho do kit de ferramentas de rastreamento de transação no script de início do Node Manager. O comando para configurar o caminho é a linha que segue a linha de comentário `# Certifique-se de que o caminho executável disponível para o servidor WebLogic inclua o diretório lib do kit de ferramentas` no arquivo `weblogic_nodemanager_dc_opts`.

        – Linux Copie a linha LD_LIBRARY_PATH do arquivo `weblogic_nodemanager_dc_opts.linux` gerado e cole-a abaixo da linha `export JAVA_OPTIONS` no script de início do Node Manager. Por exemplo, *`WEBLOGIC_HOME`*`/user_projects/domains/`*`domain_name`*`/bin/startNodeManager.sh`.

        – Windows Copie o PATH do arquivo `weblogic_nodemanager_dc_opts.win` gerado e cole-o abaixo da linha `export JAVA_OPTIONS` no script de início do Node Manager. Exemplo, *`WEBLOGIC_HOME`*`\user_projects\domains\`*`domain_name`*`\bin\startNodeManager.bat`.

        em que *`WEBLOGIC_HOME`* é o diretório de instalação do servidor WebLogic e *`domain_name`* é o nome do domínio do WebLogic.
   - Atualize o ambiente para a conta do usuário que inicia o Node Manager.

     Nota: Todos os aplicativos iniciados pela conta do usuário têm esse caminho da biblioteca configurado com as bibliotecas do arquivo de objeto do Kit de ferramentas incluídas.

1) Edite as configurações do ambiente para o usuário que inicia o Node Manager.

   – Linux AIX Edite o arquivo de recursos de shell ou o arquivo de perfil de shell. Por exemplo, no shell bash, `.bashrc` ou `.bash_profile`.

   – Windows Edite **Painel de Controle** > **Sistema e segurança** > **Sistema** > **Configurações avançadas do sistema** > **Variáveis de ambiente...** > **Variáveis do usuário para *user_name*** > **Caminho**, em que *user_name* é o nome da conta do usuário que é usada para iniciar o servidor WebLogic.

2) Configure o caminho do kit de ferramentas de rastreamento de transação no ambiente da conta do usuário. O comando para configurar o caminho é a linha que segue a linha de comentário `# Certifique-se de que o caminho executável disponível para o servidor WebLogic inclua o diretório lib do kit de ferramentas` no arquivo `weblogic_nodemanager_dc_opts`.

   – Linux AIX Copie a linha `export LD_LIBRARY_PATH` do arquivo `weblogic_nodemanager_dc_opts.linux` gerado. Se uma linha `export LD_LIBRARY_PATH` não existir, inclua-a. Se existir, edite-a para incluir somente o caminho da direita do sinal de igual ao caminho existente com o delimitador de caminho correto.

   – Windows Copie a linha `set PATH` do arquivo `weblogic_nodemanager_dc_opts.win` gerado. Se uma variável de **Caminho** não existir na seção **Variáveis do usuário para *user_name***, em que *user_name* é o nome da conta do usuário que é usada para iniciar o servidor WebLogic, inclua-a inserindo `Caminho` como o nome da variável e o caminho à direita do sinal de igual como o valor. Se existir, edite o valor para incluir somente o caminho da direita do sinal de igual ao caminho existente com o delimitador de caminho correto.

3) Recarregue o ambiente.

Aviso: Os scripts `startNodeManager` são gerados pelo utilitário de configuração do WebLogic. Portanto, você pode perder suas mudanças quando a configuração do WebLogic for executada novamente.

7. Se o servidor WebLogic e o agente estiverem em execução, reinicie-os.

Resultados

Arquivos do servidor WebLogic que são mudados durante a configuração do rastreamento de transação:

- O `startManagedWebLogic` script.
  – Linux AIX *WEBLOGIC_HOME*`/bin/startManagedWebLogic.sh`
  – Windows *WEBLOGIC_HOME*`\bin\startManagedWebLogic.cmd`

  em que *WEBLOGIC_HOME* é o diretório de instalação do servidor WebLogic.

  Esse arquivo é atualizado com definições de configuração para o recurso de rastreamento de transação. Os marcadores de configuração são inseridos no arquivo para uso quando você desativar o recurso de rastreamento de transações. Um arquivo de backup é salvo no diretório *WEBLOGIC_HOME*`/bin/bak/` antes do script incluir ou remover as mudanças no recurso de rastreamento de transação.

Arquivos do agente que são mudados durante a configuração de rastreamento de transações:

- Arquivo de configuração da instância de agente
  – Linux AIX *install_dir*`/config/`*hostname*`_wb_`*instance_name*`.cfg`
  – Windows *install_dir*`\TMAITM6_x64 \`*hostname*`_WB_`*instance_name*`.cfg`
- Arquivo de configurações do ambiente do agente
  – Linux AIX *install_dir*`/config/wb_`*instance_name*`.environment`
  – Windows *install_dir*`\TMAITM6_x64\KWBENV_`*instance_name*

em que

install_dir
Caminho onde o agente está instalado. Os caminhos padrão para estes logs são conforme a seguir.

- Linux AIX `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

nome do host
Nome do computador host no qual o agente está instalado.

instance_name
Nome da instância de agente que é designado no tópico do método de configuração do agente:

- Configurando o agente em sistemas Windows, etapa "3" na página 819
- Configurando o agente respondendo aos prompts, etapa "1" na página 823
- Configurando o agente usando o arquivo de resposta silencioso, etapa "2" na página 824

Desativando o rastreamento de transação para uma instância do Agente WebLogic
O recurso de rastreamento de transação do Agente WebLogic pode ser removido. É fornecido um script para remover o recurso de rastreamento de transação para uma instância de agente.

Antes de Iniciar

Certifique-se de que o servidor WebLogic e o Agente WebLogic estejam encerrados.

A conta do usuário que executa esse script deve ter permissão de gravação para os diretórios e arquivos a seguir:

1. O diretório *WEBLOGIC_HOME*.
2. O diretório *WEBLOGIC_HOME*`/bin` e arquivos.
3. O diretório *install_dir*`/config`.
4. O arquivo *install_dir*`/config/`*hostname*`_wb_`*instance_name*`.cfg`.

Procedimento

Execute o script **unconfig** com a opção **remove**.

1. Efetue login no servidor WebLogic com o Agente WebLogic instalado.
2. Vá para o diretório de instalação do agente.
   - Linux AIX *install_dir*
   - Windows *install_dir*`\TMAITM6_x64`
3. Mude o diretório para `wbdchome/8.1.4.0.0/bin`.
4. Execute **unconfig** com a opção **remove** e o nome da instância de agente e o nome do subnó.
   - Para desativar um subnó para uma instância de agente, use o parâmetro *subnode_name*.
     - Linux AIX `./unconfig.sh` **remove** *instance_name subnode_name*
     - Windows `unconfig.bat` **remove** *instance_name subnode_name*
   - Para desativar todos os subnós para uma instância de agente, omita o parâmetro *subnode_name*.
     - Linux AIX `./unconfig.sh` **remove** *instance_name*
     - Windows `unconfig.bat` **remove** *instance_name*
5. Inicie o servidor WebLogic e o agente.

   em que

   WEBLOGIC_HOME
   Diretório de instalação do servidor WebLogic.

nome do host
Nome do computador host no qual o agente está instalado.

instance_name
Nome da instância de agente que é designado no tópico do método de configuração do agente:

- Configurando o agente em sistemas Windows, etapa “3” na página 819
- Configurando o agente respondendo aos prompts, etapa “1” na página 823
- Configurando o agente usando o arquivo de resposta silencioso, etapa “2” na página 824

subnode_name
Nome do subnó da instância de agente que é designado ao parâmetro de **Nome do servidor WebLogic** no tópico do método de configuração do agente:

- Configurando o agente em sistemas Windows, etapa “6” na página 821
- Configurando o agente respondendo aos prompts, etapa “2” na página 823
- Configurando o agente usando o arquivo de resposta silencioso, etapa “2” na página 824

install_dir
Caminho onde o agente está instalado. Os caminhos padrão para estes logs são conforme a seguir.

- Linux AIX `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

Desinstalando o rastreamento de transação para o Agente WebLogic
O recurso de rastreamento de transações do Agente WebLogic pode ser desinstalado. É fornecido um script para remover o recurso de rastreamento de transação de todas as instâncias de agente e também para remover o kit de ferramentas de rastreamento de transação.

Antes de Iniciar

Certifique-se de que o servidor WebLogic e todas as instâncias do Agente WebLogic estejam encerrados.

A conta do usuário que executa esse script deve ter permissão de gravação para os diretórios e arquivos a seguir:

1. O diretório *WEBLOGIC_HOME*.
2. O diretório *WEBLOGIC_HOME*`/bin` e arquivos.
3. O diretório *install_dir*`/config`.
4. O arquivo *install_dir*`/config/`*hostname*`_wb_`*instance_name*`.cfg`.

Procedimento

Execute o script **unconfig** com o a opção **uninstall**.

1. Efetue login no servidor WebLogic com o Agente WebLogic instalado.
2. Vá para o diretório de instalação do agente.
   - Linux AIX *install_dir*
   - Windows *install_dir*`\TMAITM6_x64`
3. Mude o diretório para `wbdchome/8.1.4.0.0/bin`.
4. Execute **unconfig** com a opção **uninstall**.
   - Linux AIX `./unconfig.sh` **uninstall**
   - Windows `unconfig.bat` **uninstall**
5. Inicie o servidor WebLogic e todas as instâncias de agente.

em que

WEBLOGIC_HOME
Diretório de instalação do servidor WebLogic.

nome do host
Nome do computador host no qual o agente está instalado.

instance_name
Nome da instância de agente que é designado no tópico do método de configuração do agente:

- Configurando o agente em sistemas Windows, etapa "3" na página 819
- Configurando o agente respondendo aos prompts, etapa "1" na página 823
- Configurando o agente usando o arquivo de resposta silencioso, etapa "2" na página 824

install_dir
Caminho onde o agente está instalado. Os caminhos padrão para estes logs são conforme a seguir.

- Linux AIX `/opt/ibm/apm/agent`
- Windows `C:\IBM\APM\TMAITM6_x64`

Configurando o Application Performance Dashboard para exibir dados de rastreamento de transação para o Agente WebLogic

A visualização de dados que são reunidos pelo recurso de rastreamento de transação do Agente WebLogic requer mudanças na configuração para o Application Performance Dashboard.

Antes de Iniciar

Execute o "Configurando o rastreamento de transações para o Agente WebLogic" na página 826 antes de seguir este procedimento.

Procedimento

1. Ative os dados de rastreamento de transações no Application Performance Dashboard se você possuir o Agente WebLogic com o recurso de rastreamento de transações, que está na oferta do Cloud APM, Advanced, e você desejar ativar o recurso de rastreamento de transações.
   a) A partir da barra de navegação, clique em **Configuração do Sistema** > **Configuração do Agente**.
   A página **Configuração do Agente** é exibida.
   b) Selecione o **WebLogic** guia.
   c) Selecione as caixas de seleção para as instâncias do agente do servidor WebLogic que você deseja monitorar e execute uma das seguintes ações da lista **Ações**:
   - Para ativar o rastreamento de transações, clique em **Configurar rastreamento de transações** > **Ativado**. O status na coluna **Rastreamento de Transações** é atualizado para *Enabled*.
   - Para desativar o rastreamento de transação, clique em **Configurar Rastreamento de Transação** > **Desativado**. O status na coluna **Rastreamento de Transações** é atualizado para *Disabled*.
2. Para visualizar os painéis de dados de rastreamento de transações do Agente WebLogic, inclua a instância do Agente WebLogic em um aplicativo em seu Application Performance Dashboard.
   Para obter informações adicionais sobre o editor de Aplicativos, consulte Gerenciando aplicativos.
3. Assegure-se de que as contas de usuário sejam designadas a uma função que inclua a permissão Painel de Diagnóstico para ter acesso aos seguintes botões do Application Dashboard de rastreamento de transação do Agente WebLogic.
   Caso contrário, esses botões serão desativados para esse usuário no Application Dashboard.
   a. O botão de drill-down **Diagnosticar** no widget **5 Tempos de resposta mais lentos**.
   b. O botão **Solicitações em andamento** no widget **Aplicativos**.

Configurando o monitoramento de aplicativos WebSphere

A configuração do monitoramento de aplicativos WebSphere envolve a configuração de um coletor de dados para os servidores de aplicativos. O coletor de dados pode ser independente ou integrado ao WebSphere Applications agent.

Coletor de dados integrado

A maioria dos WebSphere Application Servers pode ser monitorada pelo coletor de dados integrado, exceto para o perfil Liberty no IBM Cloud. O coletor de dados integrado pode fornecer todos os recursos de monitoramento disponíveis.

Para configurar o coletor de dados integrado, deve-se primeiro instalar o WebSphere Applications agent no sistema em que o servidor de aplicativos está em execução. Depois disso, use os utilitários de configuração fornecidos para configurar o coletor de dados de modo interativo ou silencioso.

Coletor de dados independente

O coletor de dados independente é aplicável apenas ao WebSphere Application Server Liberty no Linux for System x e ao perfil do WebSphere Liberty no IBM Cloud.

Se você optar por configurar um coletor de dados independente, poderá ignorar o procedimento de instalação do agente e configurar diretamente o coletor de dados no Liberty.

No entanto, alguns dados diagnósticos on demand não serão coletados pelo coletor de dados independente, como dump do heap no momento atual ou informações de solicitação em andamento. Isso significa que é possível ativar o coletor de dados para coletar automaticamente as informações de dump do heap somente em intervalos especificados, mas não é possível obter captura instantânea de heap quando quiser usando o botão **Obter captura instantânea** no Console do Cloud APM. Todos os painéis relacionados a uma solicitação em andamento, que podem ser fornecidos pelo coletor de dados integrado, não estão disponíveis para o coletor de dados independente.

Use o Tabela 222 na página 833 para determinar o coletor de dados apropriado para o servidor de aplicativos.

Tabela 222. Aplicativos WebSphere para coletores de dados aplicáveis

Aplicativo a ser monitorado	Coletor de dados aplicável	Documentação
WebSphere Application Server tradicional	Coletor de dados integrado	“Configurando o coletor de dados para WebSphere Applications agent” na página 833
WebSphere Application Server Liberty (no local)	• Coletor de dados integrado • Coletor de dados independente (somente Linux for System x)	• “Configurando o coletor de dados para WebSphere Applications agent” na página 833 • “Configurando o coletor de dados Liberty para aplicativos no local” na página 880
Perfil do WebSphere Liberty no IBM Cloud	Coletor de dados independente	“Configurando o coletor de dados Liberty para aplicativos IBM Cloud” na página 884
Perfil do WebSphere Liberty no contêiner Docker	Coletor de dados integrado	“Monitorando o WebSphere Application Server Liberty dentro de um contêiner Docker” na página 867

Configurando o coletor de dados para WebSphere Applications agent

O WebSphere Applications agent não precisa de nenhuma configuração após a instalação do agente, a menos que deseje mudar a porta padrão. No entanto, você deve configurar o coletor de dados, que é um componente do agente, para configurar o monitoramento do ambiente do WebSphere.

Sobre Esta Tarefa

As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte “Histórico de Mudanças” na página 50.

Procedimento

- (Caminho rápido) Se você usar somente o WebSphere Applications agent sem o produto anterior ITCAM Agent for WebSphere Applications em seu ambiente, para configurar rapidamente o ambiente para monitoramento, consulte “Caminho rápido: configurando o coletor de dados para o WebSphere Applications agent” na página 834 para um fluxo de configuração simplificada.
- (Configuração simples) Para um fluxo de configuração completa para um ambiente puro do IBM Cloud Application Performance Management, consulte “Configurando o coletor de dados com o utilitário de configuração simples” na página 837.
- (Configuração completa) Para configurar o coletor de dados com mais opções de configuração, use os utilitários de configuração completa. Para obter instruções, veja “Configurando ou reconfigurando o coletor de dados com utilitários de configuração completos” na página 839.
- (Configuração silenciosa) Para implementar o mesmo monitoramento para muitas instâncias do servidor de aplicativos, configure o coletor de dados no modo silencioso. Para obter instruções, veja “Configurando o Coletor de Dados no Modo Silencioso” na página 848.
- (WebSphere Portal Server) Para monitorar instâncias do WebSphere Portal Server, use o procedimento de configuração avançada. Para obter instruções, veja “Configurando ou reconfigurando o coletor de dados com utilitários de configuração completos” na página 839.
- (Configuração manual) Se não for possível usar os utilitários de configuração fornecidos para configurar o coletor de dados para o WebSphere Applications agent, configure manualmente o coletor de dados no Console Administrativo do WebSphere. Para obter instruções, veja “Configurar manualmente o coletor de dados se os utilitários de configuração falharem” na página 855.
- (Coexistência do agente) Se desejar configurar o coletor de dados para funcionar em um ambiente de coexistência do agente no qual o WebSphere Applications agent e o ITCAM Agent for WebSphere Applications estão instalados, consulte “(Coexistência do agente) Configurando o WebSphere Applications agent e o coletor de dados” na página 859.
- (Monitoramento do Docker) Para monitorar o WebSphere Application Server Liberty em execução dentro de um contêiner do Docker, consulte “Monitorando o WebSphere Application Server Liberty dentro de um contêiner Docker” na página 867.

Caminho rápido: configurando o coletor de dados para o WebSphere Applications agent

O WebSphere Applications agent não precisa de nenhuma configuração após a instalação do agente. No entanto, você deve configurar o coletor de dados, que é um componente do agente, para configurar o monitoramento do ambiente do WebSphere.

Antes de Iniciar

1. Instale o WebSphere Applications agent no sistema em que o servidor de aplicativos a ser monitorado está instalado e em execução.
2. Verifique os requisitos de acesso de usuário.
   - Windows Use o ID de administrador que é usado para instalar o servidor de aplicativos para configurar o coletor de dados. Certifique-se de que esse ID do usuário tenha total permissão de gravação no diretório inicial do coletor de dados, *install_dir*\dchome\7.3.0.14.08.
   - Linux AIX Use o ID do usuário que é usado para instalar o servidor de aplicativos para configurar o coletor de dados. Certifique-se de que esse ID do usuário tenha permissões de leitura e gravação para os seguintes subdiretórios em *install_dir*/yndchome/7.3.0.14.08:

     – bin

- data
- runtime

Sobre Esta Tarefa

Um utilitário de configuração simples, `simpleconfig`, é usado neste procedimento para fornecer a configuração básica do coletor de dados.

O utilitário `simpleconfig` configura o coletor de dados com configurações padrão. Para configurar o coletor de dados com mais opções de customização, use o utilitário de configuração completa, `config`, no mesmo diretório. Para obter instruções, veja "Configurando ou reconfigurando o coletor de dados com utilitários de configuração completos" na página 839.

Na maioria dos casos, o utilitário `simpleconfig` é suficiente. Para um ambiente mais complexo, é possível usar o utilitário de configuração `config` para configurar o coletor de dados. Se o utilitário `simpleconfig` falhar, use o utilitário `config` no lugar.

Procedimento

1. Efetue login no sistema com o ID do usuário que é usado para instalar o servidor de aplicativos.
2. Mude o diretório `bin` no diretório inicial do coletor de dados.
   - Windows *install_dir*\dchome\7.3.0.14.08\bin
   - Linux AIX *install_dir*/yndchome/7.3.0.14.08/bin
3. Execute o seguinte utilitário de configuração simples:
   - Windows **simpleconfig.bat**
   - Linux AIX **./simpleconfig.sh**
4. Siga os prompts para continuar com a configuração do coletor de dados.

   É necessário fazer algumas ou todas as seguintes coisas, dependendo das configurações do servidor de aplicativos:

   - Para WebSphere Application Server traditional:
     - Selecione o diretório de instalação autodescoberto do WebSphere ou especifique manualmente o diretório de instalação.
     - Selecione o perfil do WebSphere Application Server a ser monitorado.
     - Selecione o perfil de propriedades de segurança a ser usado ou forneça o nome do usuário e a senha do console administrativo do WebSphere (se a segurança estiver ativada para o servidor de aplicativos).
   - Para WebSphere Application Server Liberty:
     - Especifique o caminho completo do diretório inicial do Liberty que contém os diretórios `bin` e `servers`. Por exemplo, `/opt/ibm/wlp`.
     - Especifique o diretório inicial do JRE que é usado pelo Liberty.
5. Após a conclusão da configuração do coletor de dados, reinicie o servidor de aplicativos.
   a) Acesse o diretório `bin` sob o diretório inicial para o perfil do servidor de aplicativos. Por exemplo, `opt/IBM/WebSphere/AppServer/profiles/`*profile_name*`/bin`.
   b) Pare o servidor de aplicativos inserindo o comando **stopServer** no console de comando.
      - Linux AIX `./stopServer.sh` *server_name*
      - Windows `stopServer.bat` *server_name*
   c) Quando solicitado, insira o ID do usuário e a senha do administrador do console administrativo do WebSphere.

d) Inicie o servidor de aplicativos novamente inserindo o comando **startServer** no console de comando.

- Linux AIX `./startServer.sh server_name`
- Windows `startServer.bat server_name`

6. Efetue login no Console do Cloud APM para visualizar dados nos painéis.
   a) Acesse o console usando o link fornecido no e-mail que alerta que seu serviço está pronto. Como alternativa, acesse o console a partir do website do IBM Marketplace. Para obter instruções detalhadas, consulte "Iniciando o Console do Cloud APM" na página 975.
   b) Use o Editor de aplicativos para incluir o servidor de aplicativos monitorado no Application Performance Dashboard. É possível incluí-lo como um novo componente para seu aplicativo existente ou criar um aplicativo para conter esse componente.

      Para obter informações adicionais sobre o Editor de aplicativos, consulte "Gerenciando aplicativos" na página 1098.

Resultados

O coletor de dados é configurado para monitorar a instância do servidor de aplicativos. Lembre-se de que a coleta de dados pode aumentar a sobrecarga do servidor de aplicativos. É possível controlar a coleta de dados com opções de configuração mais avançadas para ajuste.

Verificando requisitos de acesso de usuário

O WebSphere Applications agent possui alguns requisitos de acesso de usuário para o ID do usuário que irá configurar o coletor de dados.

Sobre Esta Tarefa

Use o ID que é usado para instalar o servidor de aplicativos para configurar o coletor de dados depois de conceder permissões apropriadas para o ID de instalação do servidor de aplicativos.

Procedimento

- Windows Use o ID de administrador que é usado para instalar o servidor de aplicativos para configurar o coletor de dados. Certifique-se de que esse ID do usuário tenha total permissão de gravação no diretório inicial do coletor de dados, *install_dir*\dchome\7.3.0.14.08.
- Linux AIX Use o ID do usuário que é usado para instalar o servidor de aplicativos para configurar o coletor de dados. Certifique-se de que esse ID do usuário tenha permissões de leitura e gravação para os seguintes subdiretórios em *install_dir*/yndchome/7.3.0.14.08:
  - bin
  - data
  - logs
  - runtime

  Lembre-se: Se você usar IDs do usuário diferentes para instalar servidores de aplicativos, pode ser necessário usar IDs do usuário diferentes para configurar o coletor de dados. Depois de configurar o coletor de dados pela primeira vez, conceda a permissão de gravação aos seguintes arquivos sempre que usar um ID do usuário diferente para configurar o coletor de dados, em que *profile_name* é o nome do perfil do servidor de aplicativos:
  - *install_dir*/yndchome/7.3.0.14.08/data/findservers.inputlist
  - *install_dir*/yndchome/7.3.0.14.08/data/*profile_name*.findservers.progress
  - *install_dir*/yndchome/7.3.0.14.08/data/config_inputlist
  - *install_dir*/yndchome/7.3.0.14.08/runtime/custom/connections.properties

Manipulando outro coletor de dados existente no servidor de aplicativos

Se já existir um coletor de dados no servidor de aplicativos, será necessário decidir o que fazer com o coletor de dados existente, para que ele não entre em conflito com o coletor de dados do WebSphere Applications agent.

Sobre Esta Tarefa

Os seguintes tipos de coletor de dados já podem existir no servidor de aplicativos que será monitorado:

- O coletor de dados do WebSphere Applications agent, que está instalado em uma versão anterior do IBM Cloud Application Performance Management
- O coletor de dados do ITCAM Agent for WebSphere Applications, que está instalado no antigo IBM® Tivoli® Monitoring Infrastructure
- Qualquer outro coletor de dados não fornecido pela IBM

Procedimento

Execute as ações apropriadas para evitar conflitos de coletores de dados.

- Para uma versão anterior do coletor de dados do WebSphere Applications agent, que está instalado em uma versão anterior do IBM Cloud Application Performance Management, existem as seguintes opções:
  - Migrar o coletor de dados com o utilitário de migração do diretório inicial do coletor de dados mais recente. Para obter instruções, veja "WebSphere Applications agent: migrando o coletor de dados" na página 1147.
  - Desconfigurar a versão anterior do coletor de dados e, em seguida, configurar o coletor de dados novamente com o utilitário de configuração do diretório inicial do coletor de dados mais recente. Para obter informações sobre como desconfigurar o coletor de dados, consulte "WebSphere Applications agent: desconfigurando o coletor de dados" na página 145.
- Para o coletor de dados do ITCAM Agent for WebSphere Applications, conclua as seguintes etapas se desejar implementar o monitoramento em um ambiente de coexistência do agente:
  a) Desinstale o coletor de dados do ITCAM Agent for WebSphere Applications.
  b) Configure somente um coletor de dados para enviar dados para o WebSphere Applications agent e o ITCAM Agent for WebSphere Applications. Para obter instruções, veja "(Coexistência do agente) Configurando o WebSphere Applications agent e o coletor de dados" na página 859.
- Para outros coletores de dados não fornecidos pela IBM, avalie se é necessário remover esses coletores de dados. O coletor de dados do WebSphere Applications agent usa a manipulação de Java Byte Code para coletar dados. Outros coletores de dados que usam a mesma forma para coletar dados podem entrar em conflito com o coletor de dados do WebSphere Applications agent.

Configurando o coletor de dados com o utilitário de configuração simples

O WebSphere Applications agent inicia automaticamente após a instalação, mas você deve configurar o coletor de dados manualmente, que é um componente do agente, para monitorar instâncias de servidor de aplicativos.

Antes de Iniciar

- Certifique-se de que os requisitos de acesso de usuário sejam atendidos em seu ambiente. Para obter instruções, veja "Verificando requisitos de acesso de usuário" na página 836.
- Se existirem outros coletores de dados no servidor de aplicativos que será monitorado, execute as ações apropriadas para evitar conflitos do coletor de dados. Para obter instruções, veja "Manipulando outro coletor de dados existente no servidor de aplicativos" na página 837.

Sobre Esta Tarefa

Importante:

- Se desejar configurar o coletor de dados somente para monitoramento de recursos ou para configurar opções extras, use o procedimento de configuração completa. Para obter instruções, veja "Configurando ou reconfigurando o coletor de dados com utilitários de configuração completos" na página 839.
- Se desejar mudar o nome do servidor na interface com o usuário de monitoramento, reconfigure o coletor de dados e especifique um alias de servidor. Para obter instruções, veja "Configurando ou reconfigurando o coletor de dados com utilitários de configuração completos" na página 839.

Para o WebSphere Applications agent, as variáveis *dc_home* referem-se ao diretório inicial do coletor de dados. O local da variável *dc_home* em cada sistema operacional é o seguinte:

- Windows *install_dir*\dchome\7.3.0.14.08
- Linux AIX *install_dir*/yndchome/7.3.0.14.08

Procedimento

1. Efetue login no sistema com o ID do usuário que é usado para instalar o servidor de aplicativos.
2. Mude o diretório `bin` no diretório inicial do coletor de dados.
   - Windows *install_dir*\dchome\7.3.0.14.08\bin
   - Linux AIX *install_dir*/yndchome/7.3.0.14.08/bin
3. Execute o seguinte utilitário de configuração simples:
   - Windows `simpleconfig.bat`
   - Linux AIX `./simpleconfig.sh`

   O utilitário **simpleconfig** descobre automaticamente os diretórios iniciais dos servidores de aplicativos.
4. Siga os prompts para continuar com a configuração do coletor de dados.

   É necessário fazer as seguintes coisas, dependendo das configurações do servidor de aplicativos:
   - Para WebSphere Application Server traditional:
     - Selecione o diretório de instalação autodescoberto do WebSphere ou especifique manualmente o diretório de instalação.
     - Selecione o perfil do WebSphere Application Server a ser monitorado.
     - Selecione o perfil de propriedades de segurança a ser usado ou forneça o nome do usuário e a senha do console administrativo do WebSphere (se a segurança estiver ativada para o servidor de aplicativos).
   - Para WebSphere Application Server Liberty:
     - Especifique o caminho completo do diretório inicial do Liberty que contém os diretórios `bin` e `servers` (por exemplo, `/opt/ibm/wlp`).
     - Especifique o diretório inicial do JRE que é usado pelo Liberty.
5. Se possível, reinicie a instância do servidor de aplicativos após a conclusão da configuração do coletor de dados.
   a) Acesse o diretório `bin` sob o diretório inicial para o perfil do servidor de aplicativos. Por exemplo, `opt/IBM/WebSphere/AppServer/profiles/profile_name/bin`.
   b) Pare o servidor de aplicativos inserindo o comando **stopServer** no console de comando.
      - Linux AIX `./stopServer.sh server_name`
      - Windows `stopServer.bat server_name`
   c) Quando solicitado, insira o ID do usuário e a senha do administrador do console administrativo do WebSphere.

d) Inicie o servidor de aplicativos novamente inserindo o comando **startServer** no console de comando.

- Linux AIX `./startServer.sh server_name`
- Windows `startServer.bat server_name`

Resultados

- O coletor de dados é configurado para monitorar todas as instâncias em um perfil ou, para o WebSphere Application Server Liberty, uma única instância ou várias instâncias no mesmo diretório. Para monitorar mais perfis ou instâncias, repita a configuração.
- O coletor de dados está configurado nas instâncias do servidor, fornecendo monitoramento máximo.
- Para o Cloud APM, Base, o monitoramento de recursos é ativado.
- Para o Cloud APM, Advanced, o monitoramento de recursos, rastreamento de transações e dados diagnósticos são ativados.

Limitação conhecida: Ao monitorar o WebSphere Application Server Liberty, o coletor de dados não pode gerar eventos da Java Naming and Directory Interface (JNDI).

O que Fazer Depois

- Efetue login no Console do Cloud APM e use o Editor de aplicativos para incluir o servidor de aplicativos monitorado no Application Performance Dashboard. Para obter instruções sobre como iniciar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975. Para obter informações sobre como usar o Editor de aplicativos, consulte "Gerenciando aplicativos" na página 1098.

  Lembre-se: Se o WebSphere Applications agent estiver configurado para monitorar o WebSphere Portal Server, o agente estará relacionado ao componente de aplicativo WebSphere Portal Server no Application Performance Dashboard, não no WebSphere Application Server.
- Se a interface com o usuário de monitoramento no Application Performance Dashboard não mostrar informações para a instância do servidor de aplicativos, reinicie o componente do agente de monitoramento do WebSphere Applications agent concluindo as seguintes etapas:
  - Windows

    ```
    cd install_dir\bin
    was-agent.bat stop
    was-agent.bat start
    ```
  - Linux AIX

    ```
    cd install_dir/bin
    ./was-agent.sh stop
    ./was-agent.sh start
    ```

Configurando ou reconfigurando o coletor de dados com utilitários de configuração completos
Para configurar opções de configuração adicionais, é possível usar os utilitários de configuração completos (interativos ou silenciosos) para configurar o coletor de dados em vez do utilitário de configuração simples. Também é possível usar utilitários de configuração completos para reconfigurar o coletor de dados quando ele já está configurado. Além disso, é preciso usar o utilitário de configuração completo para configurar o monitoramento para instâncias do WebSphere Portal Server.

Antes de Iniciar

- Certifique-se de que os requisitos de acesso de usuário sejam atendidos em seu ambiente. Para obter instruções, veja "Verificando requisitos de acesso de usuário" na página 836.
- Se existirem outros coletores de dados no servidor de aplicativos que será monitorado, execute as ações apropriadas para evitar conflitos do coletor de dados. Para obter instruções, veja "Manipulando outro coletor de dados existente no servidor de aplicativos" na página 837.

Sobre Esta Tarefa

Os utilitários de configuração e reconfiguração podem ser localizados nos seguintes diretórios:

- Windows *install_dir*\dchome\7.3.0.14.08\bin
- Linux AIX *install_dir*/yndchome/7.3.0.14.08/bin

Procedimento

- O utilitário de configuração é chamado **config**. Pode ser necessário configurar o coletor de dados com o utilitário de configuração completo nos seguintes casos:
  - O utilitário de configuração **simpleconfig** falha.
  - Você deseja configurar o monitoramento para instâncias do WebSphere Portal Server.
  - Você deseja especificar um alias de servidor que é exibido na interface com o usuário de monitoramento durante a configuração do coletor de dados.
  - Você deseja ter mais controle de quais dados serão coletados. Por exemplo, você deseja usar somente o monitoramento de recursos e desativar o rastreamento de dados diagnósticos e de transações.
  - Você não deseja configurar todos os servidores de aplicativos no mesmo perfil de uma vez.
  - O coletor de dados não está configurado no servidor de aplicativos e você deseja reconfigurá-lo.

  Para obter informações sobre o utilitário de configuração completo interativo, consulte "Configurando o coletor de dados interativamente" na página 840.
- O utilitário de reconfiguração é chamado **reconfig**. Talvez seja necessário reconfigurar o coletor de dados nos casos a seguir:
  - Você deseja reconfigurar o coletor de dados após ele ter sido configurado de forma interativa ou silenciosa.

  Para obter informações sobre o utilitário de reconfiguração interativo, consulte "Reconfigurando o coletor de dados interativamente" na página 845.
- Para configuração silenciosa, consulte "Configurando o Coletor de Dados no Modo Silencioso" na página 848.

Configurando o coletor de dados interativamente

Use o utilitário de configuração interativo (`config.sh` ou `config.bat`) para configurar o coletor de dados quando o utilitário `simpleconfig` falhar. É possível usar o utilitário `config.sh` ou `config.bat` para configurar o coletor de dados para cada instância do servidor de aplicativos que você deseja monitorar.

Antes de Iniciar

Se você for configurar o coletor de dados para monitorar o WebSphere Application Server Liberty, configure a variável de ambiente do sistema **JAVA_HOME** para a mesma JVM que a usada para o servidor de aplicativos. Por exemplo, em um sistema Windows, configure o valor **JAVA_HOME** como `C:\Program Files\IBM\java`. Ou em um sistema Linux, execute `export JAVA_HOME=/opt/IBM/java`.

Sobre Esta Tarefa

Use o seguinte utilitário de configuração completa para configurar o coletor de dados:

- Windows *install_dir*\dchome\7.3.0.14.08\bin\config.bat
- Linux AIX *install_dir*/yndchome/7.3.0.14.08/bin/config.sh

Procedimento

Para reconfigurar o coletor de dados respondendo aos prompts, conclua estas etapas:

1. Efetue login no sistema com o ID do usuário que é usado para instalar o servidor de aplicativos.
2. Acesse o diretório `bin` no diretório inicial do coletor de dados *dc_home*.
3. Inicie o utilitário de configuração, emitindo o seguinte comando:
   - Windows `config.bat`
   - Linux AIX `./config.sh`

   O utilitário de configuração exibe os endereços IP e os nomes de hosts de todas as placas de rede localizadas no sistema de computador local.
4. Insira o número que corresponde ao endereço IP e nome do host. Se o endereço IP e o nome do host que você deseja usar não estiverem na lista, insira o endereço IP ou o nome do host.
5. Especifique o diretório inicial do servidor de aplicativos que será monitorado.
   - Para o WebSphere Application Server traditional, insira o número que corresponde a um diretório inicial do servidor de aplicativos autodescoberto ou especifique um caminho completo para um diretório inicial do servidor de aplicativos.
   - Para o WebSphere Application Server Liberty, insira o caminho completo para o diretório inicial do WebSphere Application Server Liberty que contém os diretórios `bin` e `servers`, por exemplo, `/opt/ibm/wlp`.
6. Se estiver configurando o coletor de dados para o WebSphere Application Server Liberty, será solicitado o diretório inicial Java. Especifique o diretório inicial Java usado para o servidor de aplicativos. Por exemplo, `/opt/IBM/java`.
7. Quando o utilitário de configuração listar todos os perfis no diretório inicial do servidor de aplicativos, insira o número que corresponde ao perfil do servidor de aplicativos que você deseja configurar.
   - Para o WebSphere Application Server traditional, o utilitário de configuração indica então se a Segurança Global do WebSphere está ativada para o perfil do WebSphere Application Server especificado. Se a segurança global não estiver ativada, continue com a Etapa “9” na página 841.
   - Para o WebSphere Application Server Liberty, continue com a Etapa “10” na página 841.
8. Se a segurança global estiver ativada para o perfil do WebSphere Application Server, especifique se irá recuperar as configurações de segurança de um arquivo de propriedades do cliente. Insira 1 para permitir que o utilitário de configuração recupere o nome do usuário e a senha do arquivo de propriedades do cliente apropriado. Caso contrário, insira 2 para inserir o nome de usuário e a senha.

   O coletor de dados se comunica com o WebSphere Administrative Services usando a Chamada de Método Remoto (RMI) ou o protocolo SOAP. Se a segurança global estiver ativada para um perfil, é necessário especificar o ID do usuário e a senha de um usuário que está autorizado a efetuar login no console administrativo do WebSphere Application Server para o perfil do servidor de aplicativo. Como alternativa, é possível criptografar o nome de usuário e a senha e armazená-los nos arquivos de propriedades do cliente antes de configurar o coletor de dados. Você deve usar o arquivo `sas.client.props` para uma conexão RMI ou o arquivo `soap.client.props` para uma conexão SOAP.
9. Quando for solicitado o nome do host do console administrativo do WebSphere, pressione Enter para aceitar o padrão ou especifique o nome do host ou endereço IP do console administrativo do WebSphere. O valor padrão é `localhost`.

   Lembre-se: Para um ambiente do Network Deployment, insira o nome do host ou endereço IP do Deployment Manager.
10. Quando o utilitário de configuração listar todas as instâncias do servidor que ainda não estão configuradas para coleta de dados, selecione uma ou mais instâncias do servidor de aplicativos da lista. Insira o número que corresponde à instância do servidor de aplicativos para configurar para a coleta de dados ou insira um asterisco (`*`) para configurar todas as instâncias do servidor de aplicativos para coleta de dados. Para especificar um subconjunto de servidores, insira os números, separados por vírgulas, que representam os servidores.
    Por exemplo, `1,2,3`.

    Lembre-se:

- Para um ambiente independente, as instâncias do servidor de aplicativos devem estar em execução durante a configuração. (Uma instância do WebSphere Application Server Liberty não precisa estar em execução).
- Para um ambiente do Network Deployment, o Deployment Manager deve estar em execução.
- Assegure-se de que as instâncias do servidor de aplicativos que você selecionar sejam os servidores reais que hospedam os aplicativos ou serviços que deseja monitorar.

11. Na seção **Integração com o Agent for WebSphere Applications**, especifique que você deseja integrar o coletor de dados com o WebSphere Applications agent. Deve-se inserir 1 para selecionar essa opção de integração e pressionar Enter.

    O servidor selecionado será registrado para o monitoramento de recurso PMI.

12. Se estiver configurando o coletor de dados para o WebSphere Application Server traditional, especifique se deseja configurar o coletor de dados na instância do servidor de aplicativos.

    - Insira 1 para configurar o coletor de dados no servidor de aplicativos. Com essa opção, o coletor de dados é integrado com o servidor de aplicativos, o que é necessário para o intervalo completo de monitoramento operacional e coleta de dados diagnósticos. No entanto, configurar o coletor de dados no servidor de aplicativos requer a reinicialização do servidor de aplicativos. Além disso, o coletor de dados pode afetar o desempenho do servidor.
    - Insira 2 para não configurar o coletor de dados no servidor de aplicativos e continuar com a Etapa “14” na página 842. Com essa opção, o coletor de dados é executado como um processo independente e somente o monitoramento de recursos pode ser ativado.

13. Quando solicitado, especifique se deseja ativar o coletor de dados para dados diagnósticos. Insira 1 para ativar a coleta de dados diagnósticos. O padrão é 2.
14. Quando for solicitado o nome do host do agente de monitoramento V8, insira o nome do host ou endereço IP do WebSphere Applications agent ou pressione Enter para aceitar o padrão. O valor padrão corresponde à sua opção na Etapa 3.

    O agente de monitoramento V8 se refere ao WebSphere Applications agent, que é instalado com o IBM Cloud Application Performance Management.

15. Quando for solicitado o número da porta do agente de monitoramento V8, insira o número da porta do WebSphere Applications agent ou pressione Enter para aceitar o padrão. O padrão é 63335.
16. Quando for perguntado se deseja configurar o agente de monitoramento V6 para Aplicativos WebSphere, pressione Enter para aceitar o padrão para Não.

    O agente de monitoramento V6 se refere ao ITCAM Agent for WebSphere Applications, que é instalado na antiga infraestrutura do IBM® Tivoli® Monitoring. A configuração do agente de monitoramento V6 é necessária somente para o ambiente de coexistência do agente.

17. Quando for solicitado que você forneça o alias de servidor, pressione Enter para aceitar o padrão ou insira outro alias. Se você estiver configurando várias instâncias do servidor de aplicativos, o utilitário de configuração solicitará um alias para cada instância.

    Importante: O alias pode conter somente os seguintes caracteres: `A-Z`, `a-z`, sublinhado (`_`), traço (`-`) e ponto (`.`). Não use outros caracteres no alias.

    O alias de servidor é o primeiro qualificador do nome da instância de agente (também conhecido como MSN) que é exibido no Console do Cloud APM. O padrão é o nome do nó combinado com o nome do servidor. Por exemplo, o alias **node1server1** indica o servidor denominado **server1** no nó denominado **node1**.

18. Quando for solicitado um número da porta para o monitoramento de recursos de PMI, pressione Enter para aceitar o padrão ou insira um novo número. A porta padrão é 63355.

    Esta porta é usada para comunicação interna entre componentes que estão em execução no mesmo host. Se o padrão estiver em uso, é possível configurar um número diferente.

19. Na seção **Suporte para rastreamento de transação**, especifique se deve ativar o rastreamento de transação. Insira 1 para ativar o suporte para o rastreamento de transações. Caso contrário, insira 2 e vá para a Etapa “22” na página 843.

20. Quando for solicitado o nome do host ou endereço IP do Transaction Framework Extension, pressione Enter para aceitar o padrão ou insira outro nome do host ou endereço IP.

    O Transaction Framework Extension é um componente interno do WebSphere Applications agent que reúne métricas do coletor de dados.
21. Quando for solicitado o número da porta que o coletor de dados usa para se conectar ao Transaction Framework Extension, pressione Enter para aceitar o padrão ou insira outro número de porta. O padrão é 5457.
22. Especifique se deseja integrar o coletor de dados ao Application Performance Diagnostics Lite. Pressione Enter para aceitar o padrão para não.
23. Na seção **Configurações avançadas**, verifique se deseja mudar o caminho de log da coleta de lixo. Insira 1 para selecionar um caminho de log da coleta de lixo. Caso contrário, insira 2 e vá para a Etapa "25" na página 843. Para usar o caminho de log que já está especificado no argumento da JVM do servidor de aplicativos, insira 2.
24. Especifique o caminho de log da coleta de lixo. Insira um nome de arquivo com seu caminho completo. Para o WebSphere Application Server Liberty, não use as variáveis no caminho. O coletor de dados automaticamente modifica o nome do arquivo de log, incluindo nele as informações da instância do servidor.

    Por exemplo, se você especificar `gc.log` como o nome do arquivo, o nome atual será configurado como *`profile_name.cell_name.node_name.server_name`*`.gc.log` para cada instância do servidor de aplicativos configurada.

    Importante: No caminho de log da coleta de lixo, é possível usar variáveis do WebSphere, tais como `${SERVER_LOG_ROOT}`. Entretanto, não use modelos, tais como `%pid`.
25. Revise o resumo da configuração do coletor de dados que deve ser aplicado às instâncias do servidor de aplicativos especificado. Se necessário, reconfigure partes da configuração do coletor de dados antes de aplicar as mudanças.
26. Insira a para aceitar suas mudanças.
27. Quando solicitado, especifique se deseja criar um backup de sua configuração atual. Insira 1 para criar um backup da configuração atual. Caso contrário, insira 2.

    O utilitário de configuração aplica as mudanças e apresenta uma mensagem de status para indicar que a configuração do coletor de dados para o perfil foi concluída.
28. Se estiver configurando o coletor de dados para o WebSphere Application Server traditional, reinicie as instâncias do servidor de aplicativos ou reinicie o agente, dependendo de sua opção na Etapa "12" na página 842.
    - Se você ativou o coletor de dados no servidor de aplicativos, reinicie as instâncias do servidor de aplicativos, conforme indicado pelo utilitário de configuração.
    - Se você ativou o monitoramento de recursos de PMI sem ativar o coletor de dados no servidor de aplicativos, reinicie o WebSphere Applications agent executando os seguintes comandos:
      – Windows

      ```
      cd install_dir\bin
      was-agent.bat stop
      was-agent.bat start
      ```

      – Linux AIX

      ```
      cd install_dir/bin
      ./was-agent.sh stop
      ./was-agent.sh start
      ```

    A configuração do coletor de dados entra em vigor após a reinicialização do servidor de aplicativos ou do agente.
29. Efetue login no Console do Cloud APM para visualizar dados nos painéis.

a) Acesse o console usando o link fornecido no e-mail que alerta que seu serviço está pronto. Como alternativa, acesse o console a partir do website do IBM Marketplace. Para obter instruções detalhadas, consulte "Iniciando o Console do Cloud APM" na página 975.

b) Use o Editor de aplicativos para incluir o servidor de aplicativos monitorado no Application Performance Dashboard. É possível incluí-lo como um novo componente para seu aplicativo existente ou criar um aplicativo para conter esse componente.

Para obter informações adicionais sobre o Editor de aplicativos, consulte "Gerenciando aplicativos" na página 1098.

O que Fazer Depois

- Se o ID do usuário atual que é usado para configurar o coletor de dados não for o mesmo ID do usuário que está executando o servidor de aplicativos, verifique se o ID do usuário para configurar o coletor de dados tem permissões de leitura e gravação nos diretórios `runtime` e `logs` no diretório inicial do coletor de dados. Esses dois subdiretórios são criados pelo ID do usuário que está executando o servidor de aplicativos quando o servidor é reiniciado.
- Efetue login no Console do Cloud APM para visualizar os dados de monitoramento nos painéis. Se os dados de monitoramento não estiverem disponíveis imediatamente, reinicie o WebSphere Applications agent executando os seguintes comandos:
  - Windows

```
cd install_dir\bin
was-agent.bat stop
was-agent.bat start
```

  - Linux AIX

```
cd install_dir/bin
./was-agent.sh stop
./was-agent.sh start
```

- A mudança do alias de servidor muda o nome da instância de agente registrado com Console do Cloud APM. Se essa não for a primeira vez que você configura o coletor de dados e se você mudou o alias de servidor, deverá limpar alguns arquivos de cache concluindo as seguintes etapas:
  1. Pare o agente de monitoramento se ele estiver em execução.
  2. Abra o arquivo *hostname*_yn.xml no diretório a seguir com um editor de texto, em que *hostname* é o nome do host onde o WebSphere Applications agent está instalado.
     - Windows *install_dir*\TMAITM6_x64 (O padrão é C:\IBM\APM\TMAITM6_x64)
     - Linux AIX *install_dir*/config (O padrão é /opt/ibm/apm/agent/config)
  3. Localize a linha que começa com a seguinte sequência e que contém o nome do servidor anterior. Por exemplo, `was85.win4net01Cell02.win4net01Node02.AppSrv01.server1`, em que `server1` é o nome anterior do servidor de aplicativos.

     ```
     <!ENTITY was_product_code.cellname.nodename.profilename.servername
     ```

     em que *was_product_code* é o código do produto do WebSphere Application Server; *cellname* é o nome da célula; *nodename* é o nome do nó; *profilename* é o nome do perfil do servidor de aplicativos; *servername* é o nome anterior do servidor de aplicativos.
  4. Localize o arquivo .XML indicado na linha no diretório atual e exclua o arquivo.
  5. Remova a linha que você localizou na Etapa 3 do arquivo *hostname*_yn.xml.
  6. No final do arquivo *hostname*_yn.xml, remova a linha que contém os nomes de servidores anteriores.
  7. Salve e feche o arquivo.
  8. Reinicie o agente de monitoramento.

Reconfigurando o coletor de dados interativamente
Se você configurou o coletor de dados para monitorar uma ou mais instâncias do servidor de aplicativos, é possível reconfigurar o coletor de dados usando o utilitário de reconfiguração (`reconfig.sh` ou `reconfig.bat`).

Antes de Iniciar

Se você for configurar o coletor de dados para monitorar o WebSphere Application Server Liberty, configure a variável de ambiente do sistema **JAVA_HOME** para a mesma JVM que a usada para o servidor de aplicativos. Por exemplo, em um sistema Windows, configure o valor **JAVA_HOME** como `C:\Program Files\IBM\java`. Ou em um sistema Linux, execute `export JAVA_HOME=/opt/IBM/java`.

Sobre Esta Tarefa

Use o seguinte utilitário de reconfiguração completa para configurar o coletor de dados:

- Windows *install_dir*`\dchome\7.3.0.14.08\bin\reconfig.bat`
- Linux AIX *install_dir*`/yndchome/7.3.0.14.08/bin/reconfig.sh`

Lembre-se: O utilitário **reconfig** não é aplicável nos seguintes casos. Use o utilitário de configuração **config** no lugar. Embora o utilitário **config** avise que o servidor já está configurado, ainda é possível fazer qualquer mudança necessária.

- O coletor de dados já está configurado somente para monitoramento de recursos e você deseja reconfigurar o coletor de dados.
- Você deseja reconfigurar o coletor de dados para o WebSphere Portal Server.

Dica: Nos prompts solicitando definições de configuração do agente, o aviso de reconfiguração oferece os valores atualmente configurados como padrões.

Procedimento

Para reconfigurar o coletor de dados respondendo aos prompts, conclua estas etapas:

1. Efetue login no sistema com o ID do usuário que é usado para instalar o servidor de aplicativos.
2. Acesse o diretório `bin` no diretório inicial do coletor de dados *dc_home*.
3. Inicie o utilitário de reconfiguração emitindo o seguinte comando:
   - Windows `reconfig.bat`
   - Linux AIX `./reconfig.sh`

   Dica: A execução desse utilitário de reconfiguração tem o mesmo efeito que executar o script `config.bat` com o argumento `-reconfig` nos sistemas Windows ou o script `config.sh` com o argumento `-reconfig` nos sistemas Linux ou AIX.

   O utilitário de reconfiguração exibe os endereços IP de todas as placas de rede localizadas no sistema de computador local.
4. Insira o número que corresponde ao endereço IP a usar.

   O utilitário de reconfiguração exibe todas as instâncias do servidor de aplicativos para as quais o coletor de dados está configurado nesse host e solicita a seleção de uma ou mais instâncias de servidor da lista.
5. Selecione uma ou mais instâncias do servidor de aplicativos a partir da lista. Insira o número que corresponde à instância do servidor de aplicativos para reconfigurar para coleta de dados ou insira um asterisco (`*`) para reconfigurar todas as instâncias do servidor de aplicativos para coleta de dados. Para especificar um subconjunto de servidores, insira os números, separados por vírgulas, que representam os servidores. Por exemplo: `1,2,3`.

   Lembre-se:

- Para um ambiente independente, as instâncias do servidor de aplicativos devem estar em execução durante a configuração. (Uma instância do WebSphere Application Server Liberty não precisa estar em execução).
- Para um ambiente do Network Deployment, o Deployment Manager deve estar em execução.
- Assegure-se de que as instâncias do servidor de aplicativos que você selecionar sejam os servidores reais que hospedam os aplicativos ou serviços que deseja monitorar.

6. Na seção **Integração com o Agent for WebSphere Applications**, especifique que você deseja integrar o coletor de dados com o WebSphere Applications agent. Deve-se inserir 1 para selecionar essa opção de integração e pressionar Enter.
7. Se estiver configurando o coletor de dados para o WebSphere Application Server traditional, especifique se deseja configurar o coletor de dados na instância do servidor de aplicativos.
   - Insira 1 para configurar o coletor de dados no servidor de aplicativos. Com essa opção, o coletor de dados é integrado com o servidor de aplicativos, o que é necessário para o intervalo completo de monitoramento operacional e coleta de dados diagnósticos. No entanto, configurar o coletor de dados no servidor de aplicativos requer a reinicialização do servidor de aplicativos. Além disso, o coletor de dados pode afetar o desempenho do servidor.
   - Insira 2 para não configurar o coletor de dados no servidor de aplicativos e prosseguir para a Etapa “9” na página 846. Com essa opção, o coletor de dados é executado como um processo independente e somente o monitoramento de recursos de PMI pode ser ativado.
8. Quando solicitado, especifique se deseja ativar a coleta de dados diagnósticos para o coletor de dados. Insira 1 para sim ou 2 para não.
9. Quando solicitado o nome do host, insira o nome do host ou endereço IP do WebSphere Applications agent ou pressione Enter para aceitar o padrão. O valor padrão corresponde à sua opção na Etapa “4” na página 845.
10. Quando solicitado o número da porta, insira o número da porta do agente de monitoramento ou pressione Enter para aceitar o padrão. O padrão é 63335.
11. Quando for perguntado se deseja configurar o agente de monitoramento V6 para Aplicativos WebSphere, pressione Enter para aceitar o padrão para Não.

    O agente de monitoramento V6 se refere ao ITCAM Agent for WebSphere Applications, que é instalado na antiga infraestrutura do IBM® Tivoli® Monitoring. A configuração do agente de monitoramento V6 é necessária somente para o ambiente de coexistência do agente.
12. Quando for solicitado que você forneça o alias de servidor, pressione Enter para aceitar o padrão ou insira outro alias. Se você estiver configurando várias instâncias do servidor de aplicativos, o utilitário de configuração solicitará um alias para cada instância.

    Importante: O alias pode conter somente os seguintes caracteres: `A-Z`, `a-z`, sublinhado (`_`), traço (`-`) e ponto (`.`). Não use outros caracteres no alias.

    O alias de servidor é o primeiro qualificador do nome da instância de agente (também conhecido como MSN) que é exibido no Console do Cloud APM. O padrão é o nome do nó combinado com o nome do servidor. Por exemplo, o alias **node1server1** indica o servidor denominado **server1** no nó denominado **node1**.
13. Quando for solicitado um número da porta para o monitoramento de recursos de PMI, pressione Enter para aceitar o padrão ou insira um novo número. A porta padrão é 63355.

    Esta porta é usada para comunicação interna entre componentes que estão em execução no mesmo host. Se o padrão estiver em uso, é possível configurar um número diferente.
14. Na seção **Suporte para rastreamento de transação**, especifique se deve ativar o rastreamento de transação. Insira 1 para ativar o suporte para o rastreamento de transações. Caso contrário, insira 2 e vá para a Etapa “17” na página 847.
15. Quando for solicitado o nome do host ou endereço IP do Transaction Framework Extension, pressione Enter para aceitar o padrão ou insira outro nome do host ou endereço IP.

    O Transaction Framework Extension é um componente interno do WebSphere Applications agent que reúne métricas do coletor de dados.

16. Quando for solicitado o número da porta que o coletor de dados usa para se conectar ao Transaction Framework Extension, pressione Enter para aceitar o padrão ou insira outro número de porta. O padrão é 5457.
17. Especifique se deseja integrar o coletor de dados ao Application Performance Diagnostics Lite. Pressione Enter para aceitar o padrão para Não.
18. Na seção **Configurações avançadas**, verifique se deseja mudar o caminho de log da coleta de lixo.

    Insira 1 para selecionar um caminho de log da coleta de lixo. Caso contrário, insira 2 e vá para a Etapa "20" na página 847. Para usar o caminho de log que já está especificado no argumento da JVM do servidor de aplicativos, insira 2.
19. Especifique o caminho de log da coleta de lixo. Insira um nome de arquivo com seu caminho completo. Para o WebSphere Application Server Liberty, não use as variáveis no caminho. O coletor de dados automaticamente modifica o nome do arquivo de log, incluindo nele as informações da instância do servidor.

    Por exemplo, se você especificar `gc.log` como o nome do arquivo, o nome atual será configurado como *`profile_name`*`.`*`cell_name`*`.`*`node_name`*`.`*`server_name`*`.gc.log` para cada instância do servidor de aplicativos configurada.

    Importante: No caminho de log da coleta de lixo, é possível usar variáveis do WebSphere, tais como `${SERVER_LOG_ROOT}`. Entretanto, não use modelos, tais como `%pid`.
20. Revise o resumo da configuração do coletor de dados que deve ser aplicado às instâncias do servidor de aplicativos especificado. Reconfigure partes da configuração do coletor de dados antes de aplicar as mudanças, se necessário.
21. Insira a para aceitar suas mudanças.
22. Quando solicitado, especifique se deseja criar um backup de sua configuração atual. Insira 1 para criar um backup da configuração atual. Caso contrário, insira 2.

    O utilitário de configuração aplica as mudanças e apresenta uma mensagem de status para indicar que a configuração do coletor de dados para o perfil foi concluída.
23. Se estiver configurando o coletor de dados para o WebSphere Application Server traditional, reinicie as instâncias do servidor de aplicativos ou reinicie o agente, dependendo de sua opção na Etapa "7" na página 846.

    - Se você ativou o coletor de dados no servidor de aplicativos, reinicie as instâncias do servidor de aplicativos, conforme indicado pelo utilitário de configuração.
    - Se você ativou o monitoramento de recursos de PMI sem ativar o coletor de dados no servidor de aplicativos, reinicie o WebSphere Applications agent executando os seguintes comandos:
      - Windows

        ```
        cd install_dir\bin
        was-agent.bat stop
        was-agent.bat start
        ```
      - Linux AIX

        ```
        cd install_dir/bin
        ./was-agent.sh stop
        ./was-agent.sh start
        ```

    A configuração do coletor de dados entra em vigor após a reinicialização do servidor de aplicativos ou do agente.

O que Fazer Depois

- A mudança do alias de servidor muda o nome da instância de agente registrado com Console do Cloud APM. Se você mudou o alias de servidor durante o procedimento de reconfiguração, deverá limpar alguns arquivos de cache concluindo as seguintes etapas:

  1. Pare o agente de monitoramento se ele estiver em execução.

2. Abra o arquivo *hostname*_yn.xml no diretório a seguir com um editor de texto, em que *hostname* é o nome do host onde o WebSphere Applications agent está instalado.
   - Windows *install_dir*\TMAITM6_x64 (O padrão é C:\IBM\APM\TMAITM6_x64)
   - Linux AIX *install_dir*/config (O padrão é /opt/ibm/apm/agent/config)
3. Localize a linha que começa com a seguinte sequência e que contém o nome do servidor anterior. Por exemplo, was85.win4net01Cell02.win4net01Node02.AppSrv01.server1, em que server1 é o nome anterior do servidor de aplicativos.

   ```
   <!ENTITY was_product_code.cellname.nodename.profilename.servername
   ```

   em que *was_product_code* é o código do produto do WebSphere Application Server; *cellname* é o nome da célula; *nodename* é o nome do nó; *profilename* é o nome do perfil do servidor de aplicativos; *servername* é o nome anterior do servidor de aplicativos.
4. Localize o arquivo .XML indicado na linha no diretório atual e exclua o arquivo.
5. Remova a linha que você localizou na Etapa 3 do arquivo *hostname*_yn.xml.
6. No final do arquivo *hostname*_yn.xml, remova a linha que contém os nomes de servidores anteriores.
7. Salve e feche o arquivo.
8. Reinicie o agente de monitoramento.

Configurando o Coletor de Dados no Modo Silencioso

Se você desejar configurar diversas instâncias do servidor de aplicativos, talvez seja mais conveniente configurar o coletor de dados no modo silencioso.

Sobre Esta Tarefa

Ao configurar o coletor de dados no modo silencioso, é necessário primeiro especificar as opções de configuração em um arquivo de propriedades. Um arquivo de propriedades de amostra, sample_silent_config.txt, é empacotado com o utilitário de configuração. O arquivo está disponível nos diretórios a seguir, em que *dc_home* é o diretório no qual o coletor de dados está instalado. Para obter o caminho completo do diretório *dc_home*, consulte a introdução em Configurando o coletor de dados para o agente de aplicativos WebSphere.

- Windows *dc_home*\bin
- Linux AIX *dc_home*/bin

Para obter informações detalhadas sobre cada propriedade de configuração disponível nesse arquivo, consulte “Arquivo de propriedades para configuração silenciosa de coletor de dados” na página 849.

Procedimento

Conclua as etapas a seguir para executar uma configuração silenciosa:

1. Especifique as opções de configuração no arquivo de propriedades. É possível copiar o arquivo de propriedades de amostra e alterar as opções necessárias.
2. Configure o local do diretório inicial Java antes de executar o utilitário.
   Por exemplo:
   - Windows

     ```
     set JAVA_HOME=C:\Program Files\IBM\WebSphere\AppServer80\java
     ```
   - Linux AIX

     ```
     export JAVA_HOME=/opt/IBM/AppServer80/java
     ```

Importante: Se o monitoramento do WebSphere Application Server Liberty estiver sendo configurado, você deve usar a mesma versão JVM que a usada pelo servidor do aplicativo. Caso contrário, o monitoramento pode falhar.

3. Acesse o diretório a seguir:
   - Windows *dc_home*\bin
   - Linux AIX *dc_home*/bin
4. Execute o comando para configurar o coletor de dados no modo silencioso.
   - Windows Execute o comando a seguir como o administrador que instalou o WebSphere Application Server.

     ```
     config.bat -silent [dir_path]\silent file
     ```

   - Linux AIX Execute o comando a seguir com privilégios de usuário raiz.

     ```
     config.sh -silent [dir_path]/silent file
     ```

   Dica: Se o usuário `wsadmin` tiver sido usado para instalar o servidor de aplicativos, execute o utilitário `config` como o usuário `wsadmin` ou com privilégios de usuário raiz.
5. Depois de configurar o coletor de dados para monitorar instâncias do servidor de aplicativos, se você tiver ativado o coletor de dados no servidor de aplicativos, deverá reiniciar as instâncias. A configuração do coletor de dados entra em vigor quando as instâncias do servidor de aplicativos são reiniciadas.
6. Se você ativou o monitoramento de recursos de PMI sem ativar o coletor de dados no servidor de aplicativos, pode ser necessário reiniciar o WebSphere Applications agent para iniciar o monitoramento. Se os dados de monitoramento não estiverem disponíveis imediatamente, reinicie o agente de monitoramento executando os comandos a seguir:
   - Windows

     ```
     cd install_dir\bin
     was-agent.bat stop
     was-agent.bat start
     ```

   - Linux AIX

     ```
     cd install_dir/bin
     ./was-agent.sh stop
     ./was-agent.sh start
     ```

O que Fazer Depois

Após a configuração silenciosa, para reconfigurar o coletor de dados, você tem duas opções:

- Reconfigure-o interativamente usando o utilitário de reconfiguração **reconfig**. Para obter instruções, veja “Reconfigurando o coletor de dados interativamente” na página 845.
- Desconfigure-o silenciosamente e, em seguida, use o mesmo procedimento para configurá-lo silenciosamente outra vez. Para obter instruções, veja “Removendo a Configuração do Coletor de Dados no Modo Silencioso” na página 147.

Referências relacionadas

“Arquivo de propriedades para configuração silenciosa de coletor de dados” na página 849
Para configurar silenciosamente o coletor de dados, primeiro você especifica opções de configuração em um arquivo de propriedades e, em seguida, executa o utilitário de configuração.

Arquivo de propriedades para configuração silenciosa de coletor de dados

Para configurar silenciosamente o coletor de dados, primeiro você especifica opções de configuração em um arquivo de propriedades e, em seguida, executa o utilitário de configuração.

Ao criar seu arquivo de propriedades, tenha em mente as seguintes considerações:

- Uma linha no arquivo que inicia com um sinal de número (#) é tratado como um comentário e não é processada. Se o sinal de número é usado em qualquer lugar na linha, ele não é considerado com o início de um comentário.
- Cada propriedade é descrita em uma linha separada, no seguinte formato: *property* = *value*.

  property
  Nome da propriedade. A lista de propriedades válidas que é possível configurar é mostrada na Tabela 223 na página 850.

  value
  Valor da propriedade. Os valores padrão para algumas propriedades já foram fornecidos. É possível excluir valores padrão para deixar valores de propriedade em branco ou vazios. Um valor vazio será tratado como se a propriedade não tivesse sido especificada, em vez de usar o valor padrão. Se você desejar usar valores padrão, é possível comentar a linha da propriedade no arquivo.
- As senhas estão em texto simples.
- As propriedades e seus valores fazem distinção entre maiúsculas e minúsculas.

Tabela 223 na página 850 descreve as propriedades que estão disponíveis ao configurar o coletor de dados no modo silencioso.

Importante: Se você estiver configurando o coletor de dados para uma instância do WebSphere Application Server Liberty, algumas das propriedades não são usadas.

Tabela 223. Propriedades Disponíveis para Executar o Utilitário de Configuração no Modo Silencioso

Propriedade	**Comentário**
default.hostip	Se o sistema de computador usa diversos endereços IP, especifique o endereço IP para o coletor de dados a usar.
Integração do coletor de dados com o ITCAM for Application Diagnostics Managing Server **Importante:** O Managing Server está disponível somente se você tiver o ITCAM for Application Diagnostics. Para uma instância do WebSphere Application Server Liberty ou em um ambiente Cloud APM, essas propriedades não são usadas.	
ms.connect	Especifica se o coletor de dados está configurado para se conectar ao servidor de gerenciamento em um ambiente do ITCAM for Application Diagnostics. Os valores válidos são `True` e `False`.
ms.kernel.host	Especifica o nome completo do host do servidor de gerenciamento.
ms.kernel.codebase.port	Especifica a porta do código base no qual o servidor de gerenciamento está atendendo.
ms.am.home	Especifica o diretório inicial do servidor de gerenciamento.
ms.am.socket.bindip	Especifica o endereço IP ou nome do host a ser usado pelo coletor de dados para se comunicar com o servidor de gerenciamento. Se mais de uma interface de rede ou endereço IP for configurado no sistema de computador do coletor de dados, escolha um deles.
ms.probe.controller.rmi.port	Se o coletor de dados estiver atrás de um firewall ou se você tiver requisitos especiais para alterar a porta RMI do Controlador do coletor de dados, configure esse intervalo de números da porta. Configure esse número de porta conforme permitido pelo firewall para o host do coletor de dados. Por exemplo: `ms.probe.controller.rmi.port=8300-8399` ou ms.probe.controller.rmi.port=8300.

Tabela 223. Propriedades Disponíveis para Executar o Utilitário de Configuração no Modo Silencioso (continuação)

Propriedade	Comentário
ms.probe.rmi.port	Se o coletor de dados estiver atrás de um firewall ou se você tiver requisitos especiais para alterar a porta RMI do coletor de dados, configure este intervalo de números de porta. Configure esse número de porta conforme permitido pelo firewall para o host do coletor de dados. Por exemplo: `ms.probe.rmi.port=8200-8299` ou `ms.probe.rmi.port=8200`.
Suporte para rastreamento de transações Para visualizar informações de rastreamento de transação, deve-se ter visualizações de topologia disponíveis no Console do Cloud APM e ativar o rastreamento de transação na janela Configuração do Agente.	
ttapi.enable	Especifica se o coletor de dados suporta o rastreamento de transações. Os valores válidos são `True` e `False`.
ttapi.host	Especifica o host do Transaction Framework Extension, que é o componente do Agente de Monitoramento para WebSphere Applications que reúne métricas do coletor de dados. Use o valor de host local, `127.0.0.1`.
ttapi.port	Especifica a porta do Transaction Framework Extension. Use 5457.
Integração do coletor de dados com o ITCAM for SOA **Importante:** Para uma instância do WebSphere Application Server Liberty ou em um ambiente Cloud APM, essa propriedade não é usada.	
soa.enable	Especifica se você deseja integrar o coletor de dados com o ITCAM para SOA. O agente ITCAM para SOA deve estar instalado para concluir a configuração.
Integração do coletor de dados com o Tivoli Performance Monitoring **Importante:** Para uma instância do WebSphere Application Server Liberty ou em um ambiente Cloud APM, essa propriedade não é usada.	
tpv.enable	Especifica se você deseja integrar o coletor de dados com o Tivoli Performance Monitoring quando o coletor de dados está incluído como parte do ITCAM for WebSphere Application Server versão 8.5. O Tivoli Performance Monitoring é acessado com o console administrativo do WebSphere Application Server. Os valores válidos são *True* e *False*.
Integração do coletor de dados com Application Performance Diagnostics Lite **Importante:** Para uma instância do WebSphere Application Server Liberty, esta propriedade não é usada.	

Tabela 223. Propriedades Disponíveis para Executar o Utilitário de Configuração no Modo Silencioso (continuação)

Propriedade	Comentário
de.enable	Especifica se deve coletar os dados diagnósticos, necessários para Application Performance Diagnostics e Application Performance Diagnostics Lite. Os valores válidos são `True` e `False`. Ative essa integração se você tiver o Application Diagnostics ou puder tê-lo no futuro. Neste caso, a coleta de dados diagnósticos é ativada na inicialização do servidor. Caso contrário, ele é desativado na inicialização; é possível ativá-lo usando a página Configuração do Agente na interface com o usuário, mas se o servidor for reiniciado, a coleta de dados diagnósticos é desativada novamente. Essa configuração também permite a integração com o Application Performance Diagnostics Lite, que é a ferramenta para investigação de diagnóstico dos aplicativos em execução no WebSphere Application Server e WebSphere Portal Server. Usando esta ferramenta, é possível analisar dados em tempo real ou salvar informações de diagnóstico em um arquivo para análise posterior.
Monitoramento de recurso PMI e do coletor de dados O servidor selecionado é sempre configurado para monitoramento de recurso (PMI), sem quaisquer mudanças no servidor de aplicativos. Esta opção de monitoramento fornece métricas limitadas e funciona somente com o WebSphere Applications agent, mas não requer a reinicialização do servidor de aplicativos e não pode afetar o desempenho.	
tema.appserver	Especifica se você deseja configurar o coletor de dados dentro da instância do servidor de aplicativos. O coletor de dados dentro da instância do servidor de aplicativos é necessário para o intervalo completo de métricas no WebSphere Applications agent e para integração com quaisquer outros produtos. Entretanto, a configuração do coletor de dados requer o reinício do servidor de aplicativos. Além disso, o coletor de dados pode afetar o desempenho do servidor. Os valores válidos são `True` e `False`. Se esse parâmetro estiver configurado para `False`, os parâmetros de configuração do coletor de dados para integração com produtos além do WebSphere Applications agent serão desconsiderados. Quando este parâmetro está configurado para `False`, recursos de diagnósticos e de rastreamento de transação não estão disponíveis e somente dados de monitoramente de recurso são coletados.
tema.jmxport	Número da porta TCP/IP para monitoramento de recurso. A porta é usada para comunicação interna entre componentes em execução no mesmo host. A porta padrão é `63355`; se esta porta estiver em uso, é possível configurar um número diferente.
Integração do coletor de dados com o componente de agente de monitoramento do WebSphere Applications agent e com o Application Performance Diagnostics Lite	
temaconnect	Especifica se o coletor de dados se conecta ao componente de agente de monitoramento do WebSphere Applications agent. Os valores válidos são `True` e `False`. **Importante:** Deve-se usar o valor `True` para usar o WebSphere Applications agent.

Tabela 223. Propriedades Disponíveis para Executar o Utilitário de Configuração no Modo Silencioso (continuação)

Propriedade	Comentário
tema.appserver	Especifica se você deseja configurar o coletor de dados dentro da instância do servidor de aplicativos. O coletor de dados dentro da instância do servidor de aplicativos é necessário para o intervalo completo de métricas no WebSphere Applications agent e para integração com quaisquer outros produtos. No entanto, ela requer a reinicialização do servidor de aplicativos. Além disso, o coletor de dados pode afetar o desempenho do servidor. Os valores válidos são `True` e `False`. Se esse parâmetro estiver configurado para `False`, os parâmetros de configuração para integração do coletor de dados com outros que não o WebSphere Applications agent serão ignorados, bem como os parâmetros tema.host e tema.port a seguir. Quando este parâmetro está configurado para `False`, recursos de diagnósticos e de rastreamento de transação não estão disponíveis e somente dados de monitoramente de recurso são coletados.
tema.host	Especifica o nome completo do host ou o endereço IP do componente do agente de monitoramento do WebSphere Applications agent. Use o endereço do host local (127.0.0.1).
tema.port	Especifica o número da porta do componente do agente de monitoramento do WebSphere Applications agent. Não altere o valor padrão de 63335.
tema.jmxport	Número da porta TCP/IP para monitoramento de recurso. A porta é usada para comunicação interna entre componentes em execução no mesmo host. A porta padrão é 63355; se esta porta estiver em uso, é possível configurar um número diferente.
Integração do coletor de dados com o ITCAM Agent for WebSphere Applications versão 6 Use as propriedades a seguir para configurar um coletor de dados para coletar dados para WebSphere Applications agent e ITCAM Agent for WebSphere Applications versão 6.	
config.tema.v6	Especifica se você deve integrar o coletor de dados ao componente do agente de monitoramento do ITCAM Agent for WebSphere Applications versão 6. Os valores válidos são `True` e `False`. O padrão é `False`.
tema.host.v6	Especifica se você deve integrar o coletor de dados ao componente do agente de monitoramento do ITCAM Agent for WebSphere Applications versão 6. Os valores válidos são `True` e `False`. O padrão é `False`.
tema.port.v6	Especifica o número da porta do componente do agente de monitoramento do ITCAM Agent for WebSphere Applications versão 6. Não mude o valor padrão 63336.
Backup do WebSphere Application Server	
was.backup.configuration	Especifica se você deseja fazer backup da configuração atual do WebSphere Application Server antes de aplicar a nova configuração. Os valores válidos são `True` e `False`.
was.backup.configuration.dir	Especifica o local do diretório de backup.
Definições de configuração avançadas	

Tabela 223. Propriedades Disponíveis para Executar o Utilitário de Configuração no Modo Silencioso (continuação)

Propriedade	Comentário
was.gc.custom.path	Especifica se você deseja configurar um caminho customizado para o log de Coleta de Lixo.
was.gc.file	Especifica o caminho para o log de Coleta de Lixo customizado. Configure este valor como um nome de arquivo com seu caminho completo. O coletor de dados automaticamente modifica o nome do arquivo de log, incluindo nele as informações da instância do servidor. Por exemplo, se você especificar `gc.log` como o nome do arquivo, o nome atual será configurado como *`profile_name.cell_name.node_name.server_name`*`.gc.log` para cada instância do servidor de aplicativos configurada. **Importante:** No caminho de log de Coleta de Lixo, é possível usar variáveis do WebSphere, tais como `${SERVER_LOG_ROOT}`. Entretanto, não use modelos, tais como %pid.
Configurações de conexão do WebSphere Administrative Services	
was.wsadmin.connection.host	Especifica o nome do host ao qual a ferramenta wsadmin está se conectando. Em um ambiente de Implementação de Rede, especifique a conexão wsadmin com o Gerenciador de Implementação. Em um ambiente independente, especifique a conexão wsadmin com o servidor. **Lembre-se:** Se o console administrativo do WebSphere estiver no mesmo sistema, o valor de `localhost` será usado para conexão. No entanto, em alguns casos, `localhost` não é permitido para comunicação devido às configurações de rede e de segurança do sistema. Nesse caso, esse parâmetro deve ser especificado no arquivo de resposta silencioso.
was.wsadmin.connection.type	Especifica a porta que a ferramenta wsadmin deve usar para se conectar ao WebSphere Application Server.
was.wsadmin.connection.port	Especifica a porta que a ferramenta wsadmin deve usar para se conectar ao WebSphere Application Server.
Configurações de segurança global do WebSphere Application Server	
was.wsadmin.username	Especifica o ID de um usuário que está autorizado a efetuar login no console administrativo do IBM WebSphere Application Server. Esse usuário deve ter a função de agente no servidor de aplicativos.
was.wsadmin.password	Especifica a senha que corresponde ao usuário especificado na propriedade `was.wsadmin.username`.
was.client.props	Especifica se você recuperar as configurações de segurança a partir de um arquivo de propriedades do cliente. Os valores possíveis são are `True` e `False`.
Configurações do WebSphere Application Server	
was.appserver.profile.name	Especifica o nome do perfil do servidor de aplicativos que você deseja configurar. Não usado para WebSphere Application Server Liberty.
was.appserver.home	Especifica o diretório inicial do WebSphere Application Server.
was.appserver.cell.name	Especifica o nome da célula do WebSphere Application Server. Não usado para WebSphere Application Server Liberty.

Tabela 223. Propriedades Disponíveis para Executar o Utilitário de Configuração no Modo Silencioso (continuação)	
Propriedade	**Comentário**
was.appserver.node.name	Especifica o nome do nó do WebSphere Application Server. Não usado para WebSphere Application Server Liberty.
Configurações da instância de tempo de execução do WebSphere Application Server	
was.appserver.server.name	Especifica a instância do servidor de aplicativos no perfil do servidor de aplicativos a configurar. **Dica:** • O arquivo de resposta silencioso pode ter várias instâncias dessa propriedade • Ao incluir um segundo servidor, remova o comentário do segundo servidor (ou seja, #[SERVER]) e inclua o nome do servidor.
tema.serveralias	Especifica o nome do nó na interface com o usuário de monitoramento que contém as informações de monitoramento para esta instância do servidor de aplicativos. O padrão é o nome do nó combinado com o nome do servidor. **Importante:** O alias pode conter somente os seguintes caracteres: A-Z, a-z, sublinhado (_), traço (-) e ponto (.). Não use outros caracteres no alias. **Dica:** O arquivo de resposta silencioso pode ter diversas instâncias desta propriedade. **Lembre-se:** A mudança do alias de servidor muda o nome da instância de agente registrado com Console do Cloud APM. Se essa não for a primeira vez que você configura o coletor de dados e você tiver mudado o alias de servidor, deve-se limpar alguns arquivos de cache. Para obter instruções detalhadas, consulte Limpando os arquivos de cache com antigos nomes de servidor.

Configurar manualmente o coletor de dados se os utilitários de configuração falharem
Se não for possível usar o utilitário de configuração fornecido para configurar o coletor de dados para o WebSphere Applications agent, é possível configurar manualmente o coletor de dados no Console Administrativo do WebSphere.

Antes de Iniciar

- Instale o WebSphere Applications agent.
- Saiba qual é o diretório inicial do coletor de dados, que é requerido pela configuração do coletor de dados. O padrão é `/opt/ibm/apm/agent/yndchome/7.3.0.14.08` em sistemas Linux e UNIX ou `C:\IBM\APM\dchome\7.3.0.14.08` em sistemas Windows.
- Se você desejar configurar o coletor de dados para um servidor Liberty, conheça qual é o diretório inicial do servidor Liberty. Por exemplo, `/opt/ibm/was/liberty/usr/servers/defaultServer`.
- Certifique-se de que um arquivo chamado `itcam_wsBundleMetaData.xml` exista na pasta *dc_home*`/runtime/wsBundleMetaData` e que possua o conteúdo a seguir. Se a pasta ou o arquivo não existir, crie-o manualmente.

  Lembre-se: O valor *plugins_dir_within_dc_home* deve ser configurado para o caminho absoluto da pasta `plugins` dentro do diretório inicial do coletor de dados. O padrão é `/opt/ibm/apm/agent/`

yndchome/7.3.0.14.08/plugins em sistemas Linux e UNIX ou C:\IBM\APM\dchome\7.3.0.14.08\plugins em sistemas Windows.

```
<bundles>
  <directory path="plugins_dir_within_dc_home">
      <bundle>com.ibm.tivoli.itcam.bundlemanager_7.2.0.jar</bundle>
  </directory>
  <directory path="plugins_dir_within_dc_home">
      <bundle>com.ibm.tivoli.itcam.classicsca_7.2.0.jar</bundle>
  </directory>
  <directory path="plugins_dir_within_dc_home">
      <bundle>com.ibm.tivoli.itcam.toolkitsca.classicsca_7.2.0.jar</bundle>
  </directory>
</bundles>
```

Sobre Esta Tarefa

Importante:

- Você deverá fazer mudanças manuais na configuração dos coletores de dados do WebSphere Application Server como usuário administrativo do WebSphere.
- Você deve ter experiência como administrador do WebSphere para fazer mudanças manuais no WebSphere Application Server para coleção de dados. Qualquer erro na alteração de configuração manual pode resultar no servidor de aplicativos não iniciado.
- Depois de configurar manualmente o coletor de dados para monitorar instâncias do servidor de aplicativos, não é possível usar o utilitário de desconfiguração para desconfigurar o coletor de dados. Em vez disso, deve-se desconfigurar manualmente o coletor de dados.

Procedimento

- Para configurar manualmente o coletor de dados para o WebSphere Application Server, consulte “Configurando manualmente o coletor de dados para o WebSphere Application Server tradicional” na página 856.
- Para configurar manualmente o coletor de dados para o servidor Liberty, consulte “Configurando manualmente o coletor de dados para WebSphere Application Server Liberty” na página 858.

Configurando manualmente o coletor de dados para o WebSphere Application Server tradicional

Procedimento

1. Efetue login no Console Administrativo do WebSphere como o administrador.
2. Na área de janela de navegação, clique em **Servidores**, expanda **Tipos de servidor** e clique em **Servidores de aplicativos WebSphere**.
3. Na seção **Infraestrutura do Servidor** na guia Configuração, expanda **Java e Gerenciamento de Processo** e clique em **Definição de Processo**.
4. Na seção **Propriedades Adicionais**, clique em **Java Virtual Machine**.
5. No campo **argumentos genéricos da JVM** , inclua as seguintes entradas.

   ```
   -agentlib:am_ibm_16=${WAS_SERVER_NAME} -Xbootclasspath/p:${ITCAMDCHOME}/
   toolkit/lib/bcm-bootstrap.jar -Djava.security.policy=${ITCAMDCHOME}/itcamdc/
   etc/datacollector.policy -verbosegc
   ```

   Ao incluir as entradas, anote o seguinte:

   - Todas as entradas devem estar em uma única linha.
   - Separe argumentos diferentes por espaços antes do sinal de menos (-), e não use espaços em nenhum outro lugar.
6. Clique em **Aplicar** e, em seguida, salve as mudanças na configuração principal.
   - Se você não estiver em um ambiente de Implementação de Rede, clique em **Salvar**.

- Se você estiver em um ambiente do Network Deployment, certifique-se de que **Sincronizar mudanças com nós** esteja selecionado nas opções **Preferências do console** e, em seguida, clique em **Salvar**.

7. Na área de janela de navegação, clique em **Servidores**, expanda **Tipos de servidor**, clique em **Servidores de aplicativos WebSphere** e, em seguida, clique no nome do servidor.
8. Na guia Configuração, acesse **Infraestrutura do servidor** > **Gerenciamento de Java e processos** > **Definição de processo** > **Entradas de ambiente**.
9. Dependendo do sistema operacional, da plataforma de hardware e da JVM do servidor de aplicativos, configure a seguinte entrada de ambiente.

Tabela 224. Entrada de ambiente

Plataforma	Nome da entrada de ambiente	Valor da entrada de ambiente
AIX R6.1 (JVM de 64 bits)	LIBPATH	`/lib:${ITCAMDCHOME}/toolkit/lib/aix536`
AIX R7.1 (JVM de 64 bits)	LIBPATH	`/lib:${ITCAMDCHOME}/toolkit/lib/aix536`
Solaris 10 (JVM de 64 bits)	LIBPATH	`/lib:${ITCAMDCHOME}/toolkit/lib/sol296`
Solaris 11 (JVM de 64 bits)	LIBPATH	`/lib:${ITCAMDCHOME}/toolkit/lib/sol296`
Linux Intel R2.6 (JVM de 32 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/li6263`
Linux x86_64 R2.6 (JVM de 64 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/lx8266`
Linux on Power Little Endian (JVM de 64 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/lpl266`
Linux on System z (JVM de 32 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/ls3263`
Linux on System z (JVM de 64 bits)	LD_LIBRARY_PATH	`/lib:${ITCAMDCHOME}/toolkit/lib/ls3266`
Windows (JVM de 32 bits)	PATH	`/lib;${ITCAMDCHOME}/toolkit/lib/win32`
Windows (JVM de 64 bits)	PATH	`/lib;${ITCAMDCHOME}/toolkit/lib/win64`

10. Clique em **Aplicar** e, em seguida, salve as mudanças na configuração principal.
    - Se você não estiver em um ambiente de Implementação de Rede, clique em **Salvar**.
    - Se você estiver em um ambiente do Network Deployment, certifique-se de que **Sincronizar mudanças com nós** esteja selecionado nas opções **Preferências do console** e, em seguida, clique em **Salvar**.
11. Na área de janela de navegação, clique em **Ambiente** > **Variáveis do WebSphere**.
12. Especifique o escopo para o nível do servidor apropriado e inclua a variável *ITCAMDCHOME*. Configure o valor da variável *ITCAMDCHOME* para o diretório inicial do coletor de dados. Por exemplo, `/opt/ibm/apm/agent/yndchome/7.3.0.14.08`.
13. Clique em **Aplicar** e, em seguida, salve as mudanças na configuração principal.
    - Se você não estiver em um ambiente de Implementação de Rede, clique em **Salvar**.

- Se você estiver em um ambiente do Network Deployment, certifique-se de que **Sincronizar mudanças com nós** esteja selecionado nas opções **Preferências do console** e, em seguida, clique em **Salvar**.

14. Reinicie o servidor da aplicação.

Resultados

Agora é possível verificar os dados do WebSphere Applications agent no Console do Cloud APM depois de incluir o componente de aplicativo em seus aplicativos. Para obter instruções sobre como iniciar o Console do Cloud APM, consulte "Iniciando o Console do Cloud APM" na página 975. Para obter instruções sobre como incluir ou editar um aplicativo, consulte "Gerenciando aplicativos" na página 1098.

O que Fazer Depois

Depois de configurar manualmente o coletor de dados, não é possível usar o utilitário `unconfig` fornecido para desconfigurar o coletor de dados. Em vez disso, desconfigure manualmente o coletor de dados. Para obter instruções, veja "Desconfigurar manualmente o coletor de dados" na página 151.

Configurando manualmente o coletor de dados para WebSphere Application Server Liberty

Procedimento

1. Navegue para o diretório inicial do servidor Liberty. Por exemplo, `/opt/ibm/wlp/usr/servers/defaultServer`.
2. Edite o arquivo `jvm.options` incluindo os parâmetros a seguir, em que *dc_home* é o diretório inicial do coletor de dados e *server_name* é o nome do servidor Liberty. Se o arquivo `jvm.options` não existir, crie-o com um editor de texto.

```
-agentlib:am_ibm_16=server_name
–Xbootclasspath/p:dc_home/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=dc_home/itcamdc/etc/datacollector.policy
-verbosegc
```

   Quando incluir as entradas, anote o seguinte:

   - Cada entrada deve estar em uma única linha.
   - Substitua *server_name* pelo nome do servidor Liberty real. Por exemplo, `defaultServer`.
   - Substitua *dc_home* pelo diretório inicial do coletor de dados real. Por exemplo, `/opt/ibm/apm/agent/yndchome/7.3.0.14.08`.

3. Abra o arquivo `server.env` no mesmo diretório e inclua o caminho a seguir na entrada de ambiente de acordo com o sistema operacional, em que *dc_home* é o diretório inicial do coletor de dados. Se o arquivo `server.env` não existir, crie-o com um editor de texto.

Tabela 225. Entrada de ambiente

Plataforma	Nome da entrada de ambiente	Valor da entrada de ambiente
AIX R6.1 (JVM de 64 bits)	LIBPATH	/lib:*dc_home*/toolkit/lib/aix536
AIX R7.1 (64 bit JVM)	LIBPATH	/lib:*dc_home*/toolkit/lib/aix536
Solaris 10 (JVM de 64 bits)	LIBPATH	/lib:*dc_home*/toolkit/lib/sol296
Solaris 11 (JVM de 64 bits)	LIBPATH	/lib:*dc_home*/toolkit/lib/sol296
Linux x86_64 R2.6 (JVM de 64 bits)	LD_LIBRARY_PATH	/lib:*dc_home*/toolkit/lib/lx8266

Tabela 225. Entrada de ambiente (continuação)		
Plataforma	**Nome da entrada de ambiente**	**Valor da entrada de ambiente**
Linux Intel R2.6 (JVM de 32 bits)	LD_LIBRARY_PATH	/lib:*dc_home*/toolkit/lib/li6263
Windows (JVM de 32 bits)	PATH	/lib;*dc_home*/toolkit/lib/win32
Windows (JVM de 64 bits)	PATH	/lib;*dc_home*/toolkit/lib/win64

4. Abra o arquivo `server.xml` no mesmo diretório e inclua as linhas a seguir para ativar o recurso de monitoramento:

```
<featureManager>
              <feature>webProfile-7.0</feature>
              <feature>monitor-1.0</feature>
              <feature>usr:itcam-730.140</feature>
   </featureManager>
```

5. Reinicie o servidor Liberty.

Resultados

Agora é possível verificar os dados do WebSphere Applications agent no Console do Cloud APM depois de incluir o componente de aplicativo em seus aplicativos. Para obter instruções sobre como iniciar o Console do Cloud APM, consulte “Iniciando o Console do Cloud APM” na página 975. Para obter instruções sobre como incluir ou editar um aplicativo, consulte “Gerenciando aplicativos” na página 1098.

O que Fazer Depois

Depois de configurar manualmente o coletor de dados, não é possível usar o utilitário `unconfig` fornecido para desconfigurar o coletor de dados. Em vez disso, desconfigure manualmente o coletor de dados. Para obter instruções, veja “Desconfigurar manualmente o coletor de dados” na página 151.

(Coexistência do agente) Configurando o WebSphere Applications agent e o coletor de dados

No ambiente de coexistência do agente em que o WebSphere Applications agent e o ITCAM Agent for WebSphere Applications estão instalados, você deve fazer alguma configuração adicional para o agente e seguir um procedimento diferente para configurar o coletor de dados.

Sobre Esta Tarefa

No ambiente de coexistência do agente, você configura somente um coletor de dados para enviar dados para o WebSphere Applications agent e o ITCAM Agent for WebSphere Applications. Ambos os agentes devem usar diferentes portas para atender às solicitações do coletor de dados.

Procedimento

1. Se o coletor de dados do ITCAM Agent for WebSphere Applications, que está instalado na antiga infraestrutura do IBM® Tivoli® Monitoring existir em seu ambiente, desinstale-o.
2. Instale o WebSphere Applications agent fornecido no IBM Cloud Application Performance Management 8.1.3 ou mais recente. Ele garante que a versão do coletor de dados 7.3.0.11.0 ou mais recente, que é suportada para coexistência do agente, esteja instalada.
3. Certifique-se de que o ID do usuário que irá configurar o coletor de dados e o ID do usuário que instalou o servidor de aplicativos tenham os privilégios de usuário apropriados requeridos pelo agente. Para obter instruções, veja “Verificando requisitos de acesso de usuário” na página 836.
4. Certifique-se de que o WebSphere Applications agent e o ITCAM Agent for WebSphere Applications estejam usando números de porta diferentes para atender a solicitações do coletor de dados. Os

números de porta devem ser exclusivos, não podem ser usados por nenhum outro componente em seu ambiente. Configure o agente novamente para mudar a porta, se necessário.

- Para obter informações sobre como configurar o WebSphere Applications agent, consulte "Configurando o WebSphere Applications agent" na página 860.
- Para obter informações sobre como configurar o ITCAM Agent for WebSphere Applications, consulte a documentação do ITCAM for Application Diagnostics ou ITCAM for Applications.

5. Use o utilitário de configuração fornecido para configurar o coletor de dados. Para obter instruções, veja "Configurando o coletor de dados para ambiente de coexistência de agente" na página 861.

   Dica: Se estiver familiarizado com a configuração do coletor de dados, também será possível configurar o coletor de dados no modo silencioso. Para obter instruções, veja "Configurando o Coletor de Dados no Modo Silencioso" na página 848.

Configurando o WebSphere Applications agent

No ambiente de coexistência de agentes, o coletor de dados é compartilhado pelo WebSphere Applications agent e ITCAM Agent for WebSphere Applications. Ambos os agentes devem usar diferentes portas para atender às solicitações do coletor de dados. Você deve configurar o agente para mudar a porta, se necessário.

Sobre Esta Tarefa

- Em sistemas Linux ou AIX, é possível configurar o agente interativamente executando o script de configuração e depois respondendo aos prompts ou silenciosamente criando um arquivo de resposta silencioso e executando o script de configuração sem interação.
- Em sistemas Windows, é possível configurar o agente criando um arquivo de resposta silencioso e executando o script de configuração ou com o utilitário Gerenciar Serviços de Monitoramento fornecido. Para obter informações sobre como iniciar Gerenciar Serviços de Monitoramento em sistemas Windows, consulte "Usando a janela IBM Cloud Application Performance Management em sistemas Windows" na página 180.

Procedimento

- Para configurar o agente ao editar o arquivo de resposta silenciosa e executar o script sem nenhuma interação, conclua as seguintes etapas:

  a) Crie um arquivo `.txt` como arquivo de resposta silencioso.

  b) Especifique os parâmetros a seguir no arquivo de resposta silencioso. A sintaxe é *`parameter_name=parameter_value`*.

  configure_type
  Especifica o tipo de configuração. Este parâmetro é requerido.

  O valor válido é `tema_configure` para configuração do agente.

  KYN_ALT_NODEID
  Especifica o ID do nó alternativo para identificar o agente. Este parâmetro é requerido.

  O valor válido é uma sequência alfanumérica de até 24 caracteres.

  KYN_PORT
  Especifica a porta de recebimento usada pelo agente. Ela é o soquete TCP que o agente usa para atender às solicitações de conexão do coletor de dados. Este parâmetro é requerido.

  O valor padrão é 63335.

  Lembre-se: No ambiente de coexistência de agentes, certifique-se de que o número da porta especificado aqui não esteja sendo usado pelo ITCAM Agent for WebSphere Applications.

  Por exemplo, inclua as linhas a seguir no arquivo `.txt` que você criou.

```
configure_type=tema_configure
KYN_ALT_NODEID=WASAgent
KYN_PORT=63335
```

c) Salve e feche o arquivo e, em seguida, insira o comando a seguir para executar o script de configuração:

- Linux AIX *install_dir*/bin/was-agent.sh config *path_to_responsefile*
- Windows *install_dir*\bin\was-agent.bat config *path_to_responsefile*

em que *install_dir* é o diretório de instalação do agente. O padrão é C:\IBM\APM nos sistemas Windows, /opt/ibm/apm/agent nos sistemas Linux e AIX.

d) Após a configuração ser concluída, reinicie o WebSphere Applications agent se ele não estiver em execução com o comando a seguir:

- Linux AIX *install_dir*/bin/was-agent.sh start
- Windows *install_dir*\bin\was-agent.bat start

- Para configurar o agente executando o script e respondendo aos prompts, conclua as seguintes etapas:

a) Na linha de comandos, vá para o diretório *install_dir*/bin, em que *install_dir* é o diretório de instalação do agente.

O padrão é /opt/ibm/apm/agent nos sistemas Linux e AIX.

b) Execute o script de configuração a partir do diretório:

```
./was-agent.sh config
```

c) Quando solicitado, insira 1 e pressione Enter para editar as configurações para o agente de monitoramento do WebSphere Applications agent.

d) Pressione Enter até que seja solicitado um ID do nó alternativo para identificar o agente de monitoramento.

e) Forneça o ID do nó e pressione Enter. O formato válido do ID do nó é uma sequência alfanumérica de até 24 caracteres.

f) Quando for solicitado o número da porta, forneça a porta usada pelo agente para atender às solicitações de conexão do coletor de dados e pressione Enter.

Lembre-se: Para o ambiente de coexistência de agentes, certifique-se de que a porta especificada não esteja sendo usada pelo ITCAM Agent for WebSphere Applications.

g) Após a configuração ser concluída, reinicie o WebSphere Applications agent.

Resultados
Você configurou o WebSphere Applications agent.

O que Fazer Depois
Em seguida, deve-se configurar o coletor de dados. Na configuração do coletor de dados, será solicitado que você forneça o número da porta configurado para o WebSphere Applications agent e ITCAM Agent for WebSphere Applications. Para obter instruções, veja "Configurando o coletor de dados para ambiente de coexistência de agente" na página 861.

Configurando o coletor de dados para ambiente de coexistência de agente
Se você tiver WebSphere Applications agent e ITCAM Agent for WebSphere Applications em seu ambiente, é possível configurar somente um coletor de dados para ambos os agentes.

Antes de Iniciar
Certifique-se de que tenha concluído outras etapas que estão documentadas em "(Coexistência do agente) Configurando o WebSphere Applications agent e o coletor de dados" na página 859.

Sobre Esta Tarefa

Use o utilitário de configuração interativo fornecido para configurar o coletor de dados para um ambiente no qual WebSphere Applications agent e ITCAM Agent for WebSphere Applications existem e compartilham o coletor de dados.

Limitação: A integração do coletor de dados com os seguintes componentes ou produtos não é suportada para ITCAM Agent for WebSphere Applications:

- ITCAM for Application Diagnostics Managing Server
- ITCAM para Transações
- Tivoli Performance Viewer

Lembre-se: O monitoramento do WebSphere Application Server Liberty não é suportado pelo ITCAM Agent for WebSphere Applications. Para monitorar o WebSphere Application Server Liberty, use somente WebSphere Applications agent. Para obter informações sobre a configuração do coletor de dados para monitoramento do Liberty, consulte "Configurando o coletor de dados interativamente" na página 840 ou "Configurando o Coletor de Dados no Modo Silencioso" na página 848.

Procedimento

1. Efetue login no sistema com o ID do usuário que é usado para instalar o servidor de aplicativos.
2. Na linha de comandos, vá para o diretório `bin` dentro do diretório *dc_home*. O diretório *dc_home* é o seguinte:
   - Windows *install_dir*\dchome\7.3.0.14.08
   - Linux AIX *install_dir*/yndchome/7.3.0.14.08
3. Execute o comando a seguir para iniciar o utilitário de configuração:
   - Windows `config.bat`
   - Linux AIX `./config.sh`

   O utilitário de configuração é iniciado e exibe os endereços IP de todas as placas de rede localizadas no sistema de computador local.
4. Insira o número que corresponde ao endereço IP a ser usado e pressione Enter.

   O utilitário de configuração exibe os diretórios iniciais do WebSphere Application Server que são descobertos no sistema.
5. Quando for solicitado o diretório inicial do servidor de aplicativos, insira o número que corresponde a um diretório inicial do WebSphere Application Server ou um caminho completo para um diretório inicial do servidor de aplicativos e pressione Enter.

   O utilitário de configuração exibe todos os perfis do servidor de aplicativos que são descobertos no diretório inicial especificado.
6. Quando for solicitado o perfil do servidor de aplicativos a ser configurado, insira o número que corresponde ao perfil do WebSphere Application Server e pressione Enter.

   O utilitário de configuração indica se o WebSphere Global Security está ativado para o perfil do WebSphere Application Server especificado. Se a segurança global não estiver ativada, vá para a Etapa "8" na página 863.
7. Especifique se deseja recuperar as configurações de segurança a partir de um arquivo de propriedades do cliente. Insira 1 para permitir que o utilitário de configuração recupere o nome do usuário e a senha do arquivo de propriedades do cliente apropriado. Caso contrário, insira 2 para inserir o nome do usuário e a senha do administrador do WebSphere.

   O coletor de dados se comunica com o WebSphere Administrative Services usando a Chamada de Método Remoto (RMI) ou o protocolo SOAP. Se a segurança global estiver ativada para um perfil, é necessário especificar o ID do usuário e a senha de um usuário que está autorizado a efetuar login no console administrativo do WebSphere Application Server para o perfil do servidor de aplicativo. Como alternativa, é possível criptografar o nome de usuário e a senha e armazená-los nos arquivos de

propriedades do cliente antes de configurar o coletor de dados. Você deve usar o arquivo `sas.client.props` para uma conexão RMI ou o arquivo `soap.client.props` para uma conexão SOAP.

8. Quando for solicitado o nome do host do console administrativo do WebSphere, pressione Enter para aceitar o padrão ou especifique o nome do host ou endereço IP do console administrativo do WebSphere. O valor padrão é `localhost`.
9. Quando o utilitário de configuração listar todas as instâncias do servidor que ainda não estão configuradas para coleta de dados, selecione uma ou mais instâncias do servidor de aplicativos da lista. Insira o número que corresponde à instância do servidor de aplicativos para configurar para coleta de dados ou insira um asterisco (`*`) para configurar todas as instâncias do servidor de aplicativos para coleta de dados e pressione Enter. Para especificar um subconjunto de servidores, insira os números, separados por vírgulas, que representam os servidores.
   Por exemplo, `1,2,3`.

   Lembre-se:

   - Para um ambiente independente, as instâncias do servidor de aplicativos devem estar em execução durante a configuração.
   - Para um ambiente do Network Deployment, o Deployment Manager deve estar em execução.
   - Assegure-se de que as instâncias do servidor de aplicativos que você selecionar sejam os servidores reais que hospedam os aplicativos ou serviços que deseja monitorar.

   O utilitário de configuração fornece uma opção para integrar o coletor de dados para WebSphere Applications agent.
10. Na seção **Integração com Agente para WebSphere Applications**, especifique que deseja integrar o coletor de dados ao agente de monitoramento. Deve-se inserir 1 para selecionar essa opção de integração e pressionar Enter.

    O servidor selecionado será registrado para o monitoramento de recurso PMI.
11. Especifique se você deseja configurar o coletor de dados dentro da instância do servidor de aplicativos. É necessário inserir 1 para yes e depois pressionar Enter.
12. Especifica se deseja ativar o coletor de dados para dados diagnósticos. Insira 1 para sim ou 2 para não.
13. Quando for solicitado o nome do host do componente do agente de monitoramento V8, insira o nome do host ou endereço IP do WebSphere Applications agent ou aceite o padrão.
14. Quando for solicitado o número da porta do agente de monitoramento V8, insira o número da porta que é usada pelo WebSphere Applications agent.

    Lembre-se: O valor padrão pode não ser adequado para uso se ele estiver sendo usado por outro componente. É necessário certificar-se de que a porta especificada não esteja sendo usada por nenhum outro componente em seu ambiente.
15. Especifique que deseja configurar o agente de monitoramento V6. Insira 1 para configurar o ITCAM Agent for WebSphere Applications e pressione Enter.
16. Quando for solicitado o nome do host ou endereço IP do agente de monitoramento V6, especifique o nome do host ou endereço IP do ITCAM Agent for WebSphere Applications.
17. Quando for solicitado o número da porta do agente de monitoramento V6, insira o número da porta que é usada pelo componente do agente de monitoramento do ITCAM Agent for WebSphere Applications.

    Lembre-se: O valor padrão pode não ser adequado para uso se ele estiver sendo usado por outro componente. É necessário certificar-se de que a porta especificada não esteja sendo usada por nenhum outro componente em seu ambiente.
18. Quando for solicitado o alias de servidor, não use o valor padrão e especifique um alias de servidor exclusivo que deseja usar. Se você estiver configurando várias instâncias do servidor de aplicativos, o utilitário de configuração solicitará um alias para cada instância.

    Importante: O alias pode conter somente os seguintes caracteres: `A-Z`, `a-z`, sublinhado (`_`), traço (`-`) e ponto (`.`). Não use outros caracteres no alias.

O alias de servidor é o primeiro qualificador do nome da instância de agente (também conhecido como MSN) que é exibido no Console do Cloud APM. O padrão é o nome do nó combinado com o nome do servidor. Por exemplo, o alias **node1server1** indica o servidor denominado **server1** no nó denominado **node1**.

19. Quando for solicitado o número da porta TCP/IP para o monitoramento de recursos de PMI, pressione Enter para aceitar o padrão ou insira um novo número. A porta padrão é 63355.

    A porta é usada para comunicação interna entre componentes que estão executando no mesmo host. Se a porta padrão estiver em uso, configure um número diferente.

20. Na seção **Suporte para rastreamento de transação**, especifique se deve ativar o rastreamento de transação. Insira 1 para sim ou insira 2 para não e vá para 22.

    Lembre-se: Para visualizar informações de rastreamento de transações, é preciso ativar o rastreamento de transações na página Configuração do agente do Console do Cloud APM.

21. Aceite o nome do host ou endereço IP padrão do Transaction Framework Extension, que é um componente interno do WebSphere Applications agent que reúne métricas do coletor de dados.
22. Aceite o número de porta padrão que o coletor de dados usa para se conectar ao Transaction Framework Extension. O padrão é 5457.
23. Especifique se deseja integrar o coletor de dados ao Application Performance Diagnostics Lite. Pressione Enter para aceitar o padrão para não.
24. Na seção **Configurações avançadas**, especifique se deseja mudar o caminho de log da coleta de lixo. Insira 1 para selecionar um caminho de log da coleta de lixo. Caso contrário, insira 2 e vá para a etapa “26” na página 864.
25. Especifique o caminho de log da coleta de lixo. Insira um nome de arquivo com seu caminho completo.

    Por exemplo, se você especificar `gc.log` como o nome do arquivo, o nome atual será configurado como *`profile_name.cell_name.node_name.server_name`*`.gc.log` para cada instância do servidor de aplicativos configurada.

    Importante: No caminho de log da coleta de lixo, é possível usar variáveis do WebSphere, tais como `${SERVER_LOG_ROOT}`. Entretanto, não use modelos, tais como `%pid`.

26. Na seção **Resumo da Configuração do Coletor de Dados**, revise o resumo da configuração do coletor de dados que deve ser aplicada às instâncias do servidor de aplicativos especificadas. Se necessário, modifique as definições de configuração.
27. Insira a para aceitar as mudanças.
28. Quando solicitado, especifique se deseja criar um backup de sua configuração atual. Insira 1 para criar um backup da configuração atual. Caso contrário, insira 2.
29. Reinicie a instância do servidor de aplicativos conforme indicado pelo utilitário de configuração.
    a) Acesse o diretório `bin` sob o diretório inicial para o perfil do servidor de aplicativos. Por exemplo, `opt/IBM/WebSphere/AppServer/profiles/`*`profile_name`*`/bin`.
    b) Pare o servidor de aplicativos inserindo o comando **`stopServer`** no console de comando.
    - Linux AIX `./stopServer.sh` *`server_name`*
    - Windows `stopServer.bat` *`server_name`*

    c) Quando solicitado, insira o ID do usuário e a senha do administrador do console administrativo do WebSphere.
    d) Inicie o servidor de aplicativos novamente inserindo o comando **`startServer`** no console de comando.
    - Linux AIX `./startServer.sh` *`server_name`*
    - Windows `startServer.bat` *`server_name`*

    A configuração do coletor de dados entra em vigor após a reinicialização do servidor de aplicativos.
30. Efetue login no Console do Cloud APM para visualizar dados nos painéis.

a) Acesse o console usando o link fornecido no e-mail que alerta que seu serviço está pronto. Como alternativa, acesse o console a partir do website do IBM Marketplace. Para obter instruções detalhadas, consulte "Iniciando o Console do Cloud APM" na página 975.

b) Use o Editor de aplicativos para incluir o servidor de aplicativos monitorado no Application Performance Dashboard. É possível incluí-lo como um novo componente para seu aplicativo existente ou criar um aplicativo para conter esse componente.

Para obter informações adicionais sobre o Editor de aplicativos, consulte "Gerenciando aplicativos" na página 1098.

O que Fazer Depois

- Se o ID do usuário atual que é usado para configurar o coletor de dados não for o mesmo ID do usuário que está executando o servidor de aplicativos, verifique se o ID do usuário para configurar o coletor de dados tem permissões de leitura e gravação nos diretórios `runtime` e `logs` no diretório inicial do coletor de dados. Esses dois subdiretórios são criados pelo ID do usuário que está executando o servidor de aplicativos quando o servidor é reiniciado.
- Para WebSphere Applications agent, efetue login no Console do Cloud APM para visualizar os dados de monitoramento nos painéis. Para ITCAM Agent for WebSphere Applications, efetue login no Tivoli Enterprise Portal para visualizar dados. Se os dados de monitoramento não estiverem disponíveis imediatamente, reinicie o agente de monitoramento executando os comandos a seguir:
  - Windows

    ```
    cd install_dir\bin
    was-agent.bat stop
    was-agent.bat start
    ```

  - Linux AIX

    ```
    cd install_dir/bin
    ./was-agent.sh stop
    ./was-agent.sh start
    ```

- A mudança do alias de servidor muda o nome da instância de agente registrado com Console do Cloud APM. Se essa não for a primeira vez que você configura o coletor de dados e se você mudou o alias de servidor, deverá limpar alguns arquivos de cache concluindo as seguintes etapas:
  1. Pare o agente de monitoramento se ele estiver em execução.
  2. Abra o arquivo *hostname*_yn.xml no diretório a seguir com um editor de texto, em que *hostname* é o nome do host no qual o WebSphere Applications agent ou ITCAM Agent for WebSphere Applications está instalado.
     - Windows *install_dir*\TMAITM6_x64 (O padrão é C:\IBM\APM\TMAITM6_x64 para WebSphere Applications agent ou C:\IBM\ITM\TMAITM6_x64 para ITCAM Agent for WebSphere Applications)
     - Linux AIX *install_dir*/config (O padrão é /opt/ibm/apm/agent/config para WebSphere Applications agent ou /opt/ibm/itm/agent/config para ITCAM Agent for WebSphere Applications)
  3. Localize a linha que começa com a seguinte sequência e que contém o nome do servidor anterior. Por exemplo, was85.win4net01Cell02.win4net01Node02.AppSrv01.server1, em que server1 é o nome anterior do servidor de aplicativos.

     ```
     <!ENTITY was_product_code.cellname.nodename.profilename.servername
     ```

     em que *was_product_code* é o código do produto do WebSphere Application Server; *cellname* é o nome da célula; *nodename* é o nome do nó; *profilename* é o nome do perfil do servidor de aplicativos; *servername* é o nome anterior do servidor de aplicativos.
  4. Localize o arquivo .XML indicado na linha dentro do diretório atual e exclua o arquivo.
  5. Remova a linha que você localizou na Etapa 3 do arquivo *hostname*_yn.xml.

6. No final do arquivo *hostname*_yn.xml, remova a linha que contém os nomes de servidores anteriores.
7. Salve e feche o arquivo.
8. Reinicie o agente de monitoramento.

Reconfigurando o coletor de dados se você mudar o tipo de oferta no Servidor Cloud APM
Se você mudou o tipo de oferta instalada no Servidor Cloud APM de Cloud APM, Base para Cloud APM, Advanced e o WebSphere Applications agentfoi instalado e configurado com a oferta Cloud APM, Base, para usar as capacidades avançadas do agente fornecidas na oferta Cloud APM, Advanced, você deve desinstalar o WebSphere Applications agent anterior e instalar o agente novamente com a oferta Cloud APM, Advanced. Como alternativa, é possível reconfigurar o coletor de dados para que as capacidades fiquem disponíveis na nova oferta.

Sobre Esta Tarefa

O WebSphere Applications agent é configurado de maneira diferente, dependendo de qual pacote de agente é utilizado para instalar o agente. Depois de alterar o tipo de oferta no Servidor Cloud APM, você tem duas opções para tomar as capacidades do agente na nova oferta disponíveis:

- Remover o agente instalado com a oferta anterior e, em seguida, instalar o agente na nova oferta.
- Reconfigurar o coletor de dados novamente para usar os recursos na nova oferta.

Procedimento

- Remova o agente instalado com a oferta anterior e, em seguida, instale o agente na nova oferta.
  a) Desconfigure o coletor de dados. Para obter instruções, veja "WebSphere Applications agent: desconfigurando o coletor de dados" na página 145.
  b) Desinstale o WebSphere Applications agent que você instalou com o pacote de agente da oferta anterior. Para obter instruções, veja "Desinstalando os agentes" na página 143.
  c) Instale o WebSphere Applications agent com o pacote de agente na nova oferta e configurar o coletor de dados novamente. Para obter instruções, veja "Configurando o coletor de dados com o utilitário de configuração simples" na página 837.
- Reconfigurar o coletor de dados novamente para usar os recursos na nova oferta.
  a) Edite o arquivo `offering.id` no diretório inicial do coletor de dados, mudando o valor **IOFFERING** para um dos seguintes valores, dependendo do novo tipo de oferta:

     BASE
     Se o novo tipo de oferta for Cloud APM, Base Private.

     AVANÇADO
     Se o novo tipo de oferta for Cloud APM, Advanced Private.

     O diretório inicial do coletor de dados é semelhante ao seguinte:

     – Windows *install_dir*\dchome\7.3.0.14.08
     – Linux AIX *install_dir*/yndchome/7.3.0.14.08

  b) Reconfigure o coletor de dados para ativar diagnósticos, rastreamento de transações, ou ambos, no coletor de dados, com base no que é suportado no novo tipo de oferta. Para obter instruções sobre como configurar o coletor de dados, consulte "Configurando o coletor de dados com o utilitário de configuração simples" na página 837.
  c) Reinicie o WebSphere Application Server novamente.
  d) Em qualquer página do Console do Cloud APM, clique em **Configuração do Sistema** > **Configuração do Agente** para abrir a página **Configuração do Agente**. Certifique-se de que a configuração de rastreamento de transações corresponda aos recursos disponíveis em seu novo tipo de oferta. Caso contrário, atualize a configuração.

A configuração de rastreamento de transação deve estar ativada para o Cloud APM, Advanced, mas desativada para o Cloud APM, Base.

Monitorando o WebSphere Application Server Liberty dentro de um contêiner Docker
Para monitorar um perfil Liberty dentro de um contêiner Docker, deve-se usar o comando **docker run** com algumas opções para configurar o coletor de dados antes que o WebSphere Application Server Liberty possa ser iniciado.

Antes de Iniciar
Você deve instalar o WebSphere Applications agent no host Docker.

Sobre Esta Tarefa

Cada perfil Liberty em execução dentro de um contêiner Docker requer um coletor de dados para coletar métricas de recursos, métricas da transação e os dados diagnósticos e, em seguida, transmitir os dados para o agente de monitoramento que está em execução no host Docker. Todos os coletores de dados que são configurados no mesmo host Docker compartilham o mesmo agente de monitoramento no host.

Procedimento

Para configurar o coletor de dados para um contêiner do perfil Liberty, conclua as etapas a seguir:

1. Crie um arquivo de resposta silencioso `.txt`, especifique as opções de configuração a seguir no arquivo e salve-o.

   ```
   tema.host=agent_host
   was.appserver.server.name=liberty_profile_name
   ```

   em que **tema.host** é usado para especificar o endereço IP do host do agente de monitoramento; **was.appserver.server.name** é usado para especificar o nome do perfil Liberty.

   Dica: Um arquivo de resposta silencioso de amostra (`sample_silent_liberty_config.txt`) é fornecido no diretório *<agent_install_dir>*`/agent/yndchome/7.3.0.14.08/bin`. É possível criar seu próprio arquivo de resposta com base neste arquivo de amostra.
2. Execute o comando a seguir para ativar o novo contêiner Docker. Observe que você deve aceitar a licença para concluir a configuração definindo o parâmetro **LICENÇA** como `accept`.

   ```
   $docker run -d -e LICENSE=accept \
   -e JAVA_HOME=<java_home_dir> \
   -p <port_number>:<port_number> \
   -v <web_app_dir>:<liberty_install_dir>/usr/servers/<liberty_profile_name> \
   -v <agent_install_dir>/agent/yndchome:<agent_install_dir>/agent/yndchome
   websphere-liberty /bin/bash \
   -c "<agent_install_dir>/agent/yndchome/<dcversion>/bin/config.sh -silent
   <absolute_path_to_silent_response_file> && <liberty_install_dir>/bin/server
   run <liberty_profile_name>"
   ```

   em que:

   - *<java_home_dir>* é o diretório do JRE que é usado pelo perfil Liberty. Por exemplo, `/opt/ibm/java/jre`.
   - *<port_number>* é o número da porta que é usado para comunicação entre o contêiner e o host.
   - *<web_app_dir>* é o diretório no qual o aplicativo da web está localizado.
   - *<liberty_install_dir>* é o diretório de instalação do WebSphere Application Server Liberty. O padrão é `/opt/ibm/wlp`.
   - *<liberty_profile_name>* é o nome do perfil Liberty.
   - *<agent_install_dir>* é o diretório de instalação do WebSphere Applications agent. O padrão é `/opt/ibm/apm`.
   - *<dcversion>* é o número da versão do coletor de dados para WebSphere Applications agent. Por exemplo, 7.3.0.14.08.

- *<absolute_path_to_silent_response_file>* é o caminho absoluto para o arquivo de resposta silencioso que você criou.

Por exemplo, o comando a seguir configura o coletor de dados para o perfil Liberty denominado newitcam. O WebSphere Applications agent e o perfil Liberty são instalados nos diretórios padrão. A versão do agente de monitoramento e do coletor de dados é 7.3.0.14.08.

```
$docker run -d -e LICENSE=accept \
-e JAVA_HOME=/opt/ibm/java/jre \
-p 9082:9082 \
-v /home/kub/liberty-docker/newitcam:/opt/ibm/wlp/usr/servers/newitcam \
-v /opt/ibm/apm/agent/yndchome:/opt/ibm/apm/agent/yndchome websphere-liberty
/bin/bash \
-c "/opt/ibm/apm/agent/yndchome/7.3.0.14.08/bin/config.sh -silent
/opt/ibm/wlp/usr/servers/newitcam/silent_config.txt && /opt/ibm/wlp/bin/server
run newitcam"
```

Resultados
Agora é possível verificar se os dados do WebSphere Applications agent são exibidos no Console do Cloud APM. A coluna **Nome da Célula** no widget **Informações do WAS** mostra o ID do contêiner do Docker no qual o perfil Liberty está em execução.

O que Fazer Depois
Para desconfigurar o coletor de dados interativamente, use o comando a seguir para iniciar o utilitário de desconfiguração:

```
docker exec -i container_id "<agent_install_dir>/yndchome/7.3.0.14.08/bin
/unconfig.sh"
```

Configurando manualmente o coletor de dados para monitorar os servidores de cluster dinâmico
É possível configurar o coletor de dados para monitorar instâncias do servidor de aplicativos em um cluster dinâmico, incluindo alguns parâmetros de configuração do coletor de dados para o modelo de servidor que foi usado para criar as instâncias de servidor de cluster dinâmico. Este é um método alternativo para configurar as instâncias do servidor de cluster dinâmico para criar os modelos de servidor específicos para o WebSphere Applications agent.

Sobre Esta Tarefa

Para configurar o coletor de dados para monitoramento de cluster dinâmico, você deve criar dois arquivos de configurações e, em seguida, incluir manualmente as configurações no console administrativo do WebSphere para modificar o modelo de servidor dinâmico. O diretório `runtime` é criado automaticamente quando o coletor de dados é iniciado para a instância do servidor de aplicativos. Observe que qualquer upgrade para o modelo de servidor apagará essas mudanças feitas desta maneira.

Importante:

- O nome do cluster não pode conter um espaço.
- Você deverá fazer mudanças manuais na configuração dos coletores de dados do WebSphere Application Server como usuário administrativo do WebSphere.
- Você deve ter experiência como administrador do WebSphere para fazer mudanças manuais no WebSphere Application Server para coleção de dados. Qualquer erro na alteração de configuração manual pode resultar no servidor de aplicativos não iniciado.
- Se você configurar manualmente o coletor de dados para monitorar instâncias do servidor de aplicativos, não será possível usar o utilitário de desconfiguração para desconfigurar o coletor de dados. Para desconfigurar o coletor de dados, você deve mudar manualmente as configurações de volta.

Procedimento

1. Crie o arquivo `dcManualInput.txt` no diretório `runtime` do coletor de dados.
   Siga as instruções em “Criando o arquivo dcManualInput.txt” na página 869.

2. Crie o arquivo `itcam_wsBundleMetaData.xml` no diretório `wsBundleMetaData` do coletor de dados. Siga as instruções em "Criando o arquivo itcam_wsBundleMetaData.xml" na página 871.
3. Use o console administrativo do WebSphere para modificar o modelo de servidor dinâmico, incluindo o parâmetro de configuração do coletor de dados. Siga as instruções em "Incluindo configurações com o console administrativo do WebSphere" na página 872.

   Dica: O nome do membro de cluster dinâmico é usado como o qualificador intermediário do nome da instância do WebSphere Applications agent exibido no Console do Cloud APM. Às vezes, o nome do membro de cluster pode ficar truncado devido ao limite de comprimento no nome da instância de agente. Nesse caso, é possível modificar o modelo de servidor dinâmico incluindo uma variável denominada *${MEP_NAME}* e configurando o valor para o nome da JVM para cada instância de servidor. Em seguida, é possível distinguir cada membro de cluster pelo nome da JVM real no Console do Cloud APM. Para obter instruções, veja "Opcional: Mostrando o nome da JVM real para distinguir membros de cluster" na página 875.

Criando o arquivo dcManualInput.txt

Sobre Esta Tarefa

O arquivo `dcManualInput.txt` contém alguns valores que são requeridos para a configuração inicial do coletor de dados.

Procedimento

Para criar o arquivo `dcManualInput.txt` , conclua as seguintes etapas:

1. Verifique se um arquivo nomeado *plataform*`_Template.DCManualInput.txt` existe no diretório a seguir. Se não existir, crie-o.
   - Linux AIX *install_dir*`/yndchome/7.3.0.14.08/runtime`
   - Windows *install_dir*`\dchome\7.3.0.14.08\runtime`

   A variável *platform* no nome do arquivo indica a arquitetura do sistema operacional, por exemplo, aix32, xLinux64.

   É possível nomear o arquivo como desejar. No entanto, *platform*`_Template.DCManualInput.txt` segue a convenção de nomenclatura padrão quando o arquivo é criado executando o script `configtemplate.sh`. Será necessário especificar esse arquivo para o modelo de servidor com o console administrativo do WebSphere na etapa subsequente.
2. Copie o conteúdo do arquivo a seguir para o arquivo `.txt` localizado ou criado na etapa anterior.
   - Linux AIX *dc_home*`/itcamdc/etc/was/dcInput_manual.properties`
   - Windows *dc_home*`\itcamdc\etc\was\dcInput_manual.properties`
3. Edite o conteúdo do arquivo `.txt`. Você deve configurar os parâmetros na seção 1 do arquivo de acordo com as descrições fornecidas na Tabela 226 na página 869.

   Lembre-se:

   - Não altere os parâmetros na seção 2.
   - Alguns dos parâmetros de configuração que são usados pelo coletor de dados para criar diretórios de tempo de execução são sempre configurados como none. Isso ocorre porque, no monitoramento de cluster dinâmico, o coletor de dados usa a configuração da instância do servidor WebSphere para criar os diretórios quando a JVM for iniciada.

Tabela 226. Parâmetros de Configuração para a Seção 1

Parâmetro	Valor
local.hostname	O endereço IP ou o nome completo do domínio do sistema local.

Tabela 226. Parâmetros de Configuração para a Seção 1 (continuação)	
Parâmetro	**Valor**
was.profile.home	O diretório inicial do perfil. Sempre configure-o para none para o servidor de cluster dinâmico
was.version	Um número curto da versão. Sempre configure-o para none para o servidor de cluster dinâmico
itcam.home	O diretório inicial do coletor de dados. Exemplo: `/opt/ibm/apm/agent/yndchome/7.3.0.14.08`
was.nodename	Nome do nó. Sempre configure-o para none para o servidor de cluster dinâmico
was.servername	Nome do servidor. Sempre configure-o para none para o servidor de cluster dinâmico
was.profilename	Nome do perfil do WebSphere. Sempre configure-o para none para o servidor de cluster dinâmico
am.camtoolkit.gpe.dc.operation.mode	modo de operação do coletor de dados. Os valores válidos são qualquer combinação de `WR`, `TT` e `DE`, em que: **WR** Integra o coletor de dados ao WebSphere Applications agent. **TT** Integra o coletor de dados ao ITCAM for Transactions. **DE** Integra o coletor de dados à Ferramenta de Diagnóstico ITCAM. A ferramenta é visualizada no ITCAM para Diagnósticos de Aplicativos beta. Você deve especificar somente os modos de operação necessária. Por exemplo, se você estiver conectando o coletor de dados ao WebSphere Applications agent somente, especifique `WR`. Separe os vários modos de operação com uma vírgula. Exemplo: `am.camtoolkit.gpe.dc.operation.mode=WR, DE`
interp	código de plataforma. Exemplo: `interp=win64` ou `interp=lx6266`

Tabela 226. Parâmetros de Configuração para a Seção 1 (continuação)	
Parâmetro	**Valor**
kwj.serveralias	Nome alternativo do WebSphere Application Server. Sempre configure-o para none para o servidor de cluster dinâmico
temagclog.path	(Opcional) O nome do arquivo de log de Coleta de Lixo. Insira um nome de arquivo exclusivo com caminho completo. O nome do caminho não deve incluir espaços.
tema.host	O nome do host ou o endereço IP do WebSphere Applications agent. Obrigatório se o modo de operação inclui o WebSphere Applications agent (WR). Geralmente, o agente de monitoramento é instalado em cada sistema no qual o coletor de dados está em execução e o endereço de loopback pode ser especificado. Exemplo: `tema.host=127.0.0.1`
tema.port	Porta a ser usada para se comunicar com o WebSphere Applications agent. Obrigatório se o modo de operação inclui o WebSphere Applications agent (WR). O valor padrão é 63335. Exemplo: `tema.port=63335`
tt.connection.string	O nome do host ou o endereço IP e o número da porta do componente coletor de transação do ITCAM for Transactions no formato de `tcp:`*`host_name`*`(IP):`*`port`*. Obrigatório se o modo de operação inclui o ITCAM for Transactions (TT). Exemplo: `tt.connection.string=192.38.234.77:5455`

4. Inclua as linhas a seguir na seção 1 do arquivo `.txt`.

```
bcm.helper=com.ibm.tivoli.itcam.was.bcm.websphere.DefaultWASBCMHelper
BCM_HELPER=@{bcm.helper}
```

5. Salve e feche o arquivo.

Criando o arquivo `itcam_wsBundleMetaData.xml`

Sobre Esta Tarefa

O arquivo `itcam_wsBundleMetaData.xml` contém alguns dos valores que são requeridos para a configuração inicial do coletor de dados.

Procedimento

Para criar esse arquivo, conclua as seguintes etapas:

1. Crie um diretório denominado `wsBundleMetaData` no diretório a seguir:
   - Linux AIX *`install_dir`*`/yndchome/7.3.0.14.08/runtime`
   - Windows *`install_dir`*`\dchome\7.3.0.14.08\runtime`
2. Crie um arquivo denominado `itcam_wsBundleMetaData.xml` e copie o conteúdo do arquivo a seguir nele:

- Linux AIX *install_dir*/yndchome/7.3.0.14.08/itcamdc/etc/was/itcam_wsBundleMetaData_template.xml
- Windows *install_dir*\dchome\7.3.0.14.08\itcamdc\etc\was\itcam_wsBundleMetaData_template.xml

3. No arquivo `itcam_wsBundleMetaData.xml`, substitua a variável *@{CONFIGHOME}* pelo caminho completo para seu diretório inicial do coletor de dados.

   O diretório inicial do coletor de dados em cada sistema operacional é o seguinte:

   - Linux AIX *install_dir*/yndchome/7.3.0.14.08
   - Windows *install_dir*\dchome\7.3.0.14.08

4. Coloque o arquivo `itcam_wsBundleMetaData.xml` no diretório `wsBundleMetaData` que você criou na Etapa 1.

Incluindo configurações com o console administrativo do WebSphere

Procedimento

Conclua as etapas a seguir para modificar o modelo de servidor dinâmico com o console administrativo do WebSphere.

1. Efetue login no Console Administrativo do WebSphere.
2. Clique em **Servidores**.
3. Expanda **Clusters** e selecione **Clusters Dinâmicos**.
4. Clique no nome do cluster do servidor dinâmico que você deseja configurar com o coletor de dados.
5. Na seção **Propriedades Adicionais**, clique em **Modelo de Servidor**.
6. Na seção **Infraestrutura do Servidor**, expanda **Java e Gerenciamento de Processo** e clique em **Definição de Processo**.
7. Na seção **Propriedades Adicionais**, clique em **Java Virtual Machine**.
8. No campo **argumentos genéricos da JVM** , inclua as seguintes entradas.

```
-agentlib:am_$jvm-vendor_$jvm-version=${WAS_SERVER_NAME}
-Xbootclasspath/p:${ITCAMDCHOME}/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=${ITCAMDCHOME}/itcamdc/etc/datacollector.policy
-verbosegc -Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=${ITCAMDCHOME}/runtime/
$platform_Template_DCManualInput.txt
-Dsun.rmi.dgc.client.gcInterval=3600000
-Dsun.rmi.dgc.server.gcInterval=3600000
-Dsun.rmi.transport.connectionTimeout=300000
-Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData
–Ditcamdc.dyncluster=true
```

   Quando estiver incluindo as entradas, anote o seguinte:

   - Todas as entradas devem estar em uma única linha.
   - Separe os diferentes argumentos por espaços antes do sinal de `-` , não use espaços em nenhum outro lugar.
   - Substitua as seguintes variáveis com os nomes reais :
     - *$jvm-vendor*: O fornecedor da JVM que é usado.
     - *$jvm-version*: as informações da versão da JVM, como 15 baseada em Java 5, 16 baseada em Java 6 ou 17 baseada em 7.
     - *$platform_Template_DCManualInput.txt*: O arquivo `.txt` que você criou na etapa anterior.

     Por exemplo:

```
-agentlib:am_ibm_16=${WAS_SERVER_NAME}
-Xbootclasspath/p:${ITCAMDCHOME}/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=${ITCAMDCHOME}/itcamdc/etc/datacollector.policy
-verbosegc -Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=${ITCAMDCHOME}/runtime/
aix64_Template_DCManualInput.txt
```

```
-Dsun.rmi.dgc.client.gcInterval=3600000
-Dsun.rmi.dgc.server.gcInterval=3600000
-Dsun.rmi.transport.connectionTimeout=300000
-Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData
–Ditcamdc.dyncluster=true
```

9. Clique em **Aplicar**.
10. Na caixa de diálogo Mensagens, clique em **Salvar**.
11. Na caixa de diálogo Salvar na Configuração Principal, conclua as seguintes etapas:
    - Se você estiver em um ambiente de implementação de rede, assegure-se de que **Sincronizar Mudanças com Nós** esteja selecionado e, em seguida, clique em **Salvar**.
    - Se você não estiver em um ambiente de Implementação de Rede, clique em **Salvar**.
12. Volte para expandir **Clusters**, clique em **Clusters Dinâmicos** e clique no mesmo nome do servidor.
13. Na guia **Configuração**, acesse **Infraestrutura do Servidor** > **Java e Gerenciamento de Processo** > **Definição de Processo** > **Entradas de Ambiente**.
14. Dependendo do sistema operacional, a plataforma de hardware, e o servidor de aplicativos da JVM, configure a seguinte entrada de ambiente :

Tabela 227. Entrada de ambiente

Plataforma	Entrada de Ambiente de nome	Entrada de Ambiente do valor
AIX R6.1 (JVM de 32 bits)	LIBPATH	/lib:${ITCAMDCHOME}/toolkit/lib/aix533:${ITCAMDCHOME}/toolkit/lib/aix533/ttapi
AIX R6.1 (JVM de 64 bits)	LIBPATH	/lib:${ITCAMDCHOME}/toolkit/lib/aix536:${ITCAMDCHOME}/toolkit/lib/aix536/ttapi
AIX R7.1 (JVM de 32 bits)	LIBPATH	/lib:${ITCAMDCHOME}/toolkit/lib/aix533:${ITCAMDCHOME}/toolkit/lib/aix533/ttapi
AIX R7.1 (JVM de 64 bits)	LIBPATH	/lib:${ITCAMDCHOME}/toolkit/lib/aix536:${ITCAMDCHOME}/toolkit/lib/aix536/ttapi
Linux x86_64 R2.6 (JVM de 64 bits)	LD_LIBRARY_PATH	/lib:${ITCAMDCHOME}/toolkit/lib/lx8266:${ITCAMDCHOME}/toolkit/lib/lx8266/ttapi
Linux Intel R2.6 (JVM de 32 bits)	LD_LIBRARY_PATH	/lib:${ITCAMDCHOME}/toolkit/lib/lx6263:${ITCAMDCHOME}/toolkit/lib/lx6263/ttapi
Linux ppc R2.6 (JVM de 32 bits)	LD_LIBRARY_PATH	/lib:${ITCAMDCHOME}/toolkit/lib/lpp263:${ITCAMDCHOME}/toolkit/lib/lpp263/ttapi
Linux ppc R2.6 (JVM de 64 bits)	LD_LIBRARY_PATH	/lib:${ITCAMDCHOME}/toolkit/lib/lpp266:${ITCAMDCHOME}/toolkit/lib/lpp266/ttapi

Tabela 227. Entrada de ambiente (continuação)		
Plataforma	**Entrada de Ambiente de nome**	**Entrada de Ambiente do valor**
Windows (JVM de 32 bits)	PATH	/lib;${ITCAMDCHOME}/toolkit/lib/win32;${ITCAMDCHOME}/toolkit/lib/win32/ttapi
Windows (JVM de 64 bits)	PATH	/lib;${ITCAMDCHOME}/toolkit/lib/win64;${ITCAMDCHOME}/toolkit/lib/win64/ttapi

15. Configure o nome da entrada de ambiente NLSPATH com o valor a seguir:

```
${ITCAMDCHOME}/toolkit/msg/%L/%N.cat
```

16. Clique em **Aplicar** e clique em **Salvar**.
17. Na caixa de diálogo Salvar na Configuração Principal, conclua as seguintes etapas:
    - Se você estiver em um ambiente de implementação de rede, assegure-se de que **Sincronizar Mudanças com Nós** esteja selecionado e, em seguida, clique em **Salvar**.
    - Se você não estiver em um ambiente de Implementação de Rede, clique em **Salvar**.
18. Volte para expandir **Clusters**, clique em **Clusters Dinâmicos** e, em seguida, clique no mesmo nome do servidor.
19. Na guia **Configuração**, acesse **Infraestrutura do Servidor** > **Java e Gerenciamento de Processo** > **Definição de Processo** > **Java Virtual Machine** > **Propriedades Adicionais: Propriedades Customizadas**.
20. Clique em **Novo** para incluir os pares de nome e valor a seguir e, em seguida, clique em **Aplicar**.
    - Crie uma propriedade `am.home` e configure seu valor para o seguinte diretório:
      - Linux AIX *install_dir*/yndchome/7.3.0.14.08/itcamdc
      - Windows *install_dir*\dchome\7.3.0.14.08\itcamdc
    - Crie uma propriedade `am.orig.wascell` e configure seu valor para o diretório da célula. Por exemplo, `am.orig.wascell =cellname1`.
    - Crie uma propriedade `com.ibm.tivoli.itcam.toolkit.ai.runtimebuilder.enable.rebuild` e configure seu valor como `true`.
    - Crie uma propriedade `ITCAM_DC_ENABLED` e configure seu valor como `true`.
    - Crie uma propriedade `TEMAGCCollector.gclog.path`. Se o argumento `verlogsegclog` da JVM genérica estiver configurado, defina o valor da propriedade `TEMAGCCollector.gclog.path` com o mesmo valor. Caso contrário, configure a propriedade `TEMAGCCollector.gclog.path` como `None`.

      Dica: Para identificar o valor da propriedade `verlogsegclog`, na guia **Configuração**, clique em **Infraestrutura do Servidor** > **Java e Gerenciamento de Processo** > **Definição de Processo** > **Java Virtual Machine**. O valor de `verlogsegclog` está no campo **Argumentos da JVM Genérica**.
21. Na caixa de diálogo Mensagens, clique em **Salvar**.
22. Na caixa de diálogo Salvar na Configuração Principal, conclua as seguintes etapas:
    - Se você estiver em um ambiente de Implementação de Rede, assegure-se de que **Sincronizar Mudanças com Nós** está selecionado. Clique em **Salvar**.
    - Se você não estiver em um ambiente de Implementação de Rede, clique em **Salvar**.
23. Na Área de Janela de Navegação, clique em **Ambiente** > **Variáveis do WebSphere**.

24. Configure as variáveis a seguir. Para cada variável, você deve escolher o nível do escopo apropriado, dependendo do diretório de instalação do coletor de dados em vários sistemas. Se sistemas diferentes possuem diretórios de instalação diferentes para o coletor de dados, estas variáveis devem ser configuradas corretamente para cada escopo no nível do nó. Se eles todos tiverem o mesmo diretório de instalação, o escopo poderá ser maior, tal como no nível do cluster.
    - Configure *ITCAMDCHOME* no diretório a seguir:
        - Linux AIX *install_dir*/yndchome/7.3.0.14.08/itcamdc
        - Windows *install_dir*\dchome\7.3.0.14.08\itcamdc
    - Configure *ITCAMDCVERSION* com a versão do coletor de dados, por exemplo, 7.3.0.14.08.
25. Clique em **Aplicar** e clique em **Salvar**.
26. Na caixa de diálogo Salvar na Configuração Principal, conclua as seguintes etapas:
    - Se você estiver em um ambiente de implementação de rede, assegure-se de que **Sincronizar Mudanças com Nós** esteja selecionado e, em seguida, clique em **Salvar**.
    - Se você não estiver em um ambiente de Implementação de Rede, clique em **Salvar**.

    Após o modelo ser modificado, os valores são sincronizados com todas as instâncias do servidor no cluster dinâmico. Qualquer novo servidor que for criado dinamicamente também terá os mesmos parâmetros de configuração do coletor de dados.
27. Reinicie a instância do servidor de aplicativos para o coletor de dados a ser ativado. O coletor de dados lê os arquivos de configuraçõe e cria o diretório de tempo de execução.

Opcional: Mostrando o nome da JVM real para distinguir membros de cluster

Sobre Esta Tarefa

No Console do Cloud APM, o nome da instância do WebSphere Applications agent tem o formato *host_name:*:*was_server_name*:KYNS e tem o comprimento máximo de 32 caracteres. No ambiente em cluster dinâmico, os nomes de membro de cluster dinâmico são usados para o qualificador intermediário *was_server_name*.

Às vezes, os nomes de membro de cluster ficam truncados devido ao limite de comprimento de caractere. Nesse caso, é possível especificar o nome da JVM real para ser usado no qualificador intermediário no nome da instância de agente.

Procedimento

Execute as etapas a seguir para mostrar o nome da JVM real no nome da instância de agente:

1. Efetue login no WebSphere Administrative Console para atualizar os argumentos de JVM genéricos incluindo uma nova variável de ambiente *${MEP_NAME}*, como a seguir:

```
-agentlib:am_$jvm-vendor_$jvm-version=${MEP_NAME}${WAS_SERVER_NAME}
-Xbootclasspath/p:${ITCAMDCHOME}/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=${ITCAMDCHOME}/itcamdc/etc/datacollector.policy
-verbosegc -Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=${ITCAMDCHOME}/runtime/
$platform_Template_DCManualInput.txt
-Dsun.rmi.dgc.client.gcInterval=3600000
-Dsun.rmi.dgc.server.gcInterval=3600000
-Dsun.rmi.transport.connectionTimeout=300000
-Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData
–Ditcamdc.dyncluster=true
```

   Por exemplo:

```
-agentlib:am_ibm_16=${MEP_NAME}${WAS_SERVER_NAME}
-Xbootclasspath/p:${ITCAMDCHOME}/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=${ITCAMDCHOME}/itcamdc/etc/datacollector.policy
-verbosegc
-Dcom.ibm.tivoli.itcam.ai.runtimebuilder.inputs=${ITCAMDCHOME}/runtime/
aix64_Template_DCManualInput.txt
-Dsun.rmi.dgc.client.gcInterval=3600000
-Dsun.rmi.dgc.server.gcInterval=3600000
```

```
-Dsun.rmi.transport.connectionTimeout=300000
-Dws.bundle.metadata=${ITCAMDCHOME}/runtime/wsBundleMetaData
–Ditcamdc.dyncluster=true
```

2. Salve e aplique as mudanças.
3. Na área de janela de navegação, clique em **Ambiente** > **Variáveis do WebSphere** para definir a variável *${MEP_NAME}* para cada membro de cluster dinâmico. Configure o valor para o nome da JVM real do membro de cluster.
4. Salve e aplique as mudanças.
5. Reinicie a instância do servidor de aplicativos.

   No Console do Cloud APM, uma nova instância do WebSphere Applications agent cujo nome contém o valor *${MEP_NAME}* que você acabou de especificar é exibida.

Configuração dinâmica da coleta de dados na página Configuração do Agente
Depois de ativar o suporte para o rastreamento de transações ou a coleta de dados diagnósticos no coletor de dados, use a página **Configuração do Agente** para ativar ou desativar dinamicamente a coleta de dados.

Antes de Iniciar

- Instale e configure o Monitoring Agent for WebSphere Applications.
- Para ativar ou desativar o rastreamento de transações para os servidores de aplicativos monitorados, instale o Rastreamento de Transações. Também é necessário ativar o suporte para o rastreamento de transações no agente, conforme descrito em “Configurando o coletor de dados interativamente” na página 840. Se você seguir o procedimento de configuração simples, o coletor de dados será automaticamente configurado com suporte para rastreamento de transação.
- Para ativar ou desativar a coleta de dados diagnósticos, incluindo rastreios de método, deve-se ter o Cloud APM, Advanced. Também é necessário ativar o suporte para a coleta de informações de diagnóstico e de rastreio de método no coletor de dados, conforme descrito em “Configurando o coletor de dados interativamente” na página 840. (Não disponível para Cloud APM, Base).

Dica: A página **Configuração do Agente** exibe todos os servidores que são monitorados pelo agente. Se algum servidor estiver ausente, ele pode não estar corretamente monitorado. Verifique os arquivos de log do agente no sistema monitorado para obter mensagens de erro, por exemplo, erros de conexão.

Lembre-se: O WebSphere Applications agent suporta apenas Db2 e Oracle como a origem de dados. Para outros tipos de origens de dados, alguns valores de KPI podem parecer estar nulos nos painéis Rastreamento de transações e widgets de grupos.

Procedimento

Conclua as etapas a seguir para configurar a coleta de dados para cada servidor:

1. A partir da barra de navegação, clique em **Configuração do Sistema** > **Configuração do Agente**.

   A página **Configuração do Agente** é exibida.
2. Clique na guia **Aplicativos WebSphere**.
3. Marque as caixas de seleção dos servidores nos quais você deseja configurar a coleta de dados e execute uma das ações a seguir a partir da lista de **Ações**:
   - Para ativar o rastreamento de transações, clique em **Ativar rastreamento de transações**. O status na coluna **Rastreamento da Transação Atual** é atualizado para Sim para cada servidor selecionado.
   - Para ativar somente a coleta de dados diagnósticos, clique em **Ativar Modo de Diagnóstico**. O status na coluna **Modo de Diagnóstico Atual** é atualizado para Sim para cada servidor selecionado.
   - Para coletar dados diagnósticos e informações de rastreio de método, clique em **Ativar Modo de Diagnóstico e Rastreio de Método**. O status nas colunas **Modo de Diagnóstico Atual** e **Rastreio de Método Atual** é atualizado para Sim para cada servidor selecionado.

- Para desativar o rastreamento de transações para o servidor selecionado, clique em **Desativar o Rastreamento de Transações**. O status na coluna **Rastreamento da Transação Atual** é atualizado para Não para cada servidor selecionado.
- Se somente a coleta de dados diagnósticos estiver ativada para o servidor selecionado, para desativar a coleta de dados, clique em **Desativar Modo de Diagnóstico**. O status na coluna **Modo de Diagnóstico Atual** é atualizado para Não para cada servidor selecionado.
- Se os dados diagnósticos e os dados de rastreio de método estiverem ativados para o servidor selecionado, para desativar a coleta de dados, clique em **Desativar Modo de Diagnóstico e Rastreio de Método**. O status nas colunas **Modo de Diagnóstico Atual** e **Rastreio de Método Atual** é atualizado para Não para cada servidor selecionado.

Lembre-se:

- A menos que o suporte para o rastreamento de transações ou a coleta de dados diagnósticos esteja configurado no coletor de dados, as operações na página **Configuração do Agente** não ativam a coleta de dados e o valor da coluna é configurado como No.
- Se o perfil do servidor de aplicativos foi configurado para usar `127.0.0.1` como o nome do host, a coluna **Endereço IP** na página **Configuração do Agente** exibirá o endereço IP do host no qual o WebSphere Applications agent está instalado e em execução.

Resultados
A coleta de dados foi configurada para cada servidor selecionado. Os dados de rastreamento de transações e os dados diagnósticos podem ser exibidos nos painéis de topologia após a ativação da coleta de dados.

Importante: Caso um servidor de aplicativos seja reiniciado, talvez seja necessário ativar o rastreamento de transações ou a coleta de dados diagnósticos para o servidor novamente.

Ativando o monitoramento de fuga de memória
Para que o painel Análise de memória contenha dados, deve-se ativar o monitoramento de fuga de memória para o coletor de dados. Se o JRE usado pelo servidor de aplicativos for suportado, a função de monitoramento de fuga de memória será ativada, por padrão, após a ativação da coleta de dados diagnósticos.

Antes de Iniciar

- Certifique-se de que `-Xtrace:none` não esteja definido nos argumentos da JVM para o servidor de aplicativos.
- Quando o monitoramento de fuga de memória é ativado, as seguintes configurações são definidas nos argumentos da JVM para o servidor de aplicativos. Se você definiu essas configurações em seus argumentos da JVM atuais, certifique-se de que a configuração do coletor de dados irá mudá-las.

```
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
```

- Certifique-se de que o JRE usado pelo servidor de aplicativos seja uma das seguintes versões:
  - IBM JRE 1.6.0 SR16 FP3 ou mais recente
  - IBM JRE 1.6.1 SR8 FP3 ou mais recente
  - IBM JRE 1.7.0 SR8 FP10 ou mais recente
  - IBM JRE 1.7.1 SR2 FP10 ou mais recente
  - IBM JRE 1.8 ou mais recente
  - Outro IBM JRE mais recente que o 1.6.0 SR7 com iFix para APAR IV67574

Sobre Esta Tarefa

A função de monitoramento de fuga de memória requer o componente IBM Health Center do IBM JRE. Deve-se assegurar que o JRE usado pelo servidor de aplicativos seja suportado por essa função.

- Em sistemas AIX ou Linux, ao configurar o coletor de dados para ativar a coleta de dados diagnósticos, se o JRE atual for suportado, o utilitário de configuração verificará automaticamente se o componente Health Center é elegível e fará upgrade do Health Center, se não for.
- Em sistemas Windows, deve-se fazer upgrade manualmente do componente Health Center se a versão atual não for suportada, porque o utilitário de configuração não pode substituir arquivos para um JRE em execução.

Lembre-se: O procedimento a seguir é necessário somente em sistemas Windows. Para sistemas AIX ou Linux, para ativar o monitoramento de fuga de memória, é necessário somente assegurar que a versão do JRE seja suportada e que a coleta de dados diagnósticos esteja ativada. Para sistemas Solaris, o Health Center do IBM JRE não é suportado, portanto, o monitoramento de fuga de memória não pode ser ativado em sistemas Solaris.

Procedimento

1. Verifique a versão do IBM Health Center que está incluída no JRE usado pelo servidor de aplicativos.
   a) No prompt de comandos, mude para o diretório `bin` no diretório inicial do JRE.
   b) Digite `java -Xhealthcenter -version` e pressione Enter.

   O comando retorna a versão do JRE e a versão do IBM Health Center. A função de monitoramento de fuga de memória requer o IBM Health Center 3.0.11 ou mais recente.
2. Se a versão do IBM Health Center não for elegível, faça upgrade do JRE para uma versão que contenha o IBM Health Center 3.0.11 ou mais recente.
3. Execute o utilitário de configuração ou reconfiguração do coletor de dados para ativar a coleta de dados diagnósticos.
   - Se você não configurou o coletor de dados, use `simpleconfig` ou `config`.
   - Se você configurou o coletor de dados, use o utilitário `reconfig`.

   Lembre-se: Se você ativou a coleta de dados diagnósticos antes de fazer upgrade do JRE, ainda precisará executar o utilitário de configuração de coleta de dados novamente.

Configurando o PMI

Para visualizar dados de desempenho em painéis de monitoramento operacional, o Performance Monitoring Infrastructure (PMI) no WebSphere Application Server deve ser configurado para reunir dados de desempenho.

Sobre Esta Tarefa

Use o WebSphere Administrative Console para ativar o PMI e configurar o nível de PMI no WebSphere Application Server.

O PMI fornece quatro níveis predefinidos:

1. Nenhum
2. Básico
3. Estendido
4. Todos

É possível usar uma opção customizada para ativar ou desativar seletivamente estatísticas individuais. Cada nível inclui as estatísticas do nível abaixo dele.

Para exibir dados nos painéis de monitoramento operacional, os atributos que são usados nos cálculos do painel devem ser incluídos no nível selecionado.

Por padrão, o WebSphere Applications agent configura o nível de PMI alto o suficiente para coletar os atributos necessários.

Restrição: Para configurar os dados em alguns dos widgets de grupo do Process Server e do Transaction Manager, você deve configurar manualmente o nível PMI. Para obter mais informações, consulte a ajuda detalhada nos widgets de grupo.

Se você modificar o nível de PMI com o WebSphere Administrative Console, deve-se verificar se o nível é alto o suficiente para coletar os dados necessários.

Procedimento

- Para ativar o PMI no servidor de aplicativos, conclua estas etapas:
  a) No WebSphere Administrative Console, expanda **Monitoramento e Ajuste** e, em seguida, selecione **Performance Monitoring Infrastructure (PMI)**.
  b) Na lista de servidores, clique no nome do seu servidor.
  c) Clique na guia Configuração e, em seguida, marque a caixa de seleção **Ativar Performance Monitoring Infrastructure (PMI)**.
  d) Clique em **Aplicar** ou **OK**.
  e) Clique em **Salvar** para ativar o PMI.
- Para configurar o nível de PMI no servidor de aplicativos, conclua estas etapas:
  a) No console administrativo do WebSphere, expanda **Monitoramento e Ajuste** e, em seguida, selecione **Performance Monitoring Infrastructure (PMI)**.
  b) Na lista de servidores, clique no nome do seu servidor.
  c) Clique na guia Configuração e, em seguida, selecione o conjunto de estatísticas para usar; Básico, Estendido, Todos ou Customizado.
  d) Clique em **Aplicar** ou **OK**.
  e) Clique em **Salvar** para configurar o nível de PMI.

  Para obter informações sobre o nível de PMI que é necessário para cada atributo, consulte a seção "Dashboard attributes" no WebSphere Applications agent Reference. A sobrecarga de monitoramento que é incorrida quando você ativa a coleta de cada atributo é exibida.

Restaurando a Configuração do Servidor de Aplicativos a Partir de um Backup
Se você configurou uma instância do servidor de aplicativos independente para a coleta de dados manualmente ou com o utilitário de configuração ou migração e o servidor de aplicativos falhar ao iniciar, é necessário restaurar a configuração do servidor de aplicativos a partir de um backup. Se você não tiver criado um backup, entre em contato com o Suporte IBM.

Sobre Esta Tarefa

Em um ambiente de implementação de rede, se você tiver configurado uma instância do servidor de aplicativos para coleta de dados manualmente ou com o utilitário de configuração ou migração e o servidor de aplicativos falhou ao ser iniciado, você tem as seguintes opções:

- É possível restaurar a configuração do servidor de aplicativos a partir de uma configuração de backup. Se você não tiver criado um backup, entre em contato com o Suporte IBM.
- É possível desconfigurar manualmente o coletor de dados. O Deployment Manager e o Agente do Nó no servidor de aplicativos devem estar em execução. Para obter mais informações, consulte “Removendo Manualmente a Configuração do Coletor de Dados de uma Instância do Servidor de Aplicativos” na página 149.

Essa seção se aplica apenas aos sistemas operacionais Windows, UNIX e Linux.

Procedimento

Para aplicar a configuração de backup usando o comando **`restoreConfig`**, use um dos seguintes procedimentos:

- Em um ambiente não do Network Deployment, conclua as seguintes etapas:
  a) Localize o arquivo de configuração de backup.

  O diretório padrão é *dc_home*/`data`. Se vários arquivos de backup estiverem presentes, verifique a data e hora de modificação do arquivo. Ele deve ser a data e a hora da configuração que falhou. Se

você não concluir todas as configurações do coletor de dados no mesmo host depois daquela com falha, use o arquivo mais recente no diretório.

b) Pare todas as instâncias do servidor de aplicativos.

c) Execute o comando **restoreConfig** a partir do diretório *appserver_home*/profiles/*profile_name*/bin.

A sintaxe de comandos é a seguinte:

– Windows `restoreConfig.bat` *full_path_to_backup_file*

– Linux AIX `./restoreConfig.sh` *full_path_to_backup_file*

Para obter informações adicionais sobre os argumentos do comando **restoreConfig**, consulte WebSphere Application Server Knowledge Center.

d) Inicie as instâncias do servidor de aplicativos novamente.

- Em um ambiente do Network Deployment, conclua as seguintes etapas:

a) Localize o arquivo de configuração de backup.

O diretório padrão é *dc_home*/data. Se diversos arquivos de backup estiverem presentes, verifique a data e hora da modificação do arquivo; deve ser a data e hora da configuração com falha. Se você não concluir todas as configurações do coletor de dados no mesmo host depois daquela com falha, use o arquivo mais recente no diretório.

b) Pare todas as instâncias do servidor de aplicativos.

c) Crie um diretório temporário em qualquer caminho conveniente (*temp_directory*). Em um sistema UNIX ou Linux, crie-o no diretório /tmp.

d) Execute o comando restoreConfig a partir do diretório *appserver_home*/profiles/*profile_name*/bin.

A sintaxe de comandos é a seguinte:

– Windows `restoreConfig.bat` *full_path_to_backup_file*

– Linux AIX `./restoreConfig.sh` *full_path_to_backup_file*

O comando **restoreConfig** restaura a configuração do servidor de aplicativos original para o diretório temporário.

e) Copie os arquivos server.xml, variables.xml e pmi-config.xml do diretório temporário para o sistema Deployment Manager.

– Diretório de origem: *temp_directory*/*restored_configuration_home*/cells/*cell_name*/nodes/*node_name*/servers/*server_name*

– Diretório de destino: *appserver_home*/profiles/*profile_name*/config/cells/*cell_name*/nodes/*node_name*/servers/*server_name*

f) Conclua uma sincronização de nó a partir do console administrativo do Gerenciador de Implementação para o nó.

g) No console administrativo do Gerenciador de Implementação, salve as mudanças na configuração principal.

h) Inicie as instâncias do servidor de aplicativos.

Configurando o coletor de dados Liberty para aplicativos no local

Para monitorar o perfil Liberty no Linux for System x, é possível implementar diretamente um coletor de dados independente no diretório local do Liberty sem instalar o WebSphere Applications agent.

Antes de Iniciar

1. Faça download do pacote coletor de dados do `IBM_Data_Collectors_Install.tgz` do website do IBM Passport Advantage. Para obter instruções detalhadas, consulte "Fazendo download de seus agentes e coletores de dados" na página 101.
2. Se suas regras de firewall não permitem conexões transparentes de HTTPS de saída com hosts externos, é possível configurar os coletores de dados para enviar o tráfego para um proxy de encaminhamento. Para obter instruções, veja "Configurando coletores de dados para se comunicarem através de um proxy de encaminhamento" na página 161.
3. O recurso monitor-1.0 é requerido pelo coletor de dados. É possível fazer download desse recurso do repositório do recurso Liberty com o comando **`installUtility`**. Para obter instruções, consulte a seção sobre como fazer download de ativos no WebSphere Application Server Network Deployment Knowledge Center.
4. Para que o painel Análise de memória contenha dados, você deve ativar a coleção de alocação de memória para o coletor de dados durante a configuração. Este recurso diagnóstico requer o IBM Health Center 3.0.8 ou mais recente. Se a versão do IBM Health Center não for elegível, faça upgrade do JRE que é usado pelo servidor de aplicativos para uma versão que contém o IBM Health Center 3.0.8 ou mais recente.

   Dica: Para verificar a versão do IBM Health Center que está incluída no JRE usado pelo servidor de aplicativos, mude para o diretório `bin` no diretório inicial do JRE e, em seguida, emita `java -Xhealthcenter -version`.

Sobre Esta Tarefa

É possível optar por configurar manualmente o coletor de dados ou usar o script de configuração fornecido para configurar o coletor de dados.

Procedimento

- Para configurar manualmente o coletor de dados, obtenha os arquivos do coletor de dados do pacote coletor de dados e, em seguida, modifique alguns arquivos locais para o servidor Liberty.
  a) Execute o comando a seguir para extrair arquivos do pacote coletor de dados.

  ```
  tar -xzf IBM_Data_Collectors_Install.tgz
  ```

  O pacote `liberty_datacollector_8.1.4.0.tgz` é incluído no diretório extraído.

  b) Extraia arquivos do pacote do `liberty_datacollector_8.1.4.0.tgz` para um diretório local com o seguinte comando. O diretório extraído será o diretório inicial do coletor de dados.

  ```
  tar -xzf liberty_datacollector_8.1.4.0.tgz
  ```

  Por exemplo, para extrair os arquivos para o diretório `/opt/ibm/apm/`, emita os comandos a seguir:

  ```
  cd /opt/ibm/apm
  tar -xzf liberty_datacollector_8.1.4.0.tgz
  ```

  É possível localizar os arquivos extraídos no diretório `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.08`. Esse diretório é referido como o diretório inicial do coletor de dados (*dc_home*) nas etapas a seguir.

  c) Navegue para o diretório inicial do servidor Liberty. Por exemplo, `/opt/ibm/wlp/usr/servers/defaultServer`.

  d) Edite o arquivo `jvm.options` incluindo os parâmetros a seguir. Se o arquivo `jvm.options` não existir, crie-o com um editor de texto.

  ```
  -agentlib:am_ibm_16=server_name
  -Xbootclasspath/p:dc_home/toolkit/lib/bcm-bootstrap.jar
  -Djava.security.policy=dc_home/itcamdc/etc/datacollector.policy
  -Dliberty.home=liberty_home
  ```

```
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
-verbosegc
-Xverbosegclog:absolute_path_to_log_file,1,10000
```

Quando incluir as entradas, anote o seguinte:

- Cada entrada deve estar em uma única linha.
- Substitua *server_name* pelo nome do servidor Liberty.
- Substitua *dc_home* pelo diretório inicial do coletor de dados. Por exemplo, `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.08`.
- Substitua *liberty_home* pela raiz do diretório de instalação do Liberty. Por exemplo, `/opt/ibm/wlp`.
- Se o servidor Liberty estiver funcionando com uma carga de trabalho intensa, inclua o parâmetro `-Xmx` para alocar um tamanho de heap extra de 512M para o coletor de dados. Por exemplo, `-Xmx1024M`.
- As linhas `-Xhealthcenter:level=inprocess` e `-Xgc:allocationSamplingGranularity=10000` são opcionais. Inclua as duas linhas somente se desejar ativar a coleta de alocação de memória, que é desativada por padrão. A ativação da coleta de alocação de memória é necessária para o painel Análise de memória conter dados.
- A linha `-Xverbosegclog:`*absolute_path_to_log_file*`,1,10000` é opcional, que especifica o caminho para o arquivo de log de coleta de lixo redirecionado. Se não for especificada, os logs serão gravados em um arquivo e irão girar a cada 10000 falhas de alocação. O arquivo original `stdout` ou `stderr` (`console.log`) pode ficar muito grande, conforme o servidor é executado. Inclua esta linha se desejar salvar os arquivos de log de saída de coleta de lixo em outro diretório e limitar o número e tamanho do arquivo de log. Se o caminho especificado for inválido, esta linha não terá nenhum efeito e o arquivo de log de coleta de lixo permanecerá o arquivo `stdout` ou `stderr`.

e) Abra o arquivo `server.env` no mesmo diretório e inclua o seguinte caminho na entrada de ambiente. Se o arquivo `server.env` não existir, crie-o com um editor de texto.

```
$LD_LIBRARY_PATH: /lib:dc_home/toolkit/lib/lx8266:dc_home/
Toolkit/lib/lx8266/ttapi
```

Quando incluir as entradas, anote o seguinte:

- Cada entrada deve estar em uma única linha.
- Substitua *dc_home* pelo diretório inicial do coletor de dados. Por exemplo, `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.08`.

f) Modifique o `server.xml` no mesmo diretório para ativar o recurso de monitoramento incluindo a seguinte linha na seção `<featureManager>`:

```
<feature>monitor-1.0</feature>
```

g) Reinicie o servidor Liberty.

- Para configurar o coletor de dados respondendo aos prompts, use o script de configuração que é fornecido nos pacotes coletores de dados.

a) Execute o comando a seguir para extrair arquivos do pacote coletor de dados.

```
tar -xzf IBM_Data_Collectors_Install.tgz
```

O pacote `liberty_datacollector_8.1.4.0.tgz` é incluído no diretório extraído.

b) Extraia arquivos do pacote do `liberty_datacollector_8.1.4.0.tgz` com o seguinte comando.

```
tar -xzf liberty_datacollector_8.1.4.0.tgz
```

Por exemplo,

```
cd /opt/ibm
tar -xzf liberty_datacollector_8.1.4.0.tgz
```

Os arquivos extraídos do coletor de dados estão no diretório `liberty_dc`.

c) Mude para o diretório `liberty_dc/.gdc/7.3.0.14.08/bin` e inicie o script de configuração executando o seguinte comando:

```
./config_liberty_dc.sh
```

d) Quando solicitado, insira a raiz do diretório de instalação do Liberty ou aceite o padrão. Por exemplo, `/opt/ibm/wlp`.

e) Quando solicitado, insira o início da JVM que é usado pelo servidor de aplicativos ou aceite o padrão. Por exemplo, `/opt/ibm/java`.

f) O programa de configuração pode descobrir e listar automaticamente os servidores de aplicativos que não estão configurados dentro do diretório especificado. Insira o número que corresponde ao servidor Liberty que você deseja configurar. Para selecionar mais de um servidor, separe os números por espaço ou insira `*` para selecionar tudo.

g) Após o programa de configuração concluir a atualização de arquivos para todos os servidores Liberty, atualize manualmente o tamanho de heap da JVM para alocar um heap extra de 512M para o coletor de dados.

h) Reinicie os servidores para que a configuração entre em vigor.

Resultados

O coletor de dados é configurado e está conectado ao Servidor Cloud APM. O monitoramento de recursos, rastreamento de transações e dados diagnósticos são ativados. No entanto, a coleção de heap e a coleção de alocação de memória são desativadas. É possível ativá-las com os arquivos de propriedades do coletor de dados, se você precisar dos dados nos painéis Dump do heap e Análise de memória.

O que Fazer Depois

- Para visualizar os dados de monitoramento para seus servidores Liberty, inicie o Console do Cloud APM. Para obter instruções, consulte Iniciando o Console do APM de Nuvem. Para obter informações sobre o uso do Editor de aplicativos, consulte Gerenciando aplicativos.

  Lembre-se: Ao incluir a instância do coletor de dados Liberty no Application Dashboard, selecione **Tempo de execução do Liberty** em vez de **WebSphere Application Server** da lista de componentes.
- Para que o painel Dump do Heap e/ou Análise de Memória contenha dados, também é necessário ativar o coletor de dados para o coletor de captura instantânea de heap e/ou para a coleção de alocação de memória, o que pode ser feito nos arquivos `.properties` do coletor de dados. Consulte “Ativando ou desativando o rastreamento de transação e a coleta de dados diagnósticos” na página 892.
- Se o arquivo-chave ou o Servidor Cloud APM mudar, reconecte o coletor de dados ao Servidor Cloud APM. Para obter instruções, veja “Reconectando o coletor de dados ao Servidor Cloud APM” na página 183.

Desconfigurando o coletor de dados para aplicativos no local

Se não precisar monitorar seus servidores Liberty ou desejar fazer upgrade do coletor de dados para uma nova versão, você deve desconfigurar o coletor de dados implementado no servidor Liberty.

Sobre Esta Tarefa

Para desconfigurar o coletor de dados implementado no servidor Liberty, recupere as mudanças feitas ao configurar o coletor de dados. É possível optar por configurar o coletor de dados manualmente ou com o script `unconfig_liberty_dc` fornecido.

Procedimento

- Para desconfigurar manualmente o coletor de dados, conclua as seguintes etapas:
  a) Navegue para o diretório inicial do servidor Liberty. Por exemplo, `/opt/ibm/wlp/usr/servers/defaultServer`.
  b) Edite o arquivo `jvm.options` para remover os seguintes parâmetros, se houver.

```
-agentlib:am_ibm_16=server_name
-Xbootclasspath/p:dc_home/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy=dc_home/itcamdc/etc/datacollector.policy
-Dliberty.home=liberty_home
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
-verbosegc
-Xverbosegclog:absolute_path_to_log_file,1,10000
```

  c) Edite o arquivo `server.env` no mesmo diretório para remover o seguinte valor para **LD_LIBRARY_PATH**

```
/lib:dc_home/toolkit/lib/lx8266:dc_home/toolkit/lib/lx8266/ttapi
```

  em que *dc_home* é o diretório inicial do coletor de dados. Por exemplo, `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.08`.
  d) Edite o arquivo `server.xml` no mesmo diretório para remover `<feature>monitor-1.0</feature>` da seção `<featureManager>`.
  e) Reinicie o servidor Liberty.
- Para desconfigurar o coletor de dados com o script `unconfig_liberty_dc.sh`, conclua as seguintes etapas:
  a) Mude para o diretório *dc_home*`/bin`. Por exemplo, `/opt/ibm/apm/liberty_dc/.gdc/7.3.0.14.08/bin`.
  b) Inicie o script de desconfiguração executando o seguinte comando:

```
./unconfig_liberty_dc.sh
```

  c) Quando solicitado, insira a raiz do diretório de instalação do Liberty ou aceite o padrão. Por exemplo, `/opt/ibm/wlp`.
  d) O programa de desconfiguração pode descobrir e listar automaticamente os servidores de aplicativos que estão configurados no diretório especificado. Insira o número que corresponde ao servidor Liberty que você deseja desconfigurar. Para selecionar mais de um servidor, separe os números por espaço ou insira * para selecionar tudo.
  e) Após o programa de desconfiguração concluir a atualização de arquivos para todos os servidores Liberty, reinicie os servidores para que as mudanças entrem em vigor.

O que Fazer Depois

Depois de desconfigurar o coletor de dados, o Console do Cloud APM continua a exibir o coletor de dados em quaisquer aplicativos nos quais você incluiu o coletor de dados. O Console do Cloud APM mostrará que nenhum dado está disponível para o aplicativo e não indicará que o coletor de dados está off-line. Para obter informações sobre como remover o coletor de dados de aplicativos e de grupos de recursos, consulte “Removendo coletores de dados do Console do Cloud APM” na página 186.

Também é possível excluir o diretório inicial do coletor de dados, caso ele não seja mais necessário.

Configurando o coletor de dados Liberty para aplicativos IBM Cloud

Para monitorar um perfil Liberty em execução no ambiente do IBM Cloud, deve-se fazer download do pacote do coletor de dados a partir do IBM Marketplace, implementar o coletor de dados nos seus arquivos de aplicativo locais e, em seguida, enviar por push as atualizações para o IBM Cloud.

Antes de Iniciar

Supõe-se que o aplicativo Liberty é enviado por push para o ambiente do IBM Cloud usando os comandos do Cloud Foundry. O arquivo `manifest.yml` e o diretório inicial do servidor Liberty (que contém o arquivo `server.xml`) já existem.

Se o seu aplicativo Liberty for implementado como um arquivo WAR, deve-se modificar alguns arquivos locais para atualizar seu aplicativo enviando por push um diretório local que contenha o arquivo WAR e os arquivos do coletor de dados. Um exemplo é fornecido aqui para explicar como obter um diretório inicial do servidor Liberty local, se você tiver apenas um arquivo WAR.

1. Emita o seguinte comando para executar o aplicativo Liberty localmente:

   ```
   mvn install liberty:run-server
   ```

   No diretório que contém o arquivo WAR do Liberty, um subdiretório, `/liberty/wlp/usr/servers/defaultServer`, é criado. Esse diretório pode servir como o diretório inicial do servidor Liberty no procedimento a seguir.
2. No diretório-raiz que contém o arquivo WAR do Liberty, copie a pasta *application_name*-SNAPSHOT inteira para o diretório `/liberty/wlp/usr/servers/defaultServer`.
3. No diretório `/liberty/wlp/usr/servers/defaultServer`, edite o arquivo `bootstrap.properties` para modificar o caminho de **appLocation**. O caminho **appLocation** deve ser configurado para o caminho relativo para o diretório do aplicativo no IBM Cloud.
4. Remova as pastas `logs` e `workarea`. Elas não precisam ser enviadas para o IBM Cloud.
5. Modifique o valor de **path** no arquivo `manifest.yml` para apontar para o diretório `defaultServer`.

   Por exemplo, `path: target/liberty/wlp/usr/servers/defaultServer`.

Procedimento

Conclua as seguintes etapas para configurar o coletor de dados Liberty:

1. Faça download do pacote coletor de dados denominado `IBM_Data_Collectors_Install.tgz` do IBM Marketplace. Para obter instruções detalhadas, consulte “Fazendo download de seus agentes e coletores de dados” na página 101.
2. Execute o comando a seguir para extrair arquivos do pacote coletor de dados.

   ```
   tar -xzf IBM_Data_Collectors_Install.tgz
   ```

   O pacote `liberty_datacollector_8.1.4.0.tgz` é incluído no diretório extraído.
3. Extraia arquivos do pacote do `liberty_datacollector_8.1.4.0.tgz` para um diretório temporário.

   ```
   tar -xzf liberty_datacollector_8.1.4.0.tgz
   ```

   Por exemplo,

   ```
   cd /root/tmp
   tar -xzf liberty_datacollector_8.1.4.0.tgz
   ```

   É possível localizar os arquivos extraídos no diretório `liberty_dc` dentro do diretório temporário.
4. Copie o diretório `.gdc` a partir do diretório `liberty_dc` para o diretório inicial do servidor Liberty no qual o arquivo `server.xml` está armazenado. O diretório inicial do servidor Liberty é referido como *liberty_server_home* nas etapas a seguir.

   ```
   cp -rf temp_dir/liberty_dc/.gdc liberty_server_home
   ```

   Por exemplo,

   ```
   cp -rf /root/tmp/liberty_dc/.gdc /opt/liberty855/wlp/usr/servers/defaultServer/
   ```

5. Copie ou mescle o conteúdo dos arquivos `jvm.options` e `server.env` do diretório `liberty_dc/etc` para o diretório *liberty_server_home*.
   - Se os arquivos `jvm.options` e `server.env` não existirem no diretório *liberty_server_home*, copie os dois arquivos a partir de *temp_dir*`/liberty_dc/etc` para *liberty_server_home*.

     ```
     cp temp_dir/liberty_dc/etc/jvm.option liberty_server_home
     cp temp_dir/liberty_dc/etc/server.env liberty_server_home
     ```

   - Se o arquivo `jvm.options` ou `server.env` existir no diretório *liberty_server_home*, mescle o conteúdo com aqueles do diretório *temp_dir*`/liberty_dc/etc`.
6. Se seus aplicativos IBM Cloud não puderem se conectar ao Servidor Cloud APM devido a configurações de rede ou de firewall, configure o coletor de dados para enviar o tráfego por meio de um proxy de encaminhamento. Para isso, edite o arquivo `jvm.options` de uma das seguintes maneiras:
   - Se a autenticação não for necessária, inclua as seguintes linhas no arquivo:

     ```
     -Dhttp.proxyHost=http_proxy_host
     -Dhttp.proxyPort=http_proxy_port
     -Dhttps.proxyHost=http_proxy_host
     -Dhttps.proxyPort=http_proxy_port
     -Djava.net.useSystemProxies=true
     ```

   - Se um nome do usuário e senha forem necessários para acessar o servidor proxy de encaminhamento, inclua as seguintes linhas no arquivo:

     ```
     -Dhttp.proxyHost=http_proxy_host
     -Dhttp.proxyPort=http_proxy_port
     -Dhttp.proxyUser=http_proxy_user
     -Dhttp.proxyPassword=http_proxy_password
     -Dhttps.proxyHost=http_proxy_host
     -Dhttps.proxyPort=http_proxy_port
     -Dhttps.proxyUser=http_proxy_user
     -Dhttps.proxyPassword=http_proxy_password
     -Djava.net.useSystemProxies=true
     ```

7. Modifique o arquivo `server.xml` dentro do diretório inicial do servidor Liberty para ativar o recurso de monitoramento, incluindo a seguinte linha na seção `<featureManager>`:

   ```
   <featureManager>
                <feature>monitor-1.0</feature>
   </featureManager>
   ```

8. Modifique o arquivo `manifest.yml` de seu aplicativo Liberty para alocar 512M de memória adicional.
9. Abra um prompt de comandos, mude para o diretório local que contém o arquivo `manifest.yml` para o servidor Liberty. Por exemplo, `/opt/liberty855/`.
10. Efetue login no IBM Cloud e atualize o perfil Liberty com o comando **`cf push`**.

Resultados

O coletor de dados é configurado e está conectado ao Servidor Cloud APM. O monitoramento de recursos, rastreamento de transações e dados diagnósticos são ativados. No entanto, a coleção de heap e a coleção de alocação de memória são desativadas. É possível ativá-las com os arquivos de propriedades do coletor de dados, se você precisar dos dados nos painéis Dump do heap e Análise de memória.

O que Fazer Depois

- Para visualizar os dados de monitoramento para seu aplicativo IBM Cloud, inicie o Console do Cloud APM. Para obter instruções, consulte Iniciando o Console do APM de Nuvem. Para obter informações sobre o uso do Editor de aplicativos, consulte Gerenciando aplicativos.

  Lembre-se: Quando desejar incluir a instância do coletor de dados Liberty no Application Dashboard, selecione **Tempo de Execução do Liberty** em vez de **WebSphere Application Server** na lista de componentes.

- Para que o painel Dump do Heap e/ou Análise de Memória contenha dados, também é necessário ativar o coletor de dados para o coletor de captura instantânea de heap e/ou para a coleção de alocação de memória, o que pode ser feito nos arquivos `.properties` do coletor de dados. Consulte "Customizando o coletor de dados com arquivos de propriedades" na página 889.
- Se o arquivo-chave ou o Servidor Cloud APM mudar, reconecte o coletor de dados ao Servidor Cloud APM. Para obter instruções, veja "Reconectando o coletor de dados ao Servidor Cloud APM" na página 183.

Variáveis de ambiente para customizar o coletor de dados Liberty
Para customizar o coletor de dados Liberty para os aplicativos IBM Cloud, use a IU do IBM Cloud para incluir as variáveis de ambiente que são suportadas pelo coletor de dados.

Dica: Para incluir variáveis de ambiente na IU do IBM Cloud, primeiramente efetue login na IU do IBM Cloud e clique em seu aplicativo e, em seguida, clique em **Tempo de execução** > **Variável de ambiente**. Na seção **definida pelo usuário**, inclua as variáveis de ambiente.

- Use as variáveis listadas em Tabela 228 na página 887 para configurar a conexão entre o coletor de dados Liberty e o Servidor Cloud APM.
- Use a variável que é listada em Tabela 229 na página 888 para ativar ou desativar o rastreio de método para seus aplicativos IBM Cloud .
- Após a ativação do rastreio de método, use as variáveis listadas em Tabela 230 na página 888 para especificar limites para os diferentes tipos de solicitações, para que diferentes níveis de dados de monitoramento possam ser coletados.

Lembre-se: Depois de incluir ou modificar a variável de ambiente, reinicie seu aplicativo para que as mudanças entrem em vigor.

Tabela 228. Varáveis de ambiente para conexões do servidor

Nome de variável	Valores ou intervalos	Descrição
APM_BM_GATEWAY_URL	• `https://` *`server_ip_or_hostname`*`:443` • `http://` *`server_ip_or_hostname`*`:80`	A URL do gateway de destino do Servidor Cloud APM.
APM_KEYFILE_PSWD	Senha criptografada do arquivo-chave	A senha do arquivo-chave criptografado que é pareada com o arquivo-chave. Se você for um usuário Linux, poderá usar o comando `echo -n` *`<keyfile password>`* `| base64` para criptografar sua senha. **Lembre-se:** Configure esta variável somente quando tiver configurado a variável *APM_BM_GATEWAY_URL* para usar HTTPS.
APM_KEYFILE_URL	`http://` *`hosted_http_server`*`:`*`port`*`/keyfile.jks`	A URL para fazer download do arquivo-chave. **Lembre-se:** Configure esta variável somente quando tiver configurado a variável *APM_BM_GATEWAY_URL* para usar HTTPS.

Tabela 229. Variável de ambiente para rastreio de método		
Nome de variável	**Valores ou intervalos**	**Descrição**
METHOD_TRACE_ENABLE	• `verdadeiro` • `false`	Use esta variável para ativar ou desativar o rastreio de método. O valor de `true` ativa o rastreio de método. O valor padrão é `false`.

Após o rastreio de método ser ativado, é possível configurar limites para diferentes tipos de solicitações para customizar o rastreio de método. Os seguintes limites, que acionam a coleta de diferentes níveis de dados de monitoramento, podem ser configurados para cada tipo de solicitação:

Limites primários
Se você configurar o limite primário para um tipo de solicitação, as informações de sincronização desse tipo de solicitação serão capturadas, como tempo de CPU e tempo de resposta para esse tipo de solicitação. Como resultado, quando uma solicitação demorar mais tempo para ser concluída do que o tempo especificado para o limite primário, a sincronização da solicitação será capturada.

Limites secundários
Se você configurar o limite secundário para um tipo de solicitação, dados de contexto profundos serão capturados, como rastreios de pilha e SQL para solicitações do banco de dados. Os dados de contexto que são capturados diferem com base no tipo de solicitação. Quando uma solicitação demorar mais tempo para ser concluída do que o tempo especificado para o limite secundário, seus dados de contexto serão capturados.

A variável de ambiente para limites de solicitação diferentes é nomeada como *<request_type>_<threshold level>*. Por exemplo, para configurar um limite primário para a solicitação JMS, inclua a variável JMS_PRIMARY e configure seu valor.

O Tabela 230 na página 888 lista as variáveis de ambiente correspondentes que é possível incluir para diferentes tipos de solicitação. Os valores estão em milissegundos.

Tabela 230. Variáveis de ambiente para limites de solicitação diferentes	
Nome de variável	**Valor padrão (em milissegundos)**
SERVLET_PRIMARY	20
SERVLET_SECONDARY	50
JDBC_PRIMARY	20
JDBC_SECONDARY	50
JNDI_PRIMARY	20
JNDI_SECONDARY	50
EJB_PRIMARY	20
EJB_SECONDARY	50
WEBSERVICES_PRIMARY	20
WEBSERVICES_SECONDARY	50
APP_METHODS_PRIMARY (métodos de aplicativo – não J2EE)	50
APP_METHODS _SECONDARY	1000
JCA_PRIMARY	50
JCA_SECONDARY	80

Tabela 230. Variáveis de ambiente para limites de solicitação diferentes (continuação)	
Nome de variável	**Valor padrão (em milissegundos)**
JMS_PRIMARY	40
JMS_SECONDARY	70

Customizando o coletor de dados com arquivos de propriedades

Por padrão, o rastreamento de transação e o rastreio de método são ativados para o coletor de dados. A coleção de capturas instantâneas de heap e a coleção de alocação de memória são desativadas. É possível customizar a coleta de dados ou os intervalos nos quais os dados diagnósticos são coletados editando os arquivos `.properties` do coletor de dados.

Sobre Esta Tarefa

Os arquivos de propriedades do coletor de dados estão no diretório *dc_home*, por exemplo, `/opt/liberty855/wlp/usr/servers/defaultServer/.gdc/7.3.0.14.08`. Use propriedades diferentes para customizar o coletor de dados para os propósitos a seguir:

- Ativar ou desativar o rastreamento de transações.
- Ativar ou desativar a coleta de captura instantânea de heap.
- Especifique o intervalo no qual o coletor de dados obtém a captura instantânea de dump do heap.
- Ativar ou desativar o monitoramento de alocação de memória.
- Especifique o intervalo no qual o coletor de dados coleta informações de alocação de memória.
- Ative ou desative o rastreio de método.

Lembre-se: Depois de modificar os arquivos `.properties`, use o comando **`cf push`** para enviar por push as atualizações para o ambiente do IBM Cloud.

Procedimento

- Para ativar ou desativar o rastreamento de transação, configure a propriedade **`com.ibm.tivoli.itcam.dc.bluemix.transaction.enabled`** no arquivo a seguir como `true` ou `false`:

  dc_home`/ldc/etc/ldc.properties`

  Se o rastreamento de transação estiver ativado, será possível monitorar a pilha de aplicativos IBM Java nas topologias.
- Para ativar ou desativar a coleção de capturas instantâneas de heap, configure as propriedades **`com.ibm.tivoli.itcam.hc.send.heap.enable`** e **`com.ibm.tivoli.itcam.hc.snapshot.automatic.enable`** no arquivo a seguir como `true` ou `false`.

  dc_home`/healthcenter/etc/hc.properties`

  Se a coleção de capturas instantâneas de heap estiver ativada, o coletor de dados poderá obter uma captura instantânea de heap nos intervalos especificados. As informações do dump do heap podem ser exibidas no painel Dump do Heap.
- Para mudar o intervalo no qual a captura instantânea de heap é obtida pelo coletor de dados, configure a propriedade **`com.ibm.tivoli.itcam.hc.snapshot.automatic.interval`** no mesmo arquivo como um número inteiro positivo. A unidade do intervalo é minuto e o padrão é `360`.

  dc_home`/healthcenter/etc/hc.properties`
- Para ativar ou desativar a coleção de alocação de memória, configure a propriedade **`com.ibm.tivoli.itcam.hc.events.collection.automatic.enable`** no arquivo a seguir como `true` ou `false`.

  dc_home`/healthcenter/etc/hc.properties`

Lembre-se: Para ativar a coleção de alocação de memória, também é necessário assegurar que as duas linhas a seguir sejam incluídas no arquivo `jvm.options` do servidor Liberty.

```
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
```

Após a coleção de alocações de memória ser ativada, os dados ficam disponíveis no painel Análise de Memória.

- Para especificar o intervalo no qual as informações de alocação de memória são coletadas, configure a propriedade **com.ibm.tivoli.itcam.hc.events.collection.automatic.interval** no mesmo arquivo como um número inteiro positivo. A unidade do intervalo é minuto e o padrão é 15.

  dc_home/healthcenter/etc/hc.properties
- Para ativar ou desativar o rastreio de método, configure a propriedade **dfe.enable.methoddata** no arquivo a seguir como `true` ou `false`:

  dc_home/gdc/etc/gdc_dfe.properties

O que Fazer Depois

- Após a ativação do rastreio de método, é possível configurar limites para diferentes tipos de solicitações usando as variáveis de ambiente, para que os diferentes níveis de dados de monitoramento possam ser coletados para diferentes solicitações. Para variáveis de ambiente aplicáveis, consulte Tabela 230 na página 888.
- Se você desativou a coleção de alocação de memória, lembre-se de remover as linhas a seguir do arquivo `jvm.options` do servidor Liberty:

```
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
```

Desconfigurando o coletor de dados para aplicativos IBM Cloud

Se você não precisar monitorar seus perfis Liberty no ambiente do IBM Cloud ou se desejar fazer upgrade do coletor de dados para uma nova versão, deve-se desconfigurar o coletor de dados que você implementou anteriormente.

Sobre Esta Tarefa

Para desconfigurar o coletor de dados para o perfil Liberty no ambiente do IBM Cloud, retroceda as mudanças que são feitas nos arquivos `jvm.options`, `server.env` e `server.xml` e, em seguida, atualize o perfil Liberty no IBM Cloud com o comando **cf push**.

Procedimento

1. No diretório local do perfil Liberty, modifique o arquivo `jvm.options` para remover os seguintes parâmetros. É possível excluir o arquivo se ele está vazio após a mudança.

```
-agentlib:am_ibm_16=defaultServer
-Xbootclasspath/p:../../../../.gdc/7.3.0.14.08/toolkit/lib/bcm-bootstrap.jar
-Djava.security.policy= ../ ../ ../ ../.gdc/7.3.0.14.08/itcamdc/etc/datacollector
.policy
-Dliberty.home=/home/vcap/app/.liberty
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
-verbosegc
-Xverbosegclog:/home/vcap/app/wlp/usr/servers/defaultServer/logs/gc.log,1,10000
```

2. No arquivo `server.env`, remova o seguinte valor para a variável de ambiente **LD_LIBRARY_PATH**. É possível excluir o arquivo se ele está vazio após a mudança.

```
: ../../../../.gdc/7.3.0.14.08/toolkit/lib/lx8266
: ../../../../.gdc/7.3.0.14.08/toolkit/lib/lx8266/ttapi
```

3. Modifique o arquivo `server.xml` para remover o recurso monitor-1.0 removendo a seguinte linha da seção `<featureManager>`

```
<feature>monitor-1.0</feature>
```

4. Exclua o diretório `.gdc` no diretório inicial do Liberty.
5. Abra um prompt de comandos, mude para o diretório que contém o arquivo `manifest.yml` do servidor Liberty.
6. Efetue login no IBM Cloud e atualize o perfil Liberty com o comando **`cf push`**.

O que Fazer Depois
Depois de desconfigurar o coletor de dados, o Console do Cloud APM continua a exibir o coletor de dados em quaisquer aplicativos nos quais você incluiu o coletor de dados. O Console do Cloud APM mostrará que nenhum dado está disponível para o aplicativo e não indicará que o coletor de dados está off-line. Para obter informações sobre como remover o coletor de dados de aplicativos e de grupos de recursos, consulte "Removendo coletores de dados do Console do Cloud APM" na página 186.

Configuração avançada do coletor de dados

É possível modificar os arquivos de configuração do coletor de dados para alterar as configurações adicionais de monitoramento.

Arquivos de propriedades para o coletor de dados do Liberty
Vários arquivos de configuração são fornecidos para você para controlar ainda mais a configuração e o comportamento do coletor de dados.

Depois de extrair o pacote coletor de dados para um diretório local, os arquivos do coletor de dados estarão localizados no diretório *local_dir*`/liberty_dc/.gdc/7.3.0.14.08`. Por exemplo, `/opt/ibm/apm/.gdc/7.3.0.14.08`. Essa pasta se torna o diretório inicial do coletor de dados, que é referido como *dc_home* nas instruções a seguir para simplificação.

Arquivos de propriedades do coletor de dados

Cada instância do servidor de aplicativos que é monitorada pelo coletor de dados tem seu próprio arquivo de propriedades. O coletor de dados cria automaticamente o arquivo de propriedades. O nome do arquivo é *dc_home*`/runtime/`*appserver_version.node_name.profile_name.server_name*`/datacollector.properties`.

Para facilitar futuros upgrades, não mude este arquivo.

Em vez disso, inclua as configurações que deseja modificar para o arquivo de propriedades customizadas do coletor de dados. Este arquivo é chamado *dc_home*`/runtime/`*app_server_version.node_name.profile_name.server_name*`/custom/datacollector_custom.properties`. As configurações no arquivo de propriedades customizadas do coletor de dados substituem os valores que estão no arquivo de propriedades do coletor de dados.

Importante: Se o arquivo *dc_home*`/runtime/`*app_server_version.node_name.profile_name.server_name*`/custom/datacollector_custom.properties` não existir, crie-o quando desejar fazer mudanças. Também pode ser necessário criar o diretório `custom`.

Arquivo de propriedades do kit de ferramentas

O arquivo de propriedades do kit de ferramentas é criado automaticamente pelo coletor de dados na inicialização, usando diversos arquivos de entrada. Ele é exclusivo para cada instância do servidor de aplicativos monitorada pelo coletor de dados. Seu nome é *dc_home*`/runtime/`*appserver_version.node_name.profile_name.server_name*`/toolkit.properties`.

Como este arquivo é recriado a cada inicialização do coletor de dados, **não faça nenhuma mudança** neste arquivo; se você o fizer, elas são sobrescritas.

Ao invés disso, inclua as configurações que deseja modificar no arquivo de propriedades customizadas do kit de ferramentas. Este arquivo é chamado *dc_home*/runtime/*app_server_version*.*node_name*.*profile_name*.*server_name*/custom/toolkit_custom.properties. As configurações no arquivo de propriedades customizadas do kit de ferramentas substituem os valores no arquivo de propriedades do kit de ferramentas.

Também é possível configurar as propriedades do kit de ferramentas de todas as instâncias do servidor de aplicativos monitoradas por esta instalação do coletor de dados. Para fazer isso, inclua as configurações no arquivo de propriedades customizadas do kit de ferramentas global: *dc_home*/runtime/custom/toolkit_global_custom.properties. Entretanto, se uma propriedade for configurada no arquivo toolkit_custom.properties específico da instância, ela substitui o valor no arquivo global para esta instância.

Importante: Se o arquivo *dc_home*/runtime/*app_server_version*.*node_name*.*profile_name*.*server_name*/custom/toolkit_custom.properties ou o arquivo *dc_home*/runtime/custom/toolkit_custom.properties não existir, crie-o quando desejar fazer mudanças. Também pode ser necessário criar o diretório custom.

Outros Arquivos de Propriedades

Além do arquivo de propriedades do coletor de dados e do arquivo de propriedades do kit de ferramentas, há outros arquivos de propriedades que são exclusivos para cada instância do servidor de aplicativos monitorada pelo coletor de dados.

***dc_home*/runtime/*appserver_version.node_name.profile_name.server_name*/custom/gdc/gdc_custom.properties**
Define os detalhes para a coleta de dados de diagnóstico e de rastreio de método. Para obter informações sobre este arquivo, consulte "Configurando a Coleta de Informações de Diagnóstico Detalhadas" na página 894.

***dc_home*/runtime/*appserver_version.node_name.server_name*/hc.properties**
Define os detalhes da coleção de capturas instantâneas de heap e a coleção de alocação de memória. Para obter informações sobre este arquivo, consulte "Configurando a Coleta de Informações de Diagnóstico Detalhadas" na página 894.

***dc_home*/runtime/*app_server_version.node_name.profile_name.server_name*/cynlogging.properties**
Define os nomes do arquivo de log e detalhes de criação de log para a parte Java do coletor de dados.

***dc_home*/runtime/*app_server_version.node_name.profile_name.server_name*/cyncclog.properties**
Define os nomes do arquivo de log e detalhes de criação de log para a parte C++ do coletor de dados.

Arquivos de rastreio do coletor de dados

Os arquivos de rastreio do coletor de dados são armazenados por padrão nos locais a seguir:

- Windows *dc_home*\logs\CYN\logs.
- Linux AIX *dc_home*/logs/CYN/logs.

Ativando ou desativando o rastreamento de transação e a coleta de dados diagnósticos
Por padrão, o rastreamento de transação e o rastreio de método são ativados para o coletor de dados. A coleção de capturas instantâneas de heap e a coleção de alocação de memória são desativadas. É possível customizar a coleta de dados ou os intervalos nos quais os dados diagnósticos são coletados editando os arquivos .properties do coletor de dados.

Sobre Esta Tarefa

Os arquivos de propriedades do coletor de dados estão no diretório *dc_home*, por exemplo, `/opt/ibm/apm/.gdc/7.3.0.14.08`. Use propriedades diferentes para customizar o coletor de dados para os propósitos a seguir:

- Ativar ou desativar o rastreamento de transações.
- Ativar ou desativar a coleta de captura instantânea de heap.
- Especifique o intervalo no qual o coletor de dados obtém a captura instantânea de dump do heap.
- Ativar ou desativar o monitoramento de alocação de memória.
- Especifique o intervalo no qual o coletor de dados coleta informações de alocação de memória.
- Ative ou desative o rastreio de método.

Lembre-se: Caso você tenha reiniciado o servidor Liberty após a configuração do coletor de dados, diferentes arquivos `.properties` são aplicáveis. Se você reiniciou o servidor Liberty após a configuração do coletor de dados, um diretório `runtime` é criado no diretório *dc_home*. Depois disso, é possível usar os arquivos `.properties` somente no diretório *dc_home*`/runtime/`*appserver_version.node_name.profile_name.server_name* para customizar o coletor de dados para cada servidor de aplicativos.

Procedimento

- Para ativar ou desativar o rastreamento de transação, configure a propriedade **com.ibm.tivoli.itcam.dc.bluemix.transaction.enabled** no arquivo a seguir como `true` ou `false`:

  dc_home`/runtime/`*appserver_version.node_name.server_name*`/ldc.properties` (se o diretório `runtime` não existir, use *dc_home*`/ldc/etc/ldc.properties`)

  Após o rastreamento da transação ser ativado, é possível monitorar a pilha de aplicativos IBM Java nas topologias.
- Para ativar ou desativar a coleção de capturas instantâneas de heap, configure as propriedades **com.ibm.tivoli.itcam.hc.send.heap.enable** e **com.ibm.tivoli.itcam.hc.snapshot.automatic.enable** no arquivo a seguir como `true` ou `false`.

  dc_home`/runtime/`*appserver_version.node_name.server_name*`/hc.properties` (se o diretório `runtime` não existir, use *dc_home*`/healthcenter/etc/hc.properties`)

  Após a coleção de capturas instantâneas de heap ser ativada, o coletor de dados pode obter a captura instantânea de heap em intervalos especificados. As informações do dump do heap podem ser exibidas no painel Dump do Heap.
- Para mudar o intervalo no qual a captura instantânea de heap é obtida pelo coletor de dados, configure a propriedade **com.ibm.tivoli.itcam.hc.snapshot.automatic.interval** no mesmo arquivo como um número inteiro positivo. A unidade do intervalo é minuto e o padrão é `360`.

  dc_home`/runtime/`*appserver_version.node_name.server_name*`/hc.properties` (se o diretório `runtime` não existir, use *dc_home*`/healthcenter/etc/hc.properties`)
- Para ativar ou desativar a coleção de alocação de memória, configure a propriedade **com.ibm.tivoli.itcam.hc.events.collection.automatic.enable** no arquivo a seguir como `true` ou `false`.

  dc_home`/runtime/`*appserver_version.node_name.server_name*`/hc.properties` (se o diretório `runtime` não existir, use *dc_home*`/healthcenter/etc/hc.properties`)

  Lembre-se: Para ativar a coleção de alocação de memória, também é necessário assegurar que as duas linhas a seguir sejam incluídas no arquivo `jvm.options` do servidor Liberty.

```
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
```

Após a coleção de alocações de memória ser ativada, os dados ficam disponíveis no painel Análise de Memória.

- Para especificar o intervalo no qual as informações de alocação de memória são coletadas, configure a propriedade **com.ibm.tivoli.itcam.hc.events.collection.automatic.interval** no mesmo arquivo como um número inteiro positivo. A unidade do intervalo é minuto e o padrão é 15.

  dc_home/runtime/*appserver_version.node_name.server_name*/hc.properties (se o diretório runtime não existir, use *dc_home*/healthcenter/etc/hc.properties)
- Para ativar ou desativar o rastreio de método, configure a propriedade **dfe.enable.methoddata** no arquivo a seguir como true ou false:

  dc_home/runtime/*appserver_version.node_name.profile_name.server_name*/custom/gdc/gdc_custom.properties (se o diretório runtime não existir, use *dc_home*/gdc/etc/gdc_dfe.properties)

Resultados

Depois de modificar os arquivos .properties, reinicie o servidor Liberty para que a mudança entre em vigor.

Para obter informações adicionais sobre os arquivos .properties do coletor de dados para cada servidor de aplicativos, consulte "Arquivos de propriedades para o coletor de dados do Liberty" na página 891.

O que Fazer Depois

- Após a ativação do rastreio de método, é possível configurar limites para diferentes tipos de solicitações, para que diferentes níveis de dados de monitoramento possam ser coletados para diferentes solicitações. Para obter instruções, veja "Customizando os limites de solicitação" na página 896.
- Se você desativou a coleção de alocação de memória, lembre-se de remover as linhas a seguir do arquivo jvm.options do servidor Liberty:

```
-Xhealthcenter:level=inprocess
-Xgc:allocationSamplingGranularity=10000
```

Configurando a Coleta de Informações de Diagnóstico Detalhadas

Se você tiver um IBM Cloud Application Performance Management, Advanced, poderá usar o coletor de dados para coletar informações detalhadas de diagnóstico sobre a instância do servidor de aplicativos monitorada. Para configurar o comportamento da coleta de dados diagnósticos, incluindo a quantidade de informações de diagnóstico que o coletor de dados armazena, customize o arquivo de configuração gdc_custom.properties.

Sobre Esta Tarefa

É possível localizar o arquivo gdc_custom.properties no diretório *dc_home*/runtime/*appserver_version.node_name.profile_name.server_name*/custom/gdc.

O exemplo a seguir descreve como usar as propriedades no arquivo de configuração gdc_custom.properties para fazer o seguinte:

- Configurando os limites para o tamanho e o número de arquivos de informações detalhadas
- Configurando a Coleção Completa ou Parcial de Dados Diagnósticos de Solicitação e Método

Também é possível configurar outras propriedades no arquivo gdc_custom.properties para customizar a coleção de dados diagnósticos. Consulte os comentários no arquivo que descrevem as propriedades.

Lembre-se: Após você concluir a edição do arquivo gdc_custom.properties, deve-se reiniciar a instância do servidor de aplicativos monitorada para que as mudanças entrem em vigor.

Configurando os limites para o tamanho e o número de arquivos de informações detalhadas

Sobre Esta Tarefa

O coletor de dados armazena informações de diagnóstico em diversos arquivos. Por padrão, ele armazena 100 arquivos; se 100 arquivos já estão armazenados e um novo arquivo for criado, o arquivo mais antigo será excluído. O coletor de dados cria um novo arquivo a cada 15 minutes minutos ou quando o tamanho do arquivo atual excede 200 megabytes. Quando o tamanho total do diretório que contém os arquivos exceder 2 gigabytes, o coletor de dados excluirá o arquivo mais antigo.

Procedimento

É possível alterar as seguintes configurações no arquivo *dc_home*/runtime/*appserver_version.node_name.profile_name.server_name*/custom/gdc/gdc_custom.properties:

- Para configurar o número máximo de arquivos com informações de diagnóstico, configure a propriedade com.ibm.itcam.gdc.dfe.filelimit.
  Por exemplo:

  ```
  com.ibm.itcam.gdc.dfe.filelimit=100
  ```

- Para configurar o horário, em minutos, após o qual o coletor de dados cria um novo arquivo de dados diagnósticos, configure a propriedade com.ibm.itcam.gdc.dfe.frequency.
  Por exemplo:

  ```
  com.ibm.itcam.gdc.dfe.frequency=15
  ```

- Para configurar o tamanho máximo do arquivo de dados diagnósticos, em megabytes, configure a propriedade dfe.file.maxlimit.
  Por exemplo:

  ```
  dfe.file.maxlimit=200
  ```

  Se o arquivo de dados diagnósticos atual alcança este tamanho, o coletor de dados cria um novo arquivo de dados diagnósticos.
- Para configurar o tamanho total máximo de todos os arquivos de dados, em bytes, configure a propriedade trace.dir.size.limit.
  Por exemplo:

  ```
  trace.dir.size.limit=2147483648
  ```

  Se a soma dos tamanhos de todos os arquivos de dados diagnósticos exceder este valor, o coletor de dados excluirá o arquivo de dados mais antigo. O tamanho mínimo total é de 25 megabytes.

Configurando a Coleção Completa ou Parcial de Dados Diagnósticos de Solicitação e Método

Sobre Esta Tarefa

O coletor de dados possui as configurações padrão a seguir:

- O coletor de dados coleta dados diagnósticos somente para as solicitações selecionadas. A seleção (amostragem) das solicitações tem como objetivo incluir todos os erros e algumas solicitações válidas.
- A coleta de dados de método está desativada na inicialização do servidor.
- Quando a coleta de dados de método está ativada, o coletor de dados reúne dados de método somente para algumas solicitações (para as quais dados diagnósticos são coletados). Esta seleção adicional (amostragem) tem como objetivo novamente incluir todos os erros e algumas solicitações válidas.

Importante: A alteração destas configurações afeta o desempenho do servidor de aplicativos. Em servidores de produção, a degradação de desempenho pode ser crítica.

Procedimento

É possível mudar essas configurações usando propriedades no arquivo *dc_home*/runtime/*appserver_version.node_name.profile_name.server_name*/custom/gdc/gdc_custom.properties.

- Para ativar a coleta de dados de método, configure a propriedade da seguinte forma:

  ```
  dfe.enable.methoddata=true
  ```

  Dica: Também é possível usar a página **Configuração de Agente** para ativar ou desativar dinamicamente a coleta de dados de rastreio de método.
- Para coletar dados diagnósticos para cada solicitação, desative a amostragem configurando a propriedade da seguinte forma:

  ```
  dc.sampling.enable=false
  ```
- Para ativar a coleta de dados de método para cada solicitação para as quais dados diagnósticos são coletados, configure a propriedade da seguinte forma:

  ```
  dc.sampling.enable=false
  dc.sampling.methsampler.enabled=false
  ```

  Lembre-se: A propriedade dc.sampling.methsampler.enabled entra em vigor apenas quando a coleta de dados de métodos é ativada na página Configuração do agente ou pela propriedade dfe.enable.methoddata.

Customizando os limites de solicitação

Algumas das solicitações podem não ter informações suficientes se os limites padrão forem altos. É possível customizar os limites de solicitação para que mais solicitações ou dados de contexto de solicitação possam ser capturados pelo coletor de dados.

Sobre Esta Tarefa

Cada tipo de solicitação tem dois tipos de limites, que são denominados **perfThreshold** e **secondaryPerfThreshold**. Uma solicitação é capturada pelo coletor de dados apenas quando ele leva mais tempo que o especificado para o limite **perfThreshold**. Dados de contexto, como um rastreio de pilha e instrução SQL, são capturados apenas quando a solicitação leva mais tempo do que o especificado para o limite **secondaryPerfThreshold**. É possível ajustar esses valores de limite para atender às suas necessidades.

Procedimento

1. Acesse o diretório *dc_home*\gdc\etc, em que *dc_home* é o diretório inicial do coletor de dados.
2. Em um editor de texto, abra o arquivo XML para o tipo de solicitação que você deseja customizar. É possível informar qual arquivo destina-se a qual tipo de solicitação a partir do nome de arquivo XML. Por exemplo, o arquivo ejb.xml destina-se a solicitações EJB, o arquivo custom.xml destina-se a solicitações customizadas e o arquivo appMethods.xml destina-se à classe e métodos quando o rastreio de método é ativado.
3. Configure as tags <collectContextData>, <collectStackTrace> e <createDataRow> para ifThresholdExceeded.

   ```
   <collectContextData>ifThresholdExceeded</collectContextData>
   <collectStackTrace>ifThresholdExceeded</collectStackTrace>
   <createDataRow>ifThresholdExceeded</createDataRow>
   ```
4. Configure as tags <perfThreshold> e <secondaryPerfThreshold> para os valores de limite desejados. A unidade do limite é milissegundo.
   Por exemplo, o arquivo ejb.xml tem as seguintes configurações para solicitações EJB. Como resultado, apenas as solicitações EJB com mais de 1 segundo (1000 milissegundos) são capturadas pelo coletor de dados. Além disso, os dados de contexto relacionados ao EJB, como o rastreio de pilha

e início de EJB, são capturados apenas quando a solicitação EJB leva mais de 1,5 segundos (1500 milissegundos).

```
<requestProbePoint id="EJB">
<interface>com.ibm.tivoli.itcam.toolkit.ai.boot.aspectmanager.ITurboEJBEventListener</
interface>
<family>EJB</family>
<collectContextData>ifThresholdExceeded</collectContextData>
<collectStackTrace>ifThresholdExceeded</collectStackTrace>
<perfThreshold>1000</perfThreshold>
<secondaryPerfThreshold>1500</secondaryPerfThreshold>
<dataToCollect>instanceAndSummary</dataToCollect>
<createDataRow>ifThresholdExceeded</createDataRow>
<requestType>EJB Method</requestType>
</requestProbePoint>
```

5. Salve suas mudanças e reinicie o servidor de aplicativos.

Desativando vários tipos de instrumentação de bytecode para APIs Java EE
Na Instrumentação de bytecode (BCI), o coletor de dados intercepta a entrada de método e chamadas de saída para vários tipos de APIs Java Platform Enterprise Edition (Java EE) para criar um fluxo de execução de cada solicitação de aplicativo. Alguns recursos são usados para o monitoramento. É possível ajustar o coletor de dados de forma que algumas APIS não sejam monitoradas, reduzindo o uso do recurso.

Para desativar o monitoramento de BCI para APIs Java EE, inclua as seguintes propriedades para o arquivo de propriedades customizadas do kit de ferramentas. Para obter mais informações sobre este arquivo, veja “Arquivo de propriedades do kit de ferramentas” na página 891.

Tabela 231. Incluindo Linhas no Arquivo de Propriedades Customizado do Kit de Ferramentas

Tipo de API Java EE	**Linha para incluir no arquivo `toolkit_custom.properties`**
Enterprise JavaBeans (EJB)	`com.ibm.tivoli.itcam.toolkit.ai.enableejb=false`
Java Connector Architecture (JCA)	`com.ibm.tivoli.itcam.toolkit.ai.enablejca=false`
Java Database Connectivity (JDBC)	`com.ibm.tivoli.itcam.toolkit.ai.enablejdbc=false`
Java Naming and Directory Interface (JNDI)	`com.ibm.tivoli.itcam.toolkit.ai.enablejndi=false`
Java Message Service (JMS)	`com.ibm.tivoli.itcam.toolkit.ai.enablejms=false`
Contêineres de Web para Servlets/JavaServer Pages (JSP)	`com.ibm.tivoli.itcam.dc.was.webcontainer=false`
Rastreio de Contagem de Sessões HTTP	`com.ibm.tivoli.itcam.toolkit.ai.enablesessioncount=false`
CICS Transaction Gateway (CTG)	`com.ibm.tivoli.itcam.dc.ctg.enablectg=false`
IMS	`com.ibm.tivoli.itcam.dc.mqi.enableims=false`
Java Data Objects (JDO)	`com.ibm.tivoli.itcam.dc.mqi.enablejdo=false`
Message Queue Interface (MQI)	`com.ibm.tivoli.itcam.dc.mqi.enablemqi=false`

Tabela 231. Incluindo Linhas no Arquivo de Propriedades Customizado do Kit de Ferramentas (continuação)	
Tipo de API Java EE	**Linha para incluir no arquivo `toolkit_custom.properties`**
Serviço da Web do Axis	`com.ibm.tivoli.itcam.toolkit.ai.axis.enablewebservice=false`
RMI (Remote Method Invocation)	`am.ejb.rmilistener.enable=false`
Contêiner EJB do WebSphere Application Server	`com.ibm.tivoli.itcam.dc.was.enableEJBContainer=false`

Desativando o rastreamento de transação para um determinado tipo de transação
Quando o rastreamento de transação é ativado para o coletor de dados, todos os tipos de transações são monitorados por padrão. É possível usar o arquivo de propriedades do kit de ferramentas para desativar o rastreamento de transação para tipos específicos de transações.

Sobre Esta Tarefa

Edite o arquivo `toolkit_custom.properties` para customizar o rastreamento de transação para cada servidor de aplicativos ou edite o arquivo `toolkit_global_custom.properties` para todas as instâncias do servidor de aplicativos.

O arquivo `toolkit_custom.properties` é usado no procedimento a seguir para um único servidor de aplicativos. As propriedades também são suportadas no arquivo `toolkit_global_custom.properties`. Para obter mais informações sobre os arquivos de propriedades do kit de ferramentas, consulte Arquivos de propriedades para o coletor de dados Liberty.

Procedimento

1. Abra o arquivo `toolkit_custom.properties` do servidor de aplicativos com um editor de texto. Esse arquivo pode ser encontrado no seguinte diretório:

   dc_home/runtime/*app_server_version*.*node_name*.*profile_name*.*server_name*/custom
2. De acordo com suas necessidades, especifique uma ou mais das seguintes propriedades e configure o valor da propriedade para `false` para desativar o rastreamento de transações para um determinado tipo de transação.

   Para solicitações do CICS
   `com.ibm.tivoli.itcam.dc.ttapi.cics.enabled=false`

   Para solicitações customizadas
   `com.ibm.tivoli.itcam.dc.ttapi.ims.enabled=false`

   Para solicitações do EJB
   `com.ibm.tivoli.itcam.dc.ttapi.ejb.enabled=false`

   Para chamadas do cliente HTTP
   `com.ibm.tivoli.itcam.dc.ttapi.httpclient.enabled=false`

   Exception: Para desativar o rastreamento de transações para chamadas do Apache HTTP Client, especifique `com.ibm.tivoli.itcam.toolkit.dc.enable.apache.httpclient=false`.

   Para solicitações do IMS
   `com.ibm.tivoli.itcam.dc.ttapi.ims.enabled=false`

   Para solicitações do JDBC
   `com.ibm.tivoli.itcam.dc.ttapi.jdbc.enabled=false`

   Para solicitações do JMS
   `com.ibm.tivoli.itcam.dc.ttapi.jms.enabled=false`

Para solicitações do JNDI
`com.ibm.tivoli.itcam.dc.ttapi.jndi.enabled=false`

Para solicitações do MQI
`com.ibm.tivoli.itcam.dc.ttapi.mqi.enabled=false`

Para solicitações do Portal
`com.ibm.tivoli.itcam.dc.ttapi.portal=false`

Para solicitações de Chamada de Método Remoto sobre IIOP
`com.ibm.tivoli.itcam.dc.ttapi.rmiiiop.enabled=false`

Para solicitações do Servlet
`com.ibm.tivoli.itcam.dc.ttapi.arm.servlet.enabled=false`

Para solicitações de serviço da web
`com.ibm.tivoli.itcam.dc.ttapi.webservice.enabled=false`

Dica: Para obter mais informações sobre essas propriedades, consulte o arquivo *dc_home*/`ttdc/etc/ttdc.properties`.

3. Salve e feche o arquivo `toolkit_custom.properties`.
4. Inicie o servidor de aplicativos novamente para que as alterações tenham efeito.

Excluindo classes do monitoramento
É possível customizar a coleta de dados excluindo determinadas classes do monitoramento. Use o arquivo de propriedades do kit de ferramentas para esta customização.

Sobre Esta Tarefa

Edite o arquivo `toolkit_custom.properties` para customizar o rastreamento de transação para cada servidor de aplicativos ou edite o arquivo `toolkit_global_custom.properties` para todas as instâncias do servidor de aplicativos.

O arquivo `toolkit_custom.properties` é usado no procedimento a seguir para um único servidor de aplicativos. As propriedades também são suportadas no arquivo `toolkit_global_custom.properties`. Para obter mais informações sobre os arquivos de propriedades do kit de ferramentas, consulte Arquivos de propriedades para o coletor de dados Liberty.

Procedimento

1. Abra o arquivo `toolkit_custom.properties` do servidor de aplicativos com um editor de texto. Esse arquivo pode ser encontrado no seguinte diretório:

   dc_home/`runtime/`*app_server_version.node_name.profile_name.server_name*/`custom`
2. Edite o arquivo para incluir a propriedade a seguir e salve suas mudanças.

```
am.camtoolkit.gpe.customxml.exclude=excludes.xml
```

3. No mesmo diretório `custom`, crie o arquivo `excludes.xml` com o seguinte conteúdo e especifique o nome da classe a ser excluída na tag <exclude>. É possível incluir tantas classes quantas forem necessárias e o curinga asterisco (*) é suportado.

```
<gpe>
  <bci>
    <classExcludes>
      <exclude>class_name_to_be_exclued</exclude>
      <exclude>class_name_to_be_exclued</exclude>
    </classExcludes>
  </bci>
</gpe>
```

   Por exemplo:

```
<gpe>
  <bci>
    <classExcludes>
```

```
      <exclude>org.apache.struts.action.ActionServlet</exclude>
      <exclude>com.company.package.*</exclude>
    </classExcludes>
  </bci>
</gpe>
```

4. Reinicie o servidor da aplicação.

O que Fazer Depois
Para verificar se a classe foi excluída, consulte o arquivo `toolkit.xml` e o nome da classe deve estar listado na seção `<classExcludes>`.

Lembre-se: O arquivo `toolkit.xml` contém configurações de tempo de execução e é atualizado toda vez que o servidor de aplicativos é reiniciado.

Customizando o Mapeamento de Informações da Solicitação
Em alguns casos, talvez seja necessário alterar as informações que identificam as solicitações monitoradas pelo agente. Essas informações incluem o nome da solicitação e dados que possam ser exibidos para a solicitação (por exemplo, o texto da consulta para uma solicitação SQL). Para alterar as informações, instale uma configuração customizada de mapeador de solicitações.

Sobre Esta Tarefa

Para customizar o mapeamento de informações, você deve definir uma configuração do mapeador de solicitação customizada em um arquivo XML.

Nesse arquivo, alguns *símbolos* integrados representam valores do contexto de tempo de execução da solicitação. É possível criar símbolos extras, que calculam novos valores. O cálculo pode incluir valores da solicitação original, expressões, chamadas para métodos Java (incluindo métodos no aplicativo monitorado), condicionais e a iteração sobre um conjunto de valores.

Depois, é possível *mapear* o conteúdo dos símbolos nos novos dados de solicitação fornecidos para o Servidor Cloud APM. Se uma variável específica nos dados da solicitação não for mapeada, o valor original será retido.

Como diferentes dados são coletados para tipos de solicitações, uma configuração customizada de mapeador de solicitações deve ser específica para um tipo de solicitação. Você pode configurar diferentes mapeadores de solicitação para diferentes tipos de solicitações no mesmo coletor de dados.

Procedimento

Para definir uma configuração do mapeador de solicitações customizado para um tipo de solicitação, conclua as seguintes etapas:

1. Defina uma configuração customizada de mapeador de solicitações em um arquivo XML.
   Para obter informações sobre a sintaxe XML, consulte "Sintaxe do Arquivo XML" na página 900.
2. Coloque o arquivo XML no diretório *dc_home*`/runtime/custom` para usá-lo para todas as instâncias do servidor de aplicativos ou no diretório *dc_home*`/runtime/`*appserver_version.node_name.profile_name.server_name*`/custom` para usá-lo para uma instância do servidor de aplicativos.
3. Ative o mapeamento de solicitação customizado para esse tipo no arquivo de configuração customizado do kit de ferramentas, `toolkit_custom.properties` ou `toolkit_global_custom.properties`.
   Para obter instruções, veja "Ativando um mapeador de solicitações" na página 910.
4. Faça referência ao arquivo XML definido para o mesmo arquivo de configuração customizado do kit de ferramentas.
   Para obter instruções, veja "Ativando um mapeador de solicitações" na página 910.

Sintaxe do Arquivo XML
O arquivo XML que você cria para configuração do mapeador de solicitações deve ser um XML válido e deve permanecer disponível quando a configuração estiver em uso. Coloque o arquivo XML no diretório

dc_home/runtime/custom para usá-lo para todas as instâncias do servidor de aplicativos ou no diretório *dc_home*/runtime/*appserver_version.node_name.profile_name.server_name*/custom para usá-lo para uma instância do servidor de aplicativos.

Nível mais alto

A tag de nível superior é <gpe>. Nessa tag, use a tag <runtimeConfiguration>. Essas tags não possuem atributos.

Na tag <runtimeConfiguration>, crie uma tag <requestMapperDefinition>. Esse tag deve ter um atributo type. Configure-o para o nome de tipo de mapeador de solicitação para o tipo de solicitação requerido. Para obter mais informações, consulte Tabela 233 na página 912.

Na tag <requestMapperDefinition>, as seguintes duas tags devem estar presentes:

<symbolDefinitions>
Contém todas as definições de símbolos. Símbolos representam valores que o agente calcula sempre que uma solicitação desse tipo é detectada.

<selection>
Contém o mapeamento de chaves de contexto para valores. As chaves representam os dados customizados que são passados para o agente. Elas são predefinidas para cada tipo de solicitação. O mapeamento pode ser condicional.

Para obter mais informações sobre o mapeador de solicitação que ativa propriedades e nomes de tipos, consulte Tabela 233 na página 912.

Além disso, na tag <runtimeConfiguration>, é possível criar uma tag <requestMapperClassPath>. Nessa tag, é possível definir arquivos JAR. É possível referenciar classes Java nesses arquivos JAR nas definições do Mapeador de Solicitações.

Definindo uma Expressão
Para definir símbolos, você deve usar expressões. O agente avalia as expressões para designar valores para símbolos.

Usando dados em uma expressão
Uma expressão pode usar os dados a seguir:

- Os símbolos de dados de entrada para o tipo de solicitação
- Outros símbolos descritos na mesma definição do mapeador de solicitação
- Constantes numéricas
- Constantes de sequência (delimitadas com ", por exemplo, "string")
- Constantes booleanas (true, TRUE, false, FALSE)
- A constante null

Para obter mais informações sobre símbolos de dados de entrada, consulte Tabela 234 na página 914.

Se o valor de um símbolo for uma instanciação de uma classe Java, as expressões poderão conter referências a campos e métodos que estão definidos na classe. Para se referir a um campo, use *symbol.fieldname*. Para se referir a um método, use *symbol.methodname*(*parameters*). A chamada de método deve retornar um valor. Por exemplo, é possível usar os métodos de sequência Java com um símbolo que tenha um valor de Sequência.

Para se referir a um campo estático ou um método de uma classe, também é possível usar *classname.fieldname* e *classname.methodname*(*parameters*).

Se um símbolo se referir a um objeto de matriz, a expressão poderá selecionar um elemento (*symbol*[*selector*]) e determinar o comprimento da matriz (*symbol*.length)

Operadores

É possível usar os operadores a seguir em uma expressão:

- Operadores booleanos: AND, &, OR, |, NOT, !
- Comparação: ==, !=, GT, >, LT, <, GE, >=, LE, <=
- Operadores numéricos: +, -, *, /
- Parênteses para forçar a ordem de avaliação: (,)

Importante: Você deve escapar os símbolos <, > e & em XML. Alternativamente, é possível usar os operadores GT (maior que), GE (maior ou igual), LT (menor que), LE (menor ou igual) e AND.

A expressão pode avaliar se um valor é uma instância de uma classe, usando o operador `instanceof`:

```
expression instanceof java.class.name
```

Este operador, semelhante ao operador Java `instanceof`, produz um valor booleano. Nesse exemplo, o valor é true se a classe à qual o valor *expression* pertence atenda qualquer uma das condições a seguir:

- Chama-se *java.class.name*
- É uma subclasse direta ou indireta da classe identificada por *java.class.name*.
- Implementa, direta ou indiretamente, a interface identificada por *java.class.name*.

A expressão também pode instanciar um novo objeto de uma classe Java, usando o operador new. Esse operador é semelhante ao operador Java new:

```
new java.class.name(expression1, expression2, ... expressionN)
```

Precedência do Operador
Os operadores são avaliados na ordem de precedência. Os operadores da mesma ordem de procedência são avaliados da esquerda para a direita. Você pode alterar a ordem de avaliação usando parênteses (e).

A ordem de precedência é como segue:

1. . operador (chamada de método ou referência de campo)
2. [ ] (seletor de elemento de matriz)
3. new
4. !, NOT
5. *, /
6. +, -
7. GT, >, LT, <, GE, >=, LE, <=, instanceof
8. ==, !=
9. AND, &
10. OR, |

Exemplo

```
$s1 >= ( 2 * ($s2.sampMethod($s3, true) + 1))
```

O agente avalia essa expressão da maneira a seguir:

1. O símbolo $s1 é avaliado. Ele deve dar um valor numérico.
2. O símbolo $s2 é avaliado. Ele deve produzir um objeto Java.
3. O símbolo $s3 é avaliado.
4. O método sampMethod para o objeto que resulta da avaliação de $s2 é chamado. O resultado da avaliação de $s3 é passado como o primeiro parâmetro, e o valor booleano true é passado como o segundo parâmetro. A chamada para sampMethod deve retornar um valor numérico.
5. 1 é incluído no resultado da etapa “4” na página 902.

6. O resultado da etapa “5” na página 902 é multiplicado por 2.
7. O resultado da etapa “1” na página 902 é comparado com o resultado da etapa “6” na página 903. Se o resultado da etapa “1” na página 902 for maior ou igual ao resultado da etapa “6” na página 903, será retornado `true`. Caso contrário, `false` será retornado.

Definindo Símbolos Básicos
Para definir símbolos, você deve usar expressões. O agente avalia as expressões para designar valores para símbolos.

Na tag <symbol>, use as seguintes tags:

<nome>
O nome do símbolo. É uma sequência e deve iniciar com o caractere $.

<eval>
A expressão que o agente deve avaliar para produzir o valor para este símbolo. Para obter mais informações sobre expressões, veja “Definindo uma Expressão” na página 901.

<type>
O tipo do valor retornado pelo símbolo. Especifique este valor como um nome completo de classe Java ou uma primitiva Java. A especificação do tipo do símbolo é opcional. Se não estiver definido, o mapeador de solicitação tenta estabelecer o tipo de campo com base na expressão. Se o mapeador de solicitação não puder determinar o tipo de símbolo antes de avaliar a expressão, o desempenho será afetado. Portanto, para obter melhor desempenho, é melhor especificar o tipo.

<args>
Os argumentos para o símbolo. Essa tag é opcional; se for especificada, deverão ser fornecidos argumentos para avaliar o símbolo. Para obter mais informações, consulte “Definindo argumentos símbolo” na página 903.

Exemplo

```
<symbol>
   <name>$doubles1</name>
   <eval>$s1*2</eval>
   <type>int</type>
</symbol>
```

Esse símbolo retorna o dobro do valor de outro símbolo, `$s1`.

Definindo argumentos símbolo
Na tag <args> de uma definição de símbolo, é possível definir tipos de argumentos para o símbolo.

Nessa tag, use a tag <type> para especificar os tipos de argumentos. Especifique este valor como um nome completo de classe Java ou uma primitiva Java. É possível especificar qualquer número de tags <type>; cada uma dessas tags define um argumento.

Neste caso, o símbolo deve ser referenciado com argumentos entre parênteses:

```
$symbol(argumento1,argument2...)
```

O número de argumentos deve ser igual ao número de definições de tipos de argumentos.

Na definição do símbolo, refira-se ao primeiro argumento como `$p0`, o segundo argumento como `$p1`, e assim por diante.

Um símbolo com argumentos funciona como um método Java. Ele usa argumentos de entrada e retorna um valor que depende dos valores dos argumentos.

Exemplo

```
<symbol>
   <name>$double</name>
   <eval>$p0*2</eval>
   <type>int</type>
```

```
    <args>
        <type>int</type>
    </args>
 </symbol>
```

Esse símbolo retorna o dobro do valor do argumento. Para avaliá-lo, forneça um argumento numérico: `$double(2)`, `$double($s1)`.

Definindo Símbolos de Iteração
Na tag <symbolDefinitions>, é possível definir um símbolo de iteração usando a tag <iterationSymbol>. Um símbolo de iteração representa um valor adquirido iterando por meio de um conjunto de objetos em uma matriz, enumeração ou coleção Java. Para cada um dos membros, o mapeador de solicitação avalia uma ou mais expressões de condições. Se uma expressão retornar `true`, o mapeador de solicitação usará o membro para calcular o valor de retorno. Quando um membro atende à expressão de condição, o mapeador de solicitação não avalia o restante dos membros.

Na tag <iterationSymbol>, use as tags a seguir.

<nome>
O nome do símbolo. É uma sequência e deve iniciar com o caractere $.

<type>
O tipo do valor retornado pelo símbolo. Especifique esse valor como um nome de classe Java completo ou como uma primitiva Java. A especificação do tipo do símbolo é opcional. Se não estiver definido, o mapeador de solicitação tenta estabelecer o tipo de campo com base na expressão. Se o mapeador de solicitação não puder determinar o tipo de símbolo antes de avaliar a expressão, o desempenho será afetado. Portanto, para obter melhor desempenho, é melhor especificar o tipo.

<args>
Os argumentos para o símbolo. Essa tag é opcional; se for especificada, deverão ser fornecidos argumentos para avaliar o símbolo. Para obter mais informações, consulte "Definindo argumentos símbolo" na página 903.

<iterate over="*expression*">
Define o objeto (matriz, Enumeração, ou Coleta) que contém os membros para iterar através de. A expressão deve retornar um objeto desse tipo. O mapeador de solicitação itera com seus membros até que um deles faça com que uma expressão de condição retorne `true` ou nenhum outro membro permaneça. Defina o conjunto de expressões de iteração em tags dentro desta tag:

<test>
Defina a condição e a expressão de retorno nesta tag. Uma tag <iterate> pode conter várias tags <test>. Neste caso, o mapeador de solicitação avalia todos eles. Se qualquer expressão de condição for verdadeira, o símbolo retorna um valor usando a expressão de resultado no mesmo tag <test>, e nenhuma avaliação adicional é executada.

<castTo>
Opcional: Se essa tag estiver presente, especifique o nome de um tipo Java dentro dele, como um nome de classe Java completo ou como uma primitiva Java. O mapeador de solicitação efetua cast do elemento iterado para este tipo antes que ele avalie a condição e retorne expressões. Se essa tag não estiver presente, o mapeador de solicitação efetuará cast de um membro de uma matriz para o tipo base de matriz e um membro de uma enumeração ou coleção para `java.lang.Object`. Para um membro de matriz, o tipo base de matriz geralmente será a opção correta; portanto, use essa tag para que o mapeador de solicitação iteraja em uma enumeração ou coleção.

<condition>
Uma expressão que deve produzir um valor booleano. Use `$iterElement` para referir-se ao elemento que está sendo iterado.

<return>
Se a expressão na tag <condition> retornar `true`, o mapeador de solicitação avaliará a expressão na tag <return>. O símbolo de iteração retornará o valor produzido por essa expressão. Use `$iterElement` para referir-se ao elemento que está sendo iterado.

<defaultValue>
Opcional. Se o mapeador de solicitação tiver iterado em todos os membros do objeto, mas nenhuma expressão de condição tiver retornado `true`, o mapeador de solicitação avaliará a expressão na tag <defaultValue>. O símbolo de iteração retorna o valor que a expressão produz. Se essa tag não estiver presente, o valor padrão será `null`.

Exemplos

```
<iterationSymbol>
  <name>$userNameCookieValue</name>
  <iterate over="$httpServletRequest.getCookies()">
     <test>
        <condition>$iterElement.getName().equals("userName")</condition>
        <return>$iterElement.getValue()</return>
     </test>
   </iterate>
</iterationSymbol>
```

Esse símbolo localiza o cookie denominado "username" e retorna seu valor. `$httpServletRequest.getCookies()` retorna uma matriz, portanto não há necessidade para o elemento <castTo>.

```
<iterationSymbol>
  <name>$headerNameStartingWithA</name>
  <iterate over="$httpServletRequest.getHeaderNames()">
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.startsWith("A")</condition>
       <return>$iterElement</return>
    </test>
  </iterate>
</iterationSymbol>
```

Esse símbolo localiza o cabeçalho com um nome começado com "A" e retorna seu nome. `$httpServletRequest.getHeaderNames()` retorna uma Enumeração, portanto, o elemento <castTo> é necessário.

```
<iterationSymbol>
  <name>$determined_gender</name>
  <iterate over="$children">
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.equals("male")</condition>
       <return>"It's a boy"</return>
    </test>
    <test>
       <castTo>java.lang.String</castTo>
       <condition>$iterElement.equals("female")</condition>
       <return>"It's a girl"</return>
    </test>
  </iterate>
  <defaultValue>"unknown"</defaultValue>
</iterationSymbol>
```

Esse símbolo itera por `$children`, que deve ser uma matriz, uma Enumeração ou uma Coleção de sequências. Se alguma das sequências for igual a "male", ela retornará "it's a boy". Se alguma das sequências for igual a "female", ela retornará "it's a girl". Por fim, se nenhuma sequência no objeto `$children` for igual a "male" ou "female", o símbolo retornará "unknown".

Definindo Símbolos Condicionais
Na tag <symbolDefinitions>, você pode definir um símbolo condicional usando a tag <conditionalSymbol>. Um símbolo condicional representa um valor que é adquirido por avaliação de uma série de expressões de condição. Se qualquer expressão retornar `true`, o mapeador de solicitação usará o membro para calcular o valor de retorno. Quando um membro satisfaz a expressão de condição, o mapeador de solicitação avalia uma expressão de retorno correspondente e retorna o resultado. Depois que o mapeador de solicitação localiza um resultado para retornar, ele não avalia nenhuma expressão posterior.

No tag <conditionalSymbol>, use os tags a seguir.

<nome>
O nome do símbolo. É uma sequência e deve iniciar com o caractere $.

<type>
O tipo do valor retornado pelo símbolo. Especifique este valor como um nome completo de classe Java ou uma primitiva Java. A especificação do tipo do símbolo é opcional. Se não estiver definido, o mapeador de solicitação tenta estabelecer o tipo de campo com base na expressão. Se o mapeador de solicitação não puder determinar o tipo de símbolo antes de avaliar a expressão, o desempenho será afetado. Portanto, para obter melhor desempenho, é melhor especificar o tipo.

<args>
Os argumentos para o símbolo. Essa tag é opcional; se for especificada, deverão ser fornecidos argumentos para avaliar o símbolo. Para obter mais informações, consulte "Definindo argumentos símbolo" na página 903.

<if condition="*expression*">
O atributo `condição` define uma expressão de condição para avaliar. A expressão deve produzir um valor Booleano. Se o valor for `true`, o mapeador de solicitação usará o conteúdo da tag <if> para tentar determinar o valor de retorno. O tag <if> deve conter um, mas não ambos, do conteúdo a seguir:

- Um tag <return>. Este tag contém uma expressão. Se a expressão de condição for true, o mapeador de solicitação avaliará a expressão e retornará o resultado.
- Qualquer número de tags <if>, aninhado dentro desse tag <if>. Se a expressão de condição for true, o mapeador de solicitação processará as tags <if> aninhadas da mesma forma que a tag <if> de nível superior. Ou seja, ele avalia a expressão no atributo `condição`, e se a expressão for true, usa o conteúdo do tag para tentar determinar o valor de retorno.

Importante: Se um valor de retorno estiver determinado, o mapeador de solicitação não avaliará nenhuma expressão adicional. No entanto, se uma expressão de condição em uma tag <if> for true, mas contiver tags <if> aninhadas e nenhuma das expressões de condição for true, nenhum valor será determinado. Neste caso, o mapeador de solicitação continua avaliando expressões subsequentes.

<defaultValue>
Opcional. Se o mapeador de solicitação tiver avaliado todas as expressões de condição, mas nenhuma das expressões de condição retornou `true`, o mapeador de solicitação avaliará a expressão na tag <defaultValue>. O símbolo condicional retorna o valor que a expressão produz. Se essa tag não estiver presente, o valor padrão será `null`.

Exemplo

```
<symbol>
  <name>$GET</name>
  <eval>"GET"</eval>
</symbol>
<symbol>
  <name>$PUT</name>
  <eval>"PUT"</eval>
</symbol>
<conditionalSymbol>
  <name>$sessionAttribute</name>
  <if condition="$httpServletRequest.getSession(false) != null>
     <if condition="$httpServletRequest.getSession(false).getAttribute($GET)
!= null">
       <return>$httpServletRequest.getSession(false).getAttribute($GET)</return>
     </if>
     <if condition="true">
       <return>$httpServletRequest.getSession(false).getAttribute($PUT)</return>
      </if>
  </if>
</conditionalSymbol>
```

Este símbolo é assumido como sendo parte do mapeador de solicitação de servlet. Primeiro, ele verifica se uma sessão de HTTP existe para o servlet; se não existir, o símbolo retorna `null`. Se uma sessão estiver presente, o símbolo verificará se o servlet tem um atributo GET, e retornará o valor desse atributo.

Caso contrário, ele retornará o valor do atributo PUT. A segunda expressão de condição é true; esse valor é usado como uma cláusula else. Se a primeira condição for true, o mapeador de solicitações não avaliará nenhuma expressão adicional; caso contrário, ele continuará com a segunda expressão.

Definindo Símbolos de Classe Externos
Na tag <symbolDefinitions>, você pode definir uma classe externa usando a tag <externalClassSymbol>. Um símbolo da classe externa representa uma classe Java externa. A definição do símbolo de classe externa é opcional; é possível usar classes Java externas em expressões diretamente. No entanto, ele pode aprimorar a leitura da configuração do mapeador de solicitação.

Na tag <externalClassSymbol>, use as tags a seguir.

<nome>
O nome do símbolo. É uma sequência e deve iniciar com o caractere $.

<className>
O nome da classe definida pelo cliente.

Importante: Para se referir a qualquer classe Java na configuração do mapeador de solicitação, se em uma definição de símbolo de classe externa ou em qualquer expressão, você deve incluir o caminho e o nome completos do arquivo JAR que contém a classe na tag <requestMapperClassPath> dentro da tag <runtimeConfiguration>.

Após definir um símbolo externo, você pode encaminhar a classe com o nome do símbolo. Também é possível se referir a métodos estáticos e campos da classe usando o símbolo.

Exemplo

```
<externalClassSymbol>
  <name>$rand</name>
  <className>user.class.Random</className>
</externalClassSymbol>
```

Esse símbolo refere-se a uma classe gravada pelo usuário, gerando um número aleatório. O caminho e nome completos do arquivo JAR que contém essa classe devem estar presentes na tag <requestMapperClassPath> dentro da tag <runtimeConfiguration>.

Para se referir ao método estático `user.class.Random.generate()` em uma expressão, é possível usar o símbolo externo:

```
$rand.generate()
```

Mapeando Valores para Chaves de Contexto
Na tag <requestMapperDefinition>, mapeie valores para chaves de contexto usando a tag <selection>. Esse de mapeamento fornece as mudanças nas informações de monitoramento.

É possível mapear valores para as chaves de saída definidas para o tipo de solicitação. Para obter mais informações, consulte Tabela 233 na página 912.

Se nenhum valor for mapeado para uma chave após a avaliação da configuração do mapeador de solicitações o ITCAM usará o valor original extraído da solicitação.

Na tag <selection>, use as tags a seguir.

<matchCriteria>
Uma expressão que deve retornar um valor booleano. O mapeamento que está definido nesta tag só será usado se essa expressão retornar `true`.

<mapTo>
Define uma chave e o valor a ser mapeado para ele. Nessa tag, uma tag <key> contém a chave, e uma tag <value> contém o valor.

<selection>
É possível aninhar tags <selection> colocando uma dentro da outra.

Se tags <selection> forem aninhadas, o mapeamento aninhado será usado apenas se ambas as expressões <matchCriteria>, externa e aninhada, retornarem `true`.

Você pode usar várias tags <selection> dentro de um tag <requestMapperDefinition> ou dentro de outra tag <selection>. Se a mesma chave for mapeada diversas vezes vezes em diversas tags <selection> no mesmo nível de aninhamento, (ou seja, dentro da mesma ta pai), então o primeiro mapeamento para o o qual a expressão <matchCriteria> for retornada como `true` será usado.

Não mapeie a mesma chave em ambas as tags <selection>, externa e aninhada.

Normalmente, use o valor <matchCriteria> de `true` como um valor "else" para a última tag de seleção em um nível de aninhamento. Se você deseja mapear valores diferentes em diferentes casos, utilize vários tags <selection> dentro desse tag externo; cada um deles pode conter os critérios e valores para um caso específico. O último tag, com um valor de `true`, abrange o caso quando os dados disponíveis não atenderem nenhum dos critérios.

Exemplos

```
<selection>
   <matchCriteria>true</matchCriteria>
   <mapTo>
      <key>Result</key>
      <value>$s1</value>
   </mapTo>
</selection>
```

Nessa configuração de mapeamento, `Result` é configurado com o valor do símbolo `$s1`.

```
<matchCriteria>true</matchCriteria>
   <selection>
      <matchCriteria>$b1</matchCriteria>
      <mapTo>
         <key>Result</key>
         <value>1</value>
      </mapTo>
   </selection>
   <selection>
      <matchCriteria>true</matchCriteria>
      <mapTo>
         <key>Result</key>
         <value>2</value>
      </mapTo>
</selection>
```

Nessa configuração de mapeamento, o símbolo $b1 deve retornar um valor booleano. `Result` será configurado como 1 se $b1 retornar `true`, e como 2 se $b1 retornar `false`. Se $b1 retornar `true`, o mapeador de solicitação usará o mapeamento para `Result` na primeira tag <selection>; o mapeamento para a mesma chave na segunda tag não será usado.

Definindo Pedidos Customizados

Por padrão, apenas certos tipos de classes e métodos Java são monitorados como solicitações pelo coletor de dados. Servlets, JSPs, métodos de negócios EJB e determinadas APIs Java EE padrão são reconhecidos como solicitações. É possível designar classes extras e métodos como *solicitações customizadas*.

Sobre Esta Tarefa

Para ativar o monitoramento de solicitações customizadas pelo coletor de dados, defina as solicitações customizadas em um arquivo XML e configure a propriedade `am.camtoolkit.gpe.customxml.custom` no arquivo de propriedades customizadas do kit de ferramentas.

Por exemplo, o coletor de dados não reconhece as classes Ação do Struts como solicitações, por padrão. No entanto, é possível configurar definições de solicitação customizadas e fazer com que as ações sejam reconhecidas como Solicitações Aninhadas.

Procedimento

Conclua o seguinte procedimento para ativar o monitoramento de solicitações customizadas e designar um ou mais métodos como solicitações customizadas:

1. Faça uma cópia do arquivo *dc_home*/itcamdc/etc/custom_requests.xml em um local temporário. Em seguida, abra a cópia em um editor de texto.
2. Modifique os parâmetros no arquivo.

   A tabela a seguir descreve os parâmetros que podem ser modificados:

Tabela 232. Parâmetros para o arquivo de configuração de pedidos customizados

Nome da Tag	Descrição
edgeRequest	Identifica um ou mais métodos de aplicativo que serão Instrumentados por Código de Byte para processamento de pedido customizado. Modificando as tags requestName, Matches, type e methodName dentro da tag edgeRequest, você pode customizar a seleção. Cada tag edgeRequest deve conter exatamente uma tag methodName e uma ou mais tags Matches. Várias tags edgeRequest podem ser especificadas.
requestName	Define um nome exclusivo para este pedido. O nome da solicitação é exibido para o usuário quando a entrada e a saída de método são rastreadas.
Matches	Identifica uma ou mais classes que contêm os métodos que serão Instrumentados por Código de Byte para processamento de pedido customizado. Várias tags Matches podem ser apresentadas dentro de uma única tag edgeRequest.
type	Indica se uma classe deve ser uma classe de sistema ou aplicativo para corresponder à tag edgeRequest.
methodName	Identifica os nomes dos métodos dentro de uma das classes identificadas pela tag Matches que devem ser instrumentadas por bytecode para processamento de solicitação customizada. Exatamente uma tag methodName pode ser especificada em cada tag edgeRequest.
requestMapper	Opcional. Se essa tag for especificada, o coletor de dados usará um mapeador de solicitações para determinar informações que identifiquem a solicitação. É possível definir maneiras não padrão de extrair essas informações. Para obter mais informações sobre como ativar e definir mapeadores de solicitações, consulte "Customizando o Mapeamento de Informações da Solicitação" na página 900.

Lembre-se: As tags Matches e methodName podem incluir caracteres curinga. Como os caracteres curingas funcionam está descrito a seguir:

- O asterisco (*) representa zero ou mais ocorrências de qualquer caractere quando utilizado sozinho. Quando integrado a uma sequência de caracteres (por exemplo, java.*.String), corresponde zero ou mais ocorrências de qualquer caractere, exceto o separador de pacote (.).
- Dois pontos (..) podem ser usados para especificar todos os subpacotes. Corresponde qualquer sequência de caracteres que inicia e termina com o separador de pacote (.). Por exemplo, java..String corresponde a java.lang.String e com.ibm..* corresponde a qualquer declaração começando com com.ibm.

Por exemplo, um aplicativo com um pacote denominado com.mycompany.myapp tem os seguintes requisitos:

- Na classe Cliente, o método creditCheck() deve ser tratado como uma solicitação customizada denominada CreditCheck.
- Na classe Fornecedor, o método inventoryCheck() deve ser tratado como uma solicitação customizada chamada SupplyCheck.

O conteúdo do arquivo `custom_requests.xml` customizado que atende aos requisitos é o seguinte:

```
<customEdgeRequests>
      <edgeRequest>
              <requestName>CreditCheck</requestName>
              <Matches>com.mycompany.myapp.Customer</Matches>
              <type>application</type>
              <methodName>creditCheck</methodName>
      </edgeRequest>
      <edgeRequest>
              <requestName>SupplyCheck</requestName>
              <Matches>com.mycompany.myapp.Supplier</Matches>
              <type>application</type>
              <methodName>inventoryCheck</methodName>
      </edgeRequest>
</customEdgeRequests>
```

3. Execute uma das seguintes etapas:
   - Salve o arquivo no diretório *dc_home*/runtime/*app_server_version*.*node_name*.*profile_name*.*server_name*/custom. Em seguida, no arquivo de propriedades customizadas do kit de ferramentas, configure a propriedade `am.camtoolkit.gpe.customxml.custom` com o nome (sem o caminho) do arquivo modificado na Etapa "2" na página 909.
   - Salve o arquivo em qualquer diretório do computador. Em seguida, no arquivo de propriedades customizadas do kit de ferramentas, configure a propriedade `am.camtoolkit.gpe.customxml.custom` com o caminho e o nome do arquivo que modificou na Etapa "2" na página 909.

   Para obter mais informações sobre o arquivo de propriedades customizadas do kit de ferramentas, consulte "Arquivo de propriedades do kit de ferramentas" na página 891.

Ativando um mapeador de solicitações

Para ativar um mapeador de solicitações para um tipo de solicitação, edite o arquivo de configuração customizada do kit de ferramentas ou o arquivo de configuração customizada global do kit de ferramentas. Procedimentos são diferentes para tipos de solicitações comuns e para solicitações customizadas.

Antes de Iniciar

Defina a configuração do mapeador de solicitação em um arquivo XML. Em seguida, coloque o arquivo XML que contém configuração do mapeador de solicitação no mesmo diretório do arquivo de propriedades do kit de ferramentas.

- Para ativar o mapeador de solicitação para todas as instâncias do servidor de aplicativos, insira-o no diretório *dc_home*/runtime/custom.
- Para ativar o mapeador de solicitação para uma instância do servidor de aplicativos, insira-o no diretório *dc_home*/runtime/*appserver_version*.*node_name*.*profile_name*.*server_name*/custom/.

Para obter informações sobre a sintaxe do arquivo XML, consulte "Sintaxe do Arquivo XML" na página 900.

Sobre Esta Tarefa

Edite o arquivo `toolkit_custom.properties` ou o arquivo `toolkit_global_custom.properties` para ativar o mapeador de solicitação para uma ou todas as instâncias do servidor de aplicativos.

Procedimento

- Para ativar um mapeador de solicitação para solicitações comuns, conclua as seguintes etapas:
  a) Em um editor de texto, abra um dos arquivos de configuração customizados do kit de ferramentas a seguir:

- Para ativar o mapeador de solicitações para todas as instâncias do servidor de aplicativos, abra o arquivo *dc_home*/runtime/custom/toolkit_global_custom.properties.
- Para ativar o mapeador de solicitações para uma instância do servidor de aplicativos, abra o arquivo *dc_home*/runtime/*appserver_version.node_name.profile_name.server_name*/custom/toolkit_custom.properties.

b) Edite o arquivo de propriedades do kit de ferramentas como a seguir:

- Inclua uma linha configurando a propriedade de ativação para esse tipo de solicitação como `true`. Para obter mais informações, consulte Tabela 233 na página 912.
- Inclua uma linha configurando a propriedade `am.camtoolkit.gpe.customxml.*` no nome do arquivo XML do mapeador. Use qualquer valor exclusivo em vez do símbolo *. Para obter mais informações, consulte "Sintaxe do Arquivo XML" na página 900.

c) Salve e feche o arquivo de propriedades.

Exemplo:

Para ativar um mapeador de solicitações que esteja definido em `renameDataSource.xml` para o tipo de solicitação SQL, inclua as seguintes linhas no arquivo de configuração customizada do kit de ferramentas ou no arquivo de configuração customizada global do kit de ferramentas:

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=renameDataSource.xml
```

- Para ativar um mapeador de solicitação para solicitações customizadas, conclua as seguintes etapas:

a) Na tag <edgerequest> no arquivo XML de definição de solicitação customizada, crie uma tag <requestMapper>. Coloque um nome de tipo de mapa de solicitação exclusivo nessa tag. Para obter informações sobre como definir solicitações customizadas, consulte "Definindo Pedidos Customizados" na página 908.

b) No arquivo XML do mapeador de solicitação, utilize o nome de tipo de mapa de solicitação exclusivo no atributo `type` da tag <requestMapperDefinition>.

c) Em um editor de texto, abra um dos arquivos de configuração customizados do kit de ferramentas a seguir:

- Para ativar o mapeador de solicitações para todas as instâncias do servidor de aplicativos, abra o arquivo *dc_home*/runtime/custom/toolkit_global_custom.properties.
- Para ativar o mapeador de solicitações para uma instância do servidor de aplicativos, abra o arquivo *dc_home*/runtime/*appserver_version.node_name.profile_name.server_name*/custom/toolkit_custom.properties.

d) Edite o arquivo de propriedades do kit de ferramentas para incluir uma linha configurando a propriedade `am.camtoolkit.gpe.customxml.*` para o nome do arquivo XML do mapeador. Use qualquer valor exclusivo em vez do símbolo *. Para obter mais informações, consulte "Sintaxe do Arquivo XML" na página 900.

e) Salve e feche o arquivo de propriedades.

Exemplo:

Para ativar um mapeador de solicitação que é definido no `customMapper.xml` para o tipo de solicitação customizado `SupplyCheck` definido no arquivo `custom_requests.xml`, conclua as seguintes etapas:

1. Use a definição a seguir no arquivo `custom_requests.xml`:

```
<customEdgeRequests>
  <edgeRequest>
    <requestName>SupplyCheck</requestName>
    <Matches>com.mycompany.myapp.Supplier</Matches>
    <type>application</type
    <methodName>inventoryCheck</methodName>
    <requestMapper>customMapper</requestMapper>
```

```
  </edgeRequest>
</customEdgeRequests>
```

2. No arquivo `customMapper.xml`, certifique-se de que o nome de tipo seja configurado:

```
<requestMapperDefinition type="customMapper">
```

3. Inclua a seguinte linha no arquivo de configuração customizada do kit de ferramentas ou no arquivo de configuração customizada global do kit de ferramentas:

```
am.camtoolkit.gpe.customxml.customMapper=customMapper.xml
```

Mapeador de nomes de tipo de Solicitação, de dados entrada e de saída

As tabelas a seguir listam as informações necessárias para configurar e ativar mapeadores de solicitações para diferentes tipos de solicitações.

O significado de cada cabeçalho da tabela é explicado como a seguir:

Tipo de solicitação
O tipo da solicitação.

Propriedade de ativação
Para ativar o mapeador de solicitações, configure essa propriedade como `true` no arquivo `toolkit_custom.properties` ou `toolkit_global_custom.properties`.

Importante: Se você copiar esse valor da tabela, remova os espaços e as quebras de linha.

Nome do tipo do mapeador de solicitações
Designe esse valor ao atributo `type` da tag <requestMapperDefinition> no arquivo XML de definição do mapeador de solicitações.

Nomes de símbolos dos dados de entrada
Os símbolos que representam as informações de solicitação. É possível usar esses símbolos nas expressões dentro das definições do mapeador de solicitação. Para obter mais informações, consulte “Definindo uma Expressão” na página 901.

Chaves de contexto dos dados de saída
Para fornecer mudanças nas informações de monitoramento, designe valores a essas chaves na definição do mapeador de solicitações. Para obter mais informações, consulte “Mapeando Valores para Chaves de Contexto” na página 907.

Tabela 233. Propriedades de ativação e nomes de tipos do mapeador de solicitações

Tipo de solicitação	Propriedade de ativação	Nome do tipo do mapeador de solicitações
servlet	`com.ibm.tivoli.itcam.toolkit.ai.enable.servletrequestmapper`	`servlet`
JNDI	`com.ibm.tivoli.itcam.toolkit.ai.enable.jndirequestmapper`	`jndiLookup`
Pedido Customizado		Definido pelo usuário na definição edgeRequest
EJB	`com.ibm.tivoli.itcam.toolkit.ai.enable.ejbrequestmapper`	`ejb`
JCA	`com.ibm.tivoli.itcam.toolkit.ai.enable.jcarequestmapper`	`jca`
Origem de dados do JDBC	`com.ibm.tivoli.itcam.toolkit.ai.enable.datasourcerequestmapper`	`dataSource`

Tabela 233. Propriedades de ativação e nomes de tipos do mapeador de solicitações (continuação)

Tipo de solicitação	Propriedade de ativação	Nome do tipo do mapeador de solicitações
Instrução SQL JDBC	`com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper`	`sqlStatement`
JMS	`com.ibm.tivoli.itcam.toolkit.ai.enable.jmsrequestmapper`	`jms`
Serviço da web JAX-RPC	`com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper`	`webServices`
Serviço da Web do Axis	`com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper`	`webServices`
MQI	`com.ibm.tivoli.itcam.toolkit.ai.enable.mqrequestmapper`	`mqi`
EJB	`com.ibm.tivoli.itcam.toolkit.ai.enable.ejbrequestmapper`	`ejb`
JDBC Connection Factory	`com.ibm.tivoli.itcam.toolkit.ai.enable.sqlconnectfactoryrequestmapper`	`connectionFactory`
SCA	`com.ibm.tivoli.itcam.toolkit.ai.enable.scarequestmapper`	`sca`
Serviço da web JAX-WS	`com.ibm.tivoli.itcam.toolkit.ai.enable.webservicerequestmapper`	`webServices`
WebSphere Portal Server Portal (estendendo a classe `org.apache.jetspeed.portlet.Portlet`)	`com.ibm.tivoli.itcam.toolkit.ai.enable.portalrequestmapper`	`portalPortal`
WebSphere Portal Server versão 6.1, 7 e 8 Portal (implementando a interface `javax.portlet.Portlet`)	`com.ibm.tivoli.itcam.toolkit.ai.enable.portal6requestmapper`	`Portal6Portal`

Importante: Não há nenhuma maneira significativa de configurar o mapeador de solicitações customizado para os tipos de solicitação que não estão listados em Tabela 233 na página 912.

Tabela 234. Dados de entrada e saída do mapeador de solicitações

Tipo de solicitação	Nomes de símbolos dos dados de entrada	Chaves de contexto dos dados de saída
servlet	Para obter mais informações, consulte Tabela 235 na página 918.	**remappedURI** define um URI renomeado **remappedURL** define um URL renomeado **appName** define um nome de aplicativo renomeado **userid** define o ID do usuário para a solicitação
JNDI	• **$jndiContext** o objeto de contexto • **$lookup** a sequência de consulta • **$context** "JNDIlookup"	**renamedLookup** define uma sequência de consulta renomeada
Pedido Customizado	• **$this** o objeto ‘this' para o método de solicitação customizada • **$0** os argumentos passados para o método de solicitação customizada, especificados como uma matriz de objetos • **$className** o nome da classe de solicitação customizada • **$methodName** o nome do método de solicitação customizada • **$context** o nome da solicitação original da definição edgeRequest	**customRequestName** define o nome da solicitação customizada renomeada
EJB	• **$ejb** o objeto de implementação EJB • **$appName** o nome do aplicativo • **$ejbType** o tipo do EJB • **$className** o nome de classe do objeto de implementação EJB • **$methodName** o nome do método de negócios EJB • **$context** "EJBBusinessMethod"	**appName** define o nome do aplicativo renomeado **ejbType** define o tipo de EJB renomeado **className** define o nome de classe renomeada **methodName** define o nome do método renomeado
JCA	• **$interaction** o objeto Interação • **$interactionSpec** o objeto InteractionSpec • **$record** o objeto Registro • **$context** "J2Cexecute"	**lookupName** é o lookupName renomeado **productName** é o nome do produto renomeado **productVersion** é a versão do produto renomeada

Tabela 234. Dados de entrada e saída do mapeador de solicitações (continuação)

Tipo de solicitação	Nomes de símbolos dos dados de entrada	Chaves de contexto dos dados de saída
Origem de dados do JDBC	• **$this**, a origem de dados ou o objeto de driver • **$dataSource**, o objeto $this, cast como uma origem de dados • **$driver** o objeto $this, convertido como um Driver • **$dataSourceName** é o nome da origem de dados, como java.lang.String • **$context** indica o tipo de solicitação, "JDBCgetConnection" ou "JDBCgetConnection FromDriver"	**dataSourceName** é o nome da origem de dados renomeada, se o objeto $this for uma origem de dados **url** é a URL do Driver renomeado, se o objeto $this for um Driver
Instrução SQL JDBC	• **$this** ou a instrução SQL, ou o de Conexão SQL • **$sqlText** contém o texto SQL como java.lang.String, se o objeto $this for uma instrução SQL • **$sqlStatement** o objeto $this, cast como uma instrução SQL • **$sqlConnection** o objeto $this, cast como uma Conexão SQL • **$dataSourceName** o nome da origem de dados • **$context** indica o tipo de solicitação: "JDBCexecute", JDBCexecuteQuery", "JDBCexecuteUpdate", "JDBCcreateStatement", "JDBCprepareStatement"	**dataSourceName** é o nome da origem de dados renomeada **sqlText** é o texto SQL renomeado

Tabela 234. Dados de entrada e saída do mapeador de solicitações (continuação)

Tipo de solicitação	Nomes de símbolos dos dados de entrada	Chaves de contexto dos dados de saída
JMS	• **$this** o objeto 'this' do método instrumentado. Pode ser um QueueBrowser, MessageConsumer, MessageProducer ou MessageListener • **$0**, o objeto Queue, para uma solicitação de envio, ou um objeto de tópico, para uma solicitação de publicação • **$queueBrowser** o objeto $this, cast como um QueueBrowser • **$messageConsumer** o objeto $this, cast como um MessageConsumer • **$messageProducer** o objeto $this, cast como um MessageProducer • **$messageListener** o objeto $this, convertido como um MessageListener • **$queue**, o objeto $0, cast como uma fila • **$topic**, o objeto $0, cast como um tópico • **$context** indica o tipo de solicitação: "JMSreceive", "JMSsend", "JMSbrowse", "JMSpublish", "JMSonmessage"	**queueName** o nome da fila renomeada **providerURL** o provedor de URL renomeado **topicName** o nome do tópico renomeado
Serviço da web JAX-RPC	• **$messageContext** o IMessageContextWrapper • **$appName** o nome do aplicativo • **$requestName** o nome da solicitação padrão • **$url** a URL • **$context** indica o tipo de solicitação: "WebServicesJaxRpc ProviderRequest", "WebServicesJaxRpc ClientRequest"	**appName** o nome do aplicativo renomeado **requestName** o nome da solicitação renomeada **url** a URL renomeada
Serviço da Web do Axis	• **$messageContext** o IMessageContextWrapper • **$appName** o nome do aplicativo • **$requestName** o nome da solicitação padrão • **$url** a URL • **$context** indica o tipo de solicitação: "WebServicesAxisClient Request", "WebServicesAxis ProviderRequest"	**appName** o nome do aplicativo renomeado **requestName** o nome da solicitação renomeada **url** a URL renomeada

Tabela 234. Dados de entrada e saída do mapeador de solicitações (continuação)

Tipo de solicitação	Nomes de símbolos dos dados de entrada	Chaves de contexto dos dados de saída
MQI	• **$queue** o objeto MQQueue, se for conhecido • **$qmgr** o objeto MQQueueManager, se for conhecido • **$message** o objeto MQMessage ou MQMsg2, se for conhecido • **$session** o objeto MQSESSION, se for conhecido • **$getMsgOptions** o objeto MQGetMessageOptions, se for conhecido • **$qmgrName** o nome do gerenciador de filas • **$queueName** o nome da fila • **$context** o tipo de solicitação do MQ: "MQCONN", "MQCONNX", "MQDISC", "MQBACK", "MQBEGIN", "MQCLOSE", "MQCMIT", "MQINQ", "MQOPEN", "MQSET", "MQGET", "MQPUT", "MQPUT1", "MQGETBROWSE"	**qmgrName** o nome do gerenciador de filas renomeado **qname** o nome da fila renomeado
EJB	• **$appName** o nome do aplicativo • **$ejbType** o tipo do EJB • **$className** o nome de classe do objeto de implementação EJB • **$methodName** o nome do método de negócios EJB • **$context** "EJBBusinessMethod"	**appName** define o nome do aplicativo renomeado **ejbType** define o tipo de EJB renomeado **className** define o nome de classe renomeada **methodName** define o nome do método renomeado
JDBC Connection Factory	• **$connectionFactory** o ConnectionFactory • **$dataSourceName** o nome da origem de dados • **$context** "JDBCgetConnection"	**dataSourceName** é o nome da origem de dados renomeada
SCA	• **$uri** o URI • **$operationName** o nome da operação • **$context** indica o tipo de solicitação: "SCA_Generic", "SCA_Ref", "SCA_Target"	**uri** é o URI renomeado **operationName** é o nome da operação renomeada

Tabela 234. Dados de entrada e saída do mapeador de solicitações (continuação)		
Tipo de solicitação	**Nomes de símbolos dos dados de entrada**	**Chaves de contexto dos dados de saída**
Serviço da web JAX-WS	• **$messageContext** o IMessageContextWrapper • **$appName** o nome do aplicativo • **$requestName** o nome da solicitação padrão • **$url** a URL • **$context** indica o tipo de solicitação: "WebServicesJAXWS ClientRequest", "WebServicesJAXWS ProviderRequest", "WebServicesJAXWS AsyncRequest"	**appName** o nome do aplicativo renomeado **requestName** o nome da solicitação renomeada **url** a URL renomeada
WebSphere Portal Server Portal (estendendo o `org.apache.jetspeed.portlet.Portlet`)	• **$portletAdapter** PortletAdapter • **$portletRequest** PortletRequest • **$portletResponse** PortletResponse • **$portletName** Nome do portlet • **$pageTitle** Título da página • **$url** URL da solicitação • **$userid** ID do usuário da solicitação • **$context** "Portal.Portlet"	**portletName** o nome do portlet renomeado **title** o título de página renomeado **url** a URL renomeada **userid**, o ID de usuário renomeado
WebSphere Portal Server versão 6.1, 7 e 8 Portal (implementando a interface `javax.portlet.Portlet`)	• **$portlet** Portlet • **$renderRequest** RenderRequest • **$renderResponse** RenderResponse • **$portletName** Nome do portlet • **$pageTitle** Título da página • **$url** URL da solicitação • **$userid** ID do usuário da solicitação • **$context** "Portal.Portlet"	**portletName** O nome do portlet renomeado **title** O título da página renomeada **url** A URL renomeada **userid** O ID do usuário renomeado

É fornecido um número maior de símbolos de dados de entrada para solicitações de servlet.

Tabela 235. Nomes de símbolos de dados de entrada para solicitações de servlet		
Nome do Símbolo	**Tipo do Valor**	**Conteúdo do Símbolo**
$context	Sequência	"ServletMethod"
$servlet	javax.servlet.http.HttpServlet	O objeto HttpServlet associado à solicitação de servlet
$httpServletRequest	javax.servlet.http.HttpServletRequest	O objeto HttpServletRequest associada com a solicitação do servlet
$httpServletResponse	javax.servlet.http.HttpServletResponse	O objeto HttpServletResponse associada a solicitação do servlet
$svrName	java.lang.String	O nome do aplicativo associado ao servlet

Tabela 235. Nomes de símbolos de dados de entrada para solicitações de servlet (continuação)		
Nome do Símbolo	**Tipo do Valor**	**Conteúdo do Símbolo**
$URL	java.lang.StringBuffer	A URL usada pelo cliente para fazer a solicitação
$RemoteUser	java.lang.String	O nome de login do usuário que faz essa solicitação, se autenticada
$URI	java.lang.String	A parte da URL de solicitação do nome do protocolo até a sequência de consultas
$ServletPath	java.lang.String	A parte da URL de solicitação que chama o servlet.
$SessionID	javax.servlet.http.HttpSession	A sessão atual associada a esta solicitação
$QueryString	java.lang.String	A cadeia de consultas contida na URL de pedido após o caminho.
$SessionAttribute	java.lang.String	Este símbolo parametrizado retorna um valor de atributo de sessão. Ele possui um parâmetro, o nome do atributo (deve ser uma sequência). Por exemplo, `$SessionAttribute("attr1")` retorna o valor do atributo denominado attr1.
$cookie	javax.servlet.http.Cookie	Este símbolo com parâmetro retorna um cookie especificado. Ele possui um parâmetro, o nome do cookie (deve ser uma sequência). Por exemplo, `$cookie("cookie1")` retorna o valor do atributo denominado cookie1.

Exemplo de Definições do Mapeador de Solicitações
Os exemplos a seguir ilustram o uso da funcionalidade do mapeador de solicitações.

Alterando o Nome do Aplicativo de Servlet
Neste exemplo, o nome do aplicativo em uma solicitação do servlet é substituído pelo URI e pela sequência de consultas.

O arquivo *dc_home*`/runtime/changeAppname.xml` contém a seguinte definição do mapeador de solicitação:

```
<gpe>
   <runtimeConfiguration>
         <requestMapperDefinition type="servlet">
               <selection>
                     <matchCriteria>true</matchCriteria>
                     <mapTo>
                           <key>appName</key>
                           <value>$URI + “.” + $QueryString</value>
                     </mapTo>
               </selection>
         </requestMapperDefinition>
```

```
   </runtimeConfiguration>
</gpe>
```

Renomeando uma Origem de Dados
Neste exemplo, o nome da origem de dados em uma solicitação SQL é alterado para uma versão que um usuário possa entender mais facilmente.

O arquivo *dc_home*/runtime/renameDataSource.xml contém a seguinte definição do mapeador de solicitação:

```
<gpe>
 <runtimeConfiguration>
   <requestMapperDefinition type=”sqlStatement”>
      <selection>
         <matchCriteria>$dataSourceName != null</matchCriteria>
         <selection>
           <matchCriteria>$dataSourceName.equals("jdbc/TradeDataSource")
</matchCriteria>
           <mapTo>
             <key>dataSourceName</key>
             <value>"Daytrader Data Source"</value>
           </mapTo>
         </selection>
         <selection>
           <matchCriteria>$dataSourceName.equals("jdbc/LongDataSource")
</matchCriteria>
           <mapTo>
             <key>dataSourceName</key>
             <value>"Long term trader Data Source"</value>
           </mapTo>
         </selection>
      </selection>
   </requestMapperDefinition>
 </runtimeConfiguration>
<gpe>
```

A primeira tag <selection> assegura que $dataSourceName não seja nulo. Depois, a seguinte tag <selection> pode avaliar com segurança $dataSourceName.equals().

Se a primeira tag <selection> não estivesse presente e um $dataSourceName nulo tivesse sido passado, o mapeador de solicitações iria gerar uma exceção. Uma exceção desse tipo poderia resultar na ausência de informações de monitoramento.

Para ativar este mapeador de solicitação, o arquivo *dc_home*/runtime/toolkit_global_custom.properties contém as seguintes linhas:

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=renameDataSource.xml
```

Removendo Informações Sigilosas de uma Solicitação SQL
Neste exemplo, um aplicativo inclui números de segurança social em solicitações SQL. O mapeador de solicitações remove os números da versão da solicitação que o usuário pode ver.

Nas solicitações SQL, o número de previdência social é listado com o nome da coluna SS, SS = *number*. O mapeador de solicitações procura a sequência SS = e remove os nove símbolos após ela.

O arquivo *dc_home*/runtime/removeSSN.xml contém a seguinte definição do mapeador de solicitação:

```
<gpe>
    <runtimeConfiguration>
         <requestMapperDefinition type="sqlStatement">
             <symbolDefinitions>
                 <symbol>
                     <name>$offsetOfSS</name>
                     <eval>$sqlText.indexOf("SS = ")</eval>
                 </symbol>
                 <symbol>
                     <name>$sqlTextContainsSS</name>
<eval>$sqlText != null E $offsetOfSS > 0 AND $sqlText.length() GE
$offsetOfSS+16</eval>
                 </symbol>
```

```
                <conditionalSymbol>
                    <name>$sqlTextPriorToSSKeyword</name>
                    <type>java.lang.String</type>
                    <defaultValue>""</defaultValue>
                    <if condition="$sqlTextContainsSS">
                      <return>$sqlText.substring(0, $offsetOfSS+5)</return>
                    </if>
                </conditionalSymbol>
                <conditionalSymbol>
                    <name>$sqlTextAfterSS</name>
                    <type>java.lang.String</type>
                    <defaultValue>""</defaultValue>
                    <if condition="$sqlTextContainsSS">
                      <return>$sqlText.substring($offsetOfSS+16)</return>
                    </if>
                </conditionalSymbol>
            </symbolDefinitions>
            <selection>
                 <matchCriteria>$sqlText != null AND $sqlText.length() >
0</matchCriteria>
                 <selection>
                      <matchCriteria>$sqlTextContainsSS</matchCriteria>
                      <mapTo>
                           <key>sqlText</key>
                           <value>$sqlTextPriorToSSKeyword + "?" +
$sqlTextAfterSS</value>
                      </mapTo>
                 </selection>
            </selection>
        </requestMapperDefinition>
    </runtimeConfiguration>
</gpe>
```

Para ativar este mapeador de solicitação, o arquivo *dc_home*/runtime/toolkit_global_custom.properties contém as seguintes linhas:

```
com.ibm.tivoli.itcam.toolkit.ai.enable.sqlrequestmapper=true
am.camtoolkit.gpe.customxml.renameDataSource=removeSSN.xml
```

Configurando o WebSphere Applications agent para monitorar o WebSphere Extreme Scale

Após instalar o WebSphere Applications agent, é possível fazer uma configuração extra para monitorar o WebSphere Extreme Scale (WXS) em um ambiente WebSphere Application Server ou independente.

Sobre Esta Tarefa

As etapas de configuração serão diferentes, dependendo do modo de instalação do WebSphere Extreme Scale e se a segurança estiver ativada. Execute as etapas a seguir antes de executar o processo de configuração.

Procedimento

1. Confirme o modo de instalação do WebSphere Extreme Scale.

   Modo independente
   O WebSphere Extreme Scale é instalado em um ambiente que não possui o WebSphere Application Server.

   Modo WAS integrado
   O WebSphere Extreme Scale é instalado em um ambiente WebSphere Application Server.
2. Confirme se a segurança está ativada para o WebSphere Extreme Scale. Se um cliente Java™ seguro for usado no modo do WebSphere Application Server integrado, deve-se concluir as etapas de conexão de segurança.
3. Clique nos links para obter instruções.

   - Para configurar o WebSphere Extreme Scale em ambiente independente, clique em "Configurando o monitoramento do WebSphere Extreme Scale em um ambiente independente" na página 922.

- Para configurar o WebSphere Extreme Scale em ambiente integrado sem segurança, clique em "Configurando o monitoramento do WebSphere Extreme Scale no ambiente do WebSphere sem segurança ativada" na página 923.
- Para configurar o WebSphere Extreme Scale em ambiente integrado com segurança ativada, clique em "Configurando o monitoramento do WebSphere Extreme Scale em ambiente WebSphere habilitado para segurança" na página 924.

Configurando o monitoramento do WebSphere Extreme Scale em um ambiente independente
Saiba como configurar o WebSphere Applications agent quando o WebSphere Extreme Scale estiver instalado em um ambiente que não tenha o WebSphere Application Server.

Procedimento

1. Pare o WebSphere Applications agent.
   a) Acesse o diretório *install_dir* no qual você instala o WebSphere Applications agent.
   b) Execute o comando `bin/was-agent.sh stop`.
2. Execute o script de configuração.

   ```
   install_dir/platform_code/yn/bin/wxs-agent-config.sh config
   ```

   Em que
   - *install_dir* é o diretório de instalação do WebSphere Applications agent.
   - *platform_code* é o código da plataforma na qual você instala o agente, por exemplo, lx8266 representa Linux x86_64 R2.6 (64 bits), aix536 representa AIX R5.3 (64 bits).

   Comando de exemplo:

   ```
   /opt/ibm/apm/agent/lx8266/yn/bin/wxs-agent-config.sh config
   ```

   ```
   /opt/ibm/apm/agent/aix536/yn/bin/wxs-agent-config.sh config
   ```
3. Quando for solicitado o caminho da instalação do agente, especifique o diretório inicial do WebSphere Applications agent.

   Nota: O script procura o nome do arquivo de configuração com base no caminho da instalação especificado. O padrão é *install_dir*`/config/${hostname}_yn.xml`. Se você for avisado de que o arquivo não existe, talvez seja porque você não iniciou o WebSphere Applications agent antes de fazer essa configuração. Inicie o WebSphere Applications agent e pare-o pelo menos uma vez.
4. Quando for solicitado o `Tipo de conector do servidor de catálogos do WebSphere Extreme Scale`, insira 1 para continuar.
5. Quando for solicitada a ação `Inserir um nome de nó para identificar este nó do agente na UI`, insira o nome do nó.

   O nome do nó é usado para identificar a zona do WebSphere Extreme Scale monitorada e é exibido no nome da instância, que pode ser visto na UI do Application Performance Dashboard.
6. Quando for solicitado `Segurança do servidor de catálogos WebSphere Extreme Scale ativada?`, insira 1 se houver segurança ativada. Em seguida, insira o nome do usuário e a senha. Se não houver segurança ativada, insira 2.
7. Especifique o nome do host e o número da porta do servidor de catálogos. Se houver vários servidores de catálogos, é possível incluí-los um por um. Também é possível incluir várias zonas uma após a outra.
   - O nome do host é o nome do sistema no qual o servidor de catálogos está localizado. Certifique-se de o nome do host possa ser acessado. Se não, use o endereço IP como o nome do host.
   - O número da porta é o número do **`JMXServicePort`** do servidor de catálogos do WebSphere Extreme Scale. O valor-padrão é 1099. Detalhes adicionais sobre o número da porta podem ser encontrados no WebSphere Extreme Scale Knowledge Center.
8. Para iniciar o agente, execute o comando a seguir.

```
install_dir/bin/was-agent.sh start
```

Nota:

- A configuração do agente é armazenada no *install_dir*/config/${hostname}_yn.xml. Se quiser alterar qualquer configuração, execute esse script novamente ou modifique o arquivo .xml diretamente.
- É feito backup da configuração anterior como *install_dir*/config/${hostname}_yn.xml.bak. É possível restaurar a configuração anterior, se necessário.
- É possível pressionar Ctrl-C para sair do script quando você executar *install_dir*/*platform_code*/yn/bin/wxs-agent-config.sh config. Sua configuração existente não será alterada.

Configurando o monitoramento do WebSphere Extreme Scale em um ambiente WebSphere integrado

Saiba como configurar o WebSphere Applications agent quando o WebSphere Extreme Scale estiver instalado em um ambiente WebSphere Application Server.

Sobre Esta Tarefa

Se a segurança não estiver ativada para o servidor WebSphere Extreme Scale, é possível executar diretamente o processo de configuração. Caso contrário, primeiro deve-se concluir o "Configurando o monitoramento do WebSphere Extreme Scale em ambiente WebSphere habilitado para segurança" na página 924.

Configurando o monitoramento do WebSphere Extreme Scale no ambiente do WebSphere sem segurança ativada

Se você instalar o WebSphere Extreme Scale em um ambiente do WebSphere Application Server sem segurança ativada, é possível configurar diretamente o WebSphere Applications agent.

Procedimento

1. Pare o WebSphere Applications agent.
   a) Acesse o diretório *install_dir* no qual você instala o WebSphere Applications agent.
   b) Execute o comando bin/was-agent.sh stop.
2. Execute o script de configuração.

   ```
   install_dir/platform_code/yn/bin/wxs-agent-config.sh config
   ```

   Em que

   - *install_dir* é o diretório de instalação do WebSphere Applications agent.
   - *platform_code* é o código da plataforma na qual você instala o agente, por exemplo, lx8266 representa Linux x86_64 R2.6 (64 bits), aix536 representa AIX R5.3 (64 bits).

   Comando de Exemplo:

   ```
   /opt/ibm/apm/agent/lx8266/yn/bin/wxs-agent-config.sh
   ```

   ```
   /opt/ibm/apm/agent/aix536/yn/bin/wxs-agent-config.sh
   ```
3. Quando for solicitado o caminho da instalação do agente, especifique o diretório inicial do WebSphere Applications agent.

   Nota: O script procura o nome do arquivo de configuração com base no caminho da instalação especificado. O padrão é *install_dir*/config/${hostname}_yn.xml. Se você for avisado de que o arquivo não existe, talvez seja porque você não iniciou o WebSphere Applications agent antes de fazer essa configuração. Inicie o WebSphere Applications agent e pare-o pelo menos uma vez.

4. Quando for solicitado o `Tipo de conector do servidor de catálogos WebSphere Extreme Scale`, insira 2 para continuar.
5. Quando for solicitada a ação `Inserir um nome de nó para identificar este nó do agente na UI`, insira o nome do nó.

   O nome do nó é usado para identificar a zona do WebSphere Extreme Scale monitorada e é exibido no nome da instância, que pode ser visto na UI do Application Performance Dashboard.
6. Quando perguntado `Segurança do servidor de catálogos do WebSphere Extreme Scale ativada?`, insira 2 para continuar.
7. Especifique o nome do host e o número da porta do servidor de catálogos. Se houver vários servidores de catálogos, é possível incluí-los um por um. Também é possível incluir várias zonas uma após a outra.
   - O nome do host é o nome do sistema no qual o servidor de catálogos está localizado. Certifique-se de o nome do host possa ser acessado. Se não, use o endereço IP como o nome do host.
   - O número da porta indica o número **`JMXServicePort`** do servidor de catálogos WebSphere Extreme Scale. Ele é herdado do valor **`BOOTSTRAP_ADDRESS`** para cada WebSphere Application Server. Detalhes adicionais sobre o número da porta podem ser encontrados no WebSphere Extreme Scale Knowledge Center.
8. Para iniciar o agente, execute o comando a seguir.

   ```
   install_dir/bin/was-agent.sh start
   ```

   Nota:
   - A configuração do agente é armazenada no *`install_dir`*`/config/${hostname}_yn.xml`. Se quiser alterar qualquer configuração, execute esse script novamente ou modifique o arquivo `.xml` diretamente.
   - É feito backup da configuração anterior como *`install_dir`*`/config/${hostname}_yn.xml.bak`. É possível restaurar a configuração anterior, se necessário.
   - É possível pressionar Ctrl-C para sair do script quando você executar *`install_dir`*`/`*`platform_code`*`/yn/bin/wxs-agent-config.sh config`. Sua configuração existente não será alterada.

Configurando o monitoramento do WebSphere Extreme Scale em ambiente WebSphere habilitado para segurança

Se você instalar o WebSphere Extreme Scale em um ambiente WebSphere Application Server com segurança ativada, deve-se concluir as etapas iniciais de definição antes de configurar o WebSphere Applications agent.

Sobre Esta Tarefa

Se quiser monitorar servidores WebSphere Extreme Scale em ambientes habilitados para segurança do WebSphere Application Server, será necessário configurar as definições de segurança manualmente.

O procedimento se aplica ao seguinte caso:

- Os servidores WebSphere Extreme Scale devem ser implementados em servidores de aplicativos WebSphere Application Server (ou agente de nó ou processos DMGR).
- O WebSphere Applications agent deve ser implementado em um nó no qual o serviço de catálogo de zonas do WebSphere Extreme esteja em execução. Configure o monitoramento do Agente para WebSphere Extreme Scale sob esse nó e configure-o para se conetar a essa instância de serviço de catálogo.
- Uma instância do Agente deve ser utilizada para monitorar apenas uma zona do WebSphere Extreme Scale.

Procedimento

1. Se a versão de JDK do WebSphere Application Server for anterior à 1.7, deve-se configurar o WebSphere Applications agent para usar o mesmo JRE que o WebSphere Application Server.
   a) Abra o arquivo *install_dir*/config/.yn.environment.
   b) Inclua o valor a seguir na primeira linha.

```
#JAVAHOME=/opt/IBM/WebSphere/AppServer/java/8.0/jre
```

2. Configure o arquivo de propriedades de segurança do WebSphere Applications agent.
   Para obter instruções, veja "Configurando o agente para trabalhar com arquivos JAR e propriedades de segurança do WebSphere Application Server" na página 925.
3. Opcional: Se um cliente Java™ seguro for usado, você deverá assegurar que a autenticação esteja configurada corretamente. Deve-se editar o arquivo de propriedades do cliente e o arquivo de propriedades SSL. Para obter instruções, veja "Configurando credenciais de conexão" na página 926.
   Nota: Se a chave não estiver assegurada pelas configurações de SSL, será necessário inserir somente um nome de usuário e uma senha e, em seguida, você poderá pular essa etapa.
4. Execute o script de configuração para ativar o console de configuração. Consulte "Executando a configuração" na página 928.

Configurando o agente para trabalhar com arquivos JAR e propriedades de segurança do WebSphere Application Server
Configure o WebSphere Applications agent para trabalhar com arquivos JAR e propriedades de segurança do WebSphere Application Server.

Sobre Esta Tarefa
Para fazer essa configuração, edite o arquivo kynwb.properties.

Procedimento

1. Abra o arquivo *install_dir*/*platform_code*/yn/config/kynwb.properties. Se esse arquivo não existir, crie um.
   - *install_dir* é o diretório de instalação do WebSphere Applications agent.
   - *platform_code* é o código da plataforma na qual você instala o agente, por exemplo, lx8266 representa Linux x86_64 R2.6 (64 bits), aix536 representa AIX R5.3 (64 bits).
2. No início do arquivo, o caminho da classe é listado. Inclua as seguintes linhas antes das linhas existentes.
   - Para WebSphere Application Server 9.0:

```
appserver_home/plugins/com.ibm.ws.runtime.jar:\
appserver_home/lib/bootstrap.jar:\
appserver_home/runtimes/com.ibm.ws.admin.client_9.0.jar:\
appserver_home/lib/wsogclient.jar:\
```

   - Para WebSphere Application Server 8.5:

```
appserver_home/plugins/com.ibm.ws.runtime.jar:\
appserver_home/lib/bootstrap.jar:\
appserver_home/runtimes/com.ibm.ws.admin.client_8.5.0.jar:\
appserver_home/lib/wsogclient.jar:\
```

   Exemplo de um caminho de classe modificado:

```
/opt/IBM/WebSphere/plugins/com.ibm.ws.runtime.jar:\
/opt/IBM/WebSphere/lib/bootstrap.jar:\
/opt/IBM/WebSphere/runtimes/com.ibm.ws.admin.client_8.5.0.jar:\
/opt/IBM/WebSphere/lib/wsogclient.jar:\
lib/kynwb.jar:\
lib/kynwxssec_api.jar:\
```

```
lib/itcam.cg.mbean.jar:\
wasdc/7.3/installer/lib/itcamfwas.jar:\
```

3. No final do arquivo *install_dir*/*platform_code*/yn/config/kynwb.properties, inclua as linhas que indicam os arquivos de propriedade de segurança para uso pelo agente. Normalmente, esses arquivos são aqueles usados pelo utilitário wsadmin:

```
-Dcom.ibm.CORBA.ConfigURL=file:/appserver_profile/properties/sas.client.props
-Dcom.ibm.SSL.ConfigURL=file:/appserver_profile/properties/ssl.client.props
```

   Se as configurações de segurança exigidas pelo agente forem diferentes das configurações usadas pelo utilitário wsadmin, crie cópias separadas dos arquivos e forneça os caminhos para eles, por exemplo:

```
-Dcom.ibm.CORBA.ConfigURL=file:/opt/IBM/ITM/config/sas.client.props
-Dcom.ibm.SSL.ConfigURL=file:/opt/IBM/ITM/config/ssl.client.props
```

   Nota: Com a instalação de um fix pack ou correção temporária para o WebSphere Applications agent, as mudanças feitas nos arquivos yn.ini e kynwb.properties são sobrescritas. Portanto, após você instalar um fix pack ou correção temporária, é necessário concluir as mudanças nesses dois arquivos novamente.

Configurando credenciais de conexão
Quando um cliente Java seguro for usado, será necessário ler um arquivo de propriedades que contém uma lista de configurações do CSIv2. Essas configurações determinam como o cliente se autentica em um servidor. Você deve assegurar que a autenticação seja configurada corretamente.

Sobre Esta Tarefa

Geralmente, o arquivo com essas configurações é especificado na propriedade JVM com.ibm.CORBA.ConfigURL. É possível encontrar mais configurações SSL no arquivo especificado na propriedade JVM com.ibm.SSL.ConfigURL.

Quando o WebSphere Applications agent é configurado para monitorar servidores eXtreme Scale integrados ao WebSphere Application Server, ele age como um cliente Java seguro. Por esse motivo, -Dcom.ibm.CORBA.ConfigURL e -Dcom.ibm.SSL.ConfigURL devem ser especificados no arquivo kynwb.properties.

Na maioria dos casos, essas propriedades apontam para os arquivos sas.client.props e ssl.client.props no diretório *appserver_profile*/properties. Esses arquivos são usados por ferramentas como wsadmin ou xscmd. Portanto, se for possível usar uma dessas ferramentas para se conectar a um servidor de catálogos do Extreme Scale sem a necessidade de inserir qualquer credencial, não será necessário customizar as configurações.

Se a conexão falhar ou exigir a inserção de um nome do usuário ou senha, você deverá concluir uma configuração extra.

Modificando o arquivo de propriedades do cliente
Edite o arquivo sas.client.props a ser usado pelo WebSphere Applications agent.

Sobre Esta Tarefa
O caminho completo para o arquivo sas.client.props é especificado em kynwb.properties, na propriedade -Dcom.ibm.CORBA.ConfigURL. Forneça as informações de conexão e segurança para a instância do WebSphere Application Server em executando a instância dos Serviços de Catálogo para a qual o agente está configurado.

Procedimento

1. Abra o arquivo *appserver_profile*/properties/sas.client.props.
2. Altere o valor da propriedade com.ibm.CORBA.loginSource para properties:

```
com.ibm.CORBA.loginSource=properties
```

3. Configure a propriedade `com.ibm.CORBA.securityServerHost` para o nome do host de um servidor de aplicativos na zona do WebSphere Extreme Scale. O servidor pode ser o servidor local ou um servidor diferente. O servidor deve estar sempre disponível quando o agente for inicializado. Por exemplo:

```
com.ibm.CORBA.securityServerHost=server.company.com
```

4. Configure a propriedade `com.ibm.CORBA.securityServerPort` para a porta RMI para o perfil do servidor de aplicativos, por exemplo:

```
com.ibm.CORBA.securityServerPort=2819
```

5. Configure a propriedade `com.ibm.CORBA.loginUserid` para o nome de login para comunicação com o servidor de aplicativos e a propriedade `com.ibm.CORBA.loginPassword` para a senha, por exemplo:

```
com.ibm.CORBA.loginUserid=admin
com.ibm.CORBA.loginPassword=password
```

6. Configure as propriedades a seguir como `true` ou `false`, correspondendo às configurações de **comunicações de entrada de CSIv2** no console administrativo do WebSphere:

```
com.ibm.CSI.performTLClientAuthenticationRequired
com.ibm.CSI.performTLClientAuthenticationSupported
com.ibm.CSI.performTransportAssocSSLTLSRequired
com.ibm.CSI.performTransportAssocSSLTLSSupported
```

   As propriedades `com.ibm.CSI.performTLClientAuthentication*` estão relacionadas com as configurações de **Autenticação por Certificado de Cliente**. As `com.ibm.CSI.performTransportAssocSSLTLS*` estão relacionadas às configurações de **Transporte**.
7. Opcional: Se o alias SSL padrão (`DefaultSSLSettings`) não for usado, configure o nome alternativo da configuração SSL na propriedade `com.ibm.ssl.alias`.
8. Salve o arquivo e, em seguida, criptografe a senha no arquivo `sas.client.props`. Para criptografar a senha, execute o seguinte comando:
   - Em sistemas Linux e UNIX, execute *appserver_profile*`/bin/PropFilePasswordEncoder.sh sas.client.props com.ibm.CORBA.loginPassword`

   Importante: Quando a autenticação por certificado de cliente for necessária e a autenticação básica estiver ativada, talvez seja necessário também configurar a propriedade `com.ibm.CORBA.validateBasicAuth=false`.

Modificando o arquivo de propriedades SSL do cliente
Modifique o arquivo de propriedades SSL que o WebSphere Applications agent usa para acessar certificados do servidor.

Sobre Esta Tarefa

Edite o arquivo `ssl.client.props` a ser usado pelo agente. O caminho completo para o arquivo é especificado no arquivo `kynwb.properties` na propriedade `-Dcom.ibm.SSL.ConfigURL`. Forneça as informações do keystore e do armazenamento confiável SSL para a instância do WebSphere Application Server executando a instância dos Serviços de Catálogo para a qual o agente está configurado.

É possível criar e gerenciar certificados usando o console administrativo do WebSphere (**Segurança** > **Certificado SSL e Gerenciamento de Chave** > **Armazenamentos de Chaves e Certificados**) ou usando a ferramenta iKeyman.

Procedimento

1. Abra o arquivo *appserver_profile*`/properties/ssl.client.props`.
2. Altere o valor da propriedade `com.ibm.ssl.alias` para corresponder ao valor da mesma propriedade no arquivo `sas.client.props`.

Dica: O arquivo `ssl.client.props` pode conter várias configurações SSL. Cada configuração inicia com a propriedade `com.ibm.ssl.alias`.

3. Configure a propriedade `com.ibm.ssl.enableSignerExchangePrompt` como `false`.
4. Configure as propriedades do keystore a seguir para permitir que o aplicativo cliente acesse a chave de criptografia:

   com.ibm.ssl.keyStoreName
   O nome que identifica este keystore

   com.ibm.ssl.keyStore
   O nome e o caminho completo do arquivo keystore

   com.ibm.ssl.keyStorePassword
   A senha para o keystore

   com.ibm.ssl.keyStoreType
   O tipo de keystore. Use o tipo PKCS12 padrão devido à sua interoperabilidade com outros aplicativos.

   Importante: Se a autenticação por certificado de cliente não for necessária, o keystore pode conter qualquer chave autoassinada. Caso contrário, o keystore deverá conter uma chave que seja assinada por um certificado que está no armazenamento confiável do servidor.
5. Configure as propriedades de armazenamento confiável a seguir para permitir que o aplicativo cliente acesse certificados de assinante:

   com.ibm.ssl.trustStoreName
   O nome que identifica este armazenamento confiável

   com.ibm.ssl.trustStore
   O nome e o caminho completo do arquivo de armazenamento confiável

   com.ibm.ssl.trustStorePassword
   A senha para o truststore

   com.ibm.ssl.trustStoreType
   O tipo de armazenamento confiável. Use o tipo PKCS12 padrão devido à sua interoperabilidade com outros aplicativos.

   Importante: Se o cliente tiver que utilizar uma conexão SSL, o certificado de assinante do servidor deverá estar em seu armazenamento confiável.

Executando a configuração
Após verificar o ambiente e a segurança, você pode executar o processo de configuração.

Procedimento

1. Pare o WebSphere Applications agent.
   a) Acesse o diretório *install_dir* no qual você instala o WebSphere Applications agent.
   b) Execute o comando `bin/was-agent.sh stop`.
2. Execute o script de configuração.

   ```
   install_dir/platform_code/yn/bin/wxs-agent-config.sh config
   ```

   Em que

   - *install_dir* é o diretório de instalação do WebSphere Applications agent.
   - *platform_code* é o código da plataforma na qual você instala o agente, por exemplo, lx8266 representa Linux x86_64 R2.6 (64 bits), aix536 representa AIX R5.3 (64 bits).

   Comando de exemplo:

   ```
   /opt/ibm/apm/agent/lx8266/yn/bin/wxs-agent-config.sh config
   ```

```
/opt/ibm/apm/agent/aix536/yn/bin/wxs-agent-config.sh config
```

3. Quando for solicitado o caminho da instalação do agente, especifique o diretório inicial do WebSphere Applications agent.

   Nota: O script procura o nome do arquivo de configuração com base no caminho da instalação especificado. O padrão é *install_dir*/config/${hostname}_yn.xml. Se você for avisado de que o arquivo não existe, talvez seja porque você não iniciou o WebSphere Applications agent antes de fazer essa configuração. Inicie o WebSphere Applications agent e pare-o pelo menos uma vez.
4. Quando for solicitado o Tipo de conector do servidor de catálogos WebSphere Extreme Scale, insira 2 para continuar.
5. Quando for solicitada a ação Inserir um nome de nó para identificar este nó do agente na UI, insira o nome do nó.

   O nome do nó é usado para identificar a zona do WebSphere Extreme Scale monitorada e é exibido no nome da instância, que pode ser visto na UI do Application Performance Dashboard.
6. Quando perguntado Segurança do servidor de catálogos do WebSphere Extreme Scale ativada?, insira 1 para continuar. Em seguida, insira o nome do usuário e a senha.
7. Especifique o nome do host e o número da porta do servidor de catálogos. Se houver vários servidores de catálogos, é possível incluí-los um por um. Também é possível incluir várias zonas uma após a outra.
   - O nome do host é o nome do sistema no qual o servidor de catálogos está localizado. Certifique-se de o nome do host possa ser acessado. Se não, use o endereço IP como o nome do host.
   - O número da porta indica o número **JMXServicePort** do servidor de catálogos WebSphere Extreme Scale. Ele é herdado do valor **BOOTSTRAP_ADDRESS** para cada WebSphere Application Server. Detalhes adicionais sobre o número da porta podem ser encontrados no WebSphere Extreme Scale Knowledge Center.
8. Para iniciar o agente, execute o comando a seguir.

   ```
   install_dir/bin/was-agent.sh start
   ```

   Nota:
   - A configuração do agente é armazenada no *install_dir*/config/${hostname}_yn.xml. Se quiser alterar qualquer configuração, execute esse script novamente ou modifique o arquivo .xml diretamente.
   - É feito backup da configuração anterior como *install_dir*/config/${hostname}_yn.xml.bak. É possível restaurar a configuração anterior, se necessário.
   - É possível pressionar Ctrl-C para sair do script ao executar *install_dir*/bin/wxs-agent-config.sh config. Sua configuração existente não será alterada.

Desconfigurando o monitoramento do WebSphere Extreme Scale
Quando não quiser monitorar o WebSphere Extreme Scale, você pode configurar o WebSphere Applications agent.

Procedimento

1. Pare o WebSphere Applications agent.
   a) Acesse o diretório *install_dir* no qual você instala o WebSphere Applications agent.
   b) Execute o comando bin/was-agent.sh stop.
2. Execute o script de desconfiguração.

   ```
   install_dir/{pc}/yn/bin/wxs-agent-config.sh unconfig
   ```

   Em que
   - *install_dir* é o diretório de instalação do WebSphere Applications agent.

- *platform_code* é o código da plataforma na qual você instala o agente, por exemplo, lx8266 representa Linux x86_64 R2.6 (64 bits), aix536 representa AIX R5.3 (64 bits).

Comando de exemplo:

```
/opt/ibm/apm/agent/lx8266/yn/bin/wxs-agent-config.sh unconfig
```

```
/opt/ibm/apm/agent/aix536/yn/bin/wxs-agent-config.sh unconfig
```

Configurando o monitoramento do WebSphere Infrastructure Manager

Configure o WebSphere Infrastructure Manager agent para monitorar o desempenho do WebSphere Deployment Manager e do Agente do Nó.

Sobre Esta Tarefa

O WebSphere Infrastructure Manager agent é um agente de múltiplas instâncias. Você deve criar a primeira instância e iniciar o agente manualmente.

Procedimento

1. Para configurar o agente, execute o seguinte comando.

   ```
   install_dir/bin/wim-agent.sh config instance_name
   ```

   Em que *instance_name* é o nome a ser fornecido para a instância e *install_dir* é o diretório de instalação do WebSphere Infrastructure Manager agent. O diretório de instalação padrão é `/opt/ibm/apm/agent`.
2. Quando for solicitado para `Editar as configurações do 'Monitoring Agent for WebSphere Infrastructure Manager'`, insira `1` para continuar.
3. Quando solicitado para `início do Java`, especifique o diretório no qual Java está instalado.

   O valor padrão é `/opt/ibm/apm/agent/JRE/lx8266/jre`.
4. Quando for solicitado o `Diretório inicial do Perfil do DMGR`, especifique o diretório inicial do perfil do Deployment Manager.

   O diretório padrão é `/opt/IBM/WebSphere/AppServer/profiles/Dmgr01`.
5. Quando for solicitado o `ID do usuário do JMX`, especifique o ID do usuário usado para se conectar ao servidor MBean.
6. Quando for solicitado `Digite a senha do JMX`, especifique a senha para o usuário.
7. Quando for solicitado `Digite novamente a senha do JMX`, digite a senha novamente.
8. Para iniciar o agente, execute o comando a seguir.

   ```
   install_dir/bin/wim-agent.sh start instance_name
   ```

Resultados

Você criou uma instância do WebSphere Infrastructure Manager agent e iniciou o agente de monitoramento para iniciar a coleta de amostras de dados para o monitoramento de recursos.

Configurando o monitoramento WebSphere MQ

Antes de iniciar o agente, você deve designar um nome de instância ao agente e concluir as diversas tarefas de configuração para o ID do usuário e nomes de sistemas gerenciados. Opcionalmente, também é possível ativar o rastreamento de transação para o agente.

Antes de Iniciar

- As direções aqui destinam-se à liberação mais atual desse agente. Para obter informações sobre como verificar a versão de um agente em seu ambiente, consulte Comando de versão do agente. Para obter informações detalhadas sobre a lista de versões do agente e o que há de novo para cada versão, consulte “Histórico de Mudanças” na página 50.
- Certifique-se de que os requisitos do sistema para o WebSphere MQ agent sejam atendidos em seu ambiente. Para obter informações atualizadas sobre requisitos do sistema, consulte o Relatório detalhado de requisitos do Sistema para o WebSphere MQ agent.

Sobre Esta Tarefa

Essas direções destinam-se à liberação mais atual do agente, exceto conforme indicado.

Para configurar o ambiente para o WebSphere MQ agent, primeiro você deve assegurar que o ID do usuário do agente possa acessar objetos do IBM MQ (WebSphere MQ), configurar o IBM MQ (WebSphere MQ) para ativação de dados e, em seguida, configurar o WebSphere MQ agent.

O procedimento a seguir é um roteiro para configurar o WebSphere MQ agent, que inclui etapas necessárias e opcionais. Conclua as etapas necessárias de acordo com suas necessidades.

Procedimento

1. Autorize o ID do usuário que é usado para configurar, iniciar e parar o agente para acessar objetos do IBM MQ (WebSphere MQ). Consulte “Autorizando os IDs dos usuários para executar o agente” na página 931.
2. Configure o IBM MQ(WebSphere MQ) para ativar os dados que você deseja monitorar. Consulte “Configurando o IBM MQ (WebSphere MQ) para ativação de dados” na página 933.
3. Configure o agente fornecendo um nome de instância de agente, um nome do gerenciador de filas e, opcionalmente, um nome de agente. Consulte “Configurando o WebSphere MQ agent” na página 935.
4. Opcional: Dependendo de seus requisitos de monitoramento, pode ser requerido um nome do sistema gerenciado exclusivo para distinguir diferentes agentes de monitoramento. Use a opção `Nome do agente` no comando `mq-agent.sh config` para especificar o qualificador intermediário do nome do sistema gerenciado. Consulte “Especificando nomes de sistemas gerenciados exclusivos para vários gerenciadores de filas” na página 938.
5. Opcional: Para configurar o agente para coletar dados de rastreamento de transação do gerenciador de filas monitoradas, use a página **Configuração do Agente**. Para obter instruções, veja “Configurando o rastreamento de transações para o WebSphere MQ agent” na página 940.
6. Opcional: Ative o agente para coletar os dados de histórico de longo prazo para filas e canais. Para obter instruções, veja “Ativando a coleta de dados para histórico de longo prazo de fila e de canal” na página 941.
7. Opcional: Para monitorar remotamente o gerenciador de filas no MQ Appliance, é necessária uma configuração adicional do agente e do IBM MQ (WebSphere MQ). Para obter instruções, consulte “Monitorando remotamente os gerenciadores de filas no MQ Appliance” na página 942 ou “Monitorando remotamente os gerenciadores de filas de HA no MQ Appliance” na página 943.

Autorizando os IDs dos usuários para executar o agente

Para um ID do usuário configurar, iniciar e parar o WebSphere MQ agent, o ID do usuário deve pertencer ao grupo **mqm**, que tem privilégios administrativos completos sobre o IBM MQ (WebSphere MQ). Além disso, para um usuário não raiz ou um usuário não administrador, deve-se conceder aos usuários o acesso aos objetos do IBM MQ (WebSphere MQ) usando o comando de controle do IBM MQ (WebSphere MQ).

Sobre Esta Tarefa

No sistema AIX ou Linux, você deve incluir o ID do usuário no grupo **mqm** e, em seguida, conceder ao ID do usuário o acesso apropriado aos objetos do IBM MQ (WebSphere MQ) com o comando **setmqaut**.

Nos sistemas Windows, é necessário incluir o ID de usuário no grupo **mqm**. Se o ID de usuário não pertencer ao grupo de usuários administrador, você também deverá usar o Editor de registro para conceder permissões ao ID de usuário para iniciar ou parar o agente.

Procedimento

- Linux AIX

  No sistema AIX ou Linux, conclua as seguintes etapas:

  a) Efetue logon no sistema AIX ou Linux usando o ID raiz.

  b) Inclua o ID de usuário que é usado para executar o agente para o grupo **mqm**.

  c) (WebSphere MQ V7.5 ou mais recente): se o ID do usuário for um usuário não raiz no sistema AIX ou Linux, configure o nível apropriado de autoridade para o ID do usuário para acessar objetos do IBM MQ (WebSphere MQ) executando o seguinte comando:

  ```
  setmqaut -m queue_manager -t qmgr -p user_ID +inq +connect +dsp +setid
  ```

  em que *queue_manager* é o nome do gerenciador de filas do WebSphere MQ V7.5 ou posterior e *user_ID* é o ID do usuário não raiz ou não administrador para executar o agente.

- Windows

  Em sistemas Windows, conclua as seguintes etapas:

  a) Efetue logon nos sistemas Windows como um administrador do sistema.

  b) Inclua o ID de usuário que é usado para executar o agente para o grupo **mqm**.

  c) Se o ID do usuário que você usa para iniciar, executar e parar o agente não é membro do grupo de Administradores, use o Editor de Registro para configurar permissões para um ID de usuário para assegurar que o agente possa ser iniciado e interrompido com êxito:

  a. Clique em **Iniciar** > **Executar** e, em seguida, digite `regedit.exe` para abrir o Editor de registro.

  b. No Editor de Registro, localize a chave, `HKEY_LOCAL_MACHINE\SOFTWARE\Candle`.

  c. Clique com o botão direito na chave e clique em **Permissões**.

  d. Se o ID de usuário do WebSphere MQ agent não estiver na lista Grupo ou nomes de usuários, clique em **Incluir** para incluir o ID de usuário na lista.

  e. Clique no ID do usuário na lista.

  f. Na lista Permissões para o *user-ID*, em que *user-ID* é o ID do usuário do WebSphere MQ agent, selecione **Controle Total** na coluna Permitir e clique em **OK**.

  g. No Editor de Registro, localize a chave `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Windows NT\CurrentVersion\Perflib`.

  h. Clique com o botão direito na chave e clique em **Permissões**.

  i. Se o ID de usuário do WebSphere MQ agent não estiver na lista Grupo ou nomes de usuários, clique em **Incluir** para incluir o ID de usuário na lista.

  j. Clique no ID de usuário na lista Grupo ou nomes de usuários.

  k. Na lista Permissões para o *user-ID*, em que *user-ID* é o ID do usuário do WebSphere MQ agent, selecione **Leitura** na coluna Permitir e clique em **OK**.

  l. Feche o Editor de registro.

  m. Localize o diretório *install_dir*, em que *install_dir* é o diretório de instalação do agente.

  n. Clique com o botão direito no diretório e clique em **Propriedades**.

  o. Na guia Segurança, se o ID de usuário do WebSphere MQ agent não estiver na lista Grupo ou nomes de usuários, clique em **Editar** e depois em **Incluir** para incluir o ID de usuário na lista.

  p. Clique no ID de usuário na lista Grupo ou nomes de usuários.

  q. Nas Permissões para a lista *user-ID*, selecione **Controle Total** na coluna Permitir, em que **user-ID** é o ID do usuário do WebSphere MQ agent.

r. Clique em **OK**.

O que Fazer Depois
A próxima etapa para configurar o IBM MQ (WebSphere MQ) para ativação de dados. Consulte "Configurando o IBM MQ (WebSphere MQ) para ativação de dados" na página 933.

Configurando o IBM MQ (WebSphere MQ) para ativação de dados

Antes de configurar o WebSphere MQ agent, é recomendado configurar o IBM MQ (WebSphere MQ) primeiro para ativar os dados que você deseja monitorar.

Sobre Esta Tarefa

Decida que tipo de dados que você deseja que o WebSphere MQ agent monitore. Ative os dados no gerenciador de filas usando os comandos do MQSC se os dados não forem produzidos pelo gerenciador de filas por padrão.

Lembre-se: Você deve iniciar o MQSC para o gerenciador de filas de destino antes de emitir os comandos do MQSC. Para obter uma lista do gerenciador de filas, emita o comando **dspmq** a partir do diretório `bin` no diretório de instalação do IBM MQ (WebSphere MQ). Para iniciar o MQSC para um gerenciador de filas, emita o seguinte comando a partir do diretório `bin`, em que *<qmgr_name>* é o nome do gerenciador de filas que você deseja configurar.

```
runmqsc <qmgr_name>
```

Procedimento

- Para ver a idade da mensagem mais antiga em uma fila, conclua as etapas conforme documentado em "Ativando o monitoramento em tempo real para filas" na página 933.
- Para monitorar alguns eventos de gerenciador de filas que não são gerados pelo gerenciador de filas por padrão, conclua as etapas conforme documentado em "Ativando o monitoramento de eventos para o gerenciador de filas" na página 934.
- Para obter os dados de rastreamento de transação, conclua as etapas conforme documentado em "Ativando o rastreio de atividade do aplicativo MQI" na página 934.
- Para monitorar um gerenciador de filas remotas, certifique-se de que o WebSphere MQ agent possa coletar dados de monitoramento por meio de um canal no sistema remoto. Para obter mais informações, consulte "Configurações de Segurança para Monitoramento Remoto" na página 934.

Ativando o monitoramento em tempo real para filas

Sobre Esta Tarefa

Para ver a idade da mensagem mais antiga (em segundos) em uma fila, deve-se ativar o monitoramento em tempo real para a fila.

Procedimento

Use os comandos a seguir para ativar o monitoramento em tempo real para as filas em seu ambiente.

- Para ativar um monitoramento em tempo real de todas as filas cujo atributo MONQ é configurado como QMGR, emita o seguinte comando:

  ```
  ALTER QMGR MONQ (collection_level)
  ```

  em que *collection_level* especifica o nível de coleta de dados de monitoramento para as filas. Pode ser configurado para LOW, MEDIUM ou HIGH para atender os requisitos de seu ambiente.
- Para ativar o monitoramento em tempo real para a fila individual, emita o comando a seguir:

  ```
  ALTER QLOCAL(queue_name) MONQ(collection_level)
  ```

em que *queue_name* é o nome da fila e *collection_level* especifica o nível de coleta de dados de monitoramento para as filas. Pode ser configurado para LOW, MEDIUM ou HIGH para atender os requisitos de seu ambiente.

Resultados
Os dados podem ser exibidos no widget de grupo Idade da Mensagem Mais Antiga para a Fila depois que o WebSphere MQ agent é iniciado.

Ativando o monitoramento de eventos para o gerenciador de filas

Sobre Esta Tarefa

O monitoramento de eventos é uma das técnicas de monitoramento que estão disponíveis para monitorar sua rede do IBM MQ. Depois de ativar o gerenciador de filas para emitir determinados tipos de eventos, as mensagens do evento são colocadas em filas de eventos quando o evento ocorre. Portanto, essas mensagens do evento podem ser monitoradas e exibidas pelo WebSphere MQ agent.

Os seguintes tipos de eventos não são monitorados e exibidos com a configuração do gerenciador de filas padrão. Use o comando **`ALTER QMGR`** para ativar o gerenciador de filas para gerar esses eventos para que eles possam ser exibidos no Application Performance Dashboard.

- Eventos do canal
- Eventos de desempenho

Procedimento

Use os seguintes comandos para ativar o gerenciador de filas para gerar os eventos de seu interesse:

- Para gerar eventos de canal, emita `ALTER QMGR CHLEV(ENABLED)`.
- Para gerar eventos de desempenho, emita `ALTER QMGR PERFMEV(ENABLED)`.

Resultados
Os eventos monitorados podem ser exibidos no widget de grupo Eventos de Gerenciador de Filas após o início do WebSphere MQ agent.

Ativando o rastreio de atividade do aplicativo MQI

Sobre Esta Tarefa
Para que dados de rastreamento de transação sejam exibidos nos painéis de middleware e de topologia, o rastreio de atividade do aplicativo MQI deve ser ativado no gerenciador de filas.

Procedimento

- Para ativar a coleta de informações de rastreio de atividade do aplicativo MQI, emite o seguinte comando MQSC:

```
ALTER QMGR ACTVTRC(ON)
```

Configurações de Segurança para Monitoramento Remoto

Sobre Esta Tarefa
Para usar o WebSphere MQ agent para monitorar um gerenciador de filas remotas, certifique-se de que as configurações de segurança do IBM MQ (WebSphere MQ) não impeçam o agente de coletar dados de monitoramento por meio de um canal no sistema remoto.

O procedimento a seguir fornece um exemplo de uma configuração de segurança simples para monitoramento remoto. Para exercer maior controle preciso sobre o acesso concedido à conexão de sistemas em um nível de canal, é possível usar registros de autenticação de canal. Para obter mais informações, consulte a Documentação dos mecanismos de segurança do IBM MQ.

Procedimento

1. Desative a autenticação do canal executando o seguinte comando MQSC:

```
ALTER QMGR CHLAUTH (DISABLED) CONNAUTH ('')
```

2. Mude as configurações de canal como a seguir, em que *channel_for_remote_monitor* é o nome do canal usado para monitoramento remoto.

   - Linux AIX

     ```
     ALTER CHANNEL(channel_for_remote_monitor) CHLTYPE(SVRCONN) MCAUSER('mqm')
     ```

   - Windows

     ```
     ALTER CHANNEL (channel_for_remote_monitor) CHLTYPE (SVRCONN) MCAUSER (MUSR_MQADMIN)
     ```

3. Atualize as configurações de segurança.

```
SEGURANÇA DA REFRESH
```

Configurando o WebSphere MQ agent

Deve-se designar um nome de instância ao WebSphere MQ agent e configurar o agente antes dele iniciar o monitoramento do ambiente do IBM MQ (WebSphere MQ).

Antes de Iniciar

- Certifique-se de que o ID do usuário do agente tem permissão apropriada para acessar objetos do IBM MQ (WebSphere MQ). Se você não tiver feito isso, siga as instruções em "Autorizando os IDs dos usuários para executar o agente" na página 931.
- Configure o IBM MQ (WebSphere MQ) para ativar a coleta de dados necessária. Se você não tiver feito isso, consulte "Configurando o IBM MQ (WebSphere MQ) para ativação de dados" na página 933.
- Você deve fornecer o nome do gerenciador de filas a ser monitorado pelo WebSphere MQ agent. Entre em contato com o administrador do IBM MQ (WebSphere MQ), se não souber o nome do gerenciador de filas apropriado. Como alternativa, emita o comando **dspmq** a partir do diretório `bin` no diretório de instalação do IBM MQ (WebSphere MQ) para obter uma lista dos gerenciadores de filas. O valor QMNAME retornado é o que você deve fornecer quando configurar o WebSphere MQ agent.

Sobre Esta Tarefa

O WebSphere MQ agent é um agente de várias instâncias; você deve criar a primeira instância e iniciar o agente manualmente.

Em sistemas UNIX ou Linux, é possível optar por configurar o agente com ou sem interações. Em sistemas Windows, é possível configurar o agente somente sem interações.

- Para configurar o agente com interação, execute o script de configuração e responda aos prompts. Consulte "Configuração interativa" na página 935.
- Para configurar o agente sem interação, edite o arquivo silencioso de resposta e execute o script de configuração. Consulte "Configuração silenciosa" na página 936.

Importante: Se você também instalou o Monitoring Agent for WebSphere MQ, que é entregue como um componente do produto ITCAM for Applications, no mesmo sistema que o WebSphere MQ agent, que é entregue no Cloud APM, não use-os para monitorar o mesmo gerenciador de filas no sistema.

Configuração interativa

Procedimento

Para configurar o agente executando o script e respondendo aos prompts, conclua as seguintes etapas:

1. Insira o comando a seguir para criar uma instância do agente:

```
install_dir/bin/mq-agent.sh config instance_name
```

em que *instance_name* é o nome que você deseja fornecer para a instância.

2. Quando for solicitado o `Nome do gerenciador de filas`, especifique o nome do gerenciador de filas a ser monitorado.
3. Quando for solicitado o `Agent Name`, especifique o nome do agente a ser usado como o qualificador intermediário do nome do sistema gerenciado. Não pressione Enter para ignorar a especificação desse parâmetro.

   Lembre-se: Este nome do agente é diferente do nome da instância do agente. O nome da instância do agente é usado no nome do arquivo de configuração do agente para distinguir os arquivos de configuração entre agentes, por exemplo, *hostname*`_mq_`*instancename*`.cfg`. O nome do agente é usado como um identificador curto para criar nomes de sistemas gerenciados exclusivos. Para entender quando um nome de sistema gerenciado exclusivo é necessário, consulte “Especificando nomes de sistemas gerenciados exclusivos para vários gerenciadores de filas” na página 938.
4. Se você deseja monitorar um gerenciador de filas remotas, especifique os parâmetros de configuração a seguir. Se você deseja monitorar um gerenciador de filas locais, pressione Enter para continuar.
   - `Connection Name`: o nome da conexão para monitoramento remoto. O formato é *IP_address* `(`*port_number*`)`, por exemplo, `127.0.0.1(1414)`. Se essa for a primeira configuração da instância do agente, será possível pressionar Enter para aceitar o padrão de nulo. O nome da conexão apropriado pode ser descoberto automaticamente.
   - `Channel`: o nome do canal usado para a coleta de dados remotos. Se essa for a primeira configuração da instância do agente, será possível pressionar Enter para aceitar o padrão de nulo. O canal SYSTEM.DEF.SVRCONN será usado.

   Limitação: Os logs de erro de um gerenciador de filas remotas não pode ser monitorado. Quando o agente está monitorando um gerenciador de filas remotas, o painel Detalhes de Erros MQ não contém dados.
5. Quando for solicitado o caminho da biblioteca do WebSphere MQ, pressione Enter para aceitar o valor padrão, que é o caminho da biblioteca de 64 bits do IBM MQ (WebSphere MQ) descoberto automaticamente pelo WebSphere MQ agent. Se nenhum valor padrão for exibido, você deve fornecer o caminho da biblioteca de 64 bits do IBM MQ (WebSphere MQ) para continuar.
   Um exemplo de um caminho da biblioteca de 64 bits é `/opt/mqm8/lib64` para um sistema Linux.
6. Para iniciar o agente, digite o seguinte comando:

```
install_dir/bin/mq-agent.sh start instance_name
```

Configuração silenciosa

Procedimento

Para configurar o agente editando o arquivo silencioso de resposta e executando o script sem interação, conclua as seguintes etapas:

1. Abra o arquivo `mq_silent_config.txt` em um editor de texto.
   - Linux AIX *install_dir*`/samples/mq_silent_config.txt`
   - Windows *install_dir*`\tmaitm6_x64\samples\mq_silent_config.txt`

   em que *install_dir* é o diretório de instalação do WebSphere MQ agent.
2. Necessário: Para **QMNAME**, especifique o nome do gerenciador de filas a ser monitorado.
3. Necessário: Para **AGTNAME**, especifique o nome do agente a ser usado como o qualificador intermediário do nome de sistema gerenciado.

   Lembre-se: Este nome do agente é diferente do nome da instância do agente. O nome da instância do agente é usado no nome do arquivo de configuração do agente para distinguir os arquivos de configuração entre agentes, por exemplo, *hostname*`_mq_`*instancename*`.cfg`. O nome do agente é usado como um identificador curto para criar nomes de sistemas gerenciados exclusivos. Para

entender quando um nome de sistema gerenciado exclusivo é necessário, consulte “Especificando nomes de sistemas gerenciados exclusivos para vários gerenciadores de filas” na página 938.

4. Se você deseja monitorar um gerenciador de filas remotas, especifique os parâmetros de configuração a seguir:
   - **CONNAME**: o nome da conexão para monitoramento remoto. O formato é *IP_address* (*port_number*), por exemplo, 127.0.0.1(1414).
   - **CHANNEL**: o nome do canal usado para a coleta de dados remotos. Se não especificado, o canal SYSTEM.DEF.SVRCONN será usado.

   Limitação: Os logs de erro de um gerenciador de filas remotas não pode ser monitorado. Quando o agente está monitorando um gerenciador de filas remotas, o painel Detalhes de Erros MQ não contém dados.
5. Opcional: Para **WMQLIBPATH**, especifique o caminho da biblioteca de 64 bits do IBM MQ (WebSphere MQ). Por exemplo, /opt/mqm8/lib64. Se nenhum valor for especificado, o caminho poderá ser descoberto automaticamente durante a configuração do agente.
6. Salve e feche o arquivo mq_silent_config.txt e, em seguida, execute o seguinte comando a partir da linha de comandos:
   - Linux AIX *install_dir*/bin/mq-agent.sh config *instance_name* *path_to_responsefile*
   - Windows *install_dir*\BIN\mq-agent.bat config *instance_name* "*path_to_responsefile*"

   em que *instance_name* é o nome da instância que você configura e *path_to_responsefile* é o caminho completo do arquivo de resposta silencioso.

   Lembre-se: Em sistemas Windows, não omita as aspas duplas ("") que cercam o caminho para o arquivo de resposta silencioso, especialmente quando o caminho contiver caracteres especiais.

   Por exemplo, se o arquivo de resposta estiver no diretório padrão, execute o comando a seguir.
   - Linux AIX

     ```
     /opt/ibm/apm/agent/bin/mq-agent.sh config instance_name
     /opt/ibm/apm/agent/samples/mq_silent_config.txt
     ```
   - Windows

     ```
     C:\IBM\APM\BIN\mq-agent.bat config instance_name
     "C:\IBM\APM\tmaitm6_x64\samples\mq_silent_config.txt"
     ```
7. Para iniciar o agente, digite o seguinte comando:
   - Linux AIX

     ```
     install_dir/bin/mq-agent.sh start instance_name
     ```
   - Windows

     ```
     install_dir\bin\mq-agent.bat start instance_name
     ```

Resultados

Agora, é possível efetuar login no Console do Cloud APM e usar o Editor de aplicativos para incluir a instância do WebSphere MQ agent no Application Performance Dashboard. Para obter instruções sobre como iniciar o Console do Cloud APM, consulte “Iniciando o Console do Cloud APM” na página 975. Para obter informações sobre como usar o Editor de aplicativos, consulte “Gerenciando aplicativos” na página 1098.

O que Fazer Depois

- Se você ativou a coleta de informações de rastreio de atividade do aplicativo MQI no gerenciador de filas, use a página **Configuração do agente** para configurar o WebSphere MQ agent para coletar dados de rastreamento de transação do gerenciador de filas monitoradas. Consulte "Configurando o rastreamento de transações para o WebSphere MQ agent" na página 940. Se o agente não aparecer na página **Configuração do agente**, reinicie o Servidor Cloud APM.
- Dependendo de seus requisitos de monitoramento, pode ser requerido um nome do sistema gerenciado exclusivo para distinguir diferentes agentes de monitoramento. Use a opção `Nome do agente` no comando `mq-agent.sh config` para especificar o qualificador intermediário do nome do sistema gerenciado. Consulte "Especificando nomes de sistemas gerenciados exclusivos para vários gerenciadores de filas" na página 938.
- Para configurar o WebSphere MQ agent para monitoramento remoto, é preciso fazer alguma configuração manual depois de criar uma instância de agente. Para obter instruções, consulte os seguintes tópicos:
  - "Monitorando remotamente os gerenciadores de filas no MQ Appliance" na página 942
  - "Monitorando remotamente os gerenciadores de filas de HA no MQ Appliance" na página 943

Especificando nomes de sistemas gerenciados exclusivos para vários gerenciadores de filas

Os nomes exclusivos do sistema gerenciado às vezes são necessários para distinguir diferentes agentes de monitoramento que se conectam ao mesmo Servidor Cloud APM. Use o parâmetro **AGTNAME** no arquivo silencioso de resposta ou a opção `Nome do Agente` no comando **mq-agent.sh config** para especificar o qualificador intermediário usado no nome do sistema gerenciado.

Sobre Esta Tarefa

Quando o WebSphere MQ agent é iniciado, ele registra o seguinte sistema gerenciado:

```
monitoredqueuemanagername:agentname:MQ
```

em que

- *monitoredqueuemanagername* é o nome do gerenciador de filas que é monitorado pelo agente.
- *agentname* é o qualificador intermediário do nome do sistema gerenciado. Se o valor *agentname* não for especificado, nenhum valor será usado.

Especificar o valor de nome do agente é útil nas seguintes circunstâncias:

- Se seu site tiver vários gerenciadores de filas com o mesmo nome que estão em execução em nós diferentes, especifique o nome do agente para cada gerenciador de filas, para que o WebSphere MQ agent possa criar nomes exclusivos do sistema gerenciado.
- Se o comprimento do nome do sistema gerenciado exceder 32 caracteres, 2 nomes de gerenciadores de filas diferentes podem ser resolvidos para o mesmo nome, em razão do truncamento. Para fazer distinção entre os nomes dos sistemas gerenciados para os gerenciadores de filas, especifique o nome do agente para cada gerenciador de filas.
- Se desejar agrupar e identificar nomes do gerenciador de filas por algo diferente do nome do host e do nome do gerenciador de filas, como um nome de cluster de alta disponibilidade.
- Se desejar ativar vários agentes que estão conectados ao mesmo Servidor Cloud APM para monitorar os gerenciadores de filas com o mesmo nome em hosts diferentes.

Configuração interativa

Procedimento

Para usar a opção `Nome do Agente` no comando **mq-agent.sh config**, conclua as etapas a seguir:

1. Na linha de comandos, execute o comando a seguir para iniciar a configuração do WebSphere MQ agent.

   ```
   ./mq-agent.sh config instance_name
   ```

   em que *instance_name* é o nome da instância que você iniciou.
2. Siga as opções para configurar a instância de agente.

   O nome do gerenciador de filas é necessário. Para as outras opções, se nenhuma mudança for necessária, use o valor padrão.
3. Quando aparecer a opção `Nome do agente`, especifique o qualificador intermediário para o nome do sistema gerenciado.

   Lembre-se: O nome do sistema gerenciado completo é *monitoredqueuemanagername*:*agentname*:MQ. O comprimento máximo para o nome completo do sistema gerenciado é de 32 caracteres, portanto, o comprimento máximo para o qualificador intermediário *agentname* depende do comprimento do nome do gerenciador de filas. Se o valor especificado para a opção `Nome do agente` excede o comprimento máximo, o valor para *agentname* é truncado para não ultrapassar 8 caracteres.

   Por exemplo, para monitorar um gerenciador de filas que é nomeado PERSONNEL no nó AIX1 enquanto outro gerenciador de filas que é denominado PERSONNEL está em um nó que é nomeado LINUX2, execute o comando a seguir primeiro no nó AIX1:

   ```
   ./mq-agent.sh config PERSONNEL
   ```

   Em seguida, especifique o nome do agente quando a opção *Nome do agente* aparecer:

   ```
   Nome do agente (o padrão é: ): AIX1
   ```

   Para monitorar simultaneamente o gerenciador de filas PERSONNEL no nó LINUX2, execute o comando a seguir primeiro:

   ```
   ./mq-agent.sh config PERSONNEL
   ```

   Em seguida, especifique o nome do agente:

   ```
   Nome do agente (o padrão é: ): LINUX2
   ```

   Lembre-se: Os nomes dos nós do agente são usados para a opção `Nome do agente` nas amostras de código para propósito exploratório somente. É possível especificar outras sequências para a opção `Nome do agente`.

Configuração silenciosa

Procedimento

Para usar o parâmetro **AGTNAME** no arquivo silencioso de resposta, conclua as etapas a seguir:

1. Abra o arquivo silencioso de resposta `mq_silent_config.txt` em um editor de texto.
2. Especifique um nome de agente para o parâmetro **AGTNAME**.

   Lembre-se: O nome do sistema gerenciado completo é *monitoredqueuemanagername*:*agentname*:MQ. O comprimento máximo para o nome completo do sistema gerenciado é de 32 caracteres, portanto, o comprimento máximo para o qualificador intermediário *agentname* depende do comprimento do nome do gerenciador de filas. Se o valor que é especificado para o parâmetro **AGTNAME** exceder o comprimento máximo, o valor para *agentname* será truncado em não menos do que 8 caracteres.
3. Salve e feche o arquivo `mq_silent_config.txt` e, em seguida, execute o seguinte comando a partir da linha de comandos:

   ```
   install_dir/BIN/mq-agent.sh config instance_name path_to_responsefile
   ```

em que *instance_name* é o nome da instância que você configura e *path_to_responsefile* é o caminho completo do arquivo silencioso de resposta.

O que Fazer Depois
Efetue login no Console do Cloud APM. Se a instância do agente com um MSN anterior ainda é exibida como off-line, edite seu aplicativo para removê-la e, em seguida, inclua a nova instância do agente com o nome de agente designado.

Configurando o rastreamento de transações para o WebSphere MQ agent

Os dados de rastreamento de transação para o IBM MQ (WebSphere MQ) podem ser exibidos nos painéis de middleware e de topologia após a ativação da coleta de dados na página **Configuração do Agente** para o WebSphere MQ agent.

Antes de Iniciar

- Certifique-se de que a coleta de informações de rastreio de atividade do aplicativo MQI esteja ativada no gerenciador de filas. Se não fez isso antes da configuração e início do WebSphere MQ agent, siga as instruções em "Ativando o rastreio de atividade do aplicativo MQI" na página 934 e, em seguida, reinicie o agente.
- Certifique-se de que a versão do IBM MQ (WebSphere MQ) que você está usando é suportada pelo recurso de rastreamento de transação. Para obter informações atualizadas sobre o IBM MQ (WebSphere MQ) suportado, consulte a instrução de pré-requisitos em Relatório de Requisitos Detalhados do Sistema para o WebSphere MQ agent.
- Certifique-se de que o WebSphere MQ agent esteja configurado para monitorar o gerenciador de filas. Para obter instruções, veja "Configurando o WebSphere MQ agent" na página 935.

Lembre-se: Verifique se você atualizou o WebSphere MQ agent para a versão mais recente. Deve-se fazer upgrade do agente e configurar e ativar o rastreamento de transações para ver os dados em alguns dos widgets, como o widget Volume de mensagens.

Procedimento

Para configurar o rastreamento de transação para o WebSphere MQ agent, conclua as etapas a seguir:

1. A partir da barra de navegação, clique em **Configuração do Sistema** > **Configuração do Agente**.
   A página **Configuração do Agente** é exibida.
2. Clique na guia **WebSphere MQ**.
3. Selecione as caixas de seleção para os gerenciadores de filas que você deseja monitorar e execute uma das ações a seguir a partir da lista de **Ações**:
   - Para ativar o rastreamento de transações, clique em **Configurar rastreamento de transações** > **Ativado**. O status na coluna **Rastreamento de Transação** é atualizado para Ativado.

     Dica: O rastreamento de filas de alias e filas remotas é ativado por padrão. Para reduzir o volume de dados que estão sendo rastreados, é possível desativar o rastreamento de filas de alias e remotas clicando em **Configurar Rastreamento de Fila de Alias** > **Desativado** a partir da lista de **Ações**. Após o rastreamento de filas de alias e remotas ser desativado, as filas de alias e filas remotas são eliminadas da visualização Topologia de Transação.
   - Para desativar o rastreamento de transação, clique em **Configurar Rastreamento de Transação** > **Desativado**. O status na coluna **Rastreamento de Transação** é atualizado para Desativado.

Resultados
Você configurou o WebSphere MQ agent para rastrear os gerenciadores de filas selecionados. Os dados de rastreamento de transação podem ser exibidos nos painéis de middleware e de topologia. Para obter mais informações, consulte "Incluindo aplicativos middleware no Painel de Desempenho do Aplicativo " na página 96.

Ativando a coleta de dados para histórico de longo prazo de fila e de canal

Por padrão o histórico de longo prazo de fila e o histórico de longo prazo de canal não são coletados e não são exibidos em nenhum dos painéis ou widgets de grupo predefinidos. No entanto, é possível ativar o agente para coletar os dados do histórico de longo prazo e, em seguida, usar a guia **Detalhes do atributo** para consultar os dados coletados.

Antes de Iniciar

Assegure que o WebSphere MQ agent esteja instalado e configurado. Para obter informações, consulte "Configurando o WebSphere MQ agent" na página 935.

Sobre Esta Tarefa

Os dados do histórico de longo prazo de canal ou os dados do histórico de longo prazo de fila podem ser úteis para detectar problemas com canais ou filas individuais.

Se você for um usuário do Tivoli Data Warehouse, o agente também poderá enviar os dados do histórico de longo prazo ao Tivoli Data Warehouse para processamento adicional.

Procedimento

Conclua as seguintes etapas para ativar o WebSphere MQ agent para coletar dados do histórico de longo prazo de fila e dados do histórico de longo prazo de canal:

1. Abra o seguinte arquivo de ambiente do agente com um editor de texto. Se o arquivo `mq.environment` não existir, crie-o.
   - Linux AIX *install_dir*`/config/mq.environment`
   - Windows *install_dir*`\Config\KMQENV_`*instance*

   em que:
   - *install_dir* é o diretório de instalação do agente. O padrão é `/opt/ibm/apm` em sistemas Linux e AIX e `C:\IBM\APM` em sistemas Windows.
   - *instance* é o nome da instância do agente.
2. Ative a coleta de dados configurando o valor **LH_COLLECTION** como ENABLED.

   ```
   LH_COLLECTION=ENABLED
   ```
3. Opcional: Se você for um usuário do Tivoli Data Warehousee desejar que o agente envie os dados coletados para o Tivoli Data Warehouse, configure o valor **LH_PVTHISTORY** como ENABLED.

   ```
   LH_PVTHISTORY=ENABLED
   ```

   Lembre-se: Ative esta opção somente se for necessário que os dados coletados sejam enviados ao Tivoli Data Warehouse.
4. Salve sua mudança e reinicie o agente.

Resultados

O WebSphere MQ agent inicia a coleta de dados do histórico de longo prazo de fila e dados do histórico de longo prazo de canal. Se você especificou LH_PVTHISTORY=ENABLED, os dados do histórico de longo prazo coletados também poderão ser enviados ao Tivoli Data Warehouse.

O que Fazer Depois

Use a guia **Detalhes do atributo** para visualizar os dados coletados no painel para a instância de agente configurada. Selecione **Channel_Long-Term_History** ou **Queue_Long-Term_History** da lista **Conjunto de dados**. Para obter informações adicionais sobre a guia **Detalhes do atributo**, consulte "Criando uma página de gráfico ou tabela customizada" na página 1093.

Ativando o monitoramento de estatísticas de fila para o gerenciador de filas do IBM MQ

Por padrão, as estatísticas de fila não são coletadas e nem exibidas em nenhum widget de grupo widget ou painel predefinido. No entanto, é possível ativar o agente para coletar estatísticas para o gerenciador de filas e, então, visualizar os dados coletados.

Antes de Iniciar

Assegure que o WebSphere MQ agent esteja instalado e configurado. Para obter informações, consulte "Configurando o WebSphere MQ agent" na página 935.

Procedimento

Conclua as etapas a seguir para permitir que o WebSphere MQ agent colete dados estatísticos:

1. Configure o gerenciador de filas para coletar informações de estatísticas de fila. Execute o seguinte comando MQSC:

   ```
   ALTER QMGR STATQ(ON)
   ```

2. Configure o intervalo no qual os dados contábeis serão coletados. Execute o seguinte comando:

   ```
   ALTER QMGR STATINT(n)
   ```

   Em que **n** é o número de segundos durante os quais os dados contábeis são coletados.

3. Ative a coleta de informações estatísticas para uma fila específica. Execute o seguinte comando MQSC:

   ```
   ALTER QLOCAL(queue_name) STATQ(QMGR)
   ```

   Em que **queue_name** é o nome da fila para a qual você deseja coletar informações estatísticas.

O que Fazer Depois

Use um dos métodos a seguir para visualizar os dados de monitoramento de estatísticas do MQ Queue:

- Visualize os dados de monitoramento da guia **Detalhes do Atributo** do conjunto de dados **MQ_Queue_Statistics**. Para obter informações adicionais sobre a guia **Detalhes do atributo**, consulte "Criando uma página de gráfico ou tabela customizada" na página 1093.
- Defina os limites com base na **Contagem de Mensagens Expiradas** e outras métricas do **MQ_Queue_Statistics**. Para obter informações adicionais sobre limites, consulte "Limites e grupos de recursos" na página 976.

Monitorando remotamente os gerenciadores de filas no MQ Appliance

É possível usar o WebSphere MQ agent para monitorar o gerenciador de filas remotas no ambiente do MQ Appliance.

Antes de Iniciar

- Instale o WebSphere MQ agent em uma plataforma suportada.
- Instale o IBM MQ Client. A versão do cliente MQ deve ser igual à versão do MQ Queue Manager remoto.

Procedimento

1. Configure a conexão com o gerenciador de filas remotas. No gerenciador de filas remotas, defina um canal de conexão do servidor e um listener que seja usado para comunicação com o agente de monitoramento. Execute o seguinte comando:

   ```
   M2000# mqcli
   M2000(mqcli)#runmqsc qmgr_remote
   > DEFINE LISTENER(listener) TRPTYPE(TCP)
   PORT(port_NO)
   > DEFINE CHANNEL(chl_name)CHLTYPE(SVRCONN)
   ```

```
TRPTYPE(TCP)
CONNAME('host_IP(port_NO)')
QMNAME(Qmgr_remote)
> END
```

em que:

- *qmgr_remote* é o nome do gerenciador de filas remotas.
- *listener* é o nome do listener no gerenciador de filas remotas.
- *port_NO* é o número da porta a ser usado para o listener.
- *chl_name* é o nome designado para ambos o canal do servidor e o canal do cliente.
- *host_IP* é o endereço IP do sistema remoto.

2. Configure o listener para iniciar automaticamente e, em seguida, inicie o listener no gerenciador de filas remotas executando os comandos a seguir no sistema remoto:

```
M2000# mqcli
M2000(mqcli)#runmqsc qmgr_remote
> ALTER LISTENER(listener) TRPTYPE(tcp)
CONTROL(qmgr_remote)
> START LISTENER(listener)
> END
```

3. Certifique-se de que as configurações de autenticação de canal estejam configuradas corretamente para o ID do usuário usado para iniciar a instância de agente do MQ. Para obter mais informações, consulte Configurando um gerenciador de filas para aceitar conexões do cliente no IBM MQ Appliance Knowledge Center.
4. Crie uma instância do WebSphere MQ agent para monitoramento remoto seguindo as instruções em “Configurando o WebSphere MQ agent” na página 935 e forneça informações de conexão do gerenciador de filas remotas nos prompts após **Configurações de Monitoramento Remoto**.

```
Remote Monitoring Settings (For a local queue manager, just press Enter in
this section) :
Connection name for remote monitoring, for example: 192.168.1.1(1415)
Connection Name (default is: null):
Channel name for remote monitoring, SYSTEM.DEF.SVRCONN is as default.
Channels (default is: null):
```

5. Inicie a instância do WebSphere MQ agent.

Monitorando remotamente os gerenciadores de filas de HA no MQ Appliance

Para monitorar remotamente o gerenciador de filas de HA no MQ Appliance, existem duas opções. Uma é usar uma única instância de agente para conectar-se a qualquer sistema que tenha o gerenciador de filas ativo. A outra opção é usar a instância de agente separada para cada appliance no qual o gerenciador de filas possa está em execução.

Sobre Esta Tarefa

Somente a segunda opção é explicada aqui. Para usar diferentes instâncias de agente, você precisa de duas instalações do WebSphere MQ agent nos sistemas Linux ou UNIX. Nos sistemas Windows, você precisa somente de uma instalação do agente e criar instâncias de agentes separadas.

Procedimento

- Linux AIX

  Execute as etapas a seguir para usar o WebSphere MQ agent instalado nos sistemas Linux ou UNIX para monitoramento remoto:

  a) Instale o WebSphere MQ agent em diferentes diretórios no sistema.

  b) Crie uma instância de cada WebSphere MQ agent instalado. Para obter instruções, veja “Configurando o WebSphere MQ agent” na página 935.

c) Modifique o arquivo de configuração de cada instância de agente para ativar o monitoramento remoto substituindo o conteúdo pelas linhas a seguir:

```
SET GROUP NAME (GROUP1) -
DEFAULT(YES) -
RETAINHIST(120) -
COMMAND (YES) -
MSGACCESS(DESC) -
EVENTS(REMOVE) -
ACCOUNTINGINFO(REMOVE) -
STATISTICSINFO(REMOVE)

SET MANAGER NAME(qmgr_name) REMOTE(YES)
SET AGENT NAME(ID_agente)
SET QUEUE NAME(*) MGRNAME(qmgr_name)
QDEFTYPE(PREDEFINED)
SET CHANNEL NAME(*) MGRNAME(qmgr_name)
PERFORM STARTMON SAMPINT(300) HISTORY(NO)
```

em que:

– *qmgr_name* é o nome do gerenciador de filas de HA.

– *agentID* é o ID para identificar o sistema do gerenciador de filas. É geralmente o nome do host ou o endereço IP do sistema remoto no qual o gerenciador de filas de HA está em execução.

O nome e o caminho do arquivo de configuração é *install_dir*/config/*hostname*_mq_*qmgr_name*.cfg.

d) Crie um par de canais do cliente e do servidor entre o gerenciador de filas primárias e o WebSphere MQ agent, entre o gerenciador de filas secundárias e o WebSphere MQ agent no sistema remoto no qual o gerenciador de filas primárias está instalado.

Lembre-se: Deve-se executar todos os comandos a seguir antes de continuar na próxima etapa.

a. Execute os comandos a seguir para o gerenciador de filas primárias:

```
M2000# mqcli
M2000(mqcli)#runmqsc qmgr_primary
>DEFINE LISTENER(listener_primary) TRPTYPE(TCP)
PORT(port_no_primary)
>DEFINE CHANNEL(chl_name_primary)
CHLTYPE(SVRCONN) TRPTYPE(TCP)
>DEFINE CHANNEL(chl_name_primary)
CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('host_IP(port_no_primary)')
QMNAME(qmgr_primary)
```

em que:

– *qmgr_primary* é o nome do gerenciador de filas primárias.

– *listener_primary* é o nome do listener para o gerenciador de filas primárias.

– *port_no_primary* é o número da porta que é usado pelo listener.

– *chl_name_primary* é o nome desejado a ser designado para ambos o canal do servidor e o canal do cliente.

– *host_IP* é o endereço IP do sistema no qual o gerenciador de filas primárias está instalado.

b. Execute os comandos a seguir para o gerenciador de filas secundárias no gerenciador de filas primárias. Isso é para incluir as informações de conexão para o gerenciador de filas secundário no arquivo de tabela de definição de canal de cliente do gerenciador de filas primário. O mesmo agente pode então se conectar ao gerenciador de filas secundário automaticamente quando o gerenciador de filas primário sofrer failover.

```
>DEFINE
LISTENER(listener_secondary) TRPTYPE(TCP)
PORT(port_no_secondary)
>DEFINE CHANNEL(chl_name_secondary)
CHLTYPE(SVRCONN) TRPTYPE(TCP)
>DEFINE CHANNEL(chl_name_secondary)
CHLTYPE(CLNTCONN) TRPTYPE(TCP)
```

```
CONNAME('host_IP(port_no_secondary)')
QMNAME(qmgr_secondary)
```

em que:

- *qmgr_secondary* é o nome do gerenciador de filas secundárias no sistema remoto. É o mesmo que o nome do gerenciador de filas primárias.
- *listener_secondary* é o nome do listener para o gerenciador de filas secundárias.
- *port_no_secondary* é o número da porta que é usado pelo listener.
- *chl_name_secondary* é o nome desejado a ser designado para ambos o canal do servidor e o canal do cliente.
- *host_IP* é o endereço IP do sistema no qual o gerenciador de filas secundárias está instalado.

c. Finalmente, execute o comando a seguir:

```
> END
>EXIT
```

e) Crie o arquivo de tabela de definição de canal de cliente (AMQCLCHL.TAB) para a instância do WebSphere MQ agent no primeiro dispositivo do MQ.

a. Use o comando **runmqsc** ou o comando **runmqsc -n** para criar o arquivo AMQCLCHL.TAB para o gerenciador de filas no primeiro dispositivo do MQ:

```
runmqsc -n
>DEFINE CHANNEL(chl_name_primary) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
>CONNAME('host_IP_appliance1(port_no_primary)') QMNAME(qmgr_name)
```

em que *host_IP_appliance1* é o endereço IP do primeiro dispositivo do MQ; *chl_name_primary* e *port_no_primary* são iguais aos definidos na Etapa 4.

Dica: Por padrão, o arquivo AMQCLCHL.TAB é criado no diretório var/mqm/qmgrs/*qmgr_name*/@ipcc.

b. Mova o arquivo primário AMQCLCHL.TAB para o diretório *agent_install_dir*/*arch*/mq/bin no sistema em que o WebSphere MQ agent está instalado para o gerenciador de filas primário.

f) Crie o arquivo de tabela de definição de canal de cliente (AMQCLCHL.TAB) para a instância do WebSphere MQ agent no segundo dispositivo do MQ.

a. Use o comando **runmqsc** ou o comando **runmqsc -n** para criar o arquivo AMQCLCHL.TAB para o gerenciador de filas no segundo dispositivo do MQ:

```
runmqsc -n
>DEFINE CHANNEL(chl_name_secondary) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
>CONNAME('host_IP_appliance2(port_no_secondary)') QMNAME(qmgr_name)
```

em que *host_IP_appliance2* é o endereço IP do segundo dispositivo do MQ; *chl_name_secondary* e *port_no_secondary* são iguais aos definidos na Etapa 4.

b. Mova o arquivo secundário AMQCLCHL.TAB para o diretório *agent_install_dir*/*arch*/mq/bin no sistema em que o WebSphere MQ agent está instalado para o gerenciador de filas secundário.

g) Certifique-se de que essas configurações de autenticação de canal estejam configuradas apropriadamente para o ID do usuário usado para configurar a conexão entre a instância de agente e o gerenciador de filas.

h) Inicie todos os listeners para o gerenciador de filas monitoradas remotamente e inicie todas as instâncias do WebSphere MQ agent.

- Windows

Execute as etapas a seguir para usar o WebSphere MQ agent instalado nos sistemas Windows para monitoramento remoto:

a) Instale o WebSphere MQ agent no sistema Windows.

b) Crie duas instâncias do WebSphere MQ agent para cada gerenciador de filas de HA.

c) Modifique o arquivo de configuração de cada instância de agente para ativar o monitoramento remoto substituindo o conteúdo pelas linhas a seguir:

```
SET GROUP NAME (GROUP1) -
DEFAULT(YES) -
RETAINHIST(120) -
COMMAND (YES) -
MSGACCESS(DESC) -
EVENTS(REMOVE) -
ACCOUNTINGINFO(REMOVE) -
STATISTICSINFO(REMOVE)

SET MANAGER NAME(qmgr_name) REMOTE(YES)
SET AGENT NAME(ID_agente)
SET QUEUE NAME(*) MGRNAME(qmgr_name)
QDEFTYPE(PREDEFINED)
SET CHANNEL NAME(*) MGRNAME(qmgr_name)
PERFORM STARTMON SAMPINT(300) HISTORY(NO)
```

em que:

– *qmgr_name* é o nome do gerenciador de filas de HA.

– *agentID* é o ID para identificar o sistema do gerenciador de filas. É geralmente o nome do host ou o endereço IP do sistema remoto no qual o gerenciador de filas de HA está em execução.

Dica: O nome e o caminho do arquivo de configuração é *install_dir* \TMAITM6_x64\mq_<*instance_name*>.cfg.

d) Crie um par de canais do cliente e do servidor entre o gerenciador de filas primárias e o WebSphere MQ agent, entre o gerenciador de filas secundárias e o WebSphere MQ agent no sistema remoto no qual o gerenciador de filas primárias está instalado.

Lembre-se: Deve-se executar todos os comandos a seguir antes de continuar na próxima etapa.

a. Execute os comandos a seguir para o gerenciador de filas primárias:

```
M2000# mqcli
M2000(mqcli)#runmqsc qmgr_primary
>DEFINE LISTENER(listener_primary) TRPTYPE(TCP)
PORT(port_no_primary)
>DEFINE CHANNEL(chl_name_primary)
CHLTYPE(SVRCONN) TRPTYPE(TCP)
>DEFINE CHANNEL(chl_name_primary)
CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('host_IP(port_no_primary)')
QMNAME(qmgr_primary)
```

em que:

– *qmgr_primary* é o nome do gerenciador de filas primárias.

– *listener_primary* é o nome do listener para o gerenciador de filas primárias.

– *port_no_primary* é o número da porta que é usado pelo listener.

– *chl_name_primary* é o nome desejado a ser designado para ambos o canal do servidor e o canal do cliente.

– *host_IP* é o endereço IP do sistema no qual o gerenciador de filas primárias está instalado.

b. Execute os comandos a seguir para o gerenciador de filas secundárias no gerenciador de filas primárias. Isso é para incluir as informações de conexão para o gerenciador de filas secundário no arquivo de tabela de definição de canal de cliente do gerenciador de filas primário. O mesmo agente pode então se conectar ao gerenciador de filas secundário automaticamente quando o gerenciador de filas primário sofrer failover.

```
>DEFINE
LISTENER(listener_secondary) TRPTYPE(TCP)
PORT(port_no_secondary)
>DEFINE CHANNEL(chl_name_secondary)
CHLTYPE(SVRCONN) TRPTYPE(TCP)
```

```
>DEFINE CHANNEL(chl_name_secondary)
CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('host_IP(port_no_secondary)')
QMNAME(qmgr_secondary)
```

em que:

- *qmgr_secondary* é o nome do gerenciador de filas secundárias no sistema remoto. É o mesmo que o nome do gerenciador de filas primárias.
- *listener_secondary* é o nome do listener para o gerenciador de filas secundárias.
- *port_no_secondary* é o número da porta que é usado pelo listener.
- *chl_name_secondary* é o nome desejado a ser designado para ambos o canal do servidor e o canal do cliente.
- *host_IP* é o endereço IP do sistema no qual o gerenciador de filas secundárias está instalado.

c. Finalmente, execute o comando a seguir:

```
> END
>EXIT
```

e) Crie o arquivo de tabela de definição de canal de cliente (AMQCLCHL.TAB) para cada instância do WebSphere MQ agent.

a. Use o comando **runmqsc** ou o comando **runmqsc -n** para criar o arquivo AMQCLCHL.TAB para o gerenciador de filas no primeiro dispositivo do MQ:

```
runmqsc -n
>DEFINE CHANNEL(chl_name_primary) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
>CONNAME('host_IP_appliance1(port_no_primary)') QMNAME(qmgr_name)
```

em que *host_IP_appliance1* é o endereço IP do primeiro dispositivo do MQ; *chl_name_primary* e *port_no_primary* são iguais aos definidos na Etapa 4.

b. Crie o arquivo AMQCLCHL.TAB para o gerenciador de filas no segundo dispositivo do MQ:

```
runmqsc -n
>DEFINE CHANNEL(chl_name_secondary) CHLTYPE(CLNTCONN) TRPTYPE(TCP)+
>CONNAME('host_IP_appliance2(port_no_secondary)') QMNAME(qmgr_name)
```

em que *host_IP_appliance2* é o endereço IP do segundo dispositivo do MQ; *chl_name_secondary* e *port_no_secondary* são iguais aos definidos na Etapa 4.

f) Renomeie o arquivo AMQCLCHL.TAB para nomes diferentes, por exemplo, NODE1.TAB e NODE2.TAB. Transfira-os para o diretório *install_dir*\TMAITM6_x64, em que *install_dir* é o diretório de instalação do WebSphere MQ agent.

g) Modifique o arquivo kmqcma_*instance_name*.ini para configurar o valor **MQCHLTAB** para o arquivo de tabela de definição de canal do cliente para cada instância de agente.
Por exemplo, configure MQCHLTAB=NODE1.TAB no arquivo kmqcma_instance1.ini e configure MQCHLTAB=NODE2.TAB no arquivo kmqcma_instance2.ini.

h) Abra o Windows Register Editor, localize a chave a seguir de **MQCHLTAB** e mude-a de AMQCLCHL.TAB para o nome do arquivo de tabela de definição de canal do cliente apropriado para cada instância de agente.

- **HKEY_LOCAL_MACHINE\SOFTWARE\Candle\KMQ\Ver730*instance1*\Environment**

  MQCHLTAB=*NODE1.TAB*

- **HKEY_LOCAL_MACHINE\SOFTWARE\Candle\KMQ\Ver730*instance2*\Environment**

  MQCHLTAB=*NODE2.TAB*

i) Certifique-se de que essas configurações de autenticação de canal estejam configuradas apropriadamente para o ID do usuário usado para configurar a conexão entre a instância de agente e o gerenciador de filas.

j) Inicie todos os listeners para o gerenciador de filas monitoradas remotamente e inicie todas as instâncias do WebSphere MQ agent.

Capítulo 8. Integrando com outros produtos e componentes

É possível integrar outros produtos e componentes ao IBM Cloud Application Performance Management para oferecer uma solução robusta.

Integrando-se ao Gerenciamento de eventos de nuvem

O Gerenciamento de eventos de nuvem fornece gerenciamento de incidente em tempo real em seus serviços, aplicativos e infraestrutura. Quando você configura a integração entre o Gerenciamento de eventos de nuvem e o IBM Cloud Application Performance Management, todos os eventos que são gerados no Cloud APM são enviados para o Gerenciamento de eventos de nuvem.

Sobre Esta Tarefa

Configure uma URL de webhook no Gerenciamento de eventos de nuvem. Então, configure o Cloud APM para usar a URL de webhook para enviar eventos para o Gerenciamento de eventos de nuvem. Para obter informações adicionais sobre o Gerenciamento de eventos de nuvem, consulte o IBM Cloud Event Management Knowledge Center.

Procedimento

1. Clique em **Integrações** na página Gerenciamento de eventos de nuvem **Administração**.
2. Clique em **Configurar uma integração**.
3. Acesse o quadro do **IBM Cloud Application Performance Management** e clique em **Configurar**.
4. Insira um nome para a integração e clique em **Copiar** para incluir a URL de webhook gerada na área de transferência. Assegure-se de salvar o webhook gerado para torná-lo disponível posteriormente no processo de configuração. Por exemplo, é possível salvá-lo em um arquivo.
5. Para iniciar o recebimento de informações de alerta do Cloud APM, assegure-se de que **Ativar o gerenciamento de eventos desta origem** esteja configurado como `Ativado` no Gerenciamento de eventos de nuvem.
6. Clique em **Salvar**.
7. Efetue login em sua assinatura do Cloud APM.
8. Navegue para **Configuração do sistema** > **Configuração avançada** > **Gerenciador de Eventos**. Para obter mais informações, consulte Configuração Avançada.
9. Cole a URL de webhook no campo **Cloud Event Management Webhook**.
10. Clique em **Salvar**.

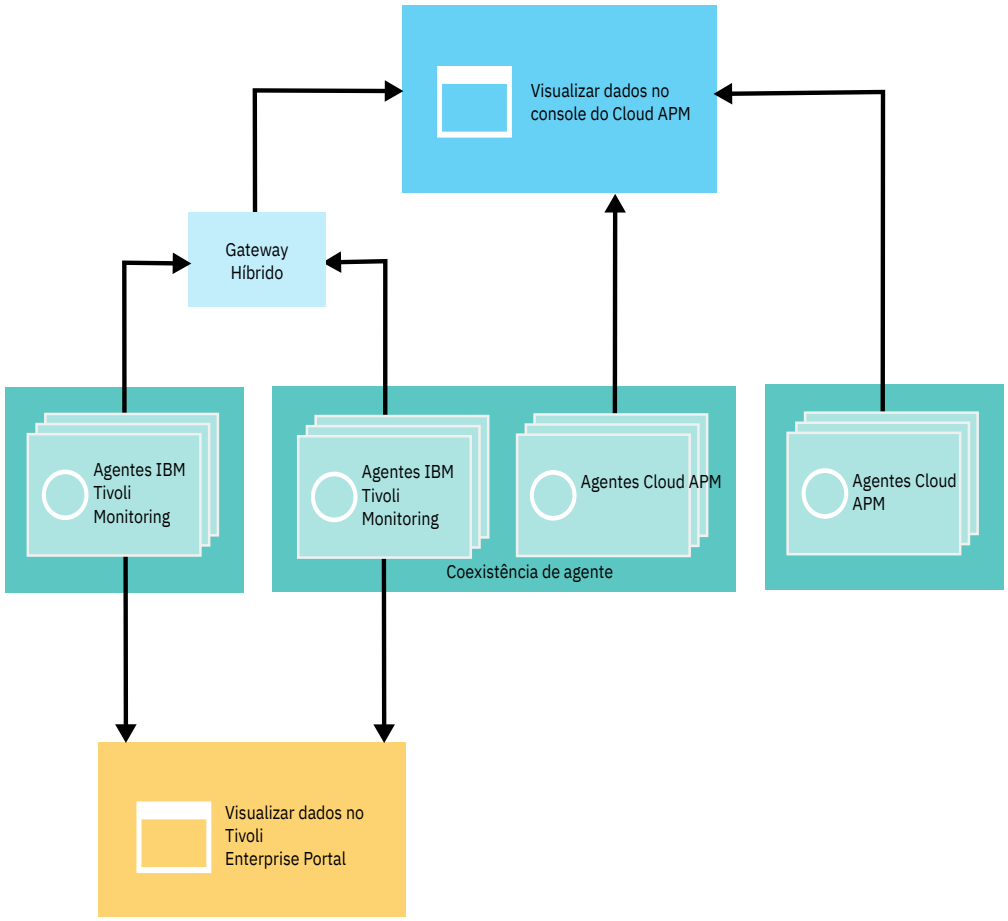
Integrando com o IBM Tivoli Monitoring V6.3

Em um ambiente que inclui produtos IBM Tivoli Monitoring e IBM Cloud Application Performance Management, é possível usar esses produtos juntos de várias formas.

As opções a seguir estão disponíveis para integração com o IBM Tivoli Monitoring:

- É possível instalar o IBM Cloud Application Performance Management Hybrid Gateway para fornecer uma visualização consolidada de sistemas gerenciados de um ou mais domínios do Tivoli Monitoring e seu domínio do Cloud APM nas páginas do Application Performance Dashboard. Para obter mais informações sobre como integrar agentes, consulte “Hybrid Gateway” na página 953.
- É possível instalar os agentes Tivoli Monitoring e Cloud APM no mesmo sistema. Quando agentes coexistem no mesmo computador, mas não no mesmo diretório, dados dos agentes Cloud APM ficam

disponíveis no Console do Cloud APM e dados dos agentes Tivoli Monitoring ficam disponíveis no Tivoli Enterprise Portal. Se agentes coexistentes estiverem monitorando os mesmos recursos, determinadas limitações se aplicam. Para obter mais informações sobre a coexistência do agente, consulte “Coexistência do agente Cloud APM e do agente Tivoli Monitoring” na página 950.



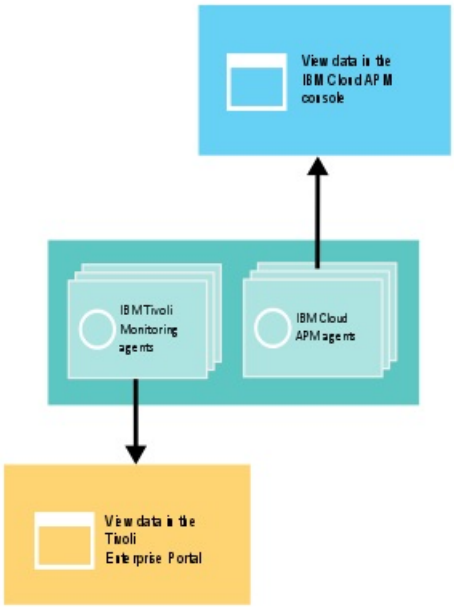
Coexistência do agente Cloud APM e do agente Tivoli Monitoring

A coexistência de agente é suportada. É possível instalar agentes do IBM Cloud Application Performance Management no mesmo computador no qual agentes do IBM Tivoli Monitoring estão instalados. Entretanto, os dois tipos de agentes não podem ser instalados no mesmo diretório.

Agentes Cloud APM são referidos como agentes da versão 8. Agentes do Tivoli Monitoring são referidos como agentes da versão 6 ou 7.

Quando agentes coexistem no mesmo computador, os dados de agentes da versão 8 ficam disponíveis no Console do Cloud APM e os dados de agentes da versão 6 ou 7 ficam disponíveis no Tivoli Enterprise Portal.

Quando agentes da versão 6 ou 7, que coexistem no mesmo computador que agentes da versão 8 e monitoram recursos diferentes, são integrados com o IBM Cloud Application Performance Management Hybrid Gateway, os dados de ambos os agentes ficam disponíveis no Console do Cloud APM. Para obter mais informações, consulte “Hybrid Gateway” na página 953.



A tabela a seguir lista os agentes Tivoli Monitoring com links da documentação:

Tabela 236. Links da documentação para agentes do Tivoli Monitoring

Agentes do Tivoli Monitoring	**Links de documentação**
IBM Monitoring Agent for Citrix Virtual Desktop Infrastructure	IBM Tivoli Monitoring for Virtual Environments Knowledge Center
IBM Tivoli Monitoring for Virtual Environments Agent for Cisco UCS	Tivoli Monitoring for Virtual Environments Knowledge Center
IBM Tivoli Monitoring for Virtual Environments Agent for Linux Kernel-based Virtual Machines	Tivoli Monitoring for Virtual Environments Knowledge Center
IBM Tivoli Monitoring for Virtual Environments Agent for VMware VI	Tivoli Monitoring for Virtual Environments Knowledge Center
IBM Tivoli Monitoring: HMC Base Agent	IBM Tivoli Monitoring Knowledge Center
IBM Tivoli Monitoring: Linux OS Agent	Tivoli Monitoring Knowledge Center
IBM Tivoli Monitoring: UNIX OS Agent	Tivoli Monitoring Knowledge Center
IBM Tivoli Monitoring: Windows OS Agent	Tivoli Monitoring Knowledge Center
ITCAM Agent for DB2	ITCAM for Applications Knowledge Center
ITCAM Agent para HTTP	ITCAM for Applications Knowledge Center
ITCAM Agent for J2EE	ITCAM for Applications Knowledge Center
ITCAM for Microsoft Applications: agente Microsoft Active Directory	IBM Tivoli Composite Application Manager for Microsoft Applications Knowledge Center
ITCAM for Microsoft Applications: Microsoft Cluster Server Agent	ITCAM for Microsoft Applications Knowledge Center
ITCAM for Microsoft Applications: Microsoft Exchange Server Agent	ITCAM for Microsoft Applications Knowledge Center
ITCAM for Microsoft Applications: Microsoft Hyper-V Server Agent	ITCAM for Microsoft Applications Knowledge Center

Tabela 236. Links da documentação para agentes do Tivoli Monitoring (continuação)	
Agentes do Tivoli Monitoring	**Links de documentação**
ITCAM for Microsoft Applications: Microsoft Internet Information Services Agent	ITCAM for Microsoft Applications Knowledge Center
ITCAM for Microsoft Applications: Skype for Business ServerAgent	ITCAM for Microsoft Applications Knowledge Center
ITCAM for Microsoft Applications: Microsoft .NET Framework Agent	ITCAM for Microsoft Applications Knowledge Center
ITCAM for Microsoft Applications: Microsoft SharePoint Server Agent	ITCAM for Microsoft Applications Knowledge Center
Monitoring Agent for Microsoft SQL Server	ITCAM for Microsoft Applications Knowledge Center
ITCAM Agent for SAP Applications	ITCAM for Applications Knowledge Center
ITCAM Agent for WebSphere Applications	IBM Tivoli Composite Application Manager for Application Diagnostics Knowledge Center para versão 7.1 e anterior e no ITCAM for Applications Knowledge Center para versão 7.2 e posterior.
ITCAM Agent for WebSphere DataPower Appliance	IBM Tivoli Composite Application Manager for Applications Knowledge Center
Monitoring Agent for WebSphere Message Broker	ITCAM for Applications Knowledge Center
Monitoring Agent for WebSphere MQ	ITCAM for Applications Knowledge Center
ITCAM Extended Agent for Oracle Database	ITCAM for Applications Knowledge Center
ITCAM Monitoring Agent for SAP HANA Database	ITCAM Monitoring Agent for SAP HANA DatabaseReferência
ITCAM Web Response Time Agent	IBM Tivoli Composite Application Manager for Transactions Knowledge Center

Se os agentes coexistentes estiverem monitorando os mesmos recursos, o seguinte cenário não será suportado:

- Os agentes da Versão 6 ou 7 são integrados com o Hybrid Gateway para exibir dados de ambos os agentes no Console do Cloud APM. Por exemplo, se os agentes da versão 6 ou 7 estiverem conectados ao mesmo Servidor Cloud APM por meio do Hybrid Gateway, não use o IBM Integration Bus agent versão 8 e o Monitoring Agent for WebSphere Message Broker versão 6 ou 7 para monitorar o mesmo broker em seu sistema.

Se um agente Tivoli Monitoring, que está integrado com o Hybrid Gateway para exibir dados no Console do Cloud APM, estiver monitorando um recurso e você desejar que seu agente Cloud APM monitore esse recurso, conclua as seguintes etapas:

1. Remova o agente Tivoli Monitoring de quaisquer aplicativos que o incluírem.
2. Remova o agente Tivoli Monitoring do grupo do sistema gerenciado Tivoli Monitoring que o Cloud APM está configurado para usar.
3. Espere pelo menos 24 horas e, em seguida, instale o agente Cloud APM e inclua-o em um aplicativo.

Quando agentes de multi-instâncias que coexistem no mesmo computador são integrados com o Hybrid Gateway e monitoram os mesmos recursos, use nomes diferentes para cada instância para exibir dados de ambos os agentes no Console do Cloud APM.

Para agentes com um coletor de dados, dois agentes do mesmo tipo são suportados. Os dados de diagnósticos de detalhamento, de recursos e de rastreamento de transação são exibidos no Console do

Cloud APM. Dados de recurso são exibidos no Tivoli Enterprise Portal. Os agentes a seguir compartilham um coletor de dados:

Monitoring Agent for HTTP Server
O Agente do Servidor HTTP é um agente Cloud APM e o ITCAM Agent para HTTP é um agente IBM Tivoli Monitoring. Se você tiver ambos os agentes em seu ambiente, é possível configurar os dois coletores de dados no mesmo HTTP Server para ambos os agentes. Para obter informações adicionais sobre o Agente do Servidor HTTP, consulte "Configurando o monitoramento do Servidor HTTP" na página 266.

Microsoft .NET agent
Para obter mais informações sobre coexistência do Microsoft .NET agent, consulte "Ativando o rastreamento de transação no ambiente de coexistência de agentes" na página 526.

WebSphere Applications agent
Para obter mais informações sobre coexistência do WebSphere Applications agent, consulte "Configurando o WebSphere Applications agent" na página 860 e "Configurando o coletor de dados para ambiente de coexistência de agente" na página 861.

Hybrid Gateway

Para visualizar dados de monitoramento e eventos para os agentes IBM Tivoli Monitoring e OMEGAMON no Console do Cloud APM, você deve criar um grupo do sistema gerenciado e instalar o IBM Cloud Application Performance Management Hybrid Gateway no domínio do Tivoli Monitoring e configurar as comunicações no Console do Cloud APM **Gerenciador de Gateway Híbrido**. Revise as informações de plano de fundo para ajudá-lo a planejar a instalação e configuração de um ou mais Hybrid Gateways nos ambientes Tivoli Monitoring e Cloud APM.

Onde instalar o Hybrid Gateway
É possível instalar o Hybrid Gateway em um ou mais domínios do Tivoli Monitoring: um Tivoli Enterprise Monitoring Server central por domínio. Para obter detalhes sobre onde instalar o Hybrid Gateway, consulte as informações de Preparando para instalar o Hybrid Gateway. Para requisitos do sistema Hybrid Gateway, que incluem Tivoli Enterprise Portal Server, consulte o Relatório de Compatibilidade do Produto de Software Gateway Híbrido, guia **Pré-requisitos**.

Agentes Tivoli Monitoring e OMEGAMON suportados
Para que um agente do Tivoli Monitoring esteja disponível para o Hybrid Gateway, ele também deve ser suportado no Cloud APM, com exceção dos agentes iOS e OMEGAMON. Para obter uma lista de agentes e versões disponíveis do Tivoli Monitoring, consulte Agentes suportados pelo Hybrid Gateway (APM Developer Center).

Para obter uma lista de agentes do OMEGAMON que podem ser exibidos no Console do Cloud APM, consulte o tópico Introdução para sua liberação na coleção de tópicos do IBM OMEGAMON for Application Performance Management no IBM Knowledge Center.

Agentes Tivoli Monitoring e OMEGAMON no Console do Cloud APM
Depois de selecionar o aplicativo predefinido "Meus Componentes" ou um aplicativo definido no Application Performance Dashboard que inclui os sistemas gerenciados Tivoli Monitoring ou OMEGAMON (ou ambos), é possível ver um painel de status do resumo de todos os sistemas gerenciados e é possível ver um painel detalhado de uma única instância de sistema gerenciado. Também é possível criar páginas do painel na guia **Visualizações customizadas**.

Será possível visualizar eventos de situações para esses agentes na guia **Eventos**. No entanto, não é possível criar novos limites para os agentes Tivoli Monitoring e OMEGAMON no Gerenciador de Limite. Em vez disso, crie novas situações em Tivoli Monitoring.

Nem todos os eventos possíveis do Tivoli Monitoring e do OMEGAMON estão disponíveis no painel Eventos. Somente eventos de nós do agente que podem ser incluídos em um aplicativo são exibidos. Por exemplo, para o agente Tivoli Monitoring para WebSphere Application Servers, os eventos que estão associados a uma determinada instância do servidor são exibidos, mas os eventos do agente como um todo não são exibidos.

Visualize até 1500 sistemas gerenciados de cada domínio do Tivoli Monitoring

O número máximo de sistemas gerenciados, incluindo subnós, que podem ser visualizados de um domínio do Tivoli Monitoring é 1500. Por padrão, o limite é 200 sistemas. É possível planejar o suporte de uma quantia maior de sistemas. Para obter instruções, veja “Planejando um grande número de sistemas gerenciados” na página 961.

O limite para todos os domínios do Tivoli Monitoring deve estar dentro do máximo suportado pelo Cloud APM. Para obter informações adicionais, consulte “Visão Geral de Arquitetura” na página 43.

Somente monitoramento de recursos

O monitoramento de recurso está disponível para os agentes do Tivoli Monitoring. Para obter mais informações sobre o monitoramento de recurso, consulte “Ofertas e complementos” na página 45 e “Capacidades” na página 52. Se você tiver a assinatura do IBM Cloud Application Performance Management, Advanced,oferta o rastreamento de transação e os painéis de diagnósticos não estarão disponíveis para sistemas gerenciados do seu ambiente Tivoli Monitoring.

O Tivoli Authorization Policy Server afeta a disponibilidade dos sistemas gerenciados do Tivoli Monitoring

Para ambientes do Tivoli Monitoring que incluem o Tivoli Authorization Policy Server, os sistemas gerenciados disponibilizados por meio do Hybrid Gateway são afetados pelas políticas de autorização. Para obter mais informações, consulte Usando políticas de autorização baseadas em função no Tivoli Monitoring Knowledge Center.

Para obter uma demonstração por vídeo, consulte Integrando-se ao Tivoli Monitoring - Hybrid Gateway.

Preparando para instalar o Hybrid Gateway

Para instalar o IBM Cloud Application Performance Management Hybrid Gateway, primeiro você deve assegurar que seu ambiente esteja configurado corretamente. Revise as informações para ajudá-lo a planejar a instalação do Hybrid Gateway.

Onde instalar o Hybrid Gateway

O Hybrid Gateway deve ser instalado em um sistema x86-64 Red Hat Enterprise Linux v6.2 (ou posterior) que tem uma conexão de rede com IBM Tivoli Monitoring e IBM Cloud Application Performance Management.

O Hybrid Gateway poderá ser instalado no mesmo sistema que o seu Tivoli Enterprise Portal Server ou em um sistema separado do Tivoli Enterprise Portal Server se os sistemas estiverem em execução no Red Hat Enterprise Linux. No entanto, o Hybrid Gateway não pode ser instalado no mesmo sistema que o Servidor Cloud APM.

Um Tivoli Monitoring domínio tem um hub Tivoli Enterprise Monitoring Server. Quando o ambiente do Tivoli Monitoring consiste em vários domínios, é possível instalar o Hybrid Gateway em mais de um domínio.

Para requisitos do sistema relacionados ao Hybrid Gateway, clique na guia **Hardware** no Hybrid Gateway Relatório de compatibilidade de produto de software.

Configurando o Tivoli Enterprise Portal Server para o Hybrid Gateway

Para ambientes do Tivoli Monitoring onde o servidor de portal tem uma carga pesada, você deve instalar um servidor de portal dedicado separado para atender às solicitações do Hybrid Gateway. Se você configurar um servidor de portal separado:

- É possível usar o mesmo host para o servidor de portal e o Hybrid Gateway se o servidor de portal estiver executando o Red Hat Enterprise Linux.
- Certifique-se de que o servidor de portal separado tenha o suporte de aplicativo para os agentes cujos dados são exibidos no Console do Cloud APM.
- Certifique-se de que os clientes do Tivoli Enterprise Portal não estejam conectados ao servidor de portal separado para concluir tarefas administrativas, como criar áreas de trabalho customizadas, criar situações e criar grupos do sistema gerenciado.

O Tivoli Enterprise Portal Server deve estar na V6.3 Fix Pack 6 ou superior. Se seu servidor de portal estiver em uma versão anterior, os agentes Tivoli Monitoring integrados poderão não estar disponíveis para incluir um aplicativo no Console do Cloud APM.

O Provedor de dados do painel do IBM Tivoli Monitoring deve ser ativado no Tivoli Enterprise Portal Server. Para obter detalhes, consulte Verificando se o provedor de dados do painel está ativado na coleção de tópico do IBM Tivoli Monitoring no IBM Knowledge Center.

As portas TCP que devem ser abertas no Hybrid Gateway
As portas TCP a seguir devem ser abertas no Hybrid Gateway. Para cada porta, um lado envia uma solicitação e o outro lado fornece uma resposta. O lado que inicia a conexão é indicado.

- O Hybrid Gateway inicia uma conexão unidirecional com o Servidor Cloud APM na porta 443 e envia solicitações de HTTPS.

  Se o Hybrid Gateway usa um proxy de encaminhamento de passagem para se conectar ao Servidor Cloud APM, configure o Hybrid Gateway para usar a porta de proxy em vez da porta 443 para conexões unidirecionais que ele inicia com o Servidor Cloud APM. Para obter instruções, veja “Usando um proxy de encaminhamento para se comunicar com o Servidor Cloud APM” na página 957.
- Se você usa HTTP para se comunicar com o servidor de portal, abra a porta 15200. Se você usar HTTPS, abra a porta 15201. O Hybrid Gateway inicia uma conexão unidirecional com o servidor de portal na porta 15200 ou 15201. Para usar uma porta customizada, atualize o valor da configuração da **Porta do Servidor de Portal**. Para obter mais informações, consulte “Gerenciador Hybrid Gateway” na página 963.

  Como alternativa, se o Hybrid Gateway usar um proxy de encaminhamento de passagem para conectar-se ao servidor de portal, configure o Hybrid Gateway para usar a porta de proxy no lugar para conexões unidirecionais que ele inicia com o servidor de portal. Configure o valor da configuração da **Porta de Proxy de Passagem**. Para obter mais informações, consulte “Gerenciador Hybrid Gateway” na página 963.
- Para que o Hybrid Gateway atenda eventos EIF de entrada a partir do Tivoli Enterprise Monitoring Server, abra a porta 9998. O servidor de monitoramento inicia uma conexão unidirecional com o Hybrid Gateway na porta 9998. O utilitário de instalação exibirá um aviso se essa porta não estiver aberta.

Privilégios de administrador necessários para executar o script de instalação do Hybrid Gateway
Você deve executar o script de instalação do Hybrid Gateway com privilégios de administrador. Para obter uma lista completa de sistemas operacionais suportados, consulte Requisitos do sistema (APM Developer Center)

Instalando o Gateway Híbrido
Faça o download e instale o IBM Cloud Application Performance Management Hybrid Gateway para visualizar sistemas gerenciados a partir de seu domínio do IBM Tivoli Monitoring no Console do Cloud APM.

Antes de Iniciar
Revise e conclua as tarefas de preparação necessárias em Preparando para instalar o Hybrid Gateway.

Procedimento

Conclua as seguintes etapas para instalar o Hybrid Gateway no domínio do Tivoli Monitoring:

1. Faça download do pacote do Hybrid Gateway.
   O arquivo `APM_Hybrid_Gateway_Install.tar` contém o Hybrid Gateway e o script de instalação.
   a) Conecte-se à sua conta e acesse Produtos e serviços no IBM Marketplace.
   b) Em **IBM Cloud APM**, clique em **Mais ações**.
   c) Clique em **Mostrar pacotes adicionais**.
   d) Selecione **Gateway Híbrido**. Se necessário, role para baixo para localizar a entrada.

e) Clique **Download**.

2. Se necessário, transfira o arquivo para o sistema no qual o Hybrid Gateway será executado.
3. Digite o seguinte comando para extrair os arquivos:

```
tar -xf APM_Hybrid_Gateway_Install.tar
```

O archive contém um script que é usado para implementar o Hybrid Gateway. O script de instalação é extraído no diretório e os arquivos do Hybrid Gateway são extraídos em subdiretórios.

4. Altere para o diretório Hybrid Gateway e execute o script de instalação com privilégios de usuário raiz:

```
cd APM_Hybrid_Gateway_Install_version
./install.sh
```

em que *version* é a versão atual, como 8.1.4.0.

Uma varredura de pré-requisito de seu ambiente é iniciada e demora alguns minutos para ser concluída. Se algum dos requisitos estiver ausente, uma mensagem direcionará você para um arquivo de log com a razão da falha. Um pré-requisito, como espaço em disco insuficiente, para a instalação. Você deverá resolver a falha e iniciar a instalação novamente. Também é possível desativar a verificação de pré-requisito, conforme descrito em Ignorando o scanner de pré-requisito.

5. Depois que o sistema passar pela varredura de pré-requisito, responda ao prompt para aceitar o contrato de licença, selecionando 1 para sim.

Uma mensagem instrui a efetuar login no Console do Cloud APM e configurar o Hybrid Gateway antes de continuar. O nome do perfil padrão, que é derivado do nome do host, também é exibido.

6. Pressione Enter para aceitar o nome padrão ou insira um nome do perfil.

Se você já criou um perfil para esse domínio do Tivoli Monitoring, use o nome idêntico que foi fornecido no Hybrid Gateway Manager. Se você ainda não criou um perfil, poderá aceitar o nome padrão ou fornecer um novo nome, mas certifique-se de acompanhar o nome, porque deve-se usar esse nome ao criar o perfil posteriormente. (Consulte “Configurando o Hybrid Gateway Utilizando o Console do Cloud APM” na página 959.)

Depois de pressionar Enter, a instalação do Hybrid Gateway continua.

Resultados

O Hybrid Gateway é instalado no diretório `/opt/ibm/hybridgateway` e é iniciado automaticamente. O arquivo de log de instalação está em `/opt/ibm/hybridgateway/logs/install-hybridgateway-`*`timestamp`*`.log`. Os arquivos de log do Hybrid Gateway estão no diretório `/opt/ibm/wlp/usr/servers/hybridgateway/logs`. Esteja ciente de que até que a conexão com o Tivoli Enterprise Portal Server esteja configurada, serão registradas falhas de conexão.

O que Fazer Depois

- É possível configurar Hybrid Gateway para usar um proxy de encaminhamento para se comunicar com o Servidor Cloud APM. Para obter instruções, veja “Usando um proxy de encaminhamento para se comunicar com o Servidor Cloud APM” na página 957.
- É possível verificar o status do Hybrid Gateway com o seguinte comando: *`install_dir`*`/hybridgateway/bin/hybridgateway.sh status`. Para mais opções, consulte “Gerenciando o Gateway Híbrido” na página 962.
- Caso você ainda não tenha criado o grupo de sistemas gerenciados para o Hybrid Gateway, siga as instruções em “Criando o grupo de sistemas gerenciados” na página 957.
- Se ainda não criou um perfil do Hybrid Gateway para o domínio do Tivoli Monitoring, siga as instruções em “Configurando o Hybrid Gateway Utilizando o Console do Cloud APM” na página 959.
- Se o ambiente do Tivoli Monitoring tiver mais de um domínio de hub, é possível instalar o Hybrid Gateway em outros domínios. Repita as etapas nesse procedimento para instalar o Hybrid Gateway em outro domínio do Tivoli Monitoring.

Usando um proxy de encaminhamento para se comunicar com o Servidor Cloud APM
É possível configurar IBM Cloud Application Performance Management Hybrid Gateway para usar um proxy de encaminhamento para se comunicar com o Servidor Cloud APM.

Procedimento

1. No host no qual você instalou o Hybrid Gateway, edite o arquivo `/opt/ibm/wlp/usr/servers/hybridgateway/bootstrap.properties`:
   - Se o Hybrid Gateway usar HTTP para se comunicar com o Servidor Cloud APM, inclua as linhas:

     ```
     http.proxyHost=proxy_host
     http.proxyPort=proxy_port
     ```

   - Se o Hybrid Gateway usar HTTPS para se comunicar com o Servidor Cloud APM, inclua as linhas:

     ```
     https.proxyHost=proxy_host
     https.proxyPort=proxy_port
     ```

   em que *proxy_host* é o nome do host ou o endereço IP do proxy, acessível a partir do host Hybrid Gateway, e *proxy_port* é a porta do proxy.
2. Reinicie o Hybrid Gateway.

Criando o grupo de sistemas gerenciados
Use o editor do grupo Objetos no cliente do Tivoli Enterprise Portal para criar um grupo com os sistemas gerenciados que você deseja visualizar no Console do Cloud APM.

Antes de Iniciar

- Os tipos de agentes IBM Tivoli Monitoring e OMEGAMON que podem ser incluídos no grupo do sistema gerenciado devem ser um dos agentes suportados. Por exemplo, para o Tivoli Monitoring, alguns agentes suportados são o Monitoring Agent for Oracle Database ou o Monitoring Agent for Linux OS.

  Para obter a lista atual de agentes do Tivoli Monitoring suportados, consulte Agentes suportados pelo Hybrid Gateway (APM Developer Center). Para obter uma lista de agentes OMEGAMON que podem ser exibidos no Console do Cloud APM, consulte o tópico Introdução na coleção de tópicos do IBM OMEGAMON for Application Performance Management no IBM Knowledge Center.
- Os agentes Tivoli Monitoring e OMEGAMON devem estar conectados à mesma infraestrutura do IBM Tivoli Monitoring. Se seu ambiente tiver vários domínios do Tivoli Monitoring, crie um grupo do sistema gerenciado para cada Tivoli Enterprise Monitoring Server central para o qual um Hybrid Gateway está instalado.
- Por padrão, é possível incluir até 200 sistemas gerenciados no grupo do sistema gerenciado para visualização do domínio do Tivoli Monitoring no Application Performance Dashboard. É possível aumentar o limite para até 1500 sistemas, executando várias etapas de planejamento. Para obter mais informações, consulte “Planejando um grande número de sistemas gerenciados” na página 961. Se você tiver vários Hybrid Gateways para um ambiente do Tivoli Monitoring com vários hubs, o grupo do sistema gerenciado para cada domínio deve estar dentro do máximo suportado pelo Cloud APM. Para obter informações adicionais, consulte Visão geral da arquitetura.
- O padrão para manipular subnós mudou na liberação do Cloud APM março 2017. Em liberações anteriores, se você tivesse agentes com subnós, como o WebSphere Applications agent, teria que designar o nó de gerenciamento ao grupo do sistema gerenciado e todos os subnós eram incluídos automaticamente. Apesar de você designar um nó de gerenciamento ao grupo do sistema gerenciado, todos os subnós eram incluídos na contagem do máximo de sistemas gerenciados.

  Na liberação do Cloud APM março de 2017 e mais recente, os subnós cujos dados de métrica você deseja exibir no Console do Cloud APM devem ser especificamente designados ao grupo do sistema gerenciado.O agente de gerenciamento será descoberto automaticamente se alguns de seus subnós forem claramente designados ao grupo do sistema gerenciado. Para aplicativos de monitoramento baseados em subnós, o Cloud APM talvez precise consultar o agente de gerenciamento para informações que são necessárias para identificar claramente os recursos de monitoramento que

aparecem no navegador do painel do Cloud APM. É por isso que, com a versão atual do modo de descoberta, o agente de gerenciamento é incluído automaticamente e pelo menos um subnó associado é designado ao grupo do sistema gerenciado configurado para uso pelo Hybrid Gateway. O modo de descoberta atual suporta o controle preciso sobre os recursos do subnó que podem ser visualizados no Console do Cloud APM e é melhor alinhado com a forma que aplicativos do Cloud APM são construídos, principalmente para aplicativos que envolvem grandes conjuntos de instâncias de recurso do subnó. Sempre use o modo de descoberta padrão atual quando estiver integrando agentes do OMEGAMON com o Cloud APM.

É possível especificar qual versão do modo de descoberta o Hybrid Gateway usa, designando o valor apropriado a uma propriedade externa chamada `MSN_DISCOVERY_MODE`, que é processada pelo Hybrid Gateway durante a inicialização.Para controlar qual modo de descoberta é usado pelo Hybrid Gateway, inclua a propriedade `MSN_DISCOVERY_MODE` (ou mude seu valor atual) no seguinte arquivo de propriedades no sistema em que o Hybrid Gateway está instalado e, em seguida, reinicie o Hybrid Gateway.

```
HG_install_dir/wlp/usr/servers/hybridgateway/bootstrap.properties
```

Os valores possíveis para a propriedade `MSN_DISCOVERY_MODE` são:

- `MSN_DISCOVERY_MODE=1` força o Hybrid Gateway a usar o modo de descoberta do agente original, no qual todos os subnós são descobertos automaticamente para qualquer agente de gerenciamento que está designado ao grupo do sistema gerenciado do Tivoli Monitoring.
- `MSN_DISCOVERY_MODE=2` força o Hybrid Gateway a usar o novo modo de descoberta do agente padrão, no qual somente os subnós que estão claramente designados ao grupo do sistema gerenciado são consultados pelo Hybrid Gateway. O agente ou agentes de gerenciamento associados são descobertos automaticamente.

- Se você preferir criar o grupo do sistema gerenciado com os comandos **`tacmd createsystemlist`** e **`tacmd editsystemlist`** IBM Tivoli Monitoring, consulte a *Referência de Comando do IBM Tivoli Monitoring* (https://www.ibm.com/support/knowledgecenter/SSTFXA_6.3.0/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm) para obter informações sobre como executar os comandos.

Procedimento

Execute estas etapas para criar um grupo de sistemas gerenciados no cliente do Tivoli Enterprise Portal.

1. Inicie o cliente do Tivoli Enterprise Portal usando um ID de usuário e senha que tenha acesso completo a todos os tipos de sistemas gerenciados (**Aplicativos Permitidos** é configurado como **Todos os Aplicativos** para o ID do usuário).
2. Clique em **Editor do Grupo de Objetos**.
3. Expanda o objeto **Sistema Gerenciado** e selecione **Todos os Sistemas Gerenciados** para combinar vários tipos de agente (como Windows OS e Oracle) no grupo do sistema gerenciado. Se você preferir que o grupo do sistema gerenciado contenha somente um tipo de agente de monitoramento, como Linux OS ou WebSphere Applications, selecione o tipo de agente.
4. Clique em **Criar Novo Grupo** e insira um nome para o grupo do sistema gerenciado.

   O nome pode ser composto por letras e números e não deve ter espaços, pontuação ou caracteres especiais, exceto o caractere sublinhado (_).

   Depois de clicar em **OK**, o novo grupo de sistemas gerenciados é exibido na pasta de sistemas gerenciados.
5. Selecione os sistemas gerenciados da lista **Sistemas gerenciados disponíveis** e para movê-los para a lista **Designados**.

   É possível selecionar vários sistemas gerenciados, mantendo pressionada a tecla Ctrl enquanto estiver clicando em cada sistema gerenciado. Depois de selecionar um sistema gerenciado, é possível pressionar Shift+clique para selecionar todos os sistemas gerenciados entre essa seleção e a primeira.
6. Depois de incluir sistemas gerenciados no grupo, clique em **OK** para salvar suas mudanças e fechar o Editor de grupo de objetos.

O que Fazer Depois

- Depois de criar o grupo do sistema gerenciado e de instalar o Hybrid Gateway, é preciso configurar o Hybrid Gateway no Console do Cloud APM.
- Para a configuração, especifique o nome do grupo de sistemas gerenciados criado, o ID de usuário do Tivoli Enterprise Portal que tem permissão para acessar todos os tipos de agentes e o nome de host e a porta do Tivoli Enterprise Portal Server.
- Para obter instruções de instalação, consulte "Instalando o Gateway Híbrido" na página 955.
- Para obter instruções de configuração, consulte "Configurando o Hybrid Gateway Utilizando o Console do Cloud APM" na página 959.

Configurando o Hybrid Gateway Utilizando o Console do Cloud APM

Use a página **Gerenciador de Gateway Híbrido** no Console do Cloud APM para configurar o IBM Cloud Application Performance Management Hybrid Gateway para conectar-se ao Tivoli Enterprise Portal Server e especificar o grupo do sistema gerenciado.É possível criar um perfil do Hybrid Gateway para cada Tivoli Enterprise Monitoring Server central em seu ambiente.

Procedimento

Conclua as seguintes etapas para configurar o Hybrid Gateway no Console do Cloud APM.

1. Caso ainda não tenha efetuado login no Console do Cloud APM, faça-o agora.

   (Consulte "Iniciando o Console do Cloud APM" na página 975.)
2. Clique em **Configuração do Sistema** > **Hybrid Gateway Gerenciador**.

   A página é exibida com uma tabela de todos os Hybrid Gateways que foram configurados para os domínios do Tivoli Monitoring. Se um perfil com um nome em branco for exibido, ele será para o Hybrid Gateway que foi instalado antes da liberação agosto de 2017. Para obter mais informações, consulte "Nome do Perfil" na página 963.
3. Clique em **Incluir** para abrir a janela **Incluir Gateway Híbrido**, insira um novo nome no campo **Nome do perfil** e clique em **Incluir**.

   Se você já instalou o Hybrid Gateway no domínio do Tivoli Monitoring, certifique-se de usar o mesmo nome fornecido ou aceito durante a instalação do Hybrid Gateway. O nome do perfil inserido durante a instalação e o nome inserido aqui devem ser uma correspondência exata.

   A janela **Editar Gateway Híbrido** é aberta.
4. No campo **Nome do Grupo de Sistemas Gerenciados**, digite o nome do grupo de sistemas gerenciados para o Hybrid Gateway.

   Este é o nome utilizado em "Criando o grupo de sistemas gerenciados" na página 957.
5. Especifique o endereço, a porta e o protocolo de comunicações da web do Tivoli Enterprise Portal Server:

Opção	Descrição
Nome do Host do Servidor de Portal	Insira o endereço IP do host do servidor de portal ou o nome completo do host ou do domínio.
Porta do Servidor de Portal	Digite o número da porta usada pelo servidor de portal para comunicações da web. A porta padrão é 15200 para HTTP ou 15201 para HTTPS. O valor de 0 configura a porta para o padrão 15200 para HTTP ou 15201 para HTTPS.
Protocolo do Servidor de Portal	Selecione o Internet Protocol **HTTP** ou o Internet Protocol **HTTPS** para se conectar ao servidor de portal.

6. Preencha os campos **Nome do Usuário do Servidor de Portal** e **Senha do Servidor de Portal** com o nome do usuário de logon e a senha correspondente para iniciar o cliente do Tivoli Enterprise Portal.

   O ID de usuário deve ter acesso a todos os tipos de agentes de monitoramento (**Aplicativos Permitidos** é configurado como **Todos os Aplicativos**), como o ID `sysadmin`. Para obter mais informações, consulte Administrar Usuários no Tivoli Monitoring IBM Knowledge Center.

7. Se o acesso ao servidor de portal passar por um servidor proxy, especifique o endereço, a porta e o protocolo da web:

Opção	Descrição
Nome do Host do Proxy de Passagem	Insira o endereço IP ou o nome completo do sistema host do proxy.
Porta de Proxy de Passagem	Digite o número da porta do sistema host do proxy.
Protocolo Proxy de Passagem	Selecione o protocolo usado para as comunicações feitas por meio do proxy: HTTP ou HTTPS

Resultados
Após clicar em **Salvar**, é estabelecida uma conexão com o serviço do Hybrid Gateway e os sistemas gerenciados do domínio do Tivoli Monitoring são descobertos. O grupo de sistemas gerenciados é pesquisado a cada cinco minutos para dados de monitoramento de recurso.

O que Fazer Depois

- Você deve configurar o Tivoli Monitoring para interagir com o Cloud APM. Para obter instruções, veja "Configurando o Tivoli Monitoring para Integração com Cloud APM" na página 960.
- É possível repetir essas etapas para incluir um perfil para cada domínio do Tivoli Monitoring que você deseja para monitorar sistemas gerenciados do Cloud APM.
- É possível gerenciar perfis existentes com as ferramentas do **Gerenciador de Gateway Híbrido**:

  Selecione um Hybrid Gateway e clique em **Editar** para abrir a janela **Editar Gateway Híbrido**.
  Selecione um Hybrid Gateway do qual você não precisa mais e clique em **Excluir**. Após confirmar que você deseja excluir o Hybrid Gateway, o perfil é removido permanentemente.
  Clique em um título da coluna para classificar a tabela por essa coluna; Ctrl + Clique em outra coluna para incluir uma classificação secundária.
  Clique dentro da caixa de texto de filtro e digite o início do valor pelo qual filtrar. Ao digitar, as linhas que não atendem aos critérios são deixadas de fora. Para limpar o filtro, clique no na caixa de filtragem ou pressione a tecla backspace.

Configurando o Tivoli Monitoring para Integração com Cloud APM
Para integrar seu IBM Tivoli Monitoring domínio ao Cloud APM, deve-se concluir tarefas como: configurar o Tivoli Enterprise Portal Server e configurar o hub Tivoli Enterprise Monitoring Server.

Procedimento

Para cada domínio do Tivoli Monitoring no qual você tem um Hybrid Gateway instalado, conclua essas etapas:

1. Configure o Tivoli Enterprise Portal Server para ativar o provedor de dados do painel.
   O provedor de dados é necessário para integrar o Cloud APM com o Hybrid Gateway. Para obter instruções, consulte os seguintes tópicos:
   - Windows Windows: Instalando o servidor de portal (etapa 16c).
   - Linux AIX Configurando o servidor de portal no Linux ou AIX: procedimento da linha de comandos (etapa 14).

   Se você estiver usando o recurso Hot Standby, deve-se especificar uma substituição de domínio. O Hybrid Gateway usa o nome de domínio para coletar dados de servidores de monitoramento centrais, independentemente do hub ao qual o servidor de portal está conectado.
2. Se desejar visualizar eventos de situação de agentes do Tivoli Monitoring no Console do Cloud APM, configure o servidor de monitoramento central para um dos seguintes cenários:
   - Para enviar eventos somente para o Hybrid Gateway.

- Para enviar eventos para o Hybrid Gateway e receptores EIF adicionais, como servidores Netcool/OMNIbus.

Conclua uma das seguintes etapas, dependendo de seu cenário aplicável.

a) Para configurar o Tivoli Enterprise Monitoring Server central para enviar eventos somente para o Hybrid Gateway, conclua as etapas no tópico Configurando o servidor de monitoramento central para encaminhar eventos.

   Especifique o número da porta 9998 para o parâmetro **`ServerPort`**.
   Cloud APM não encaminha eventos do Tivoli Monitoring para o Netcool/OMNIbus. Se desejar visualizar eventos do Tivoli Monitoring no Cloud APM e no Netcool/OMNIbus, você deve configurar o Tivoli Monitoring para enviar os eventos para ambos os sistemas.

b) Para configurar o Tivoli Enterprise Monitoring Server central para enviar eventos para o Hybrid Gateway e outro receptor EIF, como um servidor Netcool/OMNIbus, configure o receptor EIF padrão usando as etapas no tópico Configurando o servidor de monitoramento central para encaminhar eventos.

   O tópico também fornece informações sobre como criar destinos EIF adicionais usando o comando **`tacmd createEventDest`**. Especifique a porta 9998 como o número da porta EIF para o destino do Hybrid Gateway.

c) Configure quaisquer situações existentes para os agentes no grupo do sistema gerenciado do Hybrid Gateway para assegurar que os eventos de situação sejam enviados ao destino EIF para o Hybrid Gateway. Para obter instruções, consulte o tópico Especificando em quais situações encaminhar eventos para o Netcool/OMNIbus.

O que Fazer Depois
Revise o Application Performance Dashboard para confirmar se os sistemas gerenciados a partir do domínio do Tivoli Monitoring são passados através do Hybrid Gateway:

1. Clique em **Desempenho** > **Application Performance Dashboard** para abrir o painel **Todos os Meus Aplicativos**.
2. Na caixa de resumo para "Meus componentes", clique em **Componentes** para abrir o painel de resumo de status para todos os sistemas gerenciados por componente (exceto o WebSphere Applications agent). Se você não tiver um aplicativo "Meus Componentes", inclua um aplicativo conforme descrito em “Gerenciando aplicativos” na página 1098.
3. Procure os sistemas gerenciados a partir do domínio do Tivoli Monitoring, indicado por um ícone de domínio do **ITM** (IBM Tivoli Monitoring) no título do widget de grupo de resumo de status. Se alguns sistemas gerenciados estiverem ausentes, acesse o Fórum do Cloud Application Performance Management e procure em "Hybrid Gateway".

É possível criar aplicativos com sistemas gerenciados a partir de seus Tivoli Monitoring domínios e incluir sistemas gerenciados do domínio do Cloud APM. Para obter mais informações, consulte “Gerenciando aplicativos” na página 1098.

Planejando um grande número de sistemas gerenciados
O número máximo de sistemas gerenciados que podem ser visualizados do domínio do IBM Tivoli Monitoring é 1500. Se você incluir um agente que tem subnós no grupo do sistema gerenciado criado para o perfil do Hybrid Gateway, todos os subnós e o agente serão considerados com relação ao limite. Por padrão, esse limite é de 200 sistemas gerenciados, mas é possível executar diversas etapas de planejamento para estender o limite.O limite para todos os domínios do Tivoli Monitoring deve estar dentro do máximo suportado pelo Cloud APM. Para obter informações adicionais, consulte “Visão Geral de Arquitetura” na página 43.

- Configure o valor da variável de ambiente Tivoli Enterprise Portal Server **`KFW_REPORT_NODE_LIMIT`** como um número maior ou igual ao número de sistemas gerenciados para o Hybrid Gateway. O valor padrão é 200. Para obter instruções, veja Tivoli Enterprise Portal Server.
  Se os sistemas gerenciados excederem essa configuração, o log de mensagens do Tivoli Enterprise Portal Server `KfwServices` exibirá uma mensagem semelhante ao seguinte exemplo:
  `56C6246F.0000-10:ctreportmanager.cpp,2864,"CTReport::Manager::executeDefiniti`

onDual") A consulta está direcionando 1497 nós que excedem o limite atual de 200 nós.

- Se estiver visualizando um grande número de sistemas, o desempenho pode ser reduzido, dependendo do tipo de agentes, da latência de rede entre o Hybrid Gateway e os sistemas gerenciados e do tamanho do ambiente monitorado por cada agente (quantidade de dados coletados e postados). Para evitar esse efeito, selecione somente os agentes que fornecem dados necessários e asseguram uma conectividade de rede rápida entre os sistemas monitorados e o host do Hybrid Gateway.
- À medida que a latência da rede aumenta, o tempo de coleta de dados de um número específico de agentes aumenta. O Hybrid Gateway tenta reunir dados de cada agente a cada 5 minutos. Se o tempo para coletar dados de todos os agentes exceder 5 minutos, o Hybrid Gateway perderá as amostras de dados e, portanto, as métricas estarão indisponíveis para alguns dos sistemas gerenciados nas páginas do Application Performance Dashboard.
- Para compensar as velocidades de rede muito lentas, é possível tentar aumentar o número de encadeamentos usados pelo Hybrid Gateway para reunir amostras de dados. O parâmetro **MAX_COLLECTOR_THREADS** do arquivo `bootstrap.properties` do Hybrid Gateway controla o número de encadeamentos. O valor padrão é 50.

Desinstalando o Gateway Híbrido
Caso não deseje mais visualizar os sistemas gerenciados do IBM Tivoli Monitoring no Console do Cloud APM, desinstale o IBM Cloud Application Performance Management Hybrid Gateway.

Procedimento

1. No diretório Hybrid Gateway *install_dir*`/hybridgateway/bin` (como `/opt/ibm/hybridgateway/bin`), execute o seguinte comando:

   ```
   ./hybridgateway.sh uninstall
   ```

   O Hybrid Gateway é removido e uma mensagem confirma que a desinstalação foi bem-sucedida. Caso haja aplicativos no Console do Cloud APM que incluam agentes híbridos, os agentes híbridos continuarão a aparecer até que a infraestrutura de monitoramento processe sua remoção.
2. No Console do Cloud APM, clique em **Configuração do Sistema** > **Gerenciador do Hybrid Gateway**.
3. Selecione o perfil do Hybrid Gateway que não é mais necessário e clique em **Excluir**.

   Após confirmar que você deseja excluir o Hybrid Gateway, o perfil é removido permanentemente.

O que Fazer Depois

- Para remover qualquer sistema gerenciado por agente híbrido de um aplicativo no Console do Cloud APM, siga as instruções em “Gerenciando aplicativos” na página 1098 para editar um aplicativo.
- Se, em vez da remoção bem-sucedida do software, você obtiver uma mensagem de erro semelhante à mostrada neste exemplo, revise o arquivo de log para obter as possíveis causas:

  ```
  error: Failed dependencies:
  ibm-java-x86_64-jre is needed by (installed) smai-kafka-00.08.00.00-1.el6.x86_64
  Uninstallation failed. The uninstaller was unable to remove some of the components, please inspect the
   log file ("/tmp/hybridgateway/logs/uninstall-hybridgateway-20150228080551.log") for more information.
  ```

  O erro mostrado no exemplo ocorreu porque o ibm-java-x86_64-jre é necessário para um pacote instalado externamente no sistema. O instalador não remove o JRE porque isso provavelmente deixaria o outro pacote não funcional. Como uma solução alternativa, desinstale os produtos que têm dependência em ibm-java-x86-64-jre antes de desinstalar o Hybrid Gateway.

Gerenciando o Gateway Híbrido
Use os comandos disponíveis para o serviço do IBM Cloud Application Performance Management Hybrid Gateway para iniciar ou pará-lo, para verificar o status, paraa desinstalar o Hybrid Gateway e para coletar os arquivos de log se instruído pelo Suporte IBM.

Sobre Esta Tarefa

Estas etapas consideram `/opt/ibm/` como o diretório de instalação do Hybrid Gateway. No sistema em que o Hybrid Gateway está instalado, execute qualquer uma das seguintes etapas a partir do prompt de comandos:

Procedimento

- Para iniciar o serviço do Hybrid Gateway, digite **`/opt/ibm/hybridgateway/bin/hybridgateway.sh start`**.
- Para parar o serviço do Hybrid Gateway, digite **`/opt/ibm/hybridgateway/bin/hybridgateway.sh stop`**.
- Para verificar o status do serviço do Hybrid Gateway, digite **`/opt/ibm/hybridgateway/bin/hybridgateway.sh status`**.
- Para desinstalar o Hybrid Gateway, digite **`/opt/ibm/hybridgateway/bin/hybridgateway.sh uninstall`**.

  Veja também "Desinstalando o Gateway Híbrido" na página 962.
- Para verificar os arquivos de log do Hybrid Gateway, acesse `/opt/ibm/wlp/usr/servers/hybridgateway/logs`.
- Para coletar os arquivos de log do Hybrid Gateway para o suporte IBM, insira **`/opt/ibm/hybridgateway/collectLogs.sh`**.

  Os arquivos de log são coletados e uma mensagem mostra o local dos arquivos de log compactados e solicita que você os retorne para o Suporte IBM.

Gerenciador Hybrid Gateway

Configure o IBM Cloud Application Performance Management Hybrid Gateway para visualizar dados de monitoramento a partir do domínio do IBM Tivoli Monitoring no Console do Cloud APM. É possível criar um perfil do Hybrid Gateway para cada Tivoli Enterprise Monitoring Server central em seu ambiente.

Após clicar em **Configuração do Sistema** > **Gerenciador do Hybrid Gateway**, a página será exibida com uma lista de Hybrid Gateways definidos.

A página tem uma tabela de todos os gateways híbridos que foram configurados para os domínios do Tivoli Monitoring e tem ferramentas para gerenciar os perfis do Hybrid Gateway:

- **Incluir** abre a janela **Incluir Gateway Híbrido** para nomear o novo perfil. Após inserir um nome e clicar em **Incluir**, a janela **Editar Gateway Híbrido** é aberta.
- Selecione um gateway híbrido e clique em **Editar** para abrir a janela **Editar Gateway Híbrido**.
- Selecione um gateway híbrido que você não deseja mais e clique em **Excluir**. Após confirmar que você deseja excluir o gateway híbrido, o perfil será removido permanentemente.
- Clique em um título da coluna para classificar a tabela por essa coluna; Ctrl + Clique em outra coluna para incluir uma classificação secundária.
- Clique dentro da caixa de texto de filtro e digite o início do valor pelo qual filtrar. Ao digitar, as linhas que não atendem aos critérios são deixadas de fora. Para limpar o filtro, clique no × na caixa de filtragem ou pressione a tecla backspace.

Os campos obrigatórios que você deve preencher para configurar o Hybrid Gateway são marcados com um asterisco (*) na janela **Editar Gateway Híbrido**.

Nome do Perfil

O nome fornecido para o perfil do Hybrid Gateway, que pode ter até 128 letras, números e sublinhados (_).

O nome do perfil é solicitado durante a instalação do Hybrid Gateway. Se você já instalou o Hybrid Gateway no domínio do Tivoli Monitoring, use o nome fornecido ou aceito durante a instalação do Hybrid Gateway.

Versões mais antigas do Hybrid Gateway não usam um perfil nomeado para acessar seus dados de configuração. Se instalou o Hybrid Gateway antes da liberação do Cloud APM de agosto de 2017, você tem um nome do perfil especial, não definido (em branco). Somente uma versão mais antiga do Hybrid Gateway pode se conectar ao Servidor Cloud APM. Se configurou a versão anterior Hybrid Gateway, o perfil não nomeado mostrará os valores configurados. Se você não configurou a versão anterior do Hybrid Gateway, o perfil não nomeado mostrará os valores padrão. É possível manter o perfil não nomeado ou excluir e incluí-lo novamente mais tarde conforme necessário, e ele pode ser usado somente para o Hybrid Gateway versão de março de 2017 (ou anterior).

Nome do Grupo de Sistemas Gerenciados
O grupo do sistema gerenciado do Tivoli Enterprise Portal Server criado para visualizar agentes de monitoramento suportados no Console do Cloud APM. Todos os tipos de agentes de monitoramento que não são suportados pela oferta do Cloud APM não são mostrados no console, independentemente de sua inclusão no grupo do sistema gerenciado.
Para obter orientação e limitações ao criar o grupo do sistema gerenciado para ativação híbrida, consulte .

Nome do host do servidor de portal
O endereço IP do host do Tivoli Enterprise Portal Server ou o nome completo do domínio.

Porta do Servidor de Portal
O número da porta usado pelo Tivoli Enterprise Portal Server para comunicações. A porta padrão é `15200` para HTTP ou `15201` para HTTPS. Um valor 0 configura a porta para o padrão `15200` para HTTP ou `15201` para HTTPS.

Protocolo do Servidor de Portal
Determina se o protocolo da Internet HTTP ou o protocolo HTTPS seguro deve ser usado para se conectar ao Tivoli Enterprise Portal Server. Padrão: `http`.

Nome do Usuário do Servidor de Portal
O nome do usuário para iniciar o cliente do Tivoli Enterprise Portal. Este ID de usuário deve ter acesso a todos os tipos de agentes de monitoramento (**Aplicativos Permitidos** é configurado como **Todos os Aplicativos**). Para obter mais informações, consulte Administrar Usuários no Centro de Conhecimento do Tivoli Monitoring).

Senha de Usuário do Servidor de Portal
A senha associada ao nome do usuário de logon do Tivoli Enterprise Portal.

Nome do Host do Proxy de Passagem
Usado se o Tivoli Enterprise Portal Server se comunicar por meio de um servidor proxy de passagem. Insira o endereço IP ou o nome completo do sistema host do proxy.

Porta de Proxy de Passagem
Usado se o Tivoli Enterprise Portal Server se comunicar por meio de um servidor proxy de passagem. Insira o número da porta para comunicação com o proxy.

Protocolo Proxy de Passagem
Usado se o Tivoli Enterprise Portal Server se comunicar por meio de um servidor proxy de passagem. Insira o protocolo usado para comunicação por meio do proxy. Padrão: `http`.

Os agentes do Tivoli Monitoring que você está visualizando no Console do Cloud APM estão em seu ambiente do IBM Tivoli Monitoring. É possível visualizá-los nas páginas do Application Performance Dashboard, mas não é possível criar limites para esses agentes no **Gerenciador de Limite**.

Integrando-se ao OMEGAMON

É possível visualizar dados e eventos para os componentes de aplicativos do OMEGAMON no Console do Cloud APM comprando o z Systems Extension Pack e usando o Hybrid Gateway para conectar um ou mais agentes implementados do OMEGAMON ao Cloud APM.

Antes de Iniciar

- Para usar o z Systems Extension Pack, deve-se ter a oferta IBM Cloud Application Performance Management, Advanced ou IBM Cloud Application Performance Management, Base.
- Um ou mais agentes licenciados OMEGAMON devem estar em execução em LPARS do z Systems que estão sendo monitoradas.
- Os agentes OMEGAMON são conectados à infraestrutura do IBM Tivoli Monitoring.

Para obter uma lista de agentes do OMEGAMON que podem ser exibidos no Console do Cloud APM, consulte o tópico Introdução para sua liberação na coleção de tópicos do IBM OMEGAMON for Application Performance Management no IBM Knowledge Center.

Procedimento

Para integrar o OMEGAMON com o Cloud APM, conclua as seguintes etapas:

1. Após o z Systems Extension Pack ser incluído no produto Cloud APM, , conclua as seguintes tarefas do Hybrid Gateway:
   a) Instale o Hybrid Gateway.
   b) Crie o grupo do sistema gerenciado que você deseja visualizar no Console do Cloud APM.
   c) Configure o Hybrid Gateway no Console do Cloud APM para que seja possível conectar o Hybrid Gateway ao Tivoli Enterprise Portal Server e especifique um grupo do sistema gerenciado.

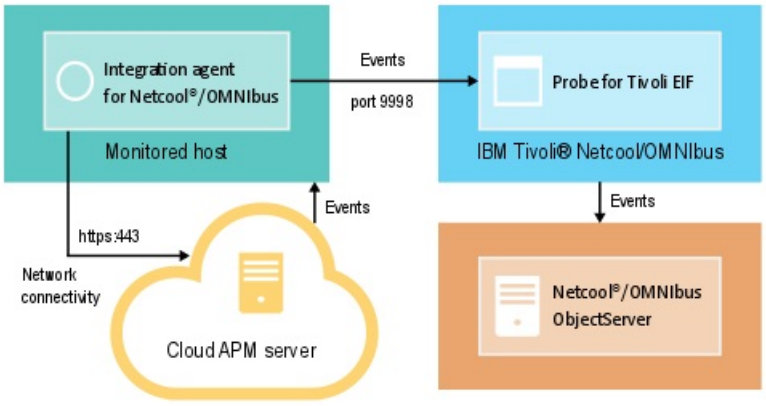
   Para obter informações adicionais, consulte os tópicos necessários na seção "Hybrid Gateway" na página 953.
2. Para visualizar o status de seus aplicativos no painel, efetue login no Console do Cloud APM a partir de seu navegador. Para obter mais informações, consulte "Iniciando o Console do Cloud APM" na página 975.

Integrando-se ao Netcool/OMNIbus

É possível encaminhar eventos do IBM Cloud Application Performance Management para o gerenciador de eventos IBM Tivoli Netcool/OMNIbus nas instalações.

Procedimento

1. Para visualizar o Integration Agent for Netcool/OMNIbus, e como ele se integra no Cloud APM ao Probe for Tivoli EIF para encaminhar eventos para o Netcool/OMNIbus, consulte a seguinte



   configuração:

   O Integration Agent for Netcool/OMNIbus se conecta automaticamente com o servidor Cloud APM. Esta conectividade permite que os eventos fluam do servidor para a rede sem quaisquer conexões de rede de entrada.
2. Configure a integração para Netcool/OMNIbus.

Instalando e configurando o Agente de Integração para Netcool/OMNIbus

Para instalar o Integration Agent for Netcool/OMNIbus, deve-se fazer download de um archive do website do IBM Marketplace, extrair os arquivos de instalação do agente e, em seguida, iniciar o script de instalação. Após a instalação, o agente é iniciado automaticamente, mas deve ser configurado.

Sobre Esta Tarefa

Apenas uma instância do Integration Agent for Netcool/OMNIbus pode encaminhar eventos de uma única instância de uma assinatura de serviço do Cloud APM para o gerenciador de eventos do Netcool/OMNIbus por vez.

Procedimento

1. Faça download do archive do Cloud APM Integration, que inclui o Integration Agent for Netcool/OMNIbus:
   a) Conecte-se à sua conta e acesse Produtos e serviços no IBM Marketplace.
   b) Em **IBM Performance Management**, clique em **Mais ações**.
   c) Clique em **Mostrar pacotes adicionais**.
   d) Selecione **IBM Performance Management OMNIbus Integration on Cloud**. Se necessário, role para baixo para localizar este item.
   e) Clique **Download**.
2. Salve o arquivo em um diretório temporário à sua escolha. Instale o agente em qualquer sistema que tenha conectividade de rede com o Tivoli Netcool/OMNIbus Probe for Tivoli Event Integration Facility (EIF). Se necessário, transfira o archive de instalação para os sistemas a serem monitorados. O archive contém o agente e o script de instalação.
3. Extraia o arquivo de instalação:

   Linux

   a. Abra uma sessão de shell de terminal no sistema Red Hat Enterprise Linux.
   b. Acesse o diretório no qual o archive está localizado.
   c. Extraia os arquivos de instalação usando o seguinte comando:

   ```
   tar -xf ./apm_integration_agents_xlinux_8.1.4.0.tar
   ```

   Windows

   Extraia o arquivo `apm_integration_agents_win_8.1.4.0.zip`.

   O script de instalação é extraído para um diretório nomeado para o archive e a versão. Por exemplo, `IPM_Agent_Install_8.1.3.2`. Os arquivos binários e relacionados à configuração do agente são extraídos em subdiretórios dentro desse diretório.
4. Execute o script de instalação com privilégios de Administrador no diretório que é nomeado para o archive e a versão.

   Se você estiver instalando o Integration Agent for Netcool/OMNIbus no mesmo sistema em que seu Probe for Tivoli EIF está localizado e o Probe for Tivoli EIF estiver usando a porta padrão de 9998, o Integration Agent for Netcool/OMNIbus será automaticamente configurado para se conectar ao seu Probe for Tivoli EIF.

   Importante: Se você estiver instalando o Integration Agent for Netcool/OMNIbus em um sistema que é diferente daquele em que seu Probe for Tivoli EIF está localizado, ou se estiver usando um número da porta diferente do padrão para o Probe for Tivoli EIF, deve-se configurar o Integration Agent for Netcool/OMNIbus após a conclusão da instalação.

   Conclua as etapas a seguir para instalar o agente:

   Linux `installAPMAgents.sh`
   Windows `installAPMAgents.bat`

Você é avisado para instalar o Integration Agent for Netcool/OMNIbus.

Uma varredura de pré-requisito de seu ambiente é iniciada e demora alguns minutos para ser concluída. Se algum dos requisitos estiver ausente, uma mensagem direcionará você para um arquivo de log com a razão da falha. A ausência de um pré-requisito, como uma biblioteca ausente ou espaço em disco insuficiente, para a instalação. Você deverá resolver a falha e iniciar a instalação novamente.

O agente é configurado com as seguintes configurações padrão:

```
Host de Análise de EIF do Tivoli: host local
Porta de Análise de EIF do Tivoli: 9998
```

Após a instalação, o Integration Agent for Netcool/OMNIbus é iniciado automaticamente.

O agente de monitoramento é instalado no diretório especificado (*install_dir*). Os seguintes diretórios padrão são utilizados:

Linux `/opt/ibm/apm/agent`

Windows `C:\IBM\APM\`

5. Se você estiver instalando o Integration Agent for Netcool/OMNIbus em um sistema que é diferente daquele em que seu Probe for Tivoli EIF está localizado, ou se o Probe for Tivoli EIF estiver usando um número de porta que é diferente da porta padrão de 9998, o Integration Agent for Netcool/OMNIbus deverá ser configurado para se conectar ao seu Probe for Tivoli EIF.

   Nota: Se você instalou o Integration Agent for Netcool/OMNIbus no mesmo sistema em que seu Probe for Tivoli EIF está localizado e o Probe for Tivoli EIF estiver usando a porta padrão de 9998, não será necessário concluir esta etapa.

   Linux Conclua as seguintes etapas para configurar o agente:

   a. Execute o seguinte comando:

   ```
   install_dir/bin/omnibus-agent.sh config
   ```

   b. Quando solicitado, forneça o nome do host e o número da porta de sua Probe for Tivoli EIF.

      Após a configuração estar concluída, o Integration Agent for Netcool/OMNIbus será iniciado automaticamente.

   Linux Como alternativa, é possível usar as etapas a seguir para revisar e mudar suas definições de configuração.

   a. Abra o arquivo de resposta *install_dir*`/samples/omnibus_silent_config.txt` em um editor de texto.
   b. Edite o arquivo para configurar ou alterar as suas definições de configuração. Assegure-se de remover o comentário das linhas de configuração.
   c. Salve e feche o arquivo de resposta.
   d. Reconfigure o agente. Execute o comando a seguir, especificando o caminho completo para o arquivo de configuração silenciosa editado:

   ```
   install_dir/bin/omnibus-agent.sh config install_dir/samples/omnibus_silent_config.txt
   ```

   e. Reinicie o agente para implementar suas mudanças:

   ```
   install_dir/bin/omnibus-agent.sh stop
   install_dir/bin/omnibus-agent.sh start
   ```

   Windows Conclua as seguintes etapas para configurar o agente:

   a. Abra o arquivo de resposta *install_dir*`\samples\omnibus_silent_config.txt` em um editor de texto.
   b. Edite o arquivo para especificar o nome do host e o número da porta de sua Probe for Tivoli EIF. Assegure-se de remover o comentário das linhas de configuração.

c. Salve e feche o arquivo de resposta.

d. Reconfigure o agente pela especificação do caminho completo para o arquivo de configuração silenciosa editado por você:

```
install_dir\BIN\omnibus-agent.bat config install_dir\samples\omnibus_silent_config.txt
```

e. Reinicie o agente para implementar suas mudanças:

```
install_dir\BIN\omnibus-agent.bat stop
install_dir\BIN\omnibus-agent.bat start
```

O que Fazer Depois

Siga as instruções em Configurando a integração para o Netcool/OMNIbus.

Se desejar parar de usar o Integration Agent for Netcool/OMNIbus ou se desejar mover o agente para um sistema diferente, desinstale o agente usando o seguinte comando:

Linux `install_dir/bin/omnibus-agent.sh uninstall`

Windows `install_dir\BIN\omnibus-agent.bat uninstall`

Configurando a integração para Netcool/OMNIbus

Depois de instalar o Integration Agent for Netcool/OMNIbus , deve-se copiar as regras de eventos para o Probe for Tivoli EIF e modificá-las. Deve-se também atualizar o Netcool/OMNIbus ObjectServer e o esquema do banco de dados.

Antes de Iniciar

Antes de concluir as etapas de integração, pare o Integration Agent for Netcool/OMNIbus usando os seguintes comandos:

Linux `install_dir/bin/omnibus-agent.sh stop`

Windows `install_dir\BIN\omnibus-agent.bat stop`

install_dir é o diretório `/opt/ibm/apm/agent` ou `C:\IBM\APM` padrão ou o diretório que você especificou durante a instalação do Integration Agent for Netcool/OMNIbus.

Sobre Esta Tarefa

Após a instalação do Integration Agent for Netcool/OMNIbus, os seguintes arquivos de configuração estarão no diretório *install_dir*`/localconfig/i0/omnibus` e *install_dir*`\localconfig\i0\omnibus`:

- `itm_apm_db_update.sql`
- `itm_event.rules`
- `itm_apm_event.rules`

em que *install_dir* é o diretório `/opt/ibm/apm/agent` ou `C:\IBM\APM` padrão que você especificou durante a instalação do Integration Agent for Netcool/OMNIbus.

Importante: Deve-se concluir estas etapas mesmo se o Probe for Tivoli EIF e Netcool/OMNIbus ObjectServer já estiverem integrados a IBM Tivoli Monitoring, Probe for Tivoli EIF, IBM SmartCloud Monitoring - Application Insight, IBM SmartCloud Application Performance Management ou uma versão anterior do Cloud APM.

Procedimento

Neste procedimento, quando você seguir os links para a documentação do IBM Tivoli Monitoring, conclua somente as etapas que são fornecidas na página vinculada.

1. Copie os arquivos Integration Agent for Netcool/OMNIbus `itm_event.rules` e `itm_apm_event.rules` no diretório de instalação do Probe for Tivoli EIF.

   Os diretórios a seguir são os diretórios padrão:

   Linux *install_dir*`/tivoli/netcool/omnibus/probes/linux2x86`

   Windows *install_dir*`\Tivoli\Netcool\omnibus\probes\win32`

   Em que *install_dir* é o padrão.
2. Abra o arquivo Probe for Tivoli EIF `tivoli_eif.rules` em um editor de texto e conclua uma das etapas a seguir:
   - Se você for um cliente do IBM Tivoli Monitoring existente e já concluiu a integração do OMNIbus, inclua esta linha no seu arquivo `itm_event.rules`: `include "itm_apm_event.rules"`.
   - Se você ainda não configurou a integração do OMNIbus, mova o comentário da linha que faz referência ao arquivo `itm_event.rules`.

   Para obter as etapas detalhadas, consulte Atualizando os arquivos de regras da análise de EIF na documentação do IBM Tivoli Monitoring.
3. Se estiver usando uma solução OMNIbus multicamada, conclua todas as tarefas conforme descrito na seção Atualizando o servidor de objeto do Netcool/OMNIbus com os atributos, as tabelas e os acionadores do IBM Tivoli Monitoring na documentação do IBM Tivoli Monitoring.
4. Atualize o esquema do banco de dados do servidor de objeto do Netcool/OMNIbus carregando o arquivo `itm_apm_db_update.sql` no banco de dados:

   Linux

   ```
   $OMNIHOME/bin/nco_sql -user user_name -password password
   -server server_name < itm_apm_db_update.sql
   ```

   Por exemplo:

   ```
   $OMNIHOME/bin/nco_sql -user smadmin -password passw0rd -server NCOMS <
   /tmp/apm/itm_apm_db_update.sql
   ```

   Windows

   ```
   itm_apm_db_update.sql | %OMNIHOME%\..\bin\isql -U user_name
   -P password -S server_name
   ```

   Por exemplo:

   ```
   \temp\apm\itm_apm_db_update.sql | %OMNIHOME%\ .. \bin\isql -U smadmin
   -P passw0rd -S NCOMS
   ```

   As mensagens de erro a seguir podem ser exibidas quando estiver executando os scripts e essas mensagens são inofensivas:
   - `Object exists` e `Attempt to insert duplicate row`, se os scripts tiverem sido executados anteriormente (por exemplo, para integração com uma versão anterior do Cloud APM ou com Tivoli Monitoring).
   - `ERROR=Object not found on line 4 of statement "-- A workspace table for the ITM event clear automation..."` at or near `itm_event_clear`.
   - `ERROR=Object not found on line 1 of statement "delete from alerts.itm_problem_events;..."` at or near `itm_problem_events`.
   - `ERROR=Object not found on line 1 of statement "drop table alerts.itm_problem_events;..."` at or near `itm_problem_events`.
5. Repita a etapa 5 para que o arquivo seja carregado no servidor de objeto duas vezes para assegurar que todas as dependências sejam carregadas corretamente.
6. Inicie (ou reinicie) o Probe for Tivoli EIF.

7. Reinicie o Integration Agent for Netcool/OMNIbus usando os seguintes comandos:

   Linux *install_dir*/bin/omnibus-agent.sh start
   Windows *install_dir*\BIN\omnibus-agent.bat start

Integrando-se ao Operations Analytics - Log Analysis

Quando seu ambiente incluir o IBM Operations Analytics - Log Analysis, será possível integrá-lo para ativar a procura em logs do aplicativo no Console do Cloud APM.

Sobre Esta Tarefa

A integração com o aplicativo do Log Analysis instalado envolve a configuração do Servidor Cloud APM com a URL. Para obter informações adicionais sobre o Log Analysis, consulte o IBM Operations Analytics - Developers Community.

Você deve fornecer a URL de nível superior para a instalação do Log Analysis, por exemplo:

```
https://loganalysis.example.com:9987/Unity
```

A URL do Log Analysis deve estar acessível a partir dos hosts nos quais os usuários trabalham com o Console do Cloud APM. Não é necessário torná-la acessível na Internet aberta.

Procedimento

1. No Console do Cloud APM, clique em **Configuração do Sistema** > **Configuração Avançada**.
2. Selecione a categoria **Integração da UI**.
3. No campo **URL do Log Analysis**, digite a URL que é usada para ativar seu aplicativo Log Analysis.

Resultados

O aplicativo do Log Analysis é integrado e o recurso é ativado para procura por meio de logs do aplicativo no Application Performance Dashboard.

Nota:

A conexão única não é suportada a partir do Console do Cloud APM com o aplicativo Log Analysis.

O que Fazer Depois

Selecione **Desempenho** > **Application Performance Dashboard** . Opcionalmente, selecione um aplicativo, utilize a caixa de procura para procurar por arquivos de log. Por padrão, as entradas para a última hora serão procuradas, mas você pode mudar esse período de tempo. Se você selecionar um aplicativo, apenas os logs em servidores associados a este aplicativo serão procurados. Para obter instruções detalhadas, consulte “Procurando Arquivos de Log” na página 1081.

Integração com Operations Analytics - Predictive Insights

Ao integrar o IBM Cloud Application Performance Management com o Operations Analytics - Predictive Insights, o Operations Analytics - Predictive Insights analisa os dados de métricas coletados pelo Cloud APM e gera alarmes quando identifica anomalias nos dados.

Anomalias são exibidas como eventos no Cloud APM Dashboard, conforme descrito em “Investigando anomalias com Operations Analytics - Predictive Insights” na página 1111. Em seguida, é possível realizar drill down para a Interface com o Usuário do Operations Analytics - Predictive Insights para visualizar mais detalhes sobre uma anomalia.

Ao incluir Operations Analytics - Predictive Insights em uma assinatura do Cloud APM, será configurado automaticamente para coletar e analisar métricas de desempenho. Nenhuma configuração adicional é

necessária. Para incluir o Operations Analytics - Predictive Insights em um assinatura do Cloud APM, acesse Suporte IBM e abra uma Solicitação de serviço.

É possível integrar os seguintes agentes do Cloud APM com o Operations Analytics - Predictive Insights:

- Monitoring Agent for Db2
- Monitoring Agent for IBM Integration Bus
- Monitoring Agent for JBoss
- Monitoring Agent for Linux OS
- Monitoring Agent for Oracle Database
- Response Time Monitoring Agent
- Monitoring Agent for UNIX OS
- Monitoring Agent for VMware VI
- Monitoring Agent for WebSphere Applications
- Monitoring Agent for WebSphere MQ
- Monitoring Agent for Windows OS
- Monitoring Agent for Tomcat

Integrando-se ao Alert Notification

Para obter mais flexibilidade além do encaminhamento básico de e-mail do Cloud APM, é possível integrar-se com o produto Alert Notification para estender os recursos do Cloud APM para notificar os usuários quando problemas ocorrem.

A integração com o Alert Notification oferece controle granular sobre quem recebe notificações e como elas são recebidas. Por exemplo, cada usuário pode decidir se deseja receber e-mail, SMS ou mensagem de voz. As notificações também podem ser roteadas para o Slack. Usuários diferentes podem receber diferentes tipos de notificações com base no horário do dia, dia da semana, etc. Cada usuário pode decidir quais tipos de alertas eles desejam receber. Por exemplo, um administrador de banco de dados talvez queira receber somente alertas do banco de dados que são de aviso ou de gravidade mais alta.

Antes de Iniciar

A Notificação de alerta é integrada automaticamente para você na assinatura do IBM Cloud Application Performance Management e em sua assinatura de teste.

Sobre Esta Tarefa

Os eventos são configurados automaticamente para envio para o Alert Notification. Portanto, é possível criar políticas de notificação para sua assinatura para determinar os alertas para os quais você deseja receber notificações.

É possível incluir aplicativos monitorados em grupos de recursos. Para cada grupo de recursos salvo, é possível configurar um ou vários endereços de e-mail. Quando o desempenho de qualquer sistema gerenciado em um grupo exceder um limite, uma notificação por e-mail será enviada para os endereços que estão configurados para o grupo.

O Alert Notification envia notificação por e-mail para quaisquer eventos que estão abertos nos sistemas gerenciados designados ao grupo.

Procedimento

Conclua as Etapas “1” na página 971 e “2” na página 972 para qualquer grupo de recursos para o qual você deseja rotear alertas com base no grupo de recursos.

1. Se desejar rotear notificações com base em grupos de recursos, conclua as seguintes subetapas:

a) No Console do Cloud APM, clique em **Configuração do Sistema** > **Gerenciador de Grupo de Recursos**.

b) Selecione um grupo de recursos e clique em **Editar** para abrir o **Editor de Grupo de Recursos**.

Importante: Você deve salvar um grupo de recursos novo ou editado antes de abrir o Alert Notification. Depois de salvar, o Editor do grupo de recursos é fechado e você deve reabri-lo se desejar continuar usando-o.

Se você não salvar, depois de configurar a notificação por e-mail na Etapa "2" na página 972 e retornar ao Editor do grupo de recursos, é possível receber uma mensagem de erro que informa que a atualização síncrona não é permitida.

2. Conclua as seguintes etapas para configurar a notificação por e-mail:

a) No Editor do grupo de recursos do console do APM, clique na URL **Configurar notificação por e-mail** para abrir o aplicativo IBM Alert Notification em uma nova guia ou janela do navegador.

Esta ação cria automaticamente uma nova política com base no grupo de recursos selecionado na Etapa "1" na página 971.

Atenção: Se o seu navegador não permitir janelas pop-up, a janela do Alert Notification será impedida de abrir. Você deve configurar o navegador para permitir que a janela do Alert Notification o abra para configurar a notificação por e-mail para um grupo de recursos.

b) No Alert Notification, configure Usuários e grupos e associe seus endereços de e-mail com grupos de recursos para receber notificações de eventos por e-mail.

É possível configurar suas próprias políticas e notificações do Alert Notification para o tipo de alertas que você deseja receber. Por exemplo, um Administrador do Linux talvez queira receber e-mail, mensagens SMS ou mensagem de voz para todos os sistemas Linux. Portanto, talvez eles queiram desativar alertas de alta gravidade que são críticos. Uma política permite que eles filtrem todos os eventos que são gerados pelo agente de S.O. Linux. Para obter informações sobre como usar o Editor de notificações no aplicativo Alert Notification, consulte Criando políticas de notificação.

O que Fazer Depois

Para obter informações adicionais sobre o Alert Notification, consulte a Documentação do IBM Alert Notification.

Integrando-se ao Control Desk

Você pode configurar seus eventos do Cloud APM para abrirem automaticamente chamados no IBM Control Desk.

Sobre Esta Tarefa

É possível integrar o IBM Cloud Application Performance Management usando a versão no local ou a versão Cloud do IBM Control Desk.

Procedimento

Use um dos procedimentos a seguir:

- Para abrir chamados no IBM Control Desk V 7.6 local, conclua as seguintes etapas:

1. Configure a sua conta de e-mail do IBM SmartCloud Notes para o Control Desk usar um cliente de correio IMAP. Durante a configuração, assegure-se de selecionar **Ativar o Acesso IMAP Agora**. Para obter mais informações, consulte Ativando o acesso ao IMAP no IBM Connections Social Cloud Knowledge Center.
2. No Console do Cloud APM, clique em **Configuração do Sistema** > **Configuração Avançada** e, em seguida, configure os seguintes parâmetros:

Endereços de Email de Destino
Especifique o seu endereço de e-mail do SmartCloud Notes que é usado para criar chamados de Solicitação de Serviço.

Linha de Assunto do Email
Especifique uma linha de assunto para o email, como `Evento do PMaaS`.

3. Vá para Marketplace support. e selecione **Solicitação de serviço** para enviar um chamado de suporte para concluir sua ativação.

   Forneça as seguintes informações em seu chamado:

   – Endereço de e-mail do SmartCloud Notes

     Por exemplo, `user@ibmserviceengage.com`.
   – Senha de e-mail do SmartCloud Notes
   – Nome completo do servidor de e-mail do SmartCloud Notes

     Por exemplo, `imap.notes.na.collabserv.com`.
   – Número da porta de e-mail do SmartCloud Notes

     Por exemplo, 993.
   – URL do cliente do IBM Control Desk

     Formate o link da seguinte forma: `https://<subscriber-id>.sccd.ibmserviceengage.com/maximo_t4hj/webclient/login/login.jsp?welcome=-true`
4. Para configurar o E-mail Listener para analisar o e-mail e manipulá-lo corretamente quando desejar designar chamados a outros grupos no IBM Control Desk on Cloud, consulte Configurando E-mail Listeners.

- Para abrir chamados no ambiente IBM Control Desk Cloud, conclua as seguintes etapas:

  1. Vá para Marketplace support. e selecione **Solicitação de serviço** para enviar um chamado de suporte para concluir sua ativação.

     Forneça as seguintes informações em seu chamado:

     – Endereço de e-mail do SmartCloud Notes

       Por exemplo, `user@ibmserviceengage.com`.
     – Senha de e-mail do SmartCloud Notes
     – Nome completo do servidor de e-mail do SmartCloud Notes

       Por exemplo, `imap.notes.na.collabserv.com`.
     – Número da porta de e-mail do SmartCloud Notes

       Por exemplo, 993.
     – URL do cliente do IBM Control Desk

       Formate o link da seguinte forma: `https://<subscriber-id>.sccd.ibmserviceengage.com/maximo_t4hj/webclient/login/login.jsp?welcome=-true`
  2. Para configurar o E-mail Listener para analisar o e-mail e manipulá-lo corretamente quando desejar designar chamados a outros grupos no IBM Control Desk on Cloud, consulte Configurando E-mail Listeners.

Integrando-se ao IBM Cloud

É possível visualizar informações de monitoramento para seus aplicativos no ambiente do IBM Cloud usando coletores de dados selecionados.

Quando configurado para coletar dados de um aplicativo IBM Cloud, um coletor de dados permite a integração de recursos de monitoramento com o IBM Cloud. Os coletores de dados transferem o monitoramento de recursos e os dados diagnósticos sobre seus aplicativos IBM Cloud para o Servidor Cloud APM. O Servidor Cloud APM recebe e processa informações de monitoramento que são coletadas pelos coletores de dados. Os seguintes tipos de aplicativos IBM Cloud podem ser monitorados:

- Aplicativos Liberty
- Aplicativos Node.js
- Aplicativos Python
- Aplicativos Ruby

Após as configurações apropriadas de um coletor de dados, é possível visualizar dados de monitoramento no Console do Cloud APM. Para obter instruções de configuração, consulte “Procedimento geral para configurar coletores de dados” na página 183.

Integrando-se ao IBM Agent Builder

É possível criar, modificar, depurar e empacotar agentes usando o Agent Builder que estendem os recursos de monitoramento de um ambiente do IBM Tivoli Monitoring ou do IBM Cloud Application Performance Management. Um agente customizado usa um desses ambientes para monitorar qualquer tipo de software interno ou customizado.

Para obter detalhes, consulte o IBM Agent Builder: Guia do Usuário.

Capítulo 9. Administrando

Iniciando o Console do Cloud APM

Efetue login no Console do Cloud APM a partir do navegador para revisar o status de funcionamento dos aplicativos nos painéis.

Antes de Iniciar

- Ative sua conta usando link que é fornecido no email de confirmação recebido após a inscrição inicial para o serviço.
- Para assegurar que a interface com o usuário não seja truncada, use uma resolução mínima de 1280 x 1024.
- Para obter o desempenho ideal, use um dos navegadores suportados. Para obter uma lista dos navegadores suportados, acesse Requisitos do sistema (APM Developer Center). Selecione um dos links do produto IBM Cloud Application Performance Management e clique no link "Servidor"; no relatório que é exibido, clique ou role para baixo para "Navegadores da Web".

Procedimento

1. Para acessar o Console do Cloud APM, use o link que é fornecido no email que alerta que o serviço está pronto.
2. Também é possível acessar o console a partir do website do IBM Marketplace:
   a. Acesse Produtos e serviços no website IBM Marketplace.
   b. Efetue login com o nome de usuário e a senha usados para se registrar para o serviço.
   c. Na linha Servidor Cloud APM, clique em **Ativar**.

Resultados

Após o login, a página **Introdução** é exibida, com opções de aprendizado para **Tarefas do Usuário** e **Tarefas do Administrador** e links para **Recursos da Comunidade**.

O que Fazer Depois

- Familiarize-se com os elementos da interface com o usuário, clicando no link de hipertexto para fazer um tour pelo painel do Cloud APM. Assista aos vídeos das tarefas do usuário e das tarefas do administrador para ajudá-lo na introdução do uso e da customização de seu ambiente do Cloud APM.
- Inclua aplicativos para visualizar painéis de seus recursos em agrupamentos lógicos, como Classificação Online. Para obter instruções, veja “Gerenciando aplicativos” na página 1098.
- Crie limites para testar condições que, quando atendidas, causam a abertura de um evento. Por exemplo, é possível ter um limite que abre um evento depois que a capacidade de armazenamento atingir 90%. Para obter instruções, veja “Gerenciador de Limites” na página 985.
- Inclua e designe usuários para grupos de usuários e funções, para controlar o acesso aos recursos e recursos gerenciados do Console do Cloud APM. Para obter mais informações, consulte “Gerenciando o acesso de usuário” na página 1001.
- Para saber sobre o monitoramento do IBM Pilha de aplicativos Java e do Pilha de integração IBM, consulte “Cenários” na página 86.
- Se, ao invés da página de Introdução ou do Application Performance Dashboard, o seu navegador acessar o website da IBM, o seu ID do usuário não tem permissões para o Console do Cloud APM. Você deve solicitar acesso a partir do seu administrador.

- Se nenhuma métrica for mostrada para uma origem de dados, consulte o Fórum do Cloud Application Performance Management sobre developerWorks. Procure o fórum para "painel", responda a uma entrada para fazer uma pergunta relacionada ou crie uma nova entrada e descreva o sintoma.
- Se você estiver iniciando o Console do Cloud APM a partir do Internet Explorer 8, 9 ou 10 e receber um erro `Esta página não pode ser exibida`, você pode precisar ativar a opção de segurança TLS 1.2. Para obter mais informações, acesse o Fórum do Cloud Application Performance Management e procure em "tls".

Limites e grupos de recursos

Os limites testam determinadas condições, como número de transações por minuto menor que 100, e abrem um evento, quando as condições forem atendidas. Use os limites para monitorar problemas reais e potenciais com seus recursos monitorados. Designe limites para grupos de recursos para o monitoramento em todos os sistemas gerenciados do mesmo tipo que pertencem ao grupo.

Informações de histórico

Revise as informações básicas para saber sobre limites, limites predefinidos para os agentes, os grupos de recursos aos quais eles são designados e sobre como customizar limites.

Limites predefinidos

Os agentes de monitoramento são fornecidos com *limites predefinidos* que são ativados e iniciados com o agente. Na primeira vez que o **Gerenciador de limites** for aberto após a instalação do agente, os limites que são listados para o tipo de origem de dados selecionado serão os limites predefinidos. Estes limites predefinidos são designados ao grupo de recursos do sistema padrão para o agente e mostrados na coluna **Grupos designados**.

Se você editar um limite predefinido, como para mudar o nome ou a condição, o limite não será mais tratado como um limite predefinido, mas considerado um *limite customizado*. No entanto, é possível mudar o grupo de recursos designados para um limite predefinido do grupo do sistema padrão para um grupo definido pelo usuário e ele permanecer um limite predefinido.

Se você preferir não usar os limites predefinidos, é possível desativá-los na página **Configuração Avançada** (consulte “Ativação de níveis” na página 1075). A desativação dos limites predefinidos não os remove do **Gerenciador de limites**; somente remove sua designação de grupo, tornando-os inativos. Após desativar os limites predefinidos, é possível abrir o **Gerenciador de Limite** e ver que a coluna **Grupos Designados** está vazia para cada limite predefinido (consulte “Exemplos de limites desativados” na página 978).

É possível ativar o limite como um limite customizado, designando-o a qualquer grupo de recursos disponíveis.

Limites customizados

Novos limites que você cria são limites customizados, conforme indicado na coluna **Gerenciador de Limite Origem**. Se você editar um limite predefinido, ele também se tornará um limite customizado e sua origem mudará de "Predefinido" para "Customizado".

Executar comando

Após a abertura de um evento para um limite avaliado como true, é possível executar automaticamente um comando ou um script de comandos no sistema monitorado para o qual o evento foi aberto. Por exemplo, você talvez queira registrar informações, acionar um sinal sonoro audível ou parar uma tarefa que está usando recursos excessivamente.

O comando utiliza a seguinte sintaxe:

```
&{data_set.attribute}
```

em que *data_set* é o nome do conjunto de dados e *attribute* é o nome do atributo, conforme mostrado no Editor de Limite. Se o conjunto de dados ou o nome do atributo contiver um espaço, substitua-o por um sublinhado.

O exemplo a seguir mostra como é possível transmitir o parâmetro de nome do disco para seu recurso gerenciado:

```
/scripts/clean_logs.sh &{KLZ_Disk.Disk_Name}
```

É possível transmitir um ou mais atributos do conjunto de dados. Se especificado, múltiplos atributos são transmitidos para o comando ordenadamente ($1, $2 e assim por diante).

O comando é executado a partir da linha de comandos com a mesma conta de usuário com a qual o agente foi iniciado. Por exemplo, se o agente estiver em execução como raiz, a raiz executará o comando no sistema gerenciado.

As opções a seguir controlam a frequência de execução do comando:

Marque a ☐ **Somente no Primeiro Evento** se o conjunto de dados retornar diversas linhas e você quiser executar o comando somente para a primeira ocorrência na amostra de dados. Desmarque a caixa de seleção para executar o comando para todas as linhas que causam um evento.

Marque a ☐ **Para Cada Intervalo Verdadeiro Consecutivo** para executar o comando cada vez que o limite for avaliado como verdadeiro. Desmarque a caixa de seleção para executar o comando quando o limite for true, mas não executá-lo novamente até que o limite seja avaliado como false, seguido por outra avaliação true em um intervalo subsequente.

Grupos de recursos

Os grupos de recursos representam uma coleção de sistemas gerenciados e controlam como os limites são distribuídos. Designe um limite ao grupo de recursos que inclui os sistemas gerenciados nos quais deseja que ele seja executado.

Todos os limites predefinidos têm uma designação de grupo de recursos padrão, que é o grupo definido pelo sistema para o tipo de agente, como Db2 e Microsoft IIS.

É possível criar grupos de recursos customizados e selecionar os sistemas gerenciados a serem incluídos em cada grupo. É possível ter vários tipos de agentes em um grupo de recursos customizados; os limites que são designados ao grupo são distribuídos somente aos sistemas gerenciados do mesmo tipo de agente. Por exemplo, um limite que é criado com atributos do Linux OS e designado a um grupo de recursos dos sistemas gerenciados Linux SO, MongoDB e Python é distribuído somente aos sistemas gerenciados Linux OS.

Para obter mais informações, consulte “Gerenciador de Grupos de Recursos” na página 980.

Status do evento do Application Performance Dashboard

As severidades dos status mostradas no Application Performance Dashboard indicam a severidade mais alta do evento do aplicativo, grupo, subgrupo e instância de sistema gerenciado selecionados.

Após selecionar um aplicativo do navegador ou de uma caixa de resumo no painel **Todos os Meus Aplicativos**, um painel tabulado exibe os diferentes aspectos de seu aplicativo. A guia **Eventos** fornece informações sobre os eventos para o item do navegador selecionado, conforme descrito em “Status da Ocorrência” na página 1109.

As mudanças de limites afetam outros limites que estão designados para o mesmo agente de monitoramento

Depois de criar, modificar ou excluir uma definição de limite ou alterar a lista de limites que são distribuídas para um agente de monitoramento, todos os eventos de amostragem são fechados para os agentes que o limite é distribuído TO . Após o encerramento do evento, os agentes de monitoramento reabrem eventos para quaisquer condições de limite que são avaliadas como true. No Console do Cloud APM, os eventos fechados desaparecer do console até que eles sejam reabertos com um novo **Registro** valor. Se estiver recebendo notificações por e-mail sobre eventos, você receberá notificações por e-mail de abertura e de encerramento de eventos.

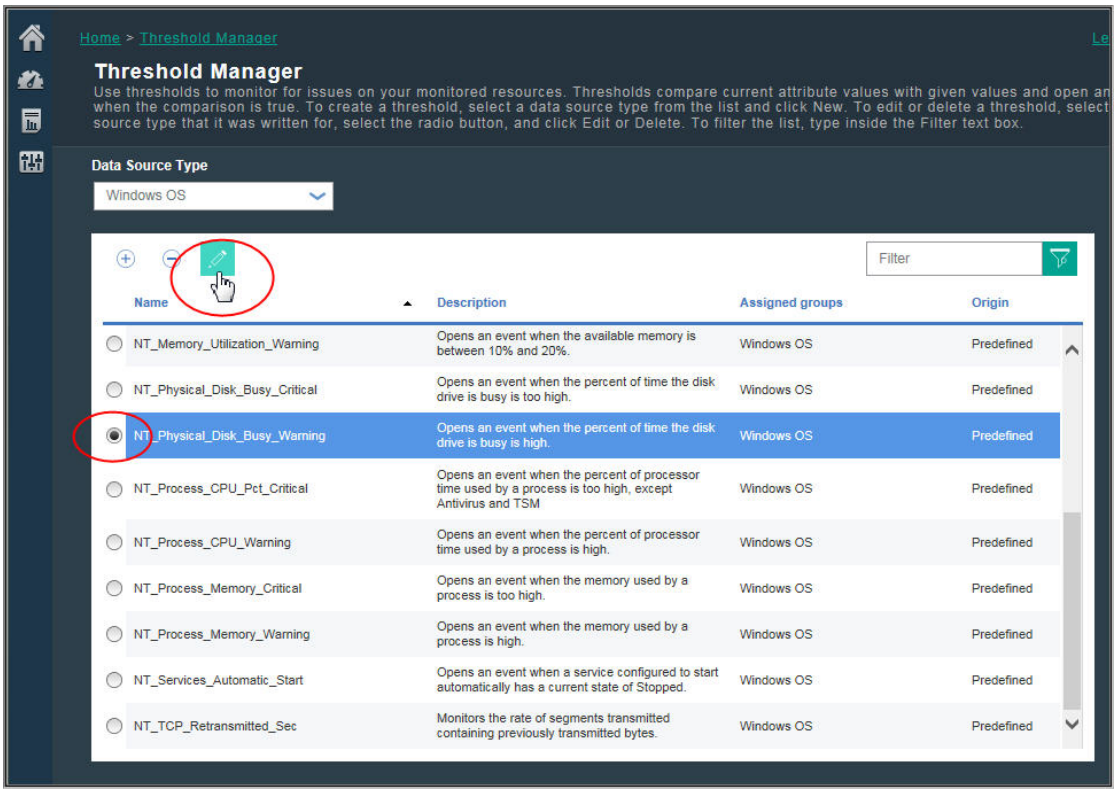
Considere, por exemplo, que você tem um grupo de recursos customizado chamado Site Systems com Linux OS e limites WebSphere Applications e agentes designados. Você cria um limite do SO Linux novo e designá-lo a Site Systems. Quaisquer eventos de amostra aberto no Linux OS agentes que são designados para o Site Systems estão fechados. Então os eventos de amostragem são reabertos se as condições de limite são ainda verdadeiros.

Exemplos de limites desativados

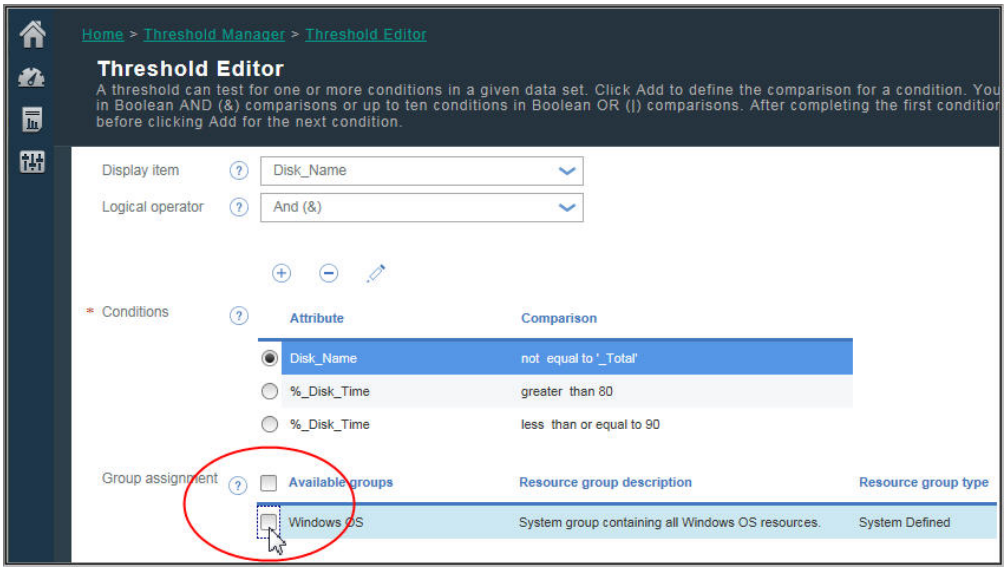
É possível desativar os limites predefinidos para todos os agentes em seu ambiente. Também é possível desativar limites individualmente, predefinidos ou customizados. Quando um limite for desativado, ele não estará em execução nos sistemas gerenciados e nenhum evento será aberto.Desative um limite removendo sua designação (ou designações) do grupo de recursos. Uma definição de **Configuração Avançada** está disponível também para desativar limites predefinidos para todos os agentes.

Desativando um único limite

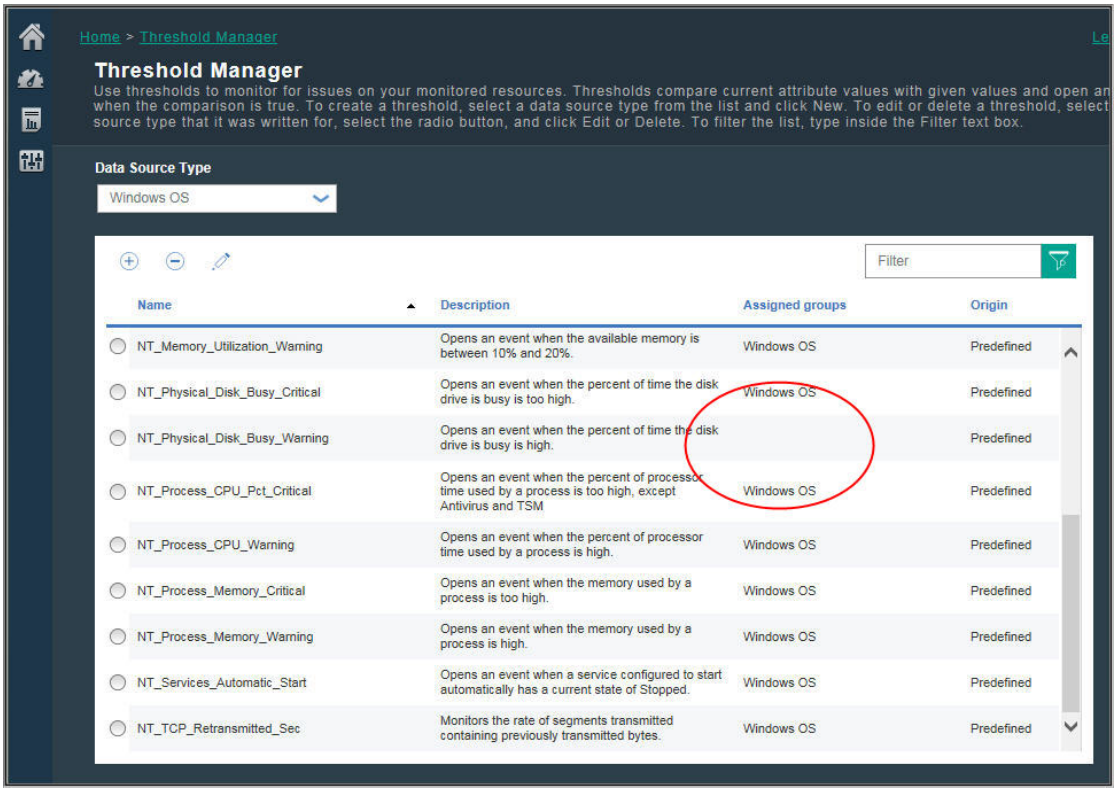
Nesta imagem, o limite a ser desativado é selecionado no **Threshold Manager** e o usuário clica em **Editar**:



O limite é aberto no Editor de limites. O usuário limpa a caixa de seleção do grupo de recursos designado no campo **Designação de Grupo**:

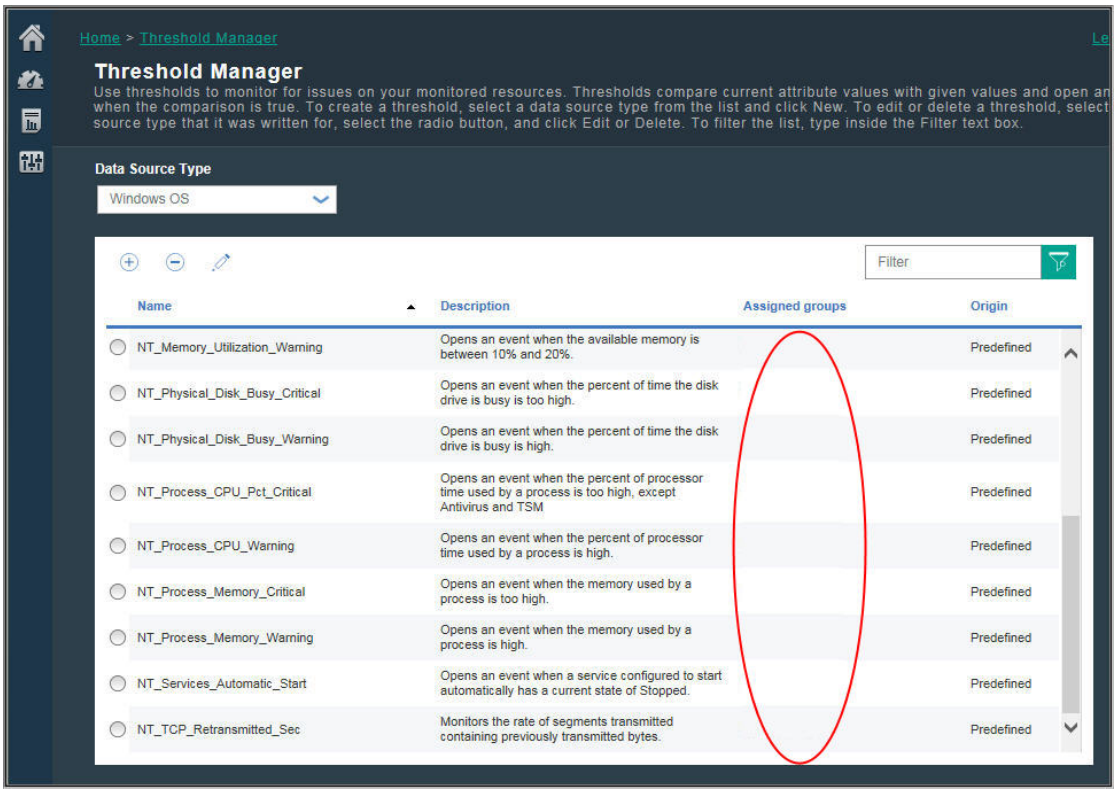


Depois que o usuário clicar em **Salvar**, o **Gerenciador de limites** será exibido. O limite é desativado e a coluna **Grupos Designados** fica vazia:



Desativando todos os limites predefinidos

Desative todos os limites predefinidos para todos os agentes de monitoramento na página **Configuração Avançada**, conforme descrito em "Ativação de níveis" na página 1075. Na próxima vez que você abrir o **Gerenciador de Limite**, a coluna **Grupos Designados** ficará vazia para cada limite predefinido, indicando que os limites estão inativos:



Conceitos relacionados

"Informações de histórico" na página 976

Revise as informações básicas para saber sobre limites, limites predefinidos para os agentes, os grupos de recursos aos quais eles são designados e sobre como customizar limites.

Referências relacionadas

"Gerenciador de Limites" na página 985

Gerenciador de Grupos de Recursos

Seu ambiente monitorado pode ter vários sistemas gerenciados que podem ser categorizados por seus propósitos. Muitas vezes, esses sistemas possuem os mesmos requisitos de limite. Use o **Gerenciador de Grupo de Recursos** para organizar sistemas gerenciados em grupos aos quais é possível designar limites. Também é possível criar grupos de recursos que se correlacionam com suas políticas de controle de acesso baseado na função (RBAC).

Após um clique em **Configuração do Sistema** > **Gerenciador de Grupo de Recursos**, a página é aberta com uma tabela de grupos de recursos definidos. Inicialmente, um grupo do sistema predefinido é mostrado para cada tipo de agente de monitoramento que está instalado, como o `S.O. Windows`. Cada grupo do sistema contém todos os limites predefinidos para o agente.

Seu acesso ao **Gerenciador de Grupos de Recursos** e grupos de recursos é controlado por suas permissões de usuário. Deve-se ter a permissão Visualizar para um grupo de recursos para vê-lo; deve-se ter a permissão Modificar para criar, editar ou excluir um grupo de recursos.

A tabela possui ferramentas para o gerenciamento de grupos de recursos:

- **Novo** abre o **Editor de Grupos de Recursos** para a designação de sistemas gerenciados e limites.
- Selecione um grupo de recursos para ver os recursos designados e os limites que são designados ao grupo na área de janela adjacente.
- Selecione um grupo de recursos e clique em **Editar** para abrir o **Editor de Grupos de Recursos** para alterar o sistema gerenciado e as designações de limites.
- Selecione um grupo de recursos que você não deseja mais e clique em **Excluir**. Após a confirmação da exclusão, os limites designados ao grupo devem ser designados a outro grupo, caso você deseje que eles continuem a ser executados nos sistemas gerenciados.
- É possível clicar dentro da caixa de texto de filtro e digitar o valor pelo qual filtrar. Ao digitar, as linhas que não atendem aos critérios são deixadas de fora. Para limpar o filtro, clique no × na caixa de filtragem ou pressione a tecla backspace.

A tabela exibe os grupos de recursos disponíveis:

Nome do grupo de recurso
Os grupos predefinidos são nomeados para seu tipo de agente; os grupos customizados são nomeados pelo autor.

Descrição do grupo de recursos
Um grupo predefinido é descrito como um *grupo do sistema* para o recurso monitorado; os grupos customizados são descritos pelo autor.

Um grupo do sistema, tal como `S.O. Linux`, inclui todos os limites predefinidos para o agente e todos os sistemas gerenciados nos quais o agente está instalado. É possível editar um grupo de sistemas para designar ou remover limites, mas não é possível designar ou remover sistemas gerenciados. Os sistemas gerenciados são designados automaticamente a um grupo do sistema do mesmo tipo, incluindo qualquer um de seu domínio do Tivoli Monitoring se um Hybrid Gateway estiver configurado.

Alguns grupos de recursos do sistema se relacionam a agentes que suportam os subnós. Dependendo do tipo do agente, os subnós, o nó do agente, ou ambos, podem ser incluídos em aplicativos. Se somente os subnós puderem ser incluídos em aplicativos definidos, não será possível ver eventos para quaisquer limites que foram definidos para o nó do agente. No entanto, os eventos podem ser encaminhados para um gerenciador de eventos tal como Netcool/OMNIbus. Além disso, os assinantes do IBM Cloud Application Performance Management podem configurar o Alert Notification.

Tipo de grupo de recursos

Os grupos predefinidos são do tipo *Definido pelo Sistema*. Você tem um grupo predefinido para cada tipo de agente que foi instalado em seu ambiente.

Grupos customizados que você ou outros em seu ambiente criam são do tipo *Definido pelo Usuário*.

Editor do Grupo de Recursos

Após clicar em **Novo** para incluir um grupo, ou depois de selecionar um grupo e clicar em **Editar** para editar um grupo, o **Editor de Grupos de Recursos** é exibido com os campos a seguir:

Nome do grupo

O nome do grupo é necessário. É possível mudar um nome de grupo customizado existente, e todas as referências ao grupo serão automaticamente atualizadas depois que você salvar suas mudanças.

Descrição do grupo

Opcional para grupos customizados. Inclua uma descrição da organização do grupo. A descrição é exibida no **Gerenciador de Grupos de Recursos**.

Designação de Recurso

Todos os sistemas gerenciados que estão disponíveis para inclusão no grupo são mostrados na lista de agentes por seu nome do sistema gerenciado, nome do host, tipo de agente e seus domínios. É possível clicar em um título da coluna para classificar a lista por nome de agente, nome do host, tipo ou domínio.

Para preencher o grupo, marque a caixa de seleção de um ou mais sistemas gerenciados.

É possível selecionar **Mostrar Somente Recursos Selecionados** para ocultar os sistemas gerenciados não designados.

Se você tiver configurado o IBM Cloud Application Performance Management Hybrid Gateway, será possível incluir sistemas gerenciados a partir de seu domínio do IBM Tivoli Monitoring para grupos de recursos definidos pelo usuário. Não é possível incluir sistemas gerenciados do Tivoli Monitoring em grupos definidos pelo sistema nem criar limites para eles.

Designação de limite

Todos os limites que são predefinidos ou foram incluídos pelo **Gerenciador de Limite** são mostrados na lista de limites por nome e tipo de agente. Você pode clicar em um título da coluna para classificar a lista.

Para incluir um limite no grupo, selecione a caixa de seleção ao lado do nome; para remover um limite do grupo, limpe a caixa de seleção. Deve-se ter a permissão Visualizar para o **Gerenciador de limite** para incluir ou remover limites. Ao incluir limites em um grupo do sistema, os limites disponíveis são limitados àqueles cujo conjunto de dados é adequado para o grupo do sistema.

Os limites designados ao grupo são distribuídos para todos os sistemas gerenciados no grupo do mesmo tipo de agente. Embora seja possível designar limites de qualquer tipo de agente de monitoramento para um grupo, os limites designados são distribuídos somente aos sistemas gerenciados do mesmo tipo que são membros do grupo. Por exemplo, ao designar o limite `MySQL_Process_Down` para o grupo, ele será incluído no grupo, mas distribuído somente para os sistemas gerenciados do Monitoring Agent for MySQL que pertencem ao grupo.

É possível selecionar **Mostrar apenas limites selecionados** para ocultar os limites não designados. Se você estiver filtrando a lista, clique em na caixa de filtragem para limpar o filtro e ativar a caixa de seleção.

Também é possível designar um grupo de recursos para um limite do **Gerenciador de Limites**.

Configuração da notificação por email

Disponível com IBM Cloud Application Performance Management: Clique em **Configurar notificação por e-mail** para abrir o aplicativo IBM Alert Notification em uma nova guia ou janela do navegador. Use Alert Notification para criar usuários e associar seus endereços de e-mail aos grupos de recursos para receber notificações de eventos por e-mail.

Atenção: Se o seu navegador não permitir janelas pop-up, a janela do Alert Notification será impedida de abrir. Você deve configurar o navegador para permitir que a janela do Alert Notification o abra para configurar a notificação por e-mail para um grupo de recursos.

Após clicar em **Salvar**, o grupo de recursos é salvo com a lista de grupos de recursos e exibido na tabela **Gerenciador de Grupo de Recursos**.

Tarefas relacionadas

"Integrando-se ao Alert Notification" na página 971
"Explorando as APIs" na página 1072

Referências relacionadas

"Gerenciador de Limites" na página 985

Tutorial: definindo um limite

Limites são o mecanismo de alerta para problemas em potencial e reais com seus recursos gerenciados. Use o tutorial para aprender as etapas básicas para definir um limite para gerar um alarme quando a condição ocorrer.

Sobre Esta Tarefa

Este tutorial usa o agente do Linux OS para mostrar como definir um limite no **Gerenciador de limite** e visualizar o alarme criado no Application Performance Dashboard. Seu ID do usuário deve ter a permissão Visualizar para o **Gerenciador de limite** para concluir estas etapas.

Procedimento

1. Na barra de navegação, clique em **Configuração do Sistema** > **Gerenciador de Limite**.
2. Clique na caixa de listagem **Tipo de origem de dados** e selecione o tipo de dados do **Linux OS**.
   Os limites que foram definidos para o agente do Linux OS são exibidos na tabela.
3. Clique em **Novo** para abrir o **Editor de Limite** para definir o limite.
4. Defina um limite para ativar um alarme de Gravidade desconhecida, quando a média da CPU estiver abaixo de 75%:
   a) No campo **Nome**, insira `CPU_average_below_75_percent`.
   b) No campo **Descrição**, insira `Tutorial de limite`
   c) Deixe os campos **Gravidade**, **Intervalo** e **Amostras consecutivas necessárias** com seus valores padrão.
   d) No campo **Conjunto de dados**, selecione **Médias da CPU KLZ**.
   e) No campo **Condições**, clique em **Novo** e inclua a comparação na caixa de diálogo que aparece:
      1) No campo **Atributo**, selecione **CPU_Usage_Current_Average**
      2) No campo **Operador**, selecione **Menor que**
      3) No campo **Valor**, insira 75

      Após clicar em **OK**, o atributo e a comparação são exibidos no campo **Condições**.
   f) No campo **Designação de grupo**, selecione o grupo do sistema **Linux OS**.
   g) Clique em **Salvar** para concluir a definição e retornar à página **Gerenciador de limite**.

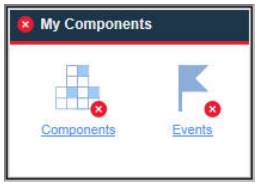
   `CPU_average_below_75_percent` é exibido na lista de limites definidos para a origem de dados do Linux OS.

Resultados

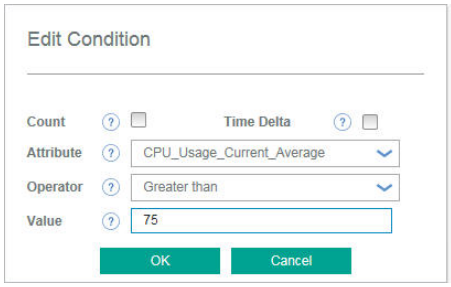
Você definiu um limite que ativa um alarme quando o uso médio da CPU em qualquer um dos sistemas gerenciados pelo sistema operacional Linux fica abaixo de 75%.

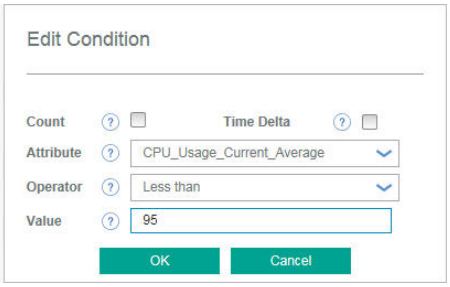
O que Fazer Depois

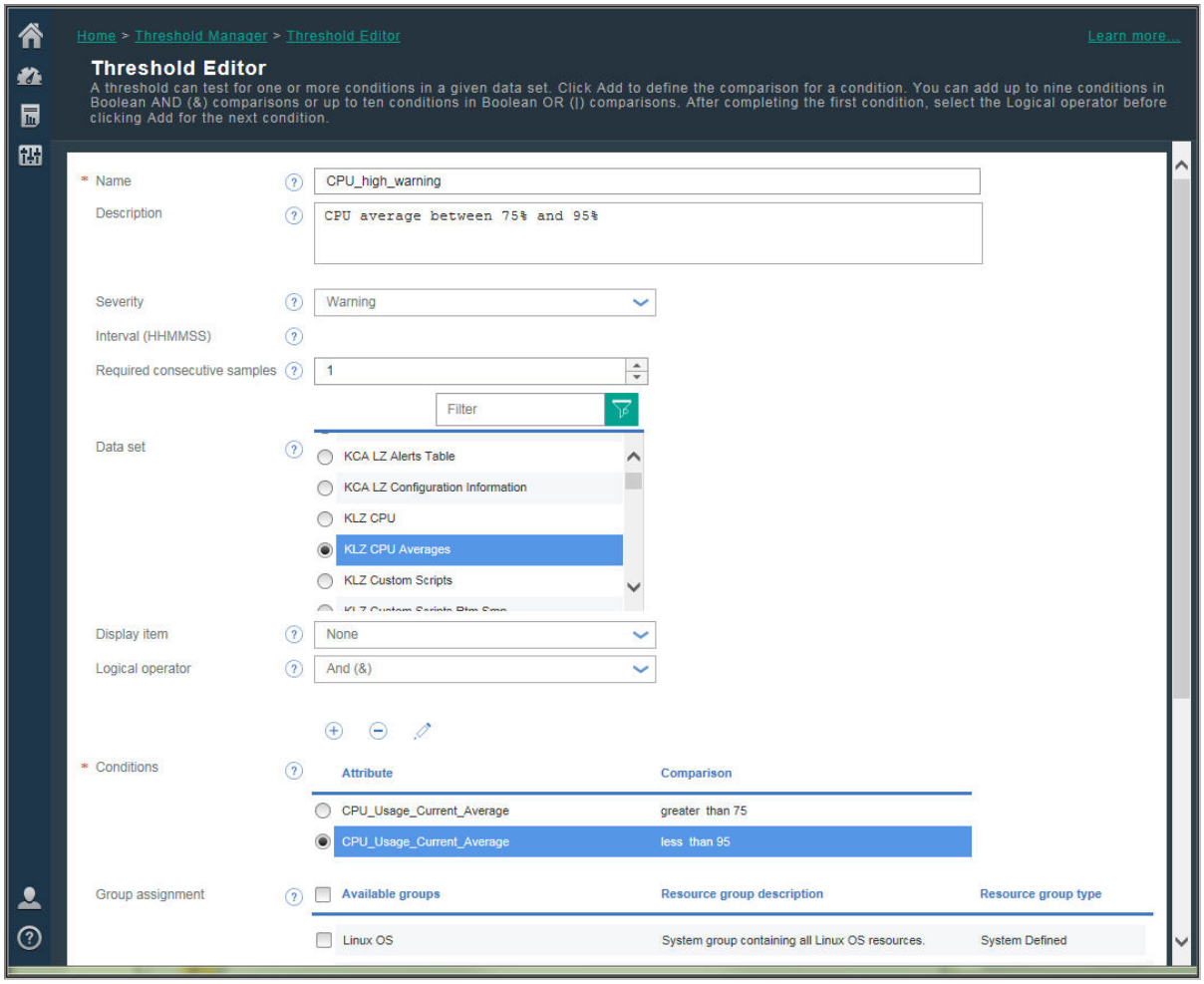
- Visualize o evento:
  1. Na barra de navegação, clique em **Desempenho** > **Application Performance Dashboard**.
  2. Na caixa de resumo **Meus componentes**, clique no link **Eventos**.



  3. Na guia **Eventos** que é aberta, procure o limite `CPU_average_below_75_percent` na lista. Pode demorar 1 ou 2 minutos para o alarme ser gerado. Se a média da CPU estiver acima de 75%, no entanto, nenhum alarme será ativado.
- Edite o limite:
  1. Na barra de navegação, clique em **Configuração do Sistema** > **Gerenciador de Limite**.
  2. Clique na caixa de listagem **Tipo de origem de dados** e selecione o tipo de dados do **`Linux OS`**.
  3. Selecione o limite `CPU_average_below_75_percent` na lista e clique em **Editar**.
  4. Mude qualquer um dos campos para uma condição sobre a qual deseja ser alertado. Por exemplo, você pode mudar **Nome** para `CPU_high_warning`, mudar **Gravidade** para **`Aviso`**, editar a condição para ser **`Maior que 75`** e incluir uma condição: **`Menor que 95`**. Para editar a comparação, clique em **Editar**, mude **Operador** para **`Maior que`** e clique em **OK**. Para incluir a nova condição, deixe o campo **Operador Lógico** no padrão **`And (&)`**, clique em **Novo** para uma nova condição, selecione **Operador `Less than`** e insira **Valor** 95.







- Revise os limites predefinidos para seus agentes e ajuste quaisquer valores de comparação, conforme necessário para seu ambiente.
- Crie novos limites para gerar alarmes em outras condições sobre as quais deseja ser alertado.

Referências relacionadas

"Gerenciador de Limites" na página 985

Tutorial: Definindo um limite para executar um comando no recurso gerenciado

É possível utilizar o **Editor de Limite** para transmitir determinados parâmetros para os agentes. É possível especificar comandos ou um script de comandos para que seja executado automaticamente quando um evento é acionado.

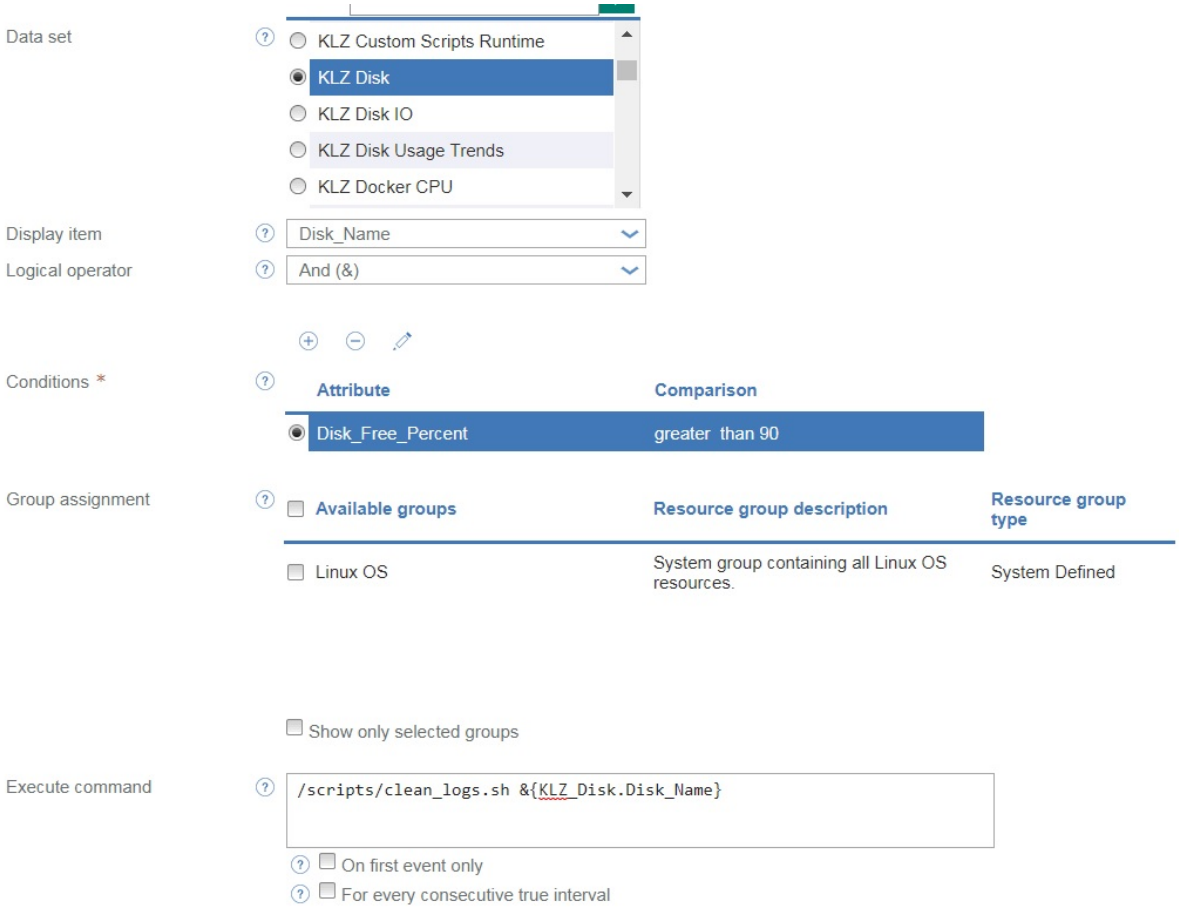
Sobre Esta Tarefa

Este tutorial mostra como usar o campo **Executar comando** para transmitir um parâmetro para seu agente do IBM Cloud Application Performance Management.

Procedimento

1. Abra o **Gerenciador de Limite** selecionando **Configuração do Sistema** > **Gerenciador de Limite**.
2. Selecione *S.O. Linux* no campo **Tipo de origem de dados**.
   Os limites que foram definidos para o agente do S.O. Linux são exibidos na tabela.
3. Clique em **Novo** para abrir o **Editor de Limite** para definir o limite.
4. Defina o limite e as condições especificando valores para os vários parâmetros, como **Name**, **Severity** e **Conditions**.

5. Selecione *KLZ Disk* no campo **Conjunto de dados**.



6. Insira o seguinte comando no campo **Executar comando**:

```
/scripts/clean_logs.sh &{KLZ_Disk.Disk_Name}
```

Deve-se substituir o espaço no nome do conjunto de dados *KLZ Disk* por um sublinhado.

O *KLZ_Disk.Disk_Name* é transmitido para o script de comando.

Resultados

O script de comandos é configurado para executar automaticamente para seu limite definido. Os comandos são executados no sistema monitorado para o qual os eventos são acionados.

Referências relacionadas

"Gerenciador de Limites" na página 985

Gerenciador de Limites

Use o **Gerenciador de limites** para revisar os limites predefinidos para um agente de monitoramento e para criar e editar limites.Os limites são usados para comparar o valor de amostra de um atributo com o valor definido no limite. Caso o valor de amostra atenda à comparação, é aberto um evento. O evento fecha automaticamente quando a comparação de limite não for mais verdadeira.

Após clicar em **Configuração do Sistema** > **Gerenciador de Limite**, a página será exibida com uma tabela dos limites que foram definidos para o tipo de origem de dados selecionado.

Os tipos de dados que são exibidos ao clicar na caixa de listagem **Tipo de Origem de Dados** destinam-se aos tipos de agentes de monitoramento e coletores de dados que estão instalados em seu ambiente gerenciado. Selecione o tipo de dados para o qual você deseja criar ou visualizar limites.

A tabela lista todos os limites que foram criados para o tipo de dados selecionado e possui ferramentas para gerenciar os limites:

- **Novo** abre o **Editor de Limite** para definir um limite para o tipo de dados selecionado.
- Selecione um limite e clique em **Editar** para abrir o **Editor de Limite** para editar a definição.
- Selecione um limite que você não deseja mais e clique em **Excluir**. Ao confirmar que você deseja excluir o limite, ele é removido da lista e de todos os grupos de recursos aos quais estava designado. Os eventos abertos para o limite são fechados.
- Para uma lista longa, é possível clicar dentro da caixa de texto de filtro e digitar o início do valor pelo qual filtrar. Ao digitar, as linhas que não atendem aos critérios são deixadas de fora. Para limpar o filtro, clique no na caixa de filtragem ou pressione a tecla backspace.

Para obter mais informações sobre os limites predefinidos e limites customizados exibidos na tabela e a significância da designação do grupo de recursos (ou falta dela), consulte "Informações de histórico" na página 976. Para obter uma lição prática rápida, consulte "Tutorial: definindo um limite" na página 982.

Editor de Limite

Após clicar em **Novo** ou selecionar um limite e clicar em **Editar**, o Editor de Limite será exibido com os seguintes campos:

Nome
Insira um nome exclusivo para o limite. O nome deve começar com uma letra e pode ter até 31 letras, números e sublinhados, como "Average_Processor_Speed_Warning". O nome do limite é exibido na guia Application Performance Dashboard **Eventos** e em certas tabelas do painel.

Descrição
Opcional. Uma descrição é útil para registrar o propósito do limite, que pode ser visto pelos usuários no **Gerenciador de Limites**.

Gravidade
Selecione a severidade do evento apropriada da lista: Fatal, Crítico, Secundário, Aviso, ou Desconhecido.

As severidades são consolidadas para exibição no Application Performance Dashboard: os eventos Fatal e Crítico aparecem como ; os eventos Secundário e Aviso aparecem como ; e os eventos Desconhecido aparecem como (consulte "Status da Ocorrência" na página 1109).

Encaminhar Evento do EIF?
Se você configurou o encaminhamento de eventos na página **Configuração do Sistema** > **Configuração Avançada** ("Gerenciador de Eventos" na página 1073), os eventos abertos serão encaminhados por padrão para os destinos de evento que você configurou, por exemplo, destinos do evento EIF, Gerenciamento de eventos de nuvem ou Alert Notification. Mude a configuração para **No** se não desejar encaminhar eventos desse limite para quaisquer destinos do evento.

Se você configurou o encaminhamento de eventos na página **Configuração do Sistema** > **Configuração Avançada** (Gerenciador de Evento), os eventos abertos serão encaminhados para um receptor EIF por padrão. Mude a configuração para **Não** se não desejar encaminhar eventos para esse limite para um receptor do EIF.

Para customizar como os limites são mapeados para eventos encaminhados, desse modo, substituindo o mapeamento padrão entre limites e eventos encaminhados para o servidor de eventos, clique em **Customização de Intervalo do EIF**. Para obter mais informações, consulte "Customizando um evento para encaminhar para um receptor EIF" na página 990.

Intervalo
Insira ou selecione o tempo de espera entre a obtenção de amostras de dados, no formato *HHMMSS*, como 00 15 00 para 15 minutos. Para limites de eventos de amostra, o intervalo mínimo é de 000030 (30 segundos) e o máximo é 235959 (23 horas, 59 minutos e 59 segundos).

Um valor igual a 000000 (seis zeros) indica um limite de *evento puro*. Eventos puros são notificações não solicitadas. Os limites para eventos puros não possuem nenhum intervalo de amostragem, portanto, não têm nenhuma métrica constante que possa ser monitorada para a obtenção de valores atuais. Eventos puros são encerrados após 24 horas ou conforme configurado no campo **Tempo de**

Fechamento do Evento Puro da página **Configuração Avançada** na categoria "Gerenciador de Eventos" na página 1073.

Amostras consecutivas necessárias
Especifique quantas amostras de limite consecutivas devem ser avaliadas como true antes que um evento seja gerado: Para qualquer limite com uma configuração de 1 e uma amostra avaliada como true, é gerado um evento imediatamente; uma configuração 2 significa que duas amostras de limite consecutivas devem ser avaliadas como true antes da abertura de um evento.

Conjunto de dados
Selecione o conjunto de dados (grupo de atributos) para o tipo de dados de amostragem. Os atributos disponíveis para inclusão na condição provêm do conjunto de dados escolhido. Se o limite tiver várias condições, elas devem ser todas do mesmo conjunto de dados.

Para obter uma descrição simples de um conjunto de dados, passe o mouse sobre o nome. É possível obter uma descrição completa do conjunto de dados e dos atributos, clicando no link "Saiba mais" na ajuda instantânea. Também é possível clicar em **Ajuda** > **Conteúdo da Ajuda** ou **Ajuda** > **Documentação** na barra de navegação e abrir a ajuda ou fazer download da referência para o agente de monitoramento.

Alguns agentes são categorizados como agentes de vários nós, que possuem subnós para monitoramento de vários recursos de agente. Um agente com vários nós pode ter conjuntos de dados que podem ser usados em um limite, mas quaisquer eventos abertos para o limite não são exibidos no Application Performance Dashboard. Uma mensagem o notifica sobre a limitação. Tais eventos podem ser encaminhados para o gerenciador de eventos do IBM Netcool/OMNIbus.

Item de exibição
Opcional. Somente para conjuntos de dados de diversas linhas. Depois que uma avaliação de linha causa a abertura de um evento, até que o evento seja fechado, não é possível abrir mais nenhum evento para esse limite no sistema monitorado. Ao selecionar um item de exibição, é possível permitir que o limite continue a avaliar as outras linhas na amostragem de dados e abra mais eventos, caso outras linhas se qualifiquem. Da mesma forma, o item de exibição é mostrado na guia **Eventos** do Application Performance Dashboard, para que seja possível distinguir facilmente entre as linhas para as quais foram abertos eventos. A lista somente contém os atributos que podem ser designados como itens de exibição.

Operador Lógico
Ignore este campo caso seu limite tenha somente uma condição. Se você estiver medindo diversas condições, selecione um dos operadores a seguir antes de clicar em **Novo** para incluir uma segunda ou terceira (ou mais) condição:

And (&) caso a condição anterior e a condição seguinte tenham que ser atendidas para que o limite seja violado
Or (|) se qualquer uma delas puder ser atendida para que o limite seja violado

Não há suporte para uma combinação de operadores lógicos; os operadores devem ser todos And ou todos Or. O limite pode ter até nove condições quando o operador Or é usado; até 10 condições ao usar o operador And.

Se estiver usando a função `Missing` (descrita posteriormente na seção **Operador**), será possível usar apenas o operador And na fórmula.

Condições
A definição de limite pode incluir logicamente vários limites ou condições simultâneos.

Clique em **Novo** para incluir uma condição. Selecione uma condição e clique em **Editar** para modificar a expressão ou clique em **Excluir** para remover a expressão.

Após clicar em **Novo** ou **Editar**, conclua os campos na caixa de diálogo **Incluir Condição** ou **Editar Condição** que é aberta:

Contagem

Para os conjuntos de dados que retornam várias linhas para cada amostra de dados, é possível fazer a contagem de todas as linhas que atendem aos critérios da condição. É aberto um evento quando a contagem do **Valor** é atingida e todas as outras condições na fórmula são atendidas. Por exemplo, se o número de processos "zumbi" exceder 10, emita um alerta.

No exemplo a seguir, a condição será verdadeira quando mais de 10 linhas forem contadas: **Atributo** Registro de Data e Hora, **Operador** Maior Que, **Valor** 10.

Marque a caixa de seleção **Contagem**, o **Atributo** a ser contado, o **Operador** relacional e o **Valor** da contagem.

Se a fórmula tiver várias condições, cada condição deverá usar o operador booleano **And**. **Contagem** e **Delta de Tempo** são mutuamente exclusivos: ao marcar a caixa de seleção de uma função, a outra função é desativada. O atributo não pode ser um identificador do sistema, como Nome do Servidor ou ORIGINNODE, ser especificado como o **Item de Exibição** ou ser proveniente de um conjunto de dados para o qual o limite abre eventos puros.

Delta de Tempo

Use a função **Delta de Tempo** em uma condição para comparar o registro de data e hora de amostragem (como o horário da gravação) com a diferença de tempo especificada.

Ao marcar a caixa de seleção **Delta de Tempo**, o campo Delta de Tempo é exibido, permitindo combinar + (mais) ou - (menos) com o número de Dias, Horas, Minutos ou Segundos. Selecione **Horário de Amostragem** ou **Horário Específico** como o Valor a ser usado na comparação.

No exemplo de Log de Eventos a seguir, a fórmula compara a hora em que o evento foi gravado com o registro de data e hora da amostragem de dados. Caso o evento tenha ocorrido sete dias antes, a comparação será true. Se o operador relacional tiver sido mudado para Menor ou Igual, a comparação deverá ser verdadeira após 8 dias, 9 dias e assim por diante:

Atributo Timestamp
Delta de horário -7 dias
Operador Igual
Valor Entry Time

Atributo

Selecione o atributo a ser comparado nessa condição. Para ver uma descrição simples do atributo, passe o mouse sobre o nome na lista.

Operador

Selecione o operador relacional para o tipo de comparação:

```
Igual
Não igual
Maior que
Maior ou Igual a
Menos do que
Menor que ou igual a
Expressão regular contains
Expressão regular does not contain
```

`Expressão regular contains` e `Expressão regular does not contain` procuram um padrão correspondente à expressão. Quanto mais fácil for corresponder uma sequência à expressão, mais eficiente será a carga de trabalho no agente. A expressão não precisa corresponder à linha inteira; somente à subsequência na expressão. Por exemplo, em `See him run`, você deseja saber se a sequência contém `him .` Você poderia compor a expressão regular usando `him`, mas também seria possível usar `.*him.*`. Ou, se estivesse procurando See, você poderia inserir See ou `^See` para confirmar que isso é o início da linha. A inserção de curingas `.*` é uma procura menos eficiente e aumenta a carga de trabalho. Para obter mais informações sobre expressões regulares, consulte o tópico developerWorks® technical library ou procure `regex` em seu navegador.

Também é possível selecionar a função `Ausente`, que compara o valor da métrica especificada com uma lista de valores fornecidos. A condição é true quando o valor não corresponde a nenhum valor na lista. Essa função é útil quando você deseja uma notificação de que algo não está presente no sistema. Requisitos e restrições:

1. A métrica selecionada deve ser um atributo de texto: atributos de tempo e numéricos não podem ser usados.
2. Separe cada valor com uma vírgula (,), por exemplo, `fred,mary,jean`.
3. É possível ter apenas uma condição `Missing` em um limite.
4. `Ausente` deve ser a última condição da fórmula. Se outras condições forem necessárias, insira-as antes de incluir a função Missing e use apenas o operador **And (&)** na fórmula. Caso contrário, todas as linhas subsequentes serão desativadas.

Valor
Insira o valor a ser comparado, usando o formato permitido para a métrica, como 20 para 20% ou 120 para 2 minutos.

Designação de grupo
Designe um grupo de recursos para distribuir o limite aos sistemas gerenciados do mesmo tipo no grupo de recursos. Os grupos de recursos que estão disponíveis são os grupos definidos pelo usuário para os quais você tem permissão Modificar e os grupos de sistemas (para o tipo de agente) para os quais você tem permissão Visualizar. Os grupos de sistemas disponíveis também estão limitados àqueles adequados para o conjunto de dados escolhido.

Um limite sem um grupo designado não é distribuído para nenhum sistema monitorado e permanece parado até que seja distribuído a um grupo de recursos.

Um grupo do sistema, como `Linux OS` ou `Servidor HTTP`, distribui o limite para todos os sistemas gerenciados em que o agente está instalado. Por padrão, cada limite predefinido é designado ao grupo do sistema para esse agente. (É possível desativar todos os limites predefinidos na página **Configuração Avançada**, conforme descrito em "Ativação de níveis" na página 1075.)

A exceção são os sistemas gerenciados do domínio do IBM Tivoli Monitoring: Sistemas gerenciados do domínio do Tivoli Monitoring devem ser monitorados com situações que foram distribuídas em seu ambiente do Tivoli Monitoring.

Para designar grupos para o limite, marque a caixa de seleção de um ou mais grupos de recursos. Se a lista de grupos designados for longa, é possível marcar a ☐ **Mostrar Somente Grupos Selecionados**.

Se você não vir um grupo de recursos para o qual deseja designar o limite, poderá salvar a definição de limite e clicar em **OK** quando for solicitado para confirmar se deseja salvar o limite sem designá-lo a um grupo. Você pode, então, criar um novo grupo no **Gerenciador de Grupo de Recursos** e designar um limite para o novo grupo no **Editor de Grupos de Recursos**. Para obter mais informações, consulte "Gerenciador de Grupos de Recursos" na página 980.

Executar comando
Após a abertura de um evento para um limite avaliado como true, é possível executar automaticamente um comando ou um script de comandos no sistema monitorado para o qual o evento foi aberto. Por exemplo, você talvez queira registrar informações, acionar um sinal sonoro audível ou parar uma tarefa que está usando recursos excessivamente.

O comando utiliza a seguinte sintaxe:

```
&{data_set.attribute}
```

em que *data_set* é o nome do conjunto de dados e *attribute* é o nome do atributo, conforme mostrado no Editor de Limite. Se o conjunto de dados ou o nome do atributo contiver um espaço, substitua-o por um sublinhado.

O exemplo a seguir mostra como é possível transmitir o parâmetro de nome do disco para seu recurso gerenciado:

```
/scripts/clean_logs.sh &{KLZ_Disk.Disk_Name}
```

É possível transmitir um ou mais atributos do conjunto de dados. Se especificado, múltiplos atributos são transmitidos para o comando ordenadamente ($1, $2 e assim por diante).

O comando é executado a partir da linha de comandos com a mesma conta de usuário com a qual o agente foi iniciado. Por exemplo, se o agente estiver em execução como raiz, a raiz executará o comando no sistema gerenciado.

As opções a seguir controlam a frequência de execução do comando:

Marque a ☐ **Somente no Primeiro Evento** se o conjunto de dados retornar diversas linhas e você quiser executar o comando somente para a primeira ocorrência na amostra de dados. Desmarque a caixa de seleção para executar o comando para todas as linhas que causam um evento.

Marque a ☐ **Para Cada Intervalo Verdadeiro Consecutivo** para executar o comando cada vez que o limite for avaliado como verdadeiro. Desmarque a caixa de seleção para executar o comando quando o limite for true, mas não executá-lo novamente até que o limite seja avaliado como false, seguido por outra avaliação true em um intervalo subsequente.

Ao clicar em **Salvar**, o limite é aplicado a todos os sistemas monitorados do mesmo tipo de dados, dentro dos grupos de recursos designados.

Dica: É possível controlar o comportamento dos eventos e o encaminhamento de eventos usando as opções do **Gerenciador de Eventos** na página **Configuração Avançada**. Consulte “Configuração Avançada” na página 1073.

Nota: Para ver uma lista dos atributos que são adequados para inclusão na definição de limite, crie uma tabela com o conjunto de dados que você planeja usar. .

Conceitos relacionados

“Informações de histórico” na página 976
Revise as informações básicas para saber sobre limites, limites predefinidos para os agentes, os grupos de recursos aos quais eles são designados e sobre como customizar limites.

Tarefas relacionadas

“Tutorial: definindo um limite” na página 982

“Tutorial: Definindo um limite para executar um comando no recurso gerenciado” na página 984
É possível utilizar o **Editor de Limite** para transmitir determinados parâmetros para os agentes. É possível especificar comandos ou um script de comandos para que seja executado automaticamente quando um evento é acionado.

“Integrando-se ao Netcool/OMNIbus” na página 965
É possível encaminhar eventos do IBM Cloud Application Performance Management para o gerenciador de eventos IBM Tivoli Netcool/OMNIbus nas instalações.

Customizando um evento para encaminhar para um receptor EIF

É possível customizar os eventos de limite que são enviados para um receptor Event Integration Facility (EIF), como o Netcool/OMNIbus ObjectServer, para o Gerenciamento de eventos de nuvem ou o Alert Notification. Use a janela **Customização de slot EIF** para customizar o conteúdo do evento que é encaminhado para os destinos de eventos, substituindo, assim, o mapeamento padrão. É possível criar definições de mapa para eventos de limite que foram enviados para o receptor do Event Integration Facility. Use a janela **Customização de slot EIF** para customizar como os eventos são mapeados para eventos do EIF encaminhados, substituindo, assim, o mapeamento padrão. Customizando o modelo de mensagem, é possível incluir informações sobre o problema que foi identificado pelo evento e dados específicos do evento.Customizando o modelo de mensagem, é possível incluir informações sobre o problema que foi identificado pelo evento e incluir dados específicos a partir do evento.

Sobre Esta Tarefa

É possível customizar o slot base do EIF, que é um slot **msg** predefinido que envia a fórmula de limite para um destino de evento. Também é possível incluir um ou mais slots customizados do EIF para o

evento. Se você estiver usando o Netcool/OMNIbus ObjectServer, deverá atualizar o arquivo de regras de análise do EIF e os acionadores do ObjectServer se você desejar ver os slots customizados na IU do Netcool/OMNIbus.

É possível customizar o slot de base do EIF, que é um slot **msg** predefinido que envia a fórmula de limite para o receptor EIF. Também é possível incluir um ou mais slots customizados EIF, o que requer uma atualização no receptor EIF e no arquivo de regras de análise.

Procedimento

Conclua estas etapas para customizar como os eventos para o limite atual são mapeados para eventos encaminhados:

1. Se o **Gerenciador de Limite** não estiver aberto, clique em **Configuração do Sistema** > **Gerenciador de Limite**.
2. Clique na caixa de listagem **Tipo de Origem de Dados** e selecione o tipo de dados com o qual deseja trabalhar.
3. Se esse for um novo limite, clique em **Novo**; caso contrário, selecione um limite e clique em **Editar**.
4. Para customizar como os eventos para esse limite são mapeados para eventos encaminhados, certifique-se de que o **Encaminhador EIF** esteja configurado como `Sim`, clique em **Customização de Slot EIF** e execute uma das etapas a seguir:
   - **Slots EIF de Base**: para customizar o slot de base, selecione o botão de opções para **msg** e clique em **Editar**.
   - **Slots EIF Customizados**: para incluir um slot customizado, clique em **Incluir**; para editar um slot customizado, selecione o botão de opções para o slot e clique em **Editar**.

   A janela **Editar Intervalo** ou **Incluir Intervalo** é aberta.
5. Complete os campos para customizar os valores do intervalo:

Campo	Descrição	Restrição
Nome do Slot	O nome do slot customizado do EIF, que deve iniciar com um caractere.	O slot base do EIF é **msg** e não pode ser mudado.
Tipo de Slot	O tipo de slot customizado do EIF: **String Type** ou **Number Type**.	O intervalo base do EIF é **String Type** e não pode ser mudado.
Subtipo	O valor que é designado para o slot, que corresponde ao tipo de slot: • **Mapped Attribute** ativa o campo **Atributo mapeado** para incluir o valor do atributo selecionado no momento em que o evento ocorreu • **Literal Value** ativa o campo **Valor literal** para incluir texto no modelo de mensagem • **Literal Value + Mapped Attribute** ativa os campos **Valor literal** e **Atributo mapeado** para incluir valores de texto e de atributo para o modelo de mensagem e ativa o botão **Incluir** para incluir múltiplos valores de texto ou de atributo (ou ambos). Um espaço é incluído após cada valor literal ou atributo. O uso típico para o intervalo base do EIF **msg**, é especificar um **Valor literal + atributo mapeado** para o modelo de mensagem.	Um slot **Number Type** pode usar apenas **Mapped Attribute**.

Campo	Descrição	Restrição
Incluir	Se desejar enviar múltiplos valores literais ou valores de atributos na mensagem encaminhada, clique em **Incluir** para incluir outro conjunto de campos **Valor literal** e **Atributo mapeado**. Cada vez que você seleciona **Incluir**, esses campos são incluídos no painel. Para remover um conjunto de campos **Valor literal** e **Atributo mapeado**, desmarque ambos os campos antes de clicar em **OK**. Consulte Exemplo .	Ativado somente quando o **Subtipo** for **`Literal Value + Mapped Attribute`**. Máximo de 6 conjuntos de campos **Valor literal** e **Atributo mapeado**. Se não for possível ver os campos incluídos, use o recurso de zoom do navegador (Ctrl-) para reduzir o layout para ajustar a caixa de diálogo.
Valor literal	O texto a ser incluído no modelo de mensagem. Por exemplo, um valor literal de `Utilização de memória é alta em` com o atributo mapeado **`%Memory Utilization`**, é mostrado na interface com o usuário do **Gerenciador de eventos** como `Memory Utilization is high at 97.3%`. O modelo de mensagem consiste em texto de mensagem fixo e referências de substituição de variável ou em símbolos. O símbolo refere-se aos dados comuns ou do intervalo de evento ou uma referência especial para a fórmula de limite. Intervalos comuns são aqueles incluídos em todos os eventos encaminhados, como *threshold_name*; intervalos de eventos são aqueles específicos ao limite `msg`.	Desativado quando **Subtipo** é **`Mapped Attribute`**.
Atributo Mapeado	O atributo cujo valor você deseja incluir no modelo de mensagem. Os atributos disponíveis são a partir do conjunto de dados que foi selecionado para o limite. Por exemplo, para um limite que monitora o tempo alto do processador, você pode desejar mapear o atributo de porcentagem de tempo do usuário.	Máximo de 6 campos **Atributo Mapeado** . Desativado quando **Subtipo** é **`Literal Value`**. Quando o **Tipo de slot** é **`Number Type`**, somente os atributos numéricos estão disponíveis.
Multiplier	O multiplicador é o valor que é definido após a customização do valor do número do atributo mapeado original por um multiplicador: valor do slot = *attribute1* * *n*. Por exemplo, se você desejar converter minutos em segundos no evento EIF, especifique o multiplicador 60. O valor do multiplicador pode ser uma fração, expressa como um decimal, como 0,5 ou 5,4.	Ativado somente para atributos numéricos (o **Tipo de slot** é **`Number Type`**).

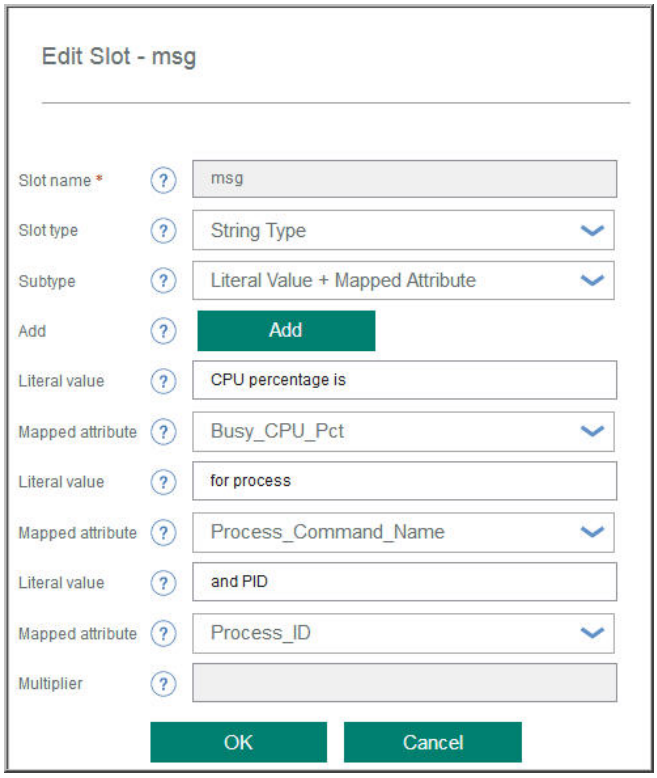
Após clicar em **OK** para fechar a janela, a janela **Customização de Intervalo do EIF** listará o nome do intervalo e se ele estiver customizado.

6. Após concluir a edição do intervalo base do EIF ou incluir, excluir ou editar intervalos customizados do EIF para o limite, clique em **OK**.
7. Após concluir a edição do limite, clique em **Salvar**.

   Para obter mais informações, consulte “Gerenciador de Limites” na página 985.

Exemplo

Os testes de limite `Linux_BP_ProcHighCpu_Critical` para consumo de CPU de 95% ou mais. Para incluir a porcentagem de CPU Ocupada, o nome do comando do processo e o ID do processo na mensagem de resumo (contida no slot msg), o slot msg foi customizado com três conjuntos de campos **Valor literal** e **Atributo mapeado**:



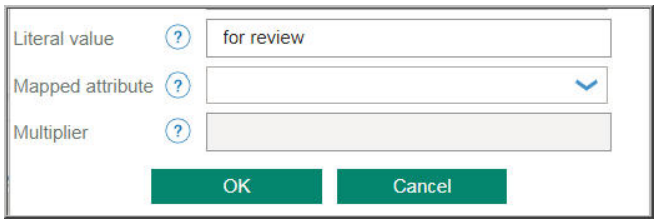
O modelo de mensagem é semelhante a este:

```
A porcentagem de CPU é
Busy_CPU_Pct para o processo Process_Command_Name e o PID
é Process_ID
```

E a mensagem resultante visualizada no Gerenciador de eventos pode ser semelhante a esta:

```
A porcentagem de CPU é 97 para o processo large.exe e o PID
é 9876
```

Também é possível incluir os campos **Valor literal** e **Atributo mapeado** e deixar um campo vazio. Por exemplo, para anexar "for review" ao modelo de mensagem, clique em **Incluir** e insira `for review` para **Valor Literal**.



O modelo de mensagem agora é semelhante a este:

```
A
porcentagem da CPU é Busy_CPU_Pct para o processo
Process_Command_Name e o PID é Process_ID para revisão
```

E a mensagem resultante visualizada no **Gerenciador de eventos** pode ser semelhante a esta:

```
A porcentagem de CPU é 96 para o processo big.exe e o PID
é 5432 para revisão
```

O que Fazer Depois
Se você criou novos slots customizados EIF, deverá identificar os novos slots na tabela `alerts.status` em seu Netcool/OMNIbus ObjectServer, em seguida, atualizar o arquivo de configuração `itm_apm_event.rules` que foi instalado durante a integração do Netcool/OMNIbus com o Cloud APM.

Incluindo slots customizados EIF no banco de dados do Netcool/OMNIbus ObjectServer
Ao incluir novos slots customizados EIF para limites, você deve identificá-los em seu receptor EIF antes de poder visualizar eventos encaminhados que usam os slots customizados. Se você tiver o Netcool/OMNIbus integrado com o Cloud APM, atualize a tabela `alerts.status` para definir os novos slots.

Sobre Esta Tarefa
Quando configurou a integração do Netcool/OMNIbus com o Cloud APM, etapa "4" na página 969, você carregou `itm_apm_db_update.sql`. No procedimento a seguir, use a interface SQL interativa para atualizar a tabela `alerts.status` no banco de dados `itm_apm_db_update.sql`.

Procedimento

Conclua essas etapas no Netcool/OMNIbus ObjectServer para definir os novos slots customizados EIF criados no **Editor de limite**:

1. Inicie a interface interativa SQL para editar o banco de dados:

   Linux

   ```
   $OMNIHOME/bin/nco_sql -user user_name -password password
   -server server_name > itm_apm_db_update.sql
   ```

   Por exemplo:

   ```
   $OMNIHOME/bin/nco_sql -user smadmin -password passw0rd -server NCOMS >
   /tmp/apm/itm_apm_db_update.sql
   ```

   Windows

   ```
   itm_apm_db_update.sql | %OMNIHOME%\..\bin\isql -U user_name
   -P password -S server_name
   ```

   Por exemplo:

   ```
   \temp\apm\itm_apm_db_update.sql | %OMNIHOME%\ .. \bin\isql -U smadmin
   -P passw0rd -S NCOMS
   ```

2. Para cada slot customizado EIF, digite o comando SQL **ALTER TABLE** com o nome e o tipo de slot customizados no formato a seguir, pressione Enter e, em seguida, digite go e pressione Enter:

   - Para um tipo de slot de sequência,

     ```
     alter table alerts.status add CustomSlotName varchar(512);
     ```

   - Para um tipo de slot de número,

     ```
     alter table alerts.status add CustomSlotName integer;
     ```

   em que *CustomSlotName* é o nome do slot customizado EIF exatamente como ele foi inserido no campo **slotName** da janela **Incluir slot** no **Editor de limite**.

Exemplo

O exemplo mostra os comandos **`alter table`** para incluir os slots customizados **`BusinessApplication`** e **`GenericMetric`**.

```
alter table alerts.status add BusinessApplication varchar(512);
```

```
alter table alerts.status add GenericMetric integer;
```

O que Fazer Depois
Atualize o arquivo de configuração `itm_apm_event.rules` que foi instalado como parte da integração do Netcool/OMNIbus com o Cloud APM. Para obter mais informações, consulte "Incluindo slots customizados EIF nas regras de evento do receptor EIF" na página 995.

Incluindo slots customizados EIF nas regras de evento do receptor EIF
Se você definiu novos slots customizados EIF para limites, deverá atualizar o arquivo de regras para identificar os novos slots para o receptor EIF.

Sobre Esta Tarefa

Estas etapas permitem atualizar o arquivo `itm_apm_event.rules` no Netcool/OMNIbus Probe for Tivoli EIF para identificar cada novo slot customizado EIF. Se estiver usando outro receptor EIF, atualize os arquivos de regras conforme requerido pelo receptor.

Procedimento

1. No sistema onde o Probe for Tivoli EIF está instalado, mude para o diretório de instalação.

   Linux Cd *install_dir*`/tivoli/netcool/omnibus/probes/linux2x86`

   Windows Cd *install_dir*`\Tivoli\Netcool\omnibus\probes\win32`

   em que *install_dir* é o `/opt/IBM/` ou `C:\IBM\` padrão ou o diretório especificado quando a análise foi instalada.
2. Faça uma cópia de backup do arquivo `itm_apm_event.rules`.
3. Abra o arquivo Probe for Tivoli EIF `itm_apm_event.rules` em um editor de texto.

   O arquivo tem três partes para ele que estão sendo editadas para incluir o slot (ou slots) EIF customizado(s) que foram criados.
4. Anexe as instruções **if** com uma nova instrução para cada slot customizado EIF que usa o seguinte formato:

   ```
   if(exists($CustomSlotName))
   {
       if(regmatch($CustomSlotName, "^'.*'$"))
       {
           $SourceType = extract($CustomSlotName, "^'(.*)'$")
       }
   }
   ```

   em que *CustomSlotName* é o nome do slot customizado EIF exatamente como ele foi inserido no campo **slotName** da janela **Incluir slot**.
5. Anexe a lista de entradas `@` com uma nova linha para cada slot customizado EIF que usa o seguinte formato:

   ```
   Utilize$CustomSlotName= $CustomSlotName
   ```

   em que *CustomSlotName* é o nome do slot customizado do EIF.
6. Anexe a lista de entradas `$tmpEventData` com uma nova linha para cada slot EIF customizado que usa o seguinte formato:

   ```
   $tmpEventData = nvp_remove( $tmpEventData, "CustomSlotName")
   ```

   em que *CustomSlotName* é o nome do slot customizado do EIF.
7. Salve e feche o arquivo `itm_apm_event.rules`.
8. Reinicie o Probe for Tivoli EIF para implementar suas atualizações.

Resultados
O arquivo de regras é atualizado e o Probe for Tivoli EIF agora pode processar eventos de limite que usam os novos slots customizados EIF e encaminham os detalhes do evento para o Netcool/OMNIbus ObjectServer.

Exemplo

Aqui está um resumo do `itm_apm_event.rules` após ele ter sido editado para incluir esses slots customizados EIF: **BusinessApplication** e **GenericMetric** (mostrados em itálico).

```
# ------------------------------------------------------------
    if(exists($SourceID))
    {
        if(regmatch($SourceID, "^'.*'$"))
        {
            $SourceID = extract($SourceID, "^'(.*)'$")
        }
    }
    ...
    ...
    ...
    if(exists($ManagedSystemGroups))
    {
        if(regmatch($ManagedSystemGroups, "^'.*'$"))
        {
            $SourceType = extract($ManagedSystemGroups, "^'(.*)'$")
        }
    }
    if(exists($BusinessApplication))
    {
        if(regmatch($BusinessApplication, "^'.*'$"))
        {
            $SourceType = extract($BusinessApplication, "^'(.*)'$")
        }
    }
     if(exists($GenericMetric))
    {
        if(regmatch($GenericMetric, "^'.*'$"))
        {
            $SourceType = extract($GenericMetric, "^'(.*)'$")
        }
    }

 @SourceID=$SourceID
 @URL=$ManagementURL
 @Service=$Service
 @SourceType=$SourceType
 @SubscriberID=$TenantID
 @APMHostname=$apm_hostname
 @ManagedSystemGroups=$ManagedSystemGroups
 @BusinessApplication=$BusinessApplication
 @GenericMetric=$GenericMetric

 # ------------------------------------------------------------------
 -RTC 66157
 # ------------------------------------------------------------------
 if ( exists ( $appl_label ) )
 {
    if ( match($appl_label, "PI:A:S"))
    {
        @Class = 87723
    }
 }
 # ------------------------------------------------------------------
 # -  RTC 48775 - APM FP5 agents do not populate data in email of EMaaS Basic
 # ------------------------------------------------------------------
 if (match( $situation_eventdata, "~" ) )
 {
    # Dump all fields into the ITMEventData field
    $tmpEventData = nvp_add($*)
    # Remove the duplicated fields
    $tmpEventData = nvp_remove( $tmpEventData, "appl_label")
    $tmpEventData = nvp_remove( $tmpEventData, "control")
    ...
    ...
    ...
    $tmpEventData = nvp_remove( $tmpEventData, "ManagedSystemGroups")
    $tmpEventData = nvp_remove( $tmpEventData, "EventSeqNo")
```

```
    $tmpEventData = nvp_remove( $tmpEventData, "BusinessApplication")
    $tmpEventData = nvp_remove( $tmpEventData, "GenericMetric")
       @ITMEventData = $tmpEventData
```

Enviando email em resposta a um evento

Somente Quando seu ambiente gerenciado incluir o IBM Alert Notification, é possível fornecer notificação por e-mail quando o desempenho do aplicativo excede os limites.

Sobre Esta Tarefa

Para configurar a notificação por e-mail, deve-se ativar IBM Alert Notification, conforme descrito no Coleção de tópico Notificação de Alerta no IBM Knowledge Center. Em seguida, inclua aplicativos monitorados para grupos de recursos. Para cada grupo de recursos, é possível configurar um ou vários endereços de email. Quando o desempenho de qualquer aplicativo em um grupo exceder um limite, você receberá uma notificação por email para os endereços que são configurados para o grupo.

Procedimento

1. Clique em **Configuração do Sistema** > **Gerenciador do Grupo de Recursos**.
2. Clique em **Novo** para criar o grupo de recursos para o qual você deseja configurar a notificação por e-mail ou selecione um grupo existente e clique em **Editar**.

   O **Editor do Grupo de Recursos** se abre.
3. Clique em **Configurar notificação por e-mail** para abrir o aplicativo IBM Alert Notification em uma nova guia ou janela do navegador. Use Alert Notification para criar usuários e associar seus endereços de e-mail aos grupos de recursos para receber notificações de eventos por e-mail.

Usando a API Serviço de Gerenciamento de Grupo de Recursos

Use a API de Serviço de Gerenciamento de Grupo de Recursos para gerenciar o ciclo de vida de grupos de sistemas gerenciados a partir da linha de comandos.

Sobre Esta Tarefa

Conclua tarefas do grupo de recursos, como criar, visualizar, atualizar e excluir grupos de sistemas gerenciados. Inclua e remova sistemas individuais de grupos customizados. Visualize uma lista de sistemas que foram incluídos em um grupo de recursos customizados específico e visualize uma lista de sistemas que são incluídos automaticamente nos grupos integrados, como o grupo de recursos do sistema.

É possível criar scripts para automatizar tarefas, como definir grupos de recursos e designar agentes a esses grupos de recursos. Os grupos de recursos podem ser destinos de distribuições de limites e ou políticas de controle de acesso.

As operações a seguir são descritas no API Explorere no Exemplo no final deste tópico.

- Retornar todos os grupos de recursos, agentes, ou um grupo de recursos ou agente específico.
- Criar um grupo de recursos customizados ou atualizar a definição de um grupo existente
- Excluir um grupo de recursos customizados especificado
- Incluir agentes em um grupo de recursos customizados
- Remover agentes de um grupo de recursos customizados

Procedimento

Conclua essas etapas para definir e mudar grupos de recursos customizados com a API Serviço de Gerenciamento de Grupo de Recursos. Os grupos de recursos e agentes do sistema não podem ser modificados.

1. Conclua a etapa 1 até a etapa 9 no tópico Explorando as APIs.

   A Etapa 10 e a Etapa 11 fornecem detalhes adicionais.

2. Clique em **USAR** e selecione uma chave, por exemplo, **Key1**.

   Nota: Clique em **Ocultar** para mostrar seu ID e seu segredo do cliente. Anote-os, já que eles serão necessários se você estiver fazendo chamadas da API com ferramentas externas fora do API Explorer. Em seguida, clique em **Mostrar** para ocultá-los.
3. Preencha todos os cabeçalhos necessários, indicados com um asterisco.

   X-IBM-Service-Location
   * cabeçalho é a localização geográfica de sua assinatura, como na para América do Norte

   Autorização
   * o cabeçalho é sua sequência codificada em base64 do IBMid e senha. Ao codificar o IBMid e a senha na ferramenta based64-encoder, o formato deverá ser *IBMid:password*, por exemplo, `Basic YXBtYWRtaW46YXBtcGFzcw==!`.
4. Deve-se incluir um cabeçalho referente em todas as solicitações de POST, PUT e DELETE. O valor para o cabeçalho Referer é:

   ```
   -H 'Referer: https://api.ibm.com'
   ```
5. Role para localizar e clique em **Testar**.

Resultados
As mudanças feitas nos grupos de recursos customizados na API são efetivadas imediatamente e exibidas no **Gerenciador de Grupos de Recursos** (consulte “Gerenciador de Grupos de Recursos” na página 980).

Exemplo

Esse comando retorna os nomes, identificadores exclusivos, status, nome do host, versão e o tipo de agente para todos os agentes:

```
GET /1.0/topology/mgmt_artifacts?_filter=entityTypes=Agent&_field=keyIndexName&
_field=online&_field=hostname&_field=version&_field=productCode&_field=description
```

Este comando retorna uma lista de todos os agentes de S.O. Linux:

```
GET /1.0/topology/mgmt_artifacts?_filter=entityTypes=Agent&_filter=description=
"Linux OS"&_field=keyIndexName
```

Esse comando retorna uma lista de grupos do sistema e customizados:

```
GET /1.0/topology/mgmt_artifacts?_filter=entityTypes:AgentGroup,
AgentSystemGroup&_field=keyIndexName&_field=displayLabel
```

Esse comando retorna a lista de agentes que são designados a um grupo que tem o identificador exclusivo {id}:

```
GET /1.0/topology/mgmt_artifacts/{id}/references/to/contains
```

O exemplo a seguir usa o comando curl para criar um grupo customizado.

```
POST /1.0/topology/mgmt_artifacts
```

Nota: O corpo da solicitação POST deve conter um objeto JSON que defina o grupo, conforme mostrado pelo parâmetro **-d**.

```
curl -X POST \
  https://api.ibm.com/perfmgmt/run/1.0/topology/mgmt_artifacts \
  -H 'Referer: https://api.ibm.com' \
  -H 'authorization: Basic REPLACE_BASE64_ENCODED_STRING' \
  -H 'content-type: application/json' \
  -H 'x-ibm-client-id: REPLACE_KEY_VALUE' \
  -H 'x-ibm-client-secret: REPLACE_KEY_VALUE' \
  -d '{
  "keyIndexName": "customGroup",
  "description": "Custom group description",
```

```
  "displayLabel": "customGroupLabel",
  "entityTypes": [
    "AgentGroup"
  ],
  "arbitraryStringProperty": "Your custom property value"
}'
```

Esse comando inclui um agente com identificador exclusivo {otherid} em um grupo customizado que possui um identificador exclusivo {id}:

```
POST /1.0/topology/mgmt_artifacts/{id}/references/to/contains/{otherid}
```

Esse comando remove um agente com identificador exclusivo {otherid} de um grupo customizado que possui um identificador exclusivo {id}:

```
DELETE /1.0/topology/mgmt_artifacts/{id}/references/to/contains/{otherid}
```

Usando a API do serviço de gerenciamento de limite

Use a API de Serviço de Gerenciamento de Limite para gerenciar o ciclo de vida de limites de monitoramento a partir da linha de comandos.

Sobre Esta Tarefa

Conclua tarefas do gerenciador de limites, como criar, visualizar, atualizar e excluir limites. Designe grupos de recursos a esses limites. Visualize uma lista de todas as designações de limites e recursos. Visualize uma lista de todos os limites que são designados a um grupo de recursos específico.

É possível criar scripts para automatizar tarefas, como definir limites e designar esses limites a grupos de recursos.

As operações a seguir são descritas no API Explorere no Exemplo no final deste tópico.

- Retornar todos os limites ou obter um limite específico. É possível filtrar a solicitação com esses atributos: **`label`**, que corresponde ao nome do limite; **`_appliesToAgentType`**, que corresponde ao código do produto de 2 caracteres e **`_uiThresholdType`**, que corresponde ao tipo de limite que é mostrado nas páginas do editor do Gerenciador de limites e do Grupo de recursos do Console do Cloud APM. É possível usar **`_offset`** ou **`_limit`** ao obter limites
- Criar um limite ou atualizar a definição de um limite existente. Você deve incluir o cabeçalho X-HTTP-Method-Override e configurar como PATCH para solicitação de atualização
- Excluir um limite especificado
- Retornar todas as designações de recursos ou uma designação de recurso específica, que mostra os limites que são designados a cada grupo de recursos. É possível filtrar a solicitação com estes atributos: **`resource._id`** e **`threshold._id`**; e os usos destes operadores suportados são **=** (equal) e **!=** (not equal)
- Crie uma designação de recurso, que designa um único limite a um único grupo de recursos
- Exclua uma designação de recurso, que remove um único limite de um único grupo de recursos

Procedimento

1. Conclua a etapa 1 até a etapa 9 no tópico Explorando as APIs.

   A Etapa 10 e a Etapa 11 fornecem detalhes adicionais.
2. Clique em **USAR** e selecione uma chave, por exemplo, **Key1**.

   Nota: Clique em **Ocultar** para mostrar seu ID e seu segredo do cliente. Anote-os, já que eles serão necessários se você estiver fazendo chamadas da API com ferramentas externas fora do API Explorer. Em seguida, clique em **Mostrar** para ocultá-los.
3. Preencha todos os cabeçalhos necessários, indicados com um asterisco.

   X-IBM-Service-Location
   * cabeçalho é a localização geográfica de seu servidor, como na para América do Norte

Autorização
* cabeçalho é sua sequência codificada com base64 do IBMid e senha. Ao codificar o IBMid e a senha na ferramenta do codificador based64, o formato deve ser *IBMid:password*. Por exemplo, `Basic YXBtYWRtaW46YXBtcGFzcw==!`.

4. Role para localizar e clique em **Testar**.

Exemplo

Este comando retorna todos os limites registrados com o servidor:

```
GET /threshold_types/itm_private_situation/thresholds
```

Este comando retorna as informações para o limite com o rótulo (nome) `My_threshold`.

```
GET
/threshold_types/itm_private_situation/thresholds?_filter=label%3DMy_threshold
```

Este comando retorna todos os limites para o tipo de agente LZ, que é o código de componente do agente do S.O. Linux.

```
GET
/threshold_types/itm_private_situation/thresholds?_filter=_appliesToAgentType%3DLZ
```

Esse comando tem a mesma saída do comando anterior, mas o nome do agente como ele aparece no Console do Cloud APM é fornecido.

```
GET
/threshold_types/itm_private_situation/thresholds?_filter=_uiThresholdType%3DLinux
OS
```

Este comando retorna todos os grupos de recursos ao qual o limite 123 é designado:

```
GET /resource_assignments?_filter=threshold._id=123
```

O exemplo a seguir usa o comando curl para criar um novo limite.

```
POST /1.0/thresholdmgmt/threshold_types/itm_private_situation/thresholds
```

Lembre-se: O corpo da solicitação POST deve conter um objeto JSON que defina o limite conforme mostrado pelo parâmetro **-d**. Exemplo:

```
curl -X POST \
 https://api.ibm.com/perfmgmt/run/1.0/thresholdmgmt/threshold_types/itm_private_situation/
thresholds  \
  -H 'authorization: Basic REPLACE_BASE64_ENCODED_STRING' \
  -H 'content-type: application/json' \
  -H 'x-ibm-client-id: REPLACE_KEY_VALUE' \
  -H 'x-ibm-client-secret: REPLACE_KEY_VALUE' \
  -d '{
  "label": "Your_Linux_Threshold_Name",
  "description": "Your Linux Threshold Definition",
  "configuration": {
    "type": "json",
    "payload": {
      "formulaElements": [
        {
          "function": "*MKTIME",
          "metricName": "KLZ_CPU.Timestamp",
          "operator": "*EQ",
          "threshold": "1455767100000",
          "timeDelta": {
            "operator": "+",
            "delta": "3",
            "unit": "Hours"
          }
        }
      ],
      "period": "011500",
      "periods": "3",
```

```
      "severity": "Fatal",
      "matchBy": "KLZCPU.CPUID",
      "operator": "*OR",
      "actions":[
        {
          "name": "command",
          "command": "ps -ef",
          "commandFrequency": "Y",
          "commandWhen": "Y",
          "commandWhere": "N"
        }
      ]
    }
  }
}'
```

Gerenciando o acesso de usuário

Use os recursos de Controle de Acesso Baseado na Função no Cloud APM para conceder aos usuários os privilégios de acesso necessários para suas funções.

A segurança no Cloud APM baseia-se em funções. Uma função é um grupo de permissões que controlam as ações que podem ser executadas no Cloud APM. É possível criar funções customizadas no Cloud APM. É possível designar permissões para funções customizadas ou designar mais permissões para as funções padrão existentes. É possível designar usuários e grupos de usuários às funções padrão existentes ou a funções customizadas. É possível designar usuários e grupos de usuários para várias funções. As permissões são acumulativas, um usuário ou grupo de usuários tem permissões para todas as funções para as quais está designado.

No Cloud APM, a autenticação do usuário é gerenciada por meio do IBM Marketplace ou pode ser gerenciada por meio de Operações Colaborativas, caso você possua uma assinatura.

A autenticação do usuário no Performance Management requer um IBMid. Crie um ID IBM selecionando o link **Criar um ID IBM** na página **Conectar-se à IBM**. Para acessar a página **Conectar-se à IBM**, acesse a página **Produtos e Serviços** (http://ibm.biz/my-prodsvcs) no IBM Marketplace, e você será direcionado para a página **Conectar-se à IBM** (poderá ser necessário efetuar logout e retornar para a página **Produtos e Serviços** (http://ibm.biz/my-prodsvcs)).

Quando tiver um IBMid, será possível efetuar login no Cloud APM, diretamente ou a partir de Produtos e Serviços. A autorização para acessar uma instância do Cloud APM é gerenciada usando **Produtos e Serviço** ou por meio de Operações Colaborativas, caso você possua uma assinatura. Por padrão, o usuário que solicita uma avaliação ou adquire uma assinatura tem privilégios de administrador.

O proprietário da assinatura do Cloud APM é o usuário padrão no Cloud APM. Este é o usuário que solicita uma avaliação ou adquire uma assinatura. Esse usuário padrão é um membro da função Administrador e tem privilégios de administrador que permitem que esse usuário inclua novos usuários. Por padrão, os usuários subsequentes são incluídos na função Usuário de Monitoramento.

Se você não for um membro de uma função e tentar efetuar login no Cloud APM, receberá uma mensagem **Não Autorizado**.

Para incluir um usuário do Cloud APM:

1. Acesse **Produtos e Serviços** no IBM Marketplace e expanda o widget **IBM Performance Management**.
2. Clique em **Gerenciar autorizações** e insira um ID IBM ou endereço de e-mail nos campos **Incluir novo usuário** ou **Procurar por usuários existentes**. Clique em **Incluir usuário** para incluir o usuário.

Não há limite no número de usuários que podem ser incluídos em uma assinatura do Cloud APM.

Nota: Não há suporte para grupos de usuários no Cloud APM.

Para obter mais informações sobre funções, consulte “Funções e permissões” na página 1002.

Funções e permissões

Uma *função* é um grupo de permissões que controlam as ações que podem ser executadas no Cloud APM. Use a página Controle de acesso baseado na função para gerenciar usuários e funções ou, como alternativa, usar a API de Autorização para concluir as tarefas de controle de acesso baseado na função a partir da linha de comandos.Para obter mais informações, consulte “Explorando as APIs” na página 1072.

Cloud APM possui quatro funções padrão:

Administrador de Função
Esta função destina-se aos usuários cuja principal função de tarefa é criar políticas de controle de acesso para o Cloud APM. Essa função possui todas as permissões. Caso o usuário padrão seja alterado, o novo usuário padrão será automaticamente um membro da função Administrador de Função. Essa função não pode ser editada. Os Administradores de Função não podem remover a si mesmos da função de Administrador de Função. Essa restrição remove o risco da remoção acidental de todos os usuários da função de Administrador de Função.

Administrador de Monitoramento
Esta função destina-se aos usuários cuja principal função de tarefa é usar o Cloud APM para monitorar sistemas. Os Administradores de Monitoramento executam tarefas como inclusão de aplicativos de monitoramento, criação de limites, inclusão de grupos de recursos e distribuição de limites para esses grupos de recursos. Essa função pode ser editada.

Administrador do Sistema
Esta função destina-se aos usuários cuja principal função de tarefa é executar tarefas de administração para o sistema Cloud APM. Os Administradores do Sistema executam tarefas como configuração do Gerenciador de Eventos ou configuração do Gateway Híbrido. Essa função pode ser editada.

Usuário de Monitoramento
Esta função destina-se aos usuários cuja principal função de tarefa é configurar e manter o funcionamento e o estado dos sistemas monitorados pelo Cloud APM. Essa função pode ser editada.

A tabela a seguir descreve as permissões que podem ser designadas para funções e as quatro funções padrão disponíveis, e as permissões associadas:

Tabela 237. Funções e permissões

	Administrador de Função		**Administrador de Monitoramento**		**Administrador do Sistema**		**Usuário de Monitoramento**	
	Visualizar	**Modificar**	**Visualizar**	**Modificar**	**Visualizar**	**Modificar**	**Visualizar**	**Modificar**
Permissões de configuração do sistema								
Configuração Avançada	✓	N/D	—	N/A	✓	N/A	—	N/A
Configuração do Agente	✓	N/A	✓	N/A	—	N/A	—	N/A
Páginas Informativas	✓	N/A	✓	N/A	✓	N/A	✓	N/A
Provedor de Procura	✓	N/A	✓	N/A	—	N/A	—	N/A
Estatísticas de Uso	✓	N/A	✓	N/A	—	N/A	—	N/A
Permissões de recurso								
Painel de desempenho do aplicativo	✓	✓	✓	✓	✓	—	✓	—
Aplicativos	✓	✓	✓	✓	—	—	✓	—
Aplicativo individual	“Permissões do grupo de aplicativos e recursos” na página 1006							
Painel de diagnósticos	✓	N/A	—	N/A	—	N/A	—	N/A

Tabela 237. Funções e permissões (continuação)								
	Administrador de Função		**Administrador de Monitoramento**		**Administrador do Sistema**		**Usuário de Monitoramento**	
	Visualizar	**Modificar**	**Visualizar**	**Modificar**	**Visualizar**	**Modificar**	**Visualizar**	**Modificar**
Gerenciador de Grupos de Recursos	✓	N/A	✓	N/A	—	N/A	—	N/A
Grupo de recursos individuais	"Permissões do grupo de aplicativos e recursos" na página 1006							
Grupos de Recursos	✓	✓	✓	✓	—	—	—	—
Gerenciador de script sintético	✓	N/A	—	N/A	—	N/A	—	N/A
Gerenciador de Limites	✓	N/A	✓	N/A	—	N/A	—	N/A

Where

✓ indica que membros dessa função têm essa permissão

— indica que membros dessa função não têm essa permissão

N/A indica que essa permissão não existe

Nota: Embora **`Usage Statistics`** seja exibido na lista de **Permissões de configuração do sistema**, essa opção não é mais aplicável ao Cloud APM.

A tabela a seguir descreve as ações que estão associadas a cada permissão:

Tabela 238. Permissões	
Permissão	**Descrição**
Configuração Avançada	Se você tiver permissão de visualização, poderá executar as seguintes tarefas: • Visualize **Configuração do Sistema** > **Configuração Avançada** na barra de menus. • Fazer e salvar mudanças na janela **Configuração avançada**. • Visualize **Configuração do Sistema** > **Gerenciador de Gateway Híbrido** na barra de menus. • Faça e salve mudanças na janela **Gerenciador de Gateway Híbrido**.
Configuração do Agente	Se você tiver permissão de visualização, poderá executar as seguintes tarefas: • Visualize **Configuração do Sistema** > **Configuração do Agente** na barra de menus. • Fazer e salvar mudanças na janela **Configuração do agente**.
Páginas Informativas	Se você tiver permissão de visualização, poderá executar a seguinte tarefa: • Visualize **Introdução** e **Ajuda** na barra de menus. **Nota:** Quando a página **Introdução** é aberta, se você limpar **Mostrar está página na inicialização**, para logins subsequentes, você verá um erro de permissão negada. No entanto, ainda será possível navegar até a página **Introdução** e quaisquer outras áreas para as quais tenha permissão.

Tabela 238. Permissões (continuação)	
Permissão	**Descrição**
Provedor de Procura	Se você tiver permissão de visualização, poderá executar as seguintes tarefas: • Visualize **Configuração do Sistema** > **Configurar Provedores de Procura** na barra de menus. • Fazer e salvar mudanças na página **Configurar provedores de procura**.
Painel de desempenho do aplicativo	Se você tiver permissão de visualização, poderá executar as seguintes tarefas: • Visualize o **Desempenho** > **Application Performance Dashboard** na barra de menus. • Visualizar o Application Performance Dashboard e **Meus Componentes** e os aplicativos predefinidos **Minhas Transações**. **Nota:** Para determinar quais permissões são necessárias para ver os sistemas no aplicativo Meus Componentes, consulte "Permissões do grupo de aplicativos e recursos" na página 1006. **Nota:** O aplicativo Minhas Transações será exibido apenas se você estiver usando o Web Site Monitoring. Todas as transações sintéticas do Web Site Monitoring são exibidas no aplicativo Minhas Transações. • Abrir páginas do painel customizado na guia Visualizações customizadas. • Criar visualizações na guia Detalhes do atributo e salvá-las para uso próprio. Se você tiver permissão de modificação, poderá executar as seguintes tarefas: • Visualize o **Desempenho** > **Application Performance Dashboard** na barra de menus. • Visualizar o Application Performance Dashboard e os aplicativos predefinidos **Meus Componentes** e **Minhas Transações**. **Nota:** Para determinar quais permissões são necessárias para ver os sistemas no aplicativo Meus Componentes, consulte "Permissões do grupo de aplicativos e recursos" na página 1006. **Nota:** O aplicativo Minhas Transações será exibido somente se você estiver usando o Web Site Monitoring. Todas as transações sintéticas do Web Site Monitoring são exibidas no aplicativo Minhas Transações. • Criar e salvar páginas de painel customizado na guia Visualizações customizadas. • Criar visualizações na guia Detalhes do Atributo e compartilhá-las com outros. • Visualizar a opção **Ações**>**Editar** nas páginas do componente; essa opção permite editar os valores de limite e outras configurações dos widgets de grupo que são exibidos no painel Componentes.

Tabela 238. Permissões (continuação)

Permissão	Descrição
Aplicativos	Se você tiver permissão de visualização, poderá executar as seguintes tarefas: • Visualizar aplicativos no Application Dashboard. Se você tiver permissão de modificação, poderá executar as seguintes tarefas: • Visualizar aplicativos no Application Dashboard • Crie, modifique e exclua aplicativos com as ferramentas no Application Dashboard.
Aplicativo individual	Consulte "Permissões do grupo de aplicativos e recursos" na página 1006.
Gerenciador de Grupos de Recursos	Se você tiver permissão de visualização, poderá executar a seguinte tarefa: • Visualize **Configuração do Sistema** > **Gerenciador de Grupo de Recursos** na barra de menus.
Grupos de Recursos	Se você tiver permissão de visualização, poderá executar as seguintes tarefas: • Visualizar os grupos de recursos e os sistemas neles no Gerenciador de Grupos de Recursos se você também tiver a permissão de visualização do Gerenciador de Grupo de Recursos. • Visualizar os sistemas no aplicativo predefinido Meus Componentes se você também tiver a permissão de visualização ou a permissão de modificação do Application erformance Management • Visualizar os sistemas na janela **Incluir aplicativo** se você também tiver permissão para modificar aplicativos. Se você tiver permissão de modificação, poderá executar as seguintes tarefas: • Visualizar grupos de recursos e seu conteúdo no Gerenciador de Grupo de Recursos se você também tiver a permissão de visualização Gerenciador de Grupo de Recursos. • Visualizar os sistemas no aplicativo predefinido Meus Componentes, se você também tiver a permissão de visualização ou de modificação do Application Performance Management. • Visualizar os sistemas na janela **Incluir aplicativo**, se você também tiver permissão para modificar aplicativos. • Criar, modificar e excluir grupos de recursos no Gerenciador de Grupo de Recursos se você também tiver a permissão de visualização Gerenciador de Grupo de Recursos. Para designar limites a um grupo de recursos, também é necessário ser membro de uma função com permissão de visualização para o Gerenciador de Limite. **Nota:** O Gerenciador de Grupo de Recursos é usado para organizar sistemas monitorados em grupos, para que os limites possam ser designados a esses grupos. Se você não tiver permissão de visualização para o Gerenciador de Limites, não será possível ver os limites que são designados aos Grupos de Recursos. Se você designar a permissão Modificar dos Grupos de Recursos a uma função, também será necessário designar a permissão de visualização do Gerenciador de Limites à função.

Tabela 238. Permissões (continuação)	
Permissão	**Descrição**
Grupo de recursos individuais	Consulte “Permissões do grupo de aplicativos e recursos” na página 1006.
Gerenciador de Limites	Se você tiver permissão de visualização, poderá executar as seguintes tarefas: • Visualize **Configuração do Sistema** > **Gerenciador de Limite** na barra de menus. • Criar, modificar e excluir limites no Gerenciador de Limites. • Visualizar e editar a designação do grupo de recursos para limites no Gerenciador de Limites, se você tiver as permissões apropriadas para um ou mais grupos de recursos. • Como alternativa, visualize e edite a designação de limites para grupos de recursos no Gerenciador de Grupo de Recursos, se você tiver as permissões apropriadas para o Gerenciador de Grupo de Recursos e para um ou mais grupos de recursos e permissão de visualização para o Gerenciador de Limites.
Gerenciador de script sintético	Se você tiver permissão de visualização, poderá executar as seguintes tarefas: • Criar, modificar e excluir as transações sintéticas no Gerenciador de transações sintéticas. **Nota:** Para trabalhar com transações sintéticas no Synthetic Transaction Manager, também é necessário ser membro de uma função que tenha permissão de visualização para **Configuração do agente**.
Painel de diagnósticos	Se você tiver permissão de visualização, o botão **Diagnosticar** está ativado nos painéis de diagnóstico para o WebSphere Applications agent, o Agente Node.js, o Agente Ruby e o Microsoft .NET agent. Clique no botão **Diagnosticar** para realizar drill down em painéis de diagnósticos.

Permissões do grupo de aplicativos e recursos
Permissões podem ser designadas a aplicativos individuais e grupos de recursos.

Permissões de aplicativo

No Cloud APM, aplicativo é um grupo de componentes e as instâncias dentro desses componentes. Use a janela **Incluir Aplicativo** para definir um aplicativo. Para obter informações adicionais sobre como definir um aplicativo, consulte Gerenciando aplicativos.

Para selecionar **Desempenho** > **Painel de Desempenho do Aplicativo** no Console do Cloud APM, deve-se ter designado a permissão de visualização ou modificação para o Application Performance Dashboard. Essa permissão também permite ver os aplicativos predefinidos **Meus Componentes** e **Minhas Transações**. O aplicativo **Minhas Transações** será exibido somente se você estiver usando o Web Site Monitoring. Para ver outros aplicativos customizados, deve-se ter permissão de visualização ou modificação para todos os aplicativos ou para um aplicativo individual.

Nota: Se um aplicativo for renomeado, as permissões não serão retidas; deve-se redesignar as permissões de visualização e modificação.

Visualizar

A permissão de visualização para um aplicativo é dominante sobre quaisquer outras permissões. Para visualizar um aplicativo, não é necessário ser membro de uma função que tenha permissão de visualização para cada componente e instância de componente dentro do aplicativo. A tabela a seguir

descreve as ações que podem ser executadas se você tiver permissão de visualização para um aplicativo:

Tabela 239. Permissão de visualização para um aplicativo

Ação	Permissão disponível
Visualizar todos os componentes de suporte nesse aplicativo.	✓
Visualizar o aplicativo e seus componentes na árvore de navegação.	✓
Visualize os componentes de aplicativo em Meus Componentes.	✓
Visualizar as páginas de painel customizadas que estejam associadas ao aplicativo.	✓
Incluir ou remover componentes do aplicativo.	—
Designar limites para os componentes dos aplicativos.	—
Visualizar os componentes de suporte de um aplicativo no Gerenciador de grupos de recursos.	—

Modificar

Se você for membro de uma função que tem permissão de modificação para um aplicativo individual, é possível

- Excluir o aplicativo.
- Crie páginas de painel customizadas na guia Visualizações customizadas. Consulte "Visualizações customizadas" na página 1112.
- Incluir ou remover componentes e instâncias de componentes usando a janela **Editar aplicativo**. Os componentes e as instâncias dos componentes disponíveis na janela **Editar aplicativo** são filtrados com base en suas permissões de função. Os seguintes componentes estarão disponíveis:
  - Componentes aos quais você possui permissão direta para acessar nos grupos de recursos do sistema e grupo de recurso customizado
  - Componentes dos quais você herdou permissões indiretamente, com base em outros aplicativos para os quais você tem permissão para modificar

Permissões de grupo de recursos

Use Grupos de recursos para agrupar componentes por seu tipo ou propósito. Para obter mais informações sobre como criar grupos de recursos, consulte "Gerenciador de Grupos de Recursos" na página 980.

Para selecionar **Configuração do sistema** > **Gerenciador de Grupo de Recursos**, deve-se estar designado à permissão de visualização do Gerenciador de Grupo de Recursos. Para visualizar os grupos de recursos no **Gerenciador de Grupo de Recursos** ou para visualizar membros do grupo de recursos no aplicativo **Meus Componentes**, deve-se também estar designado à permissão de visualização ou modificação para todos os grupos de recursos ou para grupos de recursos individuais.

Há dois tipos diferentes de grupos de recursos: grupos de recursos customizados e grupos de recursos do sistema.

Grupos de recursos definidos customizados

Crie grupos de recursos customizados no Gerenciador de grupos de recursos. Use grupos de recursos customizados para agrupar recursos com base em seu propósito.

A tabela a seguir descreve as ações que podem ser executadas se você tiver a permissão de visualização para um grupo de recursos customizados:

Tabela 240. Permissão de visualização para um grupo de recursos customizados

Ação	Permissão disponível
Visualizar o grupo de recursos customizados e os recursos nele no Gerenciador de Grupo de Recursos.	✓
Visualizar recursos que fazem parte do grupo de recursos customizados na janela **Incluir aplicativo** se você também tiver permissão de modificação para aplicativos.	✓
Visualizar recursos que fazem parte do grupo de recursos customizados no aplicativo predefinido **Meus Componentes**, se você também tiver uma das permissões do Application Performance Dashboard.	✓
Incluir recursos no grupo de recursos customizados.	–
Excluir recursos do grupo de recursos customizados.	–

A tabela a seguir descreve as ações que você pode executar se tiver a permissão de modificação para um grupo de recursos customizados:

Tabela 241. Permissão de modificação para um grupo de recursos customizados

Ação	Permissão disponível
Designar limites para o grupo de recursos customizados no Editor de Limite. **Nota:** Para designar limites, também é necessário ser um membro de uma função que tenha permissão de visualização para Editor de Limite.	✓
Incluir recursos no grupo de recursos customizados.	✓
Excluir recursos do grupo de recursos customizados.	✓

Grupos de recursos do sistema

Grupos de recursos do sistema são definidos automaticamente como parte de sua configuração de ambiente do Cloud APM. Grupos de recursos do sistema não podem ser criados, excluídos ou customizados manualmente. Somente a permissão de visualização está disponível para grupos de recursos do sistema, a permissão de modificação não está disponível.

Grupos de recursos do sistema são definidos para cada tipo de recurso no momento em que o recurso torna-se conhecido para o Servidor Cloud APM. Um grupo de recursos do sistema existe para cada tipo de recurso que está conectado ao Servidor Cloud APM.

Agentes do Cloud APM são um exemplo de um recurso. Por exemplo, a primeira vez que você fizer download, instalar e iniciar um agente Db2, será criado um grupo de recursos do sistema chamado Db2. Este grupo contém todos os agentes Db2 que serão incluídos subsequentemente no ambiente do Performance Management.

O grupo de recursos do sistema para cada tipo de recurso contém todos os recursos desse tipo, incluindo recursos do IBM Tivoli Monitoring. Se seu ambiente tiver IBM Tivoli Monitoring e IBM Cloud Application Performance Management, será possível instalar o IBM Cloud Application Performance Management Hybrid Gateway para fornecer uma visualização de agentes de ambos os domínios. Os grupos de recursos definidos pelo sistema contêm agentes de ambos os domínios. Para obter mais informações, consulte “Integrando com o IBM Tivoli Monitoring V6.3 ” na página 949.

Alguns grupos de recursos do sistema são baseados em agentes de subnó. Embora seja possível designar limites para grupos de recursos do sistema que são baseados em agentes de subnó, os eventos não são exibidos no Application Performance Dashboard. Limites são designados a grupos de recursos do sistema com base em agentes de subnó para encaminhamento de eventos. Os grupos de recursos do sistema com base em agentes de subnó possuem a descrição a seguir no Gerenciador de Grupo de Recursos: 'membros deste grupo não podem ser incluídos em um aplicativo e não têm eventos exibidos no console do Performance Management'. Para obter mais informações, consulte “Gerenciador de Grupos de Recursos” na página 980.

A tabela a seguir descreve as ações que podem ser executadas se você tiver permissão de visualização para um grupo de recursos do sistema:

Tabela 242. Permissão de visualização para um grupo de recursos do sistema

Ação	**Permissão disponível**
Visualizar o grupo de recursos do sistema no Gerenciador de Grupo de Recursos.	✓
Visualizar os recursos que fazem parte do grupo de recursos do sistema na janela **Incluir aplicativo** se você também tiver permissão de modificação para aplicativos.	✓
Visualizar recursos que fazem parte do grupo de recursos do sistema no aplicativo predefinido **Meus Componentes**, se você também tiver uma das permissões do Application Performance Dashboard.	✓
Designar limites para o grupo de recursos do sistema no Editor de Limite.	✓
Incluir recursos no grupo de recursos do sistema.	–
Excluir recursos do grupo de recursos do sistema.	–

Trabalhando com funções, usuários e permissões
Use a página Controle de Acesso Baseado na Função para trabalhar com funções, usuários e permissões.

Antes de Iniciar
Como alternativa, use a API de Autorização para concluir tarefas de controle de acesso baseado na função a partir da linha de comandos. Para obter informações adicionais, consulte “Explorando as APIs” na página 1072.

Nota: Grupos de usuários não são suportados no Cloud APM.

Procedimento

- Para filtrar a lista de funções, usuários ou grupos de usuários mostrados na página Controle de acesso baseado na função, conclua as seguintes etapas:

  a) Selecione **Configuração do Sistema> Controle de Acesso Baseado na Função**.

b) Clique dentro da caixa de texto  **Filtrar** e digite o texto parcial ou completo para a filtragem.

Durante a digitação, as linhas que não contêm o que foi digitado na caixa de filtro são removidas da tabela.

c) Para remover o filtro rápido, exclua os valores ou clique no "x".

d) Para aplicar o filtro, clique em  .

- Para criar uma nova função customizada, execute as seguintes etapas:

  a) Selecione **Configuração do Sistema > Controle de Acesso Baseado na Função**.

  b) Na guia **Funções**, clique em  . A página **Editor de Função** é exibida.

  c) Na guia **Designar Usuários para Funções**, selecione a guia **Grupos de Usuários** ou a guia **Usuários Individuais** e selecione os usuários e grupos de usuários a serem incluídos na função.

  d) Na guia **Designar Permissões para Funções**, selecione a guia **Permissões de Configuração do Sistema** ou a guia **Permissões de Recursos** e selecione as permissões a serem designadas para a função.

  e) Clique em **Salvar**.

- Para editar uma função padrão existente ou uma função customizada, execute as seguintes etapas:

  a) Selecione **Configuração do Sistema > Controle de Acesso Baseado na Função**.

  b) Na guia **Funções**, clique em  . A página **Editor de Função** é exibida.

  c) Na guia **Designar Usuários para Funções**, clique na guia **Grupos de Usuários** ou na guia **Usuários Individuais** e selecione os usuários ou grupos de usuários a serem incluídos na função.

  d) Na guia **Designar Permissões para Funções**, selecione a guia **Permissões de Configuração do Sistema** ou a guia **Permissões de Recursos** e selecione as permissões a serem designadas para a função.

  e) Clique em **Salvar**.

- Para excluir uma função, execute as seguintes etapas:

  a) Selecione **Configuração do Sistema > Controle de Acesso Baseado na Função**.

  b) Na guia **Funções**, selecione a função a ser excluída e clique em  . É exibida uma mensagem de confirmação; clique em **OK**.

  Nota: Ao excluir uma função, os usuários que são membros dessa função não são excluídos. Eles ainda ficam disponíveis na guia **Usuários Individuais** e um Administrador de Funções pode designá-los para outra função.

- Para editar as permissões de um usuário individual ou de um grupo de usuários, execute as seguintes etapas:

  a) Selecione **Configuração do Sistema > Controle de Acesso Baseado na Função**.

  b) Na guia **Usuário Individual** ou na guia **Grupos de Usuários**, selecione o usuário ou grupo de usuários a ser editado e clique em  . A página **Editor de Usuário Individual** é aberta.

  c) Selecione as funções a serem designadas para o usuário.

  d) Clique em **Salvar**.

- Para criar um arquivo csv que resuma as permissões para um usuário ou grupo de usuários, execute as seguintes etapas:

  a) Na guia **Usuário Individual** ou na guia **Grupos de Usuários**, selecione o usuário ou grupo de usuários necessário e clique em  . A página **Editor de Usuário Individual** ou **Editor de Grupo de Usuários** é aberta.

  b) Clique em **Exportar Resumo**.

  c) Selecione **Salvar Arquivo**, clique em **OK**.

Um arquivo csv, resumindo a permissão para o usuário ou grupo de usuários, é salvo no local especificado.

Resultados

Ao clicar em **Salvar**, a designação de funções e permissões entra em vigor imediatamente.

Acessando e usando a API de Serviço de Controle de Acesso Baseado na Função

Use a API de Serviço de Controle de Acesso Baseado na Função para gerenciar o ciclo de vida de políticas de controle de acesso baseado na função a partir da linha de comandos.

Sobre Esta Tarefa

Conclua as tarefas de acesso baseado em função, como criar, visualizar, atualizar e excluir funções. Inclua e exclua um conjunto de usuários ou grupos de usuários de uma função específica. Conceda permissões a uma função específica. Visualize uma lista de funções, usuários, grupos de usuários e permissões que são definidos no sistema.

É possível criar scripts para automatizar tarefas, como definir novas funções e designar usuários, grupos de usuários e permissões a essas funções.

Procedimento

1. Conclua a etapa 1 até a etapa 9 no tópico Explorando as APIs.

   A Etapa 10 e a Etapa 11 fornecem detalhes adicionais.
2. Clique em **USAR** e selecione uma chave, por exemplo, **Key1**.

   Nota: Clique em **Ocultar** para mostrar seu ID e seu segredo do cliente. Anote-os, já que eles serão necessários se você estiver fazendo chamadas da API com ferramentas externas fora do API Explorer. Em seguida, clique em **Mostrar** para ocultá-los.
3. Preencha todos os cabeçalhos necessários, indicados com um asterisco.

   X-IBM-Service-Location
   * cabeçalho é a localização geográfica de sua assinatura, como na para América do Norte

   Autorização
   * o cabeçalho é sua sequência codificada em base64 do IBMid e senha. Ao codificar o IBMid e a senha na ferramenta based64-encoder, o formato deverá ser *IBMid:password*, por exemplo, `Basic YXBtYWRtaW46YXBtcGFzcw==!`.
4. Deve-se incluir um cabeçalho referente em todas as solicitações de POST, PUT e DELETE. O valor para o cabeçalho Referer é:

   ```
   -H 'Referer: https://api.ibm.com'
   ```
5. Role para localizar e clique em **Testar**.

Exemplo

O exemplo a seguir usa o comando curl para criar uma nova função.

```
POST /1.0/authzn/roles
```

Nota: O corpo da solicitação POST deve conter um objeto JSON que defina a função, conforme mostrado pelo parâmetro **-d**.

```
curl -X POST \
  https://api.ibm.com/perfmgmt/run/1.0/authzn/roles  \
  -H 'Referer: https://api.ibm.com' \
  -H 'authorization: Basic REPLACE_BASE64_ENCODED_STRING' \
  -H 'content-type: application/json' \
  -H 'x-ibm-client-id: REPLACE_KEY_VALUE' \
  -H 'x-ibm-client-secret: REPLACE_KEY_VALUE' \
  -d '{
```

```
    "description": "Your Role Description",
    "id": "/authzn/roles/Your_Role_Id",
    "label": "Your Role Name"
}'
```

Administrando seus agentes

Sua instalação do IBM Cloud Application Performance Management tem ferramentas para gerenciar seus agentes de monitoramento.

Algumas dessas ferramentas também são usadas durante a configuração inicial de seus sistemas gerenciados: “Utilizando comandos do agente” na página 175, “Página Configuração do Agente” na página 180 e “Usando a janela IBM Cloud Application Performance Management em sistemas Windows” na página 180.

Iniciando agentes como um usuário não raiz

Se você deseja iniciar agentes como usuários diferentes, crie um grupo comum no sistema e torne cada usuário um membro desse grupo.

Antes de Iniciar

Se você instalou e configurou o agente como o mesmo usuário não raiz e deseja iniciar o agente como o mesmo usuário, nenhuma ação especial será necessária. Se você instalou e configurou seu agente como um usuário selecionado e deseja iniciar o agente como um usuário diferente, crie um grupo comum no sistema. Torne todos os usuários do gerenciamento de agente membros deste grupo comum. Transfira a propriedade de todos os arquivos e diretórios do agente para esse grupo.

Sobre Esta Tarefa

Um script de autoinicialização é gerado por uma instalação, upgrade ou configuração. Esse script (denominado `ITMAgentsN` ou `rc.itmN`, dependendo do sistema operacional UNIX) contém uma entrada para cada aplicativo de uma instalação específica. Por padrão, todos os agentes são iniciados com acesso de usuário raiz. Para atualizar scripts de inicialização do sistema e iniciar agentes como um usuário não raiz, deve-se editar o arquivo `install_dir/config/kcirunas.cfg`, que contém um superconjunto da sintaxe XML. Cada seção **`productCode`** no arquivo `kcirunas.cfg` está desativada por padrão. Ative uma seção **`productCode`** para o seu agente, removendo o indicador de comentário de **`!productCode`**. As seções comentadas ou desativadas são ignoradas. As seções não comentadas ou ativadas para aplicativos que não estão instalados são ignoradas.

Procedimento

1. Instale seus agentes de monitoramento no Linux ou UNIX, conforme descrito no “Instalando agentes” na página 122 em sistemas AIX ou no “Instalando agentes” na página 130 em sistemas Linux.
2. Opcional: Configure seus agentes de monitoramento no Linux ou UNIX conforme necessário; consulte Capítulo 7, “Configurando seu Ambiente”, na página 157.
3. Execute o script `./secure.sh` com o nome do grupo do usuário não raiz para proteger os arquivos e configure a propriedade do grupo de arquivos para os arquivos.
   Por exemplo: **`./secure.sh -g db2iadm1`**
4. Para atualizar os scripts de inicialização do sistema, conclua as etapas a seguir:
   a) Atualize o arquivo `install_dir/config/kcirunas.cfg`. Ative as seções **`productCode`** para seus agentes. Para agentes que não requerem um valor de instância, especifique product_code, instância e usuário, em que o valor de *product_code* é o código de duas letras especificado no Tabela 11 na página 175. Para agentes que requerem um valor de instância, como o agente de monitoramento do Db2 (código do produto: ud), especifique o product_code, instância, usuário e nome.
   Por exemplo:

```
<productCode>ud</productCode>
<instance>
<name>db2inst1</name>
<user>db2inst1</user>
</instance>
<instance>
<name>db2inst2</name>
<user>root</user>
</instance>
```

b) Execute o script a seguir com acesso de usuário raiz ou de usuário sudo: *install_dir*/bin/UpdateAutoRun.sh

O que Fazer Depois

Para obter mais informações sobre o script **./secure.sh**, consulte Protegendo os arquivos de instalação do agente.

Use o mesmo ID de usuário para a instalação e os upgrades do agente.

Limites de evento para Monitoramento de transação

É possível usar os limites de evento para monitorar imediatamente seu ambiente. Também é possível criar limites de evento customizados que testam certas condições e levantam um evento quando os principais indicadores de desempenho excedem o limite.

Eventos do Response Time Monitoring

Eventos de Tempo de Resposta são criados quando transações da web excedem um limite de **Tempo de Resposta**.

Após clicar em **Configuração do Sistema** > **Gerenciador de Limite**, selecione **Tempo de Resposta** como o **Tipo de Origem de Dados**. Todos os limites de evento para o ambiente Response Time Monitoring são aplicados a todos os sistemas gerenciados do mesmo tipo.

Os seguintes limites predefinidos estão disponíveis para o Agente de Monitoramento de tempo de resposta.

Tabela 243. Limites do Response Time Monitoring

Limite	Descrição	Fórmula
Response_Time_Availability_Crit	Uma porcentagem alta de transações da web falhou.	Se o WRT Transaction Status.Percent_Failed for maior que 10 e o WRT Transaction Status.Transaction_Definition_Name não for igual a 'Ignorar Recursos', então Response_Time_Availability_Crit será verdadeiro
Response_Time_Availability_Warn	Uma porcentagem moderada de transações da web falhou.	Se WRT Transaction Status.Percent_Failed for maior que 0, WRT Transaction Status.Percent_Failed for menor que 10 e WRT Transaction Status.Transaction_Definition_Name não for igual a 'Ignorar Recursos', então Response_Time_Availability_Warn será verdadeiro

Tabela 243. Limites do Response Time Monitoring (continuação)		
Limite	**Descrição**	**Fórmula**
`Response_Time_Critical`	A porcentagem das transações da web com um tempo de resposta lento é alta.	Se WRT Transaction Status.Percent_Slow for maior que 5, WRT Transaction Status.Percent_Available for igual a 100 e WRT Transaction Status.Transaction_Definition_Name não for igual a 'Ignorar Recursos', entãoResponse_Time_Critical será true
`Response_Time_Warning`	A porcentagem das transações da web com um tempo de resposta lento é moderada.	Se WRT Transaction Status.Percent_Slow for maior que 1, WRT Transaction Status.Percent_Slow for menor que 5, WRT Transaction Status.Percent_Available for igual a 100 e WRT Transaction Status.Transaction_Definition_Name não for igual a 'Ignorar Recursos', então Response_Time_Warning será true

Boas solicitações têm um tempo de resposta menor que 10 segundos. *Solicitações lentas* têm um tempo de resposta maior que 10 segundos. O valor de 10 segundos usado para determinar o tempo de resposta bom vs lento não é configurável.

Eventos do Rastreamento de Transação

Eventos do Rastreamento de Transação são criados quando transações da middleware excedem um limite de Rastreamento de Transação.

Para visualizar limites padrão do Rastreamento de Transação, clique em **Configuração do Sistema** > **Gerenciador de Limite** e selecione **Rastreamento de Transação** como o **Tipo de Origem de Dados**.

Dica: É possível criar seus próprios limites do Rastreamento de Transação se necessário.

Os seguintes limites predefinidos estão disponíveis para transações de middleware.

Tabela 244. Limites do Rastreamento de Transação		
Limite	**Descrição**	**Fórmula**
`Interaction_Avail_Critical`	Uma porcentagem alta das interações de middleware falhou.	Se KTE INTERACTION AGGREGATE DATA.PERCENTAGE_FAILED for maior que 10, Interaction_Avail_Critical será true
`Interaction_Avail_Warning`	Uma porcentagem moderada de interações de middleware falhou.	Se KTE INTERACTION AGGREGATE DATA.PERCENTAGE_FAILED for maior que 0 e KTE INTERACTION AGGREGATE DATA.PERCENTAGE_FAILED for menor ou igual a 10, `Interaction_Avail_Warning` será true

Tabela 244. Limites do Rastreamento de Transação (continuação)

Limite	Descrição	Fórmula
`Interaction_Time_Critical`	A porcentagem de interações de middleware com um tempo total lento é alta.	Se KTE INTERACTION AGGREGATE DATA.PERCENTAGE_SLOW for maior ou igual a 5 e KTE INTERACTION AGGREGATE DATA.PERCENTAGE_FAILED for igual a 0, Interaction_Time_Critical será true
`Interaction_Time_Warning`	A porcentagem de interações de middleware com um tempo total lento é moderada.	Se KTE INTERACTION AGGREGATE DATA.PERCENTAGE_SLOW for maior que 1 e KTE INTERACTION AGGREGATE DATA.PERCENTAGE_SLOW for menor que 5 e KTE INTERACTION AGGREGATE DATA.PERCENTAGE_FAILED for igual a 0, Interaction_Time_Warning será true
`Transaction_Avail_Critical`	Uma porcentagem alta das transações de middleware falhou.	Se KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_FAILED for maior que 10, Transaction_Avail_Critical será true
`Transaction_Avail_Warning`	Uma porcentagem moderada de transações de middleware falhou.	Se KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_FAILED for maior do que 0 e KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_FAILED for menor ou igual a 10, `Transaction_Avail_Warning` será true
`Transaction_Time_Critical`	A porcentagem das transações de middleware com um tempo total lento é alta.	Se KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_SLOW é maior ou igual a 5 e KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_FAILED é igual a 0, Transaction_Time_Critical é true
`Transaction_Time_Warning`	A porcentagem das transações de middleware com um tempo total lento é moderada.	Se KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_SLOW é maior que 1 e KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_SLOW é menor que 5 e KTE TRANSACTION AGGREGATE DATA.PERCENTAGE_FAILED é igual a 0, Transaction_Time_Warning é true

Boas solicitações têm um tempo de resposta menor que 10 segundos. *Solicitações lentas* têm um tempo de resposta maior que 10 segundos. O valor de 10 segundos usado para determinar o tempo de resposta bom vs lento não é configurável.

Criando limites para gerar eventos para o monitoramento de transações
Use o Gerenciador de Limite para criar limites para transações. Os limites são usados para comparar o valor de amostra de um atributo com o valor definido no limite. Caso o valor de amostra satisfaça a comparação, um evento de transação será gerado.

Sobre Esta Tarefa

É possível monitorar quando os aplicativos relatam condições específicas usando limites. Para obter mais informações sobre os limites padrão para Monitoramento de Transação, consulte "Limites de evento para Monitoramento de transação " na página 1013.

É possível criar limites extras para monitorar outros aspectos de uma transação. Por exemplo, você pode criar um limite para monitorar se a taxa de eventos de transação de middleware cai. Em seguida, se a taxa de evento de transação cai abaixo do especificado por seu limite, um evento é gerado.

Procedimento

Para criar um limite e associá-lo a uma ou mais transações, execute as tarefas a seguir:

1. Na Barra de Navegação, clique no ícone **Configuração do Sistema** > **Gerenciador de Limite**. Configure o **Tipo de Origem de Dados** como **Rastreamento de Transação**.
2. Clique em Incluir para criar um novo limite.
3. Configure uma gravidade para o evento que excede esse limite.
4. Para associar o limite a uma transação, configure os valores a seguir:
   - Conjunto de dados - `KTE TRANSACTION AGGREGATE DATA`
   - Item de exibição - `Resource_Value`
   - Operador lógico - `And (&)`
5. Como alternativa, para associar o limite com uma interação, configure os seguintes valores:
   - Conjunto de dados - `KTE INTERACTION AGGREGATE DATA`
   - Item de exibição - `Source_Resource_Value`
   - Operador lógico - `And (&)`
6. Clique em **Incluir** para incluir uma condição. Na caixa **Incluir Condição**, selecione um atributo e um operador e insira um valor.

   Por exemplo, para incluir uma condição de limite que gere um evento de transação quando o número de transações por minuto estiver abaixo de 100, configure os valores a seguir e clique em **OK**:
   - Atributo - `Transaction_Rate`
   - Operador - `Less than`
   - Valor - `100`

   Repita esta etapa para incluir mais condições em seu limite, se necessário.
7. Na seção Designação do Grupo, selecione `Rastreamento de Transação` para designar o seu limite para esse grupo de recursos.
8. Clique em **Salvar**.

Resultados

Você criou um limite e o associou a uma transação ou interação. Quando as condições de limite são atendidas, um evento é gerado. É possível monitorar a guia Eventos do Painel de Desempenho do Aplicativo.

Exemplo

Para criar limites para o agente do Response Time Monitoring para monitorar outros aspectos de uma transação da web além dos padrões:

1. No Gerenciador de Limite, configure o **Tipo de Origem de Dados** como **Tempo de Resposta**.
2. Ao incluir o limite, use as configurações a seguir:
   - Conjunto de dados - `Status da Transação do WRT`
   - Item de exibição - `Aplicativo`
   - Operador lógico - `And (&)`
   - Designação de grupo - `Tempo de Resposta da Web`

Gerenciando eventos do OS Agent

É possível configurar o OS Agent para gerenciar eventos.

Filtro de eventos e resumo

Use as opções filtragem de evento e sumarização definidas no arquivo de configuração (`.conf`) para controlar como eventos duplicados serão tratados pelo OS Agent.

Quando um log é monitorado, um evento pode ser exibido diversas vezes rapidamente. Por exemplo, essa criação de log de repetição pode ocorrer quando o aplicativo que produz o log encontra um erro e registra esse erro continuamente até que o limite seja resolvido. Quando esse tipo de criação de log ocorre, um número excessivo de eventos é enviado para a infraestrutura do Performance Management. O volume de eventos tem um impacto negativo no desempenho.

Nota: Os procedimentos de detecção de eventos e sumarização são suportados somente para agentes enviados para o Performance Management. Não é possível concluir estes procedimentos em eventos que são enviados ao OMNIbus pelo EIF.

Detectando e Filtrando Eventos Duplicados

É possível configurar o OS Agent para manipular eventos duplicados.

Para amenizar o problema de vários eventos duplicados, defina o que constitui um evento duplicado usando a tag `DupDetectionKeyAttributes` no arquivo `.conf`. Em uma lista separada por vírgula, você inclui um ou mais atributos do Performance Management definidos que você deseja usar para determinar se um evento é considerado duplicado. No exemplo a seguir, eventos com a mesma mensagem e o mesmo `CustomSlot1` devem ser considerados duplicatas:

```
DupDetectionKeyAttributes=msg,CustomSlot1
```

Eventos duplicados são detectados a partir de atributos do Performance Management. Portanto, se desejar que a detecção de duplicatas seja baseada em slots específicos que você definiu, conclua as etapas a seguir:

1. Mapeie o valor do slot para um atributo do Performance Management.
2. Mapeie o atributo do Performance Management para a tag `DupDetectionKeyAttributes` no arquivo `.conf`.

Usando o exemplo a seguir, no qual os slots importantes, `eventclass` e `eventid`, são mapeados para *CustomSlot1* e *CustomSlot2*:

```
REGEX BaseAuditEvent
^([A-Z][a-z]{2} [0-9]{1,2} [0-9]{1,2}:[0-9]{2}:[0-9]{2}
 [0-9] {4}) [0-9] (\S+) (\S+) \
Microsoft-Windows-Security-Auditing (\S+) ([0-9]+) (.*)
timestamp $1
severity $2
eventclass $3 CustomSlot1
eventkeywords $4
eventid $5 CustomSlot2
msg $6
END
```

se desejar especificar certos eventos como duplicados, no arquivo `.conf`, mapeie os atributos do Performance Management para a tag `DupDetectionKeyAttributes`, conforme mostrado aqui:

```
DupDetectionKeyAttributes=CustomSlot1,CustomSlot2
```

Nota:

1. Os nomes do atributo `CustomSlot` fazem distinção entre maiúsculas e minúsculas e, portanto, você deve inserir os nomes exatamente conforme mostrado no exemplo precedente.
2. Se você não fornecer uma lista de atributos, os valores serão padronizados como `Class` e `Logname`.

Os eventos nos quais estes atributos correspondem são considerados como sendo eventos duplicados pelo agente.

Como a detecção de duplicata é global, é uma boa prática escolher um conjunto de slots customizados para usar como chaves e usá-los desta maneira em todas as instruções de formato. Por exemplo, use os slots 1 - 3 para chaves. Se um formato precisar apenas de uma chave, mas também precisar de mais slots, use o slot um para conter o valor de nome e os slots quatro a n para conter os outros dados.

Intervalo de Resumo
O procedimento de detecção de duplicação opera durante um período de tempo que é conhecido como Intervalo de resumo.

Eventos duplicados são contados durante este intervalo e, em seguida, reconfigurados quando o intervalo expira. O contador inicia a contagem novamente iniciando em 0 no início de cada novo intervalo de resumo.

O agente envia um evento de resumo para cada evento configurado que ele monitora durante o intervalo. O evento de resumo contém os valores de atributos do primeiro evento correspondido. O evento de resumo também contém uma contagem que indica quantas duplicatas desse evento ocorreram durante o intervalo de resumo.

O intervalo de resumo é configurado no arquivo de configuração (`.conf`) conforme mostrado no exemplo a seguir:

```
EventSummaryInterval=300
```

O valor que é designado ao intervalo de resumo está em segundos, portanto, neste exemplo, o intervalo de resumo é de 5 minutos.

Filtrando Eventos
Se a filtragem de eventos estiver em execução, a configuração EventFloodThreshold no arquivo (`.conf`) informará ao agente quando enviar um evento.

A tabela a seguir mostra os valores EventFloodThreshold.

Tabela 245. Valores de EventFloodThreshold

Valores de EventFloodThreshold	**Descrição**
send_all	O valor *send_all* é o valor padrão. Todos os eventos são enviados, mesmo se estes eventos são eventos duplicados.
send_none	O valor *send_none* significa que nenhum evento individual é enviado. Somente os eventos de resumo são enviados.

Tabela 245. Valores de EventFloodThreshold (continuação)	
Valores de EventFloodThreshold	**Descrição**
send_first	Use o valor *send_first* para enviar o primeiro evento assim que ele for encontrado. Se duplicatas desse primeiro evento ocorrerem dentro de um tempo especificado, duplicatas subsequentes deste primeiro evento não serão enviadas. Para obter mais informações, consulte "Intervalo de Resumo" na página 1018.
número inteiro *n*	Use o valor de número inteiro *n* para enviar apenas cada *n* ocorrência de um evento (por exemplo toda quinta duplicata) durante um tempo específico. Para obter mais informações, consulte "Intervalo de Resumo" na página 1018.

Atributos de Resumo
Os atributos Tipo de Evento e Contagem de Ocorrências são usados para ajudar a resumir eventos.

Quando o resumo de evento é ativado, os atributos Tipo de Evento e Contagem de Ocorrências se tornam significativos. O atributo Tipo de Evento indica o tipo do evento, sendo um *Evento* ou um *Evento de Resumo*. Eventos gerais que correspondem a registros localizados no log em uma base de um para um são identificados como *Evento*. Eventos de resumo que são enviados no final do Intervalo de Resumo, são identificados como *Evento de Resumo*.

O atributo Contagem de Ocorrências indica a quantidade total de registros duplicados localizados no log para o evento. Os eventos de resumo incluem esta contagem, pois ela mostra o número de eventos recebidos que corresponderam ao evento de resumo durante o intervalo de resumo anterior.

Eventos de Resumo e Limites

Independentemente do valor de filtro descrito no "Filtrando Eventos" na página 1018, você sempre obtém os eventos de resumo no final de cada intervalo de resumo, para qualquer evento ocorrido pelo menos uma vez durante esse intervalo. Se você não estiver esperando os eventos de resumo, seus limites poderão ser acionados acidentalmente. Para evitar esse acionamento acidental de um limite, inclua uma cláusula no limite para *`Tipo de Evento== Evento`* ou *`Tipo de Evento!= Evento de Resumo`*.

Log de Eventos do Windows
O agente de S.O. usa o arquivo .conf para monitorar eventos do Log de eventos do Windows.

O agente de S.O. continua usando a opção do arquivo (`.conf`) de configuração `WINEVENTLOGS` para monitorar eventos do Log de eventos do Windows. O agente monitora uma lista separada por vírgula de logs de eventos conforme mostrado no exemplo a seguir:

```
WINEVENTLOGS=System,Security,Application
```

O OS Agent também continua usando a configuração `WINEVENTLOGS=All`. A configuração `All` refere-se aos seguintes logs de eventos padrão: Segurança, Aplicativo, Sistema, Diretório, Sistema de Nomes de Domínio (DNS) e Serviço de Replicação de Arquivo (FRS) que são fornecidos com versões do Windows anteriores a 2008. No entanto, todos os logs de eventos no sistema não são verificados.

A tag do arquivo de configuração `UseNewEventLogAPI` permite que o log de eventos (Log de eventos do Windows 2008 ou mais recente) acesse todos os novos logs incluídos pela Microsoft, e todos os logs de eventos do Windows criados por outros aplicativos ou pelo usuário. Os novos logs são listados pela palavra-chave `WINEVENTLOGS`.

No exemplo a seguir, a tag `UseNewEventLogAPI` é configurada como `y`.

```
UseNewEventLogAPI=y
WINEVENTLOGS=Microsoft-Windows-Hyper-V-Worker-Admin
```

Neste exemplo, o `Microsoft-Windows-Hyper-V/Admin` é monitorado em um sistema Windows que possui a função Hyper-V.

No Log de eventos do Windows, cada evento tem os seguintes campos, nessa ordem:

- Data no seguinte formato: mês, dia, hora e ano
- Categoria de evento como um número inteiro
- Event Level
- ID de segurança do Windows. Quaisquer espaços no ID de segurança do Windows são substituídos por um sublinhado se `SpaceReplacement=TRUE` no arquivo (`.conf`) de configuração.

  Nota: `SpaceReplacement=TRUE` é o padrão se você configurar `UseNewEventLogAPI` para y no arquivo (`.conf`) (designando que você está usando o log de eventos).
- Origem do Windows. Quaisquer espaços na origem do Windows são substituídos por um sublinhado se `SpaceReplacement=TRUE` no arquivo (`.conf`) de configuração.
- Palavras-chave do log de eventos do Windows. Quaisquer espaços nas palavras-chave de log de eventos do Windows são substituídas por um sublinhado se `SpaceReplacement=TRUE` no arquivo (`.conf`) de configuração.

  Nota: O campo de palavras-chave descrito aqui é novo para a versão do Log de eventos do Windows 2008. Ele não existia no Log de eventos anterior, portanto, sua presença impede que você reutilize instruções de formato do Log de eventos anterior diretamente. Elas devem ser modificadas para considerarem esse campo adicional.
- Identificador de eventos do Windows
- Texto da Mensagem

Por exemplo, quando um usuário administrativo efetua logon em um sistema Windows 2008, um evento é gerado no log de Segurança indicando os privilégios que são designados à nova sessão do usuário:

```
Mar 22 13:58:35 2011 1 Information N/A Microsoft-Windows-
Security-Auditing Audit_Success 4672 Special privileges assigned to new logon.
S-1-5-21-586564200-1406810015-1408784414-500    Account Name:
Administrator   Account Domain:     MOLDOVA     Logon ID:
0xc39cb8e    Privileges:        SeSecurityPrivilege
SeBackupPrivilege          SeRestorePrivilege
SeTakeOwnershipPrivilege            SeDebugPrivilege
SeSystemEnvironmentPrivilege            SeLoadDriverPrivilege
SeImpersonatePrivilege
```

Para capturar todos os eventos que foram criados pela origem de eventos `Microsoft-Windows-Security-Auditing`, grave uma instrução de formato conforme mostrado aqui:

```
REGEX BaseAuditEvent
^([A-Z][a-z]{2} [0-9]{1,2} [0-9]{1,2}:[0-9]{2}:[0-9]{2} [0-9]
{4}) [0-9] (\S+) (\S+) Microsoft-Windows-Security-Auditing (\S+)
([0-9]+) (.*)
timestamp $1
severity $2
login $3
eventsource "Microsoft-Windows-Security-Auditing"
eventkeywords $4
eventid $5
msg $6
END
```

Para o evento de exemplo anterior, o exemplo a seguir indica os valores que são designados aos slots:

```
timestamp=Mar 22 13:58:35 2011
severity=Information
login=N/A
eventsource=Microsoft-Windows-Security-Auditing
eventid=4672
msg="Special privileges assigned to new logon.
S-1-5-21-586564200-1406810015-1408784414-500    Account Name:
Administrator   Account Domain:     MOLDOVA     Logon ID:
0xc39cb8e    Privileges:        SeSecurityPrivilege
SeBackupPrivilege          SeRestorePrivilege
```

```
SeTakeOwnershipPrivilege            SeDebugPrivilege
SeSystemEnvironmentPrivilege            SeLoadDriverPrivilege
SeImpersonatePrivilege
```

Como é difícil prever exatamente como serão esses eventos, uma abordagem útil para gravar suas expressões regulares é capturar os eventos reais em um arquivo. Em seguida, é possível examinar o arquivo, escolher os eventos que você deseja que o agente capture, e gravar expressões regulares para corresponderem a esses eventos. Para capturar todos os eventos do Log de eventos do Windows, use as seguintes etapas:

1. Crie um arquivo de formato que contenha apenas um padrão que não corresponda a nada, conforme mostrado no exemplo a seguir:

   ```
   REGEX NoMatch
   This doesn't match anything
   END
   ```

2. Inclua a configuração a seguir no arquivo (`.conf`) de configuração:

   ```
   UnmatchLog=C:/temp/evlog.unmatch
   ```

3. Execute o agente e capture alguns eventos de amostra.

Mapeamento de eventos

O Tivoli Event Integration Facility (EIF) interface é utilizada para encaminhar eventos de situação para Tivoli Netcool/OMNIbus, Tivoli Enterprise Console, ou Operations Analytics - Log Analysis .

Eventos EIF especificam uma classe de eventos e os dados do evento são especificados como pares nome-valor que identificam o nome de um slot de eventos e o valor do slot. Uma classe de eventos pode ter subclasses. O Performance Management fornece as definições da classe de evento de base e um conjunto de slots de base incluídos em todos os eventos de monitoramento. Os agentes ampliam as classes de evento base para definir subclasses que incluem intervalos específicos do agente. Para eventos do arquivo de log do agente do SO, as classes de eventos correspondem aos grupos de atributos do agente e os slots específicos do agente correspondem aos atributos no grupo de atributos.

Para eventos gerados por limites no grupo de atributos LFAProfiles, eventos são enviados usando a classe de eventos ITM_KLO_LFAPROFILES. Esta classe de eventos contém os seguintes slots:

- node: STRING
- timestamp: STRING
- subnode_msn: STRING
- subnode_affinity: STRING
- subnode_type: STRING
- subnode_resource_name: STRING
- subnode_version: STRING
- subnode_config_file: STRING
- subnode_description: STRING
- subnode_description_enum: STRING

Para eventos gerados por limites no grupo de atributos Estatísticas de Expressão Regular do Arquivo de Log, eventos são enviados usando a classe de eventos ITM_KLO_LOG_FILE_REGEX_STATISTICS. Esta classe de eventos contém os seguintes slots:

- node: STRING
- timestamp: STRING
- table_name: STRING
- attrib_name: STRING

- filter_number: INTEGER
- average_processor_time: REAL
- average_processor_time_enum: STRING
- total_processor_time: REAL
- total_processor_time_enum: STRING
- max_processor_time: REAL
- max_processor_time_enum: STRING
- min_processor_time: REAL
- min_processor_time_enum: STRING
- filter_count: REAL
- filter_count_matched: REAL
- filter_count_unmatched: REAL
- regex_pattern: STRING
- last_matched_time: STRING
- last_matched_time_enum: STRING
- last_unmatched_time: STRING
- last_unmatched_time_enum: STRING
- result_type: INTEGER
- result_type_enum: STRING

Para eventos gerados por limites no grupo de atributos Status do Arquivo de Log, eventos são enviados usando a classe de eventos ITM_KLO_LOG_FILE_STATUS. Esta classe de eventos contém os seguintes slots:

- node: STRING
- timestamp: STRING
- table_name: STRING
- file_name: STRING
- regex_pattern: STRING
- file_type: INTEGER
- file_type_enum: STRING
- file_status: INTEGER
- file_status_enum: STRING
- num_records_matched: INTEGER
- num_records_not_matched: INTEGER
- num_records_not_matched_enum: STRING
- num_records_processed: INTEGER
- current_file_position: REAL
- current_file_position_enum: STRING
- current_file_size: REAL
- current_file_size_enum: STRING

- last_modification_time: STRING
- last_modification_time_enum: STRING
- codepage: STRING

Para eventos gerados por limites no grupo de atributos LogfileEvents, eventos são enviados usando a classe de eventos ITM_KLO_LOGFILEEVENTS. Esta classe de eventos contém os seguintes slots:

- node: STRING
- timestamp: STRING
- klo_class: STRING
- logname: STRING
- eifevent: STRING
- klo_msg: STRING
- customslot1: STRING
- customslot2: STRING
- customslot3: STRING
- customslot4: STRING
- customslot5: STRING
- customslot6: STRING
- customslot7: STRING
- customslot8: STRING
- customslot9: STRING
- customslot10: STRING
- occurrence_count: INTEGER
- occurrence_count_enum: STRING
- event_type: INTEGER
- event_type_enum: STRING
- custominteger1: REAL
- custominteger1_enum: STRING
- custominteger2: REAL
- custominteger2_enum: STRING
- custominteger3: REAL
- custominteger3_enum: STRING
- remotehost: STRING

Para eventos gerados por limites no grupo de atributos LogfileProfileEvents, eventos são enviados usando a classe de eventos ITM_KLO_LOGFILEPROFILEEVENTS. Esta classe de eventos contém os seguintes slots:

- node: STRING
- timestamp: STRING
- klo_class: STRING
- logname: STRING
- eifevent: STRING

- klo_msg: STRING
- customslot1: STRING
- customslot2: STRING
- customslot3: STRING
- customslot4: STRING
- customslot5: STRING
- customslot6: STRING
- customslot7: STRING
- customslot8: STRING
- customslot9: STRING
- customslot10: STRING
- occurrence_count: INTEGER
- occurrence_count_enum: STRING
- event_type: INTEGER
- event_type_enum: STRING
- custominteger1: REAL
- custominteger1_enum: STRING
- custominteger2: REAL
- custominteger2_enum: STRING
- custominteger3: REAL
- custominteger3_enum: STRING
- remotehost: STRING

Para eventos gerados por limites no grupo de atributos Status do Objeto de Desempenho, eventos são enviados usando a classe de eventos ITM_KLO_PERFORMANCE_OBJECT_STATUS. Esta classe de eventos contém os seguintes slots:

- node: STRING
- timestamp: STRING
- query_name: STRING
- object_name: STRING
- object_type: INTEGER
- object_type_enum: STRING
- object_status: INTEGER
- object_status_enum: STRING
- error_code: INTEGER
- error_code_enum: STRING
- last_collection_start: STRING
- last_collection_start_enum: STRING
- last_collection_finished: STRING
- last_collection_finished_enum: STRING

- last_collection_duration: REAL
- average_collection_duration: REAL
- average_collection_duration_enum: STRING
- refresh_interval: INTEGER
- number_of_collections: INTEGER
- cache_hits: INTEGER
- cache_misses: INTEGER
- cache_hit_percent: REAL
- intervals_skipped: INTEGER

Para eventos gerados por limites no grupo de atributos pró Status do Objeto de Desempenho, eventos são enviados usando a classe de eventos ITM_KLO_PRO_PERFORMANCE_OBJECT_STATUS. Esta classe de eventos contém os seguintes slots:

- node: STRING
- timestamp: STRING
- query_name: STRING
- object_name: STRING
- object_type: INTEGER
- object_type_enum: STRING
- object_status: INTEGER
- object_status_enum: STRING
- error_code: INTEGER
- error_code_enum: STRING
- last_collection_start: STRING
- last_collection_start_enum: STRING
- last_collection_finished: STRING
- last_collection_finished_enum: STRING
- last_collection_duration: REAL
- average_collection_duration: REAL
- average_collection_duration_enum: STRING
- refresh_interval: INTEGER
- number_of_collections: INTEGER
- cache_hits: INTEGER
- cache_misses: INTEGER
- cache_hit_percent: REAL
- intervals_skipped: INTEGER

Para eventos gerados por limites no grupo de atributos Status do Conjunto de Encadeamentos, eventos são enviados usando a classe de eventos ITM_KLO_THREAD_POOL_STATUS. Esta classe de eventos contém os seguintes slots:

- node: STRING
- timestamp: STRING

- thread_pool_size: INTEGER
- thread_pool_size_enum: STRING
- thread_pool_max_size: INTEGER
- thread_pool_max_size_enum: STRING
- thread_pool_active_threads: INTEGER
- thread_pool_active_threads_enum: STRING
- thread_pool_avg_active_threads: REAL
- thread_pool_avg_active_threads_enum: STRING
- thread_pool_min_active_threads: INTEGER
- thread_pool_min_active_threads_enum: STRING
- thread_pool_max_active_threads: INTEGER
- thread_pool_max_active_threads_enum: STRING
- thread_pool_queue_length: INTEGER
- thread_pool_queue_length_enum: STRING
- thread_pool_avg_queue_length: REAL
- thread_pool_avg_queue_length_enum: STRING
- thread_pool_min_queue_length: INTEGER
- thread_pool_min_queue_length_enum: STRING
- thread_pool_max_queue_length: INTEGER
- thread_pool_max_queue_length_enum: STRING
- thread_pool_avg_job_wait: REAL
- thread_pool_avg_job_wait_enum: STRING
- thread_pool_total_jobs: INTEGER
- thread_pool_total_jobs_enum: STRING

Gerenciando transações e eventos sintéticos com o Website Monitoring

Crie transações sintéticas que monitoram o desempenho e a disponibilidade de aplicativos internos, aplicativos externos e aplicativos da web públicos em locais diferentes.

Crie uma *transação sintética* no Gerenciador de Script Sintético. Gere scripts simples no Synthetic Script Manager para testar a disponibilidade de um aplicativo, ou use o Selenium IDE para registrar scripts sintéticos que replicam diferentes ações do usuário com um aplicativo. Em seguida, configure uma transação sintética para reproduzir o script em intervalos e locais de reprodução específicos.

Importante: Somente os usuários existentes do complemento do IBM Website Monitoring on Cloud podem usar o Synthetic Playback agent e o Synthetic Script Manager. O Website Monitoring foi substituído pelo IBM Cloud Availability Monitoring para a liberação de agosto de 2017. Para obter mais informações, consulte “Sobre o Monitoramento de Disponibilidade” na página 1045.

Os seus locais de reprodução disponíveis são os locais onde você instalou o Monitoring Agent for Synthetic Playback e os 15 pontos de presença (PoPs) que são fornecidos para monitoramento de aplicativos da web voltados para o público. Os PoPs estão disponíveis para os locais a seguir:

- Amsterdam
- Chennai
- Dallas
- Frankfurt

- Hong Kong
- London
- Melbourne
- México
- Paris
- São José
- São Paulo
- Cingapura
- Tokyo
- Toronto
- Washington

Crie limites e grupos de recursos para gerar eventos e notificar as partes interessadas quando os aplicativos estiverem lentos ou indisponíveis. Visualize dados de desempenho e gere relatórios de histórico no Application Performance Dashboard.

Se você monitorar o tempo de resposta do usuário final para um aplicativo com o agente do Tempo de Resposta. será possível visualizar KPIs para transações de usuário final e sintéticas no Application Performance Dashboard. Inclua transações sintéticas como componentes no aplicativo que você está monitorando com o agente do Tempo de Resposta.

Nota: Para trabalhar no Gerenciador de Script Sintético, deve-se ser um membro de uma função que tenha permissão de visualização para o Gerenciador de Script Sintético e Configuração do Agente. Para obter mais informações, consulte “Funções e permissões” na página 1002.

Registrando scripts sintéticos

Registre um script sintético usando o navegador da web Firefox e o complemento do Selenium IDE.Com o Selenium IDE, é possível registrar ações do usuário em uma página da web, como carregamento de uma página, clique em um link ou seleção de um objeto. Quando o Selenium IDE está gravando, ele gera um comando para cada ação do usuário em um script. Em seguida, usando o Gerenciador de Script Sintético, é possível configurar scripts para simular o comportamento do usuário no website, em intervalos configurados e em diferentes locais.

Antes de Iniciar

Deve-se usar o navegador da web Firefox ao registrar scripts

O Selenium IDE está disponível somente como um complemento do Firefox. Se o Selenium IDE não estiver instalado ou em execução, conclua as seguintes etapas:

1. Assegure-se de estar executando uma versão do Firefox 60 ou posterior que suporte Selenium IDE 3.2.X ou 3.3.X. Se você tiver uma versão mais recente do Selenium IDE, ela não será suportada; é preciso desinstalar e instalar a versão 3.2.X ou 3.3.X.

   Nota: Por padrão, o Selenium IDE é atualizado automaticamente após a instalação da versão 3.2.X ou 3.3.X. Desative atualizações automáticas para o Selenium IDE para evitar upgrades de versão.
2. Faça download e instale o Selenium IDE 3.2.X ou 3.3.X a partir da página inicial do **Selenium** (https://addons.mozilla.org/firefox/addon/selenium-ide/versions/). Permita que o Selenium IDE instale todos os plug-ins.
3. Após o Selenium IDE ser instalado, reinicie o Firefox.
4. Navegue para a página da web que você deseja testar e feche todas as outras guias. Para abrir o Selenium IDE, clique em **Ferramentas** > **Selenium IDE**. Na janela **Selenium IDE**, assegure que o campo **URL Base** contenha a URL da página da web exibida. O Selenium IDE começa a registrar todas as ações do usuário na página da web exibida.

Formato de script .side do Selenium

Os scripts criados com versões mais recentes do Selenium usam o formato `..side`. Com o Selenium IDE 3.2.X ou 3.3.X, é possível importar scripts mais antigos que foram criados com o formato `.html` e salvar no formato `.side`. Para obter mais informações, consulte "Atualizando scripts de versões anteriores do Selenium IDE" na página 1031.

Se você estiver usando scripts do Selenium `.side`, primeiro será necessário desinstalar essas atualizações:

- IBM Cloud Application Performance Management V8.1.4.0 Synthetic Playback agent correção temporária 5 ou posterior em sistemas nos quais você instalou o Synthetic Playback agent.
- Entre em contato com a IBM para assegurar que sua assinatura do Cloud APM tenha sido atualizado para o IBM IBM Cloud Application Performance Management, Private Cloud APM V8.1.4.0 Server correção temporária 8 ou posterior.
- Se você estiver usando um ponto de presença (PoP) privado de Monitoramento de Disponibilidade, verifique se o número da compilação do PoP sintético é `APM_201903090832` ou posterior inserindo o comando **`cat build.info`** do diretório de instalação do PoP. Versões de compilação anteriores não suportam o formato `.side`.

Correções temporárias para Cloud APM V8.1.4.0 estão disponíveis para download no IBM Support > Fix Central > IBM APM 8.1.4.0.

Sobre Esta Tarefa

Nesta tarefa, você executa ações do usuário em uma página da web e usa o Selenium IDE para registrar essas ações como comandos em um script simples. É possível usar scripts para monitorar o desempenho e a disponibilidade de seu aplicativo da web no Application Performance Dashboard.

Procedimento

Conclua as seguintes etapas para registrar um script de ações do usuário em uma página da web:

1. Clique em **Registrar** para iniciar a gravação de um script. Execute ações do usuário em sua página da web, como clicar em um link.

   Para cada ação do usuário em uma página da web, o Selenium IDE registra um comando e o inclui em um script.

   Por exemplo, conclua as seguintes ações para registrar quando um usuário carrega a página da web do IBM Marketplace e navega para uma avaliação grátis do Cloud APM, em um script:

Tabela 246. Ações do usuário registradas e comandos do Selenium IDE

Ação do Usuário	**Comandos incluídos no script**
Para registrar quando a página da web do Cloud APM no website do IBM Marketplace é aberta, abra a página da web IBM Marketplace. Clique com o botão direito em qualquer lugar na página da web exibida e selecione **abrir**.	`abrir`
Para assegurar que o script verifique se a página da web é carregada, clique com o botão direito no texto do título da página da web (IBM Cloud Application Performance Management) e clique em **Mostrar todos os comandos disponíveis** > **verifyTitle IBM Cloud Application Performance Management**.	`verifyTitle`
Para registrar quando o usuário clica em um link para visualizar detalhes sobre o Cloud APM, clique no link **Detalhes**. A página **Detalhes** é carregada.	`clickAndWait`

Tabela 246. Ações do usuário registradas e comandos do Selenium IDE (continuação)	
Ação do Usuário	**Comandos incluídos no script**
Para assegurar que o script verifique se a página **Detalhes** foi carregada, clique com o botão direito no título "Destaques do recurso" e selecione **Mostrar todos os comandos disponíveis** > **verifyText css=h2.heading --TERTIARY**.	`verifyText`
Para registrar quando o usuário clica em um link para visualizar detalhes sobre como comprar o Cloud APM, clique no link **Comprar**. A página **Compra** é carregada.	`clickandWait`
Para registrar quando o usuário clica em um botão para registrar-se para uma avaliação grátis do Cloud APM, clique no botão **Tentar grátis**.	`click`

2. Na janela do Selenium IDE, clique em **Gravar** para parar a gravação. Clique na ferramenta **Salvar projeto**, dê a seu script um nome significativo e salve como um arquivo `.side` (como `open_webpage.side`).
3. Na janela do Selenium IDE, revise seu script registrado. Clique na guia **Tabela** para exibir o script em um formato de tabela. Na janela Selenium IDE, clique em **Reproduzir caso de teste atual** para testar a reprodução do script que você registrou.

   Nesse exemplo, o Selenium IDE exibe o script de ações do usuário no site do IBM Marketplace, conforme descrito na etapa 1.

Tabela 247. Exemplo de uma gravação de script de ações do usuário do Selenium IDE no IBM Marketplace Website		
Comando	**Target**	**Valor**
`abrir`	`/`	
`verifyTitle`	`IBM Cloud Application Performance Management`	
`clickAndWait`	`css=ul > #details > a`	
`verifyText`	`css=h2.heading--TERTIARY`	Destaques do recurso
`clickAndWait`	`css=ul > #purchase > a`	
`click`	`link=Try Free`	

Resultados
Você registrou um script que pode ser usado para monitorar o desempenho e a disponibilidade de um aplicativo da web.

O que Fazer Depois

Se você registrou um script complexo, é possível organizar o seu script em scripts mais simples, de forma que cada script represente um processo de negócios específico ou ação do usuário em seu aplicativo da web.

Use o Gerenciador de Script Sintético para fazer upload do arquivo de script para uma transação sintética nova ou existente.

Estruturando scripts complexos
Organize um script complexo em vários scripts; em seguida, salve scripts juntos em uma coleção de scripts chamada *suíte de testes*.

Sobre Esta Tarefa

Se você criar um script complexo, é possível organizar esse script em scripts simples que representem diferentes processos de negócios ou do usuário em seu aplicativo da web. Salve os scripts juntos como um suíte de testes. É possível, então, usar esses scripts para monitorar o desempenho e a disponibilidade de seu aplicativo da web em resposta a ações do usuário específicas no Application Performance Dashboard.

Deve haver apenas uma suíte de testes e todos os testes devem ser incluídos nela.

Importante: Uma boa prática é organizar scripts complexos em scripts separados, em que cada script representa um processo típico de usuário ou de negócios que você deseja monitorar. Por exemplo, crie scripts separados que registrem quando um usuário efetua login em um website ou procura um item. Se você organizar seus scripts de acordo com processos de usuário ou de negócios, será possível, então, monitorar a resposta de seu aplicativo da web para esses processos específicos no Application Performance Dashboard.

Procedimento

Para organizar seu script complexo em scripts separados e salvar seus scripts como um suíte de testes, conclua as etapas a seguir:

1. Para criar um script separado para cada processo do usuário que é registrado em seu script, clique em **Testes** > **+** no Selenium IDE. Dê a cada script um nome significativo que descreva o processo do usuário e salve cada script como um arquivo `.side`, como `load_homepage.side`.

   Para obter mais informações, consulte “Registrando scripts sintéticos” na página 1027.

   Importante: O nome dado ao script no Selenium IDE é o nome que identifica o processo de negócios ou do usuário registrado que é monitorado no Application Performance Dashboard.
2. No Selenium IDE, abra um script complexo registrado anteriormente. Organize seus comandos de script em scripts separados, de acordo com as ações de usuários diferentes. Comandos **Recortar** do script complexo original na janela **Caso de teste** e comandos **Colar** na janela **Caso de teste** diferente.

   Por exemplo, o exemplo de script completo em Gravando scripts sintéticos contém comandos do Selenium IDE para três diferentes processos do usuário.

   - Abra a página inicial do Cloud APM no website IBM Marketplace.
   - Abra a página **Detalhes** no IBM Marketplace.
   - Abra a página **Precificação** e registre quando o usuário abrir a página de registro de uma avaliação grátis.

   As ações do usuário serão, então, organizadas em três scripts diferentes.

Tabela 248. Script de amostra para abrir a página do IBM Marketplace (`load_homepage.side`)

Comando	Target	Valor
`abrir`	`/`	
`verifyTitle`	`IBM Cloud Application Performance Management`	

*Tabela 249. Script de amostra para abrir a página **Detalhes** no IBM Marketplace (`load_products.side`)*

Comando	Target	Valor
`clickAndWait`	`css=ul > #details > a`	
`verifyText`	`css=h2.heading--TERTIARY`	Destaques do recurso

*Tabela 250. Script de amostra para abrir as páginas **Compra** e de registro de avaliação no IBM Marketplace (`load_APM.side`)*

Comando	Target	Valor
clickAndWait	css=ul > #purchase > a	
click	link=Try Free	

3. Para colocar casos de teste individuais em uma suíte de testes, mude para a janela **Suíte de testes** e inclua testes na suíte de testes, de acordo com a sequência de lógica de negócios. Por último, clique na ferramenta **Salvar projeto** para salvar o suíte de testes e todos os testes no suíte de testes em um arquivo `.side`.
   Como um exemplo, considere a sequência lógica `Load_URL`, `Select Manage inventory`, `Select IBM Machine Type`. Quando incluímos esses casos de testes na suíte de testes, primeiro verificamos `Load_URL`, seguido por `Select Manage inventory`, em seguida, `Select IBM Machine Type`

Resultados
Você registrou um conjunto de scripts que pode ser usado para monitorar o desempenho e a disponibilidade de seus aplicativos da web. Use o Gerenciador de Script Sintético para fazer upload de seu `.side` suíte de testes de scripts para uma nova ou existente transação sintética.

Atualizando scripts de versões anteriores do Selenium IDE
As versões 2.2.X e 3.2.X suportadas do Selenium IDE usam o formato `.side` para gravar scripts sintéticos diferentes do formato `.html` usado por versões mais antigas do Selenium IDE. Se você tiver os scripts `.html` existentes, ainda é possível usá-los. Scripts que foram criados com versões mais antigas do Selenium IDE podem não funcionar completamente com os drivers mais recentes do Firefox e Selenium usados pelo IBM Cloud Availability Monitoring. Em alguns casos, talvez você queira editar os scripts `.html`, regravá-los no novo formato `.side` ou importá-los no script `.html` e salvar no novo formato `.side`.

Procedimento

- Exceção: Se desejar interagir com o elemento `Select2`, não use o comando **`select`** (consulte https://github.com/SeleniumHQ/selenium-ide).
  O script antigo é

```
<td>select</td>
<td>id=country</td>
<td>label=United States</td>
```

  Ele deve ser mudado para

```
<tr>
   <td>runScript</td>
   <td>window.scrollTo(0,810)</td>
   <td></td>
</tr>
<tr>
   <td>click</td>
   <td>id=select2-country-container</td>
   <td></td>
</tr>
<tr>
   <td>click</td>
   <td>xpath=(//ul[@id='select2-country-results']/li[text() = 'United States'])</td>
   <td></td>
</tr>
```

- Limitação: scripts `.side` registrados com Selenium IDE 3.2.X ou 3.3.X são suportados; o localizador **`linkText`** não é suportado.

Gerenciando transações sintéticas
Use o Gerenciador de Script Sintético para criar, configurar e excluir transações sintéticas.

Para exibir o Gerenciador de Script Sintético, clique no ícone **Configuração do Sistema** e selecione **Gerenciador de Script Sintético**. Para trabalhar no Gerenciador de Script Sintético, deve-se ser um membro de uma função que tenha permissão de visualização para **Gerenciador de Script Sintético** e **Configuração do agente**. Para obter mais informações, consulte "Funções e permissões" na página 1002.

É possível visualizar dados sobre o uso da transação sintética para aplicativos da web destinados ao público externo no mês atual. Visualize o número de instâncias de reprodução executadas e as instâncias de reprodução previstas, com base na configuração atual para o mês atual na tabela Uso mensal de reprodução no Synthetic Script Manager.

Importante: Para criar transações sintéticas para aplicativos da web internos privados e aplicativos da web externos privados, você deve instalar o Synthetic Playback agent em cada local que contém um aplicativo da web que você deseja monitorar.

É possível executar as seguintes tarefas com o Gerenciador de script sintético:

- Criar e editar uma transação sintética.
- Configurar variáveis de transação sintética.
- Excluir uma transação sintética.

Criando e editando uma transação sintética

Para visualizar dados sobre o desempenho e a disponibilidade de um aplicativo da web, deve-se primeiro criar uma transação sintética no Gerenciador de Script Sintético.

Sobre Esta Tarefa

Use o Gerenciador de Script Sintético para criar, editar e configurar uma transação sintética. Insira a URL de um aplicativo da web no Editor de Script Sintético para gerar um script simples para sua transação sintética. Para simular processos do usuário complexos, faça upload de um script sintético para uma transação sintética no Editor de Script Sintético. Em seguida, configure a transação sintética para ser executada a intervalos regulares e em diferentes locais.

Procedimento

Para criar uma transação, ou para editar uma transação existente, conclua as etapas a seguir:

1. Opcional: Se o Synthetic Script Manager não for exibido, clique no ícone **Configuração do Sistema** e selecione **Synthetic Script Manager**.
2. Para criar uma nova transação, clique no ícone **Novo**. Para editar uma transação existente, clique no ícone **Editar**.
3. Em **Editor de Script Sintético**, clique na guia **Fazer Upload de um Script** e insira um nome de transação na caixa de texto **Nome da Transação**. Insira uma descrição de sua transação na caixa de texto **Descrição**.

   Importante: Não dê à transação o mesmo nome que o de uma transação que foi excluída nas últimas 24 horas. Se você der à sua transação o mesmo nome que uma transação excluída recentemente, os dados de ambas as transações serão atribuídos incorretamente ao nome dessa transação no Application Performance Dashboard.
4. Para gerar um script simples para testar um aplicativo da web, selecione **Inserir a URL da Página da Web para Testar** e insira uma URL. O Synthetic Script Manager gera um script sintético simples baseado nessa URL.
5. Para designar um arquivo de script criado anteriormente a sua transação, selecione **Fazer Upload do Arquivo de Script**. Clique em **Fazer Upload do Script** para procurar scripts em seu sistema. Escolha um script e clique em **Abrir**.

   Importante: O arquivo de script sintético deve ser um dos tipos de arquivo a seguir:

   - `.html`
   - `:NONE.`

Salve os scripts individuais simples (casos de teste) como arquivos `.html`. Compacte casos de teste e suítes de teste em um arquivo `.zip`.

6. Para configurar reprodução simultânea ou escalonada de uma transação sintética, clique na guia **Planejar um Script**. Selecione **Simultâneo** para executar a transação a partir de todos os locais simultaneamente ou selecione **Escalonado** para executar a transação a partir de um local diferente em cada intervalo.
7. Para escolher a frequência com que um script é executado, clique na guia **Planejar um Script**. Clique na caixa de texto **Intervalo** e insira um número, com base na frequência com que você deseja monitorar seu aplicativo da web. Escolha uma duração de intervalo entre `1` e `60` minutos.

   Nota: Scripts grandes ou complexos podem levar mais tempo para serem executados. Escolha uma duração de intervalo mais longa para scripts grandes ou complexos.
8. Para escolher os locais de reprodução para seu script, clique na guia **Planejar um script** e, em seguida, selecione os locais do datacenter e locais de instalação do agente onde você deseja executar seu script.
9. Para configurar limites de tempo de resposta para transações e subtransações sintéticas, clique na guia **Configurações avançadas**, em seguida, clique e expanda uma transação sintética para revelar todas as subtransações. Clique duas vezes no valor do limite de tempo de resposta e insira um valor. Escolha um valor entre `0` e `3600` segundos. Se você não desejar configurar um limite, insira `0`. O valor do limite de tempo de resposta padrão é 10 segundos.

   Nota: Alguns comandos podem levar mais tempo que outros. Escolha um limite de tempo de resposta que seja adequado para o comando que você deseja testar. Se a sua transação testar quanto tempo uma página da web leva para abrir, escolha um tempo de resposta mais longo.
10. Para concluir a criação ou edição de sua transação, clique em **Salvar**.

Resultados

Você configurou uma transação sintética. A transação sintética é listada no Gerenciador de Script Sintético.

O que Fazer Depois

É possível visualizar métricas e KPIs registrados por uma transação sintética no Application Performance Dashboard. Também é possível incluir transações como componentes em um aplicativo e visualizar todas as transações sintéticas que estão associadas a esse aplicativo.

Importante: Ao incluir sua primeira transação sintética, um espaço em branco pode aparecer no widget de grupo **Disponibilidade ao Longo do Tempo** no Application Performance Dashboard. O espaço em branco desaparece rapidamente quando o servidor recebe os primeiros resultados da reprodução da transação.

Configurando variáveis de transação sintética

Use o Gerenciador de Scripts Sintéticos para atualizar valores da variável, como nomes do usuário e senhas que estão armazenados em scripts sintéticos, sem a necessidade de editar os arquivos de script. Os valores de suas variáveis podem ser exclusivos para cada local de reprodução.Configure variáveis para seus scripts sintéticos quando seus aplicativos da web precisarem de valores de variáveis diferentes em diferentes locais. Por exemplo, se o seu aplicativo da web não permitir os mesmos detalhes de login em locais diferentes, use o Gerenciador de Scripts Sintéticos para fornecer detalhes de login diferentes em cada local. É possível criar variáveis em scripts sintéticos usando o comando `store` no plug-in Selenium-IDE.

Sobre Esta Tarefa

Nessa tarefa, use o Gerenciador de Script Sintético para configurar as variáveis armazenadas em seu script sintético.

Procedimento

Para configurar as variáveis de uma transação sintética, conclua as etapas a seguir:

1. Se o Synthetic Script Manager não for exibido, clique no ícone **Configuração do Sistema** e selecione **Synthetic Script Manager**. Selecione uma transação sintética da lista e clique no ícone **Editar**.
2. Selecione os locais de reprodução para sua transação sintética.
3. Clique na guia **Configurações Avançadas**. Se o script sintético contiver variáveis, será possível editar essas variáveis na janela **Configurar substituições de variáveis para diferentes locais**. Para editar uma variável, dê um clique duplo no valor. Para concluir, clique em **Salvar**.

   Por exemplo, o script a seguir contém as variáveis *username* e *password*. Os valores dessas variáveis, `user1` e `pass`, são salvos usando o comando `store` em Selenium-IDE. As variáveis têm o mesmo valor em dois locais, Dallas e San Jose.

Tabela 251. Exemplo de um script com variáveis		
Comando	**Target**	**Valor**
`store`	`user1`	*username*
`store`	`aprovado`	*senha*
`tipo`	`id=j_username`	*${username}*
`tipo`	`id=j_password`	*${password}*

   Os valores das variáveis de script são exibidas na janela **Configurar substituições de variáveis para diferentes locais**. Mude o valor de *username* no local `Dallas` de `user1` para `admin1` para que a transação sintética use diferentes detalhes de login em diferentes locais.

Tabela 252. Valores de variáveis de script em diferentes locais		
Local	**nome do usuário**	**senha**
São José	user1	passar
Dallas	admin1	passar

Resultados
Você configurou as variáveis de uma transação sintética. Agora é possível usar essa transação sintética para testar o desempenho e a disponibilidade de um aplicativo da web em diferentes locais.

O que Fazer Depois
É possível visualizar métricas e KPIs registrados por uma transação sintética no Application Performance Dashboard. Também é possível incluir transações como componentes em um aplicativo e visualizar todas as transações sintéticas que estão associadas a esse aplicativo.

Filtrando URLs e nomes de domínio para suas transações sintéticas
Use o Synthetic Script Manager para permitir ou bloquear o acesso a URLs e domínios específicos, incluindo regras na lista de desbloqueio e na lista de bloqueio para seu teste.

Sobre Esta Tarefa

É possível controlar quais dependências e recursos contribuem com os tempos de resposta de seus aplicativos da web testados. Use a lista de bloqueio para filtrar solicitações de domínios especificados para remover essas solicitações de seus tempos de resposta medidos. Use a lista de desbloqueio para incluir solicitações de domínios especificados para incluir essas solicitações em seus tempos de resposta medidos. Use a lista de bloqueio e a lista de desbloqueio para filtrar ou incluir dependências que estão associadas a seu aplicativo da web, como métricas de terceiros.

O campo **Lista de bloqueio** contém uma lista de regras que bloqueiam o acesso a URLs e domínios especificados.

O campo **Lista de desbloqueio** contém uma lista de regras que permitem acesso a URLs e domínios especificados.

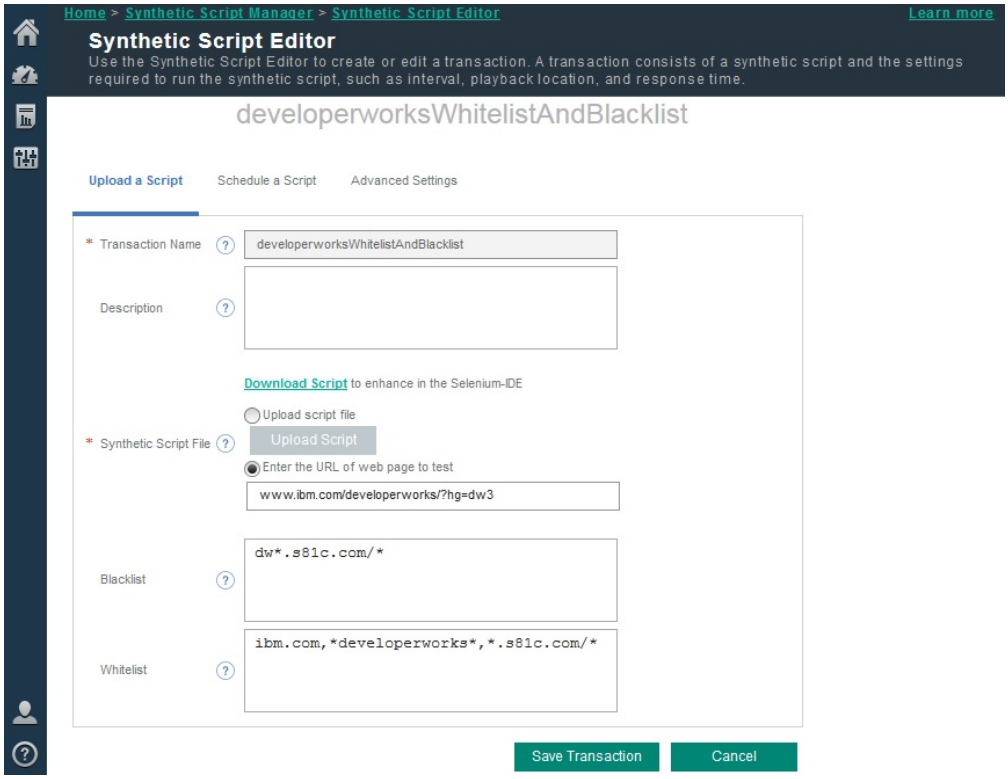
Use vírgulas (,) para separar regras em sua lista de bloqueio e lista de desbloqueio. Use o símbolo curinga (*) para filtrar nomes de domínio e URLs. Por exemplo, `ibm.com, *.bluemix.net, *developerworks*, *.profile.*.cloundfront.net/*.png`.

Nota: Se você configurar uma lista de bloqueio e uma lista de desbloqueio para sua transação sintética, a lista de bloqueio terá prioridade mais alta.

Procedimento

Para incluir uma regra na lista de bloqueio ou na lista de desbloqueio para sua transação sintética, conclua as seguintes etapas:

1. Se o Synthetic Script Manager não for exibido, clique no ícone **Configuração do Sistema** e selecione **Synthetic Script Manager**.
2. Para configurar sua lista de bloqueio ou lista de desbloqueio para uma transação existente, clique no ícone **Editar**. Se nenhuma transação for listada, clique no ícone **Novo** para criar uma nova transação.
3. Em **Editor de Script Sintético**, clique na guia **Fazer Upload de um Script** e insira um nome de transação na caixa de texto **Nome da Transação**. Inclua regras nas caixas de texto **Lista de bloqueio** e **Lista de desbloqueio**.



Resultados

Sua transação sintética agora filtra solicitações indesejadas para seu aplicativo da web e permite acesso a outras solicitações específicas.

Ocultando senhas no Synthetic Script Manager

Armazene senhas como variáveis em seus scripts sintéticos para ocultar valores de senha no Synthetic Script Manager.

Antes de Iniciar

Este procedimento requer a edição de um script sintético. Registre um script sintético usando o Selenium IDE. Para obter mais informações, consulte "Registrando scripts sintéticos" na página 1027.

Sobre Esta Tarefa

Modifique manualmente seus scripts sintéticos no Selenium IDE para armazenar sua senha como uma variável. É possível então criar transações sintéticas com senhas ocultas no Synthetic Script Manager. As senhas ocultas são exibidas como asteriscos no Synthetic Script Manager.

Importante: É recomendável armazenar suas senhas em scripts sintéticos para que os valores de senha não sejam exibidos no Synthetic Script Manager. As senhas ocultas tornam seus aplicativos da web mais seguros, evitando que outros visualizem as senhas.

Procedimento

1. Abra o script que você deseja modificar no Selenium IDE. Use o comando `store` para designar uma senha à variável *password*, seguindo o exemplo descrito nesta etapa; em seguida, salve o script.

   Importante: Deve-se armazenar a senha como o nome de variável *password* para que a senha não seja exibida no Synthetic Script Manager.

   Por exemplo, o seguinte script sintético contém um nome do usuário *test@example.com* e um valor de senha *ibm4value*.

   ```
   <tr>
      <td>type</td>
      <td>id=username</td>
      <td>test@example.com</td>
   </tr>
   <tr>
      <td>type</td>
      <td>id=password</td>
      <td>ibm4value</td>
   </tr>
   ```

   O seguinte script mostra como designar o valor de senha *ibm4value* à variável *password* usando o comando `store`.

   ```
   <tr>
      <td>store</td>
      <td>ibm4value</td>
      <td>password</td>
   </tr>
   <tr>
      <td>type</td>
      <td>id=username</td>
      <td>test@example.com</td>
   </tr>
   <tr>
      <td>type</td>
      <td>id=password</td>
      <td>$(password)</td>
   </tr>
   ```

2. Opcional: Para ocultar a senha no nível de script, designe um valor em branco à variável *password* usando o comando `store`; em seguida, salve o script.

   É possível configurar a senha posteriormente no Synthetic Script Manager.

   Por exemplo, seguinte o script mostra como designar um valor em branco à variável *password* usando o comando `store`.

   ```
   <tr>
      <td>store</td>
      <td></td>
      <td>password</td>
   </tr>
   <tr>
      <td>type</td>
      <td>id=username</td>
   ```

```
   <td>test@example.com</td>
</tr>
<tr>
   <td>type</td>
   <td>id=password</td>
   <td>$(password)</td>
</tr>
```

3. Efetue login no Console do Cloud APM e abra o **Synthetic Script Manager**. Crie uma transação e faça upload de seu script para essa transação. Clique na guia **Configurações Avançadas**.

   A senha para cada local fica oculta. É possível mudar a senha para cada local. Para obter mais informações, consulte "Gerenciando transações sintéticas" na página 1031.

Excluindo uma transação sintética

Use o Gerenciador de Script Sintético para excluir transações sintéticas.

Procedimento

Para excluir uma transação sintética, conclua as etapas a seguir:

1. Se uma transação sintética for designada a um aplicativo, primeiro você deverá remover a transação desse aplicativo. No Application Performance Dashboard, clique e expanda **Todos os meus aplicativos** e, em seguida, clique no aplicativo que está associado à transação sintética que você deseja excluir. Clique no ícone **Editar** . Na janela **Editar Aplicativo**, remova o componente de transação sintética do aplicativo. Para obter mais informações, consulte Gerenciando aplicativos.

   Agora, a transação sintética pode ser excluída.
2. Na barra de navegação, clique no ícone **Configuração do Sistema** e selecione **Gerenciador de Script Sintético**. Selecione uma transação sintética e, em seguida, clique no ícone **Excluir** . Para confirmar que deseja excluir esta transação sintética, clique em **OK**.

Resultados

A transação sintética foi excluída.

Visualizando dados de transações sintéticas no Application Performance Dashboard

Visualize dados da transação sintética no Application Performance Dashboard. Associe transações sintéticas a um aplicativo novo ou existente e visualize todas as transações sintéticas associadas juntas no Application Performance Dashboard.

Sobre Esta Tarefa

É possível visualizar dados da transação sintética na janela **Minhas Transações** no Application Performance Dashboard.

Também é possível criar grupos de transações sintéticas, associando as transações a um aplicativo. Use a ferramenta **Incluir Aplicativo** ou **Editar Aplicativo** no Application Performance Dashboard para incluir transações sintéticas como componentes no aplicativo da web novo ou existente. É possível visualizar dados para todas as transações sintéticas associadas ao aplicativo juntas no Application Performance Dashboard.

Se você já estiver usando o agente de Tempo de Resposta para monitorar o tempo de resposta do usuário para um aplicativo, é possível incluir uma transação sintética para esse aplicativo. É possível, então, visualizar mais métricas e KPIs para esse aplicativo no Application Performance Dashboard.

Procedimento

- Para visualizar transações sintéticas, execute a seguinte etapa:

  a) Clique no ícone **Desempenho** e selecione **Application Performance Dashboard**. Na janela **Aplicativos**, expanda **Todos os Meus Aplicativos** e selecione **Minhas Transações**. Na janela **Grupos**, expanda **Transações** e selecione **Transações Sintéticas**.

b) Clique em uma transação sintética para visualizar dados de disponibilidade e desempenho para essa transação, junto com um gráfico de tempos de resposta para instâncias da transação por um período definido.

- Para associar transações sintéticas a um aplicativo, execute as seguintes etapas:

  a) Clique no ícone **Desempenho** e selecione **Application Performance Dashboard**. Selecione e edite um aplicativo existente ou crie um novo aplicativo. Para obter mais informações, consulte Gerenciando aplicativos.

  b) Na janela **Incluir Aplicativo**, clique no ícone **Incluir Componentes** e selecione **Transações Sintéticas** na lista de componentes. Na janela **Editor de Componente**, selecione uma transação sintética e clique em **Incluir** para associar a transação sintética ao aplicativo.

  c) Clique em **Voltar**. Clique em **Fechar** para fechar a janela **Editor de Componente**. Clique em **Salvar**. Para incluir outra transação sintética como um componente, repita as etapas 1 - 3.

Resultados

Você associou uma transação sintética a um aplicativo. Agora é possível visualizar o aplicativo e suas transações sintéticas associadas no Application Performance Dashboard. Para obter mais informações, consulte Gerenciando aplicativos.

Nota: Ao associar uma transação sintética a um aplicativo, a disponibilidade inicial desse aplicativo é desconhecida. O status pode levar vários minutos para ser atualizado.

Gerenciando eventos sintéticos

Use O Gerenciador de Limite e o Gerenciador de Grupo de Recursos para configurar limites e designá-los a transações sintéticas. Eventos sintéticos são gerados quando o valor de um atributo de transação corresponde à condição que está definida no limite. É possível monitorar eventos sintéticos no Application Performance Dashboard.

Criando um limite para transações sintéticas

Use o Gerenciador de limite para criar limites para transações sintéticas. Os limites são usados para comparar os valores de atributo com os valores configurados no limite. Caso o valor de amostra satisfaça a comparação, um evento é gerado.

Sobre Esta Tarefa

Os limites permitem que os usuários monitorem quando os aplicativos relatam condições específicas. Por exemplo, é possível criar um limite para monitorar o tempo que um website leva para responder a um comando de usuário específico. Se o website demorar mais do que o tempo especificado pelo limite, um evento sintético será gerado.

Procedimento

Para criar um limite e associá-lo a uma ou mais transações sintéticas, conclua as etapas a seguir:

1. Na barra de navegação, clique no ícone **Configuração do Sistema** e selecione **Gerenciador de Limite**. Configure o tipo **Origem de Dados** como **Transação Sintética**.
2. Crie um limite. Para obter mais informações, consulte “Gerenciador de Limites” na página 985.
3. Para associar o limite a uma transação, selecione **KSO TRANSACTION** como o **Conjunto de Dados** e, em seguida, selecione **TRANSNAME** como **Item de Exibição**. Para o **Operador Lógico**, selecione **And (&)**.

   Nota: Você deve selecionar **TRANSNAME** como o **Item de Exibição**. Se você não selecionar **TRANSNAME**, não poderá visualizar os eventos sintéticos no Painel de Desempenho do Aplicativo.
4. Para incluir uma condição, clique no ícone **Nova Condição**. Na caixa Nova Condição, selecione um **Atributo** e um **Operador**. Em seguida, insira um valor do limite para **Valor**. Para incluir esta condição no limite, clique em **OK**.

   Por exemplo, para incluir uma condição de limite que gera um evento sintético quando mais de 50% das transações são lentas, selecione **PSLOW** como **Atributo** e, em seguida, selecione **Maior que** como

Operador. Para configurar a porcentagem de transações lentas para gerar um evento, insira 50 como o **Valor**.

5. Para definir mais atributos de limite, inclua mais condições em seu limite.
6. Quando concluir, clique em **Salvar**. Se você não desejar designar o limite a um grupo de recursos, clique em **OK**.

Resultados
Você criou um limite e o associou a uma transação sintética. Quando as condições de limite são atendidas, um evento é gerado. É possível monitorar eventos no Application Performance Dashboard, na guia **Eventos**.

O que Fazer Depois
É possível agrupar as transações sintéticas em grupos de recursos.

Criando um grupo de recursos para transações sintéticas
Organize suas transações sintéticas em um grupo de recursos e aplique limites a todas as transações desse grupo de recursos.

Antes de Iniciar
Crie um limite a ser aplicado a todas as transações sintéticas em seu grupo de recursos.

Sobre Esta Tarefa

É possível organizar suas transações sintéticas em grupos de recursos e aplicar limites a cada transação sintética desse grupo de recursos. Use o Gerenciador de Grupo de Recursos para criar um grupo de recursos e designar um limite para esse grupo de recursos. Em seguida, designe um ou mais subnós de transações sintéticas a esse grupo de recursos. O limite que está associado ao grupo de recursos agora se aplica a todas as transações sintéticas associadas.

Procedimento

Para criar um grupo de recursos para transações sintéticas, execute as seguintes etapas:

1. Clique no ícone **Configuração do Sistema** e selecione **Gerenciador de Grupo de Recursos**. Crie um grupo de recursos ou edite um grupo de recursos existente. Para obter mais informações, consulte “Gerenciador de Grupos de Recursos” na página 980.

Para criar um grupo de recursos para transações sintéticas, execute as seguintes etapas:

2. Dê ao seu grupo de recursos um nome e uma descrição. Designe um limite para seu grupo de recursos na tabela **Designação de limite** e clique em **Salvar**. No Gerenciador de Grupo de Recursos, selecione seu grupo de recursos novamente e clique no ícone **Editar** .
3. Associe seu grupo de recursos aos subnós de transação sintética da tabela **Designação de Recurso** e clique em **Salvar**.

   O formato dos subnós de transação sintética é `S0:TransactionName`. Por exemplo, se você tiver uma transação `open_webpage`, o subnó disponível será chamado `S0:open_webpage`.

Resultados
Você organizou suas transações sintéticas em um grupo de recursos e aplicou um limite a cada transação desse grupo de recursos.

Criando limites críticos para transações sintéticas simultâneas e escalonadas
Use o Threshold Manager para criar limites críticos para transações sintéticas simultâneas e escalonadas.

Sobre Esta Tarefa

Crie limites que notifiquem as partes interessadas quando transações escalonadas consecutivas falham ou quando transações simultâneas falham em todos os locais de reprodução. Para obter mais informações, consulte “Criando e editando uma transação sintética” na página 1032.

Procedimento

Para criar um limite crítico que crie um evento quando instâncias de reprodução de transação escalonada falham, conclua as seguintes etapas:

1. Crie um limite para transações sintéticas no Threshold Manager. Para obter mais informações, consulte “Criando um limite para transações sintéticas” na página 1038.
2. No Threshold Manager, selecione **Crítico** como a **Gravidade** e insira 1 minuto como o limite **Intervalo (HHMMSS)**. Use a seguinte fórmula para determinar as **Amostras consecutivas requeridas**:

   Amostras consecutivas requeridas = (intervalo de reprodução * falhas consecutivas esperadas) - 1

   Por exemplo, se o intervalo de reprodução da transação sintética que você deseja monitorar for 5 minutos e você quiser detectar 8 falhas de reprodução consecutivas, deverá configurar **Amostras consecutivas requeridas** como (5 * 8) - 1 = 39.
3. Inclua uma condição. Na caixa Nova condição, selecione **LOCATION** como **Atributo**, selecione **Equals** como **Operador** e insira None como o **Valor**. Inclua uma segunda condição e configure **PFAILED** = 100. Salve o limite.
4. Na barra de navegação, abra o **Resource Group Manager**. Crie um grupo de recursos. Designe uma ou mais transações sintéticas escalonadas para seu grupo de recursos e depois designe o limite criado nas etapas 1-3 para seu grupo de recursos. Salve o grupo de recursos. Para obter mais informações, consulte “Criando um grupo de recursos para transações sintéticas” na página 1039.

Para criar um limite crítico que crie um evento quando instâncias de reprodução de transação simultâneas falham em diversos locais, conclua as seguintes etapas:

5. Crie um limite para transações sintéticas no Threshold Manager. Para obter mais informações, consulte “Criando um limite para transações sintéticas” na página 1038.
6. No Threshold Manager, selecione **Crítico** como **Gravidade** e insira 1 minuto como **Intervalo (HHMMSS)**. Configure **Amostras consecutivas requeridas** como o mesmo valor do intervalo de reprodução da transação que você deseja monitorar.

   Por exemplo, se o intervalo de reprodução da transação sintética que você deseja monitorar for 5 minutos, configure **Amostras consecutivas requeridas** como 5.
7. Inclua uma condição. Na caixa Nova condição, selecione **LOCATION** como **Atributo**, selecione **Equals** como **Operador** e insira None como o **Valor**. Inclua uma segunda condição e configure **PFAILED** = 100. Salve o limite.
8. Crie um grupo de recursos. Designe uma ou mais transações sintéticas e o novo limite crítico para seu grupo de recursos. Para obter mais informações, consulte “Criando um grupo de recursos para transações sintéticas” na página 1039.

Resultados

Você criou um limite crítico para uma transação sintética simultânea ou escalonada. Quando as condições de limite são atendidas, um evento é gerado. É possível monitorar eventos no Application Performance Dashboard, na guia **Eventos**.

Gerenciando notificações por e-mail para eventos sintéticos

Use o Gerenciador de Grupo de Recursos e o IBM Alert Notification para gerar notificações por e-mail quando o desempenho de seu aplicativo exceder os limites.

Antes de Iniciar

Para configurar notificações por e-mail para eventos sintéticos, deve-se primeiramente ativar o Alert Notification para sua assinatura. Para obter mais informações, consulte Notificação de alerta no IBM Knowledge Center.

Sobre Esta Tarefa

No Gerenciador de Grupo de Recursos, use o Alert Notification para configurar notificações por e-mail. Notificações por e-mail são geradas quando o desempenho de seus aplicativos atende às condições configuradas pelos limites associados ao seu grupo de recursos.

Procedimento

Para gerenciar notificações por e-mail, conclua as seguintes etapas:

1. Clique no ícone **Configuração do Sistema** e selecione **Gerenciador de Grupo de Recursos**. Crie ou edite um grupo de recursos.
2. Selecione um limite na tabela **Designação de limite** e clique em **Salvar**. Em seguida, associe seu grupo de recursos a um recurso Reprodução Sintética ou a um recurso do agente Eventos Sintéticos na tabela **Designação de recurso**. Clique em **Salvar**. No Gerenciador de Grupo de Recursos, selecione o grupo de recursos novamente e clique no ícone **Editar** .
3. Para iniciar o Alert Notification em uma nova guia, clique em **Configurar notificação por e-mail** no Gerenciador de Grupo de Recursos. Em Notificação de alerta, clique em **Usuários** na barra de navegação para criar ou editar destinatários de notificações por e-mail. Para obter mais informações, consulte Notificação de alerta no IBM Knowledge Center.
4. No Alert Notification, clique em **Políticas de notificação** na barra de navegação. O **Editor de notificações** é automaticamente provisionado com uma nova política. O nome e o filtro da política são derivados do grupo de recursos. Clique em **Incluir regra** para definir as condições que determinam quando uma notificação por e-mail é enviada. Para obter mais informações, consulte Notificação de alerta no IBM Knowledge Center.
5. Para concluir a configuração de notificações por e-mail, clique em **Salvar**. A sua política é listada em uma tabela na guia **Políticas de notificação**.

Diretrizes para maximizar o desempenho do agente e do servidor para monitoramento do arquivo de log

Para assegurar que você obtenha o máximo desempenho dos agentes de S.O. e do servidor Performance Management, é preciso definir as expressões regulares no arquivo de formato (.fmt) e também limitar o número de eventos de monitoramento do arquivo de log que são relatados ao Console do Cloud APM.

Diretrizes para definir expressões regulares no arquivo `.fmt`

O arquivo `.fmt` usa expressões regulares que requerem muito processamento da CPU. Para melhorar o desempenho do agente e do servidor, minimize o tempo gasto verificando registros no log de origem de monitoramento com relação à expressão regular no arquivo `.fmt` usando as diretrizes a seguir:

Minimize o uso de padrões multilinhas.

Os padrões de multilinhas são dispendiosos porque o agente deve determinar quais são os registros e se eles se correspondem. Ao usar um padrão de multilinhas que é uma expressão regular que contém o caractere "\n", ou um formato de estilo TEC que contém o token '%n', o agente deve dividir o arquivo monitorado em registros de vários tamanhos primeiro. Em seguida, o agente deve verificar os registros com relação às expressões no arquivo de formato. Esse procedimento requer a verificação das expressões regulares duas vezes, portanto o processamento é lento. Se você usar o padrão de linha única, pressupõe-se que cada linha do arquivo seja um registro e o processamento seja muito mais rápido.

Em alguns casos, poderá ser possível ignorar algumas das linhas e alcançar melhor desempenho. Por exemplo, um único registro de um log de rastreio de RAS1 é mostrado aqui:

```
(4D66DACB.0001-1:RAS1,400,"CTBLD")
```

```
+4D66DACB.0001 Component: ira
```

```
+4D66DACB.0001
Driver: agent_fac:15/4114877.7
```

```
+4D66DACB.0001
Timestamp: Feb 24 2011 13:18:54
```

```
+4D66DACB.0001
Target: sos510amdx6-d
```

Neste exemplo, se você estiver interessado somente em processar esta linha:

```
+4D66DACB.0001
Driver: agent_fac:15/4114877.7
```

será possível gravar o seguinte padrão de linha única:

```
^\+.*Driver: agent_fac:([0-9\.\/]+)$
```

Esse padrão de linha única processa o valor importante necessário sem requerer o formato de multilinhas. As outras quatro linhas do registro lógico são tratadas como registros de linha única que não correspondem a nada e são descartadas.

Classifique as expressões no arquivo de formato pela frequência de ocorrência no log de monitoramento.

O agente verifica cada registro que ele lê a partir do log com relação às expressões no arquivo de formato, até que ele localize uma correspondência. Ele inicia com a expressão final no arquivo, e procura acima. Quando localiza uma correspondência, ele para a procura. Se a expressão registrada mais comumente for listada por último, em seguida, quando essa expressão for registrada, será a única expressão que é verificada.

Se houver 100 expressões no arquivo de formato, cada vez que um registro de log corresponder à primeira que é listada no arquivo de formato, o agente deverá verificar as outras 99 expressões primeiro, o que retarda o processamento. Quando um registro que é lido a partir do log não corresponder a nenhum dos padrões no arquivo de formato, o agente deverá verificá-lo com relação a todos os padrões, antes que ele saiba que não é correspondido. Esse processo é lento e dispendioso.

Inclua tantos dados constantes quanto possível nas expressões regulares.

Por exemplo, se o erro a seguir for retornado no log:

```
Disk error on device: /dev/sda1 Disk error on device:
/dev/sdb2 yyy
```

será possível gravar esta expressão:

```
^Disk.*: .*$
```

Essa expressão causa uma correspondência, mas força o mecanismo de expressão regular a considerar mais possibilidades em outras linhas que podem ser semelhantes, mas que no final não se correspondem, por exemplo, se os dois pontos estiverem ausentes.

A expressão a seguir é mais precisa e faz com que o mecanismo de expressão regular pare de processar erros que não correspondem:

```
^Disk error on device:
/dev/sd[a-b][0-9]$
```

Não use subexpressões desnecessárias.

As subexpressões que são mostradas em parênteses no exemplo que segue são usadas para informar o mecanismo de expressão regular que você deseja usar um valor que é retornado nos dados correspondidos. Essas subexpressões causam processamento extra e não serão necessárias, se você não usar o valor retornado. Por exemplo, quando o erro a seguir for retornado no log:

```
write failure in writing to client
9.27.135.191. Error Broken pipe
```

caso inclua a expressão regular a seguir no arquivo de formato, a mensagem de erro será capturada no término, mas, se você não usar o valor retornado, o desempenho será afetado negativamente:

```
REGEX
WriteFailure

^write failure in writing to client (.*)\. Erro
(.*)$

ClientAddr $1
CustomSlot1

END
```

Use parênteses em expressões para propósitos de agrupamento.

É possível usar o operador ? para informar o mecanismo de expressão regular não para capturar o valor retornado. Portanto, é possível usar o operador ? para agrupar somente os valores que são retornados. Esse agrupamento tem um impacto positivo no desempenho. Por exemplo, se os dados do log a seguir forem retornados:

```
Login succeeded on the first
attempt for user Bob.
Login succeeded on the third attempt for user Joe.
```

Para corresponder ambos os valores que são retornados, deve-se considerar a primeira ou a terceira tentativa de login. Se você não se importar com a tentativa de login específica que foi bem-sucedida ou com usuário específico que foi bem-sucedido, será possível incluir essa expressão para agrupar os valores retornados:

```
REGEX
LoginSuceeded

^login succeeded on the (?:[a-z]+) attempt for user ([A-Z][a-z]*)\.$

UserName $1
CustomSlot1
END
```

Se possível, não use o operador OR (|) em expressões.

O operador | é dispendioso para o processo. O operador | faz com que o mecanismo de expressão regular conclua um backup e tente corresponder valores que não corresponderam inicialmente. Esse procedimento é muito mais ineficiente do que ter duas expressões separadas. Por exemplo, se você tiver a expressão a seguir:

```
REGEX DiskError
^.*disk error.*4|^.*disk failure.*4
END
```

será muito mais eficiente usar estas duas expressões:

```
REGEX DiskError
^.*disk error.*4
END

REGEX DiskError
^.*disk failure.*4
END
```

Essas expressões retornam os mesmos resultados.

Importante: Essas expressões violam a diretriz para usar tantos dados constantes quanto possível, mas demonstram somente os problemas com o operador |.

Não use expressões ambíguas.
As expressões ambíguas forçam o mecanismo de expressão regular a fazer backup e procurar por maneiras diferentes para corresponderem a uma expressão. Para obter mais informações, consulte Dicas de Desempenho.

As expressões ambíguas podem ocorrer como um resultado de uma expressão que é incluída para dividir um longo registro em muitas subexpressões. Nessa versão corrompida desse problema, a expressão tem um espaço entre os dois (.*):

```
(.*) (.*)
```

Nesse exemplo da versão corrompida, o mecanismo regex procura duas sequências de quaisquer expressões que são separadas por um espaço. No entanto, * também corresponde a um espaço, portanto, o mecanismo de expressão regular pode designar o primeiro espaço que vem inicialmente para o primeiro (.*). Se ele atingir o término do registro de entrada sem localizar outro espaço, ele deverá fazer backup e tentar novamente usando o espaço como o espaço literal exigido na expressão.

Para melhorar o desempenho, use somente expressões específicas. É possível usar a ferramenta Regex Pal para verificar se o arquivo de formato definido corresponde ao log de monitoramento. Para obter mais informações, consulte Regex Pal.

Diretrizes para limitar os eventos do arquivo de log que são relatados.

As seguintes diretrizes limitam os eventos do arquivo de log que podem prejudicar o desempenho dos agentes de S.O. ou do Servidor Cloud APM:

Grave formatos específicos no arquivo `.fmt`.
Grave formatos no arquivo `.fmt`, que são específicos e retornam registros relevantes. Por exemplo, é possível gerar um evento para um erro específico, como as linhas que iniciam com `Error:` e ignorar as linhas que iniciam com `Warning:`

```
Error:  disk failure
Error: out of memory
WARNING: incorrect login
```

Não ative a configuração de log não correspondente no arquivo `.conf`.
Assegure-se de não ativar a configuração de **log não correspondente** no arquivo `.conf`, porque essa configuração registra todos os arquivos não correspondidos e sobrecarrega o sistema de arquivos.

Especifique a classe de eventos `*DISCARD*` no arquivo `.fmt`.
Tente limitar o uso de CPU do agente especificando a classe de eventos `*DISCARD*` predefinida no arquivo `.fmt` para descartar dados intencionalmente. Ao usar a classe de eventos `*DISCARD*`, os eventos não são criados para registros de log que correspondem ao padrão no arquivo `.fmt`. Por exemplo:

```
REGEX *DISCARD*
```

Ative a detecção de eventos duplicados durante um período de tempo mais longo.
É possível ativar a detecção de eventos duplicados usando as chaves a seguir no arquivo `.conf` :

- DupDetectionKeyAttributes
- EventSummaryInterval
- EventFloodThreshold

Neste exemplo, as linhas duplicadas são reconhecidas pelos valores *msg* e *CustomSlot1*:

```
DupDetectionKeyAttributes=msg,CustomSlot1
EventSummaryInterval=300
EventFloodThreshold=send_first
```

Se você tiver numerosos eventos duplicados, aplique os valores do limite *send_first* ou *send_none* aos eventos. Para obter mais informações, consulte “Detectando e Filtrando Eventos Duplicados” na página 1017.

Grave condições de limite específicas.
Grave condições de limite específicas que limitam o conjunto de linhas que correspondem ao limite. Por exemplo, a fórmula de limite a seguir faz com que o limite seja disparado somente quando um evento da classe de eventos FileSystemUsage tiver um valor maior ou igual a 95 em CustomInteger1:

```
( Class == 'FileSystemUsage' AND CustomInteger1 >= 95)
```

Forneça o conjunto correto de arquivos `.conf` e `.fmt` para o agente.
Assegure-se de fornecer o conjunto correto de arquivos `.conf` e `.fmt` para o agente. Por exemplo, se você estiver configurando o monitoramento do arquivo de log para o agente do S.O. Windows, assegure-se de configurar os arquivos `.conf` e `.fmt` criados especificamente para o agente do S.O. Windows.

Consulte o banco de dados de alarmes MongoDB para determinar o número de eventos abertos ou a taxa do evento.

- Conclua as etapas a seguir para consultar o banco de dados de alarmes MongoDB para determinar o número de eventos abertos ou a taxa do evento:
  1. Crie um arquivo `event-query.js` com uma consulta do MongoDB para o banco de dados de alarmes, por exemplo:
     - Essa consulta conta todos os eventos abertos e fechados com o nome do limite a seguir:

       ```
       UDB_DB_Pool_Hit_Rat_Pct_Crit_2 db.alarms.count
       ```

       ```
       ({"threshold_name" : "UDB_DB_Pool_Hit_Rat_Pct_Crit_2"})
       ```

     - Essa consulta conta eventos abertos e fechados no MongoDB:

       ```
       db.alarms.count()
       ```

  2. Execute esse comando para obter os resultados para a consulta no arquivo `event-query.js`: **`/opt/ibm/mongodb/bin/mongo 127.0.0.1:27000/alarm -u user -p mongoUsrpasswd@08 <event-count.js`**.
- Limite a quantidade de CPU especificada para monitoramento de log. Para obter mais informações, consulte "Variáveis de ambiente de monitoramento de arquivo de log" na página 637.

Monitoramento de Disponibilidade

Com o IBM Cloud Availability Monitoring, é possível criar, editar, visualizar e excluir testes sintéticos que imitam o comportamento do usuário final em seus aplicativos da web.

O painel Monitoramento de Disponibilidade exibe informações de disponibilidade e de tempo de resposta para aplicativos monitorados, URLs e APIs de REST. Use o painel para monitorar alertas e atividades que estão associadas ao aplicativo, à URL ou à API de REST em locais diferentes usando gráficos, tabelas de detalhamento e visualizações de mapas.

O Monitoramento de Disponibilidade está disponível para usuários da oferta do IBM Cloud Application Performance Management, Advanced on Cloud com o complemento do Monitoramento de Disponibilidade.

Sobre o Monitoramento de Disponibilidade

Use o Monitoramento de Disponibilidade para criar testes sintéticos que monitoram a disponibilidade e o desempenho de aplicativos da web de diferentes locais públicos e privados todos os dias.

Crie testes com o Monitoramento de Disponibilidade. Configure os testes a serem executados em intervalos definidos e locais escolhidos. Faça download e implemente seus próprios pontos customizados de presença (PoPs) em servidores locais ou privados. Execute testes de 15 PoPs públicos nos locais a seguir:

Asia
Chennai, Hong Kong, Cingapura e Tóquio

Austrália
Melbourne

Europa
Amsterdã, Frankfurt, Londres e Paris.

América Central
México

América do Norte
Dallas, San Jose, Toronto e Washington D.C.

América do Sul
São Paulo

Quando tiver criado e configurado os testes, em seguida, você poderá visualizar os dados de disponibilidade e desempenho para os aplicativos no painel do Monitoramento de Disponibilidade.

O Monitoramento de Disponibilidade possui os recursos-chave a seguir:

Inicie em menos de 5 minutos
Crie facilmente testes de ação única para monitorar o desempenho e a disponibilidade do aplicativo da web em minutos.

Maximize o tempo de atividade e a satisfação do usuário
Monitore frequentemente o tempo de atividade e o tempo de resposta dos aplicativos a partir de vários locais geográficos. Execute testes sintéticos para medir o desempenho do carregamento do website e das chamadas API. Monitore os scripts Selenium que você usa para imitar fluxos de usuários de localizações diferentes.

Seja proativo
Receba notificações para alertá-lo sobre problemas antes que eles impactem os usuários. É possível usar o serviço integrado do Alert Notification para criar políticas de alerta que reduzem o ruído de alerta.

Identificar as razões para a falha com precisão e rapidez
A análise em cascata o ajuda a identificar a etapa exata quando uma falha ocorreu e o motivo para a falha; por exemplo, links quebrados, imagens muito grandes, consultas lentas ou solicitações externas. As capturas de tela são criadas automaticamente para ajudá-lo a diagnosticar falhas do navegador e problemas de desempenho históricos. Faça download de relatórios de disponibilidade mensal, semanal e diária e médias de tempo de resposta para os seus testes.

Para trabalhar no Monitoramento de Disponibilidade, você deve ser um membro de uma função que tenha permissão de visualização para o aplicativo que você deseja monitorar. Para obter mais informações, consulte “Funções e permissões” na página 1002.

Acessando o Monitoramento de Disponibilidade

A guia Monitoramento de Disponibilidade **Visão Geral de Status** para seu aplicativo exibe informações de resumo sobre a disponibilidade e o status de seus testes. É possível acessar o painel do Monitoramento de Disponibilidade a partir da guia **Visão Geral de Status** do Monitoramento de Disponibilidade.

Sobre Esta Tarefa

Acesse a página de resumo do Monitoramento de Disponibilidade clicando em um aplicativo elegível na área de janela **Todos os meus aplicativos** no Application Performance Dashboard. Na página de resumo, é possível incluir testes para seu aplicativo, visualizar testes existentes para o aplicativo e visualizar o painel do Monitoramento de Disponibilidade.

Procedimento

Para acessar o Monitoramento de Disponibilidade, conclua as etapas a seguir:

1. Clique no ícone **Desempenho**; depois, clique em **Application Performance Dashboard**.

2. Na área de janela **Todos os meus aplicativos**, clique em um aplicativo que você deseja monitorar e, em seguida, clique em **Monitoramento de disponibilidade** na área de janela **Grupos**.

   Se nenhum aplicativo estiver listado, você deverá criar um aplicativo. Assegure-se de selecionar **Aplicativo Customizado** como o **Modelo**. Para obter mais informações, consulte "Gerenciando aplicativos" na página 1098.

   A guia **Visão Geral de Status** do Monitoramento de Disponibilidade exibe três calibradores que mostram a Disponibilidade Média do Teste nas últimas 24 horas, o Status Atual do Teste em todos os testes e o Uso de Serviço de sua alocação para o plano atual.

   É possível configurar como o Monitoramento de Disponibilidade calcula a Disponibilidade média do teste selecionando testes para inclusão no **Cálculo de disponibilidade**. Clique no ícone de seta  no gráfico Disponibilidade média de teste para visualizar seus cartões de teste; em seguida, clique em **Cálculo de disponibilidade**. Clique em um cartão para incluí-lo ou removê-lo do cálculo. Os cartões de teste excluídos ficam sem cor. Quando tiver concluído, clique em **Terminei**. O gráfico Disponibilidade média do teste é atualizado.

   É possível visualizar o status de todos os seus testes clicando no ícone de seta no gráfico Status do teste atual. Os cartões de teste são exibidos. Clique em um cartão para acessar o painel **Detalhamento** para esse teste em específico.
3. Clique em **Ver Detalhes do Monitoramento** para acessar o painel do Monitoramento de Disponibilidade e visualizar os dados para todos os testes para o aplicativo. Clique em **Visualizar Todos os Testes** para visualizar e editar os testes na área de janela **Testes sintéticos**. Clique em **Incluir Novo Teste** para criar um teste.

   Nota: A primeira vez que você executar o Monitoramento de Disponibilidade, deverá incluir um teste antes que possa visualizar os dados no painel do Monitoramento de Disponibilidade.

Criando e configurando testes

Crie e configure testes que relatem a disponibilidade e o desempenho de seus aplicativos da web.

Crie e configure testes para monitorar a disponibilidade e o tempo de resposta de seus aplicativos frequentemente a partir de vários locais geográficos. Execute testes sintéticos para medir o desempenho do carregamento do website e das chamadas API de REST. Crie testes de comportamento de script para executar e monitorar scripts Selenium que imitam fluxos do usuário a partir de diferentes locais.

Criando um teste de API de REST

Crie um teste de API de REST para testar o tempo de resposta e a disponibilidade do aplicativo da web usando os métodos de HTTP a seguir: GET, POST, PUT e DELETE.

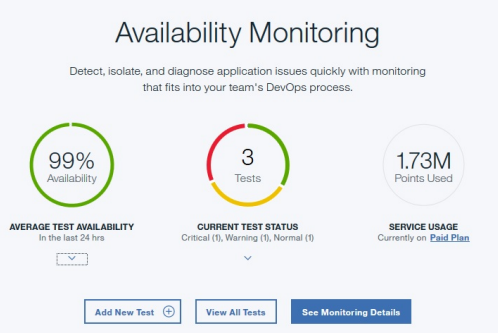
Sobre Esta Tarefa

Use testes de API de REST para monitorar a disponibilidade e o desempenho do aplicativo da web e outras URLs em resposta às chamadas de REST.

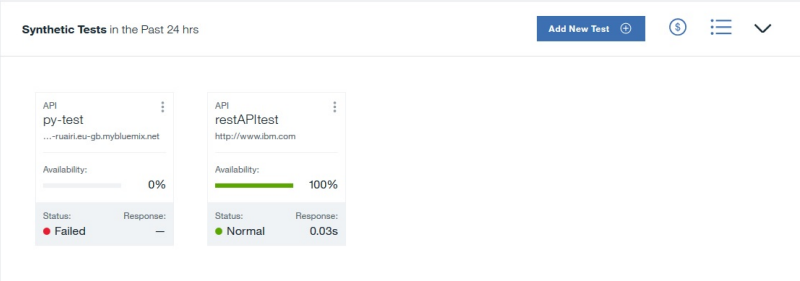
Procedimento

Para criar um teste de API de REST, conclua as etapas a seguir.

1. Se estiver visualizando a página de resumo do Monitoramento de Disponibilidade para seu aplicativo, clique em **Incluir novo teste**.



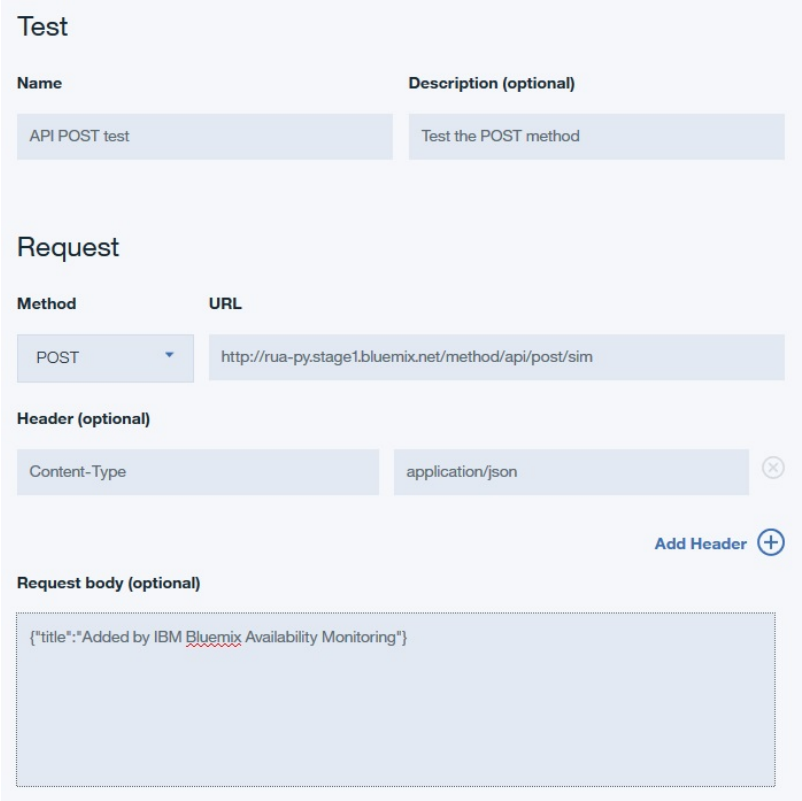
Se estiver visualizando o painel do Monitoramento de Disponibilidade, clique em **Incluir novo teste** na área de janela **Testes sintéticos**.



2. Clique em **Ação única** na página **Configuração de monitoramento**; em seguida, clique em **API de REST** na página **Ação única**.
3. Insira um nome significativo para o seu teste no campo **Nome**. Inclua uma descrição do propósito de seu teste no campo **Descrição**.
4. Na seção **Solicitação**, selecione o tipo de método na lista de **Métodos** e insira uma **URL** que você deseja testar com esse método.

   É possível escolher **GET**, **PUT**, **POST** ou **DELETE**. Se você escolher o método **PUT** ou **POST**, será possível inserir o conteúdo de corpo para testar no campo **Corpo da solicitação (opcional)**.

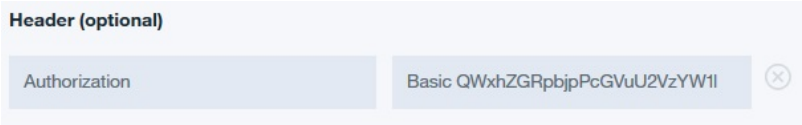
   Por exemplo, o teste de API de REST a seguir usa o método POST para solicitar que seu app da web aceite dados, além de testar a disponibilidade e o desempenho desse aplicativos da web.



5. Opcional: Configure o teste para incluir um cabeçalho e valor específicos. Insira um nome de cabeçalho e valor de cabeçalho nos campos de **Cabeçalho**.

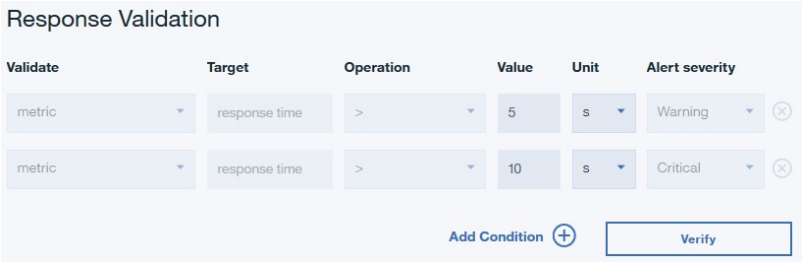
   Se o aplicativo da web que você deseja testar requerer um login de usuário e senha, insira `"Autorização"` no campo **Nome do Cabeçalho**. Insira a palavra "Básico", um caractere de espaço e o valor codificado base64 de seu *username:password* no campo de **Valor de cabeçalho**.

   Por exemplo, se o seu nome de usuário for *Aladdin* e sua senha for *OpenSesame*, em seguida, insira a palavra "Basic", um caractere de espaço, e o valor codificado base64 para *Aladdin:OpenSesame* no campo **Valor do Cabeçalho**.



6. Configure o aviso e os limites de alerta crítico para o seu teste na seção **Validação de resposta**. Edite o **Valor** e a **Unidade** para cada linha.

   Os tempos de resposta que excedem o seu aviso e os limites críticos acionam alertas.



7. Opcional: Clique em **Incluir condição** para definir e incluir condições de validação de resposta customizadas.

   As condições de validação de resposta customizadas são avaliadas em conjunto para gerar um alerta. É possível definir e incluir até seis condições customizadas para o seu teste.

   Importante:

Em Monitoramento de Disponibilidade, cada teste pode gerar até um total de três alertas. Seu teste relata o alerta com a maior severidade até que todas as condições que causem alertas sejam resolvidas. Para obter mais informações, consulte “Geração de alertas no Monitoramento de disponibilidade” na página 1059.

É possível validar os dados a seguir:

Código de resposta de cabeçalho
Selecione **Código de resposta de cabeçalho** para testar um código de resposta ou um intervalo de códigos de resposta de HTTP.

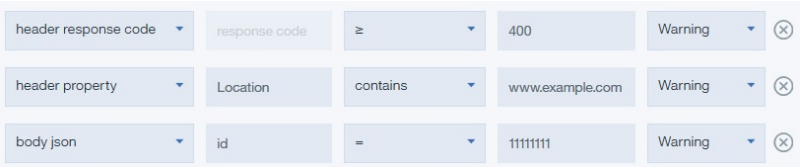
Propriedade de cabeçalho
Selecione **Propriedade de cabeçalho** para testar para uma propriedade e valor específicos do campo de cabeçalho de HTTP.

Corpo JSON
Selecione **Corpo JSON** para testar uma propriedade específica a partir de um corpo JSON.

Para cada condição, insira uma propriedade para a qual testar no campo de **Destino** e um valor a ser testado no campo de **Valor**. Selecione um operador no menu suspenso **Operação**. Finalmente, escolha uma **Severidade do alerta** de Aviso ou Crítico para a sua condição.

Importante:

Os valores numéricos que você insere no campo de **Valor** são tratados como números, e não sequências, por padrão. Para inserir um **Valor** para uma condição de validação de resposta, use aspas "" para distinguir entre uma sequência e um número. Por exemplo, para testar a sequência 123, insira `"123"` no campo **Valor**. Para verificar o número 400, insira `400` sem aspas.



8. Clique em **Verificar** para criar o seu teste de API de REST e para determinar se a sua solicitação de teste é válida.

   O Monitoramento de Disponibilidade determina a validade do teste usando o método de HTTP selecionado e os cabeçalhos da solicitação definidos para o teste. Nenhuma validação de resposta ocorre durante a verificação de teste.

   O seu teste validado é exibido na tabela **Itens verificados**. É possível incluir mais URLs repetindo as etapas 3 a 8.
9. Para definir as suas configurações de teste, clique em **Avançar**.

   Um resumo da configuração de teste é exibido. A mensagem a seguir é exibida para as configurações padrão:

   ```
   O teste ocorrerá: a cada 15 minutos a partir de três locais públicos e
   nenhum local privado simultaneamente para determinar se o teste excede o
   limite especificado.
   ```
10. Na área de janela **Configurações**, clique em **Editar** para exibir as configurações atuais para o seu teste.

    É possível atualizar as seguintes configurações:

    - **Intervalo** define com que frequência o teste é executado.
    - **Frequência de teste** determina se o teste é executado em todos os locais simultaneamente ou em um local diferente a cada intervalo. Selecione **Simultâneo** para executar o seu teste em todos os locais simultaneamente ou selecione **Escalonado** para executar o seu teste de um local selecionado diferente a cada intervalo.
    - **Locais** determina os locais em que seu teste será executado

11. Selecione seus locais da lista de **Locais públicos**. Para selecionar um local privado do qual executar o teste, você deve primeiro instalar e configurar um PoP privado na máquina a partir da qual deseja executar o teste. Para obter mais informações, consulte "Instalando e configurando locais de PoP privado" na página 1056.
12. Clique em **Salvar** para concluir a configuração de seu teste; em seguida, clique em **Concluir**.

    O painel Monitoramento de Disponibilidade é exibido. Após um minuto, o painel exibe informações e dados para o novo teste.

Criando um teste de página da web

Crie um teste da página da web para testar a disponibilidade do aplicativo da web e monitorar quanto tempo leva para que a página seja aberta.

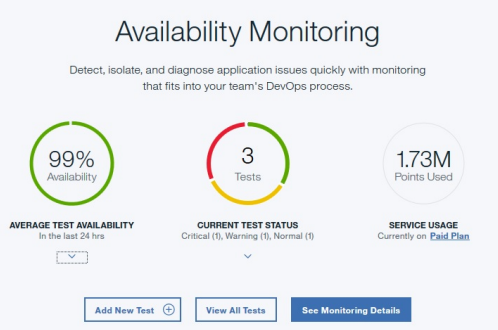
Sobre Esta Tarefa

Os testes da página da web relatam o tempo de resposta para carregar a URL do aplicativo da web. Crie um teste da página da web para monitorar a disponibilidade e o tempo de resposta do aplicativo da web.

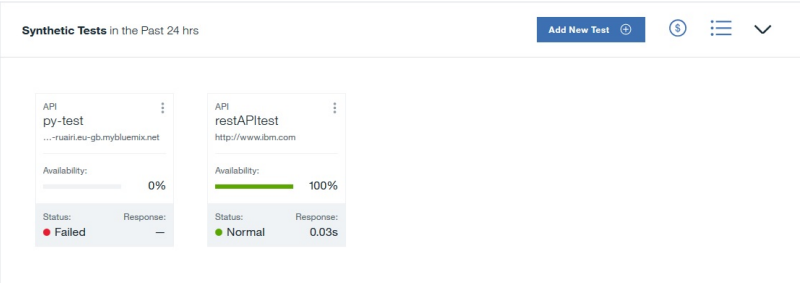
Procedimento

Para criar um teste de página da web, conclua as etapas a seguir.

1. Se estiver visualizando a página de resumo Monitoramento de Disponibilidade, clique em **Incluir novo teste**.

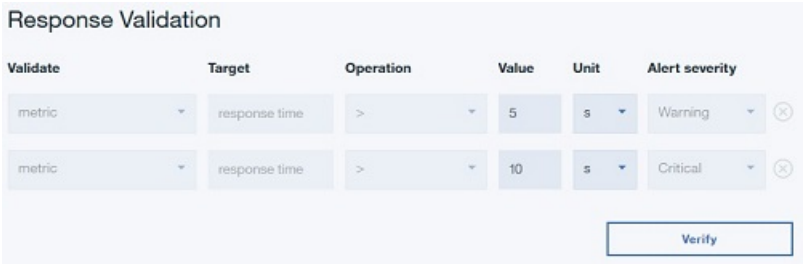


   Se estiver visualizando o painel do Monitoramento de Disponibilidade, clique em **Incluir novo teste** na área de janela **Testes sintéticos**.



2. Clique em **Ação única** na página **Configuração de monitoramento**; em seguida, clique em **Página da web** na página **Ação única**.
3. Insira um nome significativo para o seu teste no campo **Nome**. Inclua uma descrição do propósito de seu teste no campo **Descrição**.
4. Insira a **URL** do aplicativo da web que deseja testar.
5. Configure o aviso e os limites de alerta crítico para o seu teste na seção **Validação de resposta**. Edite o **Valor** e a **Unidade** para cada linha.

   Os tempos de resposta que excedem o seu aviso e os limites críticos acionam alertas.



6. Use a **Lista de bloqueio** e a **Lista de desbloqueio** para especificar para quais URLs e domínios enviar solicitações e com quais URLs e domínios contribuir para as métricas e o status de seus testes de aplicativo. Inclua URLs e domínios que você deseja incluir ou bloquear na **Lista de desbloqueio** e na **Lista de bloqueio**.

   Para obter mais informações, consulte "Bloqueando e filtrando com a lista de desbloqueio e a lista de bloqueio" na página 1054.
7. Clique em **Verificar** para criar seu teste de página da web e para determinar se a sua solicitação de teste é válida.

   O Monitoramento de Disponibilidade determina a validade do teste enviando uma solicitação GET para sua URL de teste. Nenhuma validação de resposta ocorre durante a verificação de teste.

   O seu teste validado é exibido na tabela **Itens verificados**. É possível incluir mais URLs repetindo as etapas 3 a 7.
8. Para definir as suas configurações de teste, clique em **Avançar**.

   Um resumo da configuração de teste é exibido. A mensagem a seguir é exibida para as configurações padrão:

   ```
   O teste ocorrerá: a cada 15 minutos a partir de três locais públicos e
   nenhum local privado simultaneamente para determinar se o teste excede o
   limite especificado.
   ```

   O uso estimado e número estimado de testes por mês são exibidos com base em sua configuração de teste atual.
9. Na área de janela **Configurações**, clique em **Editar** para exibir as configurações atuais para o seu teste.

   É possível atualizar as seguintes configurações:

   - **Intervalo** define com que frequência o teste é executado.
   - **Frequência de teste** determina se o teste é executado em todos os locais simultaneamente ou em um local diferente a cada intervalo. Selecione **Simultâneo** para executar o seu teste em todos os locais simultaneamente ou selecione **Escalonado** para executar o seu teste de um local selecionado diferente a cada intervalo.
   - **Locais** determina os locais em que seu teste será executado

   Selecione os locais na lista de **Locais públicos**. Para selecionar um local privado do qual executar o teste, você deve primeiro instalar e configurar um PoP privado na máquina a partir da qual deseja executar o teste. Para obter mais informações, consulte "Instalando e configurando locais de PoP privado" na página 1056.

   Clique em **Salvar** para concluir a configuração do seu teste.
10. Clique em **Concluir**.

    O painel Monitoramento de Disponibilidade é exibido. Após um minuto, o painel exibe informações e dados para o novo teste.

Criando um teste de script por meio de um script transferido por upload

Faça upload de um script do Selenium para criar um teste de script que testa a disponibilidade e o desempenho do aplicativo da web em resposta ao comportamento do usuário simulado.

Antes de Iniciar

Para criar um script de teste, deve-se, primeiramente, criar um script do Selenium. Para obter mais informações sobre a criação de scripts do Selenium, consulte Gravação de scripts sintéticos.

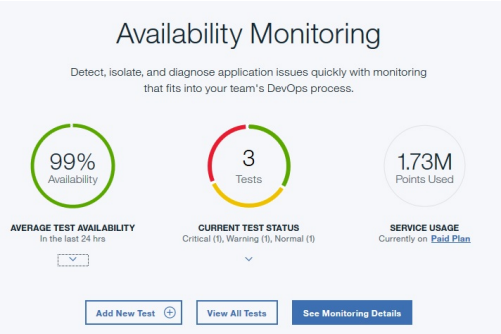
Sobre Esta Tarefa

Crie um teste de script para monitorar um script do Selenium que simula as interações de usuários com o aplicativo da web. Se você criar um script do Selenium que imita um usuário que está efetuando login no aplicativo, você poderá executar um teste de script periodicamente para testar o desempenho do aplicativo em resposta às ações do usuário simulado.

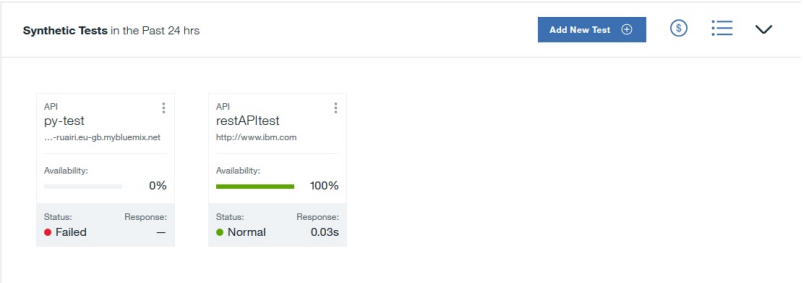
Procedimento

Para criar um teste de script, conclua as etapas a seguir.

1. Se estiver visualizando a página de resumo Monitoramento de Disponibilidade, clique em **Incluir novo teste**.



   Se estiver visualizando o painel do Monitoramento de Disponibilidade, clique em **Incluir novo teste** na área de janela **Testes sintéticos**.



2. Clique em **Comportamento em script** na página **Configuração de monitoramento**. A página **Configuração de comportamento em script** é exibida. Clique em **Carregar arquivo**.

   Se você retornar para editar esse teste em um momento posterior, será possível fazer download do arquivo de script transferido por upload. Clique no ícone **Download** para fazer download do seu script.

3. Insira um nome significativo para o seu teste no campo **Nome**. Inclua uma descrição do propósito de seu teste no campo **Descrição**.
4. Clique em **Procurar** para localizar e fazer upload de um arquivo de script.
5. Use a **Lista de bloqueio** e a **Lista de desbloqueio** para especificar para quais URLs e domínios enviar solicitações e com quais URLs e domínios contribuir para as métricas e o status de seus testes de aplicativo. Inclua URLs e domínios que você deseja incluir ou bloquear na **Lista de desbloqueio** e na **Lista de bloqueio**.

   Para obter mais informações, consulte “Bloqueando e filtrando com a lista de desbloqueio e a lista de bloqueio” na página 1054.

6. Para definir as suas configurações de teste, clique em **Avançar**.

   Um resumo da configuração de teste é exibido. Por exemplo, a mensagem a seguir é exibida para as configurações padrão:

```
O teste ocorrerá: a cada 15 minutos a partir de três locais públicos e
nenhum local privado simultaneamente para determinar se o teste excede o
limite especificado.
```

O uso estimado e número estimado de testes por mês são exibidos com base em sua configuração de teste atual.

7. Na área de janela **Configurações**, clique em **Editar** para exibir as configurações atuais para o seu teste.

   É possível atualizar as seguintes configurações:

   - **Intervalo** define com que frequência o teste é executado.
   - **Frequência de teste** determina se o teste é executado em todos os locais simultaneamente ou em um local diferente a cada intervalo. Selecione **Simultâneo** para executar o seu teste em todos os locais simultaneamente ou selecione **Escalonado** para executar o seu teste de um local selecionado diferente a cada intervalo.
   - **Limite crítico** define o tempo de resposta para alertas críticos do teste.
   - **Limite de aviso** define o tempo de resposta para alertas de aviso do teste.
   - **Locais** determina os locais onde seu teste é executado.

   Selecione os locais na lista de **Locais públicos** que são exibidos por padrão. Para selecionar um local privado do qual executar o teste, você deve primeiro instalar e configurar um PoP privado na máquina a partir da qual deseja executar o teste. Para obter mais informações, consulte “Instalando e configurando locais de PoP privado” na página 1056.

   Se necessário, é possível inserir os valores para variáveis que estão definidas em seu script de teste. Por exemplo, se o seu script requerer um nome de usuário e uma senha para se conectar a um site, será possível inserir os valores para essas variáveis. É possível configurar valores diferentes para suas variáveis em locais diferentes na tabela **Variáveis de script**.

   Clique em **Salvar** para concluir a configuração do seu teste.

8. Clique em **Concluir**.

   O painel Monitoramento de Disponibilidade é exibido. Após um minuto, o painel exibe informações e dados para o novo teste.

Bloqueando e filtrando com a lista de desbloqueio e a lista de bloqueio

Use a lista de desbloqueio e a lista de bloqueio para determinar para quais recursos enviar solicitações e quais recursos contribuem para as métricas e o status de seus testes de aplicativos. As listas de desbloqueio e as listas de bloqueio estão disponíveis somente para testes de página da web e de comportamento em script.

Os campos **Lista de desbloqueio** e **Lista de bloqueio** definem os recursos que seu teste pode ou não pode acessar e os recursos que contribuem para as métricas e o status de seus testes. A Lista de desbloqueio e a Lista de bloqueio controlam quais dependências e recursos contribuem para os tempos de resposta de seus aplicativos da web testados, como métricas de terceiros. É possível configurar suas listas de desbloqueio e de bloqueio quando você criar um teste de página da web ou de comportamento em script.

É possível usar a **Lista de desbloqueio** para definir domínios e URLs permitidos; em seguida, use a **Lista de bloqueio** para bloquear elementos específicos de seus locais permitidos.

Sintaxe

Use vírgulas (,) para separar itens na Lista de bloqueio e na Lista de desbloqueio. Use o símbolo curinga (*) para filtrar elementos de cada URL ou domínio.

Lista de desbloqueio

Inclua URLs, esquemas ou domínios que você deseja incluir em solicitações e cálculos de métricas no campo Lista de desbloqueio. É possível listar até 10 itens em sua Lista de desbloqueio. Cada

comprimento de item não pode exceder 200 caracteres. Todos os domínios, esquemas e URLs que não correspondem aos itens em sua lista de desbloqueio são bloqueados.

Por exemplo: `ibm.com, *developerworks*, *.s81c.com/*, https://www.ibm.com*, https://*`

Nota: Se o filtro de URL da lista de desbloqueio incluir `http://` ou `https://`, você deve incluir o símbolo curinga (*) diretamente após a URL, por exemplo, `https://www.ibm.com*`.

Lista de bloqueio

Inclua URLs, esquemas ou domínios que você deseja bloquear de solicitações e de cálculos de métricas no campo Lista de bloqueio. É possível listar até 20 itens em sua Lista de bloqueio. Cada comprimento de item não pode exceder 200 caracteres.

Por exemplo: `*.profile.*.cloudfront.net/*.png, http://*`

Nota: Se o filtro de URL da lista de bloqueio incluir `http://` ou `https://`, você deve incluir o símbolo de curinga (*) diretamente após a URL, por exemplo, `https://www.ibm.com*`.

Comportamento de filtragem e bloqueio

Os testes podem ter uma Lista de desbloqueio e uma Lista de bloqueio. Ao determinar quais locais são permitidos ou bloqueados, a Lista de bloqueio sempre substituirá a Lista de desbloqueio. A tabela a seguir exibe o comportamento de filtragem e bloqueio para todos os cenários que envolvem a Lista de desbloqueio e a Lista de bloqueio.

Tabela 253. Filtrando e bloqueando o comportamento para a Lista de desbloqueio e a Lista de bloqueio

Lista de bloqueio	Lista de desbloqueio	Comportamento	Razão
Vazio	Vazio	Permitir acesso	Não foram inseridas regras de filtragem.
Vazio	A URL não corresponde à entrada da lista	Bloquear acesso	A URL não está na lista de desbloqueio.
Vazio	A URL corresponde à entrada da lista	Permitir acesso	A URL está na lista de desbloqueio. Nenhuma entrada da lista de bloqueio para bloquear o acesso.
A URL não corresponde à entrada da lista	Vazio	Permitir acesso	A URL não está na lista de bloqueio. Não há nenhuma entrada da lista de desbloqueio para impedir o acesso a URLs que não estão na lista de desbloqueio.
A URL corresponde à entrada da lista	Vazio	Bloquear acesso	A URL está na lista de bloqueio.
A URL não corresponde à entrada da lista	A URL não corresponde à entrada da lista	Bloquear acesso	A URL não está na lista de desbloqueio.
A URL não corresponde à entrada da lista	A URL corresponde à entrada da lista	Permitir acesso	A URL está na lista de desbloqueio. A URL não está na lista de bloqueio.

Tabela 253. Filtrando e bloqueando o comportamento para a Lista de desbloqueio e a Lista de bloqueio (continuação)

Lista de bloqueio	Lista de desbloqueio	Comportamento	Razão
A URL corresponde à entrada da lista	A URL não corresponde à entrada da lista	Bloquear acesso	A URL não está na lista de desbloqueio. A URL está na lista de bloqueio.
A URL corresponde à entrada da lista	A URL corresponde à entrada da lista	Bloquear acesso	A URL está na lista de bloqueio. A entrada da lista de bloqueio substitui a entrada da lista de desbloqueio.

Instalando e configurando locais de PoP privado

Faça download e instale um PoP privado em uma máquina local; em seguida, configure o PoP privado para uso como um local para os testes no Monitoramento de Disponibilidade.

Antes de Iniciar

Para instalar um PoP privado, o local de instalação para o PoP privado deve preencher os requisitos a seguir:

- O Linux é instalado com um kernel versão 3.1.0 ou superior.
- O serviço Docker versão 1.7.1 ou superior é instalado e iniciado.
- O espaço em disco disponível é de 4 GB ou mais.
- A memória disponível é de 2 GB ou mais.
- Núcleos de CPU:
  - Se você precisar somente de reproduções de API de REST no PoP privado, tenha pelo menos 2 núcleos de CPU disponíveis.
  - Se quiser executar reproduções de página da web e reproduções de script no PoP privado, tenha 1 núcleo de CPU para cada 1 ou 2 testes para executar a cada minuto.
- Verifique o uso de memória e CPU do PoP privado antes e depois de incluir novos testes e após aplicar atualizações de software do PoP privado que incluam versões atualizadas do Firefox ou Selenium IDE, pois versões posteriores podem ter requisitos de sistema superiores.

A melhor prática para determinar quando incluir núcleos de CPU é executar os processos mais exigentes no host do PoP privado para obter o uso de CPU e o uso de memória: se o uso total de CPU for maior que 70% e o principal processo de uso de CPU for Firefox, inclua núcleos de CPU até que o uso total de CPU fique abaixo de 50%; se a memória livre no host do PoP privado for menor que 500 MB, aumente a memória.

Se você não tiver mais recursos de hardware, mas quiser que o PoP privado seja executado sem exceção, execute essas etapas para reduzir a contagem de instâncias em execução paralela do Firefox (faz com que seus testes sejam executados com intervalos mais longos do que o configurado na UI, pois o recurso de hardware não pode executar muitos testes):

1. Edite o elemento script `start-pop.sh` para incluir a variável de ambiente **MAX_TASKPOOL_SIZE**, inserindo os núcleos de CPU disponíveis no host do PoP privado como valor e, em seguida, execute **stop-pop.sh** seguido por **start-pop.sh**.
2. Configure os testes para um intervalo mais longo na UI.

Você deve ter acesso de usuário à interface da linha de comandos (CLI) da máquina na qual deseja instalar o PoP privado. Você também deve ter as permissões de usuário necessárias para incluir pacotes no Docker.

Importante:

- Certifique-se de que o horário do sistema da máquina na qual deseja executar um PoP privado esteja e permaneça sincronizado com o horário padrão. Caso contrário, suas instâncias de teste exibirão registros de data e hora incorretos no painel do Monitoramento de Disponibilidade.
- O PoP privado do Monitoramento de Disponibilidade é totalmente suportado para as seguintes plataformas: Red Hat Enterprise Linux 7.4 e CentOS Linux 7.4.

Sobre Esta Tarefa

Além dos locais públicos, é possível implementar Pontos de Presença (PoPs) privados ao criar ou editar um teste no Monitoramento de Disponibilidade. Use PoPs privados para testar aplicativos que estão localizados atrás do firewall da empresa, como aplicativos com maior privacidade ou requisitos de segurança. É possível registrar no máximo 50 locais privados no Monitoramento de Disponibilidade. Faça download do script de pré-verificação e do pacote de PoP privado; em seguida, salve o script e o pacote na máquina em que você deseja executar o PoP privado.

Procedimento

1. Crie um teste ou edite um teste existente.

   Para criar um teste, clique em **Incluir Novo Teste** na área de janela **Testes sintéticos**. Para editar um teste, clique em **Ações** ; em seguida, clique em **Editar**. Se você estiver criando um teste, configure e verifique o teste. Na seção **Configurações**, clique em **Editar**.

   Para obter mais informações, consulte “Criando um teste de API de REST” na página 1047, “Criando um teste de página da web” na página 1051 e “Criando um teste de script por meio de um script transferido por upload ” na página 1052.
2. Clique em **Editar** na seção **Configurações** para exibir a seção **Locais**; em seguida, clique em **Locais Privados**. Se você estiver editando um teste anterior, clique em **Locais Privados** na seção **Locais**.

   Se você instalou anteriormente um ou mais PoPs privados, uma lista de todos os PoPs privados instalados será exibida. Se nenhum PoP privado estiver instalado e configurado, o Monitoramento de Disponibilidade poderá orientá-lo a configurar um PoP privado.
3. Clique em **Fazer download de pré-verificação** e salve o script de pré-verificação para uma máquina da qual deseja executar testes.

   Importante: Deve-se extrair e executar scripts a partir da interface da linha de comandos (CLI) para instalar um PoP privado. Os scripts e o pacote de PoP privado podem ser instalados em uma máquina diferente e acessados por meio da CLI para essa máquina. Não feche ou atualize o Monitoramento de Disponibilidade em seu navegador enquanto estiver trabalhando com scripts de PoP privado, ou você perderá todas as configurações de teste não salvas.

   Abra uma CLI para a máquina em que deseja localizar o PoP privado. Na CLI, navegue para o local onde salvou o script de pré-verificação; em seguida, execute o script de pré-verificação da maneira a seguir:

   ```
   ./precheck.sh
   ```

   Assegure-se de que tenha as permissões necessárias para executar shell scripts em sua máquina.

   O script de pré-verificação exibe o resultado da verificação. Se o seu ambiente reprovar a verificação, atualize sua máquina para atender aos requisitos exibidos.
4. Retorne para Monitoramento de Disponibilidade, clique em **Fazer Download do Pacote** e salve o pacote. Mova o pacote para a máquina na qual deseja executar os testes. Na CLI, navegue para o local onde salvou o pacote de download; em seguida, execute o seguinte comando para extrair o pacote:

   `tar -xvf` *`Availability_Monitoring_PoP.tar`*

   Em que *Availability_Monitoring_PoP.tar* é o nome do arquivo `.tar` que contém o pacote do PoP privado que foi transferido por download.
5. Configure o PoP privado. Na CLI, execute o script a seguir:

```
./config-pop.sh
```

Quando solicitado, insira as seguintes informações para seu PoP privado:

- Nome do PoP
- Local do país
- Local da cidade
- Latitude do PoP
- Longitude do PoP
- Descrição do PoP

6. Se algum dos testes de API de REST se conectar a um servidor que usa um certificado autoassinado ou não for assinado por um provedor de certificado de autoridade de certificação conhecido, coloque todos os certificados de autoridade de certificação confiáveis no formato de arquivo `.pem` no diretório `keyfiles`.

   Nota:

   - Quaisquer mudanças nos arquivos de certificado `.pem` requerem que o PoP privado seja reiniciado.
   - O servidor sendo testado deve enviar todos os certificados, exceto o certificado de autoridade de certificação raiz, durante o handshake TLS; se isso não acontecer, corrija a configuração do servidor, se possível. Caso contrário, é possível incluir quaisquer certificados ausentes no diretório `keyfiles`, conforme descrito nesta etapa. Entretanto, o teste (ou testes) do PoP pode não refletir a experiência de outros clientes.

7. Para configurar seu PoP privado para usar um servidor proxy ao executar testes de página da web ou testes de comportamento com script, insira uma das opções a seguir:

   Importante: Testes da API de REST que são executados a partir de sua localização de PoP privado com uma configuração de proxy manual ou automática não usam esse proxy. Somente os testes de página da web e comportamento com script podem usar um servidor proxy para execução a partir dos locais PoP privados.

   no
   Insira `não` para configurar seu PoP privado para não usar um proxy ao executar testes.

   Manual
   Insira `manual` para configurar manualmente um endereço IP proxy e o número da porta para seu proxy de PoP privado para uso ao executar testes. O script solicita o endereço IP do servidor proxy e o número da porta no seguinte formato: *`ip address:port number`*. Também é possível criar uma lista sem proxies para bloquear elementos de domínio, nomes de host ou elementos de endereço IPv4. Quando solicitado, insira um ou mais elementos de domínio ou elementos de endereço IPv4. Separe cada item da lista com um espaço em branco ou com uma vírgula (","). O operador curinga (*) não é suportado.

   - Para bloquear um domínio e quaisquer subdomínios, insira um sufixo de domínio, iniciando com um ponto, por exemplo: `.example.org, example.org`.
   - Para bloquear uma rede, insira um endereço IP com um sufixo CIDR para identificar um intervalo de endereços IP para bloquear, por exemplo: `10.0.0.0/8`.

   Pac
   Insira `ucp` para configurar seu PoP privado para usar uma URL de configuração automática de proxy. Quando solicitado pelo script, insira a URL de configuração automática de proxy.

   As configurações do PoP privado são salvas no arquivo `pop.properties`.

8. Inicie o PoP privado. Na CLI, execute o script a seguir:

   ```
   ./start-pop.sh
   ```

   Quando o PoP privado estiver em execução, ele poderá ser localizado pelo Monitoramento de Disponibilidade.

9. Retorne ao Monitoramento de Disponibilidade e clique em  **Atualizar Locais** para localizar e exibir seu novo PoP privado.

   O PoP privado é listado em uma tabela.
10. Para escolher o PoP privado como um local para o teste, marque a caixa de seleção para a linha da tabela que contém um PoP privado. Para excluir um PoP privado, conclua as seguintes etapas:
    a) Na CLI, execute o script **./stop-pop.sh** na máquina na qual o PoP privado está localizado.
    b) Retorne ao Monitoramento de Disponibilidade e clique em  **Excluir** na linha da tabela que contém o PoP privado que deseja excluir.
11. Repita as etapas 3 a 10 para incluir PoPs privados adicionais em diferentes máquinas para seleção como locais no Monitoramento de Disponibilidade. Clique em **Concluir** para salvar e iniciar o teste.

    O painel Monitoramento de Disponibilidade é exibido. Depois de aproximadamente 1 minuto, o painel exibe informações e dados para seu novo teste.
12. Opcional: Para fazer upgrade de um PoP privado existente, conclua as seguintes etapas:
    a) Faça download do novo pacote de PoP privado em uma nova pasta e, em seguida, use o comando **tar -xvf** para descompactar o novo PoP nessa pasta.
    b) Na CLI, mude o diretório para a pasta na qual seu PoP privado antigo está localizado. Execute o script a seguir para parar o PoP privado antigo:

       ./stop-pop.sh
    c) No diretório em que seu antigo PoP privado está localizado, faça backup de seus arquivos `system.properties` e `pop.properties` existentes.

       Importante: O arquivo `system.properties` contém informações críticas que permitem que seu PoP privado se conecte ao Servidor Cloud APM. O arquivo `pop.properties` contém os dados de configuração para seu PoP privado. Se desejar manter essa configuração, certifique-se de preservar os arquivos `pop.properties` e `system.properties` para seu antigo PoP privado antes de fazer upgrade de seu PoP privado.
    d) Copie todos os arquivos da nova pasta de seu PoP privado, exceto `pop.properties` e `system.properties` e substitua os arquivos onde seu antigo PoP privado está localizado.
    e) Se precisar reconfigurar seu PoP privado atualizado, execute o script a seguir a partir da CLI:

       ./config-pop.sh
    f) Execute **./start-pop.sh** na CLI para iniciar o PoP privado atualizado.
    g) Retorne ao Monitoramento de Disponibilidade e clique em  **Atualizar Locais** para localizar e exibir seu PoP privado atualizado.

Geração de alertas no Monitoramento de disponibilidade

No Monitoramento de Disponibilidade, os testes podem gerar um total de até três alertas. Seu teste relatará o alerta com a maior severidade até que a condição que causa o alerta seja resolvida.

Um alerta separado é criado para três situações diferentes:

- Quando o tempo de resposta de seu aplicativo da web ou da URL exceder os limites de aviso ou críticos configurados para o seu teste. Cada teste mede o tempo de resposta por padrão e levanta um alerta com base no aviso e nos limites críticos para esse teste.
- Quando o teste retorna um código de resposta de HTTP que indica que seu aplicativo da web ou URL está indisponível devido a um erro do cliente ou servidor. Cada teste verifica o código de resposta por padrão, para determinar se o teste é bem-sucedido ou falha.
- Quando o seu teste determina que uma ou mais condições customizadas estão satisfeitas, um alarme é levantado com a gravidade mais alta conforme definido por uma ou mais de suas condições customizadas. O Monitoramento de Disponibilidade considera todas as condições customizadas em

conjunto ao determinar se um alarme é levantado. Esse alarme permanece até que o teste determine que nenhuma de suas condições customizadas geram mais aviso ou alertas críticos.

Quando mais de um alerta for levantado, o Monitoramento de Disponibilidade relatará o alerta com a maior severidade enquanto os alertas estiverem presentes.

Por exemplo, se você incluir uma condição customizada que cria um alerta crítico e outra condição customizada que cria um alerta de aviso, um alerta crítico é gerado pelo teste. Esse alerta é visível no painel Monitoramento de Disponibilidade. Se a condição que causar um alerta crítico não for mais verdadeira, então a gravidade de seu alerta de teste mudará para "aviso". Um alerta permanecerá até que nenhuma condição cause mais um alerta.

Visualizando a disponibilidade e o desempenho do app no painel Monitoramento

É possível visualizar os detalhes da disponibilidade e do desempenho do aplicativo, juntamente com alertas e os testes associados no painel Monitoramento de Disponibilidade.

O painel do Monitoramento de Disponibilidade é dividido nas áreas de janela a seguir:

- Sumarização do aplicativo
- Frequência do alerta
- Testes sintéticos
- Tempo de Resposta e Disponibilidade

Use o menu suspenso **Navegar para** 

para navegar rapidamente para qualquer área de janela.

Use as guias para ajudá-lo a aprender sobre os recursos do Monitoramento de Disponibilidade. Para abrir uma guia, clique no ícone **Ajuda**  ; em seguida, clique no guia que deseja visualizar.

Vídeo da biblioteca do tutorial
A biblioteca de tutoriais de Vídeo contém vídeos sobre como criar testes do Monitoramento de Disponibilidade, criar scripts de teste com Selenium IDE e enviar alertas.

Bem-vindo ao Monitoramento!
A guia Bem-vindo ao Monitoramento destaca as áreas do painel e explica cada recurso do Monitoramento de Disponibilidade.

É possível acessar o painel **Detalhamento** por meio da área de janela Resumo do aplicativo, da área de janela Frequência de alertas, da área de janela Testes sintéticos ou da área de janela Tempo de resposta e disponibilidade. O painel **Detalhamento** exibe informações estatísticas chave para suas instâncias de teste.

É possível mudar a ordem das áreas de janela para atender as suas necessidades. Para mover uma área de janela, clique no título e arraste a área de janela para uma posição diferente. Para salvar essas mudanças, de forma que elas persistam após você efetuar logout, clique em **Salvar layout**.

É possível configurar o painel para ser atualizado automaticamente a cada minuto. Clique no ícone **Configurar**  ; em seguida, clique na barra deslizante **Atualizar** para selecionar **1 minuto**. Para atualizar sua página a qualquer momento, clique em **Atualizar**.

Sumarização do aplicativo
A área de janela Resumo do Aplicativo exibe uma visão geral do status de alerta nas últimas 24 horas e informações de status do teste atual.

A área de janela Resumo do aplicativo exibe as informações a seguir:

- **Status atual** exibe o status de maior severidade de todos os seus testes. A severidade pode ser Normal, Aviso ou Crítico.
- **Alertas** exibe o número de alertas abertos e os divide em aviso e alertas críticos.

- O **Relatório de Disponibilidade** permite fazer download de um relatório de arquivo `.csv` das médias de tempo de resposta e disponibilidade mensal, semanal e diária para o aplicativo. Clique no ícone **Relatório**  para fazer download do relatório.

Frequência do alerta
O painel **Frequência de alertas** contém um mapa que exibe os alertas mais recentes. Os alertas são agrupados por local e listados na tabela **Alertas**.

Mapa de frequência de alerta

O mapa **Frequência de alerta** exibe informações em uma visão rápida para todos os pontos de presença (PoPs) públicos ou privados para os testes.

Use a função de zoom para ampliar qualquer área do mapa ou para restaurá-lo para o seu tamanho original. Passe o mouse sobre cada local para visualizar o nome desse local e o número de avisos e alertas críticos nesse local. É possível filtrar os alertas que são exibidos no mapa selecionando **Todos**, **Abertos** ou **Fechados** na lista suspensa **Alertas**.

Locais de PoP

Ícones **Local de PoP** 

indicam os locais de PoP para os seus testes. A cor de cada **Local de PoP** representa a severidade do alerta mais recente em cada local: ícone Normal 

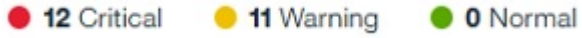
, ícone Aviso 

ou ícone Crítico 

. Um ícone de **Local de PoP** animado indica que esse local tem a maioria dos alertas com o nível mais alto de severidade de todos os locais para as suas instâncias de teste.

Inclua locais de PoP no teste selecionado passando o mouse sobre o ícone **Local de PoP Inativo**  e clicando em **Testar Aqui**. A página **Testar modo de edição** é exibida para o seu teste selecionado. É possível selecionar um teste no menu suspenso **Teste** na área de janela **Tempo de resposta** e **Disponibilidade**.

Locais de PoP privados são representados por ícones **Local de PoP Privado** 

Número de alertas
Os ícones de **Local de PoP** exibem o número de alertas abertos e encerrados ou todos que sejam gerados em cada local. Os ícones **Crítico**, **Aviso** e **Normal**


exibem o número de alertas de cada severidade para seus locais.

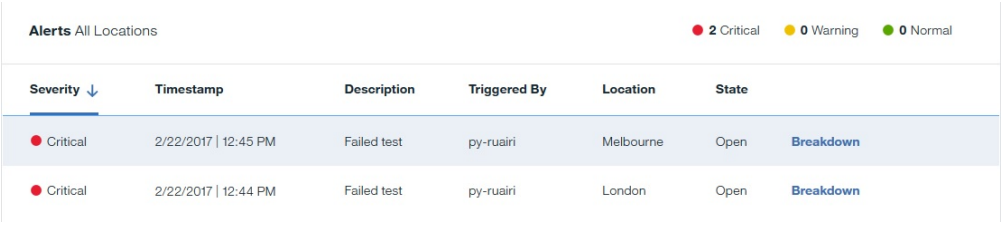
Testes com falha
Os locais nos quais ocorrem os testes com falha são indicados por um ícone **Local de PoP** com um ícone de borda quebrada 

.

Use a função de zoom para ampliar qualquer área do mapa ou para restaurá-lo para o seu tamanho original. Passe o mouse sobre cada local para visualizar o nome desse local e o número de avisos e alertas críticos nesse local. É possível filtrar os alertas que são exibidos no mapa selecionando **Todos**, **Abertos** ou **Fechados** na lista suspensa **Alertas**.

Tabela Alertas

Os alertas para todos os locais são exibidos em uma tabela.



A tabela exibe as informações a seguir sobre seus alertas:

- **Severidade** descreve o alerta como crítico ou aviso.
- **Registro de data e hora** mostra o horário em que o alerta é criado.
- **Descrição** resume o desempenho de sua instância de teste.
- **Acionado por** mostra o nome do teste que acionou o alerta.
- **Local** indica onde o problema ocorreu.
- **Estado** mostra se o alerta está aberto ou fechado.

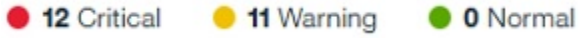
Visualizando Detalhes de Alerta

Cada alerta na tabela contém um link para o painel **Detalhamento**. Use o painel de detalhamento para ajudá-lo a resolver o problema que causou o alerta.

Filtrando alertas

Para filtrar alertas para um determinado local, clique em um ícone **Local de PoP** no mapa. Para mostrar alertas para todos os locais, clique em qualquer lugar no mapa que não seja um ícone **Local de PoP**.

Para filtrar os alertas na tabela por severidade, clique nos ícones **Crítico**, **Aviso** ou **Normal**



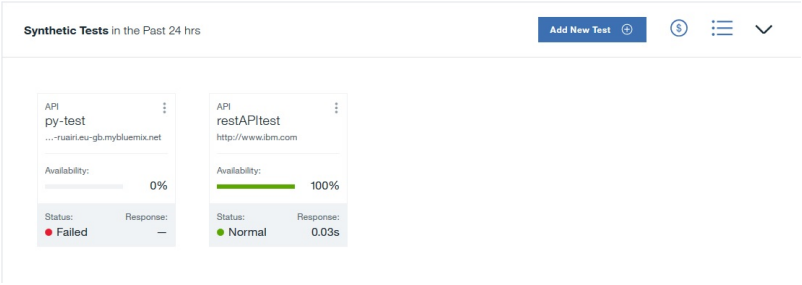
. Para remover o filtro e incluir alertas de cada severidade na tabela, clique novamente no ícone selecionado.

Mudando os limites de alerta

Os alertas são acionados por limites que você especifica ao criar um teste. Na maioria dos casos, eles são gerados devido a falhas de disponibilidade ou tempos de resposta lentos. Para alterar as configurações de limite, clique no ícone **Ações** no teste que gerou o alerta na área de janela **Testes sintéticos** e clique em **Editar**.

Testes sintéticos

Na área de janela **Testes sintéticos**, é possível criar, editar, excluir e visualizar *testes sintéticos* que monitoram o desempenho e a disponibilidade dos aplicativos. Os testes são exibidos em uma visualização de lista ou de cartão na área de janela **Testes sintéticos**.



Cada cartão de teste exibe informações sobre o teste:

Disponibilidade
Exibe a porcentagem de disponibilidade do teste nas últimas 24 horas.

Estado
Exibe o status atual do teste. O status pode ser Crítico, Aviso, Normal, Falha, Inativo ou Desconhecido.

Média Resposta
Exibe o tempo médio de resposta do teste nas últimas 24 horas.

É possível monitorar três tipos diferentes de teste:

API REST
Relata o tempo de resposta de uma chamada REST. Todos os formatos de solicitação de HTTP, tais como GET, POST, PUT e DELETE são suportados.

Página da Web
Relata o tempo de resposta para carregar o website na URL que você inserir.

Comportamento do script
Monitora scripts Selenium que você cria para imitar as interações de um usuário com um website. Por exemplo, é possível criar um script Selenium que imita um usuário que está efetuando login no seu aplicativo. Execute esse script periodicamente para testar o desempenho do seu aplicativo em resposta às ações do usuário que são automatizadas pelo script. Para obter mais informações sobre a criação de scripts do Selenium, consulte “Registrando scripts sintéticos” na página 1027.

Para incluir outro teste, clique em **Incluir novo teste**.

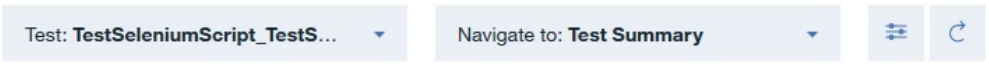
Para parar, iniciar, excluir ou editar um teste sintético, clique em **Ações** ícone e clique na ação desejada. Para visualizar os detalhes em **Detalhamento** do teste, clique no teste.

Para visualizar o uso específico de cada teste sintético, clique em **Custo** ícone . Se estiver inscrito no plano pago, seu uso será exibido nos pontos de dados.

Pane
O painel **Detalhamento** exibe informações estatísticas chave para os seus testes. O painel também resume informações de disponibilidade e de tempo de resposta, tendências históricas e dados de desempenho de teste nas últimas 24 horas.

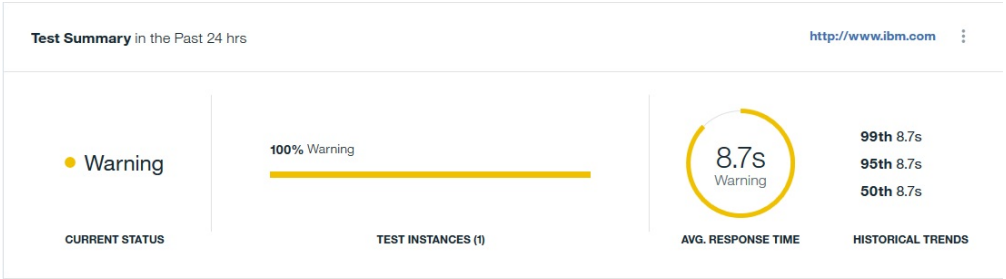
Para visualizar um detalhamento detalhado de um teste, clique no teste na área de janela **Testes sintéticos**. Também é possível abrir o painel **Detalhamento** clicando em **Detalhamento** na tabela **Alerta** na área de janela Frequência de alertas.

Use o menu suspenso **Testar** para visualizar os detalhamentos de diferentes testes. Use o menu suspenso **Navegar para** para navegar rapidamente para qualquer área de janela.



O painel Detalhamento exibe quatro áreas de janela.

Resumo de Teste

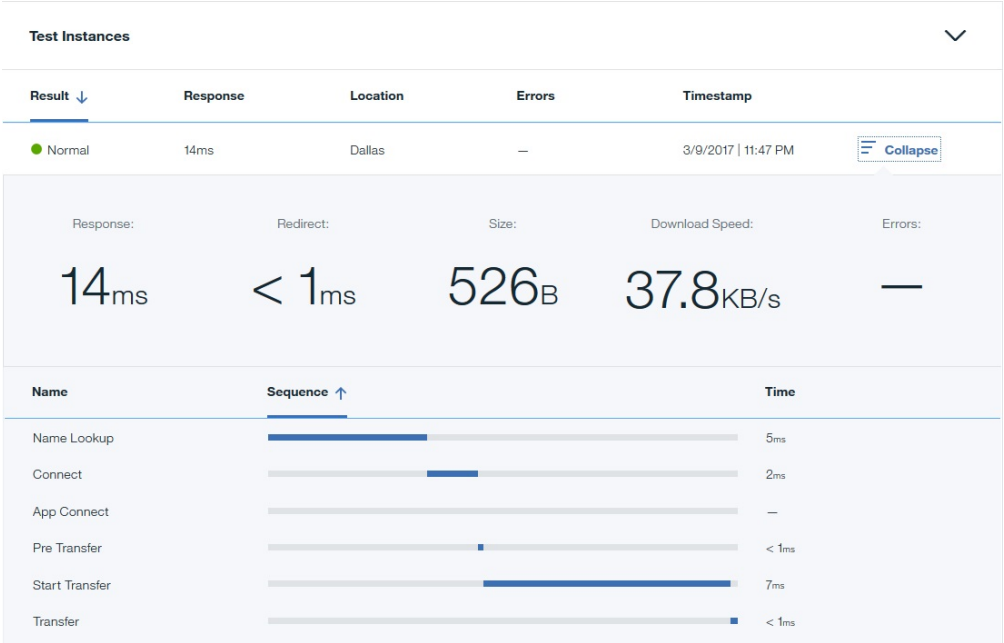


A área de janela **Resumo do teste** exibe as informações de teste a seguir para as últimas 24 horas:

- **Status atual** exibe o status de teste.

- **Instâncias de teste** exibe um detalhamento de porcentagem de instâncias de teste normais, de aviso e críticas.
- **Tempo médio de resposta** exibe o tempo médio de resposta do teste.
- **Tendências históricas** exibe as tendências históricas do desempenho do seu teste para o 50º, 95º e 99º percentis em segundos ou milissegundos.

Instâncias de Teste



A tabela **Instâncias de teste** exibe informações detalhadas sobre cada instância de teste, incluindo o status, o tempo de resposta, o local onde o teste foi executado, o número de erros e o registro de data de hora de quando o teste foi executado. Para realizar drill down em uma instância de teste, clique em **Expandir**. As informações de resposta detalhadas são listadas para cada etapa na instância de teste. É possível classificar quaisquer colunas para ajudar a identificar rapidamente a etapa exata em que uma lentidão ou falha ocorreu. A visualização dos erros, a sequência de teste e o tempo de resposta ajudam a identificar problemas facilmente.

As informações que são exibidas dependem do tipo de teste Sintético que está sendo monitorado:

API

Quando você clicar em **Expandir** para uma instância de teste de API, um resumo de alto nível dos detalhes a seguir será exibido:

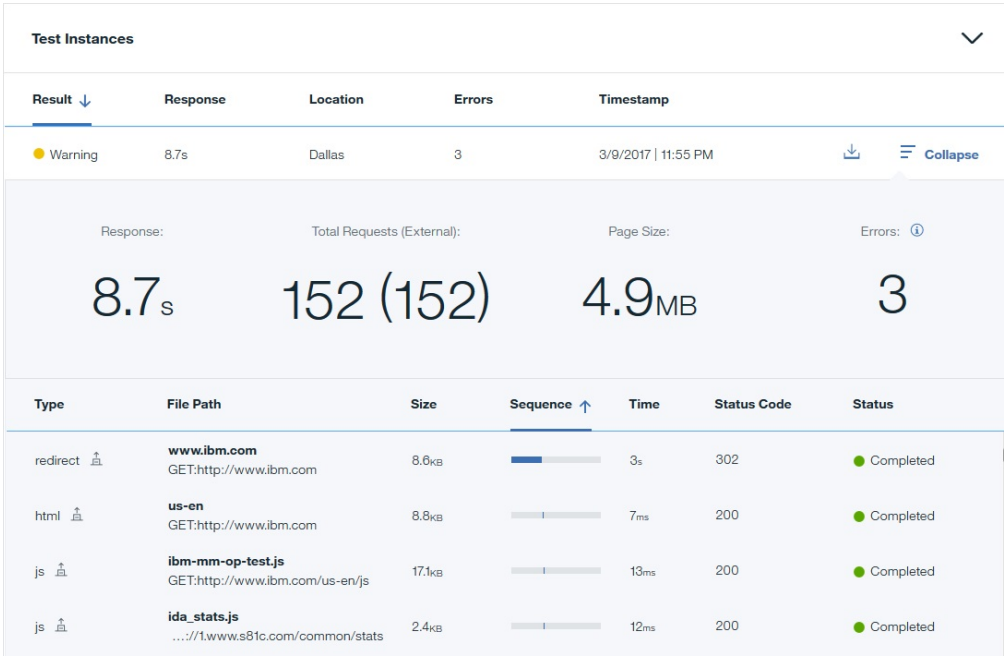
- **Resposta** exibe o tempo de resposta total para a instância de teste, incluindo o tempo de redirecionamento.
- **Redirecionamento** exibe o tempo de redirecionamento total para a instância de teste.
- **Tamanho** exibe o tamanho do objeto.
- **Velocidade de download** exibe a velocidade na qual cada objeto é transferido por download.
- **Erros** exibe o número de erros que ocorreram durante a instância de teste. Para visualizar os detalhes do erro, clique no ícone **Informações**.

Uma tabela exibe cada etapa na chamada API, juntamente com o nome da etapa, a sequência de etapas e o tempo de resposta para cada etapa. Os nomes de etapa a seguir são exibidos:

- **Consulta de nome** representa o tempo que a instância de teste levou para resolver o nome do objeto.
- **Conectar** representa o tempo que a instância de teste levou desde o início da etapa até a conclusão de uma conexão com o host remoto ou proxy.

- **Conexão do app** representa o tempo que a instância de teste levou desde o início da etapa até a conclusão da conexão SSL com o host remoto.
- **Pré-transferência** representa o tempo que a instância de teste levou desde o início da etapa até pouco antes do início do comando de transferência de arquivos.
- **Iniciar transferência** representa o tempo que a instância de teste levou desde o início da etapa até o primeiro byte ser recebido.
- **Transferência** representa o tempo que a instância de teste levou para transferir o arquivo.

Página da Web



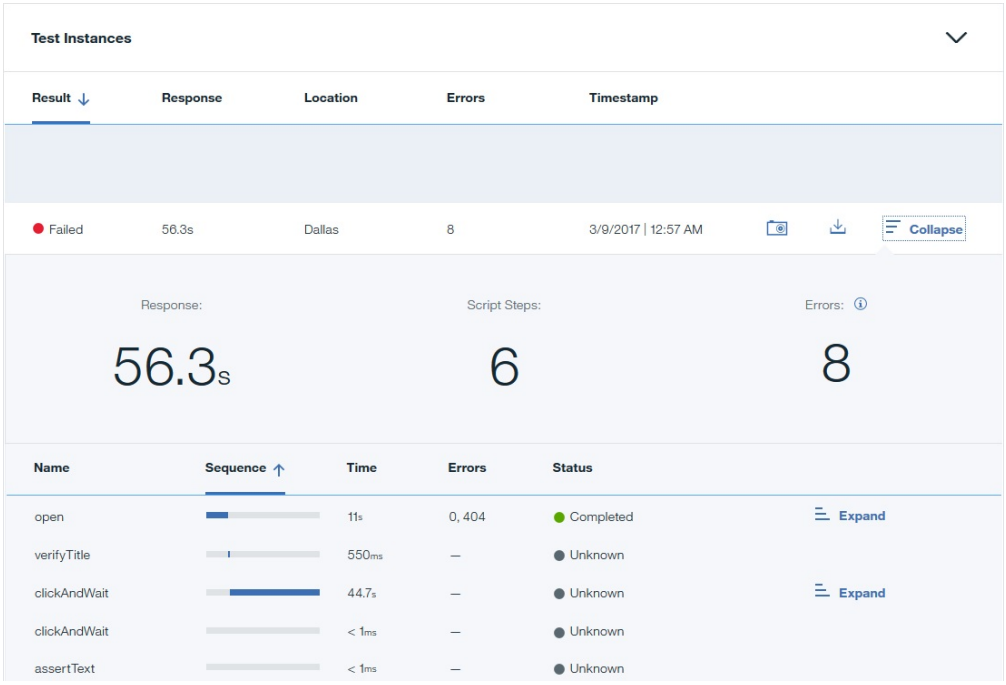
Quando você clicar em **Expandir** para uma instância de teste da página da web, um resumo de alto nível dos detalhes a seguir será exibido:

- **Resposta** indica o tempo de resposta para a instância de teste.
- **Total de solicitações (externas)** exibe o número total de solicitações para a instância de teste. O número de solicitações externas está entre parênteses.
- **Tamanho da página** exibe o tamanho da página da web.
- **Erros** exibe o número de erros que ocorreram durante a instância de teste. Para visualizar os detalhes do erro, clique no ícone **Informações**.

Uma tabela que lista os detalhes a seguir para cada solicitação que é feita pelo teste também será exibida:

- **Tipo** exibe o tipo de solicitação, por exemplo, HTML, CSS, JavaScript ou imagem. Solicitações externas e internas são representadas por ícones.
- **Caminho do arquivo** descreve o local do objeto solicitado.
- **Tamanho** exibe o tamanho do objeto solicitado.
- **Sequência** exibe a sequência de solicitações que são feitas pelo teste.
- **Tempo** exibe o tempo que cada solicitação leva.
- **Código de status** exibe o código de status da solicitação HTTP.
- **Status** descreve o resultado da solicitação, por exemplo, Concluído, Desconhecido ou Com falha.

Script

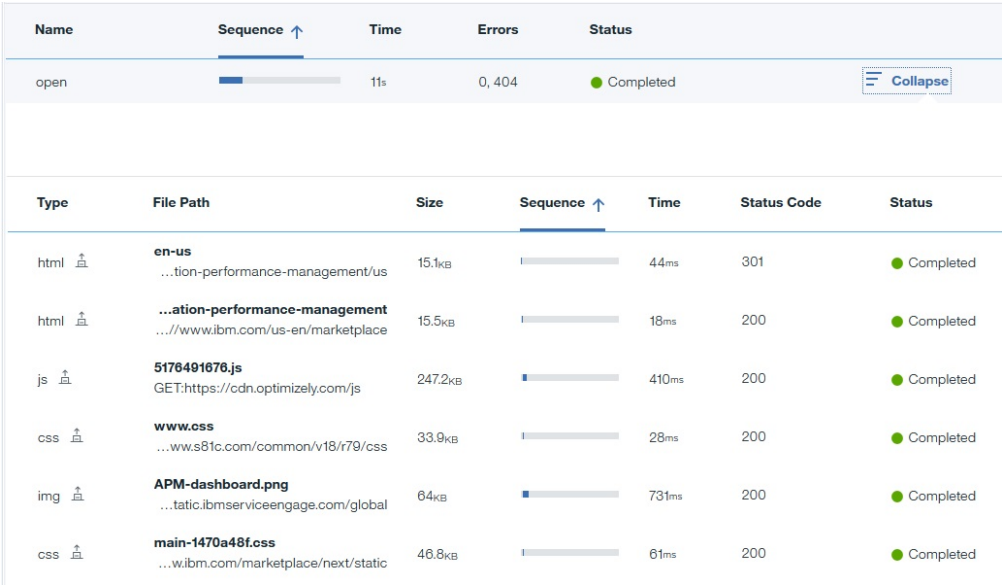


Quando você clicar em **Expandir** para uma instância de teste de script, o tempo de resposta, o número de etapas do script e o número de erros serão exibidos. Para visualizar os detalhes do erro, clique no ícone **Informações**.

Os detalhes a seguir para cada etapa de script serão exibidos em uma tabela:

- **Nome** exibe cada comando Selenium que é chamado por sua instância de teste, por exemplo `Open`, `ClickAt` ou `VerifyBodyText`.
- **Sequência** exibe a sequência de etapas do script desde o início até o fim da instância de teste.
- **Tempo** exibe o tempo que cada etapa do script leva.
- **Erros** exibe o número de erros que ocorreram durante cada etapa do script.
- **Status** descreve o resultado da etapa de script, por exemplo, Concluído, Desconhecido ou Com falha.

É possível realizar drill down e visualizar detalhes sobre as solicitações que são geradas por cada etapa do script.



Clique em **Expandir** para visualizar uma tabela que contém os detalhes a seguir:

- **Tipo** exibe o tipo de solicitação, por exemplo, HTML, CSS, JavaScript ou imagem. Solicitações externas e internas são representadas por ícones.
- **Caminho do arquivo** descreve o local do objeto solicitado.
- **Tamanho** exibe o tamanho do objeto solicitado.
- **Sequência** exibe a sequência de solicitações que são feitas pelo teste.
- **Tempo** exibe o tempo que cada solicitação leva.
- **Código de status** exibe o código de status da solicitação HTTP.
- **Status** descreve o resultado da solicitação, por exemplo, Concluído, Desconhecido ou Com falha.

O Monitoramento de Disponibilidade poderá criar automaticamente uma captura de tela se a página da web falhar ao carregar ou se uma etapa no script falhar. Por exemplo, se uma das etapas em seu script abrir uma página da web, mas ela não for carregada, o Monitoramento de Disponibilidade automaticamente criará uma captura de tela. Para visualizar uma captura de tela da página da web ou script, clique no ícone **Erro de Captura de Tela** . Este recurso está disponível somente para a página da web e os testes com script. Ele não funciona com testes da API de REST.

Também é possível fazer download de um registro do tráfego de rede para uma determinada instância de teste como um arquivo `.har` clicando no ícone **Download** . Esse recurso está disponível a página da web e testes de comportamento com script.

Tempo de Resposta e Disponibilidade

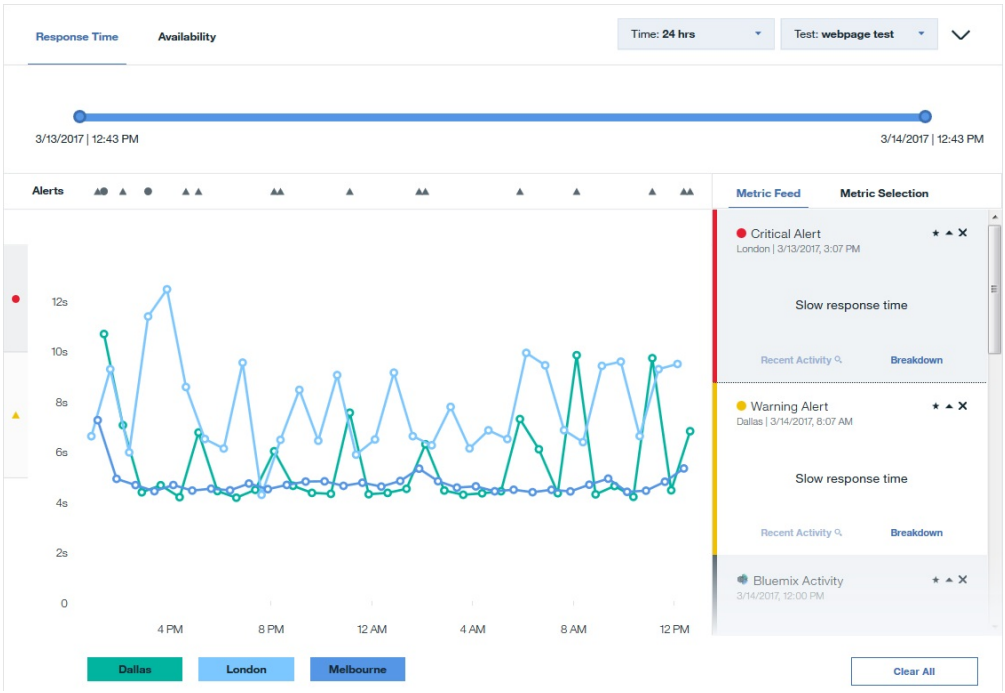
A área de janela **Tempo de resposta e disponibilidade** exibe um gráfico dos tempos de resposta medidos e da disponibilidade para as instâncias de seu teste durante um período definido. Para obter mais informações, consulte "Tempo de Resposta e Disponibilidade" na página 1067.

Tempo de Resposta e Disponibilidade

Use a área de janela **Tempo de Resposta** e **Disponibilidade** para ajudá-lo a visualizar o tempo de resposta, as tendências de disponibilidade e os alertas ao longo do tempo.

Gráfico do Tempo de Resposta

As informações de tempo de resposta são exibidas em um gráfico de linhas. Para visualizá-las, clique na guia **Tempo de resposta**.



Importante: Os tempos de resposta que são medidos por Monitoramento de Disponibilidade são um pouco maiores do que os tempos de resposta que os usuários têm. O Monitoramento de Disponibilidade simula o comportamento do usuário real, que é incluído na medição de tempo de resposta. O tempo de resposta maior é devido aos fatores a seguir:

- O Monitoramento de Disponibilidade cria uma nova instância do Firefox para cada teste para evitar que instâncias de teste anteriores influenciem o teste atual. Os usuários reais podem experimentar tempos de resposta mais rápidos devido ao armazenamento em cache do navegador.
- O Monitoramento de Disponibilidade instala o plug-in do driver da web do Firefox antes de cada teste.

Tempos de resposta individuais para testes são representados por um ícone **Ponto de Resposta** no gráfico de linhas. Diferentes cores indicam diferentes localizações geográficas nas quais o aplicativo está em execução. O eixo y do gráfico usa ícones de alerta para identificar os intervalos de limites de aviso e críticos. O ícone de aviso amarelo representa o intervalo de limites de aviso e o ícone crítico vermelho representa o intervalo de limites críticos. Clique no ícone de aviso amarelo ou no ícone crítico vermelho para identificar facilmente as instâncias de teste que aparecem nos intervalos de limites de aviso e críticos. Para visualizar os detalhes para uma instância de teste específica, clique no ícone **Ponto de Resposta** no gráfico.

Filtros

Escolha um teste no menu suspenso **Teste**. É possível filtrar dados para 3 horas, 24 horas, 7 dias, 30 dias e 12 meses. Ao filtrar por um intervalo de tempo maior que 24 horas, os valores que são exibidos no gráfico são medidos. Para visualizar informações mais específicas, clique no gráfico para realizar drill down nos alertas e avisos individuais. Também é possível usar a régua de controle para restringir ou expandir o intervalo de tempo.

Com o gráfico Tempo de resposta, é possível destacar e ocultar os dados de locais de PoP específicos. Para destacar os dados de tempo de resposta para um local específico, passe o mouse sobre o nome do local PoP; em seguida, clique no ícone **Destacar Local** . Para ocultar dados de horário para um local, passe o mouse sobre o nome do local PoP; em seguida, clique no ícone **Ocultar Local** .

Para restaurar dados da localização de PoP para o gráfico, clique em **Incluir mais localizações** ou a guia **Seleção de métrica** e, em seguida, clique na localização do PoP que você removeu anteriormente.

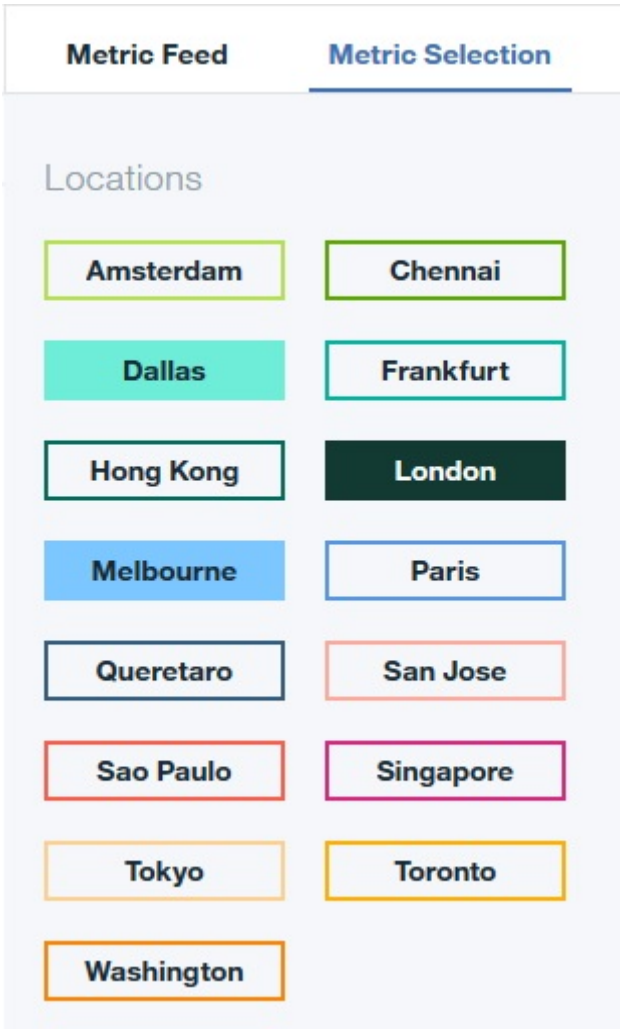
Alertas

É possível identificar facilmente alertas de aviso e críticos na linha Alertas. Passe o mouse sobre um **ícone de alerta** para identificar a severidade e o registro de data e hora do alerta. Clique em um **ícone de alerta** para exibir detalhes para esse alerta no **Feed de métrica**.

Se houver mais de um ícone próximo na linha Alertas, um **ícone de número** exibirá o número de alertas naquele momento. Passe o mouse sobre um **ícone de número** para exibir os alertas individuais e clique em um alerta para visualizar informações no **Feed de métrica**

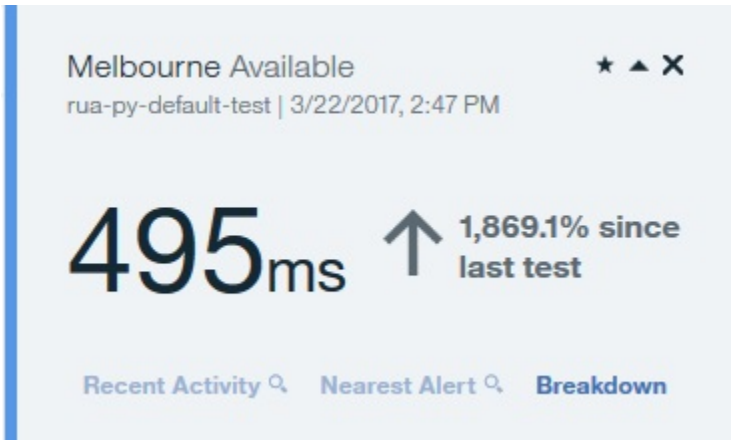
Seleção de métrica e Feed de métrica

Para filtrar para métricas por região geográfica, clique em **Seleção de métrica**. Clique em um local para incluir ou remover métricas que são medidas nesse local por meio do gráfico. Clique em **Incluir mais localizações** para abrir a página Testar modo de edição e incluir uma localização de PoP no seu teste selecionado.

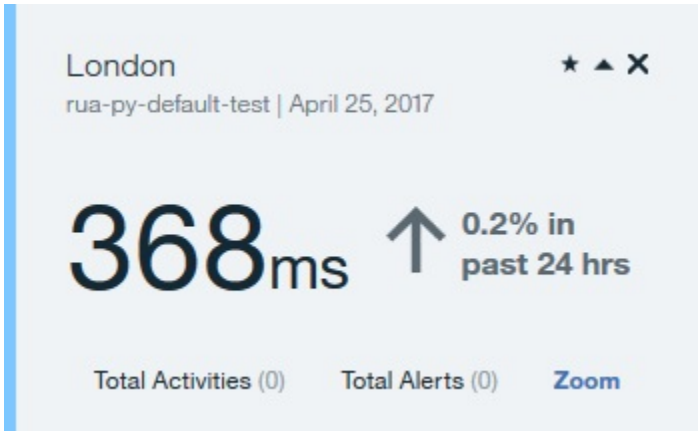


Para visualizar uma lista de detalhes de métrica, clique em **Feed de métrica**. O **Feed de métrica** exibe uma lista de instâncias nas quais uma métrica é preenchida.

Clique no **ícone de alerta** ou no **ponto de resposta** no gráfico para incluir os detalhes dessa métrica no **Feed de métrica**.



Se você filtrar o gráfico Tempo de resposta para um intervalo de tempo maior que 24 horas e clicar em um **ponto de resposta**, será possível ver os detalhes agregados para esse dia no **Feed de métrica**.

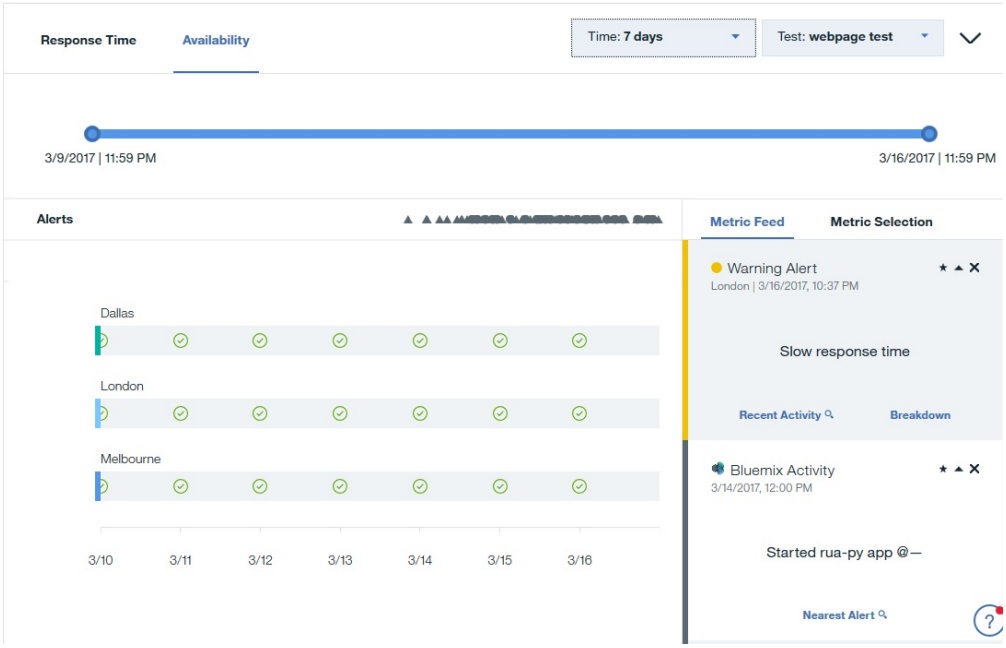


Clique em **Zoom** para visualizar todos os tempos de resposta e alertas que foram gerados pelo teste para esse dia no gráfico Tempo de Resposta.

Para visualizar informações detalhadas sobre um tempo de resposta de alerta ou teste, clique em **Detalhamento** no **Feed de métrica**. Se um alerta ocorrer, clique em **Alerta mais próximo** para visualizar o alerta mais próximo a essa instância de teste no **Feed de métrica**.

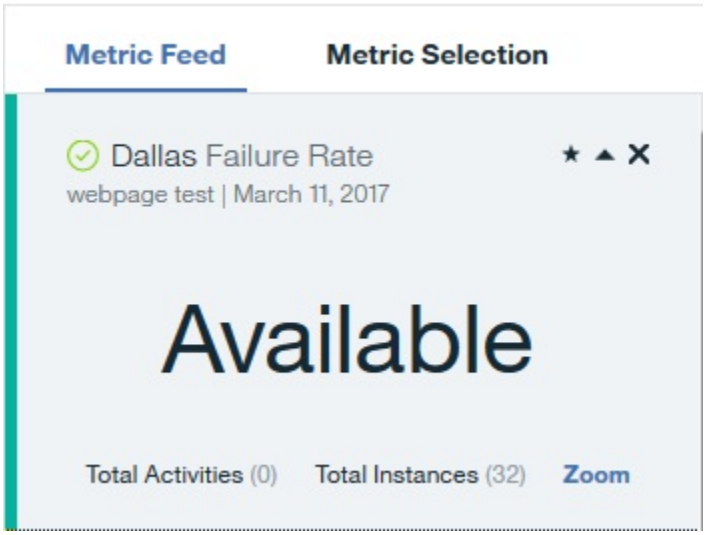
Disponibilidade

Para visualizar as informações de disponibilidade para seus aplicativos, clique em **Disponibilidade**. O gráfico Disponibilidade mostra a disponibilidade diária de cada ponto de presença (PoP) para o teste selecionado.



Com o gráfico Disponibilidade, é possível destacar e ocultar os dados de locais de PoP específicos. Para destacar dados de disponibilidade para um local específico, passe o mouse sobre o nome do local PoP; em seguida, clique no ícone **Destacar Local**  . Para ocultar dados de disponibilidade para um local, passe o mouse sobre o nome do local PoP; em seguida, clique no ícone **Ocultar Local**  . Para restaurar dados da localização de PoP para o gráfico, clique na guia **Seleção de métrica**; em seguida, clique na localização do PoP que você removeu anteriormente.

Passe o mouse sobre um ponto gráfico para exibir a taxa de falha e o número de instâncias de teste para um dia e local específicos. Clique em um ponto gráfico para exibir essas informações no **Feed de métrica**.



Clique em **Zoom** para filtrar o gráfico **Disponibilidade** e o gráfico **Tempo de resposta** para exibir informações para o dia selecionado.

Uso Monitoramento de Disponibilidade

É possível visualizar detalhes sobre seu uso do Monitoramento de Disponibilidade na guia **Monitoramento** na área de janela do aplicativo e no painel principal do Monitoramento de Disponibilidade.

Para ver uma visão geral do seu uso do painel principal do Monitoramento de Disponibilidade, clique no ícone **Configurar**  . Se você for um usuário da avaliação do Monitoramento de Disponibilidade, seu uso será exibido como um gráfico de barras e como uma porcentagem, junto do número de testes em uso. Se você for um usuário do plano Pago, seu uso será exibido nos pontos de dados. É possível visualizar os detalhes de uso para cada teste individual na área de janela **Testes sintéticos**.

Seu uso é medido em pontos de dados. O número estimado de pontos de dados é calculado por meio da fórmula a seguir:

Número estimado de pontos de dados = T * L * (60/M * 24 * 30) por mês

Em que T = número de testes sintéticos que são executados, L = número de locais e M = intervalo entre os testes (minutos).

Testes simples, tais como testes de página da web e de API de REST usam um ponto de dados para cada teste. Testes avançados, tais como scripts Selenium e scripts API de REST usam 100 pontos de dados para cada teste.

Explorando as APIs

Use as APIs do IBM Cloud Application Performance Management para criar scripts para automatizar a migração de seu ambiente do Cloud APM .Na oferta de serviços gerenciados pela API do Cloud APM no API Explorer no IBM developerWorks, é possível acessar e explorar a API de Serviço de Gerenciamento do Grupo de Recursos, a API de Serviço de Gerenciamento de Limites e a API de Serviço de Controle de Acesso Baseado na Função disponíveis.

Antes de Iniciar
É necessário que você possua uma assinatura ativa do Cloud APM para obter uma chave de ID do cliente e executar operações API.

Procedimento

1. Abra o API Explorer em seu navegador: https://developer.ibm.com/api.
2. Conecte-se com seu IBMid.
3. No campo **Procurar todas as APIs**, insira `Gerenciamento de desempenho` e clique no .
4. Selecione o quadro da API do IBM Cloud Application Performance Management.
5. Clique em **Documentação** no lado esquerdo da janela do API Explorer.
6. Selecione a API específica.
7. Selecione a subseção para expandir a lista de operações da API.
8. Para continuar, é necessária uma assinatura do Cloud APM ativa. Execute uma das seguintes etapas:
   a) Se você ainda não tem uma assinatura do Cloud APM, inscreva-se para uma assinatura de teste gratuita de 30 dias.
   b) Se você já tiver uma assinatura, conecte-se clicando em **Minhas APIs** para testar algumas das operações da API no API Explorer.

   Quando sua assinatura está ativa e você está conectado à página do API Explorer, é exibida uma lista de suas assinaturas da API.
9. Selecione uma operação da API para obter mais detalhes.
10. Selecione uma das linguagens (como shell ou curl) na parte superior da página do API Explorer para visualizar um exemplo de solicitação.
11. Recupere sua chave de ID do cliente e sua chave secreta de cliente e armazene-as em um local seguro para uso externo.

    Envie o ID do cliente e as chaves secretas do cliente com cada solicitação da API de tempo. Você deve ter uma assinatura do Cloud APM para concluir esta ação.

O que Fazer Depois
Para obter informações adicionais sobre como executar operações da API, consulte os seguintes tópicos:

"Acessando e usando a API de Serviço de Controle de Acesso Baseado na Função" na página 1011
"Usando a API Serviço de Gerenciamento de Grupo de Recursos" na página 997
"Usando a API do serviço de gerenciamento de limite" na página 999

Configuração Avançada

Use a página **Configuração Avançada** para controlar as configurações de comunicações e os recursos avançados, como encaminhamento de eventos.

Após você clicar no **Configuração do Sistema** > **Configuração Avançada**, as categorias de configuração a seguir serão exibidas na página Configuração Avançada.

Integração de UI
Para produtos que se integram com o Console do Cloud APM, é possível incluir ou editar a URL para ativar o aplicativo integrado. Os campos são preenchidos com qualquer URL que foi enviada durante o procedimento de configuração de integração.

- **URL de análise de log** é usado para ativar o IBM Operations Analytics - Log Analysis para procurar seus logs de aplicativos usando Application Performance Dashboard. Para obter mais informações, consulte "Procurando Arquivos de Log" na página 1081.
- **Ativar eventos de subnó**, para agentes com subnós, controla se os subnós são mostrados na guia Eventos. Quando os eventos de subnó estão ativados, são exibidos o nó e o subnó para os quais um evento é aberto. Especificamente, se você desejar exibir situações de monitoramento do arquivo de log na guia Eventos, deverá assegurar que os Eventos de subnó estejam ativados. Padrão: `False`.
- **Taxa de Atualização de Painel** controla a frequência da atualização automática do Application Performance Dashboard. É possível ajustar a configuração para qualquer valor de 1 a 60 minutos. A configuração afeta o status do recurso que é exibido no navegador e na guia Visão Geral do Status. Ela não afeta as entradas da guia Eventos. Padrão: 1 minuto.

Gerenciador de Eventos

O Gerenciador de Eventos controla o encaminhamento de eventos usando Protocolo Simples de Transporte de Correio, bem como notificações por e-mail. Se você inserir um valor para Endereços de e-mail de destino, será enviado um e-mail para cada evento aberto, fechado e parado. É possível usar os campos do **Gerenciador de Eventos** para configurar seus eventos a partir do Cloud APM para abrir automaticamente chamados no IBM Control Desk. Para tarefas de configuração adicionais, consulte Integrando-se com o Control Desk "Integrando-se ao Control Desk" na página 972.

Se você configurar o encaminhador SMTP para usar SSL, deve incluir o certificado de autoridade de certificação de assinatura do SMTP Server para o keystore do Servidor Cloud APM. Inclua o certificado de autoridade de certificação no keystore usando o comando de keytool da JVM:

```
install_dir/java/jre/bin/keytool -importcert\
-noprompt \
-alias your_CA cert_alias \
-file path_to_your_CA_cert_file (*.cer)
 -keystore /install_dir/wlp/usr/servers/min/resources/security/key.jks \
-storepass ccmR0cKs! \
-storetype jks \
-trustcacerts
```

Para visualizar um email de amostra, consulte "Email de Eventos" na página 1075.

- **Endereços de Email de Destino** especifica os endereços de email para os quais os eventos são encaminhados. Separe cada endereço com uma vírgula (,), como `annette@ibm.com,jim@ibm.com,owen@ibm.com`.
- **Alert Notification for ITMv6** é a opção para ativar eventos do Alert Notification for ITMv6 configurando o valor como `True`. Padrão: `False`

- O **Cloud Event Management Webhook** é a URL do Webhook que é gerada no Gerenciamento de eventos de nuvem ao configurar a integração entre o IBM Cloud Application Performance Management e o Gerenciamento de eventos de nuvem. Deve-se colar a URL do Webhook gerada aqui para que os eventos sejam encaminhados a partir do Cloud APM.

É possível usar o Alert Notification em vez da função de e-mail do Gerenciador de Eventos, que permite controlar quem será notificado para diferentes eventos e como serão notificados. Para obter mais informações adicionais, consulte “Integrando-se ao Alert Notification” na página 971.

Se você estiver encaminhando eventos para um receptor EIF (Event Integration Facility), será possível customizar os slots do EIF, como incluir um atributo ao evento EIF. Para obter mais informações, consulte “Customizando um evento para encaminhar para um receptor EIF” na página 990. Para obter informações sobre como encaminhar eventos para o gerenciador de eventos do IBM Netcool/OMNIbus, consulte o tópico “Integrando-se ao Netcool/OMNIbus” na página 965.

Tracking Analytics Service

As configurações usadas para o Tracking Analytics Service. As configurações aplicam-se somente na oferta do Cloud APM, Advanced e se você estiver configurando o rastreio de transações em seu ambiente.

- **Tamanho do Conjunto de Conexões** é o número de conexões simultâneas do Db2 que o Tracking Analytics Service mantém no conjunto de conexões para as "*N* principais" consultas. Aumente esse valor se estiverem ocorrendo tempos de consulta lentos devido a um grande número de usuários simultâneos do Console do Cloud APM. Padrão: `10`.
- **Pseudonós** permitem a visualização de serviços que não são instrumentados. Padrão: `True`.
- **Tempo limite de consulta, em segundos** é o número de segundos antes de cada consulta "*N* principais" (em que *N* é um número, como "5 principais" ou "10 principais") feita antes do tempo esgotar. O valor de tempo limite pode ser aumentado, se necessário, para aplicativos que possuem uma maior carga de trabalho e possuem maiores tempos de consulta esperados. Padrão: `120` segundos.
- **Nova otimização de consulta DB2 ativada** normalmente não deve precisar de mudança. O parâmetro afeta o otimizador de consulta do Db2. Em alguns ambientes, desligar o otimizador pode melhorar o desempenho de alguns conjuntos de transações. Padrão: `False`.

Agent Subscription Facility

O Agent Subscription Facility inclui interface REST (Representative State Transfer) do agente e servidor Central Configuration Services HTTP. A interface REST é usada por agentes e coletores de dados para enviar dados de monitoramento que são persistidos no Db2 Server e em eventos de limite. O servidor Central Configuration Services HTTP manipula solicitações de agentes para seus arquivos de configuração, como definições de limite. Use esses parâmetros para configurar a comunicação entre o Agent Subscription Facility e o Servidor Cloud APM.

- **Limite de Pesquisa Ausente (Pulsação Rápida)** é o número máximo de vezes que um agente de monitoramento com um intervalo de pulsação de 60 segundos ou inferior falha ao se conectar antes de ser marcado como off-line. Padrão: `30` intervalos.
- **Limite de Pesquisa Ausente (Pulsação Lenta)** é o número máximo de vezes que um agente de monitoramento com um intervalo de pulsação maior que 60 segundos falha ao se conectar antes de ser marcado como off-line. Padrão: 3 intervalos.
- **Tempo Limite da Transação** é a quantia de tempo, em segundos, que o servidor espera por uma resposta para uma solicitação. Padrão: `120` segundos.
- **Remover atraso do sistema off-line** determina o número de minutos para aguardar antes de remover a exibição de um sistema gerenciado que esteja off-line. No Application Performance Dashboard, sistemas gerenciados off-line são indicados pelo indicador de status desconhecido  . O sistema gerenciado continua a ser exibido, mesmo se você desinstalar o agente, até que o tempo de atraso tenha passado. Para obter mais informações, consulte “Visualizando e removendo agentes off-line” na página 1104. Padrão: `5760` minutos (4 dias).

Ativação de níveis
Cada um de seus agentes de monitoramento é fornecido com um conjunto de limites predefinidos que são ativados e iniciados com o agente. Esses limites predefinidos são designados ao grupo de recursos do sistema padrão para o agente.

- **Escolher ação para definir a política para limites predefinidos de melhor prática** controla se os limites predefinidos para seus recursos gerenciados são ativados ou desativados por padrão. Configure o campo como **Desativar todos** se não desejar executar os limites predefinidos. A configuração **Desativar todos** remove a designação do grupo do sistema de todos os limites predefinidos. Um limite sem um grupo designado não é distribuído para nenhum sistema monitorado e permanece parado até que seja distribuído a um grupo de recursos. Posteriormente, se você decidir que deseja ativar os limites predefinidos, configure o campo como **Ativar todos**.

Para obter informações sobre limites predefinidos e limites customizados, consulte "Informações de histórico" na página 976 e "Exemplos de limites desativados" na página 978.

Email de Eventos

Use os campos do Gerenciador de Eventos na página Configuração avançada para configurar a notificação de eventos por email para uma lista de destinatários.

Email de evento aberto
Quando uma condição de limite se torna verdadeira, um evento é aberto e a mensagem de e-mail é enviada pelo Servidor Cloud APM, que contém os atributos de base que se aplicam a todos os eventos de agente e também os atributos da primeira linha do conjunto de dados que corresponderam à condição de limite. O atributo situation_status possui um valor de Y para eventos abertos.

E-mail para eventos próximos
Quando a condição de limite não é mais verdadeira, um evento de fechamento é gerado. A mensagem de e-mail para eventos próximos contém apenas os atributos de base que se aplicam a todos os eventos do agente e o valor de situation_status é N. Os atributos de agente não são incluídos nessas mensagens de e-mail, já que a condição de limite não é atendida.

Email de evento de parada
Quando um limite é interrompido, um evento de parada é gerado. A mensagem de e-mail para eventos de parada contém somente os atributos de base que se aplicam a todos os eventos do agente e o valor de situation_status é P. Os atributos do agente não são incluídos nessas mensagens de e-mail, já que a condição de limite não é atendida.

Um limite será interrompido por um agente se você excluir a definição de limite ou se você fizer uma mudança em qualquer uma das definições de limite que estiverem distribuídas para o agente.

As amostras a seguir exibem um e-mail para um evento aberto:

```
De: noreply@apm.ibmserviceengage.com
Para:         tester@us.ibm.com
Data:    25/10/2017 13h56
Assunto:    Linux_Disk_Space_Low no nc049048 :LZ (Notificação)
O texto abaixo lista as
informações recebidas do agente que acionaram este evento.
Os valores de IP e de Agente identificam o agente que detectou o
evento.
Os valores de Descrição e da Severidade especificam o nome da
definição de limite e sua gravidade.
A seguir há uma descrição de todos os pares de valores de atributo presentes no evento, em seu
formato
bruto.
    Servidor IP: 10.107.76.230 (SIDR26APAP1BLUE.test.ibm.com)
    Agente IP: 9.42.49.48
    Agente      : nc049048:LZ
    Severidade: Aviso
    Descrição: Linux_Disk_Space_Low[Disk_Free_Percent <= 20  AND Disk_Free_Percent > 10
                AND FS_Type != nfs  AND FS_Type != iso9660 ]
      ITM_KLZ_Disk
      ManagedSystemGroups = '*LINUX_SYSTEM'
      TenantID=F43E-D704-DADC-6270-1ED8-543E-A388-6513
      Adapter_host=nc049048.tivlab.raleigh.ibm.com
      Apm_hostname=SIDR26APAP1BLUE.test.ibm.com
      Appl_label = A:P: S
      Date=01/25/2017
```

```
      Disk_free=5843
      Disk_free_percent=20
      Disk_name=/dev/sda2
      Disk_used=22676
      disk_used_percent=80
      File_system_status= 2
      File_system_status_enum=Up
      Fqhostname=nc049048.test.ibm.com
      Fs_type=ext4
      Hostname=nc049048.test.ibm.com
      Identificador = Linux_Disk_Space_Lownc049048:LZ/ITM_KLZ_Disk
      Inodes_free=1721587
      Inodes_free_percent=88
      Inodes_used=232477
      inodes_used_percent=12
      Integration_type=U
      Mount_options=rw
      Ponto_de_montagem = /
      msg='Linux_Disk_Space_Low[Disk_Free_Percent <= 20  AND Disk_Free_Percent > 10  AND FS_Type !
= nfs
     E fs_type! = iso9660 ] '
      Origin=9.42.49.48
      severity=WARNING
      Situation_displayitem = /
      situation_eventdata='disk_name=/dev/
sda2;inodes_used_percent=12;mount_options=rw;fs_type=ext4;
     System_name=nc049048:LZ; mount_point=/; disk_used_percent=80; disk_free=5843;
file_system_status_enum=Up;
     size=30040;disk_used=22676;inodes_used=232477;disk_free_percent=20;file_system_status=2;
     total_inodes=1954064;inodes_free=1721587;timestamp=1170125135553000;inodes_free_percent=88;~'
      Situation_name=Linux_Disk_Space_Low
      Situation_origin=nc049048 :LZ
      Situation_origin_uuid=09fb36afd6b3.22.02.09.2a.31.30.56.9d
      Situation_status=Y
      Situation_thrunode=nc049048 :LZ
      Situation_time= '25.01.2017 13 :55:55.000'
      Situation_type=S
      Size=30040
      source='ITM Agent: Private Situation'
      Sub_origin = /
      Sub_source=nc049048 :LZ
      System_name=nc049048 :LZ
      Timestamp=1170125135553000
      Tmz_diff=18000
      Total_inodes=1954064
Para cancelar a assinatura desses e-mails: efetue login no console do Cloud APM e remova seu
endereço de e-mail
da lista de endereços de e-mail de destino na categoria Gerenciador de Eventos da página
Configuração
avançada.
```

A amostra a seguir exibe um e-mail para um evento de fechamento.

```
De: noreply@apm.ibmserviceengage.com
Para:      tester@us.ibm.com
Data:    25/01/2017 14h01
Assunto:    Linux_Disk_Space_Low no nc049048:LZ (encerrado)
O texto abaixo lista as
informações recebidas do agente que acionaram este evento.
Os valores de IP e de Agente identificam o agente que detectou o
evento.
Os valores de Descrição e da Severidade especificam o nome da
definição de limite e sua gravidade.
A seguir há uma descrição de todos os pares de valores de atributo presentes no evento, em seu
formato bruto.
    Servidor IP: 10.107.76.230 (SIDR26APAP1BLUE-12f.test.ibm.com)
    Agente IP: 9.42.49.48
    Agente      : nc049048:LZ
    Severidade: Aviso
    Descrição: Linux_Disk_Space_Low[Disk_Free_Percent <= 20  AND Disk_Free_Percent > 10
                AND FS_Type != nfs  AND FS_Type != iso9660 ]
      ITM_KLZ_Disk
      ManagedSystemGroups = '*LINUX_SYSTEM'
      TenantID=F43E-D704-DADC-6270-1ED8-543E-A388-6513
      Adapter_host=nc049048.tivlab.raleigh.ibm.com
      Apm_hostname=SIDR26APAP1BLUE-12f.test.ibm.com
      Appl_label = A:P: S
      Date=01/25/2017
      Fqhostname=nc049048.test.ibm.com
      Hostname=nc049048.test.ibm.com
      Identificador = Linux_Disk_Space_Lownc049048:LZ/ITM_KLZ_Disk
      Integration_type=U
```

```
      msg='Linux_Disk_Space_Low[Disk_Free_Percent <= 20  AND Disk_Free_Percent > 10  AND FS_Type !
= nfs
     E fs_type! = iso9660 ] '
      Origin=9.42.49.48
      severity=WARNING
      Situation_displayitem = /
      Situation_eventdata = ~
      Situation_name=Linux_Disk_Space_Low
      Situation_origin=nc049048 :LZ
      Situation_origin_uuid=09fb36afd6b3.22.02.09.2a.31.30.56.9d
      Situation_status=N
      Situation_thrunode=nc049048 :LZ
      Situation_time= '25.01.2017 14 :00:55.000'
      Situation_type=S
      source='ITM Agent: Private Situation'
      Sub_origin = /
      Sub_source=nc049048 :LZ
      Tmz_diff=18000
Para cancelar a assinatura desses e-mails: efetue login no console do Cloud APM e remova seu
endereço de e-mail
da lista de endereços de e-mail de destino na categoria Gerenciador de Eventos da página
Configuração
avançada.
```

Capítulo 10. Usando os painéis

Selecione **Desempenho** > **Application Performance Dashboard** para obter uma visão geral de status abrangente de seus aplicativos. É possível realizar drill down a partir da visão geral do nível mais alto para métricas em profundidade na mesma exibição.

Use as ferramentas disponíveis nos painéis para investigar condições críticas e de aviso no ambiente, criar visualizações métricas adicionais e executar ações, como procurar logs de rastreio e comparar métricas ao longo do tempo.

Todos os Meus Aplicativos - Application Performance Dashboard

O Application Performance Dashboard apresenta o status do resumo para seus domínios monitorados em **Todos os Meus Aplicativos**. Uma *caixa de resumo* é exibido para cada usuário definido do aplicativo, como "Inventory Management", e para os aplicativos predefinidos, "My Components" ou "Minhas Transações" se seu ambiente incluir Eles . Nas caixas de sumarização ou no navegador, realize drill down em cada aplicativo e seus constituintes para ver as métricas detalhadas.

Conforme você seleciona os itens, o caminho é mostrado e é possível clicar em um dos links do caminho para retornar a essa visualização. Em qualquer página do Console do Cloud APM, é possível clicar em **Desempenho** > **Application Performance Dashboard** para abrir o painel **Todos os Meus Aplicativos**. Visualize áreas de interesse, selecionando no navegador ou clicando em uma caixa de resumo para fazer drill down para o nível seguinte.

Caixas de Resumo

Todos os Meus Aplicativos possui uma caixa de resumo para cada aplicativo definido. Os indicadores mostram a severidade de status mais alta para o aplicativo na barra de título e para cada grupo na caixa de resumo. Os seguintes grupos predefinidos estão disponíveis, dependendo de quais produtos de monitoramento estão incluídos no aplicativo definido:

- **Monitoramento de Disponibilidade** sem subgrupos
- **Componentes** tem um subgrupo para cada tipo de agente de monitoramento que suporta seu aplicativo
- **Transações** podem incluir **Transações de usuário final** e **Transações sintéticas** (IBM Website Monitoring on Cloud anterior à liberação de agosto de 2017)

Além disso, cada caixa de resumo inclui **Eventos**, que mostra a gravidade do evento com a gravidade mais alta aberto para o aplicativo. É possível clicar no link Eventos para investigar quaisquer eventos abertos (consulte “Status da Ocorrência” na página 1109).

 Clique na barra de título de em uma caixa de resumo para abrir a guia Visão Geral do Status para o aplicativo. Ou clique em um dos ícones de caixa de resumo para abrir a guia Visão geral de status para o grupo Componentes ou o subgrupo Usuários ou Transações, ou para abrir a guia Eventos para o grupo ou subgrupo do aplicativo.

É possível reduzir as caixas de resumo e filtrá-las, marcando ou limpando as caixas de seleção:

- Para mostrar somente as barras de título de caixa de resumo para facilitar a rolagem por seus aplicativos definidos, limpe a caixa de seleção **Mostrar Detalhes**.
- Para filtrar as caixas de resumo para o status da severidade que deseja ocultar, desmarque a caixa de seleção para um contador, como 12 . A caixa de seleção para uma gravidade sem eventos é desativada. Por exemplo, nesse gráfico, os filtros para Crítico e Normal são ativados; Aviso e Desconhecido são desativados porque têm contagem 0: 2 0 1 0 .

Procura

Use o Campo de busca para localizar entradas de log a partir da última hora contendo o texto inserido. É possível clicar em para mostrar resultados de um intervalo de tempo diferente. O texto de Procura é comparado a entradas de log que são associadas à seleção do navegador e quaisquer correspondências são mostradas em um novo guia do navegador ou janela. Para obter instruções, veja "Procurando Arquivos de Log" na página 1081. O recurso de procura é fornecido pela IBM Operations Analytics - Log Analysis.

Ações

O menu **Ações** tem opções para copiar a URL, abrindo o log do painel e configurando um rastreio para resolução de problemas. Para obter mais informações, consulte "Copiando a URL do painel" na página 1122 e "Configurando um Rastreio" na página 1123.

Use a opção **Log do painel** para revisar a lista de painéis do agente que foram atualizados desde a última reinicialização do servidor.

Quando o painel inicial **Todos os Meus Aplicativos** ou um dos aplicativos é selecionado, o menu Ações inclui **Ativar para Relatórios** para ajudá-lo a analisar tendências de uso e de desempenho se os relatórios baseados no Cognos estiverem disponíveis e seu ambiente incluir Tivoli Common Reporting. Para obter mais informações, consulte "Relatórios" na página 1124.

Quando o grupo **Componentes** for selecionado, a partir da seção **Grupos** do navegador ou de uma caixa de resumo, o menu **Ações** incluirá uma opção **Editar** para editar o painel visão geral de status do Componente. A opção **Editar** está disponível apenas se o usuário conectado tiver permissão para modificar no Performance Management Dashboard e a permissão para criar em Aplicativos. Para obter mais informações, consulte "Editando os widgets do grupo do painel Componentes" na página 1090.

Ajuda

Abra a ajuda pop-up para obter uma descrição simples do painel atual, com os seguintes links: **Saiba mais** abre o tópico completo do painel no sistema de ajuda local do Cloud APM; e **Faça um tour pelo painel** inicia o tour pelo Painel do IBM Cloud APM, que apresenta uma breve descrição dos elementos do painel conforme ele o guia através dos recursos.

Navegador

O navegador exibe uma hierarquia de aplicativos definidos e seus usuários, suas transações e seus componentes que refletem como eles estão organizados. O navegador possui uma seção para cada nível da hierarquia do aplicativo. A cada nível do navegador, as métricas do painel são alteradas para mostrar dados do componente. Selecione um item para alternar o contexto do painel para a seleção. O escopo do que é possível ver é determinado por suas permissões de usuário.

Cada item do navegador possui um indicador de status crítico, de aviso, normal ou desconhecido, que indica que o agente está indisponível. Cada seção do navegador apresenta uma contagem de eventos para cada gravidade associada ao item do navegador selecionado. Para um mapeamento de status para eventos de limite, consulte "Status da Ocorrência" na página 1109.

Para fazer mais espaço para outras seções, clique em uma barra de título para reduzir a seção e clique novamente para restaurar a seção. Também é possível ocultar totalmente o navegador clicando no na borda do navegador, restaurá-lo clicando no ou ajustar a largura arrastando a borda .

O navegador possui três seções:

- A seção **Aplicativos** lista todos os aplicativos definidos em seus domínios ou que são permitidos para a sua função de usuário.
  - Após você selecionar um aplicativo, o painel muda para um resumo de status de alto nível na guia **Visão Geral de Status** e um indicador do status de severidade mais alta é exibido na guia **Eventos**. Para obter mais informações, consulte "Aplicativo - Application Performance Dashboard" na página 1082.

  - Quaisquer componentes em seu domínio que foram descobertos pela infraestrutura de monitoramento são mostrados no aplicativo predefinido denominado "Meus Componentes", que não pode ser editado ou excluído.
  - Se você tiver privilégios de função de administrador, a barra de ferramentas **Aplicativos** incluirá as ferramentas para gerenciar aplicativos. Para obter instruções, veja "Gerenciando aplicativos" na página 1098.
- Depois de selecionar um aplicativo, a seção **Grupos** mostra os grupos que suportam o aplicativo. Para obter mais informações, consulte "Grupo e instância - Application Performance Dashboard" na página 1087.
- Após selecionar um subgrupo, a seção **Instâncias** é renomeada para o título de subgrupo e preenchida com os nomes de sistema gerenciados individualmente. As mudanças de **Visão Geral do Status** para mostrar as KPIs dos subgrupos selecionados. Depois de selecionar um sistema gerenciado, os widgets de grupo detalhados são exibidos com KPIs do sistema gerenciado. Para as instâncias do componente, você também tem uma guia **Detalhes de atributos** para visualizar os KPIs dos atributos do conjunto de dados de sua escolha. Para obter mais informações, consulte "Visualizando e gerenciando gráficos e tabelas customizados" na página 1092.

Se tiver um **Erro de Rede** mensagem pop-up no navegador, os indicadores de status pode ser alterado para Normal até que a conexão seja Restaurado . Naquela época, os eventos abertos são reprocessados e o status pode aparecer normal até que o processamento seja concluído.

Procurando Arquivos de Log

Para localizar a causa raiz de um problema que ocorre com usuários, como uma lentidão ou uma falha, é possível procurar através dos dados de log associados aos aplicativos. O IBM Operations Analytics - Log Analysis fornece o recurso de procura. Dados de log do aplicativo e dados de desempenho são colocados juntos para ajudar você a localizar a causa-raiz de um problema com seus aplicativos e expedir a resolução de problemas.

Procedimento

Realize as seguintes etapas para localizar as entradas de log que podem estar correlacionadas a um problema que você esteja investigando, como uso alto de CPU.

1. Se o Application Performance Dashboard não for exibido, selecione-o a partir do **Desempenho**.
2. Se desejar procurar dentro de um aplicativo, selecione um dos aplicativos no painel "Todos os meus Aplicativos".
   Por exemplo, clique em "Meus Componentes" para procurar os logs de todos os recursos de componentes.
3. Insira o texto do arquivo de log para localizar na caixa de procura .
   Por exemplo, insira `retrocedido` para procurar recursos do WebSphere Applications agent que foram retrocedidos para o nível anterior.
4. Se desejar localizar dados a partir de um intervalo de tempo diferente da **Última hora**, clique em e selecione um período diferente.
5. Clique em .

Resultados

Todas as entradas de log que contêm o texto de procura no contexto do nível do navegador atual são exibidas na nova guia ou janela do navegador. A janela do navegador é nomeada para o contexto, como o aplicativo de "Processamento de Cartão de Crédito".

O que Fazer Depois

Revise os resultados da procura. É possível selecionar outro aplicativo para alterar os resultados de procura de acordo com o contexto. Use o campo de procura para refinar ainda mais os resultados. Por exemplo, se o campo de procura mostra `db2 AND (datasourceHostName:Pear* OR`

`datasourceHostname:Persimmon* OR datasourceHostname:Pomegranate*)`, você pode excluir as origens de dados para limitar os resultados: `db2 AND (datasourceHostname:Persimmon*)`.

Para obter informações adicionais, consulte a coleção de tópicos do IBMOperations Analytics Log Analysis no IBM Knowledge Center ou acesse o IBM Operations Analytics - Developers Community.

Aplicativo - Application Performance Dashboard

Após selecionar um aplicativo do navegador ou de uma caixa de resumo no painel **Todos os Meus Aplicativos**, um painel tabulado exibe os diferentes aspectos de seu aplicativo. A guia **Visão Geral de Status** apresenta um resumo de status de alto nível de seu aplicativo. Os limites do gráfico e os indicadores de status fornecem um feedback geral de funcionamento e desempenho. Selecione a guia **Eventos** para ver quais limites de evento estão contribuindo com o funcionamento do aplicativo.

Para obter uma descrição dos elementos do navegador e do banner, veja “Navegador” na página 1080, “Procura” na página 1080, “Ações” na página 1080 e “ Ajuda” na página 1080.

Visão Geral de Status

- Dependendo da composição do aplicativo selecionado, a guia de **Visão Geral do Status** apresenta uma ou mais perspectivas para avaliar o status do aplicativo em um alto nível:

  Disponibilidade ao Longo do Tempo
  IBM Website Monitoring on Cloud antes da liberação de agosto de 2017: O gráfico de barras **Disponibilidade ao longo do tempo** será exibido se o aplicativo incluir o Synthetic Playback agent (no grupo navegador **Transações** e no aplicativo predefinido, **Minhas Transações**).

  Cada ponto de plot é uma amostra de transação com um indicador de cor para um status de **Em Funcionamento**, **Lento** ou **Indisponível**.

  Clique em qualquer lugar na linha do tempo da barra para abrir uma janela pop-up com as tabelas **Lista de Transações** e **Lista de Localizações**.

  Solicitações e Tempo de Resposta
  O gráfico de barras empilhadas **Solicitações e Tempo de Resposta** é exibido se o aplicativo incluir Response Time Monitoring Agent (**Transações do Usuário Final** no grupo navegador **Transações**).

  Use este gráfico para procurar padrões de tendência no desempenho. Cada barra empilhada cria gráfico da porcentagem de solicitações que foram concluídas com bom tempo de resposta, com tempo de resposta lento ou que falharam ao concluir. A sobreposição do gráfico de linha representa graficamente o tempo médio de resposta durante o período de 5 minutos. Use o seletor de tempo para mudar o intervalo de tempo exibido descrito em “Ajustando e comparando métricas no decorrer do tempo” na página 1091.

  Topologia de Transação de Agregado
  A **Topologia de Transação Agregada** é exibida quando o rastreamento de transação é ativado e quando o aplicativo inclui qualquer um dos seguintes agentes ou coletores de dados:

  - DataPower agent
  - Agente do Servidor HTTP
  - IBM Integration Bus agent
  - Coletor de dados J2SE
  - agente JBoss
  - Coletor de dados Liberty
  - Microsoft .NET agent
  - Microsoft SQL Server agent
  - Coletor de dados Node.js
  - Agente Response Time Monitoring

- SAP NetWeaver Java Stack
- Agente Tomcat
- Agente WebLogic (apenas Linux e Windows)
- WebSphere Applications agent
- WebSphere MQ agent

Deve-se ativar o rastreamento de transação manualmente para todos os agentes, exceto o Agente Response Time Monitoring. O rastreamento de transação é ativado automaticamente para coletores de dados. Para obter mais informações, consulte “Página Configuração do Agente” na página 180.

A **Topologia de Transação de Agregado** apresenta os recursos que estão associados com o aplicativo e seus relacionamentos. O rodapé mostra uma contagem dos nós selecionados, recursos, relacionamentos e quaisquer filtros na topologia, além do horário em que os dados foram atualizados pela última vez.

Se um componente de aplicativo for incluído em um aplicativo de negócios, e o componente transportar o tráfego para múltiplos aplicativos, a topologia de aplicativo que é exibida para esses aplicativos de negócios incluirá caminhos para nós para todos os aplicativos.

Para o IBM Pilha de aplicativos Java em que o JavaScript é nível injetado, o nó de nível mais alto representa o navegador e o nó mais granular é o banco de dados. Para outros aplicativos, o nó de nível mais alto representa o aplicativo e o nó mais granular é a instância do sistema gerenciado.

Cada nó possui um indicador de status e um destaque de plano de fundo para mostrar a gravidade de status mais alta no nível de agregação. Se você reduzir o navegador para criar mais espaço, ainda poderá ver o mesmo status na **Topologia de Transação Agregada**. O ambiente de origem do nó mostrado como **Cloud** (IBM Cloud Application Performance Management), **ITM** (IBM Tivoli Monitoring), **On Premises** (IBM Cloud Application Performance Management, Private) , **Private Cloud** (IBM Cloud Private) ou **Public Cloud** (IBM Cloud). Nenhum ícone é mostrado para **Outro** (o recurso gerenciado é de outro ambiente).

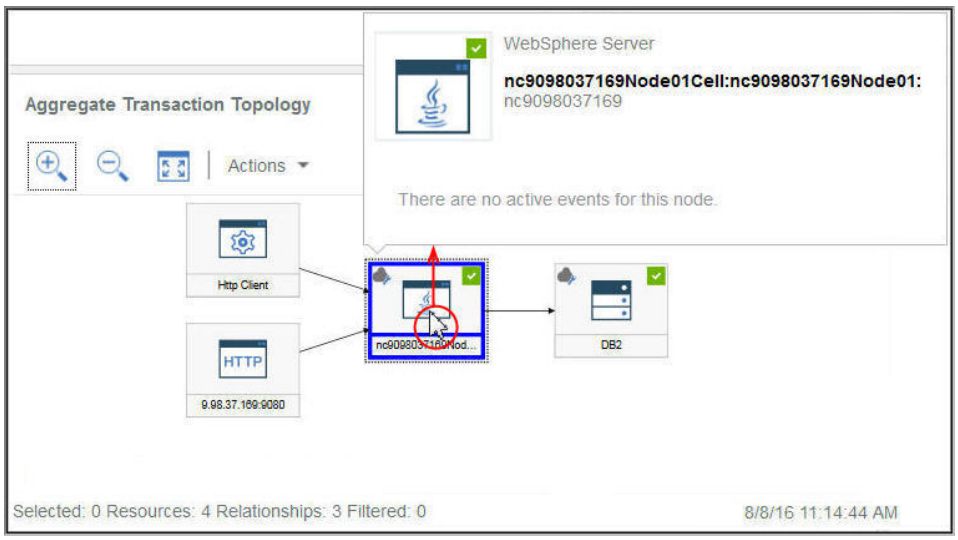
Passe o mouse sobre um nó, abra o menu de atalho e selecione nós para obter mais informações sobre o status e ajudá-lo a identificar a causa raiz de um problema:

- Conforme você passa o mouse sobre um nó, uma mensagem pop-up fornece uma lista de eventos críticos e de aviso.
- Clique duas vezes em um link da URL em um nó para abrir o painel correspondente com o componente ou detalhes da transação.
- Clique com o botão direito em um nó e selecione uma das opções drill down do painel: **Acessar Página de Resumo de Transações** do nó de subgrupo selecionado; **Acessar Página de Instância do Componente** do nó de instância; ou **Propriedades** para ver o nome do recurso, o status, o nome do sistema gerenciado e o domínio do provedor (como "Cloud").

Use os ícones da barra de ferramentas para ajustar a exibição e tomar ações conforme descrito em “Manipulando o widget Topologia de Transação Agregada” na página 1086.

Clique na ferramenta para alternar entre essa visualização e o **Status atual de componentes**, descrito a seguir.

Quaisquer agentes de monitoramento sem informações de topologia não são mostrados no widget Topologia de Transação Agregada.



Status Atual dos Componentes

O gráfico de barras empilhadas **Status do componente atual** mostra a porcentagem e uma contagem de status crítico, de aviso, normal e desconhecido para cada tipo de componente no aplicativo. Considere, por exemplo, que cinco sistemas Linux suportem o aplicativo selecionado. Uma barra empilhada que mostra 40% crítico e 60% normal indica que dois sistemas têm status crítico e três sistemas têm status normal.

Passe o mouse sobre um segmento da barra para ler o status em uma janela pop-up: a porcentagem e a contagem das instâncias do componente com esse status. O domínio ou domínios nos quais as instâncias residem também são mostrados com uma contagem de status para cada domínio: IBM Cloud, Cloud, On Premises, ITM e outros. Por exemplo, dois de seus cinco sistemas Linux estão no domínio ITM e três estão no domínio Cloud. Se um dos sistemas Críticos estiver no domínio ITM e o outro estiver no domínio Cloud, ao passar o mouse sobre o segmento da barra Crítico 40%, a janela pop-up de status mostrará um sistema no domínio ITM e um no domínio Cloud.

É possível clicar em uma barra para abrir o painel de resumo do status para o tipo de componente, com um widget de grupo para cada sistema monitorado.

Clique na ferramenta ⊕ para alternar entre essa visualização e a **Topologia de transação de agregado**, descrito anteriormente.

Monitoramento de Disponibilidade

Quando o aplicativo definido consistir somente no Monitoramento de Disponibilidade, o painel de resumo será exibido conforme descrito em “Acessando o Monitoramento de Disponibilidade” na página 1046.

- Após selecionar um subgrupo a partir da seção **Grupos**, a seção **Instâncias** é renomeada para o título do subgrupo e preenchido com os nomes da instância individual. Para obter informações sobre os painéis no grupo, subgrupo e nível de instância do navegador, e sobre o Detalhes do Atributo região voltada para arquivos **na guia que é aberta após você selecionar** um gerenciado Sistema, consulte gerenciado Sistema, consulte “Grupo e instância - Application Performance Dashboard” na página 1087 e “Visualizando e gerenciando gráficos e tabelas customizados” na página 1092.
- Alguns dos widgets do painel mostram métricas baseadas em um intervalo de tempo, enquanto que outros widgets mostram as métricas mais recentes. Se uma barra do seletor de tempo for exibida, será possível ajustar o intervalo de tempo do painel que afeta quaisquer gráficos ou tabelas cujos valores são derivados das amostras de dados históricos. Para obter mais informações, consulte “Ajustando e comparando métricas no decorrer do tempo” na página 1091.
  Durante a visualização de gráficos, é possível clicar em um ponto de plot para abrir uma dica de ferramenta com o valor do ponto de plot e outras informações pertinentes. Após visualizar um gráfico de linhas no navegador Internet Explorer Version 11, é possível continuar a ver a dica de ferramenta

aparecer conforme você move o cursor pela janela. Se você vir este comportamento, é possível fechar a dica de ferramenta clicando algumas vezes no gráfico.

- Os dados são atualizados automaticamente a cada minuto no console. Essa atividade é essencial e não pode ser pausada, interrompida ou escondida.
- Se não há dados disponíveis para uma caixa de resumo gráfico ou de status, uma mensagem de informação é mostrada.

Eventos

- Os indicadores de status que são exibidos próximos ao título da guia **Eventos**, como **14** **3**, mostram uma contagem das severidades mais altas dos eventos para o item do navegador selecionado: aplicativo, grupo, subgrupo ou instância. As severidades de limite são consolidadas, como é mostrado na tabela a seguir. Por exemplo, **Eventos** significa que o evento de severidade mais alta é secundário ou aviso.

guia Eventos	Severidade Limite
Crítico	Fatal e Crítico
Aviso	Secundário e Aviso
Normal	Desconhecido

  Quando o ambiente gerenciado inclui IBM Operations Analytics - Predictive Insights e uma anomalia é detectada, um evento é aberto. Um ícone em forma de losango sobrepõe o indicador de status, como , para notificá-lo de que pelo menos uma anomalia foi detectada pelo Operations Analytics - Predictive Insights. Por exemplo, **Eventos** , indica que o evento de status mais alto é Aviso e que pelo menos um evento com anomalia está aberto.
- Clique na guia **Eventos** para visualizar um resumo da contagem de evento total, uma contagem de cada tipo de severidade e um gráfico de porcentagem para as severidades. Para obter mais informações, consulte “Status da Ocorrência” na página 1109.

Visualizações customizadas

As páginas criadas e salvas são associadas ao aplicativo selecionado. Por exemplo, o aplicativo Gerenciamento de Inventário no Cloud APM Demo Guiada possui os seguintes agentes de monitoramento: S.O. Linux, MySQL, Node.js, Hadoop e Ruby. É possível criar e salvar uma página customizada em qualquer nível do navegador a partir do aplicativo para a instância e, em seguida, abri-la no mesmo nível em que foi criada. Uma página criada em um nível específico pode ser aberta somente no mesmo nível. As métricas disponíveis para os widgets podem ser de qualquer um dos recursos no aplicativo. Usando o exemplo de Gerenciamento de Inventário, é possível criar uma página com uma tabela no Agente Ruby, um gráfico no agente do S.O. Linux, e assim por diante.

- A guia **Visualizações Customizadas** estará disponível em qualquer nível do navegador ao selecionar um aplicativo em **Todos os Meus Aplicativos**.
- Após abrir a guia **Visualizações Customizadas**, a janela **Selecionar um Modelo para a Página Customizada** será exibida ou a página padrão será exibida se já estiver configurada.
  - Na janela **Selecionar um Modelo para a Página Customizada**, é possível selecionar um modelo para criar uma página.
  - Na página padrão, é possível clicar em para criar uma nova página.
- Na página padrão, clique em na lista de páginas e selecione uma das páginas salvas na lista.
- As opções que você vê na guia Visualizações Customizadas variam com base em se uma página está sendo editada ou visualizada. Para obter informações sobre como editar uma página, consulte “Criando

e gerenciando páginas customizadas" na página 1113. Para obter informações sobre como visualizar uma página, consulte "Visualizando páginas customizadas" na página 1119.

Manipulando o widget Topologia de Transação Agregada

Use o widget **Topologia de Transação Agregada** para visualizar a hierarquia dos recursos no aplicativo selecionado. É possível ajustar e mover ao redor da exibição para ver o status de cada componente e seu relacionamento com os outros componentes, além de abrir um painel de correspondente do nó.

Antes de Iniciar

Depois de selecionar um aplicativo no Application Performance Dashboard, a guia **Visão geral de status** é exibida com um ou mais gráficos, dependendo dos recursos monitorados que estão incluídos no aplicativo.

A **Topologia de Transação de Agregado** é exibida para os seguintes agentes que suportam rastreamento de transações:

- DataPower agent
- Agente do Servidor HTTP
- IBM Integration Bus agent
- Coletor de dados J2SE
- agente JBoss
- Coletor de dados Liberty
- Microsoft .NET agent
- Microsoft SQL Server agent
- Coletor de dados Node.js
- Agente Response Time Monitoring
- SAP NetWeaver Java Stack
- Agente Tomcat
- Agente WebLogic (apenas Linux e Windows)
- WebSphere Applications agent
- WebSphere MQ agent

O **Aggregate Transaction Topology** exibe um objeto de nó para cada recurso monitorado que suporta o recurso de topologia.

Procedimento

Execute alguma das etapas a seguir para manipular o widget **Topologia de Transação Agregada** e abra os painéis que são associados aos nós:

- Para abrir um painel vinculado, dê um clique duplo no nó de topologia. Também é possível clicar com o botão direito em um nó e selecionar uma das opções de drill-down do painel, **Acesse a página Transações** ou **Acesse a página Instância do Componente**, ou selecione **Propriedades** para ver informações sobre o sistema gerenciado.
- Para aumentar o tamanho de exibição da topologia, clique em **Aumentar Zoom**. Também é possível clicar em **Ações** > **Aumentar Zoom** se nenhum nó estiver selecionado.
- Para reduzir o tamanho de exibição da topologia, clique em **Diminuir Zoom**. Também é possível clicar em **Ações** > **Diminuir Zoom** se nenhum nó estiver selecionado.
- Para ajustar o tamanho de exibição da topologia para caber no espaço de widget atual, clique em **Ajustar Conteúdos**. Também é possível clicar em **Ações** > **Ajustar Conteúdo** se nenhum nó estiver selecionado.

- Para filtrar os nós de topologia, selecione um dos indicadores na barra de filtros. É possível alternar os filtros entre ligados e desligados, além de selecionar vários filtros. Qualquer nó com uma propriedade que não corresponda ao filtro é atenuado, e os nós que correspondem ao filtro permanecem visíveis.
  - Normal, Aviso, Crítico ou Desconhecido para filtrar por status do nó.
  - Para filtrar por ambiente, selecione **Cloud** (IBM Cloud Application Performance Management), **ITM** (IBM Tivoli Monitoring), **On Premises** (IBM Cloud Application Performance Management, Private) , **Private Cloud** (IBM Cloud Private) ou **Public Cloud** (IBM Cloud).
  - Filtrar para incluir um filtro customizado.
- Para dar mais espaço para o widget de topologia, clique em **Reduzir Seção** no navegador ou nos widgets de gráfico circundantes ou arraste uma borda do widget.

Grupo e instância - Application Performance Dashboard

Use o painel para o grupo de aplicativos, o subgrupo ou a instância selecionada para obter um status de alto nível dos sistemas gerenciados. É possível fazer drill down em painéis detalhados com métricas para a instância selecionada e criar gráficos e tabelas customizados.

Depois de selecionar um aplicativo em **Todos os meus aplicativos** no Application Performance Dashboard, as guias **Visão geral de status** e **Eventos** são exibidas.

A seção **Grupos** do navegador lista um ou mais dos diversos grupos possíveis, dependendo dos componentes do aplicativo definido.

Para obter uma descrição dos elementos do navegador e do banner, veja "Navegador" na página 1080, "Procura" na página 1080, "Ações" na página 1080 e " Ajuda" na página 1080.

Visão Geral de Status

Grupos e subgrupos

- Selecione um grupo ou expanda um grupo e selecione um subgrupo para ver um widget de grupo de resumo para cada sistema gerenciado no aplicativo. Depois de selecionar um subgrupo, os widgets do grupo de resumo na guia **Visão geral de status** são específicos para esse subgrupo.
- Os seguintes grupos predefinidos estão disponíveis, dependendo de quais produtos de monitoramento estão instalados:

  Monitoramento de Disponibilidade
  Este grupo é exibido para aplicativos customizados. O comportamento de navegação para o Monitoramento de Disponibilidade é diferente dos grupos **Componentes** e **Transações**.

  O complemento e os painéis do Monitoramento de Disponibilidade são descritos em "Monitoramento de Disponibilidade" na página 1045.

  Componentes
  Este grupo é exibido para todos os aplicativos, com exceção do Response Time Monitoring Agent, do Synthetic Playback agent e do Monitoramento de Disponibilidade.

  O **Componentes** possui um subgrupo para cada componente de software monitorado que suporta o aplicativo selecionado.

  Transações
  Este grupo inclui **Transações de usuário final** e **Transações sintéticas** (IBM Website Monitoring on Cloud antes da liberação de agosto de 2017). Para obter mais informações, consulte a ajuda para Monitoramento de transações e o Synthetic Playback agent ou seus PDFs de referência no APM Developer Center em Métricas do agente/PDFs de referência.
- Após você selecionar **Componentes** ou um subgrupo a partir da seção **Grupos**, a guia **Visão Geral de Status** muda para mostrar um painel de sumarização com um widget de grupo para cada recurso

gerenciado. O ambiente de origem é mostrado como **Cloud** (IBM Cloud Application Performance Management), **ITM** (IBM Tivoli Monitoring), **On Premises** (IBM Cloud Application Performance Management, Private) , **Private Cloud** (IBM Cloud Private) ou **Public Cloud** (IBM Cloud).. A seção **Instâncias** é renomeada para o título do subgrupo e preenchida com os nomes de instância individuais.

Se o aplicativo possuir muitas instâncias do sistema gerenciado, muitos widgets de grupo serão exibidos. É possível percorrer a lista para ver todos eles. Também é possível selecionar um tipo de sistema gerenciado da lista de subgrupos de componentes, como Windows OS, para confinar a exibição para os mesmos tipos de sistemas gerenciados. Também é possível filtrar as instâncias do sistema gerenciado.

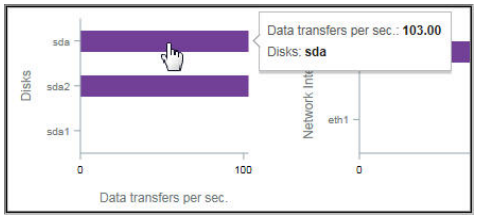
Somente o navegador Firefox: Dependendo do número de agentes e da largura da banda, conforme você rolar para baixo a página Componentes, será possível ver uma mensagem pop-up que o script para carregar a página de recursos leva um longo tempo para ser concluído. Selecione a opção "Não pergunte novamente" para desativar a mensagem e continuar abrindo os widgets. Como alternativa, é possível inserir `about:config` na caixa de endereço, procurar **`dom.max_script_run_time`** e aumentar o valor do tempo limite (em segundos). Um valor de 0 (zero) desativa o tempo limite.

Instâncias

- Clique dentro de um widget de grupo ou selecione o nome da instância no navegador para abrir um painel detalhado para o recurso gerenciado.
- Se muitas instâncias forem exibidas no navegador, use o campo de procura na barra de ferramentas de Instâncias. Conforme você digita, todas as instâncias que não correspondem são removidas da exibição.
- Para pausar a atualização automática do Application Performance Dashboard, clique em **Pausar** na barra de ferramentas de Instâncias; para continuar a atualização automática, clique em **Continuar**.
- Os widgets e KPIs mostrados para qualquer sistema gerenciado podem depender da versão do agente. Se um agente instalado no sistema gerenciado estiver em uma versão anterior, ele pode ser incapaz de fornecer a mesma quantidade de informações que a versão atual do agente. Uma mensagem é exibida em vez de um ou mais KPIs em um gráfico ou tabela quando nenhum dado está disponível. O motivo pode ser tão simples como nenhum dado foi relatado para o período de tempo. Ou pode estar relacionado a um agente de nível anterior que não suporta o conjunto de dados ou um atributo incluído no gráfico ou tabela.
  Para ver uma lista de painéis do agente que foram atualizados desde a última reinicialização do Servidor Cloud APM, selecione **Ações** > **Log do painel**.
- Alguns dos widgets do painel mostram métricas baseadas em um intervalo de tempo, enquanto que outros widgets mostram as métricas mais recentes. Se uma barra do seletor de tempo for exibida, será possível ajustar o intervalo de tempo do painel que afeta quaisquer gráficos ou tabelas cujos valores são derivados das amostras de dados históricos. Para obter mais informações, consulte “Ajustando e comparando métricas no decorrer do tempo” na página 1091.
  Durante a visualização de gráficos, é possível clicar em um ponto de plot para abrir uma dica de ferramenta com o valor do ponto de plot e outras informações pertinentes. Após visualizar um

gráfico de linhas no navegador Internet Explorer Version 11, é possível continuar a ver a dica de ferramenta aparecer conforme você move o cursor pela janela. Se você vir este comportamento, é possível fechar a dica de ferramenta clicando algumas vezes no gráfico.

- Se você estiver visualizando um gráfico com barras ausentes, isso significa que o valor é 0 (zero) para esse ponto de dados.



- Os usuários do IBM Cloud Application Performance Management, Advanced têm painéis de diagnósticos adicionais que são acessados clicando no link **Diagnosticar** de um widget de grupo no painel de detalhes.

  Restrição: O sistema gerenciado para o qual você está abrindo os painéis de diagnóstico deve residir no domínio IBM Cloud APM. Se o sistema gerenciado residir no domínio de origem do IBM Cloud ou do IBM Tivoli Monitoring, os painéis de diagnósticos não estarão disponíveis. Consulte também "Coexistência do agente Cloud APM e do agente Tivoli Monitoring" na página 950.

- Se seu ambiente incluir Synthetic Playback agent, é possível ativar relatórios do Cloud APM para a instância de agente a partir do menu **Ações**.

Eventos

- Os indicadores de status que são exibidos próximos ao título da guia **Eventos**, como **14** **3**, mostram uma contagem das severidades mais altas dos eventos para o item do navegador selecionado: aplicativo, grupo, subgrupo ou instância. As severidades de limite são consolidadas, como é mostrado na tabela a seguir. Por exemplo, **Eventos** significa que o evento de severidade mais alta é secundário ou aviso.

guia Eventos	Severidade Limite
Crítico	Fatal e Crítico
Aviso	Secundário e Aviso
Normal	Desconhecido

  Quando o ambiente gerenciado inclui IBM Operations Analytics - Predictive Insights e uma anomalia é detectada, um evento é aberto. Um ícone em forma de losango sobrepõe o indicador de status, como , para notificá-lo de que pelo menos uma anomalia foi detectada pelo Operations Analytics - Predictive Insights. Por exemplo, **Eventos** , indica que o evento de status mais alto é Aviso e que pelo menos um evento com anomalia está aberto.

- Clique na guia **Eventos** para visualizar um resumo da contagem de evento total, uma contagem de cada tipo de severidade e um gráfico de porcentagem para as severidades. Para obter mais informações, consulte "Status da Ocorrência" na página 1109.

Visualizações customizadas

As páginas criadas e salvas são associadas ao aplicativo selecionado. Por exemplo, o aplicativo Gerenciamento de Inventário no Cloud APM Demo Guiada possui os seguintes agentes de monitoramento: S.O. Linux, MySQL, Node.js, Hadoop e Ruby. É possível criar e salvar uma página customizada em qualquer nível do navegador a partir do aplicativo para a instância e, em seguida, abri-la no mesmo nível em que foi criada. Uma página criada em um nível específico pode ser aberta somente no mesmo nível. As métricas disponíveis para os widgets podem ser de qualquer um dos recursos no

aplicativo. Usando o exemplo de Gerenciamento de Inventário, é possível criar uma página com uma tabela no Agente Ruby, um gráfico no agente do S.O. Linux, e assim por diante.

- A guia **Visualizações Customizadas** estará disponível em qualquer nível do navegador ao selecionar um aplicativo em **Todos os Meus Aplicativos**.
- Após abrir a guia **Visualizações Customizadas**, a janela **Selecionar um Modelo para a Página Customizada** será exibida ou a página padrão será exibida se já estiver configurada.
  - Na janela **Selecionar um Modelo para a Página Customizada**, é possível selecionar um modelo para criar uma página.
  - Na página padrão, é possível clicar em  para criar uma nova página.
- Na página padrão, clique em na lista de páginas e selecione uma das páginas salvas na lista.
- As opções que você vê na guia Visualizações Customizadas variam com base em se uma página está sendo editada ou visualizada. Para obter informações sobre como editar uma página, consulte "Criando e gerenciando páginas customizadas" na página 1113. Para obter informações sobre como visualizar uma página, consulte "Visualizando páginas customizadas" na página 1119.

Detalhes de Atributo

- A guia **Detalhes do Atributo** é exibida após selecionar uma instância do componente a partir da seção **Instâncias** do navegador (renomeado para nome do subgrupo selecionado) ou clicando dentro de um widget de grupo sumarização.
- Se as páginas de gráfico ou de tabela tiverem sido salvas para o agente, a página aberta mais recentemente será exibida com métricas da instância do componente selecionada. Clique no título para selecionar uma página salva diferente de **Minhas Páginas** ou **Páginas Compartilhadas**.
- É possível editar o gráfico ou a tabela e clicar em **Visualizar resultados** para renderizar o gráfico ou a tabela com os atributos selecionados. Para mais opções, consulte "Criando uma página de gráfico ou tabela customizada" na página 1093.

Editando os widgets do grupo do painel Componentes

É possível editar os valores de limite dos widgets de grupo que são exibidos no painel **Componentes** (selecionados na seção **Grupos**). Também é possível controlar quais widgets de grupo são exibidos e sua posição, e decidir se o limite de um widget deve ser incluído na determinação do status do componente.

Sobre Esta Tarefa

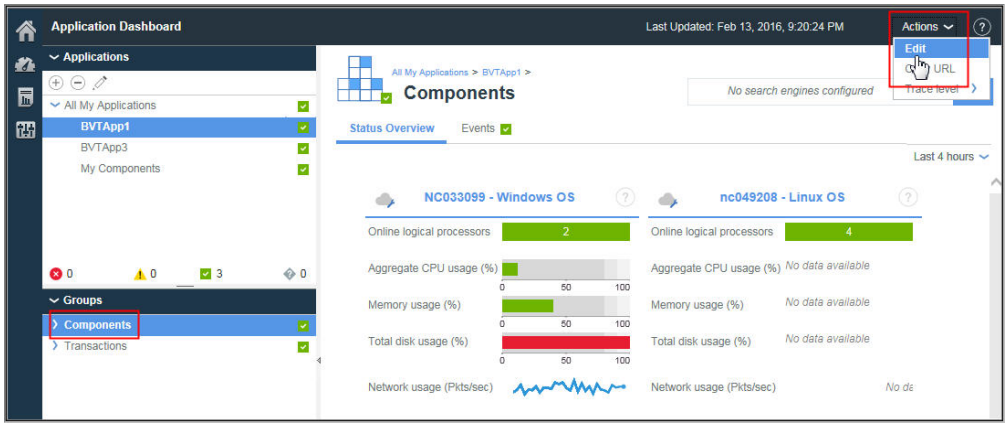
Esta tarefa envolve editar o painel do grupo Componentes e seu widget d grupo de resumo constituinte para um aplicativo definido. O editor do grupo Componentes não está disponível para o aplicativo predefinido **Meus Componentes**. Para obter mais informações sobre aplicativos definidos, consulte "Gerenciando aplicativos" na página 1098.

Seu ID do usuário também deve ter permissão de modificação para Application Performance Dashboard e permissão de criação para Aplicativos. Para obter mais informações, consulte "Funções e permissões" na página 1002.

Procedimento

1. Após abrir Application Performance Dashboard a partir do menu **Desempenho**, selecione o aplicativo cujos widgets de grupo de resumo deseja editar a partir do painel **Todos os Meus Aplicativos**.
2. Na seção **Grupos** do navegador, clique em **Componentes** para abrir um painel mostrando widgets de grupo para todos os componentes no aplicativo.
3. Clique em **Ações** > **Editar** para abrir o editor para os widgets de grupo no grupo **Componentes**.

   A opção **Editar** aparece somente quando o painel **Componentes** é aberto.



4. Faça qualquer uma das mudanças a seguir para os widgets de grupo:
   - Para remover um widget de grupo da visualização, clique no .
   - Para modificar os limites de resumo para um widget, clique em **Configurações**, selecione a guia **Limites** e altere os valores de limite para as severidades crítica, de aviso ou normal. Após editar os limites para o widget de grupo, clique em **Concluído**.
   - Para incluir um widget, clique em , clique nos ícones de aplicativos até que o desejado seja exibido, clique dentro do widget de grupo, selecione-o e clique em **Incluir**.
   - Para redimensionar um widget, arraste o ícone de alça . O redimensionamento de um widget não altera o tamanho do texto ou a altura do widget.
   - Para mover um widget, arraste-o para uma nova posição.
5. Para salvar suas mudanças e fechar o editor, clique em **Salvar**; ou para descartar suas mudanças, clique em **Cancelar**.

Resultados
O painel **Componentes** do aplicativo selecionado é exibido com as novas configurações.

O que Fazer Depois
Para obter mais informações sobre o painel quando um grupo ou subgrupo for selecionado no navegador, consulte "Grupo e instância - Application Performance Dashboard" na página 1087; para obter mais informações sobre o painel do componente monitorado, clique no botão no banner **Painel do Aplicativo**.

Ajustando e comparando métricas no decorrer do tempo

Alguns dos gráficos de painéis mostram métricas baseadas em um intervalo de tempo e outros gráficos mostram somente as métricas mais recentes. Quando um seletor de tempo for exibido na guia **Visão Geral do Status** de uma instância de sistema gerenciado, será possível ajustar o intervalo de tempo para os gráficos cujos valores são derivados de amostras de dados históricos. Para os atributos que possuem dados coletados para múltiplos dias e apresentados em uma gráfico de linhas, é possível comparar os valores de hoje com um dia anterior.

Antes de Iniciar
Se você estiver fazendo uma comparação com um intervalo de tempo de um dia anterior, até onde é possível voltar dependerá do número de dias que o Servidor Cloud APM foi salvo e o tipo de dados exibidos na página. . Para os assinantes pagos do Cloud APM, as amostras de dados são armazenados por 8 dias8 dpara a maioria dos conjuntos de dados do monitor de recursos. O número exato é publicado na ajuda do atributo e no PDF de referência do agente ou do coletor de dados (consulte Capítulo 2, "Documentação em PDF", na página 41). Para os assinantes do Cloud APM, as amostras de dados do monitor de recursos são armazenadas por 2 dias. Os dados de rastreamento de transição do Response Time Monitoring Agent ou agentes de middleware podem ser exibidos apenas apartir das últimas 24 horas (ou para as últimas 4 horas em alguns casos) e seu período de retenção não pode ser mudado.

Procedimento

Execute estas etapas para ajustar o intervalo de tempo exibido no gráfico de linha para uma instância de recurso gerenciado ou para comparar os valores com o mesmo intervalo de tempo de um dia anterior.

1. Se o Application Performance Dashboard não for exibido, selecione-o a partir do **Desempenho**.
2. Navegue na página de painel para uma instância que mostra gráficos de linha históricos e clique no seletor de tempo **Últimas 4 Horas**.
3. Selecione uma ou mais das seguintes opções:
   - Para alterar o intervalo de tempo exibido, selecione **Últimas 4 horas**, **Últimas 12 horas** ou **Último 1 dia**.
   - Para comparar o intervalo de tempo exibido em um gráfico de linha com as métricas de um dia diferente, selecione **Comparar com** e selecione um dia anterior até o número de dias mostrado no calendário pop-up como disponível (uma linha é desenhada por meio de datas indisponíveis).
   - Para que o intervalo de tempo seja aplicado aos painéis de todos os aplicativos definidos em seu ambiente monitorado, selecione **Todos os Aplicativos**. Caso contrário, deixe a configuração como **Somente este Aplicativo** para aplicar o intervalo de tempo somente ao aplicativo atual (como "Meus Componentes"). A seleção **Comparar com** entra em vigor apenas para a página atual.

Resultados

- Se estiver visualizando dados históricos sem comparação, todos os painéis no aplicativo atual (ou todos os aplicativos) são afetados pela mudança.
- Se estiver visualizando uma comparação, apenas os gráficos de linha na página atual são afetados. Uma linha é desenhada para cada KPI para mostrar as métricas do dia escolhido. Alguns gráficos de linha estão indisponíveis para comparação, conforme indicado por uma marca d'água no gráfico: "Nenhuma Comparação Disponível". Isso pode ocorrer com recursos gerenciados mais recentes que ainda não coletaram dados para a data especificada. Tente selecionar uma data mais recente para a comparação.
- Quaisquer widgets para os quais nenhum dado histórico é coletado continuam a exibir os valores mais recentes.
- Pontos de dados são distribuídos ao longo do comprimento completo do gráfico para o intervalo de tempo selecionado. Registros de data e hora são exibidos no rótulo do eixo, iniciando com o registro de data e hora mais antigo e terminando com o registro de data e hora mais recente. Verifique a amostra de dados mais antiga se um intervalo parcial ou integral de dados históricos for exibido.
- Dados enviados para gráficos e tabelas são normalizados de acordo com o GMT (Hora de Greenwich). O eixo de **Registro de data e hora** imprime registros de data e hora com base no fuso horário do seu navegador. Se seu fuso horário usar o horário padrão e horário de verão, o registro de data e hora exibido durante a hora de transição é atrasado por uma hora. Considere, por exemplo, que você está visualizando um gráfico de linha na Espanha, e o registro de data e hora muda de 2h horário padrão para 3h horário de verão. A discrepância entre o GMT da data e o horário local do registro de data e hora resulta em uma diferença de uma hora no registro de data e hora de 2h para 3h. Se estiver visualizando o mesmo gráfico na Nova Zelândia durante a mudança de 3h do horário de verão para 2h horário padrão, os registros de 2h para 3h são repetidos.

Visualizando e gerenciando gráficos e tabelas customizados

O Application Performance Dashboard fornece painéis predefinidos de seus principais indicadores de desempenho do sistema gerenciado. Enquanto você estiver visualizando o painel para uma instância do componente, use a guia **Detalhes do atributo** para visualizar páginas salvas do gráfico ou da tabela e para criar e gerenciar outras páginas.

Por exemplo, você observa um indicador crítico no painel de sumarização e realiza drill down na instância onde a condição está ocorrendo. Daqui, você inclui um gráfico que plota a taxa da CPU ocupada para ver o que está acontecendo ao longo do tempo. É possível visualizar detalhes sobre todos os atributos disponíveis da instância do componente selecionada e salvar o gráfico ou tabela customizada com o agente para exibição sempre que você abrir uma instância do sistema gerenciado.

Um subconjunto de conjuntos e atributos de dados do agente está disponível para uso em gráficos e tabelas customizados. Esses são os atributos mais úteis para exibição em painéis. O conjunto completo de atributos está disponível para uso em limites customizados (consulte "Gerenciador de Limites" na página 985).

Para melhorar o desempenho e reduzir a redundância, os agentes restringem o número de linhas mostradas para determinados conjuntos de dados nos Detalhes do Atributo. As descrições do conjunto de dados na ajuda do agente e no PDF de referência indicam se a amostra de dados padrão limita o número de linhas que são enviadas para o Servidor Cloud APM.

Para usuários com deficiência visual, a capacidade de criar tabelas de históricos fornece uma alternativa aos gráficos de linhas, que não podem ser interpretados por tecnologias assistivas, como o software de leitor de tela. Por esta razão, a guia **Detalhes do atributo** está disponível para instâncias de transação do Agente Response Time Monitoring e do Synthetic Playback agent para criar tabelas históricas. Para obter mais informações, consulte "Exemplo de criação de uma tabela customizada com controles do teclado" na página 1095.

Criando uma página de gráfico ou tabela customizada

Enquanto estiver visualizando o Application Performance Dashboard para uma instância do componente, é possível selecionar a guia **Detalhes do atributo** para visualizar páginas de gráfico ou de tabela salvas e para criar e gerenciar outras páginas.

Sobre Esta Tarefa

Depois de realizar drill down do Application Performance Dashboard página inicial para uma instância do recurso gerenciado, o **Detalhes do Atributo**da guia é Incluído no **Visão Geral do Status** e **Eventos** guias no painel Página .

Estas instruções são para criar gráficos e tabelas customizadas para instâncias do componente. É possível seguir as etapas para as instâncias de transação Agente Response Time Monitoring e Synthetic Playback agent com as seguintes limitações: somente tabelas históricas (sem gráficos); não é possível filtrar a lista **Conjunto de Dados** ou **Atributos**; todos os atributos são selecionados (não é possível selecionar ou cancelar a seleção de atributos individuais); não é possível salvar a página; e a opção **Voltar** do seletor de tempo está indisponível para o Synthetic Playback agent.

Procedimento

Conclua as etapas a seguir para construir um gráfico ou uma tabela a partir de qualquer um dos conjuntos de dados disponíveis para a instância de componente selecionada:

1. Após você abrir o Application Performance Dashboard a partir do menu **Desempenho**, faça drill down em uma instância do recurso gerenciado.

   O sistema selecionado é destacado na seção **Instâncias** do navegador, que é nomeada para o tipo de componente, como **Ruby App**.
2. Clique na guia **Detalhes do Atributo**.

   Se nenhuma página de gráfico ou tabela foi salva para esse tipo de agente de monitoramento, **Tempo Real** **Tabela** será selecionado. O tempo real é apropriado para conjuntos de dados que retornam várias linhas e está disponível somente para tabelas.
3. Se uma página de gráfico ou tabela salva for exibida, clique em **Novo**.
4. Insira um nome para a página de tabela ou gráfico no campo de título.

   Não use nenhum dos caracteres a seguir no título: `! " % & ' * ? < > } { \`.
5. Se você preferir ver amostras de dados ao longo do tempo, mude o tipo para **Histórico**.

   A opção **Gráfico** é ativada.
6. Se você selecionou **Histórico** e preferir uma renderização de gráfico em vez de uma tabela, clique em **Gráfico**.

7. Na lista **Conjunto de Dados**, selecione o botão de opções para o tipo de atributo que deseja ver. Se a lista for muito longa, use a caixa de filtragem para reduzir a lista inserindo o texto que deve ser incluído no nome do conjunto de dados.
   Por exemplo, "config" para o agente de S.O. Linux, filtra os conjuntos de dados para amostrar somente os conjuntos de dados **Linux_CPU_Config** e **Linux_OS_Config**.
8. Para incluir um atributo no gráfico ou tabela, selecione a caixa de seleção próxima ao nome na lista **Atributos**; para incluir todos os atributos, selecione a caixa de seleção no início da lista. Insira texto na caixa de filtragem para localizar atributos específicos, como "percentual".
   Por exemplo, "percent" no conjunto de dados KLZ_VM_Stats filtra a lista para mostrar **Armazenamento virtual livre (Percentual)** e mais 5 atributos "Percent".

   Gráficos podem plotar apenas valores numéricos; qualquer atributo de texto ou de tempo é desativado.
9. Clique em **Visualizar Resultados** para gerar a página com o conjunto de dados escolhido, uma coluna da tabela ou um agrupamento de linhas de gráfico para cada atributo e uma linha ou ponto de plot para cada amostra de dados.

   Você também obtém uma linha ou uma linha representada graficamente para a agregação de todos os valores.
10. Para ocultar linhas de gráfico ou linhas de tabela, execute uma das etapas a seguir:

Opção	Descrição
Gráfico	Oculte uma métrica (uma linha do gráfico) limpando a caixa de seleção ao lado do nome na legenda. Selecione uma caixa de seleção para exibir uma métrica.
Tabela de eixo duplo	Reduza o número de linhas exibidas inserindo o valor pelo qual filtrar na caixa de filtragem. Também é possível criar um filtro avançado, conforme descrito em “Definindo um filtro de tabela” na página 1096.

11. Para ajustar o intervalo de tempo, use o seletor de tempo:

Opção	Descrição
Tempo Real	Apenas para tabelas, atualiza e mostra somente a amostragem de dados mais recente.
2 horas	Cria um gráfico de um ponto ou inclui uma linha para cada amostra de dados que foi obtida nas últimas duas horas, em intervalos.
4 Horas	Cria um gráfico de um ponto ou inclui uma linha para cada amostra de dados que foi obtida nas últimas quatro horas, em intervalos.
12 Horas	Cria um gráfico de um ponto ou inclui uma linha para cada amostra de dados que foi obtida nas últimas 12 horas, em intervalos.
24 Horas	Cria um gráfico de um ponto ou inclui uma linha para cada amostra de dados que foi obtida nas últimas 24 horas, em intervalos.
Anterior	Submenu de opções para incluir dados do mesmo período de tempo **Ontem**, **2 dias atrás** ou de qualquer dia até **1 semana atrás**. Por exemplo, são 14h10 do dia 22 de agosto e você configura o gráfico ou a tabela para mostrar as últimas 4 horas. Ao selecionar **Anterior** > **1 semana atrás**, você vê pontos de dados de 10h10 a 14h10 hoje e de 10h10 a 14h10 em 15 de agosto. Depois de selecionar um dia anterior, o seletor de tempo mostra um asterisco (*) como Last 4 hours* e os dados do dia selecionado é tabela é Regenerado:

- É possível visualizar dados apenas de hoje e até uma semana atrás (mesmo que você tenha aumentado o período máximo de retenção de dados históricos para mais de 8 dias).
- Os gráficos históricos são plotados da amostra de dados mais antiga para a mais recente para o intervalo de tempo selecionado, por exemplo, as últimas 4 horas. Quando um dia anterior for selecionado, você verá os dados do intervalo de tempo selecionado no dia anterior e do intervalo

de tempo para hoje. Os dias que estão entre a data anterior e hoje mostram um ponto de plotagem com um registro de data e hora e nenhuma amostra de dados.

- As tabelas históricas são plotadas em ordem cronológica decrescente. Quando um dia anterior é selecionado para o Agente Response Time Monitoring, cada coluna é replicada para o dia anterior com "Anterior" no título da coluna.
- Independentemente do intervalo de tempo selecionado, um máximo de 11.000 linhas pode ser exibido. Por exemplo, se você escolheu exibir 12 horas de um conjunto de dados que envia 7.000 linhas em 2 horas, serão retornadas menos de 3 horas de dados históricos e as amostras de dados mais antigas serão exibidas.

12. Para salvar ou fazer outras mudanças no gráfico ou tabela, selecione uma das opções a seguir:

Opção	Descrição
Editar	Retorna-o ao editor para fazer qualquer uma das mudanças a seguir: • Editar o título • Alterar para amostras de dados em **Tempo real** ou **Históricos** • Mude para **Gráfico** ou **Tabela** • Selecione um **Conjunto de dados** ou **Atributos** diferentes ou ambos
Novo	Descarta as mudanças não salvas na visualização atual e retorna à página de seleção para criar um novo gráfico ou tabela.
Cancelar	Cancela a sessão de edição para a página de gráfico ou de tabela atual.
Excluir	Exclui a página. **Excluir** estará disponível somente após uma página ser salva e qualquer edição atual ser cancelada.
Salvar para mim	Salva a página de gráfico ou de tabela pela qual visualizar somente com o ID do usuário. Nenhum outro usuário pode ver a página salva.
Salvar para compartilhar	Salva a página de tabela ou gráfico para visualização por qualquer ID do usuário com login efetuado no Console do Cloud APM

As visualizações que você salva têm um cadeado aberto próximo ao título. Visualizações que outro usuário salvo que você não tem a autoridade para editar têm um ícone de bloqueio fechado.

Resultados

Após salvar o gráfico ou tabela customizada, ele/ela é incluído(a) na lista de páginas salvas. Na próxima vez que você selecionar uma instância do mesmo tipo de origem de dados, como WebSphere Applications, e selecionar a guia **Detalhes do Atributo**, a página salva aberta mais recentemente será exibida. Clique no título para selecionar uma página salva diferente de **Minhas Páginas** ou **Páginas Compartilhadas**.

O que Fazer Depois

Repita esse procedimento para criar e gerenciar outras páginas de gráfico ou de tabela.

Para obter orientação sobre como criar uma tabela usando controles do teclado em vez de cliques do mouse, consulte “Exemplo de criação de uma tabela customizada com controles do teclado” na página 1095.

Exemplo de criação de uma tabela customizada com controles do teclado

Os usuários com deficiência visual podem usar a guia do painel **Detalhes do atributo** para criar tabelas históricas como uma alternativa acessível aos gráficos de linha históricos, que não podem ser interpretados por tecnologias assistivas, como software de leitor de tela.

Sobre Esta Tarefa

O exemplo a seguir ilustra o uso de controles do teclado para criar uma tabela histórica para transações que são relatadas pelo Synthetic Playback agent. Para obter informações adicionais sobre o agente, consulte "Gerenciando transações e eventos sintéticos com o Website Monitoring" na página 1026.

Conforme você pressiona a tecla Tab, o foco se move para o próximo campo ou próxima seção da janela de aplicativo, da esquerda para a direita e de cima para baixo. É possível usar essas etapas para gerar uma tabela de transações para o Response Time Monitoring Agent, substituindo **Minhas Transações** por um aplicativo que inclui o agente, ou para gerar uma tabela para uma instância do componente, substituindo **Minhas Transações** por outro aplicativo e selecionando o grupo **Componentes**.

Procedimento

Siga essas etapas para criar uma tabela de transações do Synthetic Playback agent na guia **Detalhes do atributo** usando os atalhos do teclado:

1. Efetue login em IBM Cloud Application Performance Management.

   O foco está na barra de navegação.
2. Para abrir o Application Performance Dashboard, pressione a seta para baixo para mover o foco para o menu **Desempenho**, pressione Enter para selecioná-lo, pressione a seta para baixo para a opção **Application Performance Dashboard** e pressione Enter novamente.
3. Para abrir a página do painel **Transações sintéticas**, pressione Tab repetidamente (aproximadamente 7 vezes) até que o foco se mova para o navegador, pressione a seta para baixo para focalizar o aplicativo predefinido **Minhas Transações** e pressione Enter.
4. Para abrir a página do painel **Detalhes das transações**, pressione Tab (aproximadamente 10 vezes) até que o foco se mova para a seção **Instâncias** do navegador em uma instância de transação **Transações sintéticas** e pressione Enter.

   A guia **Detalhes do atributo** é exibida no painel.
5. Para abrir a guia **Detalhes do atributo**, pressione Tab (aproximadamente 6 vezes) até que o foco esteja na guia **Visão geral de status**, e pressione a seta para a direita até que o foco esteja na guia **Detalhes do atributo**.

   A **Tabela** **Histórica** e todos os atributos do conjunto de dados **Disponibilidade da Transação ao Longo do Tempo** são selecionados.
6. Para gerar a tabela, pressione Tab (aproximadamente 18 vezes) até que o foco esteja no botão **Visualizar resultados** e pressione Enter.

Resultados

Os atributos **Disponibilidade de transação ao longo do tempo** são exibidos em uma tabela, com coluna para cada atributo e uma linha para cada amostra de dados durante as últimas 4 horas.

O que Fazer Depois

- Para reduzir o número de linhas que são exibidas, é possível pressionar Tab para focalizar a caixa de texto **Filtro**, e inserir um texto parcial ou inteiro ou valor de registro de data e hora pelo qual filtrar.
- Para mudar esse intervalo de tempo, mude o foco para o menu suspenso **Últimas 4 Horas** do Seletor de Tempo e selecione outra opção. Para obter mais informações, consulte a etapa "11" na página 1094 em "Criando uma página de gráfico ou tabela customizada" na página 1093.
- Para gerar uma tabela com o conjunto de dados **Tempo de Resposta da Transação**, pressione Tab (cerca de 2 vezes) para mudar o foco para a ferramenta **Novo** e pressione Enter. O painel de seleção é exibido. Selecione o conjunto de dados **Tempo de resposta de transação** e o botão **Visualizar resultados**.

Definindo um filtro de tabela

É possível limitar as linhas em uma tabela que estão sendo visualizadas na guia **Detalhes do atributo** do painel para mostrar somente linhas de um determinado tipo, ou que possuem por valores de atributo de

texto ou de registro de data e hora. Embora valores numéricos não estão disponíveis para filtragem, como porcentagens, alguns valores de atributos numéricos são convertidos em um valor de exibição para a tabela e tratados como texto.É possível aplicar um filtro rápido ou abrir um editor para editar um filtro avançado.

Procedimento

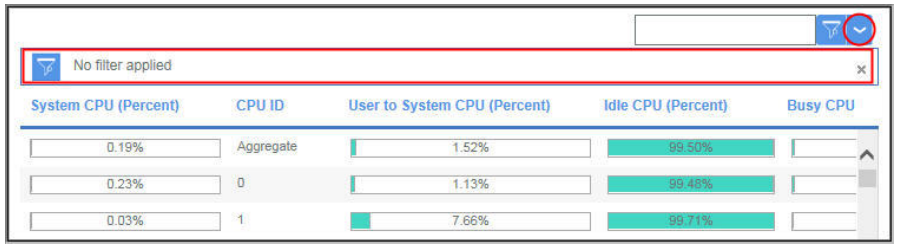
Conclua essas etapas para filtrar uma tabela customizada por valores de atributo de texto ou de registro de data e hora. Embora valores numéricos não estejam disponíveis para filtragem, como porcentagens, alguns valores de atributos numéricos são convertidos em um valor de exibição para a tabela e tratados como texto.

1. Após abrir o Application Performance Dashboard a partir do menu **Desempenho**, realize drill down para uma instância do recurso gerenciado.
2. Clique na guia **Detalhes do Atributo**.

   A página salva mais recentemente é exibido ou, se nenhum páginas foram salvas, o **Conjunto de Dados** e **Atributos** listas de seleção são exibidos.
3. Se uma página de tabela salva for exibida, continue na etapa "5" na página 1097, selecione outra página de tabela salva do menu suspenso ou clique em **Incluir** para criar uma nova tabela.
4. Se estiver criando uma nova tabela ou editando uma tabela salva, selecione o **Conjunto de dados** e **Atributos** a serem usados e clique em **Visualizar resultados**.
5. Para um filtro rápido, clique na caixa de texto **Filtro** e digite o texto parcial ou completo para filtragem.

   Conforme você digita, as linhas que não contêm o que você digitou são removidas da tabela. Para remover o filtro rápido, exclua os valores ou clique no "x".
6. Para um filtro avançado, clique no menu suspenso e selecione **Construir filtro** ou clique em qualquer lugar na barra do filtro.

   A janela **Filtro de compilação** é aberta com algumas regras que foram definidas.



7. Para definir uma regra, preencha os campos:
   a) Deixe a configuração de coluna como "Qualquer Coluna" ou selecione o atributo pelo qual filtrar da lista.
   b) Deixe a condição em "contém" ou selecione outro operador da lista e insira o valor de texto ou de registro de data e hora pelo qual filtrar na caixa de texto:

Condição	A linha é incluída na tabela quando...
contém	o valor de filtro está localizado em algum lugar na célula.
igual a	o valor da célula corresponde exatamente ao valor de filtro, incluindo letras maiúsculas e minúsculas.
iniciar por	o valor da célula começa com os mesmos caracteres que o valor de filtro.
termina com	o valor da célula tem os mesmos caracteres finais que o valor de filtro.
não é igual a	O valor da célula não é uma correspondência exata do valor de filtro.
does not contain	O valor da célula não inclui o mesmo texto ou número que o valor de filtro.

Condição	A linha é incluída na tabela quando...
does not start with	O valor da célula não começa com os mesmos caracteres que o valor de filtro.
não termina com	o valor da célula não termina com os mesmos caracteres que o valor de filtro.
está vazio	a célula não mostra dados.

c) Após concluir a regra, clique em **Filtrar**. Para ver os resultados, clique em **Incluir Regra de Filtragem** para incluir outra regra ou vá para a próxima etapa.

8. Se o filtro tiver várias regras, execute qualquer uma destas etapas:
   - A **correspondência** é configurada inicialmente como **Todas as regras**, o que significa que uma linha somente será exibida se os dados na linha seguirem todas as regras no filtro. A linha será excluída se nenhum valor de texto ou de registro de data e hora seguir uma regra. Se você tiver várias regras e desejar uma linha incluída, se ela seguir qualquer uma das regras, mude a configuração para **Qualquer regra**.
   - Para editar uma regra, altere qualquer um dos valores do campo.
   - Para excluir uma regra, selecione-a e clique em **Remover Regra**.
9. Ao terminar de definir uma regra (ou regras), clique em **Filtro** para fechar a caixa de diálogo e aplicar o filtro.

Resultados

Os grupos que não atenderem aos critérios de filtro serão removidos da exibição e a barra de filtros relatará o número de itens, por exemplo, "480 de 1200 itens mostrados".

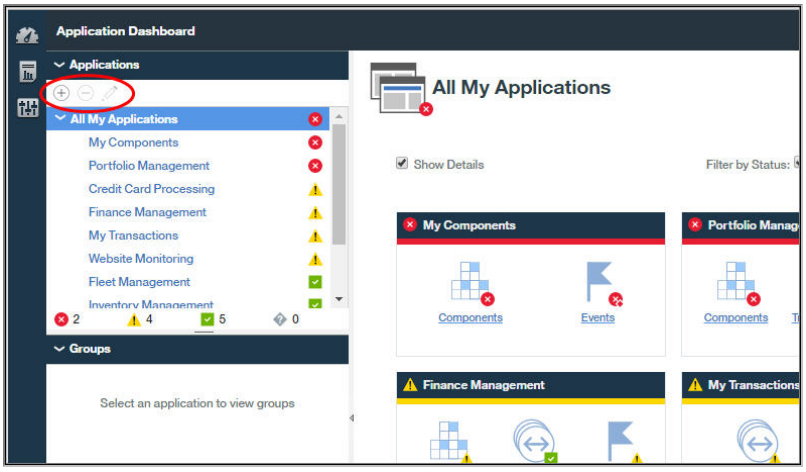
O que Fazer Depois

- Passe o ponteiro do mouse sobre a barra de filtro para abrir uma janela pop-up com os critérios de filtro. É possível excluir uma regra (clique em ×) ou clicar dentro da janela para editar os critérios de filtro.
- Clique em **Limpar Filtro** na barra de filtro ou **Limpar** na janela **Construir Filtro** para remover o filtro e exibir todas as linhas.

Gerenciando aplicativos

Use as ferramentas que estão disponíveis no Application Performance Dashboard para organizar seus recursos gerenciados nos aplicativos.

As ferramentas **Aplicativos** do navegador abrem o Editor de aplicativos para criar ou editar e aplicar os recursos gerenciados que estão disponíveis.



O aplicativo **Meus Componentes** é um aplicativo predefinido que inclui os sistemas gerenciados que foram descobertos pelo Servidor Cloud APM. O **Meus Componentes** não pode ser editado ou excluído.

Para uma demonstração de vídeo sobre a inclusão de um aplicativo, assista Application Performance Management - Definir Aplicativo.

Para obter um cenário sobre a criação de um aplicativo para monitoramento da pilha de aplicativos IBM Java, consulte “Incluindo aplicativos da web no Painel de Desempenho do Aplicativo ” na página 88 e “Associando o IBM Pilha de aplicativos Java com o aplicativo da web ” na página 89.

Restrição: Deve-se ter a permissão modificar para Aplicativos para usar a ferramenta Incluir aplicativo. Deve-se ter a permissão modificar para Aplicativos ou para o aplicativo específico para usar as ferramentas Remover e Editar. Para obter mais informações, consulte “Trabalhando com funções, usuários e permissões” na página 1009.

Incluindo um Aplicativo

Use o Editor de aplicativos para criar um novo aplicativo e aplicar os recursos gerenciados que estão disponíveis ou selecionar um a partir de qualquer aplicativo descoberto.

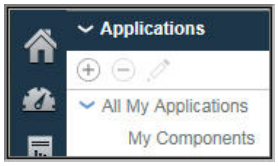
Antes de Iniciar

Deve-se ter a permissão modificar para Aplicativos para usar a ferramenta Incluir aplicativo. Para obter mais informações, consulte “Trabalhando com funções, usuários e permissões” na página 1009.

Procedimento

Conclua as seguintes etapas no Console do Cloud APM para incluir um aplicativo no Application Performance Dashboard.

1. Se o Application Performance Dashboard não for exibido, selecione-o no menu **Desempenho** ou, se estiver em outra página do console, clique no link **Início**.
2. Na seção **Aplicativos** do navegador, clique em . A janela **Incluir Aplicativo** é exibido.

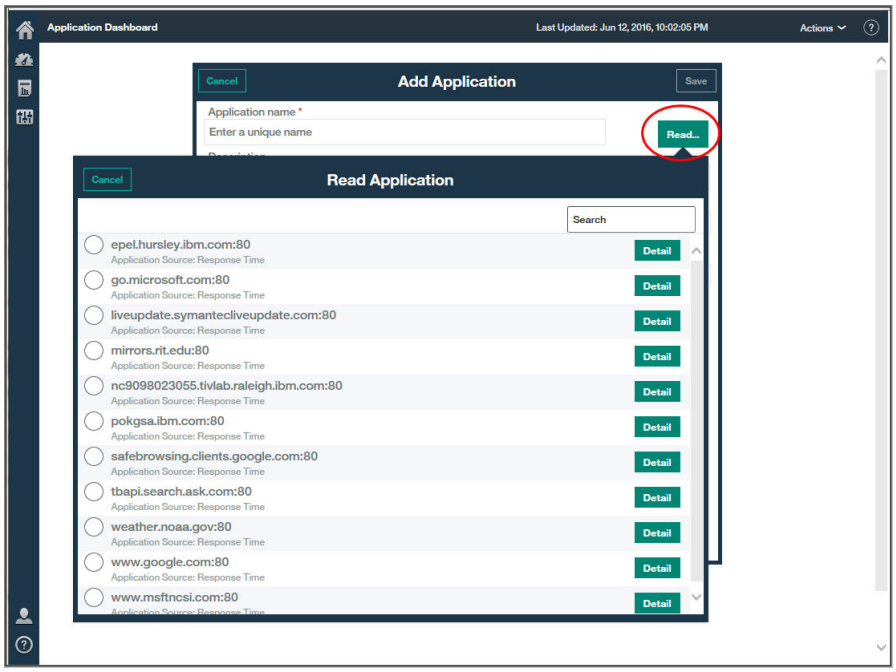


3. Insira um nome para seu aplicativo no campo **Nome do aplicativo** e, opcionalmente, uma descrição no campo **Descrição**.

   Não use os símbolos ! " % & ' * ? < > } { \ no nome ou descrição.

   É possível ver alguns exemplos de nomes de aplicativos, como "Gerenciamento de Finanças" e "Processamento de Cartão de Crédito" no Demo Guiada.

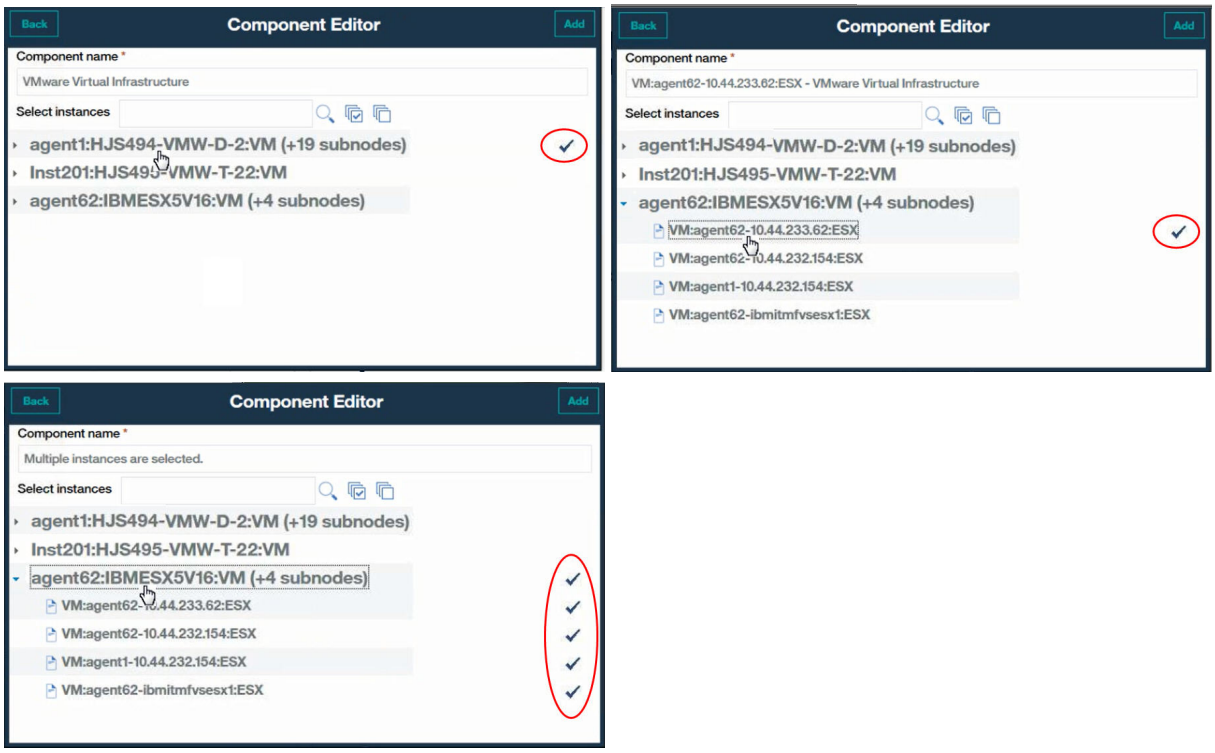
4. Clique em **Ler** para abrir a janela **Ler aplicativo** com uma lista de todos os aplicativos descobertos, e execute uma ou mais das seguintes etapas:
   - Clique em **Detalhes** para ver os componentes de um aplicativo.
   - Selecione o aplicativo que você deseja usar e clique em **Salvar**. A janela **Ler aplicativo** se fecha, o repositório de origem é exibido no campo **Leitura do aplicativo a partir de** e os componentes são listados em **Componentes de aplicativo**.
   - Clique em **Cancelar** para fechar a janela sem fazer uma opção.



5. No campo **Modelo**, mantenha o modelo **Aplicativo customizado** ou selecione um modelo diferente com o botão e clique em **Salvar**.

   Todos os tipos de componentes associados e instâncias são mostrados na lista **Componentes do aplicativo**.
6. Clique em **Incluir Componentes** e, na janela **Selecionar Componente** que é aberta, selecione um componente da lista.

   O **Editor de Componente** é exibido.
7. Para localizar e selecionar instâncias do nó do agente ou do subnó, (ou ambos) para o aplicativo, execute uma ou mais das seguintes etapas:
   - Clique em uma instância para selecioná-la.
   - Para nós do agente que possuem subnós, selecione somente o nó clicando no nome enquanto a árvore está reduzida, selecione o nó e todos os subnós expandindo a árvore do nó (clique em) e clicando no nó, ou selecione subnós individuais expandindo a árvore do nó e clicando na instância.
   - Use a barra de ferramentas para procurar instâncias contendo o texto na caixa de texto da procura, para selecionar todas as instâncias ou para limpar todas as instâncias.
   - Se deseja mudar o nome de exibição no navegador, edite o nome do componente.



V6-V7 Se você estiver incluindo uma instância do agente Tivoli Monitoring e não vê-lo na lista de instâncias disponíveis, verifique se o Tivoli Enterprise Portal Server que está associado ao Hybrid Gateway está em uma versão suportada (consulte Agentes suportados pelo Hybrid Gateway (APM Developer Center)).

8. Clique em **Incluir** para incluir os nós do agente e subnós selecionados no aplicativo e clique em **Voltar**.

   A lista Componentes do aplicativo é atualizada com os novos nomes de componentes.
9. Selecione outro componente no qual incluir instâncias e repita “6” na página 1100, “7” na página 1100 e “8” na página 1101 ou clique em **Fechar**.
10. Se outras instâncias estiverem relacionadas aos componentes na lista **Componentes do Aplicativo**, um botão que mostra o número de instâncias relacionadas é exibido e será possível executar as seguintes etapas:

    a) Clique no botão para ver as instâncias relacionadas na janela **Detalhes atualizados**. Uma barra é mostrada para cada tipo de atualização, incluindo o nome da instância. Por exemplo, se um dos componentes tiver sido removido, ele será mostrado abaixo da barra de componentes **Excluídos**.

    b) Selecione uma ou mais instâncias e clique em **Salvar** para atualizar a lista de Recursos do aplicativo.
11. Quando concluir a definição do aplicativo, feche o editor de aplicativos clicando em **Salvar** para salvar suas mudanças ou clique em **Cancelar** para desfazer as mudanças.

Resultados

As atualizações do aplicativo são concluídas pelo Servidor Cloud APM após você salvar suas mudanças. Pode levar alguns minutos para que as mudanças apareçam no painel. (Tente limpar o cache do navegador se for preciso muito tempo para que as suas mudanças sejam exibidas). O novo aplicativo e exibido no Application Performance Dashboard e na seção **Aplicativos** do navegador. Quando o aplicativo estiver selecionado, os componentes serão exibidos na seção **Grupos**.

Editando um aplicativo

Use o Editor de aplicativos para modificar um aplicativo definido a fim de incluir ou remover recursos gerenciados como componentes do aplicativo.

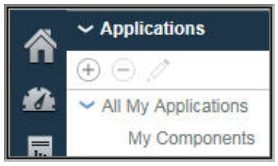
Antes de Iniciar

Deve-se ter a permissão Modificação para Aplicativos ou o aplicativo específico a fim de usar a Ferramenta de edição. Para obter mais informações, consulte "Funções e permissões" na página 1002.

Procedimento

Conclua as seguintes etapas no Console do Cloud APM para editar um aplicativo.

1. Se o Application Performance Dashboard não for exibido, selecione-o no menu **Desempenho** ou, se estiver em outra página do console, clique no link **Início**.
2. Selecione o aplicativo que você deseja editar da lista **Todos os meus aplicativos** no navegador e clique em .



   A janela **Editar Aplicativo** é exibida.
3. Opcional: Edite o **Nome do aplicativo** ou a **Descrição**.

   Não use os símbolos ! " % & ' * ? < > } { \ no nome ou descrição.
   Se as suas permissões de Visualização ou de Modificação de Aplicativos forem para aplicativos individuais e não para todos os aplicativos, talvez você não consiga ver o aplicativo no painel ou modificar o aplicativo após ele ser renomeado. Essa limitação é porque o aplicativo renomeado é tratado como um novo aplicativo. Seu administrador de função ou administrador de monitoramento deve fornecer a permissão Visualização ou Modificação para o aplicativo renomeado.
4. Para incluir componentes e instâncias no aplicativo, execute as seguintes etapas.
   a) Clique em e selecione um componente na lista na janela que se abre.

      O **Editor de Componente** é exibido.
   b) Selecione instâncias do nó do agente ou do subnó (ou ambos) para o aplicativo:
      - Clique em uma instância para selecioná-la.
      - Para nós que possuem subnós, selecione o nó clicando no nome enquanto a árvore está reduzida, selecione o nó e todos os subnós expandindo a árvore do nó (clique em) e clicando no nó, ou selecione subnós individuais expandindo a árvore do nó e clicando na instância.
      - Use a barra de ferramentas para procurar instâncias contendo o texto na caixa de texto da procura, para selecionar todas as instâncias ou para limpar todas as instâncias.
      - Se deseja mudar o nome de exibição no navegador, edite o nome do componente.
   c) Clique em **Incluir** para incluir a instância ou instâncias e clique em **Voltar**.

      A lista Componentes do aplicativo é atualizada com os novos nomes de componentes.
   d) É possível selecionar outro componente ao qual incluir instâncias ou clicar em **Fechar**.

   A lista Componentes do aplicativo é atualizada com os novos nomes de componentes. Um número entre parênteses depois do nome indica quantas instâncias estão associadas ao componente.
5. Para editar um nome do componente ou alterar a instância à qual ele está associado, selecione o componente na lista **Componentes do Aplicativo** e clique em :
   a) Para associar uma instância diferente ao componente, procure e selecione a instância desejada.
   b) Para alterar o nome do componente que é usado como o nome de exibição no navegador para esse aplicativo, edite o campo **Nome do Componente**.
   c) Clique em **Salvar**.

   A lista Componentes do aplicativo é atualizado com as atualizações feitas.
6. Para remover um componente ou uma instância do aplicativo, selecione-o e clique em . Clique em **OK** para confirmar se deseja removê-lo.

7. Se outras instâncias estiverem relacionadas aos componentes na lista **Componentes do Aplicativo**, um botão que mostra o número de instâncias relacionadas é exibido e será possível executar as seguintes etapas:
   a) Clique no botão para ver as instâncias relacionadas na janela **Detalhes atualizados**.
   Uma barra é mostrada para cada tipo de atualização, incluindo o nome da instância. Por exemplo, se um dos componentes tiver sido removido, ele será mostrado abaixo da barra de componentes **Excluídos**.
   b) Selecione uma ou mais instâncias e clique em **Salvar** para atualizar a lista de Recursos do aplicativo.
8. Quando concluir a edição do aplicativo, feche o editor de aplicativos clicando em **Salvar** para salvar suas mudanças ou em **Cancelar** para desfazer as mudanças.

Resultados
As atualizações do aplicativo são concluídas pelo Servidor Cloud APM após você salvar suas mudanças. Pode levar alguns minutos para que as mudanças apareçam no painel.
Referências relacionadas
"Funções e permissões" na página 1002

Excluindo um aplicativo

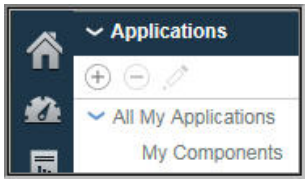
Quando não precisar mais de um aplicativo que foi definido para exibição no Application Performance Dashboard, é possível excluí-lo. Excluir um aplicativo não desinstala os componentes de apoio, somente o aplicativo no qual estão contidos. Os mesmos componentes estão disponíveis para inclusão em outros aplicativos e não são removidos de outros aplicativos aos quais pertencem.

Antes de Iniciar

Deve-se ter a permissão modificar para Aplicativos ou o aplicativo específico a fim de usar a ferramenta Remover. Para obter mais informações, consulte "Trabalhando com funções, usuários e permissões" na página 1009.

Procedimento

Conclua as seguintes etapas para remover um aplicativo do Application Performance Dashboard.

1. Se o Application Performance Dashboard não for exibido, selecione-o no menu **Desempenho** ou, se estiver em outra página do console, clique no link **Início**.
   

2. Na seção **Aplicativos** do navegador, selecione o aplicativo que você deseja excluir da lista **Todos os meus aplicativos** e clique em .
   Uma mensagem solicita a confirmação.
3. Clique em **Sim** para confirmar que deseja excluir o aplicativo; ou em **Não** se não tiver certeza.

Resultados
Depois de clicar em **Sim**, o aplicativo é excluído do Application Performance Dashboard.

O que Fazer Depois
Repita esta etapa para quaisquer outros aplicativos que você deseja excluir.

Visualizando e removendo agentes off-line

Após um agente ter ficado off-line por quatro dias, ele é removido do Console do Cloud APM. Revise como os agentes off-line são indicados e o efeito nos grupos de recursos, visualizações de topologia e outros recursos. Use o editor de aplicativos para remover um sistema gerenciado do painel antes de ter decorrido os quatro dias. .

Sobre Esta Tarefa

Após a instalação dos agentes nos sistemas que você deseja gerenciar, eles se conectam ao Servidor Cloud APM e enviam amostras de dados para o Application Performance Dashboard para apresentação e avaliação de limite. Se o agente estiver off-line, o indicador de status para será exibido no navegador e no painel. O servidor aguarda um número específico de intervalos decorrerem sem nenhuma resposta do agente antes de mostrar que o agente está indisponível. Consulte "Exemplos de agentes off-line" na página 1105.

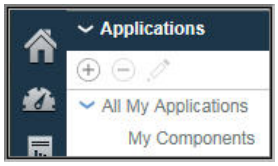
Após quatro dias, o agente off-line é removido da interface com o usuário com a exceção a seguir: se o agente for aquele que suporta o rastreamento de transação, o agente off-line continuará a ser exibido nas visualizações Topologia de Transação de Agregado e Topologia de Instância de Transação.

É possível remover o agente off-line de todos os aplicativos definidos, o que remove-o do Console do Cloud APM antes da conclusão do período de espera de quatro dias.

Procedimento

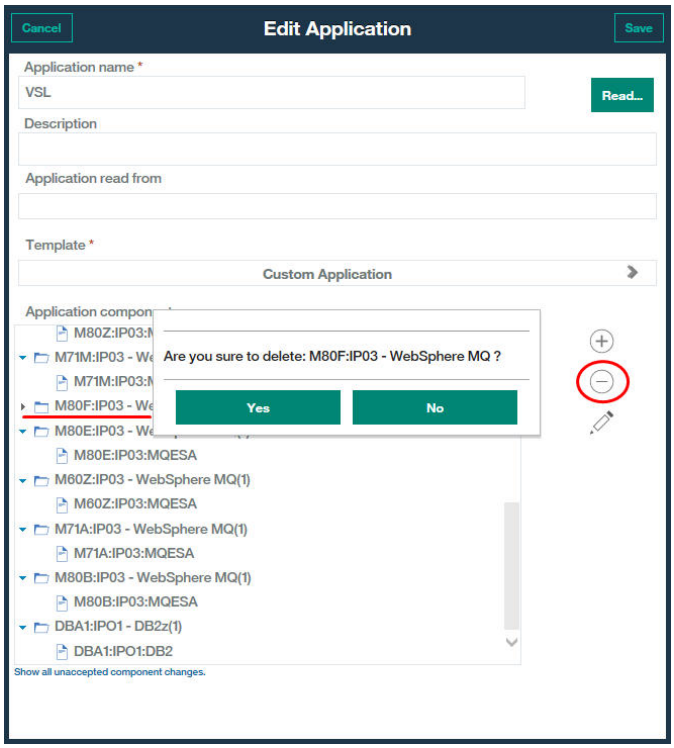
Execute essas etapas para remover um agente off-line de um aplicativo definido:

1. Se o Application Performance Dashboard não for exibido, selecione-o no menu **Desempenho** ou, se estiver em outra página do console, clique no link **Início**.
2. Na seção **Aplicativos** do navegador, selecione o aplicativo do qual o agente off-line é um componente e clique em **Editar aplicativo**.



3. Selecione o agente ou subnó do agente na lista Componentes de aplicativo e clique em .

   Para agentes que possuem subnós, selecione somente o agente clicando no nome enquanto a árvore está reduzida, selecione o nó e todos os subnós expandindo a árvore do nó (clique em) e clicando no nó, ou selecione subnós individuais expandindo a árvore do nó e clicando na instância.



4. Ao concluir a edição do aplicativo para remover o agente ou subnó off-line, clique em **Salvar**.

Resultados
As atualizações do aplicativo são concluídas pelo Servidor Cloud APM após você salvar suas mudanças. Pode levar alguns minutos antes da remoção do agente off-line do Application Performance Dashboard.

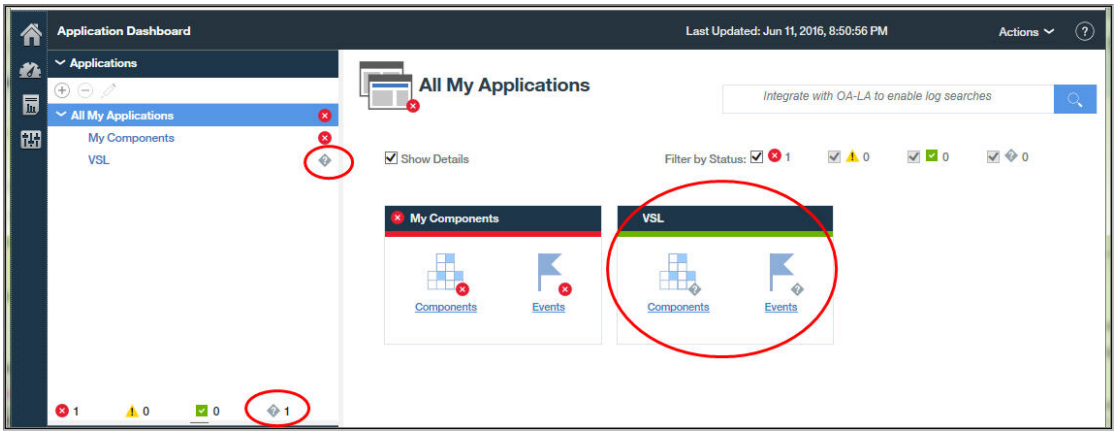
Exemplos de agentes off-line
Revise os exemplos de como agentes off-line são exibidos no Console do Cloud APM. É possível remover a exibição de qualquer agente off-line que você não deseja mais monitorar. Se o agente ficar on-line novamente mais tarde, o monitoramento será retomado.

Quando um agente está off-line, nenhum dado é enviado para o Console do Cloud APM e o Application Performance Dashboard exibe um indicador de status para o agente e os aplicativos aos quais ele pertence. O agente está indisponível para inclusão em um aplicativo definido no Editor de aplicativos ou em um grupo customizado no Gerenciador de Grupo de Recursos, ou para criação de tabelas e gráficos de linha históricos na guia Detalhes do atributo.

Application Performance Dashboard - Todos os meus aplicativos

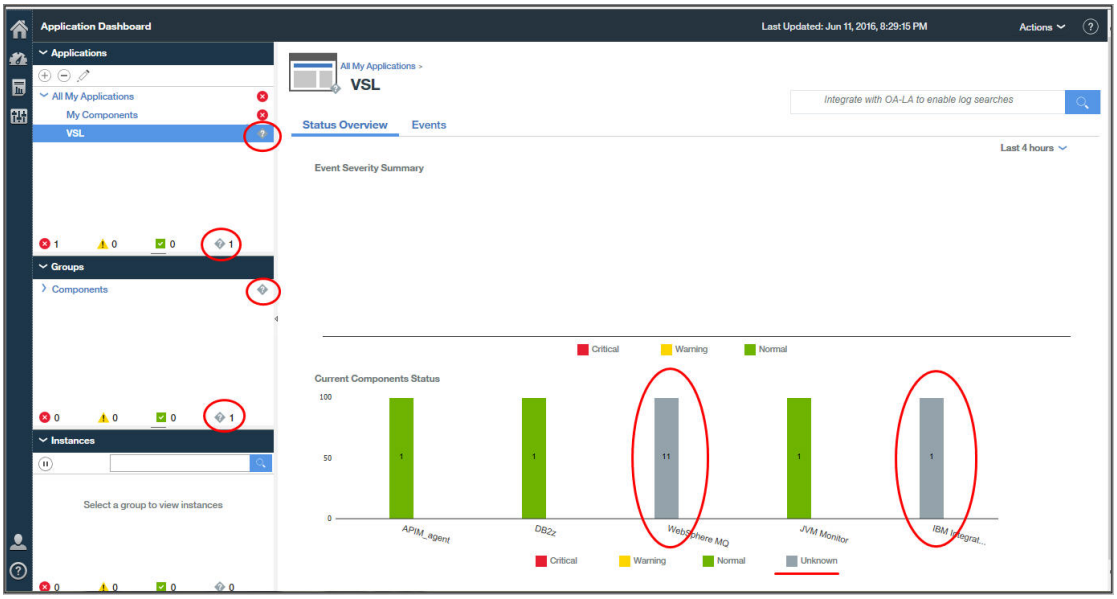
A página inicial do painel, **Todos os Meus Aplicativos**, fornece a primeira indicação de status off-line. O contador na seção Aplicativos do navegador mostra o número de aplicativos com recursos indisponíveis.

A caixa de resumo mostra status de evento Normal porque nenhum evento está aberto para os recursos gerenciados do aplicativo.



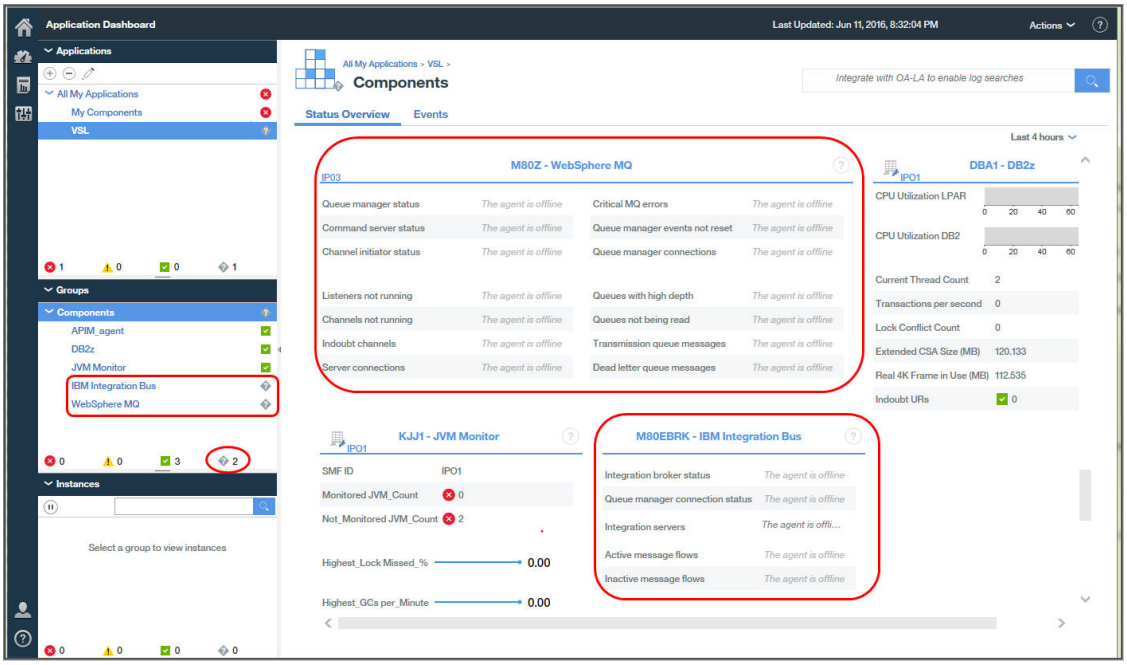
Application Performance Dashboard - Aplicativo

Após o usuário clicar na barra de título da caixa de resumo ou selecionar o aplicativo do navegador, a guia **Visão geral de status** é exibida com um gráfico vazio **Resumo da severidade do evento**. O gráfico de barras **Status do componente atual** mostra o status para agentes off-line como "Desconhecido".



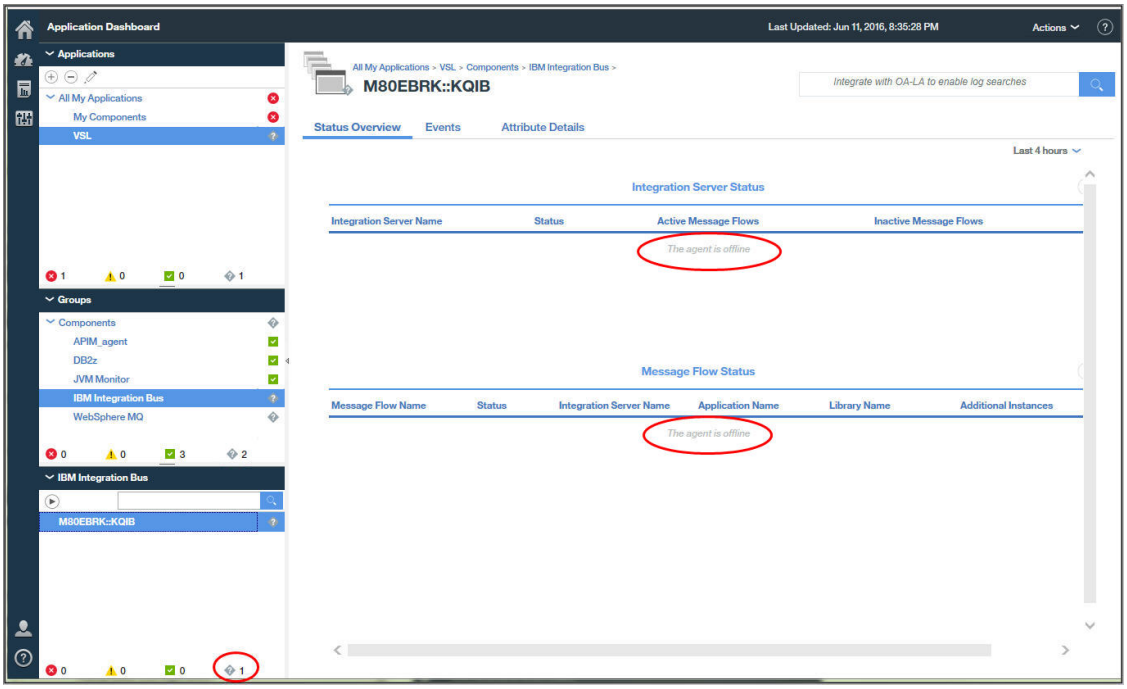
Application Performance Dashboard - Grupo

Após o usuário clicar dentro do gráfico **Status do componente atual** ou no grupo **Componentes** do navegador, a guia **Visão geral de status** muda para mostrar um widget de grupo de resumo para cada recurso gerenciado. Os widgets de grupo para os agentes indisponíveis exibem uma mensagem indicando que o agente está off-line em vez de KPIs.

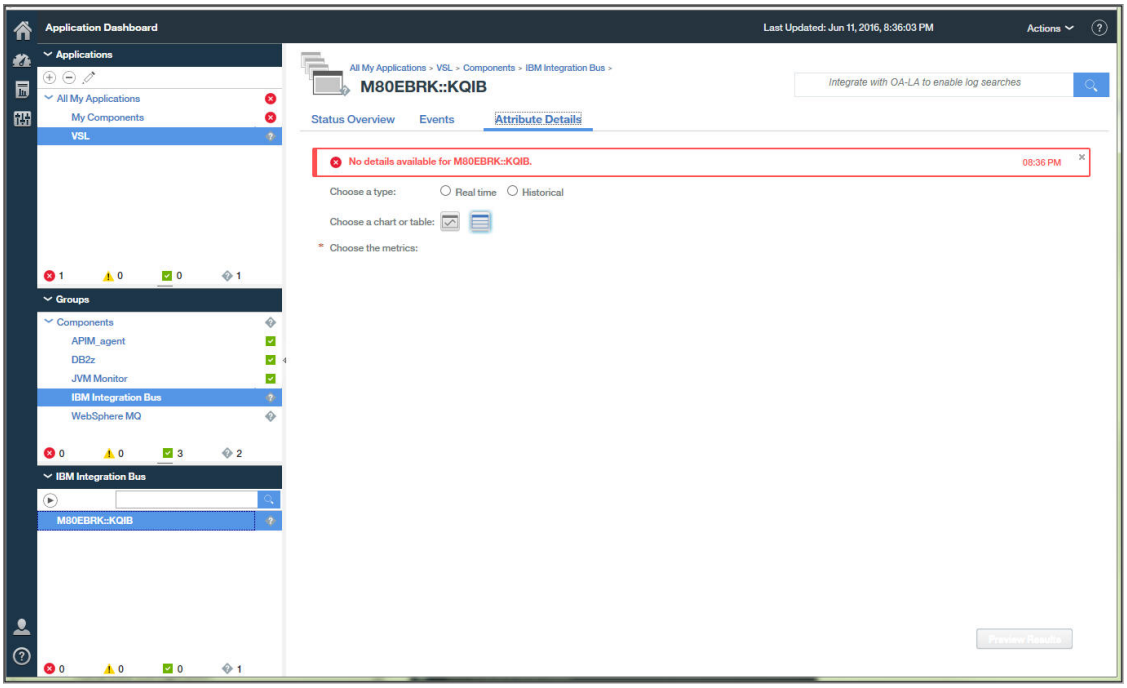


Application Performance Dashboard - Instância

Após o usuário clicar dentro de um dos widgets de grupo de resumo do agente off-line, a guia **Visão geral de status** mostra widgets de gráfico e tabela para o agente selecionado. Mas, assim como o widget de grupo de resumo, somente uma mensagem de que o agente está off-line é exibida, em vez de KPIs para a instância de agente.



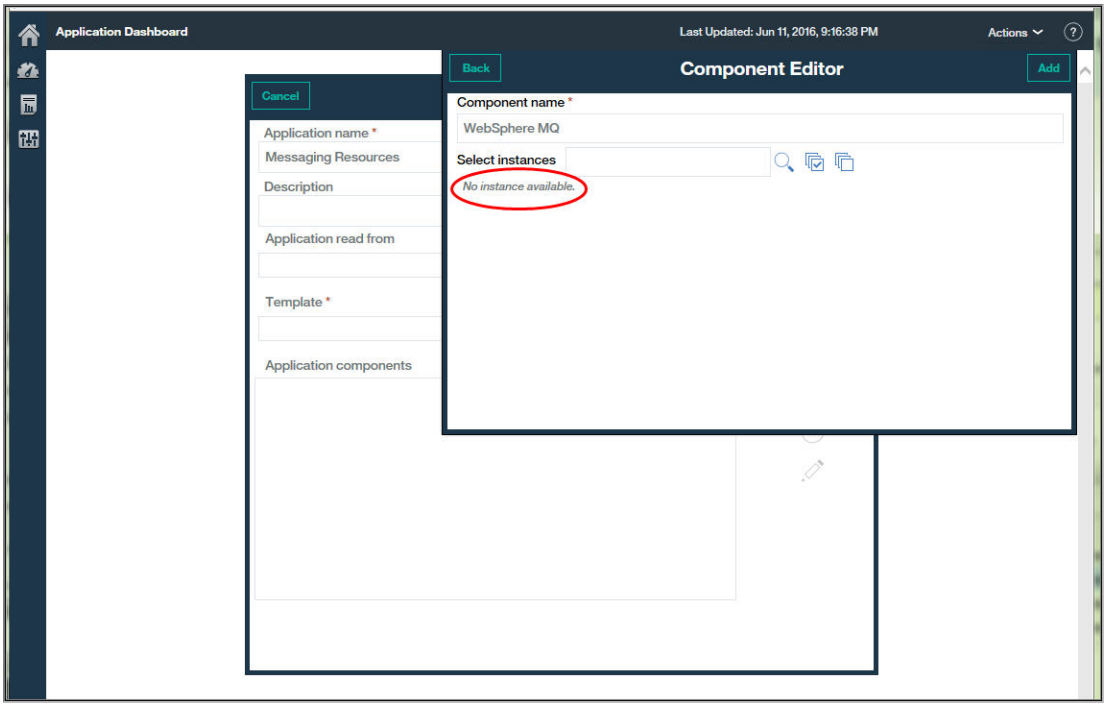
Após o usuário clicar na guia **Detalhes do Atributo**, uma mensagem informa que nenhum detalhe está disponível para a instância de agente. Não é possível criar um gráfico customizado ou tabela para a instância do agente off-line.



Editor de Aplicativos

No Application Performance Dashboard, após o usuário clicar na ferramenta Aplicativos **Incluir aplicativo** ou **Editar aplicativo** do navegador, a janela Editor de aplicativos é exibida.

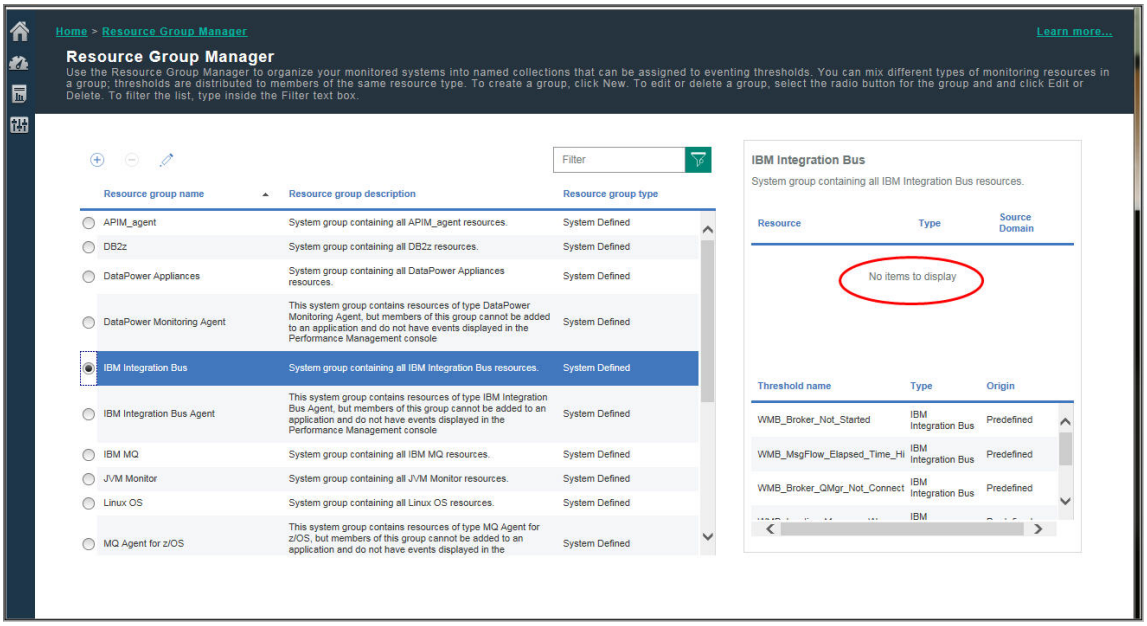
Após o usuário clicar em **Incluir componentes** e selecionar um tipo de agente, se nenhum agente desse tipo estiver instalado ou se estiver off-line, uma mensagem informará que nenhuma instância de agente está disponível. Se outras instâncias de agente estiverem disponíveis, elas aparecerão na lista.



Gerenciador de Grupos de Recursos

Após o usuário selecionar **Configuração do Sistema** > **Gerenciador de Grupo de Recursos**, a página é aberta com uma tabela de grupos de recursos. Da mesma forma que você seleciona um grupo, as suas instâncias de agentes constituintes são listadas juntamente com os limites atribuídos.

Se todas as instâncias de agente estiverem off-line, uma mensagem informará que nenhuma instância está disponível.



Conceitos relacionados

"Gerenciando aplicativos" na página 1098
Use as ferramentas que estão disponíveis no Application Performance Dashboard para organizar seus recursos gerenciados nos aplicativos.

"Usando os painéis" na página 1079

Referências relacionadas

"Gerenciador de Grupos de Recursos" na página 980
Seu ambiente monitorado pode ter vários sistemas gerenciados que podem ser categorizados por seus propósitos. Muitas vezes, esses sistemas possuem os mesmos requisitos de limite. Use o **Gerenciador de Grupo de Recursos** para organizar sistemas gerenciados em grupos aos quais é possível designar limites. Também é possível criar grupos de recursos que se correlacionam com suas políticas de controle de acesso baseado na função (RBAC).

Status da Ocorrência

Use o **Status de evento** para obter uma visão geral resumida de eventos abertos para o item de navegador selecionado e para responder aos eventos com status crítico ou de aviso, fazendo drill down em painéis detalhados.

Os indicadores de status são para eventos dos limites que estão em execução em seus sistemas gerenciados. Se o Hybrid Gateways estiver configurado, os eventos também podem ser de situações que estão em execução nos sistemas gerenciados em seu ambiente do IBM Tivoli Monitoring. Se a configuração incluir o IBM Operations Analytics - Predictive Insights, quaisquer anomalias detectadas também serão exibidas.

Eventos para alguns limites não são exibidos no Application Performance Dashboard. Os limites usam atributos para recursos que não são publicados, o que pode ocorrer em agentes que têm suporte a subnós. (Para obter uma descrição de subnós, consulte o tópico Agent Builder,).

Crítico, Aviso, Normal

- Os indicadores de status consolidam as severidades de evento a partir dos limites:

  O status Crítico indica todos os eventos com uma severidade Fatal ou Crítica

  O status Aviso indica todos os eventos com uma severidade Secundária ou de Aviso

O status Normal indica todos os eventos com uma severidade Desconhecido

O status Desconhecido indica que o sistema gerenciado está off-line. Após 4 dias off-line, o sistema gerenciado é removido de quaisquer aplicativos e não é mais exibido nos painéis. Para verificar o status, parar ou iniciar um agente, consulte "Utilizando comandos do agente" na página 175

- V6-V7 Quando um ou mais Hybrid Gateways estiverem configurados, os indicadores de status para eventos de situações do Tivoli Monitoring serão os mesmos que para os limites, exceto que o status Normal indica eventos com as severidades Inofensivo, Informativo ou Desconhecido.
- Quando seu ambiente gerenciado incluir IBM Operations Analytics - Predictive Insights, quaisquer anomalias detectadas serão indicadas por um ícone em forma de losango sobre o indicador de status, como . Para obter mais informações, consulte "Investigando anomalias com Operations Analytics - Predictive Insights" na página 1111.

Medidor de porcentagem de Resumo de Severidade de Evento

- O medidor de Resumo de Severidade do Evento mostra as porcentagens de status de evento Crítico, Aviso e Normal. Por exemplo, 50.00% 50.00% mostra que 50% dos eventos são de limites com severidade Secundário ou Aviso e 50% são de limites com severidade Fatal ou Crítico.
- Também são relatados o número total de eventos e quantos há em cada nível de status.
- A contagem de evento inclui quaisquer anomalias do Operations Analytics - Predictive Insights. Por exemplo, um total de "8 incluindo 1 anomalia" significa que há 7 eventos de limite e 1 evento de anomalia.

Tabela de eventos

- A tabela de eventos abertos e status é definida pelo item do navegador selecionado: aplicativo, grupo, subgrupo ou instância.
- Os eventos são classificados pela coluna **Severidade**, com a severidade mais alta mostrada primeiro. Clique em um título da coluna para alterar a ordem de classificação.
- Cada linha fornece as seguintes informações sobre o evento:

  Nome do limite
  O nome que foi dado ao limite.

  V6-V7 O nome que foi fornecido para a situação.

  Status
  O status do evento, como **Abrir**.

  Severidade
  O valor da severidade do evento: Crítico (aplica-se às severidades de limite Fatal e Crítico), Aviso (aplica-se às severidades de limite Secundário e Aviso) ou Normal (aplica-se às severidades de limite Desconhecido; para eventos do Tivoli Monitoring, aplica-se às severidades Inofensivo, Informativo e Desconhecido).

  O status Desconhecido indica que o sistema gerenciado está off-line. Após 4 dias off-line, o sistema gerenciado é removido de quaisquer aplicativos e não é mais exibido nos painéis. (Para verificar o status, parar e iniciar o agente, consulte"Utilizando comandos do agente" na página 175.)

  Quando seu ambiente gerenciado incluir IBM Operations Analytics - Predictive Insights, a análise de dados aplicada aos dados históricos pode detectar uma anomalia e abrir um evento. Um evento aberto para uma anomalia detectada é indicado por um ícone sobrepondo o indicador de status, como . Clique no link **Visualizar análise de anomalia** para abrir a visualização **Diagnóstico do serviço** do Predictive Insights em uma nova guia ou janela do navegador. Use a visualização **Diagnóstico de Serviço** para revisar o comportamento anômalo nos componentes que suportam o aplicativo.

Item de Exibição
Aplica-se somente a conjuntos de dados de várias linhas. O item de exibição é um atributo-chave selecionado para o limite para distinguir vários eventos um dos outros que foram abertos para o mesmo sistema gerenciado.

Origem
O nome do host do sistema ou outro nome derivado do agente de monitoramento que identifica a origem do evento.

Registro de data e hora
A data e hora em que ocorreu o evento ou em que a condição foi observada pelo agente de origem, expressas no fuso horário do usuário do Console do Cloud APM.

Se um agente for reiniciado ou as definições de limite forem modificadas para um agente, em seguida, os eventos de amostra do agente serão fechados e reabertos, se a condição de limite ainda for true. Nesses cenários, o valor de `Timestamp` é atualizado para a hora em que o agente de origem reabriu o evento.

Para eventos puros, um novo evento é aberto pelo agente e substitui a instância de evento anterior sempre que o agente de origem determina que a condição de limite é verdadeira. Um evento puro permanece aberta para 24 horas (ou um número configurável de horas) após a última vez que a condição de limite avaliada como true. Apenas a instância mais recente de um evento puro é exibida no Console do Cloud APM.

Descrição
A descrição, caso alguma tenha sido gravada para o limite.

- Clique em uma linha para expandir os detalhes sobre o evento:

Nó
O nome do sistema gerenciado da instância do nó.

Para agentes com subnós, a opção **`Ativar eventos de subnó`** controla se os subnós são mostrados. Para obter mais informações, consulte “Integração de UI” na página 1073.

ID do Limite
O identificador de limite.

Registro de Data e Hora Global
A data e hora em que o evento foi recebido do agente de origem pelo Servidor Cloud APM, expressas no fuso horário do usuário do Console do Cloud APM.

Type
Se o evento é puro ou de amostragem. Eventos puros são notificações não solicitadas. Os limites para eventos puros não possuem nenhum intervalo de amostragem ou métrica constante que pode ser monitorada para valores atuais.

Descrição
A descrição, caso alguma tenha sido gravada para o limite.

Fórmula
A fórmula como está escrita no Editor de limite. Por exemplo, `Percent Failed > 10.000 AND Transaction Definition Name != 'Ignore_Resources'`.

Se a função Customização de Slot EIF foi usada para customizar o valor do slot base **`msg`**, o valor do slot **`msg`** customizado será exibido em vez da fórmula de limite. Para obter mais informações, consulte “Encaminhar Evento do EIF?” na página 986 no tópico do Gerenciador de Limite e “Customizando um evento para encaminhar para um receptor EIF” na página 990.

É possível selecionar e expandir outras linhas ou clicar novamente para reduzir uma linha. Enquanto uma linha está expandida, é possível fazer drill down nos painéis do sistema gerenciado que podem ser usados para ajudar a determinar a causa do evento.

Investigando anomalias com Operations Analytics - Predictive Insights

Somente IBM Cloud Application Performance Management: quando o ambiente gerenciado inclui o IBM Operations Analytics - Predictive Insights, as análises aplicadas aos dados históricos podem detectar

anomalias e eventos abertos. Use o Application Performance Dashboard para localizar e visualizar anomalias que foram detectadas pelo Operations Analytics - Predictive Insights.

Antes de Iniciar

Operations Analytics - Predictive Insights deve ser integrado ao ambiente do Cloud APM para que você seja alertado sobre anomalias no Application Performance Dashboard. Para obter mais informações, consulte “Integração com Operations Analytics - Predictive Insights” na página 970.

Sobre Esta Tarefa

O Application Performance Dashboard mostra o resumo de status dos aplicativos em seus domínios e os sistemas gerenciados de seu componente. Indicadores de status de eventos nas caixas de resumo do painel **Todos os Meus Aplicativos** mostram as severidades Crítico, Aviso e Desconhecido. Se os eventos incluem anomalias que são detectados pelo Operations Analytics - Predictive Insights, o indicador de status inclui um ícone de anomalia: , , ou . O mesmo indicador de anomalias críticos e de avisoO mesmo indicador de anomalias críticos e de aviso aparece próximo ao **Eventos** da guia título como você pesquisa detalhada para o aplicativo, grupo e páginas de painel da instância: Events 2. Para obter uma demonstração prática, inicie o IBM Cloud Application Performance Management Demo Guiada, role para baixo na lista Tarefas, E selecione *Identificar & Diagnosticar Predictive Insights Anomalias* .

Procedimento

Conclua estas etapas para identificar anomalias e vê-las na visualização Operations Analytics - Predictive Insights **Diagnóstico de Serviço** do:

1. Clique em **Desempenho** > **Application Performance Dashboard** para abrir o painel **Todos os Meus Aplicativos**.
2. Se uma caixa de resumo tiver um indicador de status **Eventos** mostrando o ícone de anomalia, clique no link **Eventos**.

   O painel do aplicativo é aberto na guia **Eventos**. O **Resumo da Severidade do Evento** relata o número total de eventos incluindo o número de anomalias.
3. Clique em uma linha da tabela de um evento com anomalia, indicado na coluna **Severidade** pelo , ou .

   A linha é expandida para mostrar os detalhes do evento.
4. Clique em **Visualizar Análise de Anomalia** para abrir a visualização Operations Analytics - Predictive Insights **Diagnóstico de Serviço** em uma janela ou nova guia do navegador.

O que Fazer Depois

- Use a visualização **Diagnóstico de serviços** para revisar o comportamento anômalo nos componentes que suportam o aplicativo. Clique no para abrir a ajuda on-line da visualização **Diagnóstico de Serviço**.
- Retorne ao painel do aplicativo e procure os outros eventos no sistema gerenciado que pode indicar um problema relacionado. Clique na guia **Visão Geral do Status**, e realize drill down na instância do sistema gerenciado na qual o evento ocorreu para investigação adicional. Use as informações para determinar quais ações precisam ser executadas para evitar os problemas identificados pelo Predictive Insights.
- Se você espera ver anomalias mas nenhuma delas é exibida, o tempo de treinamento do Operations Analytics - Predictive Insights poderá não ser suficiente para produzir anomalias. Duas semanas é o tempo típico de treinamento. Também é possível que configuração adicional seja requerida.

Visualizações customizadas

Use o IBM Cloud Application Business Insights Universal View para aprimorar o valor que as páginas predefinidas do Application Performance Dashboard já fornecem customizando suas próprias páginas.

O Universal View pode ser usado para exibir os dados de monitoramento de recurso. Ele não pode ser usado para exibir dados de transações sintéticas, dados de rastreamento de transação, dados do agente de tempo de resposta e dados de diagnósticos detalhados. Usando o Universal View, é possível construir rapidamente páginas de monitoramento para um aplicativo e salvá-las para visualização. Ao visualizar uma página de painel customizada salva, é possível visualizar o painel no modo de atualização automática, exportar o painel em um arquivo de dados brutos, editar o painel ou excluir o painel.

As quatro funções padrão no Cloud APM, Administrador de função, Administrador de monitoramento, Administrador do sistema e Usuário de monitoramento, têm permissões diferentes para visualizar e modificar páginas de painel. Para obter informações adicionais, consulte Tabela 1. Funções e permissões .

As opções que estão disponíveis na guia **Visualizações customizadas** dependem se a página está sendo editada ou visualizada.

Criando e gerenciando páginas customizadas

Use a guia Visualizações customizadas para criar ou editar páginas de painel para um aplicativo, um grupo ou uma instância selecionada ao incluir ou atualizar widgets que são preenchidos com as métricas de recursos de sua escolha.

Sobre Esta Tarefa

As páginas criadas e salvas são associadas ao aplicativo selecionado. Por exemplo, o aplicativo Gerenciamento de Inventário no Cloud APM Demo Guiada possui os seguintes agentes de monitoramento: S.O. Linux, MySQL, Node.js, Hadoop e Ruby. É possível criar e salvar uma página customizada em qualquer nível do navegador a partir do aplicativo para a instância e, em seguida, abri-la no mesmo nível em que foi criada. Uma página criada em um nível específico pode ser aberta somente no mesmo nível. As métricas disponíveis para os widgets podem ser de qualquer um dos recursos no aplicativo. Usando o exemplo de Gerenciamento de Inventário, é possível criar uma página com uma tabela no Agente Ruby, um gráfico no agente do S.O. Linux, e assim por diante.

Procedimento

As páginas criadas e salvas são associadas ao aplicativo selecionado. Conclua as seguintes etapas para criar e customizar uma página de painel:

1. Depois de abrir o Application Performance Dashboard no menu **Desempenho**, selecione um aplicativo.

   A guia **Visualizações Customizadas** é exibida após as guias **Visão Geral do Status** e **Eventos**. Também é possível realizar drill down para o grupo, subgrupo ou nível de instância do navegador.
2. Clique na guia **Visualizações Customizadas**.

   A guia mostra a janela **Selecionar um Modelo para a Página Customizada** ou a página padrão se ela já estiver configurada.

   - Se a janela **Selecionar um Modelo para a Página Customizada** estiver aberta, vá para a etapa 4.
   - Se a página padrão for exibida, vá para a etapa 3.
3. Clique em **Incluir** para criar uma nova página.
4. Clique em um modelo a partir das opções de modelo padrão a seguir:
   - Modelo 1x1
   - Modelo 1x2
   - Modelo 2x2
   - Modelo 2x3
   - Modelo 3x3
   - Modelo 3x2
   - Modelo 2x1

- Modelo 1x3
- Modelo 3x1

Se você clicar em **Voltar**, a página que estiver marcada como favorita ou a primeira página na lista será aberta. Se nenhuma página existir, então, a janela **Selecionar um modelo para sua página customizada** será aberta.

5. Customize o modelo. Para detalhes, consulte Customizando modelos.
6. Crie um widget. Para detalhes, consulte “Definindo propriedades do widget” na página 1116.
7. Clique em  **Configurar intervalo de tempo padrão para a página** e configure o período de retenção de dados padrão para a página para 1, 2, 4, 12 ou 24 horas.
8. Quando estiver pronto para salvar a página, conclua estas etapas:
   a) No campo **Nome da Página**, insira o nome para a página.

      Importante: Espaço, sublinhado (_) e traço (-) são permitidos no campo **Nome da página**. No entanto, o traço seguido por sublinhado (-_) não é permitido. Por exemplo, `System-_Overview` não é permitido.

   b) Clique em **Salvar**.

      Podem ocorrer as seguintes mudanças no painel ou a mensagem pode ser exibida:

      - A mensagem `Painel salvo` é exibida.
      - Se ***** for selecionado em **Configurar condições**, a seguinte mensagem será exibida:

        ```
        Você selecionou * na Instância de recurso ou em Configurar condições, o
        que resultará em um grande número de série de dados (como linhas em um
        gráfico). O grande número de séries de dados pode tornar a capacidade de
        leitura da página ou o desempenho inutilizável. O limite recomendado
        para este gráfico é 50 série de dados. A inclusão de valores específicos
        ajuda a deixar os dados dentro dos limites recomendados e resulta em uma
        melhor experiência do usuário.
        ```

      - É exibido um indicador vermelho no  para indicar que o tipo de gráfico não está selecionado e é preciso selecioná-lo.
      - É exibido um indicador vermelho no  para indicar que a métrica de seleção não está selecionada e é preciso selecioná-la e, depois, é exibida a seguinte mensagem:

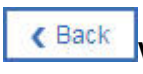
        ```
        Uma métrica deve ser salva para salvar um gráfico.
        ```

9. Selecione qualquer uma das opções a seguir na barra de título da página:

Opção	Descrição
 **Recuperar Tipos de métricas de recursos mais recentes**	Clique para atualizar tipos de métricas. Se houver mudança no tipo de métrica ou na métrica quando alguma correção de agente for aplicada, será preciso atualizar os tipos de métricas. O intervalo entre duas atualizações é restrito a 15 minutos. Se você clicar em  **Recuperar Tipos de métricas de recursos mais recentes** em 15 minutos da atualização anterior, a seguinte mensagem será exibida: `O cache de metadados foi atualizado recentemente. Espere` *`time_remaining`* `minuto(s) para recarregá-lo.` Quando os metadados estiverem carregando, uma imagem de carregamento será exibida. Quando os metadados forem carregados, a seguinte mensagem será exibida:

Opção	Descrição

	`Cache de metadados recarregado com sucesso.`
	Se a atualização de metadados levar mais de 30 segundos, a seguinte mensagem será exibida:
	`O recarregamento do cache de metadados pode levar mais algum tempo.`
	`Deseja esperar até que ele seja concluído?`
	É possível clicar em **Ok** ou em **Cancelar**.

 **Visualizar Painel**	Clique para visualizar os dados no painel. **Importante:** O limite para o número de linhas que são retornadas por definição de dados é 11.000 linhas. Por padrão, os dados mais recente são exibidos quando o limite é ultrapassado. Para um alto volume de dados, não são exibidos todos os dados para o intervalo de tempo selecionado. Por exemplo, se você selecionar para visualizar as últimas 24 horas de dados para uma origem de dados de alto volume, apenas as últimas 6 horas de dados podem ser exibidas se o limite de 11.000 linhas for atingido. Se em um gráfico as séries de dados excederem 50, a seguinte mensagem será exibida no widget: `Este gráfico não pode ser carregado porque o número de séries de dados (como linhas em um gráfico) excede 50. O número de séries de dados atualmente é` *`current_data_series`*`. É possível reduzir o número selecionando menos métricas ou instâncias de recursos, ou refinando as Condições por métrica. Para obter informações adicionais, consulte Definindo propriedades de widget: para Cloud APM - http://ibm.biz/widgetprops e para Cloud APM Private - http://ibm.biz/widgetprops-private` Se um gráfico estiver demorando mais de 30 segundos para carregar, a seguinte mensagem será exibida no widget: `Este gráfico demorou muito para carregar devido à grande quantidade de dados, à longa latência de rede ou a um problema de conectividade. Reduza o número de Instâncias de recursos ou refine as Condições por métrica para limitar os dados. Para obter informações adicionais, consulte Definindo propriedades de widget: para Cloud APM - http://ibm.biz/widgetprops e para Cloud APM Private - http://ibm.biz/widgetprops-private`
Salvar como	Clique na seta próxima a **Salvar** e clique em **Salvar como** e especifique um nome diferente no campo **Nome da página** para salvar a página com um nome diferente. **Importante:** Se você especificar um nome de página igual ao de uma página existente, a página existente será sobrescrita.
 **Excluir**	Clique para excluir a página atual.
 **Voltar**	Clique para voltar para a página anterior ou para a página favorita.

O que Fazer Depois
Visualize as páginas customizadas conforme descrito em "Visualizando páginas customizadas" na página 1119.

Customizando modelos
É possível customizar o modelo ao redimensionar, mover ou incluir itens temporários do widget, de acordo com o requisito.

Sobre Esta Tarefa

Lembre-se: É possível customizar um modelo existente e usá-lo. Mas o modelo customizado não pode ser salvo para uso futuro para criar novos painéis.

Procedimento

1. Na guia Visualizações customizadas, clique em  **Editar Modelo**.
2. Selecione um item temporário do widget.

   É possível redimensionar um item temporário do widget de todos os lados e arrastá-lo para um local diferente. Se os widgets se sobrepuserem uns aos outros enquanto você estiver redimensionando ou arrastando-os, a mensagem `Operação de redimensionamento inválida` ou `Operação de movimentação inválida` será exibida.
3. Para incluir um item temporário de widget no modelo existente, conclua as seguintes etapas:
   a) Clique em **Configurar altura da página** nas opções de menu e especifique um valor mais alto para a contagem de linhas e clique em qualquer lugar fora do menu para aumentar a altura da página.
   b) Especifique um item temporário de widget, de acordo com seu requisito na área em branco na página, colocando o ponteiro e arrastando-o para criar uma caixa.
4. Use as opções de menu a seguir para concluir operações diferentes no modelo:

Opção	Descrição
Desfazer	Para desfazer a última ação.
Refazer	Para refazer a última ação.
Excluir caixa selecionada	Para excluir um widget, selecione o widget e clique no ícone **Excluir caixa selecionada**.
Reconfigurado	Para criar um modelo em branco. Para especificar um item temporário do widget no modelo em branco, coloque o ponteiro na área Desenhar Modelos Aqui e arraste-a para criar uma caixa. É possível criar itens temporários do widget de tamanhos diferentes na área Desenhar Modelos Aqui. Os itens temporários podem ser movidos ou redimensionados, mas não podem se sobrepor uns aos outros.
Configurar altura de página	Para configurar a altura da página. É possível especificar a contagem de linhas como 20 a 120 linhas.

5. Clique em  **Editar Modelo** para usar o modelo criado.

O que Fazer Depois
Crie o widget. Vá para a Etapa 6 no tópico Criando e gerenciando páginas customizadas.

Definindo propriedades do widget
Defina propriedades diferentes para os widgets, como métricas e gráficos para visualizar dados em tempo real nos widgets.

Procedimento

Para definir as propriedades para um widget, conclua estas etapas:

1. Em um widget, clique em  para selecionar um tipo de gráfico para exibir dados.
   - Linha
   - Área
   - Barra
   - Grade

   Importante: Para gráficos de linha, de área e de barras, se houver mais de nove legendas, a cor do gráfico se repetirá após a nona legenda. A cor do gráfico é a mesma para a 1ª e a 10ª legendas, a 2ª e a 11ª legendas, e assim por diante.

   É exibido um indicador verde no  para indicar que o tipo de gráfico está selecionado.
2. Especifique as seguintes propriedades do gráfico para gráficos de linhas, áreas, e barras:
   - Rótulo do eixo X
   - Rótulo do eixo Y
   - Mostrar Legenda
   - Mostrar interpolação: os dados que são coletados para serem plotados no gráfico podem incluir alguns valores nulos. Portanto, quando o gráfico é plotado, o gráfico de linha é desconectado no ponto em que ele encontra um valor nulo e múltiplas linhas desconectadas aparecem no gráfico. Se você selecionar Interpolação, a linha no gráfico não parecerá como desconectada no ponto em que ela encontra um valor nulo, conectando-se ao próximo valor válido disponível. Portanto, você obtém uma única linha de gráfico conectado ao selecionar a interpolação.

     Nota: Para o APM V8.1.4.0 IF0005 e versões mais recentes, os gráficos de linha e de área não exibem mais linhas desconectadas para valores nulos. Portanto, o recurso Mostrar Interpolação não é mais necessário e, portanto, ele não é suportado.

   Importante: A grade não possui propriedades.
3. Clique em  para selecionar o conteúdo da métrica.

Opção	Descrição
Tipo de Recurso	Na lista **Tipo de Recurso**, selecione um recurso. Os recursos disponíveis são associados ao aplicativo. Se um recurso que é uma parte do aplicativo não estiver disponível na lista, sua definição de recurso não foi localizada. A definição de recurso não foi publicada ou o sistema gerenciado não está conectado ao Servidor Cloud APM.
Tipo de métrica	Na lista **Tipo de Métrica**, selecione um conjunto de dados que deseja incluir no widget.
Métrico	Na lista **Métrica**, selecione um atributo para incluir na visualização. Os atributos disponíveis são do conjunto de dados selecionado. Para selecionar métricas, conclua as seguintes etapas: a. Clique na lista **Métrica**. É aberta uma janela pop-up onde as métricas são listadas por ordem alfabética, classificadas em ordem crescente. b. Clique nos atributos que estão listados em Métricas (selecione um ou mais) ou clique em **Selecionar todos**.

Opção	Descrição
	Nota: Ao clicar em **Selecionar todos**, todas as métricas na lista são selecionadas. c. Clique em  para incluir métricas na lista **Métricas selecionadas**. d. Se desejar excluir uma métrica em **Métricas selecionadas**, clique em  . e. Clique na lista **Instância de recurso** para fechar a janela pop-up. **Importante:** Para gráficos de linha, de barras e de área, a métrica contendo o valor numérico precisa ser selecionada. As métricas contendo valores de sequência não podem ser exibidas nesses gráficos. **Dica:** Para a grade, limite sua seleção em métricas de acordo com a saída que se ajusta à sua visibilidade na UI.
Instância do Recurso	Inicialmente, a seleção é *, que recupera métricas de todas as instâncias na lista. Retenha a seleção padrão ou selecione a instância na lista. **Importante:** Se você selecionar uma instância, esse widget não poderá ser usado para exibir dados para qualquer outro agente ou instância. Mas é bom especificar a instância para evitar o processamento de dados grandes.
Configurar condição para grupo de métricas	Se o **Tipo de métrica** selecionado tiver vários elementos, como CPUs ou discos, **Configurar condição para o grupo de métricas** exibirá outros elementos para seleção no campo **WHERE**. **Importante:** Especifique valores para elementos no campo **WHERE**. Evite especificar ***** para reduzir o processamento de grandes quantidades de dados. Por padrão, a condição WHERE exibe as últimas 4 horas de dados. Este intervalo de tempo pode ser mudado entre 1 a 24 horas pelo administrador do sistema; consulte “Mudando o intervalo de tempo para dados de condição de WHERE” na página 1119.
Ações	Clique em  **Salvar** para salvar uma métrica. Clique em  **Editar** para editar uma métrica. Clique em  **Excluir** para excluir uma métrica.

4. Para incluir outra métrica, clique em **+ Incluir Outra Métrica**.

   Importante: Não aplicável à grade.
5. Feche a janela **Selecionar Métricas** após todas as métricas serem incluídas.

   Todas as métricas são salvas automaticamente após você fechar a janela **Selecionar Métricas**.

   Podem ocorrer as seguintes mudanças no painel ou a mensagem pode ser exibida:

   - Se ***** for selecionado na lista **Instância de recurso** em qualquer uma das métricas, a seguinte mensagem será exibida:

     ```
     Você selecionou * na Instância de recurso ou em Configurar condições, o que
     resultará em um grande número de série de dados (como linhas em um
     gráfico). O grande número de séries de dados pode tornar a capacidade de
     ```

leitura da página ou o desempenho inutilizável. O limite recomendado para este gráfico é 50 série de dados. A inclusão de valores específicos ajuda a deixar os dados dentro dos limites recomendados e resulta em uma melhor experiência do usuário.

- É exibido um indicador verde no  para indicar que as métricas estão selecionadas corretamente para deixar os dados dentro dos limites recomendados.
- É exibido um indicador laranja no  para indicar que as métricas não estão selecionadas corretamente para colocar os dados dentro dos limites recomendados. ***** é selecionado em **Instância de recurso** ou em **Configurar condições**.

6. Clique em  para inserir o título do widget.
   Se o título do widget não for incluído, o primeiro nome da métrica será designado como o título do widget automaticamente.

O que Fazer Depois
Da mesma forma, inclua gráficos, métricas e títulos em todos os widgets e, em seguida, vá para a etapa 7 no tópico Criando e gerenciando páginas customizadas.

Mudando o intervalo de tempo para dados de condição de WHERE
O intervalo de tempo pode ser mudado entre 1 a 24 horas pelo administrador do sistema.

Procedimento

Para mudar o intervalo de tempo, o administrador do sistema pode concluir as seguintes etapas:

1. Efetue login no servidor APM onde a construção está implementada.
2. Na linha de comandos, execute os seguintes comandos:

   ```
   export CLASSPATH=$CLASSPATH:/install_dir/gaian/lib/derbytools.jar:
   export CLASSPATH=$CLASSPATH:/install_dir/gaian/lib/derbyclient.jar:
   export CLASSPATH=$CLASSPATH:/install_dir/gaian/lib/derby.jar:
   java org.apache.derby.tools.ij
   connect 'jdbc:derby://localhost:port/
   gaiandb;user=gaiandb;password=gaian_db_password;';
   ```

   Nesses comandos, *install_dir* refere-se ao diretório onde o APM foi implementado, por padrão é `/opt/ibm`. No comando **connect**, *port* refere-se ao valor da porta na qual o banco de dados está configurado e *gaian_db_password* é a senha do banco de dados Gaian. Entre em contato com o suporte IBM para obter essa senha.
3. Quando o banco de dados estiver conectado, execute a seguinte consulta para modificar valores para intervalo de hora:

   ```
   UPDATE "OED_TOOL"."PREFERENCETABLE" SET PREFERENCES='-24H' WHERE
   FIELD='TIMEINTERVAL';

   Commit;

   Exit;
   ```

   Aqui o valor do intervalo de hora é fornecido no `SET PREFERENCES='-24H'`. Ele pode ser configurado de 1H para 24H.

Visualizando páginas customizadas

Após criar e salvar páginas de painel para um aplicativo, um grupo, um subgrupo ou uma instância na guia **Visualizações Customizadas**, será possível visualizá-las a qualquer momento. Algumas das opções que podem ser selecionadas incluem atualização da página, seleção de um intervalo de tempo diferente,

edição da página para recuperação de dados de diferentes recursos e exportação do painel como um arquivo de dados brutos.

Procedimento

Conclua estas etapas para visualizar uma página salva na guia **Visualizações Customizadas** do painel.

1. Depois de abrir o Application Performance Dashboard no menu **Desempenho**, selecione um aplicativo.

   A guia **Visualizações Customizadas** é exibida após as guias **Visão Geral do Status** e **Eventos**. Também é possível realizar drill down para o grupo, subgrupo ou nível de instância do navegador.
2. Selecione a guia **Visualizações customizadas**.

   A guia mostra a janela **Selecionar um Modelo para a Página Customizada** ou a página padrão se ela já estiver configurada.
3. Clique em na lista de páginas e selecione uma das páginas salvas na lista.

   As páginas disponíveis foram salvas por você ou compartilhadas por outro usuário.

   Após selecionar uma página salva, as amostras de dados atuais e históricos são relatadas na página.
4. Selecione qualquer uma das opções de visualização na barra de título da página:

Opção	Descrição
Atualizar	Indica que a atualização automática está desativada. Clique para ativar a atualização automática.
Atualizar	Indica que a atualização automática está ligado. Clique para desativar a atualização automática. **Importante:** O tempo de atualização padrão é de 1 minuto.
Exportar > Dados Brutos	Clique para exportar a página como formato DAT. Como vários arquivos DAT são exportados, eles são baixados para o seu computador no formato ZIP. **Lembre-se:** Se o arquivo transferido por download não tiver nenhuma extensão, inclua zip como a extensão para ele. **Importante:** Se o arquivo não foi transferido por download para seu computador, verifique se o software para bloquear janelas pop-up de anúncios está ativado. É possível incluir este site em sua lista de exceções. Extraia o arquivo ZIP transferido por download. Os arquivos extraídos são arquivos de texto simples. O arquivo contém o nome da página, duração, filtros, data, hora, intervalo, título do gráfico e dados. O delimitador de dados é uma barra vertical. Você pode abrir os arquivos DAT usando o editor apropriado ou importar os arquivos para o Excel especificando separadores de valores adequados.
Exportar > PDF	Clique para exportar a página como formato PDF. O arquivo contém o nome da página, o intervalo de tempo, widgets, criado por e relatório criado em.
Editar	Clique para editar a página atual.

Opção	Descrição
	É possível mudar os gráficos e métricas nos widgets, ou incluir novos widgets, mudar o prazo padrão ou editar o nome da página.
Excluir	Clique para excluir a página atual.
Incluir	Clique para criar uma nova página. Para customizar a página e salvá-la consulte “Criando e gerenciando páginas customizadas” na página 1113.

5. Selecione qualquer uma das opções de visualização a seguir no widget:

Opção	Descrição
Tipo de Gráfico	Clique no ícone **Tipo de gráfico** e selecione uma opção apropriada da lista para mudar o tipo de gráfico existente. • Para gráficos de linha e de áreas, as opções **Linhas** e **Áreas** estão disponíveis. • No gráfico de barras, as opções **Barras em cluster** e **Colunas em cluster** estão disponíveis. **Importante:** Para grade, não há opções de tipo de gráfico. Para dados exibidos em uma grade, é possível filtrar os dados da maneira a seguir: a. Clique em **Definir filtro**. A janela **Filtrar** é aberta. b. Especifique valores para **Coluna**, **Condição** e **Valor** para incluir uma regra de filtragem. **Nota:** É possível filtrar valores numéricos e valores de texto selecionando condições apropriadas. c. Clique em **Incluir Regra de Filtragem** para incluir outra regra de filtragem. É possível incluir múltiplas regras de filtragem. d. No campo **Correspondência**, selecione **Todas as regras** ou **Qualquer regra** para filtrar os dados. É possível selecionar **Corresponder maiúsculas e minúsculas** se deseja procurar conforme as maiúsculas e minúsculas do texto que você fornece no campo **Valor**. e. Clique em **Filtrar** para filtrar os dados exibidos na grade. f. Clique em **Limpar filtro** para limpar os resultados do filtro. g. Clique em **Cancelar** para fechar a janela **Filtrar**.
Reduzir	Clique para reduzir o widget.
Expandir	Clique para expandir o widget.
Maximizar	Clique para maximizar o widget para o tamanho da página.
Restaurar	Clique para restaurar o widget para seu tamanho original.

Opção	Descrição
Legendas	O widget contém caixas de seleção para cada métrica. Selecione ou desmarque as caixas de seleção para cada métrica para visualizar dados de uma determinada métrica ou de várias métricas.

6. É possível filtrar os dados na página usando as listas **Data**, **Horário** e **Intervalo**. Também é possível definir um filtro Customizado para a página para exibir dados para os intervalos de data e hora selecionados. Para usar o filtro Customizado, na lista **Intervalo**, selecione **Customizado** e, em seguida, na janela **Seleção de período de tempo**, selecione os intervalos de data e hora necessários.

   Nota:

   - A opção de filtro customizado está disponível a partir do APM V8.1.4.0 IF0005 em diante. As páginas que são criadas usando versões anteriores do Cloud APM não exibem a opção de filtro Customizado.
   - Use o filtro Customizado para filtrar dados para um intervalo de tempo mínimo de 1 minuto e o intervalo de tempo máximo de 24 horas.
   - Ao aplicar um filtro customizado na janela **Seleção de período de tempo**, se você clicar em **Cancelar** na página do painel, a lista **Intervalo** não exibirá o intervalo que foi aplicado anteriormente.
   - Se você aplicar o filtro Customizado a uma página, os dados na página não serão atualizados automaticamente.

7. Para configurar uma página padrão, clique em na lista de páginas e clique no  **Favorito** ao lado do nome da página que você deseja configurar como a página padrão.

Utilitários do painel

Use as opções disponíveis para gerenciar a aparência e o comportamento de páginas do **Application Performance Dashboard**.

Copiando a URL do painel

Após navegar para um local na hierarquia do aplicativo, a URL na caixa de endereço do navegador não será alterada para a nova visualização. É possível copiar a URL da página do Application Performance Dashboard sendo exibida. Cole a URL em uma nova janela do navegador para abrir a página do painel ou use a URL para acessar o painel posteriormente ou para compartilhar com outras pessoas.

Procedimento

1. Navegue para a página Application Performance Dashboard da qual deseja se lembrar.
2. Clique em **Ações** > **Copiar URL**.
3. Clique com o botão direito no link de hipertexto **Link para a Página Atual** e selecione a opção para copiar a URL.

O que Fazer Depois

Mantenha uma cópia da URL ou compartilhe com outros usuários no ambiente gerenciado. Após você colar a URL na caixa de endereço do navegador, a página de painel de destino é aberta no Console do Cloud APM.

Se você não tiver efetuado logon no Servidor Cloud APM, será solicitado que você insira seu ID do usuário e sua senha para que a página de painel de destino possa ser exibida. Se a página **Introdução** for aberta em vez da página do painel, pressione F5 ou clique no botão da barra de ferramentas para atualizar o navegador. É possível desativar a página **Introdução** para futuras sessões de trabalho limpando a caixa de seleção "Mostrar esta página **Introdução** na inicialização".

Configurando um Rastreio

Ajuste as configurações de rastreio para ajudar seu administrador ou o Suporte IBM a diagnosticar a causa dos problemas com Application Performance Dashboard.Vários níveis de rastreio estão disponíveis enquanto você trabalha com o navegador e a guia **Visão geral de status**. É possível iniciar um nível detalhado de rastreio exatamente no ponto na interface com o usuário em que você está com um problema e, em seguida, retornar o rastreio a um nível reduzido depois de capturar os dados de log necessários. Por exemplo, se um painel específico estiver se comportando de forma inesperada, será possível aumentar o nível de rastreio antes de abrir o painel para registrar a atividade e, em seguida, retornar a criação de logs de rastreio para o nível normal.

Sobre Esta Tarefa

Execute as etapas a seguir para configurar o nível de rastreio ao desejar aumentar ou reduzir a quantia de criação de logs de rastreio.

Procedimento

1. Se Application Performance Dashboard não estiver aberto, selecione-o na opção **Desempenho** na barra de navegação.
2. Selecione Todos os Meus Aplicativos ou um aplicativo do navegador ou guia Visão Geral de Status.
3. Clique em **Ações** > **Nível de Rastreio** e selecione um dos seguintes níveis:
   - **Detalhado** para ter toda a atividade registrada em log. O nível de rastreio detalhado inclui a criação de logs de rastreio Moderado, Leve e Mínimo.
   - **Moderado** para ter as mudanças na variável registradas, como quais parâmetros foram passados e quais cálculos foram feitos. O nível de rastreio moderado inclui criação de log de rastreio Leve e Mínimo.
   - **Leve** para registrar o erro e a atividade da variável. Você pode desejar configurar o rastreio para esse nível, se tiver um problema, como nenhum dado sendo retornado, mas o painel continua a funcionar. O nível de rastreio leve inclui a criação de log de rastreio Mínimo.
   - **Mínimo** é a configuração padrão e registra apenas os erros irrecuperáveis. É possível configurar o nível de rastreio novamente como mínimo após coletar uma sequência de atividade específica. Mesmo que um nível de rastreio diferente foi configurado antes de efetuar logout, o rastreio sempre será reconfigurado para o nível mais baixo da próxima vez que efetuar login.
4. Se desejar enviar registros de desempenho para um arquivo de criação de log comum, selecione **Ativar Estatísticas de Desempenho de Log**.

   As informações de desempenho do console são gravadas no servidor em que podem ser combinadas com estatísticas de desempenho do servidor para fornecer tempo de resposta de transação de ponta a ponta. As informações de desempenho necessárias incluem o horário que uma função foi iniciada e o horário em que foi encerrada.

Resultados

O rastreio é ajustado para o nível escolhido. A próxima vez que efetuar login, o rastreio estará como **Mínimo** até que altere-o novamente.

Para manter o tráfego de comunicações em um mínimo, as mensagens de log são transferidas em lote. Uma transferência final é feita após efetuar logout, seja manualmente ou após um período de tempo limite. (Se o navegador falhar, nenhuma criação de log final será enviada). O log é salvo no computador servidor e chamado de `itp.log`. Um novo `itp.log` é criado toda vez que o servidor for reiniciado.

Se você configurar **Ativar Estatísticas de Desempenho de Log**, registros semelhantes aqueles no exemplo a seguir serão salvos em *`install_dir`*`/usr/servers/apmui/logs/itp.log`:

```
<record>
    <date>2013-10-02T10:52:46</date>
    <millis>1380736366788</millis>
    <sequence>28008</sequence>
    <level>INFO</level>
    <class>StatusItemList</class>
    <method>tracing</method>
```

```
    <thread>96</thread>
    <message>BeginTrace:onSelectApp:272wt877d05</message>
</record>
<record>
    <date>2013-10-02T10:52:46</date>
    <millis>1380736366809</millis>
    <sequence>28009</sequence>
    <level>INFO</level>
    <class>StatusItemList</class>
    <method>tracing</method>
    <thread>96</thread>
    <message>EndTrace:onSelectApp:272wt877d05</message>
</record>
```

Bloqueando o Console do Cloud APM

É possível bloquear temporariamente sua sessão de trabalho sem precisar efetuar logout do Console do Cloud APM. O recurso de bloqueio de sessão não está disponível no iPad da Apple.

Procedimento

1. Enquanto estiver logado no Console do Cloud APM, clique em ***apmadmin*** > **Sessão de Bloqueio**, em que *apmadmin* é o nome que você usou para efetuar login.

   A tela de log in é exibida e sua sessão é bloqueada.
2. Para desbloquear sua sessão, insira a senha para seu ID do usuário.

   Sua sessão de trabalho é retomada.

Relatórios

Os relatórios de histórico estão disponíveis no Console do Cloud APM para dados que são coletados pelo Response Time Monitoring Agent, WebSphere Applications agent e o Synthetic Playback agent.

É possível executar relatórios a partir do painel **Todos os meus aplicativos**. Em qualquer página do Console do Cloud APM, clique em **Desempenho** > **Application Performance Dashboard** para abrir o painel **Todos os Meus Aplicativos**.

Nota: Na primeira vez que executar um relatório, você deverá efetuar login no Tivoli Common Reporting como um usuário com permissão para executar relatórios Cloud APM. O IBM Cognos Viewer é o visualizador de saída de relatório padrão.

Relatórios do Response Time Monitoring Agent

Para visualizar os relatórios **Desempenho e Uso do Aplicativo** ou **Comparar Desempenho do Aplicativo em Dois Períodos**, selecione um aplicativo que inclua sistemas gerenciados por Agente Response Time Monitoring e selecione **Ações** > **Ativar para Relatórios**.

Para visualizar os relatórios **Todos os Meus Aplicativos** ou **Comparar Desempenho de Vários Aplicativos**, selecione **Todos os Meus Aplicativos** e selecione **Ações** > **Ativar para Relatórios**.

Relatórios do WebSphere Applications agent

Para visualizar quaisquer relatórios WebSphere Applications agent, selecione um aplicativo que inclua sistemas gerenciados por WebSphere Applications agent e selecione **Ações** > **Ativar para Relatórios**.

Synthetic Playback agent

Para visualizar quaisquer relatórios Synthetic Playback agent, selecione um aplicativo que inclua transações sintéticas e selecione **Ações** > **Ativar para Relatórios**.

Nota: Se a opção **Ativar para Relatórios** estiver ausente no menu **Ações**, verifique se os relatórios do Cloud APM estão instalados corretamente.

Para obter informações sobre os navegadores suportados para visualizar os relatórios do Synthetic Playback agent, do Agente Response Time Monitoring e do WebSphere Applications agent, consulte os Relatórios de Compatibilidade de Produto de Software para Cognos 10.2.1.7.

Relatórios do Response Time Monitoring Agent

Relatórios de histórico estão disponíveis para dados que são coletados pelo Agente Response Time Monitoring. Os relatórios do Response Time Monitoring Agent não estão disponíveis no Cloud APM, Base. Eles estão disponíveis somente no Cloud APM, Advanced.

Há dois tipos de relatórios disponíveis para dados que são coletados pelo Agente Response Time Monitoring: ativo e simples.

Relatórios ativos
Os relatórios ativos são visualizados em um navegador no formato MHTML. O Internet Explorer suporta MHTML, por padrão. Para outros navegadores, um plug-in de suporte MHTML pode ser instalado. Os relatórios ativos também são conhecidos como relatórios interativos offline.

Relatórios simples
Os relatórios simples são visualizados no IBM Cognos Viewer. O IBM Cognos Viewer é o visualizador de saída de relatório padrão.

Os relatórios predefinidos históricos a seguir estão disponíveis para dados que são coletados pelo Agente Response Time Monitoring:

Tabela 254. Relatórios de histórico predefinidos

Relatório	**Type**
Todos os meus aplicativos	Ativo
Uso e desempenho do aplicativo	Ativo
Comparar desempenho do aplicativo em dois períodos de tempo	Simples
Comparar desempenho de múltiplos aplicativos	Simples

Os dados para os relatórios são armazenados no banco de dados DATAMART Db2. Os relatórios exibem dados resumidos por dia, por semana e por mês, que são mantidos por 26 semanas, 12 meses e 3 anos, respectivamente. O Cloud APM não fornece scripts ou instruções para mudar esses períodos de retenção.

Para obter mais informações sobre o mapeamento entre relatórios do Agente Response Time Monitoring e Performance Management, consulte Mapeamento de atributos do agente Response Time Monitoring.

Relatório Todos os Meus Aplicativos
Use o relatório Todos os meus aplicativos para visualizar informações sobre os dispositivos do usuário, volume de dados, tempos de resposta e contagens de erro.

Nesse relatório, visualize as informações para todos seus aplicativos. Especifique o período de tempo de relatório como **Último dia** (padrão), **Última semana** ou **Último mês**. Visualize as informações a seguir pelo período de tempo selecionado pelo aplicativo.

- Gráfico de colunas empilhadas de contagem de transações
- Gráfico de colunas de volume de dados de transação
- Gráfico de colunas do tempo de resposta de transação média
- Gráfico de colunas empilhadas de contagens de erro

Relatório de Uso e Desempenho do Aplicativo
Use este relatório para visualizar as informações de desempenho, disponibilidade e dispositivo do usuário para aplicativos únicos.

Na janela **Selecionar um aplicativo**, selecione um aplicativo. Clique em **Avançar**. Em **Selecionar transações chaves para aplicativo**, selecione as transações pelas quais deseja filtrar o relatório. Clique em **OK**. Este relatório possui três guias - Desempenho, Disponibilidade e Dispositivos. O intervalo de tempo padrão é semana.

Na guia Desempenho, visualize as informações a seguir pelo intervalo de tempo selecionado para o aplicativo que está visualizando atualmente no Painel do Application Performance:

- Transações do gráfico de linha do tempo médio de resposta (chave)
- Gráfico de linha do tempo de resposta médio da transação por sucesso, erro do servidor e erro do cliente
- Gráfico de barras e gráfico de linhas do volume de dados de transação, as barras mostram o volume de dados da transação e a linha mostra a média de volume de dados da transação
- Gráfico de barra e de linha da contagem de transação, as barras mostram a contagem de transação e a linha mostra os valores polinomiais e média de movimentação

Na guia Disponibilidade, visualize as informações a seguir pelo intervalo de tempo selecionado para o aplicativo que você está visualizando atualmente no Painel do Application Performance:

- Gráfico de barras empilhadas de êxito versus porcentagem de transação com falha, as falhas são divididas em erro do servidor e erro do cliente
- Gráfico de barras empilhadas de êxito versus contagem de transação com falha por tipos de dispositivo, as falhas são divididas em erro do servidor e erro do cliente
- Gráfico de pizza dos códigos de erros que ocorrem com mais frequência

Na guia Dispositivo, visualize as informações a seguir pelo intervalo de tempo selecionado para o aplicativo que está visualizando atualmente no Painel do Application Performance:

- Gráfico de barras de transações por tipo de dispositivo
- Gráfico de barras de transações por sistema operacional do dispositivo
- Gráfico de barras de transação por navegador do dispositivo
- Tabela que mostra o desempenho da transação por dimensões, é possível filtrar esta tabela com base no tipo do dispositivo, sistema operacional do dispositivo, marca do dispositivo e navegador do dispositivo

Relatório Comparar desempenho do aplicativo em dois períodos de tempo
Use este relatório para examinar o desempenho do aplicativo para um aplicativo selecionado.

Na janela **Selecionar aplicativo e frequência de tempo**, especifique um aplicativo e a frequência de tempo (semanal, diário, mensal). Na janela **Selecionar períodos de tempo**, escolha os períodos de tempo apropriados para o intervalo de tempo e clique em **OK**.

O relatório exibe os gráficos a seguir para o aplicativo selecionado, para os períodos de tempo selecionados pelo intervalo de tempo selecionado:

- Gráfico de linha de contagem de transação para tipo de dispositivo
- Gráfico de linha do volume de transação
- Gráfico de linha do tempo médio de resposta
- Gráfico de linha de contagem de erros

Relatório Comparar desempenho de vários aplicativos
Use este relatório para comparar o desempenho de múltiplos aplicativos para o mesmo período de tempo.

Em **Selecionar aplicativos e frequência de tempo**, especifique um aplicativo e a frequência de tempo (semanal, diária, mensal). Clique em **Avançar**. Escolha um período de tempo apropriado para o intervalo de tempo.

O relatório exibe os gráficos a seguir para os aplicativos selecionados, para o período de tempo selecionado pela frequência de tempo selecionada:

- Gráfico de linha de contagem de transação
- Gráfico de linha do volume de dados de transação
- Gráfico de linha do tempo médio de resposta

- Gráfico de linha de contagem de erros

Mapeamento de atributos do Response Time Monitoring Agent
Alguns dos relatórios do Cloud APM são baseados em dados que são coletados pelo Response Time Monitoring Agent . Os dados nesses relatórios são mapeados para atributos do Agente Response Time Monitoring.

A tabela a seguir fornece mapeamento de itens de dados em relatórios do Agente Response Time Monitoring para atributos de agente:

Tabela 255. Mapeamento de atributo Agente Response Time Monitoring

Item de dados do relatório	Descrição	Nome do atributo ODI	Coluna de arquivo ODI
Nome do aplicativo	O nome do aplicativo monitorado relatado para o Console do Cloud APM	Nome do aplicativo	T5TXCS.APPLICATIN
Contagem de transação	O número total de sequências de solicitação e de resposta que são observadas pelo agente de monitoramento durante o intervalo agregado atual.	Total de solicitações	T5TXINS.TOTREQ
Erros do cliente	O número de solicitações HTTP com um código de status 400 - 499.	Erros do cliente	T5TXCS.NUM4XX
Erros do servidor	O número de solicitações HTTP com um código de status 500 - 599.	Erros do servidor	T5TXCS.NUM5XX
Nome de transação	O nome de transação relatado para o Application Management Console.	Nome de transação	T5TXCS.TRANSACTN
Status de transação	O código de resposta que está associado à transação	Código de status	T5TXCS.STATUSCODE
Kilobytes da resposta do código	O número total de kilobytes em cada resposta da solicitação durante o intervalo de dados.	Bytes de resposta	T5TXCS.REPLYBYT
Kilobytes de solicitação	O número total de kilobytes na solicitação durante o intervalo de dados.	kBytes de solicitação	T5TXCS.REQBYTES

Tabela 255. Mapeamento de atributo Agente Response Time Monitoring (continuação)

Item de dados do relatório	Descrição	Nome do atributo ODI	Coluna de arquivo ODI
Total de Kilobytes	O número total de kilobytes transferidos para todas as solicitações durante o período de tempo.	Total de Bytes	T5TXCS.TOTBYTES
Total de contagem de objetos	O número total de objetos que são integrados em uma página da web para o período de tempo.	Total de contagem de objetos	T5TXCS.OBJCNT
Total do tamanho do objeto	O tamanho total de todos os objetos que estão integrados na página da web para o período de tempo.	Total do tamanho do objeto	T5TXCS.OBJSIZE
Tempo de Resposta (segundos)	O número total de segundos necessário para a conclusão da transação geral do servidor.	Tempo de resposta	T5TXCS.RESPTIME
Tempo do renderizador	O tempo decorrido, em segundos, para renderizar completamente a página da web no navegador da web usando tags JavaScript integradas.	Tempo do renderizador	T5TXCS.RENDERTIME
Tempo do cliente	O tempo médio decorrido, em segundos, que a transação gasta em execução no cliente durante o intervalo de monitoramento atual.	Tempo médio do cliente	T5TXCS.CLIENTTIME
Tempo de carregamento	O tempo médio decorrido, em segundos, desde o momento em que o usuário solicita um download até a conclusão do download de objeto da web.	Tempo médio de carregamento	T5TXCS.LOADTIME
Navegador	Uma descrição do navegador da web no qual a página da web é exibida.	Descrição do navegador	T5TXCS.BROWSEDESC

Tabela 255. Mapeamento de atributo Agente Response Time Monitoring (continuação)			
Item de dados do relatório	**Descrição**	**Nome do atributo ODI**	**Coluna de arquivo ODI**
Servidor	O nome ou o endereço IP do servidor para Transação TCP.	Descrição do servidor	T5TXCS.SERVERDESC
Nome do host de URL	O nome de host TCP/IP da URL.	Nome do host de URL	T5TXCS.URLHOST
Método de URL	O método que é usado para executar solicitações HTTP (GET, POST, HEAD, PUT, OPTIONS, DELETE, TRACE ou CONNECT).	Método	T5TXCS.METHOD
Detalhes de URL	O caminho da URL para o arquivo no servidor que está hospedando a página da Web.	Caminho de URL	T5TXCS.URLPATH

Para obter informações adicionais sobre o Agente Response Time Monitoring, consulte o Transaction Monitoring Reference.

Gerando Relatórios de Synthetic Playback agent

Execute relatórios para os aplicativos que são associados com as transações sintéticas.

Sobre Esta Tarefa

Selecione um aplicativo e uma transação sintética associada no Application Performance Dashboard e gere relatórios com base em sua seleção. Os dados para os relatórios são armazenados no banco de dados DATAMART Db2. Os relatórios exibem dados resumidos por hora, por semana e por mês, que são mantidos por 371 dias, 53 semanas e 12 meses, respectivamente. O Cloud APM não fornece scripts ou instruções para mudar esses períodos de retenção.

Cinco relatórios de multipáginas estão disponíveis:

Transações Gerais

Este relatório de duas páginas exibe os tempos de resposta e as razões de disponibilidade da transação sintética selecionada em um intervalo de data configurado.

A página um exibe os dados a seguir:

- Um gráfico de linha dos tempos de respostas das transações sintéticas selecionadas em intervalos configurados ao longo de um intervalo de data configurado
- Uma tabela da média de tempos de respostas em segundos de cada transação sintética ao longo do intervalo de data configurado

A página dois exibe os dados a seguir:

- Um gráfico de linha das razões de disponibilidade das transações sintéticas selecionadas em intervalos configurados em um intervalo de data configurado
- Uma tabela da média de razão de disponibilidade de cada transação sintética ao longo do intervalo de data configurado

É possível acessar dois relatórios extra do relatório **Transações Gerais**: **Análise Oportuna por Transações** e **Métricas HTTP por Transações**.

Análise Oportuna por Transações exibe métricas HTTP da transação sintética selecionada em intervalos configurados em um intervalo de data configurado. O relatório inclui os itens a seguir:

- Um gráfico de colunas das métricas HTTP da transação sintética selecionadas em intervalos configurados ao longo do intervalo de data configurado
- Uma tabela de métricas HTTP em milissegundos da transação sintética selecionada ao longo do intervalo de data configurado

Métricas HTTP por Transação exibe métricas HTTP da transação sintética selecionada em intervalos configurados em um intervalo de data configurado. O relatório inclui os itens a seguir:

- Um gráfico de colunas das métricas HTTP da transação sintética selecionadas em intervalos configurados ao longo do intervalo de data configurado
- Uma tabela de métricas HTTP em milissegundos da transação sintética selecionada ao longo do intervalo de data configurado

Detalhe da transação por locais

Este relatório de duas páginas exibe os tempos de resposta e as razões de disponibilidade por local das transações sintéticas e subtransações selecionadas em um intervalo de data configurado.

A página um exibe os dados a seguir:

- Gráficos de linha dos tempos de respostas por local das transações e subtransações sintéticas selecionadas em intervalos configurados ao longo de um intervalo de data configurado
- Tabelas da média de tempos de respostas em segundos de todas as subtransações sintéticas ao longo de um intervalo de data configurado em cada local

A página dois exibe os dados a seguir:

- Gráficos de linha de razões de disponibilidade por local das transações sintéticas e subtransações selecionadas em intervalos configurados em um intervalo de data configurado
- Tabelas das razões médias de disponibilidade de todas as subtransações sintéticas em um intervalo de data configurado em cada local

É possível acessar quatro relatórios extra do relatório **Detalhes da Transação por Localizações**: **Análise Oportuna por Localizações de Transação**, **Métricas HTTP por Localizações de Transação**, **Análise Oportuna por Localizações de Subtransação** e **Métricas HTTP por Localizações de Subtransação**.

Análise Oportuna por Localizações de Transação exibe métricas HTTP de uma transação sintética por localizações em intervalos configurados em um intervalo de data configurado. O relatório inclui os itens a seguir:

- Um gráfico de colunas de métricas HTTP da transação sintética selecionada por locais em intervalos configurados ao longo do intervalo de data configurado
- Uma tabela de métricas HTTP em milissegundos da transação sintética selecionada por locais ao longo do intervalo de data configurado

Métricas HTTP por Localizações de Transação exibe métricas HTTP de uma transação sintética por localizações em intervalos configurados ao longo de um intervalo de data configurado. O relatório inclui os itens a seguir:

- Um gráfico de colunas de métricas HTTP da transação sintética selecionada por locais em intervalos configurados ao longo do intervalo de data configurado
- Uma tabela de métricas HTTP em milissegundos da transação sintética selecionada por locais ao longo do intervalo de data configurado

Análise Adequada por Locais da Subtransação exibe métricas HTTP de uma subtransação por locais em intervalos configurados ao longo de um intervalo de data configurado. O relatório inclui os itens a seguir:

- Um gráfico de colunas de métricas HTTP da subtransação selecionada por locais em intervalos configurados ao longo do intervalo de data configurado

- Uma tabela de métricas HTTP em milissegundos da subtransação selecionada por locais ao longo do intervalo de data configurado

Métricas HTTP por Locais de Subtransação exibe métricas HTTP de uma subtransação sintética por locais em intervalos configurados ao longo de um intervalo de data configurado. O relatório inclui os itens a seguir:

- Um gráfico de colunas de métricas HTTP da subtransação selecionada por locais em intervalos configurados ao longo do intervalo de data configurado
- Uma tabela de métricas HTTP em milissegundos da subtransação selecionada por locais ao longo do intervalo de data configurado

Detalhe da transação por subtransações

Este relatório de duas páginas exibe os tempos de resposta e as razões de disponibilidade das subtransações sintéticas em intervalos configurados em um intervalo de data configurado.

A página um exibe os dados a seguir:

- Um gráfico de linha dos tempos de resposta das subtransações sintéticas selecionadas em intervalos configurados em um intervalo de data configurado
- Uma tabela de tempos médios de resposta em segundos de cada subtransação sintética no intervalo de data configurado

A página dois exibe os dados a seguir:

- Um gráfico de linha das razões de disponibilidade das subtransações sintéticas selecionadas em intervalos configurados em um intervalo de data configurado
- Uma tabela de razões de disponibilidade de cada subtransação sintética no intervalo de data configurado

É possível acessar dois relatórios extra do relatório **Detalhes da Transação por Subtransações**: **Análise Oportuna por Subtransações** e **Métricas HTTP por Subtransações**.

Análise Adequada por Locais da Subtransação exibe métricas HTTP de uma subtransação por locais em intervalos configurados ao longo de um intervalo de data configurado. O relatório inclui os itens a seguir:

- Um gráfico de colunas de métricas HTTP da subtransação selecionada em intervalos configurados ao longo do intervalo de data configurado
- Uma tabela de métricas HTTP em milissegundos da subtransação selecionada ao longo do intervalo de data configurado

Métricas HTTP por Locais de Subtransação exibe métricas HTTP de uma subtransação sintética por locais em intervalos configurados ao longo de um intervalo de data configurado. O relatório inclui os itens a seguir:

- Um gráfico de colunas de métricas HTTP da subtransação selecionada em intervalos configurados ao longo do intervalo de data configurado
- Uma tabela de métricas HTTP em milissegundos da subtransação selecionada ao longo do intervalo de data configurado

Tendência de transações

Este relatório de quatro páginas exibe uma análise de tendência de tempos de resposta, razões de disponibilidade e métricas HTTP na semana anterior e nas cinco semanas anteriores.

A página um exibe dados de tendência nos tempos de resposta e nas razões de disponibilidade de uma transação sintética:

- Um gráfico de linha combinado dos tempos médios de resposta de uma transação sintética selecionada na semana anterior e nas cinco semanas anteriores
- Um gráfico de linha combinado da razão de disponibilidade de uma transação sintética selecionada que compara a razão de disponibilidade para a semana anterior com a razão de disponibilidade de referência nas cinco semanas anteriores

- Uma tabela do tempo médio de resposta e da razão de disponibilidade de uma transação sintética na semana anterior e no intervalo de data de cinco semanas anteriores
- Um gráfico de linha combinado dos tempos médios de resposta de uma transação sintética selecionada na semana anterior e nas cinco semanas anteriores por localização
- Um gráfico de linha combinado da razão de disponibilidade de uma transação sintética selecionada que compara a razão de disponibilidade para a semana anterior com a razão de disponibilidade de referência nas cinco semanas anteriores por localização
- Uma tabela dos tempos médios de resposta e razões de disponibilidade de uma transação sintética selecionada na semana anterior e nas cinco semanas anteriores por localização
- Um gráfico de linha combinado dos tempos médios de resposta das subtransações de uma transação sintética selecionada na semana anterior e nas cinco semanas anteriores
- Um gráfico de linha combinado das razões médias de disponibilidade das subtransações de uma transação sintética selecionada que compara a razão de disponibilidade para a semana anterior com a razão de disponibilidade de referência nas cinco semanas anteriores
- Uma tabela dos tempos médios de resposta e razões de disponibilidade das subtransações de uma transação sintética selecionada na semana anterior e nas cinco semanas anteriores

A página dois exibe dados de tendência nas métricas HTTP de uma transação sintética:

- Um gráfico de linha combinado dos tempos médios de bloqueio de uma transação sintética selecionada na semana anterior e nas cinco semanas anteriores
- Um gráfico de linha combinado dos tempos médios de DNS de uma transação sintética selecionada na semana anterior e nas cinco semanas anteriores
- Um gráfico de linha combinado dos tempos médios de SSL de uma transação sintética selecionada na semana anterior e nas cinco semanas anteriores
- Um gráfico de linha combinado dos tempos médios de conexão de uma transação sintética selecionada na semana anterior e nas cinco semanas anteriores
- Um gráfico de linha combinado dos tempos médios de envio de uma transação sintética selecionada na semana anterior e nas cinco semanas anteriores
- Um gráfico de linha combinado dos tempos médios de recebimento de uma transação sintética selecionada na semana anterior e nas cinco semanas anteriores
- Um gráfico de linha combinado dos tempos médios de renderização de uma transação sintética selecionada na semana anterior e nas cinco semanas anteriores
- Uma tabela da média de métricas HTTP de uma transação sintética na semana anterior e nas cinco semanas anteriores

A página três exibe dados de tendência nas métricas HTTP em milissegundos de uma transação sintética por local. Os gráficos e a tabela comparam as médias de métrica HTTP na semana anterior com as médias de métrica de referência nas cinco semanas anteriores:

- Sete gráficos de linha combinados que comparam diferentes médias de métrica HTTP de uma transação sintética selecionada para a semana anterior com a métrica de referência nas cinco semanas anteriores por localização
- Uma tabela da média de métricas HTTP de uma transação sintética selecionada na semana anterior e nas cinco semanas anteriores por localização

A página quatro exibe dados de tendência nas métricas HTTP em milissegundos para subtransações. Os gráficos e a tabela comparam as médias de métrica HTTP na semana anterior com as médias de métrica de referência nas cinco semanas anteriores:

- Sete gráficos de linha combinados que comparam valores médios de diferentes métricas HTTP de uma transação sintética selecionada para a semana anterior com a métrica de referência nas cinco semanas anteriores por subtransação
- Uma tabela de valores médios de métricas HTTP de uma transação sintética selecionada na semana anterior e nas cinco semanas anteriores por subtransação

Tendência de subtransações

Este relatório de duas páginas exibe uma análise de tendência dos tempos de resposta, razões de disponibilidade e métricas HTTP para subtransações na última semana e nas cinco semanas anteriores.

A página um exibe dados de tendência nos tempos de resposta e nas razões de disponibilidade para o domingo anterior, a semana anterior e as cinco semanas anteriores:

- Uma tabela que compara tempos de resposta de subtransação e razões de disponibilidade do domingo anterior, da semana anterior e das cinco semanas anteriores
- Um gráfico de linha combinado que compara os tempos médios de resposta das subtransações para a semana anterior com o tempo de resposta de referência para as cinco semanas anteriores
- Um gráfico de linha combinado que compara a razão média de disponibilidade das subtransações para a semana anterior com a razão de disponibilidade de referência para as cinco semanas anteriores
- Uma tabela de tempos médios de resposta e razões de disponibilidade de subtransações para a semana anterior.
- Uma tabela de tempos médios de resposta e razões de disponibilidade de subtransações para as cinco semanas anteriores.

A página dois exibe dados de tendência nas métricas HTTP em milissegundos para subtransações. Os gráficos e as tabelas exibem as médias de métrica HTTP de subtransações na semana anterior com as médias de métrica de referência nas cinco semanas anteriores:

- Sete tabelas de valores médios de métricas HTTP da transação selecionada para o domingo anterior, a semana anterior e cinco semanas anteriores por subtransações
- Sete gráficos de linha combinados que comparam diferentes médias de métrica HTTP em milissegundos da transação selecionada para a semana anterior com a razão de disponibilidade de referência nas cinco semanas anteriores por subtransações
- Uma tabela de valores médios de métricas HTTP de subtransações para a semana anterior.
- Uma tabela de valores médios de métricas HTTP de subtransações para cinco semanas anteriores.

Procedimento

Para gerar relatórios, conclua as seguintes etapas:

1. Clique no ícone **Desempenho** e selecione **Painel de Desempenho do Aplicativo**. Para escolher um aplicativo, expanda **Todos os meus aplicativos** e selecione um aplicativo. Para exibir todas as transações sintéticas associadas ao aplicativo selecionado, clique em **Grupos** > **Transações** > **Transações sintéticas**.
2. Selecione uma transação sintética da tabela da Lista de transações. Para executar um relatório, clique em **Ações** > **Ativar para relatórios** e selecione um dos relatórios a seguir:
   - **Transações Gerais**
   - **Detalhe da transação por locais**
   - **Detalhe da transação por subtransações**
   - **Tendência de transações**
   - **Tendência de subtransações**

   Uma página Configuração é aberta em uma nova guia em seu navegador da web.
3. Para configurar o intervalo de data para seu relatório, selecione um intervalo de data predefinido ou insira um intervalo de data customizado.
4. Para configurar o intervalo de tempo para seu relatório, selecione um intervalo em **Tipo de tempo**. Configure seu relatório para exibir dados de transações sintéticas e subtransações nos intervalos **Por Hora**, **Por Dia** ou **Por Semana** no intervalo de data configurado. Para gerar seu relatório, clique em **Concluir**.

5. Para visualizar relatórios sobre métricas HTTP para transações, subtransações ou localizações, deve-se selecionar uma transação, subtransação ou localização nos relatórios **Transações Gerais**, **Detalhes da Transação por Localizações** ou **Detalhes da Transação por Subtransações**.
   - Para visualizar **Análise Oportuna por Transações**, clique com o botão direito no nome de uma transação no relatório **Transações Gerais** e selecione **Acessar** > **Análise de Métricas HTTP por Horário**.
   - Para visualizar **Métricas HTTP por Transações**, clique com o botão direito no nome de uma transação no relatório **Transações Gerais** e selecione **Acessar** > **Agregação da Métrica HTTP**.
   - Para visualizar **Análise Oportuna por Localizações de Transação**, clique com o botão direito no nome de uma transação no relatório **Detalhes da Transação por Localizações** e selecione **Acessar** > **Análise de Métricas HTTP por Horário**.
   - Para visualizar **Métricas HTTP por Localizações de Transação**, clique com o botão direito no nome de uma transação no relatório **Detalhes da Transação por Localizações** e selecione **Acessar** > **Agregação de Métricas HTTP**.
   - Para visualizar **Análise oportuna por locais de subtransação**, clique com o botão direito em um nome de subtransação no relatório **Detalhe da transação por locais** e selecione **Ir para** > **Análise de métricas Http por hora**.
   - Para visualizar **Métricas HTTP por locais da subtransação**, clique com o botão direito em um nome de subtransação no relatório **Detalhe da transação por locais** e selecione **Ir para** > **Agregação de métricas Http**.
   - Para visualizar **Análise Oportuna por Subtransações**, clique com o botão direito no nome de uma subtransação no relatório **Tendência de Subtransações** e selecione **Acessar** > **Análise de Métricas HTTP por Horário**.
   - Para visualizar **Métricas HTTP por Subtransações**, clique com o botão direito no nome de uma subtransação no relatório **Tendência de Subtransações** e selecione **Acessar** > **Agregação da Métrica HTTP**.

Relatórios do WebSphere Applications agent

Relatórios predefinidos estão disponíveis para dados que são coletados pelo WebSphere Applications agent.

Os dados para os relatórios são armazenados no banco de dados WAREHOUS Db2. Os relatórios exibem dados por hora, por dia, por semana e por mês, que são mantidos por um mês, três meses, um ano e um ano, respectivamente. O Cloud APM não fornece scripts ou instruções para mudar esses períodos de retenção. Os relatórios a seguir estão disponíveis para dados que são coletados pelo WebSphere Applications agent:

Desempenho de solicitação de aplicativo

Descrição

Este relatório analisa como os aplicativos são executados em um nível agregado em um servidor de aplicativos. O gráfico de setores circulares mostra as solicitações de nível agregado para aplicativos. O gráfico de barras mostra o tempo médio de resposta para os aplicativos em um nível agregado. Os dois gráficos de linha da série de tempo mostra o tempo médio de resposta e tendência de contagem total de solicitações para todos os aplicativos. Para realizar drill down das solicitações individuais de um aplicativo, clique em uma fatia do gráfico ou em uma barra.

Parameters

Intervalo de Data: selecione um dos períodos de relatório predefinidos ou selecione os horários de início e de encerramento exatos do calendário.

Parâmetros solicitados: Tipo de Resumo e Tipo de Servidor de Aplicativos

Tabelas Usadas

Request_Analysis_*V

Conjuntos de conexões do BD

Descrição

Esse relatório analisa conjuntos de conexões com o banco de dados em um servidor de aplicativos. A tabela mostra as estatísticas principais para todos os conjuntos de conexões em um nível agregado. Quando você seleciona uma origem de dados específica, dois gráficos de tendência mostram a tendência das estatísticas principais.

Parameters

Intervalo de Data: selecione um dos períodos de relatório predefinidos ou selecione os horários de início e de encerramento exatos do calendário.

Parâmetros solicitados: Tipo de Resumo, Nome do Servidor de Aplicativos

Tabelas Usadas

DB_Connection_Pools_*V

Desempenho de EJB

Descrição

Esse relatório analisa como os EJBs implementados no servidor de aplicativos são executados. O gráfico de setores circulares mostra a contagem do método de nível agregado para os EJBs. O gráfico de barras mostra o Tempo Médio de Resposta do Método em EJBs em um nível agregado. Os gráficos Duas Séries Temporais mostram as tendências Contagem de Chamada do Método e Tempo Médio de Resposta do Método para todos os EJBs. As linhas de tendência podem ser filtradas por EJB clicando em uma linha na lista.

Parameters

Intervalo de Data: selecione um dos períodos de relatório predefinidos ou selecione os horários de início e de encerramento exatos do calendário.

Parâmetros solicitados: Tipo de Resumo, Nome do Servidor de Aplicativos

Tabelas Usadas

Enterprise_Java_Beans_*V

Uso de GC do servidor de aplicativos

Descrição

Esse relatório analisa a coleta de lixo. Use este relatório para determinar se a coleta de lixo está criando problemas ou se o heap não está dimensionado de forma adequada. O primeiro gráfico mostra o percentual médio de heap que é usado e o percentual médio em tempo real da coleta de lixo no decorrer do tempo. O segundo gráfico mostra a porcentagem de execuções da coleta de lixo em um tempo real médio e a taxa média da coleta de lixo.

Parameters

Intervalo de Data: selecione um dos períodos de relatório predefinidos ou selecione os horários de início e de encerramento exatos do calendário.

Parâmetros solicitados: Tipo de Resumo, Tipo de Servidor de Aplicativos

Tabelas Usadas

Garbage_Collection_Analysis_*V

Uso de JVM para o servidor de aplicativos

Descrição

Este relatório analisa como a JVM de um servidor de aplicativos executa. O gráfico de barras empilhadas mostra como a Memória da JVM é utilizada e liberada. O gráfico de linha dupla mostra o uso da Memória da JVM em relação ao consumo da CPU da JVM.

Parameters

Intervalo de Data: selecione um dos períodos de relatório predefinidos ou selecione os horários de início e de encerramento exatos do calendário.

Parâmetros solicitados: Tipo de Resumo, Tipo de Servidor de Aplicativos

Tabelas Usadas
Application_Server_*V

Conjuntos de encadeamentos

Descrição
Esse relatório analisa os conjuntos de encadeamentos em um servidor de aplicativos. A tabela mostra as estatísticas principais para todos os conjuntos de encadeamentos em um nível agregado. Depois de selecionar um conjunto de encadeamentos na lista, o gráfico de tendência mostra a tendência das estatísticas principais para o Conjunto de Encadeamentos selecionado. Se nenhum conjunto de encadeamentos estiver selecionado, as tendências demonstrarão um resumo de todos os conjuntos de encadeamentos.

Parameters
Intervalo de Data: selecione um dos períodos de relatório predefinidos ou selecione os horários de início e de encerramento exatos do calendário

Parâmetros solicitados: Tipo de Resumo, Tipo de Servidor de Aplicativos

Tabelas Usadas
Thread_Pools_*V

Desempenho do aplicativo da web

Descrição
Este relatório analisa como os aplicativos são executados no contêiner da web de um servidor de aplicativos (Dados PMI). Os gráficos de pizza mostram as solicitações de nível agregado dos aplicativos. O gráfico de barras mostra o tempo médio de resposta para os aplicativos em um nível agregado. Os gráficos de linha de duas séries temporais mostram as tendências Tempo Médio de Resposta e Contagem Total de Solicitação de todos os aplicativos. Clique em uma gráfico de pizza ou barra ou em uma linha para realizar drill down nos servlets/jsps individuais desse aplicativo.

Parameters
Intervalo de Data: selecione um dos períodos de relatório predefinidos ou selecione os horários de início e de encerramento exatos do calendário.

Parâmetros solicitados: Tipo de Resumo, Tipo de Servidor de Aplicativos

Tabelas Usadas
Thread_Pools_*V

Desempenho de solicitação de aplicativo para clusters

Descrição
Este relatório analisa como os servidores em um cluster estão executando. O primeiro gráfico mostra o número de solicitações que são concluídas por cada um dos membros do cluster durante o intervalo de tempo selecionado. O segundo gráfico fornece informações sobre a tendência do tempo de resposta médio para cada um dos membros do cluster. Há uma linha separada neste gráfico para cada servidor no cluster. Clique em uma linha para realizar drill down dos dados do servidor individual. O relatório Desempenho de Solicitação de Aplicativo deste servidor é aberto

Parameters
Intervalo de Data: selecione um dos períodos de relatório predefinidos ou selecione os horários de início e de encerramento exatos do calendário.

Parâmetros solicitados: Tipo de Resumo, Nome do Cluster

Tabelas Usadas
Request_Analysis_*V

Uso de JVM e GC para clusters

Descrição
Este relatório analisa as tendências de uso da JVM e da coleta de lixo por cada um dos membros do cluster. O primeiro gráfico mostra a porcentagem média em tempo real das execuções da coleta de

lixo. O segundo gráfico mostra a porcentagem média de heap usada. Os últimos gráficos mostram o uso de memória da CPU e da JVM. Todos esses gráficos mostram dados para cada membro de cluster como uma linha separada.

Parameters

Intervalo de Data: selecione um dos períodos de relatório predefinidos ou selecione os horários de início e de encerramento exatos do calendário.

Parâmetros solicitados: Tipo de Resumo, Nome do Cluster

Tabelas Usadas

Garbage_Collection_Analysis_*V, Application_server_*V

Principais aplicativos com tempos de resposta mais lentos entre os servidores

Descrição

Este relatório analisa como os aplicativos são executados em um nível agregado em todos os servidores de aplicativos. Um gráfico de barras mostra o tempo médio de resposta para aplicativos em um nível agregado.

Parameters

Intervalo de Data: selecione um dos períodos de relatório predefinidos ou selecione os horários de início e de encerramento exatos do calendário.

Parâmetros solicitados: Tipo de Resumo, Número de Aplicativos

Capítulo 11. Fazendo o upgrade

Atualize seu agentes e coletores de dados para obter os recursos mais recentes e a funcionalidade que estão disponíveis na liberação atual.

Fazendo upgrade de agentes

Periodicamente, novos archives que contêm agentes de monitoramento atualizados estão disponíveis para download. Archives estão disponíveis a partir do Produtos e serviços no website do IBM Marketplace.

Antes de Iniciar

Para os agentes a seguir, uma tarefa específica do agente deve ser concluída antes de concluir o procedimento de upgrade:

- Para os agentes em AIX, se você estiver executando como um usuário não raiz, deverá limpar uma das bibliotecas da memória antes de iniciar o procedimento de instalação para fazer upgrade do agente. Siga as instruções em “Agentes em AIX: Parando o agente e executando slibclean antes de fazer upgrade” na página 1142.
- Para o Agente HMC Base em AIX, se você estiver fazendo upgrade do agente como um usuário não raiz, primeiro deve parar o Agente HMC Base e limpar bibliotecas dependentes do cache. Siga as instruções em “Agente HMC Base no AIX: parando o agente como um usuário não raiz e executando slibclean antes do upgrade” na página 1143
- Para o Microsoft .NET agent, é necessário remover o coletor de dados dos aplicativos .NET antes de fazer upgrade do agente. Siga as instruções em “Microsoft .NET agent: Removendo o coletor de dados .NET antes do upgrade” na página 1145.
- Para o Agente Node.js, é necessário remover os plug-ins de coletor de dados dos aplicativos Node.js antes de fazer upgrade do agente. Siga as instruções em “Agente Node.js: Removendo os plug-ins de coletor de dados antes do upgrade” na página 1143.
- Para o Agente Ruby, você deve remover o coletor de dados de seus aplicativos Ruby antes de fazer upgrade do agente. Siga as instruções em “Agente Ruby: Removendo os plug-ins de coletor de dados antes do upgrade” na página 1146.
- Para o Agente do Servidor HTTP, deve-se parar o HTTP Server antes do upgrade do agente.
- Para o WebSphere MQ agent, se você ativou o rastreamento de transação para o agente na liberação anterior, deve-se parar a instância de agente antes de fazer upgrade do agente.
- Para o SAP NetWeaver Java Stack, se estiver fazendo upgrade da V8.1.3.2 para a V8.1.4, pare todas as instâncias do SAP NetWeaver Java Stack que estão configuradas com o coletor de dados antes de fazer upgrade do agente.
- Para o Agente Skype for Business Server, se estiver fazendo upgrade da versão mais antiga para a V8.1.4.0.2, no lado do agente, o nome do agente muda para Skype for Business Server. Além disso, após o upgrade de suporte por meio de SDA, é preciso reiniciar o serviço APMUI para refletir o novo nome do agente (Skype for Business Server) no lado do MIN Server; caso contrário, você verá o antigo nome do agente (MS Lync Server) no painel do MIN Server.
- Para o Agente Tomcat, se você deseja fazer upgrade da estrutura principal do TEMA no Windows, deve-se parar o agente e o servidor. Siga as instruções em Agente Tomcat: fazendo upgrade do TEMA Core Framework no Windows

Sobre Esta Tarefa

Se uma nova versão do agente estiver disponível, a execução do script de instalação atualizará automaticamente o agente. Se o agente não tiver uma versão mais recente disponível, uma mensagem será exibida explicando que o agente já está instalado; o seu agente instalado não será afetado.

Para instalar um agente atualizado, use os seguintes procedimentos:

Procedimento

- "Instalando agentes em sistemas UNIX" na página 118
- "Instalando agentes nos sistemas Linux" na página 124
- "Instalando agentes nos sistemas Windows" na página 132

Resultados

O agente é atualizado para a versão mais recente. Caso não haja uma versão mais recente do agente de monitoramento disponível, será exibida uma mensagem, explicando que o agente já está instalado; seu agente instalado não será afetado.

O que Fazer Depois

Após um upgrade de um agente do Windows, é necessário reiniciar qualquer agente que não seja automaticamente configurado e iniciado pelo Windows Installer. Execute o seguinte comando para verificar o status do agente:

```
./name-agent.bat status
```

Use um dos métodos a seguir para iniciar o agente:

- Clique em **Iniciar** > **Todos os Programas** > **IBM Monitoring Agents** > **IBM Performance Management**. Clique com o botão direito em um agente e clique em **Iniciar**.
- Execute o seguinte comando:

  ```
  ./name-agent.bat start
  ```

Para obter informações sobre os comandos do agente de monitoramento, incluindo o nome a ser utilizado, como verificar o status do agente e mais, consulte "Utilizando comandos do agente" na página 175. Para obter informações sobre quais agentes são iniciados automaticamente e manualmente, consulte Capítulo 5, "Implementação do agente e do coletor de dados", na página 109

- Para o Agente do Hadoop, conclua as seguintes etapas depois de fazer upgrade do agente baseado em soquete (8.1.2, Fix Pack 2 ou anterior) para o agente baseado na API REST (8.1.3 ou mais recente):

  1. Para evitar a geração de logs desnecessários, remova o código de 17 linhas dos arquivos `hadoop-metrics2.properties` de todos os nós Hadoop.
  2. Pare os serviços Hadoop.
  3. Exclua o arquivo `Plugin.jar` que foi copiado do instalador do agente de todos os nós no cluster Hadoop.
  4. Inicie os serviços Hadoop.

  Para obter informações sobre o código de 17 linhas e o arquivo `Plugin.jar`, consulte Configurando nós Hadoop.
- Para o Agente HMC Base, depois de fazer upgrade do agente da versão 6.2.2.6 para 6.2.2.7, você deverá configurar o agente novamente e reiniciá-lo. Para obter instruções, veja "Configurando o monitoramento do HMC Base" na página 261.
- Para o Agente do Servidor HTTP, se você fizer upgrade do agente de uma versão anterior à 1.0.0.4 a 1.0.0.4 ou posterior, também deve-se atualizar o arquivo `.conf`, que é usado pelo HTTP Server, para substituir o arquivo de configuração do coletor de dados anterior pelo arquivo recém-gerado. Também

deve-se incluir a nova instância de agente no console. Para obter instruções, veja "Configurando o monitoramento do Servidor HTTP" na página 266.

- Para o Microsoft .NET agent, depois de fazer upgrade do agente, configure o coletor de dados. Para obter instruções, veja "Registrando o coletor de dados" na página 522.

  Se você instalou o agente em um novo diretório, deverá mudar o caminho do compartimento de serviço do Gerenciador de Perfis usando o comando do controlador de serviço (`sc`). Por exemplo,

  ```
  sc \\localhost config DotNetProfilerService binPath=
  "${install_dir}\qe\bin\DotNetProfilerService.exe
  ```

  em que *install_dir* é o novo diretório de instalação.
- Para o Agente Node.js, depois de fazer upgrade do agente, configure os coletores de dados do agente. Para obter instruções, veja "Configurando o Agente Node.js" na página 587.
- Para o OpenStack agent, para configurar melhor o agente para usar a API de identidade do OpenStack v3, reconfigure todas as instâncias do agente e atualize o arquivo de configuração do coletor de dados do agente. Para obter instruções, veja "OpenStack agent: Reconfigurando instâncias de agente para usar a API de identidade do OpenStack v3" na página 1146.
- Para o Agente Ruby, depois de fazer upgrade do agente, configure o coletor de dados. Para obter instruções, veja "Configurando o coletor de dados diagnósticos" na página 721.
- Para o WebSphere Applications agent, depois de fazer upgrade do agente, migre o coletor de dados, executando o comando *dc_home*`/bin/migrate.sh/bat` do diretório de instalação da nova versão do agente e reinicie a instância do servidor de aplicativos. Para obter instruções, veja "WebSphere Applications agent: migrando o coletor de dados" na página 1147.
- Linux Se você deseja fazer upgrade de uma versão mais velha do agente que está instalada no diretório `/opt/ibm/ccm/agent` deve concluir estas etapas no sistema Linux:

  1. Ao confirmar que você deseja migrar a configuração do agente do diretório de instalação antigo `/opt/ibm/ccm/agent` para o novo diretório de instalação, por exemplo, `/opt/ibm/apm/agent`, é necessário iniciar o agente no novo local de instalação.

     Restrição: A versão mais antiga do agente é parada automaticamente no local de instalação antigo, mas ele não é iniciado automaticamente no novo local de instalação.
  2. Após verificar se o agente funciona no novo diretório de instalação, deve-se desinstalar a versão mais antiga do agente do diretório `/opt/ibm/ccm/agent`. Caso deseje remover todos os agentes, execute o comando **`/opt/ibm/ccm/agent/bin/smai-agent.sh uninstall_all`**.
- Linux Se você estiver fazendo upgrade dos agentes a partir do FP6 ou anterior, após concluir o upgrade dos agentes para um novo diretório e a configuração ou reconfiguração dos agentes, você talvez queira remover o diretório de instalação antigo. Conclua estas etapas:

  1. Na VM ou no sistema em que o agente de monitoramento (ou agentes) está instalado, inicie uma linha de comandos e vá para a pasta de binários no diretório de instalação antigo, `/opt/ibm/ccm/agent/bin`.
  2. Para desinstalar todos os agentes de monitoramento que foram instalados a partir do diretório de instalação antigo, insira:`./smai-agent.sh uninstall_all`
  3. Exclua o diretório de instalação antigo.

Preservando mudanças na configuração do agente

Usuários avançados podem aplicar valores de substituição na customização do componente. A aplicação de valores de substituição assegura que os valores sejam retidos durante um upgrade. Teste as mudanças em seu ambiente primeiro antes de aplicá-las globalmente.

Sobre Esta Tarefa

- Estas instruções são para os agentes Linux e AIX. Para obter uma lista dos códigos do produto do agente e os comandos para parar e iniciar os agentes, consulte "Utilizando comandos do agente" na página 175.

- O processo do agente do Windows preserva as mudanças de configuração por design: variáveis atualizadas no arquivo k*pc*cma.ini, em que *pc* é o código do produto, são mantidas na seção Substituir configurações locais. Essas variáveis são usadas durante cada configuração para atualizar as entradas de registro do Windows que os agentes usam no tempo de execução.
- As configurações customizadas no arquivo .*pc*.environment e no arquivo .global.environment são perdidas após o upgrade do agente. Para preservar suas configurações, faça as mudanças na customização nos arquivos *pc*.environment e global.environment. As configurações nesses arquivos não são sobrescritas pelo upgrade do agente.

Procedimento

Execute as etapas a seguir para salvar as mudanças na configuração que foram feitas no arquivo de ambiente e preservá-las após o upgrade do agente:

1. Crie ou atualize qualquer um dos arquivos a seguir conforme necessário, em que *install_dir* é o diretório de instalação do agente (como o padrão do Linux /opt/ibm/apm/agent/ ou o padrão do AIX /opt/ibm/ccm/agent/):

Nome de Arquivo	Descrição
***install_dir*/config/*pc*.environment**	O *pc* no nome do arquivo é o código do produto do agente, como mq ou rz.
***install_dir*/config/global.environment**	Atualize o arquivo de ambiente global para as mudanças que você deseja afetar todos os tipos de agentes.

   Por exemplo, as.environment é o arquivo de ambiente persistente do WebSphere Applications agent. O .as.environment é sobrescrito quando é feito upgrade do agente para uma nova versão.

   Defina as variáveis no formato *key=value*, em que *key* é o nome da variável de ambiente e *value* é o valor ou configuração (como **KDC_FAMILIES=${KDC_FAMILIES}HTTP:10001**).
2. Após concluir a atualização das configurações de variável, salve e feche o arquivo de ambiente e reinicie os agentes afetados.

Resultados

As atualizações são aplicadas a todos os agentes do mesmo tipo ou, se você tiver atualizado o arquivo de ambiente global, a todos os agentes que relatam ao Servidor Cloud APM. As mudanças são persistidas com upgrades de versão do agente.

Agentes em AIX: Parando o agente e executando slibclean antes de fazer upgrade

Se estiver fazendo upgrade de um agente como um usuário não root em sistemas AIX, você deve concluir esta tarefa. Antes de executar o instalador de agente, você deve parar o agente e executar **slibclean** para limpar a biblioteca libkududp.a.

Procedimento

1. Pare o agente executando um dos comandos a seguir, dependendo de o agente suportar as múltiplas instâncias:
   - ```
     ./name-agent.sh stop
     ```
   - ```
     ./name-agent.sh stop
     instance_name
     ```

   Consulte “Utilizando comandos do agente” na página 175.
2. Execute o comando a seguir com privilégios de usuário raiz.

   ```
   slibclean
   ```

   Consulte Comando slibclean no IBM Knowledge Center.

Resultados
O agente é interrompido e a biblioteca `libkududp.a` é limpa.

O que Fazer Depois
Execute o instalador do agente para fazer upgrade do agente para a liberação que você transferiu por download. Consulte Capítulo 6, “Instalando os agentes”, na página 117. Se o upgrade falhar, reinicialize o servidor e repita o procedimento.

Agente HMC Base no AIX: parando o agente como um usuário não raiz e executando `slibclean` antes do upgrade

Antes de fazer upgrade do Agente HMC Base como um usuário não raiz no AIX, você deve parar o Agente HMC Base e executar **`slibclean`** para limpar bibliotecas dependentes do cache.

Sobre Esta Tarefa

Procedimento

1. Execute o comando a seguir como o usuário não raiz para parar o agente.

   ```
   hmc_base-agent.sh stop
   ```

2. Execute o comando a seguir com privilégios de usuário raiz.

   ```
   slibclean
   ```

   Consulte Comando slibclean no IBM Knowledge Center.

Resultados
O Agente HMC Base é parado e as bibliotecas dependentes são limpas.

O que Fazer Depois
Execute o instalador de agentes para fazer upgrade do Agente HMC Base.

Agente Node.js: Removendo os plug-ins de coletor de dados antes do upgrade

Antes de fazer upgrade do Agente Node.js, você deve remover os plug-ins de monitoramento do aplicativo Node.js.

Sobre Esta Tarefa
Com base na versão do Agente Node.js, é preciso concluir um procedimento diferente para remover os plug-ins de monitoramento de seu aplicativo Node.js. Para saber a versão do agente, consulte Comando de versão do agente.

Procedimento

1. Remova os plug-ins do coletor de dados do começo do arquivo de aplicativos Node.js.
   - Se você fizer upgrade do Agente Node.js da V01.00.12.00 para a V01.00.13.00, conclua o seguinte procedimento:
     – Caso você tenha ativado a coleta de dados, remova a linha a seguir do começo do arquivo de aplicativos Node.js:

       ```
       require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_index.js');
       ```

       em que *KNJ_NPM_LIB_LOCATION* é o diretório para a pasta `lib` de seu diretório de instalação global do pacote do npm. O diretório padrão é `/usr/local/lib`.
     – Se você ativou a coleta de dados de recurso e a coleta de dados diagnósticos de detalhamento, remova a linha a seguir do início do arquivo de aplicativo Node.js:

```
require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_deepdive.js');
```

– Se você ativou a coleta de dados de recurso, a coleta de dados diagnósticos de detalhamento e a coleta de rastreios de método, remova a linha a seguir do início do arquivo de aplicativo Node.js:

```
require('KNJ_NPM_LIB_LOCATION/node_modules/ibm-apm/knj_methodtrace.js');
```

- Se você fizer upgrade do Agente Node.js da V01.00.10.00 para a V01.00.13.00, conclua o seguinte procedimento:
  – Caso você tenha ativado a coleta de dados de recurso, remova a linha a seguir do começo do arquivo de aplicativos Node.js.

```
require('install_dir/lx8266/nj/bin/plugin/knj_index.js');
```

, em que *install_dir* é o diretório de instalação do Agente Node.js.

  – Se você ativou a coleta de dados de recurso e a coleta de dados diagnósticos de detalhamento, remova a linha a seguir do início do arquivo de aplicativo Node.js.

```
require('install_dir/lx8266/nj/bin/plugin/knj_deepdive.js');
```

  – Se você ativou a coleta de dados de recurso, a coleta de dados diagnósticos de detalhamento e a coleta de rastreios de método, remova a linha a seguir do início do arquivo de aplicativo Node.js.

```
require('install_dir/lx8266/nj/bin/plugin/knj_methodtrace.js');
```

2. Reinicie o aplicativo Node.js para desativar os plug-ins do coletor de dados.
   - Se a versão do Agente Node.js atual for V01.00.10.00, até o momento os plug-ins do coletor de dados foram removidos com sucesso.
   - Se a versão do Agente Node.js atual for V01.00.12.00, continue com a próxima etapa.
3. Execute o comando `./uninstall.sh` a partir do diretório *install_dir*`/lx8266/nj/bin` para remover suas configurações de agente anteriores.

O que Fazer Depois
Faça upgrade do Agente Node.js. Consulte “Fazendo upgrade de agentes” na página 1139.

Agente do Response Time Monitoring: fazendo upgrade do Módulo de Tempo de Resposta do IBM HTTP Server

Se você estava monitorando anteriormente o IBM HTTP Server usando o Módulo de Tempo de Resposta do IBM HTTP Server ou o Agente do HTTP Server, faça upgrade de sua instalação.

Sobre Esta Tarefa

A tabela a seguir mostra alguns cenários de instalação que podem ser semelhantes à forma como você está monitorando o IBM HTTP Server.

Agente Response Time Monitoring	Usando o Módulo de Tempo de Resposta do IBM HTTP Server?	Usando o Packet Analyzer?	Agente do HTTP Server instalado?
AIX e xLinux: 08.11.00 e mais recente Windows: 08.14.02 e mais recente	✓	–	✓
AIX e xLinux: 08.10.00	✓	–	–
AIX e xLinux: 08.10.00	✓	–	✓
7.40.07 ou anterior	–	✓	–

Agente Response Time Monitoring	Usando o Módulo de Tempo de Resposta do IBM HTTP Server?	Usando o Packet Analyzer?	Agente do HTTP Server instalado?
7.40.07 ou anterior	—	✓	✓

Para todos esses cenários, o processo de instalação é semelhante.

Procedimento

1. Instale o Agente do HTTP Server da liberação V8.1.1 ou mais recente no AIX ou Linux; da liberação V8.1.4.02 ou mais recente no Windows.

   O Módulo de Tempo de Resposta do IBM HTTP Server é instalado automaticamente com o agente.
2. Configure o Agente do HTTP Server.

   Nota: Se você estava usando anteriormente o Módulo de Tempo de Resposta do IBM HTTP Server, atualize o arquivo de configuração do servidor da web (`httpd.conf`) com o local do novo Módulo de Tempo de Resposta do IBM HTTP Server e remova o arquivo de configuração do módulo de carregamento antigo (`mod_wrt.so`).

   Nota: O Response Time Monitoring agent V8.1.1 e posterior não funciona com o arquivo do módulo de carregamento (`mod_wrt.so`) de liberações anteriores. Se você tentar usar uma versão antiga desse arquivo, mensagens de log de erro serão criadas. Transações ainda serão controladas, mas os dados de instância de transação não serão exibidos.

   Para obter mais informações, consulte o PDF de referência do Agente do HTTP Server, que pode ser transferido por download no http://ibm.biz/agent-httpserver.
3. Certifique-se de que o IBM HTTP Server e o Agente do HTTP Server estejam em execução. Se o instalador do Response Time Monitoring detectar o Agente do HTTP Server, o agente do Response Time Monitoring ativa o Módulo de Tempo de Resposta do IBM HTTP Server ao invés do Packet Analyzer.
4. Instale o agente do Response Time Monitoring para o mesmo local `AGENT_HOME` que o Agente do HTTP Server.
   - Linux AIX Instale a V8.1.1 ou mais recente como **`root`**. `AGENT_HOME` exemplo `/opt/ibm/apm/agent/`
   - Windows Instale a V8.1.4.0.2 ou mais recente com permissões de administrador. `AGENT_HOME` exemplo `C:\IBM\APM\`.
5. Se você usou Packet Analyzer em liberações anteriores, talvez seja necessário desativar o Packet Analyzer para iniciar o monitoramento do IBM HTTP Server com Módulo de Tempo de Resposta do IBM HTTP Server.
6. Reinicie o IBM HTTP Server.

Microsoft .NET agent: Removendo o coletor de dados .NET antes do upgrade

Antes de fazer upgrade do Microsoft .NET agent, deve-se remover o coletor de dados .NET de seus aplicativos .NET.

Procedimento

1. Cancele o registro de todos os módulos do coletor de dados.

   Como um administrador, digite:

   ```
   cd install_dir\qe\bin configdc unregisterdc all
   ```

   Em que *install_dir* é o diretório de instalação do Microsoft .NET agent.
2. Reinicie os aplicativos .NET.

O que Fazer Depois

Faça upgrade do Microsoft .NET agent. Consulte "Fazendo upgrade de agentes" na página 1139.

OpenStack agent: Reconfigurando instâncias de agente para usar a API de identidade do OpenStack v3

Para fazer upgrade do OpenStack agent para usar a API de identidade do OpenStack v3, depois de instalar a versão mais recente do agente, você deve reconfigurar todas as instâncias do agente e atualizar o arquivo de configuração do coletor de dados.

Sobre Esta Tarefa

Esta tarefa é obrigatória apenas ao fazer upgrade do agente para usar a API de identidade do OpenStack v3.

Procedimento

1. Reconfigure todas as instâncias do agente existentes. Para obter instruções detalhadas, consulte "Configurando o OpenStack agent" na página 610.
2. Localize o arquivo de configuração do coletor de dados do agente `ksg_dc_`*`instance_name`*`.cfg`, em que *instance_name* é o nome especificado para a instância do agente.

   Se o arquivo não existir, copie *`install_dir`*`/lx8266/sg/bin/ksg_dc.cfg` para o diretório *`install_dir`*`/config` e mude o nome do arquivo para `ksg_dc_`*`instance_name`*`.cfg`.

   Por exemplo, se o nome da instância for 0S1, mude o nome para `ksg_dc_0S1.cfg`.
3. Inclua a seguinte seção no arquivo `ksg_dc_`*`instance_name`*`.cfg`:

   ```
   #OpenStack authentication information
   [OS_authentication_info]
   OS_project_domain_name=Default
   OS_user_domain_name=Default
   OS_cert_path=
   ```
4. Reinicie a instância do agente executando os seguintes comandos:

   ```
   install_dir/bin/openstack-agent.sh stop instance_name
   install_dir/bin/openstack-agent.sh start instance_name
   ```

   em que *instance_name* é o nome da instância de agente a ser configurada.

Agente Ruby: Removendo os plug-ins de coletor de dados antes do upgrade

Antes de fazer upgrade do Agente Ruby, você deve remover os plug-ins de monitoramento do aplicativo Ruby.

Procedimento

1. Remova o coletor de dados da versão antiga, executando o seguinte comando.

   ```
   gem uninstall stacktracer
   ```
2. Navegue para o diretório inicial do aplicativo, abra o `Gemfile` e remova a seguinte linha: `gem 'stacktracer', '`*`version`*`'`
   Em que *version* é o número da versão do Agente Ruby.
3. No diretório inicial de seu aplicativo, insira: `bundle install`

O que Fazer Depois

Faça upgrade do Agente Ruby. Consulte "Fazendo upgrade de agentes" na página 1139.

WebSphere Applications agent: migrando o coletor de dados

Após fazer upgrade do agente, é necessário migrar o coletor de dados, de forma interativa ou em modo silencioso.

Migrando o coletor de dados interativamente

É possível migrar um nível de manutenção mais antigo do coletor de dados interativamente usando o utilitário de migração.

Antes de Iniciar

Linux AIX Caso você tenha instalado o WebSphere Application Server ou o WebSphere Portal Server usando uma conta de usuário não raiz, antes de executar os utilitários de configuração, verifique se o usuário não raiz possui privilégios de leitura e gravação para os seguintes diretórios do agente em *install_dir*/yndchome/7.3.0.14.08 em que *install_dir* é o diretório de instalação do WebSphere Applications agent:

- data
- bin
- runtime
- logs

Fornece permissões de leitura e gravação usando o comando chmod 777, se necessário. Além disso, efetue login como o usuário utilizado para instalar o servidor de aplicativos.

Sobre Esta Tarefa

É possível migrar um nível de manutenção mais antigo do coletor de dados interativamente usando o utilitário de migração. Se deseja migrar muitas instâncias do servidor de aplicativos, poderá ser mais conveniente usar o utilitário de migração no modo silencioso.

Importante:

- É possível migrar somente os níveis de manutenção anteriores da versão 7.3 de um coletor de dados. A versão do coletor de dados é indicada no caminho do diretório inicial do coletor de dados.
- Não é possível migrar do coletor de dados versão 7.3 para o 7.3 fix pack 1. Em vez disso, desconfigure o coletor de dados e desinstale a versão de agente 7.3. Então, instale a versão 7.3 fix pack 1 do agente e configure o coletor de dados novamente.

Procedimento

1. Linux AIX Efetue login como o usuário que foi usado para instalar o servidor de aplicativos.
2. Inicie o utilitário de migração a partir do diretório de instalação da versão mais recente do agente.

   Linux AIX Execute o comando *dc_home*/bin/migrate.sh

   Windows Execute o comando *dc_home*\bin\migrate.bat
3. O utilitário exibe os endereços IP de todas as placas de rede que estão localizadas no sistema de computador local.

   Insira o número que corresponde ao endereço IP a usar.
4. O utilitário descobre todos os servidores configurados pelos níveis de manutenção mais antigos do coletor de dados e lista-os. Os coletores de dados são agrupados pelo nível de manutenção.

   Selecione uma ou mais instâncias do servidor de aplicativos a partir da lista.

   A lista pode incluir tanto as instâncias tradicionais de servidor do WebSphere como dos servidores do Liberty. Instâncias tradicionais do servidor do WebSphere podem estar em diferentes perfis.

   Dica:

- Se várias instâncias sob um perfil são monitoradas, você deve selecionar todas elas para migrar ao mesmo tempo.
- Migre todos os servidores no perfil Liberdade ao mesmo tempo. Migrar parcialmente os servidores configurados pode causar instabilidade.

Lembre-se:

- Para um ambiente independente, as instâncias do servidor de aplicativos devem estar em execução.
- Para um ambiente do Network Deployment, o agente do nó e o gerenciador de implementação devem estar em execução.
- Os servidores Liberdade não são requeridos para execução durante a migração.

5. Insira o número que corresponde à instância do servidor de aplicativos cujo coletor de dados deve ser migrado ou insira um asterisco (*) para migrar o coletor de dados de todas as instâncias do servidor de aplicativos.

   Para especificar um subconjunto de servidores, insira os números, separados por vírgulas, que representam os servidores. Por exemplo: `1,2,3`.

   O utilitário de migração integra automaticamente cada coletor de dados com o agente de monitoramento. Os valores do host e da porta do agente de monitoramento são recuperados a partir dos arquivos de configuração existentes.
6. Insira um alias para cada um dos servidores selecionados.

   O valor padrão é o alias de servidor existente.
7. Para a instância do servidor Liberty, insira o diretório inicial da JVM quando solicitado. Por exemplo, `/opt/IBM/java`.
8. O utilitário determina se a segurança global do WebSphere é ativada para cada perfil em que o coletor de dados está sendo migrado.

   Se a Segurança Global do WebSphere for ativada para um ou mais perfis, especifique se deseja recuperar as configurações de segurança de um arquivo de propriedades do cliente:

   O coletor de dados se comunica com o WebSphere Administrative Services usando o RMI ou o protocolo SOAP. Se a segurança global estiver ativada para um perfil, é necessário especificar o ID do usuário e a senha de um usuário que está autorizado a efetuar login no console administrativo do IBM WebSphere Application Server para o perfil.

   Como alternativa, é possível criptografar o nome de usuário e a senha e armazená-los nos arquivos de propriedades do cliente do servidor de aplicativo antes de configurar o coletor de dados. Você deve usar o arquivo `sas.client.props` para uma conexão RMI ou o arquivo `soap.client.props` para uma conexão SOA.
9. Insira 1 para permitir que o utilitário recupere o nome de usuário e a senha do arquivo de propriedades do cliente adequado e vá para a etapa “11” na página 1148. Caso contrário, insira 2 para inserir o nome de usuário e a senha.

   Importante: Pode demorar algum tempo para efetuar login no console administrativo do WebSphere Application Server.
10. Insira o nome de usuário e senha para cada perfil se a Segurança Global do WebSphere estiver ativada.
11. O utilitário migra o coletor de dados para cada instância de servidor de aplicativo selecionada. Ele exibe uma mensagem de status que indica se a migração de cada servidor foi concluída com sucesso.
12. Reinicie as instâncias conforme indicado pelo utilitário. A configuração do coletor de dados entra em vigor quando as instâncias do servidor de aplicativos são reiniciadas.

Resultados

O coletor de dados é migrado para o nível de manutenção mais recente instalado.

O que Fazer Depois
O utilitário de migração preserva as configurações que foram definidas na versão mais antiga do coletor de dados. Para modificar essas configurações, é possível executar os utilitários de configuração ou de reconfiguração, no modo interativo ou silencioso, a partir do diretório *dc_home*\bin do novo coletor de dados. Para obter mais informações, consulte "Configurando ou reconfigurando o coletor de dados com utilitários de configuração completos" na página 839.

Migrando o coletor de dados no modo silencioso
É possível migrar um nível de manutenção mais antigo do coletor de dados usando o utilitário de migração no modo silencioso.

Antes de Iniciar

Linux AIX Caso você tenha instalado o WebSphere Application Server ou o WebSphere Portal Server usando uma conta de usuário não raiz, antes de executar os utilitários de configuração, verifique se o usuário não raiz possui privilégios de leitura e gravação para os seguintes diretórios do agente em *install_dir*/yndchome/7.3.0.14.08 em que *install_dir* é o diretório de instalação do WebSphere Applications agent:

- data
- bin
- runtime
- logs

Fornece permissões de leitura e gravação usando o comando chmod 777, se necessário. Além disso, efetue login como o usuário utilizado para instalar o servidor de aplicativos.

Sobre Esta Tarefa
Um arquivo de propriedades silenciosas de amostra, sample_silent_migrate.txt, é empacotado com o utilitário de migração. O arquivo está disponível no diretório *install_dir*/yndchome/7.3.0.14.08/bin.

Ao criar seu arquivo de propriedades silenciosas, tenha em mente estas considerações:

- Uma linha no arquivo que inicia com um sinal de número (#) é tratada como comentário, e não é processada. Se o sinal de número é usado em qualquer lugar na linha, ele não é considerado com o início de um comentário. Isso significa que você pode usar o sinal de número em senhas ou para outros usos.
- Cada propriedade é descrita em uma linha separada, no formato a seguir: propriedade = valor.

  propriedade
  Este é o nome da propriedade. A lista de propriedades válidas que é possível configurar é mostrada na Tabela 256 na página 1150. Não modifique ou remova propriedades no arquivo de amostra não listadas na tabela.

  valor
  Este é o valor da propriedade. Os valores padrão para algumas propriedades já foram fornecidos. É possível excluir valores padrão para deixar valores de propriedade em branco ou vazios. Um valor vazio será tratado como se a propriedade não tivesse sido especificada, em vez de usar o valor padrão. Se você desejar usar valores padrão, é possível comentar a linha da propriedade no arquivo.
- As senhas estão em texto simples.
- As propriedades e seus valores fazem distinção entre maiúsculas e minúsculas.

O Tabela 256 na página 1150 descreve as propriedades que estão disponíveis ao migrar o coletor de dados no modo silencioso.

Tabela 256. Propriedades disponíveis para execução do utilitário de migração no modo silencioso	
Propriedade	**Comentário**
migrate.type	Deve ser AD.
default.hostip	Se o sistema de computador usa diversos endereços IP, especifique o endereço IP para o coletor de dados a usar.
itcam.migrate.home	Especifica o diretório inicial do coletor de dados da versão de manutenção mais antiga do coletor de dados. O diretório não é excluído como parte da migração.
was.wsadmin.connection.host	Especifica o nome do host ao qual a ferramenta wsadmin está se conectando. Em um ambiente de Implementação de Rede, especifique a conexão wsadmin com o Gerenciador de Implementação. Em um ambiente independente, especifique a conexão wsadmin com o servidor.
was.wsadmin.username	Especifica o ID de um usuário que está autorizado a efetuar logon no console administrativo do IBM WebSphere Application Server. Esse usuário deve ter a função de agente no servidor de aplicativos.
was.wsadmin.password	Especifica a senha que corresponde ao usuário especificado na propriedade `was.wsadmin.username`.
was.appserver.profile.name	Especifica o nome do perfil do servidor de aplicativos que deseja configurar. **Lembre-se:** A propriedade não é requerida para um perfil Liberdade.
was.appserver.home	Especifica o diretório inicial do WebSphere Application Server.
was.appserver.cell.name	Especifica o nome da célula do WebSphere Application Server. **Lembre-se:** A propriedade não é requerida para um perfil Liberdade.
was.appserver.node.name	Especifica o nome do nó do WebSphere Application Server. **Lembre-se:** A propriedade não é requerida para um perfil Liberdade.
was.appserver.server.name	Especifica a instância do servidor de aplicativos dentro do perfil do servidor de aplicativos para migrar para a nova versão do coletor de dados. O arquivo de propriedades silenciosas pode ter diversas instâncias desta propriedade.

Importante:

- É possível migrar somente os níveis de manutenção anteriores da versão 7.3 de um coletor de dados. A versão do coletor de dados é indicada no caminho do diretório inicial do coletor de dados.

- Não é possível migrar do coletor de dados versão 7.3 para o 7.3 fix pack 1. Em vez disso, desconfigure o coletor de dados e desinstale a versão de agente 7.3. Então, instale a versão 7.3 fix pack 1 do agente e configure o coletor de dados novamente.

Procedimento

1. Especifique as opções de configuração no arquivo de propriedades de migração silenciosa.
2. Execute o comando para iniciar o utilitário de migração no modo silencioso a partir do diretório de instalação da versão mais recente do agente.
   - Linux AIX `dc_home/bin/migrate.sh -silent sample_silent_migration_filename`
   - Windows `dc_home\bin\migrate.bat -silent sample_silent_migration_filename`

Resultados
O coletor de dados é migrado para o nível de manutenção mais recente instalado.

O que Fazer Depois
O utilitário de migração preserva as configurações que foram definidas na versão mais antiga do coletor de dados. Para modificar essas configurações, é possível executar os utilitários de configuração ou de reconfiguração, no modo interativo ou silencioso, a partir do diretório *dc_home*\bin do novo coletor de dados. Para obter mais informações, consulte "Configurando ou reconfigurando o coletor de dados com utilitários de configuração completos" na página 839.

Agente Tomcat: Fazendo upgrade do TEMA Core Framework no Windows

Para fazer upgrade da estrutura principal do TEMA no Windows para o Agente Tomcat, deve-se parar o agente e o servidor para fazer upgrade da estrutura do TEMA com sucesso.

Procedimento

1. Prepare a configuração do servidor Tomcat.
2. Instale e configure o agente Tomcat.
3. Efetue login no painel do IBM Cloud Application Performance Management, acesse **Configuração do agente** > **Tomcat**, selecione uma instância do Agente Tomcat e clique em **Ativar TT/DD**.
4. Reinicie o Servidor Tomcat.
5. Para aplicar o IBM APM CORE FRAMEWORK, pare o Agente Tomcat e o Servidor.
6. Goto TEMA/<IBM APM CORE FRAMEWORK_HOME>. Execute o comando **apmpatch.bat <Tomcat Agent Installationdir>** .
   A estrutura é submetida a upgrade.
7. Verifique a versão do IBM APM CORE FRAMEWORK atualizada executando as instruções a seguir.
   ```
   Goto <TOMCAT_Agent_Install_Dir> \InstallITM
   Execute: KinCInfo.exe -i .
   ```
8. Inicie o servidor Tomcat e o agente.

Atualizando o coletores de dados

Periodicamente, novos archives que contêm coletores de dados atualizados estão disponíveis para download. Os archives estão disponíveis no Produtos e serviços no website do IBM Marketplace..

Antes de Iniciar

Sobre Esta Tarefa
Para fazer upgrade de um coletor de dados, conclua as seguintes etapas:

Procedimento

- Desconfigure o coletor de dados de seus aplicativos locais e/ou IBM Cloud:
  - Para o Coletor de dados J2SE, as etapas de desconfiguração não são necessárias.
  - Para o Coletor de dados Liberty, siga as instruções em "Desconfigurando o coletor de dados para aplicativos IBM Cloud" na página 890 e/ou "Desconfigurando o coletor de dados para aplicativos no local" na página 883.
  - Para o Coletor de dados Node.js, siga as instruções em "Desconfigurando o Coletor de dados Node.js para aplicativos IBM Cloud" na página 598 e/ou "Desconfigurando o Coletor de dados Node.js para aplicativos no local" na página 604.
  - Para o Coletor de dados do Python, siga as instruções em "Desconfigurando o Coletor de dados do Python para aplicativos IBM Cloud" na página 676 e/ou "Desconfigurando o Coletor de dados do Python para aplicativos no local" na página 681.
  - Para oColetor de dados Ruby, siga as instruções em "Desconfigurando o Coletor de dados Ruby para aplicativos IBM Cloud" na página 729.
- Faça download do pacote coletor de dados.
- Reconfigure o coletor de dados para monitorar seus aplicativos locais e/ou IBM Cloud:
  - Para o Coletor de dados Node.js, após o upgrade do coletor de dados, reconfigure o coletor de dados. Para obter instruções, consulte "Configurando o Coletor de dados Node.js independente para aplicativos IBM Cloud(antigo Bluemix)" na página 593 e/ou "Configurando o Coletor de dados Node.js para aplicativos no local" na página 598.
  - Para o Coletor de dados do Python, após o upgrade do coletor de dados, reconfigure o coletor de dados. Para obter instruções, consulte "Configurando o coletor de dados Python para aplicativos IBM Cloud" na página 671 e/ou "Configurando o Coletor de dados do Python para aplicativos no local" na página 677.
  - Para o Coletor de dados Liberty, após o upgrade do coletor de dados, reconfigure o coletor de dados. Para obter instruções, consulte "Configurando o coletor de dados Liberty para aplicativos IBM Cloud" na página 884 e/ou "Configurando o coletor de dados Liberty para aplicativos no local" na página 880.
  - Para o Coletor de dados J2SE, após o upgrade do coletor de dados, reconfigure o coletor de dados. Para obter instruções, veja "Configurando o monitoramento do J2SE" na página 450.
  - Para o Coletor de dados Ruby, após o upgrade do coletor de dados, reconfigure o coletor de dados. Para obter instruções, veja "Configurando o Coletor de dados Ruby para aplicativos IBM Cloud" na página 726.

Resultados

O coletor de dados é atualizado para a versão mais recente.

Capítulo 12. Resolução de problemas e suporte

Revise as entradas para resolução de problemas que podem ocorrer ao instalar, configurar ou usar o IBM Cloud Application Performance Management.

O conteúdo da resolução de problemas está disponível neste Knowledge Center. Anteriormente, o conteúdo da resolução de problemas estava disponível no Fórum do Cloud Application Performance Management no developerWorks. É possível continuar pesquisando entradas neste fórum. Procure entradas que começam com "Resolução de problemas".

Para a resolução de problemas do IBM Cloud Application Performance Management Hybrid Gateway, consulte “Gerenciando o Gateway Híbrido” na página 962.

Resolução de Problemas de Agentes

Resolução de problemas da instalação do agente e problemas de configuração.

Estamos migrando nosso conteúdo para solução de problemas do Fórum do Cloud Application Performance Management no developerWorks para este Knowledge Center. Anteriormente, o conteúdo da resolução de problemas estava disponível no Fórum do Cloud Application Performance Management no developerWorks. É possível continuar pesquisando entradas neste fórum. Procure entradas que começam com "Resolução de problemas".

Monitoramento de Serviço da

É possível encontrar aqui mais detalhes sobre problemas conhecidos do Internet Service Monitoring.

O perfil não será criado após criar página de perfil ser mantido aberto por mais de 10 minutos e outro perfil com o mesmo nome não será criado

Problema

O perfil não será criado após **criar página de perfil** ser mantido aberto por mais de 10 minutos e outro perfil com o mesmo nome não será criado.

Sintoma

Ao criar um perfil, se o usuário mantiver **criar página de perfil** inativo (aberto sem nenhuma atividade) por mais de 10 minutos e, em seguida, tentar criar o perfil, esse perfil não será criado. Depois disso, se o usuário tentar criar o perfil novamente com o mesmo nome, o perfil não será criado.

Causa

Um arquivo de bloqueio é criado no lado de MIN no momento da criação do perfil que bloqueia a atividade de criação de perfil para o mesmo perfil para outros usuários. O arquivo de bloqueio é excluído após a criação do perfil ser feita. Mas se a janela de criação estiver inativa por mais de 10 minutos, o evento de criação ficará bloqueado e o usuário não será capaz de criar o perfil.

Solução

- O usuário não deve manter a janela inativa por mais de 10 minutos enquanto cria um perfil.
- O administrador pode excluir o arquivo de bloqueio do perfil que foi criado do lado MIN em `/opt/ibm/wlp/usr/servers/min/dropins/CentralConfigurationServer.war/data_source/is`.
  Por exemplo, se o nome do perfil for ABC, um arquivo de bloqueio `$$ABC$$1UjQ9wy1boIHTAQeoWSj1IU.lock` será criado.

Monitoramento do Microsoft Active Directory

É possível encontrar aqui mais detalhes sobre problemas conhecidos de monitoramento do Microsoft Active Directory.

O agente do Microsoft Active Directory não mostra o conteúdo de ajuda on-line atualizado

Problema

As páginas de ajuda on-line não são atualizadas com o conteúdo mais recente para o agente do Microsoft Active Directory.

Sintoma

Na ajuda do painel do APM Eclipse para o Microsoft Active Directory agent, o conteúdo da ajuda está ausente para o intervalo de coleta de dados e o período de retenção dos seguintes grupos de atributos incluídos recentemente:

- Serviços de Diretório
- Kerberos Consistency Checker
- Key Distribution Center do Kerberos
- Name Service Provider
- Serviço de Diretório de Troca

Causa

O problema ocorre devido à restrição no servidor de construção.

Solução

O usuário pode encontrar o conteúdo de ajuda na ajuda contextual dos respectivos grupos de atributos no painel do APM.

Nota: O problema aparece na liberação V8.1.4.10 do APM.

Monitoramento do Microsoft IIS

É possível encontrar aqui mais detalhes sobre problemas conhecidos dos Microsoft Internet Information Services.

As páginas de ajuda on-line não são atualizadas com o conteúdo mais recente para o agente do Microsoft IIS APM

Problema

As páginas de ajuda on-line não são atualizadas com o conteúdo mais recente para o agente do Microsoft IIS APM

Sintoma

Os grupos de atributos recém incluídos estão ausentes no conteúdo de ajuda on-line:

- WPROCESS
- MEMIISUS
- Coleta de lixo ASP
- IISSVRINFO

Causa

Esse problema está ocorrendo devido a problemas do servidor de construção.

Solução Alternativa

Não Disponível. No entanto, é possível ver o conteúdo de ajuda de um grupo de atributos específico no painel do APM.

Monitoramento do Microsoft .NET

É possível encontrar aqui mais detalhes sobre problemas conhecidos de monitoramento do Microsoft .NET.

O agente Microsoft .NET não mostra o conteúdo de ajuda on-line atualizado

Problema

As páginas de ajuda on-line não são atualizadas com o conteúdo mais recente para o Microsoft .NET agent.

Sintoma

Na ajuda do painel do APM Eclipse para o Microsoft .NET agent, o conteúdo de ajuda do atributo Request Name está ausente sob o grupo de atributos Database Call Details.

Causa

O problema ocorre devido à restrição no servidor de construção.

Solução

O usuário pode encontrar o conteúdo da ajuda na ajuda contextual do widget do grupo de atributos Database Call Details no painel do APM.

Nota: O problema aparece na liberação V8.1.4.10 do APM.

Monitoramento do Microsoft SharePoint Server

É possível encontrar aqui mais detalhes sobre problemas conhecidos de monitoramento do Microsoft SharePoint Server.

O agente do Microsoft SharePoint Server não mostra o conteúdo de ajuda on-line atualizado

Problema

As páginas de ajuda on-line não são atualizadas com o conteúdo mais recente para o Microsoft SharePoint Server agent.

Sintoma

Na ajuda do painel do APM Eclipse para o Microsoft SharePoint Server agent, o conteúdo de ajuda está ausente para os widgets de grupo recém-adicionados chamados `Last 1 Hour Trace Log Count` e `Trace Log Details`.

Causa

O problema ocorre devido à restrição no servidor de construção.

Solução

O usuário pode encontrar o conteúdo de ajuda na ajuda contextual dos respectivos widgets de grupo no painel do APM.

Nota: O problema aparece na liberação V8.1.4.10 do APM.

Monitoramento do PostgreSQL

É possível encontrar aqui mais detalhes sobre problemas conhecidos do monitoramento do PostgreSQL.

O widget Buffer Hit Percentual para bancos de dados sem conexões ativas não mostra o conteúdo de ajuda

Problema

As informações não estão disponíveis para bancos de dados que não possuem conexões ativas.

Sintoma

Os bancos de dados sem conexões ativas não são exibidos no widget Porcentagem de acertos do buffer. As informações devem ser mostradas no conteúdo de ajuda do widget.

Causa

Limitação devido à compatibilidade com o IBM Cloud App Management.

Solução

Não Disponível. O usuário deve tomar nota da limitação.

Os valores de endereço de memória e de IP não são exibidos na plataforma SUSE15

Problema

Os valores de endereço de memória e de IP não são exibidos quando o agente está monitorando o PostgreSQL Server localmente na plataforma SUSE15.

Sintoma

Os valores de endereço de memória e de IP não são exibidos se o agente está monitorando o PostgreSQL Server na plataforma SUSE15.

Causa

O comando **`netstat`** falha para o agente na plataforma SUSE15.

Solução

O usuário pode usar a plataforma SUSE12 para monitorar o PostgreSQL Server localmente.

Coletando logs de agente de monitoramento para o Suporte IBM

Utilize a ferramenta de coleção de determinação de problema, *pdcollect*, para reunir os logs e outras informações sobre determinação de problemas necessários que são solicitados pelo Suporte da IBM para agentes de monitoramento. A ferramenta coletora de PD é instalada com cada agente de monitoramento.

Antes de Iniciar
Permissão raiz ou de administrador é necessária para a ferramenta coletora PD para coletar informações do sistema a partir dos agentes de monitoramento. É possível revisar os logs do agente individualmente nas seguintes pastas:

- Windows [64-bit] *install_dir*\TMAITM6_x64\logs
- Windows [32-bit] *install_dir*\TMAITM6\logs
- Linux AIX *install_dir*/logs

Restrição: É possível executar somente uma instância do script `pdcollect`.

Sobre Esta Tarefa

O local padrão de *install_dir* é:

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

Para executar a ferramenta coletora PD, conclua as etapas a seguir:

Procedimento

1. Na linha de comandos, mude para o diretório do agente:
   - Linux AIX *install_dir*`/bin`
   - Windows *install_dir*`\BIN`
2. Execute o seguinte comando:
   - Linux AIX **`./pdcollect`**
   - Windows **`pdcollect`**

   Um arquivo com um registro de data e hora no nome do arquivo é gerado no diretório `/tmp`, como `/tmp/pdcollect-nc049021.tar.Z`.
3. Envie os arquivos de saída para seu representante de Suporte IBM.

O que Fazer Depois

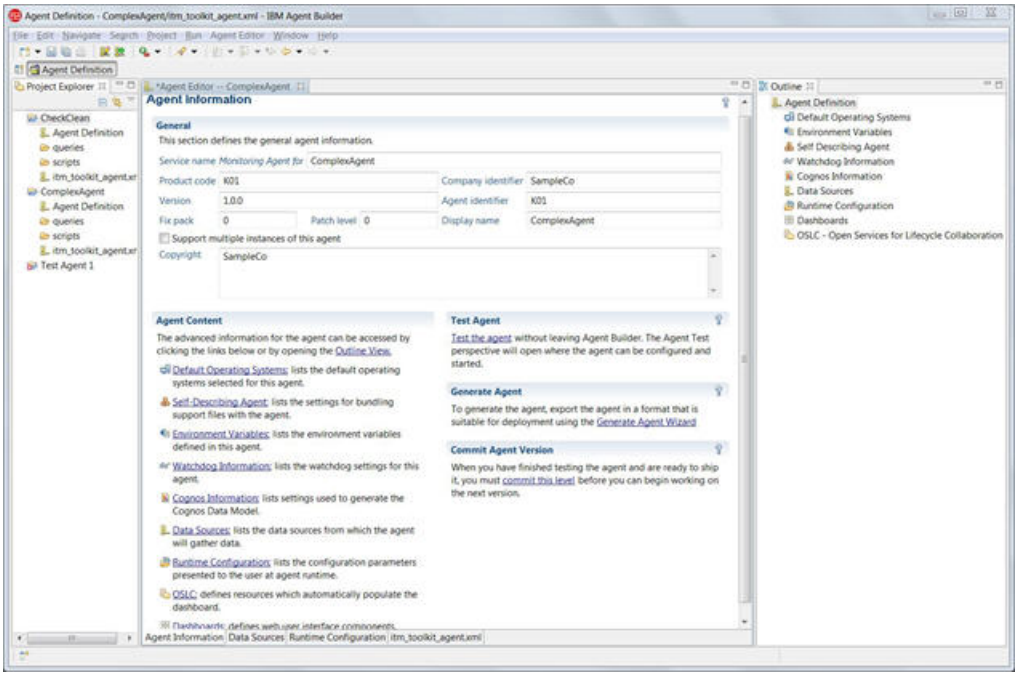
Se você instalou o Agente Ruby e o configurou para os painéis Diagnósticos, execute a ferramenta coletora kkm, *kkmCollector*, em sistemas Linux para reunir arquivos de configuração, arquivos de saída, como arquivos JSO e arquivos de log.

1. Altere para o diretório *install_dir*`/lx8266/km/bin`.
2. Execute o comando **`./kkmCollector`**

   Um arquivo com um registro de data e hora no nome do arquivo será gerado no diretório `tmp`, como `/tmp/kkm_dchome.tar.gz`
3. Envie os arquivos de saída para seu representante de Suporte IBM.

Capítulo 13. Agent Builder

A ferramenta IBM Agent Builder fornece uma interface gráfica com o usuário para ajudá-lo a criar, modificar, depurar e empacotar agentes para as origens de dados de monitoramento no IBM Cloud Application Performance Management.



Visão Geral do Agent Builder

É possível usar o IBM Agent Builder para criar e modificar agentes customizados que ampliam as capacidades de monitoramento de um ambiente IBM Tivoli Monitoring ou IBM Cloud Application Performance Management. Um agente customizado usa um desses ambientes para monitorar qualquer tipo de software interno ou customizado.

O Agent Builder é baseado no Eclipse, um ambiente de desenvolvimento integrado de software livre.

O Agent Builder inclui os recursos a seguir para os ambientes Tivoli Monitoring e Cloud APM:

Definir e modificar agentes
É possível criar e modificar agentes. Os agentes coletam e analisam dados sobre o estado e o desempenho de recursos diferentes, como discos, memória, processador ou aplicativos, e fornecem esses dados para o ambiente de monitoramento.

Testar e preparar agentes para implementação
É possível testar um agente no Agent Builder, coletar dados no host onde o Agent Builder é executado (em alguns casos, também é possível coletar informações de um host diferente). É possível empacotar o agente para fácil distribuição e implementação.

Os recursos adicionais a seguir estão disponíveis para Tivoli Monitoring:

Espaços de trabalho, situações e comandos Executar ação customizados
É possível usar o Agent Builder para empacotar áreas de trabalho, situações e comandos Executar Ação adicionais como extensões de suporte ao aplicativo com um agente novo ou existente em execução no ambiente do Tivoli Monitoring

Relatar modelos de dados
É possível usar o Agent Builder para gerar um modelo de dados Cognos que pode ser usado para construir relatórios do Tivoli Common Reporting. Esses relatórios podem ser empacotados como parte da sua imagem de agente.

Procedimentos do Common Agent Builder

A tabela a seguir lista os procedimentos principais que podem ser concluídos com o Agent Builder.

É possível usar o Agent Builder para criar agentes para os ambientes IBM Tivoli Monitoring e IBM Cloud Application Performance Management. Também é possível usá-lo para criar extensões de suporte do aplicativo para o ambiente Tivoli Monitoring. Extensões de suporte de aplicativo são criados pela criação de áreas de trabalho e situações para aprimorar um ou mais agentes existentes.

Antes de usar o Agent Builder, deve-se instalá-lo. Para obter instruções, veja "Instalando e iniciando o Agent Builder" na página 1164.

Para criar, testar e usar um agente, conclua os procedimentos na tabela a seguir na ordem em que estiverem listados.

Tabela 257. Informações de referência rápida para criação de agentes

Objetivo	Consulte
Crie um agente usando o assistente **Agent**.	• "Criar um agente" na página 1169
Crie origens de dados e atributos para seu agente. **Importante:** Para um ambiente do Cloud APM, um painel de resumo pode exibir aproximadamente até cinco atributos; um dos atributos deve denotar o agente geral ou o status do subnó.	• "Editando as propriedades da origem de dados e do atributo" na página 1191
Para o ambiente Tivoli Monitoring, crie áreas de trabalho e situações para seu agente. • Executando, no mínimo, Tivoli Monitoring Versão 6.1 Fix Pack 1 • Configurando a versão de solução do Tivoli Universal Agent de volta para "00" • Configurando o valor para "AppTag"	• "Criando Espaços de Trabalho, Comandos Executar Ação e Situações" na página 1371 • "Importando Arquivos de Suporte do Aplicativo" na página 1406
Para o ambiente Cloud APM, crie definições de recursos e painéis para seu agente.	• "Preparando o agente para Cloud APM" na página 1377
Para o ambiente Tivoli Monitoring, crie modelos de dados do Cognos para relatórios para seu agente.	• "Geração de Modelo de Dados Cognos" na página 1477
Teste e depure seu agente criado, assegurando a disponibilidade das informações de monitoramento.	• "Testando seu agente no Agent Builder" na página 1380 • "Opções de Linha de Comandos" na página 1416 • "Usando o Agent Editor para modificar o agente" na página 1172.
Gere um pacote de instalação e instale o agente no host monitorado.	• "Instalando um agente" na página 1389
Remova um agente que você criou com o Agent Builder.	• "Desinstalando um Agente" na página 1404

Também é possível usar o Agent Builder para empacotar os espaços de trabalho, as situações e os comandos Executar ação customizados como extensões de suporte do aplicativo para agentes existentes. Essas funções estão disponíveis somente para o ambiente Tivoli Monitoring:

Tabela 258. Informações de Referência Rápida para Outras Funções

Objetivo	**Consulte**
Crie espaços de trabalho customizados, situações e comandos Executar ação.	• "Criando Espaços de Trabalho, Comandos Executar Ação e Situações" na página 1371
Compacte a extensão de suporte do seu aplicativo.	• "Criando Extensões de Suporte de Aplicativo para Agentes Existentes" na página 1474
Construa pacotes configuráveis customizados.	• "Criando Pacotes Configuráveis de Arquivo Não Agente" na página 1498

Origens de dados e conjuntos de dados

Um agente pode monitorar informações a partir de uma ou de várias origens de dados. Ele apresenta as informações para a infraestrutura de monitoramento como atributos, que são organizados em conjuntos de dados.

Ao você criar um agente, deve definir uma *origem de dados* para ele. É possível incluir mais origens de dados. A origem de dados define como o agente reúne as informações de monitoramento.

É possível usar o Agent Builder para criar agentes que usam informações de monitoramento de origens de dados dos *provedores de dados* a seguir:

- Disponibilidade de processo e serviço
- Disponibilidade do sistema de rede (usando ping de ICMP)
- Códigos de retorno de comando
- Saída de script
- O Log de Eventos do Windows
- Windows Management Instrumentation (WMI)
- Windows Performance Monitor (Perfmon)
- Protocolo Simples de Gerenciamento de Rede (SNMP)
- Eventos do SNMP
- Disponibilidade e tempo de resposta do Hypertext Transfer Protocol (HTTP)
- SOAP ou outra origem de dados HTTP
- Java Database Connectivity (JDBC)
- Java Application Programming Interface (API)
- Java Management Extensions (JMX)
- CIM (Common Information Model)
- Arquivos de registro
- Logs binários do AIX
- Soquete

Você também pode utilizar outras ferramentas de desenvolvimento para criar aplicativos de monitoramento customizados que passam informações para o agente por meio do log, a saída do script e Java API de dados Origens .

Quando você inclui uma origem de dados, o Agent Builder inclui o *conjunto de dados* correspondente no agente. O conjunto de dados organiza as informações que são apresentadas ao ambiente de

monitoramento. No IBM Tivoli Monitoring, um conjunto de dados é conhecido como um *grupo de atributos*.

Um conjunto de dados pode ser composto de vários *atributos*, que são valores que a origem de dados fornece. Cada vez que o ambiente de monitoramento consulta o agente, ele busca valores a partir das origens de dados e os retorna como atributos em conjuntos de dados.

Algumas origens de dados podem retornar várias *linhas* de valores de atributos na mesma consulta, por exemplo, se a origem de dados monitora vários serviços de uma vez.

A maioria das origens de dados apresentam informações como um conjunto de dados. Origens de dados SNMP e JMX podem, dependendo da configuração, forneça diferentes conjuntos de informações. Quando você inclui um SNMP ou origem de dados JMX, o Agent Builder cria vários conjuntos de dados para acomodar essas informações.

Você pode editar os conjuntos de dados para filtrar os dados e criar adicional *derivado* atributos, ou seja, atributos que são calculados a partir de atributos existentes usando uma fórmula. Também é possível associar conjuntos de dados, criando um novo conjunto de dados com informações a partir de dois ou mais conjuntos de dados. Dessa forma, os usuários podem visualizar informações combinadas de diferentes origens de dados.

No IBM Tivoli Monitoring, é possível visualizar todo o conteúdo do atributo. Também é possível criar áreas de trabalho que apresentam informações a partir de todos os conjuntos de dados do agente em uma visualização customizada. É possível usar o IBM Tivoli Monitoring para criar situações que são acionadas quando qualquer atributo atinge um determinado valor. Uma situação pode emitir um alerta e chamar um comando do sistema.

No IBM Cloud Application Performance Management, deve-se definir um painel de *resumo* para o agente, selecionando até cinco atributos que ficam visíveis no painel. Você também pode definir um *detail* painel que exibe informações de quaisquer conjuntos de dados como tabelas. É possível criar limites que são acionados quando qualquer atributo atinge um determinado valor; não será necessário incluir esse atributo no painel. Um limite pode emitir alertas.

Monitorando vários servidores ou instâncias de um servidor

Um agente pode monitorar vários servidores, incluindo várias instâncias do mesmo servidor. Há duas maneiras de criar esses agentes: várias instâncias de um agente e subnós dentro de um agente.

Várias instâncias são uma forma padrão de monitorar servidores de aplicativos que podem ter uma série de instâncias semelhantes no mesmo host. Muitos agentes padrão no IBM Tivoli Monitoring e no IBM Cloud Application Performance Management suportam várias instâncias.

Com *várias instâncias*, você instala um agente em hosts monitorados e, em seguida, configura uma ou várias instâncias, configurando um nome para cada instância. Configure uma instância do agente para cada instância do servidor que você deseja monitorar. Cada instância é uma cópia idêntica separada do agente e ela pode ser iniciada e interrompida separadamente.

Também é possível definir um ou vários tipos de *subnó* dentro de um agente. Cada tipo deve corresponder a um tipo diferente de recurso que um agente pode monitorar. Um tipo de subnó contém origens de dados e conjuntos de dados; também é possível definir origens de dados e conjuntos de dados no nível de agente, fora de qualquer subnó. Quando você instala o agente em um host, é possível configurar o número necessário de subnós de cada tipo; para cada tipo de subnó, é possível configurar o número de subnós independentemente. Para o IBM Cloud Application Performance Management, é possível criar um painel para o agente e um painel separado para cada subnó.

Os subnós requerem etapas de configuração diferentes no host monitorado. Além disso, para reconfigurar, incluir ou remover um subnó deve-se parar e reiniciar o agente inteiro; uma instância pode ser reconfigurada, incluída ou removida sem afetar outras instâncias. No entanto, subnós têm uma série de vantagens:

- Com subnós, é possível monitorar uma grande quantia de instâncias de servidor enquanto se consome menos recursos. Como uma diretriz, o número de instâncias de agente de um tipo específico suportado em um único sistema é 10. Mas um agente pode monitorar até 100 servidores locais ou remotos usando subnós.

- Um agente pode incluir tipos de subnó para alguns tipos diferentes de servidores. No sistema monitorado, é possível configurar qualquer número de subnós de cada tipo. É possível usar esse recurso para preservar recursos ainda mais.
- Um agente com subnós pode fornecer dados de todo o sistema no nível de agente.

É possível definir várias instâncias e subnós para o mesmo agente. Nesse caso, cada instância pode incluir uma série de subnós. É possível parar e reiniciar cada instância independentemente de outras instâncias; todos os subnós em uma instância são interrompidos e reiniciados juntos.

Testando, instalando e configurando um agente

É possível criar um pacote de instalação para um agente e, em seguida, instalá-lo em qualquer número de hosts monitorados. Para algumas origens de dados, é necessário configurar valores de configuração para coletar dados.

Após definir origens de dados e atributos para um agente, é possível testá-lo executando-o dentro do Agent Builder. É possível testar um único conjunto de dados (grupo de atributos) ou o agente integral.

Para testar o agente mais extensivamente e para usá-lo, é possível criar uma imagem de instalação. Essa imagem fornece scripts para instalar e configurar o agente em qualquer host monitorado.

Dica: Antes de instalar o agente, assegure-se de que o agente de sistema operacional para o seu ambiente de monitoramento (IBM Tivoli Monitoring ou IBM Cloud Application Performance Management) esteja instalado no host.

Após instalar o agente, pode ser necessário configurá-lo. Se o agente suportar várias instâncias, deve-se configurar o agente para criar pelo menos uma instância.

Algumas origens de dados requerem valores de configuração adicionais; por exemplo, para a origem de dados SNMP, deve-se configurar o endereço IP do host que você monitora usando o protocolo SNMP. Use o script de configuração, que é implementado pelo pacote de instalação, para configurar esses valores.

Alternativamente, é possível configurar esses valores no Agent Builder antes de criar a imagem de instalação. Nesse caso, não é preciso configurá-los novamente nos hosts monitorados.

Dica: Os arquivos de ajuda para seu agente customizado podem não ser exibidos em Conteúdos da Ajuda após a atualização do servidor Cloud APM. Para exibir arquivos de ajuda, conclua as seguintes etapas:

1. Faça download da versão mais recente do IBM Agent Builder de sua assinatura do Cloud APM no IBM Marketplace.
2. Recrie o agente customizado. Certifique-se de designar um número da versão, fix pack ou nível de correção mais alto na página Informações do agente.
3. Instale seu agente customizado no host monitorado.
4. No Console do Cloud APM , clique em **Ajuda** > **Conteúdos de ajuda** na barra de navegação. A ajuda de seu agente customizado é exibida.

Requisitos do Sistema Operacional

Agentes que são criados pelo Agent Builder são suportados em sistemas operacionais diferentes, dependendo do ambiente de monitoramento e nas configurações que você seleciona ao criar o agente.

Em um ambiente do Tivoli Monitoring, os agentes que são criados pelo Agent Builder podem suportar os seguintes sistemas operacionais:

- AIX
- HP-UX
- Linux
- Solaris
- Windows

Os agentes suportam as mesmas versões do sistema operacional que os agentes de S.O. Para obter detalhes, acesse o Relatórios de compatibilidade do produto de software website. Procure o nome do

produto `Tivoli Monitoring` e selecione a caixa de seleção do componente `Agentes de S.O. & TEMA (Tivoli Enterprise Monitoring Agent)`.

Em um ambiente do IBM Cloud Application Performance Management, os agentes criados pelo Agent Builder podem suportar os seguintes sistemas operacionais:

- AIX
- Linux
- Windows

Os agentes suportam as mesmas versões que os agentes de S.O. Para obter detalhes, use os links na seção Relatórios do componente de Requisitos do sistema (APM Developer Center).

Para executar seu agente de monitoramento em um ambiente do Tivoli Monitoring , instale o agente do sistema operacional apropriado em cada Sistema monitorado onde seu agente Corre .

Para executar seu agente de monitoramento em um ambiente do IBM Cloud Application Performance Management , instale qualquer um dos agentes fornecidos com IBM Cloud Application Performance Management em cada sistema monitorado onde seu agente Corre .

Nota: Os navegadores do Agent Builder operam nas origens de dados e informações acessíveis a partir do sistema em que o Agent Builder está em execução. Certifique-se de executar o Agent Builder em um dos seguintes tipos de sistemas:

- Um sistema que é executado no mesmo nível que o sistema operacional e aplicativos monitorados para os quais você está desenvolvendo o agente
- Um sistema que se conecta a outro sistema que é executado no mesmo nível que o sistema operacional e aplicativos monitorados para os quais você está desenvolvendo o agente

Recursos específicos para o IBM Tivoli Monitoring

O Agent Builder fornece vários recursos que se aplicam somente ao IBM Tivoli Monitoring.

É possível usar grupos navegadores para organizar os dados que o agente exibe nas visualizações do navegador e nas áreas de trabalho do IBM Tivoli Monitoring. Um grupo de navegadores combina os dados de vários grupos de atributos (conjuntos de dados) em uma única visualização, enquanto oculta a conjuntos de dados separados originais do usuário.

É possível usar o Tivoli Enterprise Portal para criar áreas de trabalho, situações e comandos Executar Ação para o seu agente. É possível, então, usar o Agent Builder para salvar as áreas de trabalho, situações e comandos Executar Ação como arquivos de suporte de aplicativo e empacotá-los com o agente. Além disso, o Agent Builder também pode importar áreas de trabalho, situações e comandos Executar Ação para outros agentes e criar arquivos de suporte de aplicativo customizados para eles.

Agent Builder pode gerar um modelo de dados do Cognos para o agente. Use o modelo de dados para importar informações do agente no Cognos Framework Manager, uma parte de IBM Tivoli Common Reporting, para criação de relatório.

Instalando e iniciando o Agent Builder

Antes de você instalar o IBM Agent Builder, certifique-se de que o seu sistema atende aos pré-requisitos. Em seguida, use o assistente de instalação ou o procedimento de instalação silenciosa para instalar o Agent Builder.

Dica: Para obter informações sobre a instalação ou modificação de um *agente*, consulte “Instalando um agente” na página 1389.

Pré-requisitos para instalar e executar o Agent Builder

Para instalar e executar o Agent Builder, seu sistema deve atender a certos requisitos.

Para instalar o Agent Builder, certifique-se de que você tem:

- Um sistema com um mínimo de 1 GB de espaço livre em disco. Agentes que você desenvolve irão requerer espaço adicional em disco.
- Um sistema operacional suportado. O Agent Builder pode ser executado nos seguintes sistemas operacionais:
  - Windows Windows
  - Linux Linux (x86 de somente 64 bits)
- Linux Se você estiver usando o sistema operacional Linux, deverá instalar a biblioteca `libstdc++.so.5`. É possível instalar os pacotes a seguir que fornecem esta biblioteca:
  - No Red Hat Enterprise Linux, `compat-libstdc++-33`
  - No SUSE Enterprise Linux, `libstdc++-33`

Windows Em um sistema Windows, deve-se estar apto para executar o Agent Builder como um usuário com permissão de Administrador. Essas permissões asseguram que o Agent Builder tenha um ambiente consistente com os agentes desenvolvidos com ele.

Linux Em um sistema Linux, é possível executar o Agent Builder como raiz ou como um usuário comum. No entanto, se você executá-lo como um usuário comum, o teste de agentes será limitado e, em alguns casos, pode não estar disponível.

Requisitos do sistema detalhados para o Agent Builder
Use o Software Product Compatibility Reports para visualizar os requisitos do sistema detalhados para o Agent Builder.

Acesse o website do Relatórios de compatibilidade do produto de software. Procure o `IBM Agent Builder` nome do produto.

Instalando o Agent Builder

É possível usar o assistente de instalação ou o procedimento de instalação silenciosa para instalar o Agent Builder.

Dica: Antes de instalar o Agent Builder, desinstale qualquer versão anterior. Para obter informações adicionais sobre a desinstalação, consulte (“Desinstalando o Agent Builder” na página 1168). Nenhuma das informações do agente existente é perdida ao desinstalar.

Usando o assistente de instalação para instalar o Agent Builder
É possível usar o assistente de instalação para instalar o IBM Agent Builder.

Antes de Iniciar

Certifique-se de que o o seu sistema atende aos pré-requisitos. Para obter informações sobre pré-requisitos, consulte “Pré-requisitos para instalar e executar o Agent Builder” na página 1164

Procedimento

1. Se não estiver conectado ao IBM Marketplace, conecte-se com seu IBMid e senha e acesse **Produtos e serviços**.
   A página **Produtos e serviços** está disponível para assinantes ativos. Se você tiver algum problema, acesse o Fórum do Cloud Application Performance Management ou o Marketplace support.
2. Faça download do archive de instalação do Agent Builder:
   a) Na caixa de assinatura do Cloud APM, clique em **Gerenciar** > **Downloads**.
   b) Selecione **Multiplataforma** como sistema operacional.
   c) Selecione o pacote do IBM Agent Builder.
   d) Clique em **Download** e salve `IBM_Agent_Builder_Install.tar` em seu sistema.
3. Extraia o archive de instalação.

4. Use o comando a seguir no diretório de imagens extraído para iniciar a instalação:
   - Windows `setup.bat`
   - Linux AIX `./setup.sh`

   Importante: Execute o programa de instalação com o mesmo ID do usuário com o qual você pretende executar o Agent Builder.
5. Quando a janela **IBM Agent Builder** for aberta, selecione seu idioma e clique em **OK**.
6. Na página **Introdução**, clique em **Avançar**.
7. Na página **Contrato de Licença de Software**, clique em **Eu aceito os termos no contrato de licença** e clique em **Avançar**.
8. Na página **Escolher Pasta de Instalação**, clique em uma das opções a seguir:
   - **Avançar** para instalar o Agent Builder no diretório especificado no campo **Onde Gostaria de Instalar?**.
   - **Restaurar Pasta Padrão** para instalar o Agent Builder em um diretório padrão.
   - **Escolher** para selecionar um diretório diferente.

   Nota: O nome de diretório que você escolher não deve conter os seguintes caracteres:

   !
   #
   %
   ;

   Se ele incluir qualquer um desses caracteres, o Agent Builder pode não iniciar.
9. Na página **Resumo de Pré-instalação**, clique em **Instalar**.
10. Na página **Instalando o IBM Agent Builder**, aguarde a página **Instalação Concluída** abrir, em seguida, clique em **Pronto**.

Resultados

Windows Após o Agent Builder ser instalado, uma opção será incluída no menu Iniciar e o ícone do Agent Builder será incluído em seu desktop. Os arquivos de log de instalação estão em *install_dir* \IBM_Agent_Builder_InstallLog.xml.

Linux AIX Após o Agent Builder ser instalado, o arquivo executável do Agent Builder será nomeado para *Install_Location*/agentbuilder. Os arquivos de log de instalação estão em *install_dir*/IBM_Agent_Builder_InstallLog.xml.

Instalação Silenciosa

É possível instalar o Agent Builder usando um método de instalação silenciosa. Esse método não requer um ambiente gráfico e pode ser facilmente replicado em vários hosts.

Sobre Esta Tarefa

O arquivo de opções de instalação silenciosa, `installer.properties`, está incluído na imagem de instalação na raiz do diretório de instalação. Deve-se modificar esse arquivo para atender às suas necessidades e, em seguida, execute o instalador silencioso. É possível copiar esse arquivo para outros hosts e rapidamente instalar o Agent Builder em todos eles.

Procedimento

1. Se não estiver conectado ao IBM Marketplace, conecte-se com seu IBMid e senha e acesse **Produtos e serviços**.

   A página **Produtos e serviços** está disponível para assinantes ativos. Se você tiver algum problema, acesse o Fórum do Cloud Application Performance Management ou o Marketplace support.
2. Faça download do archive de instalação do Agent Builder:

a) Na caixa de assinatura do Cloud APM, clique em **Gerenciar** > **Downloads**.

b) Selecione **Multiplataforma** como sistema operacional.

c) Selecione o pacote do IBM Agent Builder.

d) Clique em **Download** e salve `IBM_Agent_Builder_Install.tar` em seu sistema.

3. Extraia o archive de instalação.
4. Crie uma cópia do arquivo `installer.properties`, que está localizado no diretório de imagens de instalação.
5. Edite o novo arquivo para se adequar às suas necessidades. Um exemplo dos conteúdos desse arquivo é:

```
# ----------------------------------------------------------------
# IBM Agent Builder
#
# (C) Copyright IBM Corporation 2009.  Todos os direitos reservados.
#
# Arquivo de resposta de amostra para instalação silenciosa
#
# Para usar este arquivo, use o comando a seguir:
#
# Windows:
#    setup.bat -i silent -f <path>\installer.properties
#
# Linux ou AIX:
#    setup.sh -i silent -f <path>/installer.properties
#
# Em que
#    <path> é o caminho completo para o installer.properties
#  (incluindo a letra da unidade ou nome do caminho UNC no Windows).
#    <caminho> não pode conter espaços.
# ----------------------------------------------------------------


# ----------------------------------------------------------------
# Essa propriedade indica que a licença foi aceita
# ----------------------------------------------------------------
# LICENSE_ACCEPTED=FALSE

# ----------------------------------------------------------------
# Esta propriedade especifica o diretório de instalação
#
# No Windows, o padrão é:
#     C:\\Program Files (x86)\\IBM\\AgentBuilder
#
# No Linux, o padrão é:
#     /opt/ibm/AgentBuilder
# ----------------------------------------------------------------
#USER_INSTALL_DIR=C:\\Program Files (x86)\\IBM\\AgentBuilder
#USER_INSTALL_DIR=/opt/ibm/AgentBuilder
```

6. Inicie a instalação silenciosa executando o seguinte comando no diretório de imagens de instalação extraídas:

   Windows `setup.bat -i silent -f path/installer.properties`

   Linux AIX `./setup.sh -i silent -f path/installer.properties`

   Em que *path* é o caminho completo para o arquivo `installer.properties` (incluindo a letra da unidade ou o nome do caminho UNC no Windows). O caminho não pode conter espaços.

Iniciando o Agent Builder

Após instalar o Agent Builder, é possível iniciá-lo.

Procedimento

- Iniciar o Agent Builder usando um dos métodos a seguir
  - Windows Em sistemas Windows:
    - Em um tipo de linha de comandos: *Install_Location*\agentbuilder.exe.

- Selecione **Iniciar** > **Todos os Programas** > **IBM** > **Agent Builder**.
- Clique no **ícone da área de trabalho do Agent Builder**.

- Linux Em sistemas Linux, inicie o arquivo executável a seguir: *INSTALL_DIR*/agentbuilder

Nota: Quando você executa o Agent Builder, ele solicita o local de seu diretório da área de trabalho. Os arquivos que criam os agentes são salvos nesse diretório. É possível designar qualquer diretório como seu espaço de trabalho.

Configurando o navegador padrão no Agent Builder

Linux Em sistemas Linux, talvez seja necessário configurar o navegador padrão do Agent Builder para que as áreas de janela de ajuda sejam exibidas.

Procedimento

1. Selecione **Janela** > **Preferências** para abrir a janela **Preferências**.
2. Selecione e expanda o nó **Geral**.
3. Selecione **Navegador da Web**.
4. Selecione **Usar navegador da web externo**.
5. Selecione o navegador que você deseja usar.
6. Opcional: Para incluir um navegador da web, conclua as etapas a seguir
   a) Clique em **Novo**.
   b) No campo **Nome**, insira um nome descritivo para o navegador.
   c) No campo **Local**, insira o caminho completo para o arquivo executável do navegador.
   d) Clique em **OK**.
7. Clique em **OK**.

Configurando o Time Stamping Authority padrão no Agent Builder

É possível configurar o Time Stamping Authority para arquivos JAR na janela **Preferências** do Agent Builder. Se o certificado de assinatura padrão do Time Stamping Authority expirar, ao configurar uma nova autoridade, será possível continuar a verificar arquivos JAR.

Procedimento

1. Selecione **Janela** > **Preferências** para abrir a janela **Preferências**.
2. Selecione e expanda o nó do **IBM Agent Builder**.
3. Selecione **Assinatura do JAR**.
4. Selecione **Incluir registro de data e hora em arquivos JAR assinados**.
5. Insira a URL do Time Stamping Authority.
6. Clique em **OK**.

Desinstalando o Agent Builder

Dependendo de seu sistema operacional, é possível usar diferentes procedimentos para desinstalar o Agent Builder.

Procedimento

- Linux
  Em sistemas Linux, execute o seguinte comando:
  a) *INSTALL_DIR*/uninstall/uninstaller
  em que *INSTALL_DIR* é o nome do diretório no qual o Agent Builder está instalado.
- Windows

No Windows 7, Windows Server 2008 R2 e versões mais recentes do Windows, conclua as seguintes etapas:

a) Abra os Programas e Recursos do Windows, selecionando **Iniciar** > **Painel de Controle** > **Programas** > **Programas e Recursos**.

b) Selecione **IBM Agent Builder** a partir da lista de programas instalados.

c) Clique em **Desinstalar/Alterar**.

d) Clique em **Desinstalar** na página **Desinstalar IBM Agent Builder**.

e) Clique em **Pronto** na página **Desinstalação Concluída**.

Dica: No Windows 7 e Windows Server 2008 R2, você também pode acessar a janela **Programas e Recursos do Windows**, selecionando **Iniciar** > **Computador** > **Desinstalar ou Alterar um Programa**. Em seguida, continue a partir da etapa "2" na página 1169.

- Windows

  Em outros sistemas Windows, conclua as etapas a seguir:

  a) No Painel de Controle do Windows, selecione **Adicionar ou Remover Programas**.

  b) Clique em **IBM Agent Builder**.

  c) Clique em **Alterar/Remover**.
- Em todos os sistemas operacionais, também é possível usar o método de desinstalação silenciosa. Inicie a desinstalação silenciosa executando o seguinte comando:
  - Windows Em sistemas Windows, *INSTALL_DIR*`/uninstall/uninstaller.exe -i silent`
  - Linux Em sistemas Linux, *INSTALL_DIR*`/uninstall/uninstaller -i silent`

Desinstalação Silenciosa

É possível usar o método de desinstalação silenciosa para desinstalar.

Procedimento

- Inicie a desinstalação silenciosa executando o seguinte comando:

```
INSTALL_DIR/uninstall/uninstaller[.exe] -i silent
```

Criar um agente

Para iniciar criando um agente no Agent Builder, use o novo assistente de agente. Com esse assistente é possível definir a configuração do agente básico e criar uma origem de dados. É possível, então, trabalhar no agente no Agent Builder para incluir mais origens de dados e outras opções, incluindo subnós e grupos navegadores.

Nomeando e configurando o agente

Use o agente de **Agente** para nomear seu agente, configurar sua versão, sistemas operacionais suportados e outras definições de configuração.

Procedimento

1. Use uma das maneiras a seguir para iniciar o assistente Novo agente:

   a) Clique no ícone **Criar Novo Agente** na barra de ferramentas.

   b) No menu Principal, selecione **Arquivo** > **Novo** > **Agente**.

   c) No menu Principal, selecione **Arquivo** > **Novo** > **Outro**. Na página **Selecionar um Assistente**, dê um clique duplo na pasta **Agent Builder** e, em seguida, dê um clique duplo em **Agente**.

   O assistente de **Agente** é aberto.

2. Clique em **Avançar**.
3. Na página **Novo Projeto do Agente**, configure o nome do projeto no campo **Nome do Projeto**. O Agent Builder usa esse nome para a pasta que contém os arquivos do agente. É possível opcionalmente mudar as seguintes configurações:
   - Se você deseja armazenar os arquivos do agente em um local diferente, limpe **Usar local padrão** e clique em **Procurar** para selecionar o novo diretório no **Local** Campos .
   - Você pode alterar o modo com que a Visualização do Navegador Eclipse exibe os recursos ao incluí-los em vários conjuntos de trabalho. Para obter informações adicionais, consulte a ajuda do Eclipse. Para incluir o agente em conjuntos de trabalhos do Eclipse, selecione **Incluir projeto em conjuntos de trabalhos** e clique no botão **Selecionar** para incluir os conjuntos no campo **Conjuntos de trabalhos**.
4. Clique em **Avançar**.
5. Na página **Informações Gerais**, defina as configurações a seguir:
   - Digite a instrução de copyright que você deseja usar para seus novos agentes no campo **Copyright**. Esta declaração deve atender aos requisitos legais para Copyrights. Essa instrução de copyright é inserida em todos os arquivos que são gerados para o agente; é possível editá-la posteriormente.
   - Selecione os sistemas operacionais para o qual deseja que o agente seja construído.

     Importante: Se desejar executar um teste completo do agente dentro do Agent Builder (para obter instruções, consulte "Teste integral de agente" na página 1384), assegure-se de que:
     - Se estiver executando o Agent Builder no Windows, a versão de 32 bits do sistema operacional esteja instalada.
     - Se você estiver executando o Agent Builder no Linux, a versão de 64 bits do sistema operacional esteja instalada.

     Importante: Em alguns casos raros, pode ser necessário instalar o agente em um sistema de 64 bits no qual somente um agente do sistema operacional de 32 bits é instalado. Nesse caso, assegure-se de que a versão 64-bit do sistema operacional não está selecionada e que a versão 32-bit está selecionada.

     Importante: O servidor Wndows 2003 R2 64-bit e sistemas anteriores do Windows não são suportads pelos agentes criados usando o Agent Builder.
6. Clique em **Avançar**.
7. Na página **Informações do Agente**, defina as configurações a seguir:
   - Configure o nome do serviço para o agente no campo **Nome do Serviço** . O nome é exibido na janela **Manage Tivoli Monitoring Services** em um ambiente IBM Tivoli Monitoring e no utilitário **Manage Monitoring Services** e o Editor de limite em um IBM Cloud Application Performance Management. Em sistemas Windows, ele também é o nome do serviço Windows que executa o agente. O nome completo do serviço sempre inicia com `Monitoring Agent for`. Insira a parte restante do nome, que normalmente descreve o serviço que esse agente monitora. O nome pode conter letras, números, espaços e sublinhados.
   - Configure um código do produto de três caracteres para o agente no campo **Código do Produto**. Um código do produto é necessário para ambos IBM Tivoli Monitoring e IBM Cloud Application Performance Management. Vários códigos de produto são reservados para utilização com o Agent Builder. Os valores permitidos são `K00-K99`, `K{0-2}{A-Z}` e `K{4-9}{A-Z}`.

     Importante: Esses valores destinam-se somente a uso interno e não são destinados a agentes que serão compartilhados ou vendidos fora de sua organização. Se estiver criando um agente a ser compartilhado com outros, envie uma nota para toolkit@us.ibm.com para reservar um código do produto. O pedido para um código do produto deve incluir uma descrição do agente a ser montado. Um código do produto é então designado, registrado e retornado a você. Ao receber o código de três letras do produto, você é informado sobre como ativar o Agent Builder para usar o código de produto designado.

- Configure uma sequência que identifique exclusivamente a organização que desenvolve o agente no campo **Identificador da Empresa** (`IBM` é reservado). É possível obtê-lo a partir da URL de sua empresa; por exemplo, se o website da empresa for `mycompany.com`, use o texto `mycompany`.
- Configure uma sequência que identifique exclusivamente o agente no campo **Identificador do Agente**. Por padrão, o Agent Builder configura o Identificador do Agente para ser o mesmo que o do código do Produto.

  Importante: O comprimento combinado do campo **Identificador do Agente** e do campo **Identificador da Empresa** não pode exceder a 11 caracteres.
- Configure a versão do agente no campo **Versão**. A versão do agente contém três dígitos no formato *V*`.`*R*`.`*R*, em que:

  V = Versão
  R = Liberação
  R = Liberação

  Para exibição no ambiente de monitoramento, o valor *V*`.`*R*`.`*R* é convertido no seguinte formato: `0V.RR.00.00`

  Dica: No editor de agente, um campo de **nível de correção** está disponível. O campo de **nível de correção** pode ser utilizado quando liberar uma correção para um agente, sem atualizar a versão.
- Se você deseja que seu agente suporte diversas instâncias, marque a caixa de seleção **Suportar diversas instâncias desse agente**. É possível usar várias instâncias de um agente para monitorar várias instâncias de um aplicativo no mesmo host ou usar um agente instalado em um host para monitorar vários servidores de software em diferentes hosts. Quando você instala um agente que suporta várias instâncias, é possível criar e configurar tantas instâncias quanto forem necessárias.

O que Fazer Depois
Clique em **Avançar** para definir uma origem de dados inicial para o agente. Para obter mais informações, consulte “Definindo origens de dados iniciais” na página 1171

Definindo origens de dados iniciais

Ao criar um agente, defina os dados iniciais que o agente deve monitorar. É possível incluir mais origens de dados posteriormente no editor de agente.

Sobre Esta Tarefa
Defina as origens de dados que seu novo agente deve monitorar usando a página **Origem de Dados Inicial do Agente**. Para obter instruções detalhadas sobre a criação de origens de dados a partir de vários provedores de dados, consulte “Definindo e testando origens de dados” na página 1218.

Procedimento

1. Na página **Origem de Dados Inicial do Agente**, selecione uma das **Categorias de Dados de Monitoramento** e uma das **Origens de Dados**.
2. Clique em **Avançar**. O assistente orienta você pelo processo de definição e configuração de qualquer um dos tipos de coleta de dados que você especificar.

   Dica: É possível usar esse assistente para definir uma origem de dados ou para incluir um subnó ou grupo navegador para organizar o agente. Para obter mais informações sobre subnós, consulte “Usando subnós” na página 1347. Para obter mais informações sobre grupos navegadores, que são usados somente para IBM Tivoli Monitoring, consulte “Criando um Grupo de Navegadores” na página 1346.
3. Se você definiu uma nova origem de dados que possa retornar mais de uma linha de dados, será necessário selecionar atributos-chave. Para obter mais informações, consulte (“Selecionando Atributos-Chaves” na página 1172).

4. Após definir a primeira origem de dados, a janela **Definição de Origem de Dados** é exibida. Para incluir outra origem de dados, selecione o agente, ou um subnó ou grupo navegador se um estiver presente, e clique no botão **Incluir em Selecionados**.
5. Para concluir a definição de origens de dados, clique em **Concluir**. O Agent Builder cria o novo agente e o abre no editor de agente.

Selecionando Atributos-Chaves
Quando um grupo de atributos retorna mais de uma linha de dados, você deve selecionar atributos-chave.

Sobre Esta Tarefa

Quando um grupo de atributos puder retornar mais de uma linha de dados, cada linha representará uma entidade que está sendo monitorada. Sempre que é feita uma amostragem dos dados monitorados, o ambiente de monitoramento corresponde uma linha à entidade que está sendo monitorada e às amostras anteriores dessa entidade. Esta correspondência é realizada com atributos-chave. Um ou mais atributos no grupo de atributos podem ser identificados como atributos-chaves. Esses atributos-chave, quando reunidos, distinguem uma entidade monitorada da outra. Os atributos-chave não são alterados de uma amostra para a próxima para a mesma entidade monitorada.

Os atributos de taxa e de delta são calculados comparando a amostra atual com a amostra anterior. Os atributos-chaves idênticos asseguram que o agente está comparando os valores para a mesma entidade monitorada. Da mesma forma, o agente de resumo e remoção resume as amostras que possuem atributos-chaves idênticos. Além disso, qualquer atributo que seja configurado como um atributo-chave também pode ser usado como um "Item de Exibição" em uma situação.

Você especifica os detalhes sobre a sua nova origem de dados na página **Origem de Dados Inicial do Agente**. Se a origem de dados selecionada puder retornar várias linhas de dados, o Agent Builder pode algumas vezes detectar os atributos-chave. Caso contrário, ele solicita que você selecione atributos-chave.

Procedimento

- Na página **Selecionar atributos-chave**, execute uma das etapas a seguir:
  - Clique em um ou mais atributos a partir da lista que são os atributos-chaves para essa entidade. Para selecionar mais de um atributo, mantenha pressionada a tecla Ctrl.
  - Se esse grupo de atributos retornar somente uma linha, selecione **Produz uma única linha de dados**. Se esta opção for selecionada, nenhum atributo-chave será necessário porque somente uma entidade monitorada sempre será relatada neste grupo de atributos.

Usando o Agent Editor para modificar o agente

Use o Agent Editor para alterar, salvar e confirmar uma versão do agente.

É possível criar um novo agente no Agent Builder; Para obter mais informações, consulte “Criar um agente” na página 1169. Após a criação de um agente, é possível modificá-lo usando o Agent Editor.

Para abrir um agente criado no Agent Builder no Agent Editor, na área **Explorador de Projeto**, localize o nome do agente e expanda-o. Sob o nome do agente, dê um clique duplo em **Definição do Agente**. Alternativamente, dê um clique duplo no nome do arquivo `itm_toolkit_agent.xml`.

O Agent Editor é um editor Eclipse de multipáginas que é possível usar para modificar as propriedades de um agente existente. Cada página no editor corresponde a uma função específica do agente.

A lista de páginas disponíveis é mostrada na visualização Estrutura de Tópicos sob o nó **Definição do Agente**. É possível alternar facilmente para uma outra página clicando em um nó na visualização Esboço. Se a visualização da Estrutura de tópicos estiver ausente ou oculta atrás de outra visualização, é possível reconfigurar a perspectiva Definição do agente. Reconfigure a perspectiva selecionando **Janela** >

Reconfigurar Perspectiva. Como alternativa, clique com o botão direito do mouse no **Agente Definição** guia e selecione **Reconfigurar** no menu.

Nota: Para obter informações e procedimentos detalhados para criação de um agente, consulte "Criar um agente" na página 1169.

As etapas a seguir estão incluídas no Agent Editor:

- "Página Informações do Agente" na página 1173
- Janela Definição da Origem de Dados
- Página Informações de Configuração de Tempo de Execução
- Página do Editor XML do Agente (itm_toolkit_agent.xml)

Nota: Ao visualizar uma página do Editor, também é possível alternar para uma outra página clicando na guia para a página. Algumas páginas mostram guias somente quando são selecionadas na visualização de Estrutura de Tópicos. É possível forçar uma página para ter uma guia mesmo quando ela não é selecionada. Para forçar para que uma página tenha uma guia, clique no ícone de pino para que o pino no ícone aponte em direção à página.

Página Informações do Agente

A página **Informações do agente** é a página principal do Agent Editor.

A página **Informações do Agente** contém as seguintes informações:

- Informações gerais do agente, incluindo o nome do serviço do agente e o código do produto. É possível clicar em **Avançado** para configurar diferentes nomes para diferentes usos, mas essa configuração normalmente não é necessária.
- Informações Conteúdo do Agente
  - Link **Sistemas Operacionais Padrão**
  - **Link Agente Autoexplicativo**
  - **Link Variáveis de Ambiente**
  - **Link Informações de Watchdog**
  - **Link Informações do Cognos**
  - **Link Origens de Dados**
  - **Link Configuração de Tempo de Execução**
  - **Link Recursos**
  - **Link Painéis**
- **Link Testar o Agente**
- **Link Assistente para Gerar Agente**
- **Link Confirmar Versão do Agente**

Configurando o tempo para mensagens de erro transitório

Os assistentes do Agent Editor, às vezes, exibem mensagens de erro transitório. Uma mensagem é exibida por um curto período (por padrão, 3 segundos) no cabeçalho do assistente. Você pode configurar a duração para a qual essas mensagens são exibidas. Para alterar essa configuração:

1. Selecione **Janela** > **Preferências** da barra de menus do Agent Builder. A janela **Preferências** é aberta.
2. Selecione **Agent Builder**.
3. Defina a configuração de **Tempo (segundos) em que a mensagem de erro transitório é exibida**.
4. Clique em **OK**.

Sistemas Operacionais Padrão

Use a página **Sistemas Operacionais Padrão** para mudar os sistemas operacionais para os quais seu agente é criado.

Procedimento

- Para abrir a página **Sistemas Operacionais Padrão**, clique em **Sistemas Operacionais Padrão** na seção **Conteúdo do Agente** da página **Informações do Agente** ou no nó **Sistemas Operacionais Padrão** na Visualização da Estrutura de Tópicos.
- Em **Sistemas Operacionais Padrão** página, selecione os sistemas operacionais que o agente deve suportar.

  Quando você gera um pacote de instalação para o agente, o Agent Builder inclui arquivos para os sistemas operacionais selecionados no pacote. As origens de dados que você inclui em seu agente que não são específicas para o sistema operacional Windows estão disponíveis em qualquer um dos sistemas operacionais selecionados. Os sistemas operacionais nos quais as origens de dados específicas estão disponíveis podem ser alterados a partir dessa seleção padrão. Para alterar os Sistemas Operacionais disponíveis para uma origem de dados específica, use a área de janela **Sistemas Operacionais** da página **Definição de Origem de Dados**. Se os sistemas operacionais padrão não estiverem selecionados, os sistemas operacionais devem ser selecionados para cada origem de dados específica na página **Definição de Origem de Dados**.

  Importante: Se desejar executar um teste completo do agente dentro do Agent Builder (para obter instruções, consulte "Teste integral de agente" na página 1384), assegure-se de que:

  – Se estiver executando o Agent Builder no Windows, a versão de 32 bits do sistema operacional esteja instalada.
  – Se você estiver executando o Agent Builder no Linux, a versão de 64 bits do sistema operacional esteja instalada.

  Importante: Em alguns casos raros, pode ser necessário instalar o agente em um sistema de 64 bits no qual somente um agente do sistema operacional de 32 bits é instalado. Nesse caso, assegure que a versão de 64 bits do sistema operacional não esteja selecionada e que a versão de 32 bits esteja selecionada.

Agente Autoexplicativo

Para o ambiente do IBM Tivoli Monitoring, use a página **Agente Autoexplicativo** para especificar se os arquivos de suporte do agente são empacotados com o agente. Para o ambiente do IBM Cloud Application Performance Management, deve-se deixar o Agente Autoexplicativo ativado.

Procedimento

- Para abrir a página **Agente Autoexplicativo**, clique em **Agente Autoexplicativo** na seção **Conteúdo do Agente** da página **Informações do Agente** ou no nó **Agente Autoexplicativo** na Visualização da Estrutura de Tópicos.

  Por padrão, a autoexplicação é ativada para todos os novos agentes criados com o Agent Builder 6.2.3 ou posterior. Se o agente destina-se ao ambiente do IBM Cloud Application Performance Management, a autodescrição deve ser ativada.

  Quando autoexplicação é ativada para um agente, os pacotes de suporte a aplicativo estão incluídos na imagem do agente. A inclusão permite que o agente obtenha o valor inicial dos arquivos de suporte para o Tivoli Enterprise Monitoring Server, o Tivoli Enterprise Portal Server, o Tivoli Enterprise Portal Browser. Para obter mais informações sobre agentes autoexplicativos, consulte *IBM Tivoli Monitoring Installation and Setup Guide* e *IBM Tivoli Monitoring Administrator's Guide*. Em um ambiente IBM Cloud Application Performance Management, a autodescrição permite que o agente distribua arquivos de suporte para o Servidor Cloud APM; a distribuição é uma etapa necessária no ambiente.

Nota: Em um ambiente IBM Tivoli Monitoring, deve-se ter o Tivoli Monitoring versão 6.2.3 ou posterior instalado para o recurso do agente autoexplicativo funcione e a autoexplicação deve estar ativada no Tivoli Monitoring. Por padrão, a auto-explicação fica desativada no Tivoli Monitoring.

Nota: Selecionar a caixa de seleção **Ativar Autoexplicação para Este Agente** não impede que o agente funcione nas versões anteriores do Tivoli Monitoring.

Variáveis de ambiente

Use a página **Variáveis de Ambiente** para visualizar e modificar variáveis de ambiente que estão disponíveis para o seu agente enquanto ele está em execução.

Antes de Iniciar

Para obter informações adicionais sobre a página **Agent Editor** e **Informações do Agente**, consulte"Usando o Agent Editor para modificar o agente" na página 1172.

Sobre Esta Tarefa

As variáveis de ambiente podem ser aquelas que você define para acesso dentro de um script, ou variáveis predefinidas que fazem com que o agente se comporte de uma determinada maneira. Consulte "Lista de variáveis de ambiente" na página 1175 para obter uma lista de variáveis predefinidas.

Procedimento

1. Para abrir a página **Variáveis de Ambiente**, clique em **Variáveis de Ambiente** na seção **Conteúdo do Agente** da página **Informações do Agente**. Como alternativa, clique no nó **Variáveis de Ambiente** na visualização **Estrutura de Tópicos**.
2. Na página **Variáveis de Ambiente**, clique em **Incluir** para incluir uma nova variável. Como alternativa, para editar uma variável existente, selecione-a e clique em **Editar**.
3. Na janela **Informações da Variável de Ambiente**, configure os valores a seguir:
   - No campo **Nome**, digite um nome da variável ou selecione um nome predefinido na lista.
   - No campo **Valor**, digite um valor para a variável, se desejar configurar uma variável para o agente. Se você não inserir um valor, o agente propagará um valor para a variável existente.
   - No campo **Descrição**, digite uma descrição da variável ou mantenha a descrição existente de uma variável predefinida.

   a) Clique em **OK**.

   A nova variável é listada na tabela na página **Informações do Agente**.

Lista de variáveis de ambiente
Usar as variáveis de ambiente para controlar o comportamento do agente no tempo de execução.

As variáveis de ambiente podem ser construídas no agente usando a página **Variáveis de Ambiente**. Nos sistemas Windows, as variáveis de ambiente são definidas no arquivo K*XX*ENV do agente. Nos sistemas UNIX e Linux, essas variáveis podem ser definidas no arquivo `$CANDLEHOME/config/XX.ini` do agente. *XX* é o código do produto com duas letras. O agente deve ser reiniciado para que as novas configurações tenham efeito.

Nota: As variáveis de ambiente não são configuradas corretamente em um sistema remoto que executa C Shell. Utilize um shell diferente se desejar usar variáveis de ambiente.

Tabela 259. Variáveis de ambiente. Uma tabela listando variáveis de ambiente, seus valores padrão, os intervalos de valores válidos e as descrições de cada variável

Variável de ambiente	Valor Padrão	Valores Válidos	Descrição
CDP_*ATTRIBUTE_GROUP*_ REFRESH_INTERVAL	Não Aplicável	Qualquer número inteiro positivo	O intervalo em segundos no qual um determinado grupo de atributos especificado é atualizado em segundo plano. Essa variável funciona da mesma maneira que CDP_DP_REFRESH_INTERVAL, exceto que se destina somente ao grupo de atributos especificado. O nome do grupo de atributos no nome de variável deve estar em maiúscula, mesmo se o nome do grupo de atributos real não estiver.
CDP_DP_CACHE_TTL	55	Qualquer número inteiro maior ou igual a 1.	Dados coletados para um grupo de atributos são armazenados em cache por esse número de segundos. Vários pedidos para os mesmos dados neste intervalo de tempo recebem um cópia dos dados em cache. Este valor se aplica a todos os grupos de atributos no agente.
CDP_*ATTRIBUTE_GROUP*_CACHE_ TTL	Valor de CDP_DP_CACHE _TTL	Qualquer número inteiro maior ou igual a 1.	Os dados que são coletados para o grupo de atributos especificado são armazenados em cache para esse número de segundos. Vários pedidos para os mesmos dados neste intervalo de tempo recebem um cópia dos dados em cache. Este valor substitui CDP_DP_CACHE_TTL para o grupo especificado. O nome do grupo de atributos no nome de variável deve estar em maiúscula, mesmo se o nome do grupo de atributos real não estiver.
CDP_DP_IMPATIENT_ COLLECTOR_TIMEOUT	5 se subnós estiverem definidos, caso contrário, não será definido	Qualquer número inteiro positivo	O número de segundos a aguardar para cada coleta de dados acontecer antes do tempo limite e retornar dados em cache, mesmo se os dados em cache forem antigos. (Os dados armazenados em cache serão antigos, se mais antigos do que CDP_DP_CACHE_TTL segundos). Se esta variável não for configurada, o agente aguarda até que a coleta de dados seja concluída. A espera às vezes pode atingir o tempo limite Tivoli Enterprise Portal e abandonar a espera. Se nenhum conjunto de encadeamentos estiver configurado, esta variável será ignorada e a coleta de dados será feita de maneira síncrona.

Tabela 259. Variáveis de ambiente. Uma tabela listando variáveis de ambiente, seus valores padrão, os intervalos de valores válidos e as descrições de cada variável *(continuação)*

Variável de ambiente	Valor Padrão	Valores Válidos	Descrição
CDP_DP_REFRESH_INTERVAL	60 se os subnós estiverem definidos, caso contrário, não será configurado	Qualquer número inteiro positivo	O intervalo em segundos no qual os grupos de atributos são atualizados em segundo plano. Se esta variável não estiver configurada ou estiver configurada como 0, as atualizações em segundo plano serão desativadas. Se um conjunto de encadeamentos estiver configurado (consulte a variável CDP_DP_THREAD_POOL_SIZE), em seguida, os grupos de atributos poderão ser atualizados em paralelo. Se não houver nenhum conjunto de encadeamentos, as atualizações ocorrerão serialmente, o que pode levar um longo tempo. Logicamente equivalente a um tamanho de conjunto de encadeamentos de 1.
CDP_DP_THREAD_POOL_SIZE	15 se os subnós estiverem definidos, caso contrário, não será configurado	Qualquer número inteiro positivo	O número de encadeamentos criados para executar coletas de dados em segundo plano em um intervalo definido por CDP_DP_REFRESH_INTERVAL. Se esta variável não estiver configurada ou estiver configurada como 0, não haverá nenhum conjunto de encadeamentos. Se CDP_DP_THREAD_POOL_SIZE for configurado com um valor maior que 1 e CDP_DP_REFRESH_INTERVAL for configurado como 0, o valor de CDP_DP_THREAD_POOL_SIZE será ignorado e a coleta de dados acontecerá sob demanda. O grupo de atributos de Status do Conjunto de Encadeamentos mostra como o conjunto de encadeamentos está em execução. Utilize o Status do Conjunto de Encadeamento para ajustar o tamanho do conjunto de encadeamentos e o intervalo de atualização para melhores resultados. Como padrão, a consulta para este grupo de atributos não é exibida na árvore Navigator do agente. Você pode não se lembrar de incluir a consulta em uma área de trabalho customizada para o agente. No entanto, você poderá visualizá-la facilmente designando a consulta de Status do Conjunto de Encadeamentos para uma visualização de área de trabalho no nível do agente da base.

Tabela 259. Variáveis de ambiente. Uma tabela listando variáveis de ambiente, seus valores padrão, os intervalos de valores válidos e as descrições de cada variável *(continuação)*

Variável de ambiente	Valor Padrão	Valores Válidos	Descrição
CDP_JDBC_MAX_ROWS	1000	Qualquer número inteiro positivo	O número máximo de linhas de dados que o provedor de dados JDBC retorna. Um conjunto de resultados que contém mais do que este número de linhas é processado somente até este valor máximo. É possível desenvolver consultas para evitar o retorno de dados em excesso para o IBM Tivoli Monitoring.
CDP_NT_EVENT_LOG_GET_ALL_ENTRIES_FIRST_TIME	NÃO	SIM, NÃO	Se configurado para SIM, o agente envia um evento para cada evento no log de eventos do Windows . Se configurado para NÃO, somente eventos novos no log de eventos do Windows serão enviados.
CDP_NT_EVENT_LOG_CACHE_TIMEOUT	3600	Qualquer número inteiro maior ou igual a 300.	O número de segundos durante os quais os eventos do Log de Eventos do Windows são armazenados em cache pelo agente. Todos eventos armazenados em cache são retornados quando o grupo de atributos do log de eventos é consultado. **Nota:** Esta variável não é mais usada. Use a variável CDP_PURE_EVENT_CACHE_SIZE.
CDP_PURE_EVENT_CACHE_SIZE	100	Qualquer número inteiro positivo maior ou igual a 1.	O número máximo de eventos para cache para uma origem de dados de arquivo de log configurada para processar novos registros, para o grupo de atributos de Log de Eventos do Windows. E também para os monitores JMX e notificações. Cada registro novo no log faz com que um eventos seja enviado. Esta variável de ambiente define quantos eventos são conservados em um cache pelo agente. Os valores armazenados em cache são retornados quando o grupo de atributos é consultado.
CDP_DP_ACTION_TIMEOUT	20 segundos	Qualquer número inteiro positivo maior ou igual a 1.	O número de segundos a aguardar que um Executar Ação que está sendo manipulado pelo agente complete.
CDP_DP_SCRIPT_TIMEOUT	30 segundos	Qualquer número inteiro positivo maior ou igual a 10.	O número de segundos a se esperar para que o programa iniciado por um grupo de atributos baseados em script conclua.

Tabela 259. Variáveis de ambiente. Uma tabela listando variáveis de ambiente, seus valores padrão, os intervalos de valores válidos e as descrições de cada variável *(continuação)*

Variável de ambiente	Valor Padrão	Valores Válidos	Descrição
CDP_DP_PING_TIMEOUT	30 segundos	Qualquer número inteiro positivo maior ou igual a 10.	O número de segundos a aguardar que o programa iniciado por um código de retorno de comando conclua. **Nota:** Esta variável não está relacionada ao provedor de dados de ping ICMP.
CDP_SNMP_MAX_RETRIES	2	Qualquer número inteiro positivo	O número de vezes para tentar enviar o pedido de SNMP novamente. O número total de solicitações enviadas para o agente SNMP é este valor mais um se nenhuma resposta for recebida.
CDP_SNMP_RESPONSE_TIMEOUT	2 segundos	Qualquer número inteiro positivo	O número de segundos a aguardar até que cada solicitação SNMP exceda o tempo limite. Cada linha no grupo de atributos é um pedido separado. Esse valor de tempo limite é o número de segundos a aguardar por uma resposta antes de tentar novamente. O tempo limite total para uma linha exclusiva de dados é (CDP_SNMP_MAX_RETRIES + 1) * CDP_SNMP_RESPONSE_TIMEOUT. O valor de tempo limite padrão total é (2+1) * 2 = 6 segundos.
CDP_DP_HOSTNAME	Nome da primeira interface de rede instalada	Um endereço IP ou nome do host	Configura o nome do host preferencial (interface de rede) em um sistema de interface múltipla. Use esta variável de ambiente se o agente ligar suas portas de atendimento a um endereço da interface de rede não padrão. Utilizado pelo provedor de dados SNMP. Para origens de dados do Soquete, essa variável aplica-se caso CDP_DP_ALLOW_REMOTE também seja configurado.
CDP_SNMP_ALLOW_ DECREASING_OIDS	NÃO	SIM, NÃO	Se configurado como YES, os provedores de dados SNMP não verificam se OIDs retornados estiverem aumentando. Configure como YES com cuidado, pois o agente monitorado pode ter problemas que esta verificação normalmente capturaria.
KUMP_DP_COPY_MODE_SAMPLE_I NTERVAL	60	Tempo de espera em segundos	Para um provedor de dados de arquivo de log, especifica quanto tempo esperar antes que ele releia o conteúdo de um arquivo, quando o agente é definido para **Processar todos os registros quando o arquivo for amostrado**. O tempo é especificado em segundos.

Tabela 259. Variáveis de ambiente. Uma tabela listando variáveis de ambiente, seus valores padrão, os intervalos de valores válidos e as descrições de cada variável *(continuação)*

Variável de ambiente	Valor Padrão	Valores Válidos	Descrição
KUMP_MAXPROCESS	100%	5-100%	Para um provedor de dados de arquivo de log, especifica o uso máximo do processador aplicado para processar dados de arquivo. Os valores estão na faixa de 5 a 100 por cento. O padrão é 100 por cento.
KUMP_DP_SAMPLE_FACTOR	5	Qualquer número inteiro positivo	Para um provedor de dados de arquivo de log, configura o fator de amostra quando você selecionar **Processar todos os registros quando o arquivo for amostrado** no Agent Builder. Esse tempo de espera garante que os padrões que ampliam vários registros sejam gravados antes da criação de log varrer em busca do padrão.
KUMP_DP_EVENT	5	Qualquer número inteiro positivo	Para um provedor de dados do arquivo de log, configura a frequência de amostra para dados do Evento, em segundos.
KUMP_DP_FILE_EXIST_WAIT	SIM	SIM, NÃO	Para um provedor de dados do arquivo de log, especifica que o encadeamento de monitoramento de arquivos continuará a ser executado se ele detectar que o arquivo monitorado está ausente ou vazio. O encadeamento aguarda até o arquivo existir, verifica novamente a cada alguns segundos e inicia ou reinicia o monitoramento quando o arquivo é disponibilizado.
KUMP_DP_FILE_SWITCH_ CHECK_INTERVAL	600	Qualquer número inteiro positivo	A frequência, em segundos, que o Provedor de Dados do arquivo de log procura por um arquivo de monitoramento diferente a ser alternado quando o suporte de nome do arquivo dinâmico estiver ativado.
KUMP_DP_FILE_ROW_ PAUSE_INCREMENT	none	Qualquer número inteiro positivo	Para um provedor de dados do arquivo de log, especifica como muitos registros de arquivos são lidos antes do encadeamento de monitoramento do arquivo pausar. A pausa é para que as atualizações anteriores possam ser processadas. Utilize essa variável de ambiente somente se o arquivo monitorado receber bursts de altos volumes de novos registros e você estiver preocupado que algumas atualizações de registro possam ser perdidas.

Tabela 259. Variáveis de ambiente. Uma tabela listando variáveis de ambiente, seus valores padrão, os intervalos de valores válidos e as descrições de cada variável *(continuação)*

Variável de ambiente	Valor Padrão	Valores Válidos	Descrição
CDP_COLLECTION_TIMEOUT	60 segundos	Qualquer número inteiro positivo	O número de segundos que o agente aguarda por uma resposta de um coletor de dados que foi iniciado em outro processo. Os coletores de dados JMX, JDBC, HTTP e SOAP são exemplos.
CDP_SSH_TEMP_DIRECTORY	. (ponto)	Qualquer sequência de caminhos válida no sistema remoto	Para um provedor de dados de Script ativado por SSH, especifica um local no sistema remoto. Os arquivos de script que são fornecidos com o agente serão transferidos por upload para este local. Um local relativo é relativo ao diretório inicial do usuário. O padrão de . (período) é relativo ao diretório inicial do usuário.
CDP_SSH_DEL_COMMAND	rm -Rf	Qualquer sequência de caracteres de comando válida no sistema remoto	Para um provedor de dados de Script ativado por SSH, especifica o comando para começar a excluir os arquivos de script transferidos por upload, fornecidos com o agente.
CDP_SNMP_SEND_DELAY_FACTOR	0 milissegundos	Qualquer número inteiro positivo	O envio de SNMP inicial é atrasado de 0 até o número de milissegundos especificados. Essa variável somente será ativada, se o conjunto de encadeamentos também estiver ativado. O atraso não se aplica a todos os envios, somente ao primeiro envio feito por um grupo de atributos. Esta variável é útil se o dispositivo que está sendo monitorado pode às vezes falham ao responder corretamente se ele recebe vários pedidos ao mesmo tempo.
CDP_ICMP_PING_REFRESH_INTERVAL	60 segundos	Qualquer número inteiro maior ou igual a 1	O ping é executado nos sistemas em um arquivo de lista de dispositivos nesse intervalo. Se os pings usarem muito tempo, haverá sempre um atraso de pelo menos CDP_PING_MIN_INTERVAL_DELAY segundos antes de iniciar os pings novamente. Os dados são atualizados não mais frequentemente do que esta configuração. Os dados podem ser atualizados com menos frequência, baseados no número de entradas no arquivo de lista de dispositivos e no tempo que leva para receber as respostas.

Tabela 259. Variáveis de ambiente. Uma tabela listando variáveis de ambiente, seus valores padrão, os intervalos de valores válidos e as descrições de cada variável *(continuação)*

Variável de ambiente	Valor Padrão	Valores Válidos	Descrição
CDP_ICMP_PING_MIN_INTERVAL_DELAY	30 segundos	Qualquer inteiro maior ou igual a 1 e menor do que o intervalo de atualização de Ping CDP	Após executar ping nos dispositivos em um arquivo de lista de dispositivos, o próximo intervalo de atualização de ping não será iniciado até que pelo menos esse número de segundos decorra.
CDP_ICMP_PING_BURST	10	Qualquer número inteiro maior ou igual a 0	O número de pings que são enviados antes de o agente pausar pela quantidade de tempo especificada pela variável CDP_ICMP_PING_BURST_DELAY. Um valor 0 desativa essa função.
CDP_ICMP_PING_BURST_DELAY	10	Qualquer número inteiro maior ou igual a 0	A quantidade de tempo em milissegundos a aguardar após enviar um número definido de pings, conforme definido pela variável CDP_ICMP_PING_BURST. Um valor 0 desativa essa função.
CDP_ICMP_PING_TIMEOUT	2000 milissegundos	Qualquer número inteiro maior ou igual a 1	O número de milissegundos a aguardar por uma resposta de ping. Essa configuração se aplica a cada tentativa de ping que é feita. Tentativas de ping são feitas 3 vezes para cada host. Se nenhuma resposta for recebida de qualquer uma das 3 tentativas, o tempo total aguardado para uma resposta será CDP_ICMP_PING_TIMEOUT multiplicado por 3. Por padrão, esse valor é 6000 milissegundos. Alterar o valor de CDP_ICMP_PING_TIMEOUT faz a enumeração TIMEOUT padrão do atributo Tempo de resposta atual não se aplicar mais. Altere enumeração de TIMEOUT para o novo valor de CDP_ICMP_PING_TIMEOUT multiplicado por 3.

Tabela 259. Variáveis de ambiente. Uma tabela listando variáveis de ambiente, seus valores padrão, os intervalos de valores válidos e as descrições de cada variável *(continuação)*

Variável de ambiente	Valor Padrão	Valores Válidos	Descrição
CDP_JDBC_CONNECTIONLESS	false	true, false	Se configuradas como true, as conexões de JDBC serão encerradas depois de cada tentativa de coleta de dados. Isto é, todos os grupos de atributos tentam criar sua própria conexão cada vez que os dados são coletados. As conexões não serão reutilizadas, se essa variável estiver ativada. Se configuradas como false, será feita uma conexão com o banco de dados e essa conexão será compartilhada entre os grupos de atributos.
CDP_SSH_EXCLUDED_ ENVIRONMENT_VARIABLES	none	Uma lista separada por vírgula de nomes de variáveis de ambiente	Para um provedor de dados de Script ativado por SSH, especifica o conjunto de variáveis de ambiente locais que não devem ser configuradas no ambiente do sistema remoto.
CDP_DP_EVENT_LOG_MAX_ BACKLOG_TIME	0 segundos	0, 1 ou qualquer número inteiro maior que 1	Se configuradas como 0, e CDP_DP_EVENT_LOG_MAX_BACKLOG_EVENTS não for configurado para 1 ou um inteiro maior, não processará eventos gerados enquanto o agente estiver encerrado. 0 é o padrão. Se configurado como 1, e CDP_DP_EVENT_LOG_MAX_BACKLOG_EVENTS não estiver configurado como um número inteiro maior que 1, processará todos os eventos gerados enquanto o agente estiver encerrado. Se configurado como maior que 1, e CDP_DP_EVENT_LOG_MAX_BACKLOG_EVENTS não estiver configurado como maior que 1, processará eventos gerados dentro desse valor em segundos do tempo do computador atual. Por exemplo, se o valor for configurado como 300, na inicialização, o agente processará todos os eventos gerados em 300 segundos do tempo atual. Em que um valor maior que 1 é inserido para ambas CDP_DP_EVENT_LOG_MAX_BACKLOG_TIME e CDP_DP_EVENT_LOG_MAX_BACKLOG_EVENTS, esse intervalo de tempo de eventos ou esse número de eventos é processado. Qual variável será escolhida depende de qual for correspondida primeiro.

Tabela 259. Variáveis de ambiente. Uma tabela listando variáveis de ambiente, seus valores padrão, os intervalos de valores válidos e as descrições de cada variável *(continuação)*

Variável de ambiente	Valor Padrão	Valores Válidos	Descrição
CDP_DP_EVENT_LOG_ *Windows_Event_Log*_MAX_BACKLOG_ TIME	0 segundos (Não processa eventos perdidos enquanto o agente está encerrado)	0, 1 ou qualquer número inteiro maior que 1	Se configurada para
CDP_DP_EVENT_LOG_ MAX_BACKLOG_EVENTS	0 eventos	0, 1 ou qualquer número inteiro maior que 1	Se configuradas como 0, e a variável CDP_DP_EVENT_LOG_MAX_BACKLOG _TIME não estiver configurada para 1 ou um inteiro maior, não processará eventos gerados enquanto o agente estiver encerrado. 0 é o padrão. Se configuradas como 1, e a variável CDP_DP_EVENT_LOG_MAX_BACKLOG _TIME não estiver configurada como um número inteiro maior que 1, processará todos os eventos gerados enquanto o agente estiver encerrado. Se configurado como maior que 1, e CDP_DP_EVENT_LOG_MAX_BACKLOG _TIME não for configurado como maior que 1, processará no máximo esse número de eventos gerados enquanto o agente estiver encerrado. Por exemplo, se o valor for configurado como 200, em seguida, na inicialização do agente, os 200 eventos gerados diretamente antes da inicialização serão processados. Em que um valor maior que 1 é inserido para ambas CDP_DP_EVENT_LOG_MAX_BACKLOG _EVENTS e CDP_DP_EVENT_LOG_MAX_BACKLOG _BACKLOG_TIME, esse intervalo de tempo de eventos ou esse número de eventos é processado. Qual variável será escolhida depende de qual for correspondida primeiro.
CDP_DP_EVENT_LOG_ *Windows_Event_Log*_MAX_BACKLOG_ EVENTS	0 eventos (Não processa eventos perdidos enquanto o agente está encerrado)	0 ou um número inteiro maior ou igual a 1	Se configurada para

Tabela 259. Variáveis de ambiente. Uma tabela listando variáveis de ambiente, seus valores padrão, os intervalos de valores válidos e as descrições de cada variável *(continuação)*

Variável de ambiente	Valor Padrão	Valores Válidos	Descrição
CDP_HTTP_READ_TIMEOUT	10	Qualquer número inteiro positivo	O número de segundos a aguardar por uma resposta para a solicitação de HTTP.
CDP_JAT_THREAD_POOL_SIZE	15	Qualquer número inteiro positivo	O número de encadeamentos usados pelos provedores do Java para manipular as solicitações de coleção de dados. JMX, JDBC, HTTP e provedores de dados SOAP são os provedores que podem se beneficiar desse conjunto de encadeamentos.
CDP_HTML_OBJECTS_THREAD_POOL_SIZE	10	Qualquer número inteiro positivo	O número de encadeamentos que são usados para fazer download de objetos da página localizados em URLs monitoradas com o provedor de dados HTTP.
CDP_HTTP_SOAP_MAX_ROWS	500	Qualquer número inteiro positivo	O número máximo de linhas que são retornadas pelo provedor de dados SOAP HTTP.
CDP_DP_ALLOW_REMOTE	NÃO	NO, YES	Se configurado como Sim, o agente permitirá conexões do soquete remoto. Se configurado como Não, o agente permitirá somente conexões do soquete a partir do host local. Não é o padrão.
CDP_DP_INITIAL_COLLECTION_DELAY	varies	Qualquer número inteiro positivo	O número de segundos, após o início do agente, até que o conjunto de encadeamentos inicie suas coletas de dados planejadas.

Informações do Watchdog

Use o **Informações de Watchdog** página para especificar informações de configuração para o Agent Watchdog.

Sobre Esta Tarefa

Para abrir a página **Informações de Watchdog**, clique em **Informações de Watchdog** na seção **Conteúdo do Agente** da página **Informações do Agente**. Também é possível selecionar o nó **Informações de Watchdog** na Visualização da Estrutura de Tópicos.

Você pode especificar as seguintes informações de configuração para o Agent Watchdog:

- **Monitorar este Agente por Padrão**

  Selecione esta caixa de opção para colocar o agente sob gerenciamento pelo Agent Management Services quando o agente for instalado. O agente é monitorado por comportamento inoperante ou finalização anormal e será reiniciado por um watchdog.

- **Frequência de Verificação (segundos)**

Com que frequencia o vigilante verifica o processo do agente em busca de comportamento perigoso ou finalização anormal. O padrão é a cada 180 segundos.

- **Número Máximo de Reinícios**

  Número de vezes que o Watchdog reiniciará o agente por causa do comportamento inoperante ou finalização anormal em um período de 24 horas antes de alertar o administrador sobre o problema. O período começa todos os dias à meia-noite. Assim, o primeiro período de quando o agente é iniciado pode ser "curto".

  Se o agente ficar inativo por algum motivo, haverá uma reinicialização. O Watchdog também pára e reinicia o agente se o agente se torna não responsivo ou saudável, por exemplo. Se o limite de memória for ultrapassado. O padrão é quatro reinícios em um período de 24 horas, em que o período é medido da meia-noite às 11:59. À meia-noite, a contagem do reinício diário do agente retorna para 0 automaticamente.

- **Informações de Limite de Memória**

  O tamanho do processo do agente (em megabytes) para o qual o agente pode aumentar antes que seu segurança o considere prejudicial. Há um valor separado para o Windows, o Linux e o UNIX. Se o processo do agente crescer além do limite, o watchdog parará o processo e o reiniciará. Não há padrão para essas propriedades. Se nenhum valor for especificado, o Watchdog não monitorará o tamanho do processo. A métrica usa o tamanho do conjunto de trabalho no Windows e a memória do usuário no UNIX e Linux.

Se o Watchdog parar o agente e o número máximo de reinícios tiver sido alcançado, o Watchdog enviará um alerta informando que o agente excedeu sua contagem de reinícios e parará de realizar reinícios automáticos. O Watchdog ainda relata se o agente está ativo ou inativo, assumindo que é iniciado de outra maneira, por exemplo, através do Tivoli Enterprise Portal.

Você deve reiniciar manualmente o agente utilizando o comando Executar Ação do AMS Start Agent, assim a contagem de reinícios não é redefinida.

A contagem é reiniciada em uma das seguintes maneiras (o Watchdog continua a trabalhar e relata o status, mas não realiza reinícios automáticos):

- O clock começa à meia-noite.
- O usuário usa o comando AMS Start Agent Take Action, o qual possui um parâmetro de entrada chamado **resetRestartCount**. Se você inserir um valor de 1 (significando "true"ou "yes"), a contagem de reinicializações diárias é redefinida de volta para 0.

Para obter informações adicionais, consulte as seções a seguir no *IBM Tivoli Monitoring: Guia do Administrador*:

- Para Agentes do Tivoli System Monitor

  Configurando o Agent Management Services no Tivoli System Monitor Agents

- Para Agentes de Monitoramento Corporativo Tivoli

  Instalando e Configurando o Tivoli Agent Management Services

Informações do Cognos

Use a página **Informações do Cognos** para especificar as informações usadas quando um modelo de dados Cognos é gerado para seu agente. Essas informações são usadas somente para o ambiente IBM Tivoli Monitoring.

Procedimento

1. Para abrir a página **Informações do Cognos**, clique em **Informações do Cognos** na seção **Conteúdo do Agente** da página **Informações do Agente** ou o nó **Informações do Cognos** na Visualização da Estrutura de Tópicos.
2. No campo **Origem de Dados**, insira o nome da origem de dados que conecta o Tivoli Common Reporting ao IBM Tivoli Data Warehouse.

O valor padrão é TDW.

3. No campo **Esquema**, insira o nome do esquema do banco de dados usado para o Tivoli Data Warehouse, que é usado para completar os nomes de tabelas nos relatórios do Cognos.

   O valor padrão é ITMUSER. Este valor poderá ser alterado no Framework Manager quando o modelo do Cognos for carregado no Framework Manager.

   A caixa de seleção **Incluir este grupo de atributos em uma categoria de relatório** na página **Definição de Origem de Dados** determina onde no modelo Cognos o grupo de atributos é colocado. Se não for selecionada, o grupo de atributos é colocado na pasta de atributos estendidos no modelo Cognos. Se selecionado, o grupo de atributos é colocado na subpasta selecionada (disponibilidade ou desempenho) na pasta Métricas Principais. Para obter informações sobre os campos de origem de dados, consulte Tabela 260 na página 1191.

O que Fazer Depois

Você pode usar o modelo de dados do Cognos para criar os relatórios do Tivoli Common Reporting para seu agente, consulte “Geração de Modelo de Dados Cognos” na página 1477.

Link do Assistente Gerar Agente

Quando terminar de criar ou editar o novo agente, utilize o assistente Gerar Agente para preparar a instalação.

Procedimento

- Ao concluir a criação ou edição do novo agente, na página **Agent Editor Informações do Agente**, clique no link **Gerar Assistente do Agente**.

  Com o assistente Gerar Agente, você pode:

  – Gerar os arquivos do agente com uma instalação do Tivoli Monitoring no sistema local. Para obter instruções, veja “Instalando um agente localmente” na página 1389.

  – Criar um pacote para que o agente possa ser instalado em outros sistemas. Para obter instruções, veja “Criando o pacote de agente” na página 1391.

A página Definição de Origem de Dados

Use a página **Definição de Origem de Dados** para manipular origens de dados.

Sobre Esta Tarefa

A página **Definição de Origem de Dados** lista as origens de dados que estão configuradas para o agente. Quando uma origem de dados ou um atributo é selecionado na árvore, a página é atualizada para exibir as propriedades para o objeto selecionado. Utilize os campos para modificar as propriedades para a origem de dados ou o atributo selecionado.

Nota: Para obter instruções detalhadas sobre a criação de origens de dados a partir de vários provedores de dados, consulte “Definindo e testando origens de dados” na página 1218.

Procedimento

- Para abrir a página **Definição de Origem de Dados**, clique em **Origens de Dados** na seção **Conteúdo do Agente** da página **Informações do Agente** ou nó **Origens de Dados** na visualização **Estrutura de Tópicos**.
- É possível incluir mais origens de dados ao clicar em **Incluir no Selecionado** ou clicar com o botão direito na árvore de navegação e selecionar uma das opções.
- É possível remover as origens de dados e os atributos clicando neles com o botão direito do mouse e selecionando **Remover**.
- É possível incluir, modificar e remover atributos. Para obter instruções, consulte “Editando as propriedades da origem de dados e do atributo” na página 1191

Copiando origens de dados usando a página Definição de Origem de Dados

Use a página **Definição de Origem de Dados** para copiar as origens de dados.

Antes de Iniciar

Vá para a página **Definição de Origem de Dados**. Para obter mais informações, consulte "A página Definição de Origem de Dados" na página 1187

Sobre Esta Tarefa

Origens de dados que resultam em grupos de atributos podem ser copiadas para a área de transferência e coladas de volta nesse agente ou em outro agente. As origens de dados que não resultam em grupos de atributos são origens de dados de Disponibilidade e Windows Event Log.

Procedimento

1. Selecione os grupos de atributos que deseja copiar.
2. Corte ou copie o grupo de atributos usando um dos métodos a seguir:
   - Clique em **Editar** > **Recortar** > **Editar** > **Copiar** na barra de menus.
   - Clique com o botão direito em um dos itens selecionados e clique em **Recortar** ou **Copiar** do menu.
   - Use um sistema operacional ou o pressionamento de teclas do Eclipse que chama a ação recortar ou copiar. Por exemplo, nos sistemas Windows, pressionar **Ctrl-C** chama ação de cópia.

   Para remover origens de dados de seu local existente e colocá-las na área de transferência, use **Recortar**. Para deixar as origens de dados no local e copiá-las na área de transferência, use **Copiar**.
3. Selecione o pai de um grupo de atributos (o agente, um subnó ou um grupo de navegadores) ou selecione um grupo de atributos existente.
4. Cole a seleção usando uma das opções a seguir:
   - Selecione **Editar** > **Colar** na barra de menus.
   - Clique com o botão direito do mouse no nó no qual deseja colar a seleção na árvore e clique em **Colar** no menu.
   - Use um dos sistemas operacionais ou o pressionamento de teclas do Eclipse que ativa a ação de Colar. Por exemplo, nos sistemas Windows, pressionar **Ctrl-V** chama a ação de colagem.

Resultados

Os grupos de atributos da área de transferência são colocados no pai selecionado. Como alternativa, se um grupo de atributos for selecionado, os grupos de atributos serão colocados no pai do grupo de atributos selecionado.

Se houver um conflito de nomes com outro grupo de atributos durante a colagem, o nome do grupo de atributos colado será alterado suavemente para evitar o conflito.

Página Informações de Configuração de Tempo de Execução

A página **Informações de Configuração de Tempo de Execução** exibe as variáveis configuráveis no agente. É possível configurar valores para as variáveis quando você instala o agente em um host monitorado.

Esses valores se tornam disponíveis para os códigos de retorno do comando e os scripts por meio do ambiente. Para abrir a página **Informações de Configuração de Tempo de Execução**, clique em **Configuração de Tempo de Execução** na seção **Conteúdo de Agente** da página **Informações do Agente** ou o nó **Configuração de Tempo de Execução** na Visualização da Estrutura de Tópicos. O Agent Builder automaticamente constrói o nome da variável de ambiente a partir do código do produto e do rótulo.

É possível incluir e mudar as propriedades de configuração e fornecer valores padrão usando a página **Informações de Configuração de Tempo de Execução**.

Página Editor XML do Agente

A página **Editor de XML do Agente** exibe o XML para a definição do agente.

O XML de definição do agente inclui as informações que são exibidas em todas as outras partes do Agent Builder. Se você alterar o XML, as informações exibidas em Agent Builder refletem a mudança.

Atenção: Não faça nenhuma mudança no XML. Essas mudanças podem causar erros que podem impedir você de gerar o agente ou afetar negativamente o funcionamento do agente.

Salvando as Edições e Alterações

Mudanças feitas com o editor não são armazenadas até que você as salve.

Procedimento

- Execute um salvamento de uma das maneiras a seguir:
  - Selecione **Arquivo** > **Salvar**, selecionando o ícone de salvamento (disquete).
  - Pressione **Ctrl+S**

  Ao salvar, ocorre uma validação para garantir que as informações estejam completas. Se ocorrerem problemas, informações sobre o erro serão exibidas na visualização **Problemas** do Eclipse. Se esta visualização não estiver visível, selecione **Janela** > **Mostrar Visualização** > **Problemas**. Se você tentar gerar um agente que tem erros, será exibida uma mensagem de erro.

  Nota: Você deve corrigir todos os erros e salvar as alterações antes de gerar e instalar o agente.

Confirmando a Versão do Agente

Confirmar seu agente quando estiver certo de ter terminado o desenvolvimento dessa versão do agente e estará pronto para entregá-lo.

Sobre Esta Tarefa

Sistemas IBM Tivoli Monitoring requerem que novas versões de um agente incluam todas as informações que estão contidas nas versões anteriores desse agente que foram usadas no ambiente de monitoramento. Incluir todas as informações das versões anteriores é necessário a fim de que áreas de trabalho, situações e consultas continuem a funcionar se o novo agente estiver instalado em alguns hosts monitorados, mas o antigo permanece nos outros.

Após você concluir o desenvolvimento e teste de um agente, deverá confirmar o agente como a versão final para um determinado número da versão. O Agent Builder assegura que nenhuma informação seja removida após você confirmar o agente. As compilações subsequentes do agente têm um novo número da versão.

Há um limite de 1.024 versões.

Lembre-se: Se você fizer mudanças em um agente que deve ser testado e executado em um ambiente IBM Cloud Application Performance Management, deve-se alterar a versão do agente.

Procedimento

1. Abra a janela **Agent Editor**, página **Informações do Agente**.
2. Na área **Confirmar Versão do Agente**, clique em **confirmar esse nível**.
3. Faça backup do agente confirmado ou verifique-o no sistema de controle de versão.

O que Fazer Depois

Depois de confirmar um agente, toda mudança adicional no agente será parte de uma nova versão. Você deve inserir o novo número da versão para que as mudanças adicionais possam ser salvas. Quaisquer mudanças na nova versão devem não quebrar a compatibilidade com versões anteriores do agente.

Depois de confirmar o agente, não é possível concluir estas ações nos objetos que existiam antes do agente ter sido confirmado:

- Excluir atributos de um grupo de atributos.
- Excluir grupos de atributos.
- Reordenar atributos existentes em um grupo de atributos.
- Reorganizar grupos de atributos existentes (usando itens do Navegador).
- Mova os grupos de atributos ou grupos do navegador para ou dos subnós.
- Renomear grupos de atributos.
- Renomear atributos.
- Alterar tipos de dados de atributos existentes.
- Altere um nome ou um tipo de subnó se ele contiver um grupo de atributos que existia antes da confirmação do agente.
- Altere um identificador de empresa ou identificador do agente para o agente.
- Altere o código do produto do agente. Para obter mais informações, consulte ("Alterando o Código do Produto" na página 1190).

É possível concluir as ações a seguir após confirmar o agente:

- Incluir novos atributos em grupos de atributos existentes.
- Incluir novos grupos de atributos.
- Reordenar novos atributos.
- Organizar novos grupos de atributos usando os itens do navegador.
- Criar novos tipos de subnós.
- Incluir novas consultas.
- Incluir novas situações.
- Incluir novas áreas de trabalho.

Configurando um novo número da versão para o seu agente

Para salvar alterações em um agente confirmado, deve-se inserir um novo número da versão.

Procedimento

1. Abra a janela **Agent Editor**, página **Informações do Agente**.
2. Insira uma versão, caminho de correção ou nível da correção que seja mais alto do que o nível atual após o prompt da Versão.
3. Efetua edições no seu agente.

   Dica: Se você confirmar um agente e esquecer de mudar a versão do agente, será solicitado que forneça a nova versão ao salvar qualquer uma de suas alterações.

Alterando o Código do Produto

Se você alterar o código do produto, você terá um agente que é incompatível com qualquer versão anterior do agente. Todos os registros de ações de confirmação anteriores serão perdidas e você estará desenvolvendo um novo agente.

Quaisquer arquivos, situações, comandos Executar Ação ou áreas de trabalho que foram exportados do IBM Tivoli Monitoring e importados no agente serão excluídos do agente.

Se você tentar mudar o código do produto de um agente que foi confirmado, o Agent Builder exibirá um aviso e perguntará se você deseja continuar.

Ao clicar em **Sim** na janela **Código de Produto do Agente**, você será avisado de que o conteúdo dos arquivos de suporte do agente não são mais válidos. Também será avisado que os arquivos serão removidos na próxima vez que o agente for salvo.

Editando as propriedades da origem de dados e do atributo

Quando você inclui origens de dados em seu agente, o Agent Builder cria conjuntos de dados correspondentes. É possível editar os conjuntos de dados e atributos neles para fornecer as informações de monitoramento necessárias.

Procedimento

Para editar ou remover informações de um conjunto de dados (grupo de atributos):

1. Na área **Conteúdo do Agente** da página **Informações do Agente**, clique em **Origens de Dados**.
   A página **Definição de Origem de Dados** é aberta.
2. Selecione o conjunto de dados (grupo de atributos).

   A área de informações sobre o grupo de atributos da página é atualizada para exibir as propriedades para o conjunto de dados selecionado.

   Nota: Como alternativa, se você estiver na última página do assistente de **Agente**, será possível dar um clique duplo na origem de dados para abrir a janela **Informações do Grupo de Atributos**. Essa janela possui as mesmas informações que a área de informações do grupo de atributos da página **Definição de Origem de Dados**.

   (Tabela 260 na página 1191) descreve as informações de campo que são aplicáveis a todas as origens de dados. Utilize os campos para modificar as propriedades para a origem de dados ou o atributo selecionado.

Tabela 260. Campos para edição de origens de dados

Nome do Campo	Descrição	Valores e exemplos aceitáveis
Nome do grupo de atributos	Nome da origem de dados conforme exibido no Tivoli Enterprise Portal ou no console do IBM Cloud Application Performance Management	Valores aceitáveis: Sequência descritiva inferior ou igual a 32 caracteres de comprimento. Ela deve ser exclusiva dentro do agente. O primeiro caractere deve ser uma letra e os demais caracteres podem ser letras, números ou sublinhados. Um sublinhado é exibido como um espaço. Não utilize espaços ou caracteres especiais.
Texto de ajuda	O texto de ajuda para a origem de dados	Valores aceitáveis: Sequência até 256 caracteres de comprimento.
Produz uma única linha de dados	A origem de dados retorna 1 linha de dados. Editável em todas as origens de dados amostradas.	Exemplo: Se estiver monitorando a memória do sistema físico, escolha uma única linha. Um sistema normalmente gerencia toda sua memória em um único conjunto; portanto somente uma linha de dados pode ser retornada.

Tabela 260. Campos para edição de origens de dados (continuação)		
Nome do Campo	**Descrição**	**Valores e exemplos aceitáveis**
Pode produzir mais de uma linha de dados	A origem de dados pode retornar qualquer número de linhas de dados. Editável em todas as origens de dados amostradas.	Exemplo: Se estiver monitorando unidades de disco, escolha várias linhas, pois pode haver mais de um disco em um sistema. Para chaves, escolha os atributos que distinguem um disco de outro. Para um disco, o atributo-chave é um número de disco, letra de unidade, rótulo de volume ou qualquer outro apropriado para seu ambiente.
Produzir Eventos	A origem de dados retorna dados baseados em evento, 1 linha de dados por evento.	Exemplo: Uma origem de dados baseado em evento SNMP envia notificações (traps) conforme são cruzados os limites de desempenho. **Nota:** Nem todas as origens de dados podem produzir eventos.
Incluir este grupo de atributos em uma categoria de relatório	A categoria no modelo Cognos gerado ao qual os atributos neste grupo de atributos estão designados.	Selecione a caixa de seleção para colocar o grupo de atributos na subpasta selecionada (Disponibilidade ou Desempenho) na pasta Métricas Chave. Se a caixa de seleção não for selecionada, o grupo de atributos será colocado na pasta **Métricas Estendidas** no modelo de dados Cognos.
Categoria da Métrica	A categoria para a qual os atributos nesse grupo de atributos são designados.	Selecione **Desempenho** ou **Disponibilidade**.

Nota:

a. Os campos **Produzir uma única linha de dados** e **Pode produzir mais de uma linha de dados** não afetam dados para uma origem de dados de eventos.

b. Para obter informações adicionais sobre tipos de dados de amostragem e de evento, consulte (“Tipos de Dados” na página 1213).

c. Para obter informações sobre os campos para uma origem de dados específica, consulte as informações do provedor de dados relevantes em “Definindo e testando origens de dados” na página 1218.

Criando, modificando e excluindo atributos

É possível criar, modificar ou excluir atributos em um conjunto de dados (grupo de atributos).

Para trabalhar com atributos, abra a página **Definição de Origem de Dados**. Para obter mais informações, consulte “A página Definição de Origem de Dados” na página 1187.

Criando Atributos

É possível incluir novos atributos em um conjunto de dados.

Procedimento

1. Clique com o botão direito do mouse na origem de dados e selecione **Incluir Atributo** no menu.

   A página **Informações sobre Atributo** é exibida.

   Nota: A página que é exibida depende da origem de dados para o atributo.
2. Especifique suas escolhas para o novo atributo na página **Informações sobre o Atributo**.

   Consulte "Campos e Opções para Definir Atributos" na página 1195 para obter informações sobre os campos e opções.
3. Para incluir atributos adicionais, selecione **Incluir Atributos Adicionais** e clique em **Avançar**.
4. Quando concluir a inclusão de atributos, clique em **Concluir**.

Copiando Atributos
É possível copiar atributos da página **Definição de Origem de Dados**.

Procedimento

1. No Agent Editor, página **Definição de Origem de Dados**, clique com o botão direito do mouse no atributo que deseja copiar e clique em **Copiar Atributo**.
2. Na janela **Copiar Atributo**, digite o nome do novo atributo no campo **Nome**, e clique em **OK**.

Editando Atributos
É possível editar e mudar informações sobre o atributo usando a página **Definição de Origem de Dados**.

Procedimento

1. Selecione o atributo que deseja editar.

   A área de janela **Informações sobre Atributo** da página é atualizada para mostrar as propriedades para o atributo selecionado.
2. Especifique suas opções para as novas informações sobre o atributo.

   Nota: Na última página do assistente de **Agente** (a página **Definição de Origem de Dados**), é possível dar um clique duplo no atributo para abrir a janela **Informações sobre o Atributo**. Essa janela contém as mesmas informações que a área de janela Informações sobre o Atributo da página **Definição da Origem de Dados**.

Criando Atributos Derivados
Você pode criar um atributo que deriva seu valor de outros atributos em vez de diretamente da origem de dados.

Sobre Esta Tarefa

No atributo derivado, é possível executar operações nos valores dos atributos de origem. Por exemplo, é possível executar operações aritméticas básicas ou atributos numéricos ou concatenação de sequências em atributos de sequência.

A sintaxe de expressão básica que é usada para expressões derivadas contém funções. Essas funções fornecem uma manipulação mais complicada de dados que inclui agregação de curto prazo, conversão de sequência para número inteiro e acesso a propriedades de configuração e variáveis de ambiente. Além disso, um editor ajuda a visualizar a expressão conforme ela está sendo construída.

Procedimento

1. Na página **Definição de Origem de Dados**, clique com o botão direito do mouse na origem de dados e clique em **Incluir Atributo**.
2. Na página **Informações sobre o Atributo**, digite um nome de Atributo e texto de Ajuda.
3. Selecione **Derivado de outros valores de atributos**.

4. No campo **Fórmula**, digite o texto da fórmula ou clique em **Editar** para inserir a fórmula com um editor gráfico.

   Consulte "Operadores e Funções da Fórmula" na página 1206 para obter informações sobre os operadores e as funções que podem ser usados na fórmula.

   Nota: Ao clicar em **Editar**, o Editor de Fórmula se abre. Consulte "Editando Atributos Derivados" na página 1195 para obter informações sobre como editar atributos derivados.
5. Opcional: Selecione ou limpe a caixa de opção **Cálculos específicos internos** para determinar quais dois valores de atributos de amostra são utilizados quando a função é calculada.

   Use esta opção quando sua fórmula usar as funções `rate` ou `delta`. Para obter informações adicionais sobre **Cálculos específicos internos**, consulte "Cálculos específicos de intervalo" na página 1194. Para obter mais informações sobre as funções `rate` e `delta`, consulte "Operadores e Funções da Fórmula" na página 1206.
6. Na área **Tipo de Atributo**, clique no tipo do Atributo
7. Clique em **OK**.

   A página **Definição de Origem de Dados** é exibida novamente com a origem de dados listada nela como antes.
8. Clique em **Concluir**.

   Importante: Se você criar um atributo derivado que referencia outro atributo derivado, certifique-se de que o atributo referenciado tenha sido listado antes do novo atributo. Se um atributo fizer referência a outro atributo derivado subsequente na lista, o agente não conseguirá exibir o valor desse atributo. Se você criar esse atributo, o Agent Builder exibirá um aviso.

Cálculos específicos de intervalo

É possível escolher **Cálculos específicos de intervalo** ao definir um atributo derivado baseado nas funções `rate` ou `delta`.

Você seleciona **Cálculos específicos do Intervalo** na guia **Detalhes do Atributo Derivado** da página **Informações do Atributo**. Para obter mais informações, consulte "Criando Atributos Derivados" na página 1193.

Quando você utilizar a seleção **Cálculos Específicos do Intervalo** é importante entender o conceito de um delta ou a diferença entre valores de atributo. O delta é a diferença entre o valor mais recente do atributo e um valor anterior do atributo. O delta é retornado diretamente pela função `delta` e é utilizado pela função `rate` para calcular um resultado.

A função `delta` ou `rate` deve sempre ter a função `last` como seu único argumento. A função `last` especifica quais valores de um atributo são utilizados para determinar o delta. Se **Cálculos específicos do intervalo** não for selecionado, o valor anterior que é utilizado sempre é o segundo valor mais recente. Se **Cálculos Específicos do Intervalo** for selecionado, o valor anterior que é utilizado é o valor cuja idade (relativo ao valor mais recente) é igual para o intervalo de coleta do solicitante.

Por exemplo, suponha que `CDP_DP_REFRESH_INTERVAL` é configurado para 120 segundos e `atributo A` possui as seguintes valores amostrados:

Hora	**Valor de amostra**
atual	`2800`
2 minutos (120 segundos) atrás	`2600`
4 minutos (240 segundos) atrás	`2499`
6 minutos (360 segundos) atrás	`1500`
8 minutos (480 segundos) atrás	`1200`
10 minutos (600 segundos) atrás	`1000`

Quando **Cálculos Específicos de Intervalo** não é selecionado, a função `delta` sempre retorna `200`, a diferença entre os dois valores mais recentes, `2800 - 2600`. O mesmo valor será retornado, independentemente de se o valor for exibido no Tivoli Enterprise Portal ou no console do IBM Cloud Application Performance Management, usado em uma situação ou em uma coleção histórica.

Quando **Cálculos Específicos de Intervalo** é selecionado, a função `delta` retorna um valor que depende do intervalo de coleta do solicitante.

Se um atributo derivado com a função `delta` é utilizado em uma situação com um intervalo de coleta de 4 minutos, o valor que é retornado pela função `delta` é `301`, a diferença entre o valor mais recente e o valor obtido 4 minutos antes deste,`2800 - 2499`.

Se um atributo derivado com a função `rate` é utilizado em uma situação com um intervalo de coleta de 10 minutos (600 segundos), o valor que é retornado pela função `rate` é 3, a diferença entre o valor mais recente e o valor obtido 10 minutos antes deste, dividido pelo número de segundos no intervalo `(2800 - 1000) / 600`.

Nota: O Tivoli Enterprise Portal não tem nenhum intervalo de coleta inerente, assim, os cálculos de delta e rate para solicitações Tivoli Enterprise Portal sempre usam os valores de atributo mais recente e segundo mais recente, o mesmo resultado se **Cálculos específicos de intervalo** for selecionado ou não.

Para `delta` ou `rate` funcionar corretamente com **Cálculos Específicos de Intervalo**

- O agente deve coletar dados periodicamente no segundo plano, e não on demand (`CDP_DP_THREAD_POOL_SIZE` deve ser maior que 0).
- Cada situação ou intervalo de coleta de histórico no qual o atributo é utilizado deve ser um múltiplo do intervalo de atualização em segundo plano (`CDP_DP_REFRESH_INTERVAL`).
- A contagem (o segundo argumento da última função) deve ser grande suficiente para acomodar o maior intervalo de coleta de uma situação ou coleta de histórico. Por exemplo, se o agente deve suportar 10 minutos (600 segundos) de coleta de histórico e `CDP_DP_REFRESH_INTERVAL` é 120 segundos, a contagem deve ser pelo menos`6, 1+(600 / 120)`. O valor de contagem de 6 assegura que a `last` retorne a amostra mais recente e amostras antigas até 600 segundos.

Nota: Se essas condições não forem atendidas, os valores de entrada provavelmente serão inválidos e um resultado de `0` será retornado.

Editando Atributos Derivados
Usar o Editor de Fórmula para editar atributos derivados.

O Editor de fórmula está disponível na página **Informações sobre o Atributo** para um atributo derivado, conforme descrito em “Criando Atributos Derivados” na página 1193. Para obter informações adicionais sobre o Editor de Fórmula, consulte “Editor de Fórmula” na página 1201

Removendo Atributos
É possível remover um ou vários atributos de um conjunto de dados usando a página **Definição de Origem de Dados**.

Procedimento

- Para remover um atributo ou atributos, clique com o botão direito do mouse no atributo ou nos atributos e selecione **Remover** no menu que é exibido.

  Nota: Não é possível remover um atributo usado por um atributo derivado. Você deve primeiro remover a referência pelo atributo derivado ao atributo que está sendo removido.

Campos e Opções para Definir Atributos
Descrição de informação de campo e opções para página **Informações sobre o atributo** que são aplicáveis a todas as origens de dados

Para obter informações sobre as informações de campo específicas para cada uma das origens de dados, consulte a documentação relevante para cada origem de dados.

Tabela 261. Campos e Opções para Definir Atributos		
Nomes/opções de campo	**Descrição**	**Valores Aceitáveis**
Nome do Atributo	Nome do atributo como ele é exibido no Tivoli Enterprise Portal ou no console do IBM Cloud Application Performance Management	Sequência com os caracteres a seguir: • A-Z • _ • a-z • 0-9 **Nota:** O nome deve começar com A-Z ou a-z. O nome do atributo tem um limite de 63 caracteres e o nome do grupo de atributos tem um limite de 63 caracteres
Texto de ajuda	Texto de ajuda para o atributo	Cadeia
Oculto - pode ser usado somente no atributo derivado	Se selecionado, o atributo não será exibido no Tivoli Enterprise Portal ou no console do IBM Cloud Application Performance Management. Consulte a nota na última linha.	Não aplicável
Derivado de outros valores de atributos	O valor de atributo deve ser calculada a partir de valores de outros atributos	Não aplicável
Atributo-chave	O atributo é uma chave na tabela. Verifique se esse atributo ajuda a definir exclusivamente o objeto que está sendo relatado. Se os dados forem armazenados e resumidos, os atributos-chave serão usados para sintetizar os dados nas tabelas de resumo.	Esta opção não está disponível para atributos Perfmon.
Área de janela **Informações sobre o atributo**	O conteúdo desta guia depende do tipo da origem de dados para a qual este atributo pertence. Consulte informações neste capítulo para a origem de dados que deseja monitorar para obter mais detalhes. Para um atributo derivado, no campo **Fórmula**, insira uma fórmula para calcular o valor do atributo que é baseado em outros atributos ou constantes. É possível digitar a fórmula no campo **Fórmula** ou clicar em **Editar** para usar o editor gráfico de fórmula. Consulte (“Editor de Fórmula” na página 1201).	

Tabela 261. Campos e Opções para Definir Atributos (continuação)		
Nomes/opções de campo	**Descrição**	**Valores Aceitáveis**
Tipo de Atributo	Descreve como o atributo é exibido no Tivoli Enterprise Portal ou no console do IBM Cloud Application Performance Management. Há 3 tipos: • Cadeia • Numérico • Registro de Data e Hora "Tipos de Atributos" na página 1197 contém mais informações sobre os tipos de atributos.	A Tabela 262 na página 1198 contém descrições dos valores do tipo de atributo numérico.
Enumerações	Por ser um valor numérico com escala zero ou valor de sequência.	Inclua suas enumerações na tabela usando o procedimento em ("Especificando uma Enumeração para um Atributo" na página 1200). O nome da enumeração é exibido no Tivoli Enterprise Portal ou no console do IBM Cloud Application Performance Management quando o Valor correspondente é recebido no atributo a partir do agente. Esse atributo é utilizado para um conjunto de valores específicos com significados identificados (por exemplo, 1=UP, 2=DOWN).
Nota: Nos casos em que o atributo é usado em cálculos com outros atributos, há razões para não exibir o valor base. Por exemplo, um número que representa uma contagem de bytes agrupa tão rapidamente que é de pouca utilização.		

Tipos de Atributos
Há três tipos de atributo

O três tipos de atributos são:

- Sequência
- Numérico
- Registro de Data e Hora

Atributos de Sequência

Ao selecionar **Sequência**, use o campo **tamanho máximo** para especificar o comprimento máximo da sequência em bytes. O tamanho padrão é 64 bytes.

Um valor de cadeia que pode conter quaisquer caracteres UTF-8. O tamanho máximo é o comprimento total do buffer alocado para conter a sequência em bytes. Alguns caracteres não ASCII UTF-8 utilizam mais de 1 byte, portanto, você deve considerar este espaço ao selecionar um tamanho máximo. A agregação de dados no warehouse exibe o valor mais recente coletado durante o período.

Numérico

Ao especificar **Numérico**, é possível configurar diversas opções. Consulte Tabela 262 na página 1198, para obter informações sobre essas opções.

Registro de Data e Hora

Um atributo de registro de data e hora é um atributo de sequência com um formato que está em conformidade com o formato `CYYMMDDHHMMSSmmm` (em que C=1 para o século 21). Todos os 16 caracteres devem ser usados para scripts ou clientes de soquete. Quando exibido no Tivoli Enterprise Portal ou no console do IBM Cloud Application Performance Management, um tipo de atributo de registro de data e hora será exibido no formato correto para o código de idioma.

Quando usar o recurso de navegação para WMI, o Agent Builder marca automaticamente os atributos cujo tipo CIM é `CIM_DATETIME` como registros de data e hora. O provedor de dados automaticamente converte os atributos do WMI para esse formato.

Aspectos numéricos de atributos
Descrições de tamanho, propósito, escala e aspectos de intervalo dos atributos.

Ao especificar um atributo numérico, você deve especificar o tamanho, propósito, escala e intervalo do atributo. Para obter mais informações, consulte (Tabela 262 na página 1198).

Tabela 262. Opções de Atributo Numérico

Aspectos numéricos	Opções e campos	Descrição
Tamanho	**32 bits** **64 bits**	O valor de números de 32 bits pode variar de `-2147483648` a `2147483647` (aproximadamente `-2,000,000,000` a `2,000,000,000`). O valor de números de 64 bits pode variar de `-9223372036854775808` a `9223372036854775807` (aproximadamente $-9x10^{18}$ a $9x10^{18}$)

Tabela 262. Opções de Atributo Numérico (continuação)		
Aspectos numéricos	**Opções e campos**	**Descrição**
Objetivo	**Calibrador**	Os valores de número inteiro em que os valores brutos retornados são maiores ou menores que os valores anteriores. Os valores negativos são suportados. Esse tipo é o tipo padrão para inteiros. A agregação de dados no armazém produz valores mínimo, máximo e médio.
	Contador	Um valor de número inteiro positivo que contém valores brutos que geralmente aumentam com o tempo. A agregação de dados no armazém exibe os valores total, alto, baixo e delta mais recente. No exemplo a seguir de cálculos baseados em Delta, os valores de dados detalhados em uma hora são 9, 15, 12, 20, 22 e processamento baseado delta possuem as regras a seguir: • Se o valor atual for maior ou igual ao valor anterior, a saída será igual ao valor anterior menos o valor atual • Se o valor atual for menor que o valor anterior, a saída será igual ao valor atual • Como 15 é maior que 9, a saída será igual a 6 • Como 12 é menor que 15, a saída será igual a 12 • Como 20 é maior que 12, a saída será igual a 8 • Como 22 é maior que 20, a saída será igual a 2 • O valor TOT_ é 28, que é o total das saídas • O valor LOW_ é 2, que é o menor valor das saídas • O valor HI_ é 12, que é o maior valor das saídas
	Propriedade	Uma propriedade do objeto que não é alterada com frequência. A agregação de dados no warehouse exibe o valor mais recente coletado durante o período.
	Delta	Um valor de número inteiro que representa a diferença entre o valor atual e o valor anterior para este atributo. Como esse atributo é representado como um calibre no armazém, a agregação de dados no armazém produz valores mínimo, máximo e médio.
	Alteração de porcentagem	Um valor inteiro que representa a porcentagem de alteração entre o valor atual e o valor anterior. Esse tipo é calculado como: `((novo -antigo)*100)/antigo`. Como esse tipo é representado como um calibre no warehouse, a agregação de dados no warehouse produz valores mínimo, máximo e médio.
	Taxa de alteração	Um valor de número inteiro que representa a diferença entre o valor atual e o valor anterior dividido pelo número de segundos entre as amostras. Ele converte um valor (como bytes) no valor por segundo (bytes por segundo). Como esse tipo é representado como um calibre no warehouse, a agregação de dados no warehouse produz valores mínimo, máximo e médio.

Tabela 262. Opções de Atributo Numérico (continuação)		
Aspectos numéricos	**Opções e campos**	**Descrição**
Escala	**Ajuste decimal**	Escala determina quantas casas decimais possui o número. Cada casa decimal divide o intervalo citado anteriormente por um fator 10. Por exemplo, um ajuste decimal de 2 mostra duas casas decimais e, em um número de 32 bits, o intervalo permitido torna-se -21474836.48 a 21474836.47. Quando um ajuste decimal diferente de zero é especificado, o número é manipulado internamente como um número de ponto flutuante. Portanto, a precisão de números maiores de 64 bits pode ser reduzida.
Intervalo	**Mínimo** **Maximum**	Intervalo fornece o intervalo esperado do valor. Se nenhum intervalo mínimo ou máximo for fornecido, os valores máximos descritos anteriormente serão usados. O intervalo é usado para produzir uma visualização inicial mais útil em algumas visualizações gráficas da área de trabalho do Tivoli Monitoring.

Especificando uma Enumeração para um Atributo
Especifique uma enumeração de valor usando a página **Informações do Atributo**.

Sobre Esta Tarefa
Especificar uma enumeração para um atributo envolve um procedimento curto. Quando for encontrado um valor que tenha uma enumeração definida, o nome da enumeração será exibido no Tivoli Enterprise Portal ou no console do IBM Cloud Application Performance Management em vez do valor.

Procedimento

1. Na na área **Tipo de Atributo** da página **Informações sobre o Atributo**, clique em **Numérico**.
2. Na área **Enumerações**, clique em uma enumeração e depois em **Incluir**.
   A janela **Definition de Enumeração** é exibida.
3. Digite o nome e valor da enumeração nos campos na janela.
4. Clique em **OK**.
   Será possível, então, incluir mais enumerações.

Especificando gravidade para um atributo usado como um indicador de status
Em um ambiente IBM Cloud Application Performance Management, um painel de resumo deve exibir um status. Deve-se usar um atributo para fornecer o valor de status. Para esse atributo, deve-se especificar valores que denotam a gravidade do status específico.

Sobre Esta Tarefa
O atributo usado para indicação de status deve ser numérico. Selecione este atributo no assistente **Configuração do Painel**; para obter instruções sobre como usar este assistente, consulte “Preparando o agente para Cloud APM” na página 1377.

É possível especificar valores para o atributo que correspondem às gravidades Normal, Aviso e Crítico. Qualquer outro valor denota um status de severidade "Unkown"; também é possível definir explicitamente alguns valores, como "Not defined", e as interfaces com o usuário do status "Unknown" exibidas para esses valores.

Procedimento

1. Selecione o atributo que deseja editar.

A área de janela Informações sobre o atributo da página é atualizada para mostrar as propriedades do atributo selecionado.

2. Na área de janela Informações do atributo, clique na guia **Gravidade**.
3. Selecione a gravidade necessária (Normal, Aviso, Crítico e Não Definido) e clique em **Editar**.
4. Selecione **Intervalo** ou **Número Único**, insira o intervalo de valores ou o valor numérico único e clique em **OK**.
5. Opcional: Se precisar incluir outro valor para a mesma gravidade, por exemplo; 2 e 25 indicam aviso, clique em **Incluir**, selecione a gravidade, insira o valor e clique em **OK**.

Filtrando Grupos de Atributos

É possível criar um filtro para limitar os dados que são retornados de um grupo de atributos que retorna dados de amostragem.

Antes de Iniciar

Se o grupo de atributos já existir, abra a página **Definição de Origem de Dados**. Para obter mais informações, consulte "A página Definição de Origem de Dados" na página 1187.

Se desejar criar um grupo de atributos, siga as etapas em "Definindo origens de dados iniciais" na página 1171e clique em **Avançado** na página de informações da origem de dados iniciais.

Procedimento

1. Use uma das etapas a seguir para começar a criar o filtro:
   - Se você estiver criando um grupo de atributos, clique em **Avançado** na página de informações da origem de dados inicial.
   - Se o grupo de atributos existir, selecione o grupo de atributos na página **Definição de origem de dados** e clique em **Avançado** na página **Definição de origem de dados**.
2. Na página **Propriedades de Origem de Dados Avançadas**, insira uma fórmula de seleção. A fórmula de seleção que inserir deve avaliar para um resultado booleano, true ou false.

   Na página **Propriedades Avançadas da Origem de Dados**, é possível clicar em **Editar** para inserir ou modificar a fórmula usando o Editor de Fórmula. Para obter informações adicionais sobre o Editor de Fórmula, consulte "Editor de Fórmula" na página 1201
3. Quando concluir a inserção da fórmula de seleção de filtro, clique em **OK** até retornar para a página **Definição de Origem de Dados**.

   Quando o filtro é criado, o agente usa o filtro para avaliar cada linha de dados. Quando o filtro for avaliado como *true* para uma linha de dados, os dados serão enviados ao IBM Tivoli Monitoring ou IBM Cloud Application Performance Management. Quando o filtro é avaliado como *false* a linha de dados não é enviada e é descartada.

O que Fazer Depois

É possível validar se o filtro está funcionando conforme planejado, utilizando a função de teste para o grupo de atributos. Para obter informações adicionais sobre o teste do grupo de atributos, consulte "Teste de Grupo de Atributos" na página 1380

Editor de Fórmula

Usar o Editor de fórmula para criar e mudar as fórmulas no Agent Builder.

O Editor de fórmula, que é uma ferramenta gráfica, é exibido quando você executa uma das tarefas a seguir:

1. Criar ou editar atributos derivados, consulte "Criando Atributos Derivados" na página 1193 e "Editando Atributos Derivados" na página 1195
2. Criar grupos de Atributos Filtrados, consulte "Criando um grupo de atributos filtrado" na página 1344
3. Filtrar dados de grupos de atributos, consulte "Filtrando Grupos de Atributos" na página 1201

Atenção:

- Ao criar atributos derivados, a fórmula criada deve resultar em um tipo de dados que corresponda ao tipo do atributo. Por exemplo, se o tipo de atributo derivado for um número, a fórmula criada deve ser avaliada para um resultado numérico.
- Ao criar grupos de atributos filtrados ou ao filtrar dados de grupos de atributos, a fórmula criada deve resultar em um valor booleano, "true" ou "false".

Nota: Nas visualizações a seguir, o Editor de Fórmula é mostrado criando fórmulas para atributos derivados. As visualizações são idênticas quando o Editor de Fórmula é usado com grupos de atributos filtrados ou para filtrar dados de grupos de atributos. As visualizações mostram o título **Editor de Fórmula Derivada** ou **Editor de Fórmula de Filtro** dependendo do uso.

Quando o Editor de fórmula é exibido, a fórmula atual é carregada no editor. Se uma fórmula não existir, é possível inserir uma digitando-a diretamente no espaço de fórmula na janela **Editor de Fórmula**. Como alternativa, é possível clicar em **Inserir** para iniciar a inserção de uma fórmula usando as opções de menu do editor. O editor contém duas visualizações da fórmula na janela padrão e uma opção para uma terceira visualização:

Visualização de componente (padrão)
Os componentes da fórmula editada são mostrados nas áreas **operando** e no campo **Operador**. O operador e seus dois operandos podem ser editados utilizando os menus de seleção.

Visualização de fórmula (padrão)
A fórmula completa está no campo de fórmula na janela. Você pode editar a fórmula digitando nesta caixa.

Visualização de árvore de hierarquia de fórmula (opção)
A árvore de hierarquia de fórmula é exibida selecionando a caixa de opção **Mostrar hierarquia de fórmula**. O estado da caixa de opção é lembrado nas chamadas subsequentes do Editor de Fórmula.

Alterando a visualização de componente do Editor da Fórmula

Mude a visualização de componente no Editor de Fórmula.

Sobre Esta Tarefa

O componente mostrado na visualização de componente pode ser alterado das seguintes formas:

Procedimento

- Mova o cursor no texto da fórmula.
- Selecione um nó diferente na árvore de hierarquia de fórmulas.
- Selecione **Um Nível Acima** ou em um dos botões Editar.

Tipos de Componentes

É possível usar o Editor de Fórmula para editar o componente atual e qualquer operando ou argumento de função desse componente. Alguns componentes podem aparecer diferentemente no Editor de Fórmula quando selecionados.

Componente do Atributo do Editor de Fórmula

Use o componente do atributo no Editor de Fórmula para selecionar e manipular atributos em fórmulas.

Sobre Esta Tarefa

É possível selecionar um atributo a partir de uma lista de atributos para o grupo de atributos na visualização de componente do Editor de Fórmula.

Procedimento

1. Para trabalhar com um atributo específico, selecione esse atributo a partir da lista e clique em **Editar**
   A janela **Editar o Atributo Selecionado** é exibida.

2. É possível manipular o atributo selecionado das maneiras a seguir:
   - É possível substituir o atributo por um número de sequência selecionando **Sequência** ou **Número**. A lista de atributos é substituída por um campo de entrada e o conteúdo não será mais comparado com a lista de nomes de atributos válidos.
   - É possível substituir o atributo por uma função clicando em **Função**. Parênteses são incluídos depois do nome e a lista agora contém nomes de função válidos dos quais escolher.
   - É possível digitar um nome do atributo ao invés de selecionar um. Digitar um nome é útil se você ainda não definiu todos os atributos neste grupo de atributos.
     – Um aviso é exibido se não houver nenhum atributo como nome que foi inserido.
     – Um erro é exibido se caracteres forem inseridos e não puderem fazer parte de um nome de atributo.
     – O botão **OK** é desativado até o aviso ou erro ser corrigido.
   - Os atributos não são filtrados com base no tipo. Se um atributo (ou qualquer valor) do tipo errado for selecionado ou inserido, uma mensagem de aviso será exibida.

Componentes de Literal do Editor de Fórmula
Use os componentes de sequência e número no Editor de Fórmula para manipular literais em fórmulas.

Sobre Esta Tarefa

Um literal é qualquer valor inserido diretamente na fórmula que não vem de um valor de atributo ou de uma função. Um valor literal pode ser uma sequência ou um número.

Procedimento

- É possível substituir uma sequência literal ou número por um atributo clicando em **Atributo**. Um nome de atributo válido deve ser selecionado ou inserido sem aspas.
- É possível substituir uma sequência literal ou número por uma função clicando em **Função**. Parênteses são incluídos depois do nome e a lista de seleção contém nomes de funções válidos para escolher.
  – Um aviso é exibido se um número for inserido onde é esperada uma sequência ou vice-versa.
  – Se **Número** estiver selecionado, um erro será exibido se o conteúdo do campo não for um número. **OK** é desativado até o erro ser corrigido.

Componente de Operador do Editor de Fórmula
Use o componente de operador no Editor de Fórmula para manipular operadores em fórmulas.

Sobre Esta Tarefa

Um componente de operador mostra um operador e seus operandos.

Procedimento

- Na visualização de componente do Editor de Fórmula, selecione o operador a partir da lista **Operador**, entre os dois operandos. O operador (%) multiplica o primeiro operando por 100 e, em seguida, divide pelo segundo operando.
- Selecione o operador (`+ - * / ou %`).
  – A seção **Operando Esquerdo** da página é antes do operador.
  – A seção **Operando Direito** é depois do operador.
  – Operandos simples (atributos e literais) podem ser editados sem ter que alterar o componente selecionado para o operando, conforme descrito em “Componente do Atributo do Editor de Fórmula” na página 1202 e “Componentes de Literal do Editor de Fórmula” na página 1203.

  - Operandos complexos, que consistem em outros operadores ou funções, podem ser editados clicando em **Editar**. Essa ação realça o componente do operando, em vez do operador inteiro.

Componente de expressão condicional do Editor de Fórmula Editor

O componente da expressão condicional mostra uma condição, um valor a ser retornado, se a condição for verdadeira, e um valor a ser retornado, se a condição for falsa.

- A expressão na seção **Condição** deve ser avaliada como verdadeira ou falsa. Os operadores `(==)`, `(!=)`, `(<)`, `(<=)`, `(>)`, `(>=)`, `(&&)`, `(||)`, `(!)` estão disponíveis para formar expressões que retornam verdadeiras ou falsas.
- Operandos simples (atributos e literais) podem ser editados sem ter que alterar o componente selecionado para o operando, conforme descrito em "Componente do Atributo do Editor de Fórmula" na página 1202 e "Componentes de Literal do Editor de Fórmula" na página 1203.
- Os operandos complexos, que consistem em outros operadores ou funções, podem ser editados clicando em Editar. Essa ação realça o componente do operando, em vez da expressão condicional inteira.
- Consulte "Opções comuns do Editor de Fórmula" na página 1204 para obter informações sobre como usar as seguintes opções: **Inserir**, **Remover** , **Até um Nível** e **Editar**.

Conceitos relacionados

"Editor de Fórmula" na página 1201
Usar o Editor de fórmula para criar e mudar as fórmulas no Agent Builder.

Componente de Função do Editor de Fórmula

Use o componente de função no Editor de Fórmula para selecionar e manipular os componentes de função em fórmulas.

Sobre Esta Tarefa

O componente da função mostra a função e seus argumentos.

Procedimento

- Para trabalhar com as funções, selecione **Nome da Função** na lista no Editor de Fórmulas.
  - A descrição da função selecionada é mostrada após a função.
  - Seções de **Argumento da função** são mostradas após o nome da função. O número apropriado de argumentos para a função selecionada são mostrados. Uma descrição específica da função selecionada é mostrada.
  - Argumentos simples (atributos e literais) podem ser editados sem ter que mudar o componente selecionado para o operando, conforme descrito em "Componente do Atributo do Editor de Fórmula" na página 1202 and "Componentes de Literal do Editor de Fórmula" na página 1203.
  - Argumentos complexos, que consistem em operadores ou outras funções, podem ser editados clicando em **Editar**. Essa ação realça o componente do argumento, em vez da função inteira.
- Para funções que usam um número variável de argumentos, inclua argumentos clicando em **Inserir** ou remova os argumentos clicando em **Remover** além das ações descritas em "Opções comuns do Editor de Fórmula" na página 1204.
- Para a função `getenv`, uma propriedade de configuração pode ser escolhida clicando em **Inserir**. Se você selecionar a opção Propriedade de Configuração, a janela **Propriedades de Configuração** é exibida.

Opções comuns do Editor de Fórmula

É possível usar algumas opções em todas as visualizações no Editor de Fórmula

As opções comuns do Editor de Fórmula são:

- **Inserir**

- **Remover**
- **Um Nível Acima**
- **Editar**

Inserir

Inserir insere um operador ou uma função antes do componente. O componente é rebaixado para um dos operandos do operador ou um dos argumentos da função. Por exemplo, se você clicar em **Inserir** antes da função `sqrt(attr2)`, será perguntado o que você deseja inserir e as opções a seguir serão exibidas:

- **Um operador com sqrt(attr2) como um dos operandos do operador**
- **Uma função com sqrt(attr2) como o primeiro argumento da função**
- **Uma expressão condicional com sqrt(attr2) como valores true ou false**

Se você clicar em **Inserir** antes da função `getenv`, será perguntado o que você deseja inserir e as opções a seguir serão exibidas:

- **Propriedade de configuração**: use esta opção para recuperar o valor de uma propriedade de configuração que você configurou para o agente, ou então de qualquer variável de ambiente (por exemplo, `JAVA_HOME`) no host que está executando o agente.
- **Um operador com attr2 como um dos operandos do operador**
- **Uma função com attr2 como o primeiro argumento da função**
- **Uma expressão condicional attr2 como os valores true ou false**

Remover

Remover está disponível somente para operadores e funções, e é o inverso de **Inserir**. Ao clicar em **Remover**, é solicitado o que será substituído o operador ou a função removida. Por exemplo, **Remover** antes da função `sqrt(attr2)` mostra as opções a seguir:

- **O argumento 1 atual, attr2**
- **Uma nova sequência, número ou referência de atributo**

Selecione **Uma nova sequência, número ou referência de atributo** para descartar a árvore inteira após o ponto que está sendo removido e substitua por um novo atributo ou valor literal.

Clique em **O argumento atual** para promover o operando ou argumento selecionado para substituir o operador ou a função removida. É possível clicar em opções subsequentes se houver mais argumentos ou operandos. Quaisquer outros operandos ou argumentos são descartados.

Um Nível Acima

Clique em **Um Nível Acima** para mover um nível acima na árvore.

Editar

Clique em **Editar**, antes de um operando ou argumento complexo, para torná-lo o componente a ser editado.

Clique em **Um Nível Acima** depois de clicar em **Editar** para restaurar o componente atual ao que era antes de você ter clicado em **Editar**.

Editor de Fórmula - Erros da Fórmula

Corrigindo Erros de fórmula no **Editor de Fórmula**

A visualização de componente é diferente quando não há nenhuma fórmula ou a fórmula inserida não pode ser analisada. Ela não exibe uma árvore de fórmula. Em vez disso, exibe uma mensagem de erro.

É possível corrigir uma fórmula com erros na análise digitando o campo da fórmula ou substituindo-a pela nova fórmula clicando em **Inserir**. Neste caso, **Inserir** apresenta as opções a seguir:

- **Um atributo**
- **Uma sequência**
- **Um número**
- **Um operador**
- **Uma expressão condicional**
- **Uma função**

Conceitos relacionados

"Editor de Fórmula" na página 1201

Usar o Editor de fórmula para criar e mudar as fórmulas no Agent Builder.

Operadores e Funções da Fórmula

Uma referência (incluindo exemplos) de operadores de fórmula e funções que são usados no editor de fórmula.

Um valor de atributo derivado é o resultado da avaliação de uma expressão baseada em constantes e outros valores de atributo na mesma origem de dados. A gramática de expressão é a expressão matemática normal - operando operador operando com parênteses utilizados para agrupamento. Os atributos numéricos podem ser combinados com outros atributos numéricos ou constantes usando os operadores matemáticos normais: `+ - * / e %`, que multiplica o **operando à esquerda** por 100 e divide pelo **operando à direita**. Atributos de sequência podem ser combinados com outros atributos de cadeia ou constantes com +. Também é possível usar as funções descritas a seguir. Funções são inseridas no formato: `function_name(argument_1, argument_2, argument_3)`.

Um atributo é representado por seu nome (o mesmo nome que você vê na árvore de informações de **Origens de Dados**). Constantes inteiras são especificadas como números. Constantes de sequência são colocadas entre aspas.

É possível utilizar as seguintes funções em uma fórmula:

abs
Retorna o valor absoluto de um número.

atof
Converte uma sequência em um valor de ponto flutuante

atoi
Converte uma sequência em um valor de número inteiro. Ele opera da mesma maneira que o **C atoi** normal funciona: ele para no primeiro caractere não decimal.

average
Retorna um valor único que é a média de um conjunto de valores. O conjunto de valores é fornecido dos argumentos da função. Vários valores individuais podem ser especificados (por nomes de atributos ou constantes de exemplo), cada um em um argumento separado. Alternativamente a última função pode ser o único argumento para essa função (para calcular a média dos valores mais recentes de um atributo).

Os exemplos desta função em uso são:

```
média (Attr_A, AttrB, Attr_C)
```

```
média (last (Attr_A, 10))
```

limite
Retorna o menor número inteiro que não seja inferior ao argumento.

Por exemplo, onde `attribute_a = 12.4`, `ceiling(attribute_a)` retorna o valor 13. E, onde `attribute_a = -12.4`, `ceiling(attribute_a)` retorna o valor -12.

delta
A diferença entre o valor mais recente de um atributo e um valor coletado anteriormente desse atributo. O único argumento para delta deve ser a função `last`, que obtém os valores atuais e anteriores de um atributo. Um uso normal pode se parecer com:

```
delta (last(OtherAttribute, 2))
```

Para obter informações adicionais sobre valores de atributos da última função usados para calcular o delta, consulte “Cálculos específicos de intervalo” na página 1194. Esta função é aplicável somente para atributos derivados, não para filtros de grupos de atributos.

piso
Retorna o maior número inteiro que não seja superior ao argumento.

Por exemplo, onde `attribute_a = 12.4`, `floor(attribute_a)` retorna o valor 12. E, onde `attribute_a = -12.4`, `floor(attribute_a)` retorna um valor -13.

getenv
Retorna o valor do ambiente fornecido ou da "variável de configuração".

ipAddressToName
Converte um endereço IP em um nome do host. Essa função requer um argumento, uma sequência de endereços IP em representação decimal pontuada. Se o endereço não puder ser resolvido, o endereço IP será retornado.

itoa
Converte um número inteiro em uma cadeia. Essa função é mais útil quando você deseja concatenar um valor numérico em uma cadeia. A sequência derivada + a função somente utiliza dois argumentos de sequência.

last
Retorna uma lista de valores para uso pelas funções `min`, `max`, `average`, `stddev`, `rate` e `delta`. Ele utiliza dois argumentos: o atributo para coletar e o número de valores para utilizar no cálculo. Se o atributo necessário for um valor inteiro em um argumento de sequência, o primeiro argumento pode conter a função `atoi`, como `atoi(numericalStringAttribute)`. O segundo argumento deve ser um número. Ele pode ser codificado permanentemente como uma constante ou pode ser o resultado de uma expressão `atoi(getenv("ENV_VAR"))`. Ele não pode fazer referência a um valor de atributo.

Os exemplos desta função em uso são:

```
média (last (Attr_A, 10))
```

```
last (Attribute_A, ${K01_NUM_COLLECTIONS}))
```

Restrição: É possível usar a função `last` somente uma vez em uma fórmula específica.

matches
Retorna um booleano, true ou false, indicando se uma expressão regular corresponde a um valor. Utiliza dois argumentos, a origem da sequência e uma expressão regular com cujo resultado a sequência é comparada. Essa função é útil para filtrar grupos de atributos.

max
Retorna um valor único que é o máximo de um conjunto de valores. O conjunto de valores é fornecido dos argumentos da função. Vários valores individuais podem ser especificados (por nomes de atributos ou constantes de exemplo), cada um em um argumento separado. Alternativamente a última função pode ser o único argumento para essa função (para calcular o máximo dos valores mais recentes de um atributo).

min
Retorna um valor único que é o mínimo de um conjunto de valores. O conjunto de valores é fornecido dos argumentos da função. Vários valores individuais podem ser especificados (por nomes de atributos ou constantes de exemplo), cada um em um argumento separado. Alternativamente a

última função pode ser o único argumento para essa função (para calcular o mínimo dos valores mais recentes de um atributo).

nameToIpAddress
Converte um nome de host em um endereço IP. Essa função requer um argumento, uma sequência de nomes de host. Se o endereço não puder ser resolvido, então, o nome do host será retornado.

NetWareTimeToTivoliTimestamp
Converte um valor de tempo hexadecimal do Novell NetWare em um registro de data e hora Tivoli Monitoring. Essa função requer um argumento, um valor temporal hexadecimal especial do NetWare. O tipo de atributo é registro de data e hora.

taxa
A taxa de mudança (por segundo) entre o valor mais recente de um atributo e um valor coletado anteriormente desse atributo. O único argumento para taxa deve ser a função `last`, que obtém os valores atuais e anteriores de um atributo. Um uso normal pode se parecer com:

```
rate (last(OtherAttribute, 2))
```

Para obter informações adicionais sobre valores de atributos da última função usados para calcular a taxa, consulte "Cálculos específicos de intervalo" na página 1194. Esta função é aplicável somente para atributos derivados, não para filtros de grupos de atributos.

replaceFirst
Substitui a primeira ocorrência de uma subsequência que corresponde a expressão regular com uma sequência de substituição. Essa função requer três argumentos. Primeiro: a sequência de entrada. Segundo: a expressão regular que é usada para corresponder com uma subsequência na sequência de entrada. Terceiro: a sequência de substituição. Consulte ("Expressões Regulares ICU" na página 1492) para obter detalhes sobre as expressões regulares e os valores de substituição permitidos na sequência de substituição.

replaceAll
Substitui todas as ocorrências de subsequências que correspondem a uma expressão regular com uma sequência de substituição. Essa função requer três argumentos. Primeiro: a sequência de entrada. Segundo: a expressão regular que é usada para corresponder com uma subsequência na sequência de entrada. Terceiro: a sequência de substituição. Consulte ("Expressões Regulares ICU" na página 1492) para obter detalhes sobre as expressões regulares e os valores de substituição permitidos na sequência de substituição.

round
Em termos matemáticos, arredonda o número para o número inteiro mais próximo.

sqrt
Retorna a raiz quadrada de um número

stddev
Retorna um valor único que é o desvio padrão de um conjunto de valores. O conjunto de valores é fornecido dos argumentos da função. Vários valores individuais podem ser especificados (por nomes de atributos ou constantes de exemplo), cada um em um argumento separado. Alternativamente a última função pode ser o único argumento para essa função (para calcular o desvio padrão dos valores mais recentes de um atributo).

StringToTivoliTimestamp
Converte uma sequência de data e hora em um registro de data e hora Tivoli Monitoring. Essa função requer dois argumentos. O primeiro argumento é uma representação de sequência de forma livre do registro de data e hora. O segundo argumento é uma sequência de formato que identifica como analisar a representação de sequência de forma livre de um registro de data e hora. (Tabela 263 na página 1209) descreve os parâmetros de formato válidos. O tipo de atributo é registro de data e hora.

Tabela 263. Parâmetros de formato válidos para StringToTivoliTimestamp			
Símbolo	**Significado**	**Formato**	**Exemplo**
a	Ano	aa aaaa	*96* *1996*
M	Mês **Nota:** Somente as sequências de meses em inglês são suportadas.	M ou MM MMM MMMM	*09* *Set* *Setembro*
d	dia	d dd	*2* *02*
T	Dia da semana **Nota:** Somente sequências de dias da semana em inglês são suportadas.	EE EEE EEEE	*Sa* *Sáb* *Sábado*
h	Hora em AM ou PM (1-12)	hh	*07*
H	Hora no dia (0-23)	HH	*00*
m	Minutos da hora	mm	*04*
s	Segundo no minuto	ss	*05*
S	Milissegundo	S SS SSS	*2* *24* *245*
a	marcador AM ou PM	a ou aa	*am*
Qualquer outro caractere ASCII	ignorar este caractere	- (hífen) (espaço) / (barra) : (dois pontos) * (asterisco) , (vírgula)	

Tabela 264 na página 1210 fornece exemplos de representações em sequência de registros de data e hora e as sequências de formatações que são usadas para analisá-las.

Tabela 264. Exemplos de StringToTivoliTimestamp. Uma listagem de tabela e explicação de alguns exemplos de representações em sequência de registros de data e hora.

Representação de sequência do registro de data e hora	**Sequência de formatação**
96.07.10 às 15:08:56	`aa.MM.dd ** HH:mm:ss`
Qua, Agosto 10, 2010 12:08 pm	`EEE, MMMM dd, aaaa hh:mm a`
Qui 21/01/2010 14:10:33.17	`EEE dd/MM/aaaa HH:mm:ss.SS`

sum
Retorna um valor único que é a soma de um conjunto de valores. O conjunto de valores é fornecido dos argumentos da função. Vários valores individuais podem ser especificados (por nomes de atributos ou constantes de exemplo), cada um em um argumento separado. Alternativamente a última função pode ser o único argumento para essa função (para calcular a soma dos valores mais recentes de um atributo).

TivoliLogTimeToTivoliTimestamp
Converte um registro de data e hora do arquivo de log Tivoli em um registro de data e hora Tivoli Monitoring. Essa função requer um argumento, o registro de data e hora de sequência de um arquivo de log do Tivoli. O tipo de atributo é registro de data e hora.

Converter em token
Um token de uma sequência convertida em token. Essa função requer três argumentos. O primeiro argumento é uma sequência a ser dividida em tokens. O segundo argumento fornece um ou mais caracteres na sequência que separa um token de outro. Qualquer ocorrência de qualquer um dos caracteres desse argumento é usado para identificar e separar tokens no primeiro argumento. O terceiro argumento é o índice do token a ser retornado como um resultado dessa função. O primeiro token é o índice 0, o segundo token é o índice 1, etc. Este argumento também pode ser a sequência LAST para retornar o último token.

UTCtoGMT
Converte a Hora Universal Coordenada em um registro de data e hora Tivoli Monitoring GMT. Essa função requer um argumento, o valor time_t de número inteiro. O tipo de atributo é registro de data e hora.

UTCtoLocalTime
Converte a Hora Universal Coordenada em um registro de data e hora Tivoli Monitoring local. Essa função requer um argumento, o valor time_t de número inteiro. O tipo de atributo é registro de data e hora.

As funções a seguir não utilizam nenhum argumento e retornam um número.

count
Mantém um contador que inicia em 1 na primeira vez em que é chamado e incrementa em 1 a cada momento subsequente que é chamado. Se usá-lo em uma expressão que também use `last`, ele corresponderá o número de elementos armazenados por `last()`, mas somente até `last()` atingir seu máximo. Nesse ponto, `last()` começa a excluir o mais antigo de cada valor novo, ficando assim o mesmo número de valores totais, enquanto `Contagem()` continua aumentando sempre.

cumulativeSum
Retorna a soma dos valores de argumento de eventos duplicados representados por um evento de resumo de controle de fluxo. Ou retorna o argumento se ele for um evento único a partir de uma origem de dados. Ele requer um argumento numérico único. Este função se aplica somente aos grupos de atributos de eventos com `filtragem de evento` e resumo ativados.

eventThreshold
Retorna o valor de limite configurado para o grupo de atributos com o evento gerado. Um número, com três enumerações:

- `SEND_ALL (-3)`
- `SEND_FIRST (-2)`

- SEND_NONE (-1)

  O número entre parênteses é um valor bruto. No entanto, o Agent Builder define as enumerações, portanto, por padrão, a versão do texto fica visível no Tivoli Enterprise Portal ou no console do IBM Cloud Application Performance Management. Se você especificar um limite numérico efetivo e não uma dessas opções predefinidas, esse número é retornado por essa função. O valor é um número inteiro > 0. Este função se aplica somente aos grupos de atributos de eventos com `filtragem de evento` e resumo ativados.

isSummaryEvent
Retorna 0 se for um evento único a partir de uma origem de dados, ou 1 se o evento for um evento de resumo do controle de fluxo. Os valores exibidos são Evento e Evento de Resumo se você usar o atributo padrão para a função. Se criar o atributo manualmente, os valores exibidos são 0 e 1, a menos que você defina os nomes e enumerações. Este função se aplica somente aos grupos de atributos de eventos com `filtragem de evento` e resumo ativados.

occurrenceCount
O número de eventos de correspondência representados por um evento de resumo de controle de fluxo ou 1 se for um evento único de uma origem de dados. (Um evento de resumo de controle de fluxo inclui o primeiro evento). Este função se aplica somente aos grupos de atributos de eventos com `filtragem de evento` e resumo ativados.

summaryInterval
Retorna o intervalo do resumo configurado para o grupo de atributos que gerou o evento, em segundos. Este função se aplica apenas aos grupos de atributos de eventos com `filtragem de evento` e resumo ativados.

Exemplos

exemplos do uso de operadores de fórmulas e funções para criar atributos derivados e filtrados

Exemplo 1 - Atributos Derivados

Se você tiver uma origem de dados que defina o seguinte tipo de atributo:

Nome	Cadeia
xBytes	Numérico
yBytes	Numérico
Virtual_Size	Numérico

É possível definir:

- Um atributo `totalBytes` para ser a soma de `xBytes` e `yBytes`. É possível inserir a fórmula `xBytes + yBytes`.
- Um atributo `yPercent` para ser uma porcentagem do total de bytes, que é `yBytes`, pode ser definido como `yBytes% (xBytes + yBytes)` ou `yBytes% totalBytes`.

Exemplo 2 - Atributos Derivados

Esta fórmula retorna o máximo dos valores coletados recentemente para o atributo `Virtual_Size`. O número de amostras que são coletadas é o valor da variável de configuração, *K4P_COLLECTIONS_PER_HISTORY_INTERVAL* (acessado por meio de `getenv`), convertido para um número (por `atoi`):

```
max(last(Virtual_Size,atoi(getenv("K4P_COLLECTIONS_PER_HISTORY_INTERVAL"))))
```

Exemplo 3 - Atributos Derivados

Esta fórmula retorna a raiz quadrada da soma dos quadrados dos valores de atributo `xBytes` e `yBytes`:

```
sqrt(xBytes * xBytes + yBtyes * yBytes)
```

Exemplo 4 - Atributos Derivados

Esta fórmula retorna a média do atributo `xBytes` a partir das 20 amostras mais recentes do grupo de atributos. Se menos de 20 amostras forem coletadas desde que o agente foi iniciado, ela retornará a média do atributo `xBytes` de todas as amostras:

```
average(last(xBytes,20))
```

Exemplo 5 - Atributos Filtrados

Você possui uma origem de dados que retorna:

```
Nome  Tipo Tam. Usado Livre
Memória MEM   8   4   4
Disk1  DISK  300  200  100
Disk2  DISK  500  100  400
```

Você está interessado somente no uso do disco. A solução é criar um filtro para limitar os dados que são retornados. Para limitar os dados retornados, crie um filtro simples que retorna um booleano, valor, true ou false, como segue

Filtro de Disco:

```
Type=="DISK"
```

Agora, quando o filtro `Type=="DISK"` é true, o grupo de atributos retorna somente dados de uso do disco, por exemplo:

```
Nome  Tipo Tam. Usado Livre
Disk1  DISK  300  200  100
Disk2  DISK  500  100  400
```

Exemplo 6 - Atributos Filtrados

Você possui uma origem de dados que retorna:

```
Nome   Tamnho Usado Livre
Memória  8   4   4
Disk1  300  200  100
Disk2  500  100  400
```

Os dados retornados são semelhantes ao exemplo anterior, no entanto, não há atributo Type presente neste momento. Aqui é possível usar a função matches para localizar quaisquer linhas de dados com um valor de atributo de nome que corresponda a `"Disk"` seguido por um número.

Filtro de Disco:

```
matches(Name, "Disk[0-9]*")
```

Agora, quando o filtro corresponde a sequência `"Disk"` seguida por um número no atributo `Name`, somente as linhas de dados de uso do disco são retornadas:

```
Nome   Tamnho Usado Livre
Disk1  300  200  100
Disk2  500  100  400
```

Especificando Sistemas Operacionais

Quando você define origens de dados que não estão disponíveis em todos os sistemas operacionais que o agente suporta, deve especificar os sistemas operacionais em que a origens de dados é executada.

Sobre Esta Tarefa

Por padrão, a origem de dados fornece dados em todos os sistemas operacionais que estão definidos no nível do agente, conforme descrito em "Sistemas Operacionais Padrão" na página 1174. É possível alterar os sistemas operacionais para cada origem de dados.

Procedimento

1. Para abrir a seção Sistemas Operacionais, clique em **Sistemas Operacionais** na página **Informações da Origem de Dados** ao incluir uma origem de dados.
2. Selecione os sistemas operacionais nos quais a origem de dados deve operar.

   Selecione sistemas operacionais individuais, todos os sistemas operacionais, todos os sistemas operacionais de um tipo específico ou os sistemas operacionais padrão do agente.

Configurando e Ajustando a Coleta de Dados

Quando um agente do Agent Builder é criado, é possível configurar e ajustar sua coleção de dados para conseguir os melhores resultados.

O modo de configurar e ajustar o agente pode ser diferente para os diferentes agentes do Agent Builder e até mesmo entre os grupos de atributos em um único evento. Os agentes do Agent Builder podem incluir dois tipos de dados e suportam dois métodos básicos de coleção de dados para o tipo mais comum de dados.

Tipos de Dados

Um agente coleta dois tipos de dados:

1. A maioria dos grupos de atributos do Tivoli Monitoring representa capturas instantâneas de dados. Alguém solicita os dados e eles são retornados. Agentes utilizam esse tipo de dados para representar configuração, desempenho, status e outras informações em que um conjunto de dados coletados ao mesmo tempo faz sentido. Esses dados são chamados *dados amostrados*.
2. Alguns dados do Tivoli Monitoring representam os eventos. Nesse caso, um evento acontece e o agente deve encaminhar os dados para o Tivoli Monitoring. Exemplos de eventos são Traps SNMP, entradas de Log de Eventos do Windows, e novos registros sendo gravados em um arquivo de log. Para simplicidade, esses tipos de dados são agrupados juntos e referenciados como *dados de evento*.

Dados de Amostra

Quando os dados de amostra são necessários, uma solicitação é enviada para o agente para um grupo de atributos específico. A solicitação pode ser iniciada clicando em uma área de trabalho no Tivoli Enterprise Portal. As outras coisas que podem iniciar uma solicitação são uma situação que está em execução, uma coleta de dados para Warehouse ou uma solicitação SOAP. Quando o agente recebe a solicitação, ele retorna os dados atuais para esse grupo de atributos. As solicitações do Tivoli Enterprise Portal têm como alvo um grupo de atributos específico em um Nome do Sistema Gerenciado (MSN) específico. As situações e as solicitações históricas são mais interessantes, especialmente em um agente que inclui subnós. Quando uma situação precisa de dados para um grupo de atributos em um subnó, o agente recebe uma solicitação com uma lista dos subnós de destino. O agente deve responder com todos os dados para o grupo de atributos solicitado para todos os subnós antes que o Tivoli Monitoring possa trabalhar na próxima solicitação.

A maneira mais direta para um agente satisfazer uma solicitação é coletando dados toda vez que recebe uma solicitação do Tivoli Monitoring. Os agentes do Agent Builder não coletam os dados todas as vezes. Os dados não são coletados todas as vezes porque geralmente demora ou usa recursos para coletar os dados. E, em vários casos, os mesmos dados são solicitados várias vezes em um curto período. Por exemplo, um usuário pode definir várias situações que são executadas no mesmo intervalo em um grupo

de atributos e as situações podem indicar várias condições diferentes. Cada uma dessas situações resulta em uma solicitação para o agente, mas você pode preferir que cada uma das situações veja os mesmos dados. Provavelmente, como cada situação vê os mesmos dados, você receberá resultados mais consistentes e minimizará a demanda para os recursos do sistema pelo agente de monitoramento.

O desenvolvedor do agente pode configurar os agentes para otimizarem a coleção de dados, escolhendo executar a coleção em um dos dois modos a seguir:

1. **Coleção On Demand**: O agente coleta os dados quando recebe uma solicitação e retorna esses dados.
2. **Coleção Planejada**: O agente executa a coleção de dados em segundo plano nos intervalos planejados e retorna os dados mais recentemente coletados quando recebe uma solicitação.

O agente usa um cache de curto prazo em ambos os modos. Se uma outra solicitação de dados for recebida enquanto o cache for válido, o agente retornará dados do cache sem coletar novos dados para cada solicitação. O uso de dados do cache resolve o problema causado por diversas solicitações de situações simultâneas (e outros tipos). O período de tempo em que os dados permanecem válidos, o intervalo de coleção planejado, o número de encadeamentos usados para a coleção e se o agente é executado no modo on demand ou planejado são todos definidos pelas variáveis de ambiente. Usando as variáveis de ambiente, é possível sintonizar cada agente para a melhor operação em seu ambiente.

Consulte os exemplos a seguir que ilustram como o agente funciona em ambos os modos:

- Agente 1 (coleção *on-demand*): Um agente simples que coleta uma pequena quantia de dados que normalmente é acessada somente pelas situações ou ocasionalmente no Tivoli Enterprise Portal. A coleção de dados é razoavelmente rápida, mas pode usar recursos de cálculo e de rede. Esse agente é normalmente definido para executar on demand. Se nenhuma situação estiver em execução ou ninguém clicar no Tivoli Enterprise Portal, o agente não fará nada. Quando os dados são necessários, eles são coletados e retornados. Os dados são colocados no cache de curto prazo para que solicitações adicionais quase ao mesmo tempo retornem os mesmos dados. Esse tipo de coleção provavelmente é a maneira mais eficiente para que esse agente seja executado porque coleta os dados somente quando alguém realmente precisar.
- O Agente 2 (coleção *planejada*): Um agente complexo que inclui os subnós e coleta os dados de diversas cópias do recurso monitorado. Várias cópias do recurso podem ser gerenciadas por um agente. É normal executar situações nos dados em uma base relativamente frequente para monitorar o status e desempenho do recurso monitorado. Esse agente é definido para executar uma coleção *planejada*. Um motivo para executar uma coleção *planejada* é a maneira como as situações são avaliadas pelos agentes do Tivoli Monitoring. Como as situações estão sendo executadas nos grupos de atributos nos subnós, o agente recebe uma solicitação para os dados de todos os subnós simultaneamente. O agente não pode responder a outras solicitações até que todos os dados sejam retornados para uma situação. Se o agente coletou todos os dados quando a solicitação chegou, o agente congelaria quando você clicasse em uma de suas áreas de trabalho no Tivoli Enterprise Portal. Para evitar o congelamento do agente, o construtor do agente define automaticamente todos os agentes de subnó para execução como coleção planejada. O desenvolvedor de agentes ajusta o número de encadeamentos e o intervalo de atualização para coletar os dados em um intervalo razoável para o tipo de dados. Por exemplo, o intervalo de atualização pode ser uma vez por minuto ou uma vez a cada 5 minutos.

Variáveis de ambiente

Um agente determina qual modo usar e como a coleção de dados planejados é executada com base nos valores de um conjunto de variáveis de ambiente. Essas variáveis de ambiente podem ser configuradas na definição do agente no painel **Variáveis de Ambiente**. Cada variável de ambiente é listada no menu juntamente com os valores padrão. As variáveis de ambiente também podem ser configuradas ou modificadas para um agente instalado editando o arquivo de ambiente (`env`) do agente no Windows ou o arquivo de inicialização (`ini`)no UNIX. As variáveis de ambiente que controlam as coleções de dados para grupos de atributos de amostragem são:

- `CDP_DP_CACHE_TTL=<período de validade para os dados em cache - valor padrão 55 segundos>`
- `CDP_DP_THREAD_POOL_SIZE=<número de encadeamentos a serem usados para coleção simultânea - valor padrão 15 para agentes do subnó>`

- CDP_DP_REFRESH_INTERVAL=<número de segundos entre as coleções - valor padrão 60 segundos para agentes do subnó>
- CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT=<quantia de tempo de espera por novos dados após a expiração do período de validade - valor padrão 5 segundos>

Dessas variáveis, as mais importantes são CDP_DP_CACHE_TTL, CDP_DP_REFRESH_INTERVAL e CDP_DP_THREAD_POOL_SIZE.

Se o CDP_DP_THREAD_POOL_SIZE tiver um valor maior ou igual a 1 ou o agente incluir os subnós, o agente vai operar no modo de coleção *planejada*. Se CDP_DP_THREAD_POOL_SIZE não estiver configurado ou for 0, o agente será executado no modo de coleção *on-demand*.

Se o agente estiver em execução no modo *planejado*, o coletará automaticamente todos os grupos de atributo a cada CDP_DP_REFRESH_INTERVAL segundos. Ele usa um conjunto de encadeamentos secundários para executar a coleção. O número de encadeamentos é configurado usando CDP_DP_THREAD_POOL_SIZE. O valor correto para o CDP_DP_THREAD_POOL_SIZE varia com base naquilo que o agente está fazendo. Exemplo:

- Se o agente estiver coletando dados dos sistemas remotos usando o SNMP, é melhor ter CDP_DP_THREAD_POOL_SIZE semelhante ao número de sistema remotos monitorados. Ao configurar o tamanho do conjunto semelhante ao número de sistemas remotos monitorados, o agente coleta dados em paralelo, mas limita o carregamento simultâneo nos sistemas remotos. Os daemons SNMP tendem a descartar solicitações quando eles estão ocupados. Descartar as solicitações força o agente em um modo de nova tentativa e encerra consumindo mais tempo e mais recursos para coletar os dados.
- Se o agente incluir inúmeros grupos de atributos que demoram para ser coletados, use encadeamentos suficientes para que as coleções de dados longas possam ser executadas em paralelo. Provavelmente, você pode incluir mais alguns para o restante dos grupos de atributos. Use os encadeamentos dessa maneira se o recurso de destino puder manipulá-lo. Exemplos de quando os grupos de atributos podem demorar um longo tempo para serem coletados, se o script for executado por um longo tempo ou uma consulta JDBC demorar um longo tempo.

A execução de um agente com um conjunto de encadeamentos maior faz com que o agente use mais memória (principalmente para a pilha que é alocada para cada encadeamento). No entanto, ele não aumenta o uso do processador do processo ou aumenta o tamanho do conjunto de trabalhos real do processo de forma perceptível. O agente é mais eficiente com o tamanho correto do conjunto de encadeamentos para a carga de trabalho. O tamanho do conjunto de encadeamentos pode ser sintonizado para fornecer o comportamento desejado para um determinado agente em um determinado ambiente.

Quando os dados são coletados, eles são colocados no cache interno. Esse cache é usado para satisfazer solicitações adicionais até que novos dados sejam coletados. O período de validade para o cache é controlado por CDP_DP_CACHE_TTL. Por padrão, o período de validade é configurado para 55 segundos. Quando um agente está em execução no modo planejado, é melhor configurar o período de validade para o mesmo valor que CDP_DP_REFRESH_INTERVAL. Configure-o ligeiramente maior, se a coleção de dados puder levar um longo tempo. Ao configurar o período de validade dessa maneira, os dados são considerados válidos até sua próxima coleção planejada.

A variável final é CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT. Essa variável entra em ação somente quando CDP_DP_CACHE_TTL expira antes que novos dados sejam coletados. Quando o cache expira antes que novos dados sejam coletados, o agente planeja uma outra coleção para os dados imediatamente. Ele aguarda, então, que essa coleção seja concluída até CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT segundos. Se a nova coleção for concluída, o cache será atualizado e os dados novos serão retornados. Se a nova coleção não for concluída, os dados existentes serão retornados. O agente não limpa o cache quando CDP_DP_CACHE_TTL é concluído para evitar um problema encontrado com o Universal Agent. O Universal Agent sempre limpa seu cache de dados quando o período de validade termina. Se o Universal Agent limpa seu cache de dados antes de a próxima coleção ser concluída, ele tem um cache vazio para esse grupo de atributos e não retorna dados até que a coleção seja concluída. Não retornar dados torna-se um problema quando as situações estão em execução. Qualquer situação executada após a limpeza do cache, mas antes de a próxima coleção ser

concluída, não vê dados e quaisquer situações que disparam são limpas. O resultado é de inundações de eventos que são disparados e limpos simplesmente porque a coleção de dados está um pouco lenta. Os agentes do Agent Builder não causam esse problema. Se os dados 'antigos' fazem uma situação disparar, geralmente os mesmos dados deixam essa situação no mesmo estado. Após a próxima coleção ser concluída, a situação obtém os novos dados e dispara ou limpa com base em dados válidos.

Grupos de atributos

Os agentes do Agent Builder incluem dois grupos de atributos que você pode usar para inspecionar a operação da coleção de dados e ajustar o agente para o seu ambiente. Os grupos de atributos são Status do Objeto de Desempenho e Status do Conjunto de Encadeamentos. Quando esses grupos de atributos são usados para sintonizar o desempenho da coleção de dados, os dados mais úteis são:

- `Status do Objeto de Desempenho`, atributo `Duração Média da Coleta`. Esse atributo mostra quanto tempo cada grupo de atributo está demorando para coletar dados. Geralmente, uma pequena porcentagem dos grupos de atributos em um agente representa a maioria do uso de processador ou o tempo usado pelo agente. Talvez seja possível otimizar a coleção para um ou mais desses grupos de atributos. Ou você pode modificar o intervalo de coleção para um ou mais grupos, se não precisar que alguns dados estejam tão atualizados quanto outros dados. Para obter mais informações, consulte (“Exemplos e Ajuste Avançado” na página 1217).
- `Status do Objeto de Desempenho`, atributo `Intervalos Ignorados`. Esse atributo mostra quantas vezes o agente tentou planejar uma nova coleção para o grupo de atributos e constatou que a coleção anterior ainda estava na fila esperando para ser executada ou já em execução. Em um agente com comportamento normal, esse valor de atributo é zero para todos os grupos de atributos. Se esse número começa a crescer, você ajusta a coleção de dados incluindo encadeamentos, prolongando o intervalo entre as coleções ou otimizando a coleção.
- `Status do Conjunto de Encadeamentos`, atributo `Média de Encadeamentos Ativos do Conjunto de Encadeamentos`. É possível comparar esse valor com o grupo de atributos de Tamanho do Conjunto de Encadeamentos para ver o quanto o conjunto de encadeamentos está sendo usado adequadamente. Alocar um tamanho de conjunto de encadeamentos de 100 encadeamentos quando o número médio de encadeamentos ativos é 5 é provavelmente somente desperdício de memória.
- `Status do Conjunto de Encadeamentos`, atributos `Média da Espera de Tarefa do Conjunto de Encadeamentos` e `Média do Comprimento de Fila do Conjunto de Armazenamento`. Esses atributos representam o tempo que uma coleção de dados média gasta esperando na fila para ser processada por um encadeamento e o número médio de coleções na fila. Devido à maneira como esses dados são coletados, mesmo um sistema inativo indica que, pelo menos, uma média de uma tarefa está esperando na fila. Um número maior de tarefas em espera ou um tempo de espera médio grande indica que as coleções estão se esgotando. É possível considerar a inclusão de encadeamentos, prolongando o intervalo entre as coleções ou otimizando a coleção para um ou mais grupos de atributos.

Dados do Evento

Os agentes do Agent Builder podem expor vários tipos de dados do evento. Algum comportamento é comum para todos os dados do evento. O agente recebe cada novo evento como uma linha separada de dados. Quando uma linha de dados do evento é recebida, ela é enviada imediatamente ao Tivoli Monitoring para processamento e incluída em um cache interno no agente. Situações e coleção de histórico são executadas pelo Tivoli Monitoring quando cada linha é enviada para o Tivoli Monitoring. O cache é usado para satisfazer solicitações do Tivoli Enterprise Portal ou SOAP para os dados. O agente pode usar o cache para executar a detecção duplicada, filtragem e resumo, se definido para o grupo de atributos. O tamanho do cache de eventos para cada grupo de atributos é configurado pelo `CDP_PURE_EVENT_CACHE_SIZE`. Esse cache contém os `CDP_PURE_EVENT_CACHE_SIZE` eventos mais recentes, com o evento mais recente retornado em primeiro lugar. Há caches separados para cada grupo de atributos do evento. Quando o cache para um grupo de atributos é preenchido, o evento mais antigo é eliminado da lista.

O agente do Agent Builder pode expor eventos para:

- Entradas de Log de Eventos do Windows
- Traps ou Avisos SNMP
- Registros inclusos nos arquivos de log
- Notificações do JMX MBean
- Monitores JMX
- Eventos de um provedor de API Java API ou de um provedor de soquete.
- Grupos de atributos unidos (em que uma das origens de dados é uma origem de dados do evento)

Esses eventos são manipulados do modo mais apropriado para cada uma das origens. Traps e Avisos SNMP, notificações JMX e eventos dos provedores de API Java API e de soquete são recebidos de modo assíncrono e encaminhados ao Tivoli Monitoring imediatamente. Não há necessidade de ajustar esses coletores. O agente assina para receber as entradas de Log de Eventos do Windows do sistema operacional usando a API de Log de Eventos do Windows. Se o agente estiver usando a API de Criação de Log de Eventos mais antiga, ele pesquisará o sistema para novos eventos usando as configurações do conjunto de encadeamentos. Para grupos de atributos unidos nos quais uma das origens de dados é uma origem de dados de evento, não há nenhum ajuste a ser aplicado ao grupo de atributo unido. Embora o grupo de atributos unido se beneficie de algum ajuste aplicado ao grupo de origens de eventos.

O monitoramento de arquivos é mais complicado. O agente deve monitorar a existência dos arquivos e quando novos registros são incluídos nos arquivos. O agente pode ser configurado para monitorar os arquivos usando os padrões para o nome do arquivo ou um nome estático. Como o conjunto de arquivos que corresponde aos padrões pode ser alterado com o tempo, o agente verifica os arquivos novos ou alterados a cada KUMP_DP_FILE_SWITCH_CHECK_INTERVAL segundos. Essa variável de ambiente global controla todo o monitoramento de arquivo em uma instância do agente. Quando o agente determina os arquivos apropriados a serem monitorados, ele precisa determinar quando os arquivos serão alterados. Em sistemas Windows, o agente usa as APIs do Sistema Operacional para receber essas mudanças. O agente é informado quando os arquivos são atualizados e os processa imediatamente. Em sistemas UNIX, o agente verifica as mudanças de arquivo a cada KUMP_DP_EVENT segundos. Essa variável de ambiente global controla todo o monitoramento de arquivo em uma instância do agente. Quando um agente nota que um arquivo foi alterado, ele processa todos os novos dados no arquivo e, então, aguarda a próxima mudança.

Exemplos e Ajuste Avançado

Exemplo

As variáveis de ambiente usadas para ajuste mais avançado são definidas no nível do agente. Configure as variáveis a seguir de uma vez e elas se aplicam a todos os grupos de atributos no agente:

- CDP_DP_CACHE_TTL
- CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT
- KUMP_DP_FILE_SWITCH_CHECK_INTERVAL
- KUMP_DP_EVENT

É possível fazer com que as variáveis a seguir se apliquem aos grupos de atributos individuais. Elas ainda possuem uma configuração global que se aplica a todos os outros grupos de atributos no agente:

- CDP_DP_REFRESH_INTERVAL
- CDP_PURE_EVENT_CACHE_SIZE

Se você definiu um agente para incluir os seis grupos de atributos a seguir:

- EventDataOne
- EventDataTwo
- EventDataThree
- SampledDataOne
- SampledDataTwo

- SampledDataThree

Você poderá configurar as variáveis padrão a seguir:

- `CDP_DP_CACHE_TTL=55`
- `CDP_DP_IMPATIENT_COLLECTOR_TIMEOUT=2`
- `CDP_DP_REFRESH_INTERVAL=60`
- `CDP_PURE_EVENT_CACHE_SIZE=100`

Como resultado, todos os grupos de atributos que contêm dados de amostragem (SampledDataOne, SampledDataTwo e SampledDataThree) serão coletados a cada 60 segundos. Cada um dos grupos de atributos do evento (EventDataOne, EventDataTwo e EventDataThree) armazenará os últimos 100 eventos em seu cache.

Essas configurações podem funcionar perfeitamente, ou pode haver razões pelas quais você precisará controlar as configurações em um nível mais granular. Por exemplo, e se EventDataOne geralmente recebe 10 vezes a quantidade de eventos que EventDataTwo e EventDataThree? Para complicar ainda mais as coisas, há realmente um link entre EventDataOne e EventDataTwo. Quando um evento é recebido para EventDataTwo, há sempre diversos eventos para EventDataOne e os usuários desejam correlacionar esses eventos. Não há uma única configuração correta para o tamanho do cache. Seria bom poder permitir que EventDataOne armazene um número maior de eventos e EventDataTwo armazene um número menor. É possível chegar a esse armazenamento, configurando `CDP_PURE_EVENT_CACHE_SIZE` para o tamanho que faz sentido para a maioria dos grupos de atributos do evento, 100 parece adequado. Em seguida, é possível configurar `CDP_EVENTDATAONE_PURE_EVENT_CACHE_SIZE` para 1000. Dessa maneira, todos os eventos correspondentes estão visíveis no Tivoli Enterprise Portal.

A mesma coisa pode ser feita com `CDP_DP_REFRESH_INTERVAL`. Configure um valor padrão que funciona para o maior número de grupos de atributos no agente. Em seguida, configure `CDP_`*`nome do grupo de atributos`*`_REFRESH_INTERVAL` para os grupos de atributos que precisam ser coletados de maneira diferente. Para otimizar a coleção, configure o padrão `CDP_DP_REFRESH_INTERVAL` para corresponder ao valor `CDP_DP_CACHE_TTL`. `CDP_DP_CACHE_TTL` é um valor global; portanto, se configurado para um valor inferior ao intervalo de atualização, podem ocorrer coleções inesperadas.

Definindo e testando origens de dados

O Agent Builder suporta uma série de provedores de dados. É possível criar origens de dados a partir de cada provedor de dados. O procedimento para criar e testar origens de dados é diferente para cada provedor de dados.

Para a maioria dos provedores de dados, ao criar uma origem de dados, um conjunto de dados (grupo de atributos) será incluído no agente. O conjunto de dados contém as informações que são reunidas por essa origem de dados.

Uma origem de dados com um Processo, serviço do Windows ou provedor de dados do código de retorno do Programa usa o conjunto de dados especial de Disponibilidade. Somente um conjunto de dados de Disponibilidade pode ser criado em um agente. Ele contém as informações reunidas por todas as fontes de dados com um provedor de dados de Processo, Serviço do Windows ou Código de retorno do programa neste agente.

Todas as fontes de dados de log do Windows em um agente ou subnó posicionam as informações do evento em um conjunto de dados Log do evento.

Configurando uma origem de dados para o Cloud APM

Em Cloud APM, é possível usar os dados de todos os conjuntos de dados no painel Detalhes e configurar os limites usando o gerenciador de limite. Se desejar usar as informações a partir de um conjunto de dados no painel de resumo para o agente ou subnó, incluindo o indicador de status, bem como para informações de recurso (nome do serviço, endereço e porta), o conjunto de dados deve produzir somente uma linha.

Para a maioria dos provedores de dados, é possível selecionar **Produz uma linha de dados única** na configuração do conjunto de dados. Se as informações reunidas incluírem mais de uma linha, será possível clicar em **Avançado** para configurar um filtro que assegura que a linha correta seja produzida (para obter instruções, consulte "Filtrando Grupos de Atributos" na página 1201). É possível testar a origem de dados para garantir que as informações reunidas produzam a linha necessária.

Para alguns provedores de dados, o conjunto de dados deve produzir várias linhas. Além disso, o processo, o serviço do Windows e as origens de dados do código de retorno do comando colocam dados em um conjunto de dados de Disponibilidade único, que produz várias linhas. Em tais casos, você deve criar um conjunto de dados filtrado que produza uma linha. Para obter instruções sobre como criar um conjunto de dados filtrado (grupo de atributos), consulte "Criando um grupo de atributos filtrado" na página 1344.

Alguns outros provedores de dados produzem dados do evento; uma linha será incluída para cada novo evento. Não use esses provedores de dados para informações de recurso ou resumo no Cloud APM.

Os provedores de dados a seguir devem produzir um conjunto de dados com várias linhas:

- Processo (usa o conjunto de dados de Disponibilidade)
- Serviço do Windows (usa o conjunto de dados de Disponibilidade)
- Código de retorno do Programa (usa o conjunto de dados de Disponibilidade)
- Para alguns tipos de dados, SNMP e JMX
- Dependendo do aplicativo, Soquete e API Java

Os provedores de dados a seguir produzem dados do evento:

- Evento SNMP
- Arquivo de Log
- Log binário do AIX
- Log de eventos do Windows
- Dependendo do aplicativo, Soquete e API Java

Um dos atributos do conjunto de dados deve fornecer um valor de status. Cloud APM usa esse valor para o indicador de status geral. Se a linha não incluir um atributo que pode ser usado como um indicador de status, você poderá criar um atributo derivado para calcular o status. Deve-se configurar os valores de severidade de status; para obter instruções, consulte "Especificando gravidade para um atributo usado como um indicador de status" na página 1200.

Monitorando um Processo

É possível definir uma origem de dados que monitora um processo ou vários processos que são executados em um servidor. Os processos devem ser executados no mesmo host que o agente. Para cada processo, a origem de dados inclui uma linha no conjunto de dados de Disponibilidade.

Procedimento

1. Na página **Origem de Dados Inicial do Agente** ou na página **Local de Origem de Dados**, clique em **Um Processo** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **Um processo**.
3. Clique em **Avançar**.
4. Na página **Monitor de Processo**, na área **Informações do Processo**, forneça o nome de exibição e o nome do processo. É possível digitar o nome do processo manualmente ou obtê-lo, clicando em **Procurar**. Clicar em **Procurar** mostra uma lista de processos que estão atualmente em execução no sistema local ou em um sistema remoto.

   É possível discriminar melhor os processos, selecionando as opções **Usar Correspondência de Argumento** e **Corresponder Linha de Comandos Completa**. Por exemplo, se diversas instâncias dos

mesmos processos estiverem em execução no sistema, uma instância poderá ser distinta da outra usando essas opções.

*Tabela 265. Campos na página **Monitor de Processo**.* Uma tabela listando os campos na página **Monitor de processo** e suas descrições

Nome do Campo	Descrição	Valores Aceitáveis
Nome de Exibição	Nome descritivo para o componente do aplicativo implementado pelo processo conforme mostrado no Tivoli Enterprise Portal ou no console do IBM Cloud Application Performance Management	Sequência descritiva
Nome do processo	Nome do processo que está sendo monitorado	Nome do arquivo executável válido
Utilizar correspondência de argumentos	Selecione se deseja corresponder nos argumentos do processo.	Ligado ou Desligado
Argumento	A sequência de argumentos na qual corresponder. A correspondência de argumento procura a sequência fornecida como uma subsequência dos argumentos. A correspondência será bem-sucedida se você fornecer qualquer parte dos argumentos como a sequência de entrada.	Cadeia
Corresponder à linha de comandos completa	Especificar o nome inteiro do arquivo executável que poderá incluir o caminho	Ligado ou Desligado
Linha de Comandos	Corresponde à sequência fornecida com relação ao nome do comando qualificado usado para iniciar o processo. Os argumentos de comando não estão incluídos. Completo significa que o caminho para o comando deve ser incluído.	Cadeia
Sistemas operacionais	Selecionar os sistemas operacionais nos quais este processo é executado	Qualquer seleção

5. Se você clicar em **Procurar**, a janela **Navegador de Processo** será aberta. Esta janela contém inicialmente informações detalhadas sobre cada processo no sistema Agent Builder. As informações incluem o ID, o nome do processo e a linha de comandos completa para o processo. Selecione um ou mais processos ou trabalhe com a lista na janela **Navegador de Processos** usando uma ou mais das seguintes ações:
   a) Para classificar a lista de processos, clique no título da coluna.
   b) Para atualizar as informações na janela, clique no ícone **Atualizar** (raio brilhante).
   c) Para procurar processos específicos, clique no ícone **Procurar** (binóculos).

É possível inserir uma frase de procura e selecionar a seção de opções para procurar por identificador de processo, nome e linha de comandos.

d) Para visualizar os processos em um sistema diferente, selecione um sistema definido anteriormente a partir da lista **Nome da Conexão**. Ou clique em **Incluir** para inserir as informações do sistema para um novo sistema.

Para obter mais informações, consulte "Definindo Conexões para Navegação no Processo" na página 1222. É possível carregar processos de mais de um sistema de cada vez, e alternar entre conexões enquanto os processos estiverem sendo carregados para uma ou mais conexões.

Nota: Ao procurar os sistemas remotos, os detalhes da linha de comandos ficam disponíveis somente ao procurar através de um Tivoli Enterprise Portal Server.

No exemplo a seguir, após selecionar `svchost.exe`, isso é mostrado no campo **Nome do Processo** na página **Monitor de Processo** página (Figura 31 na página 1221).

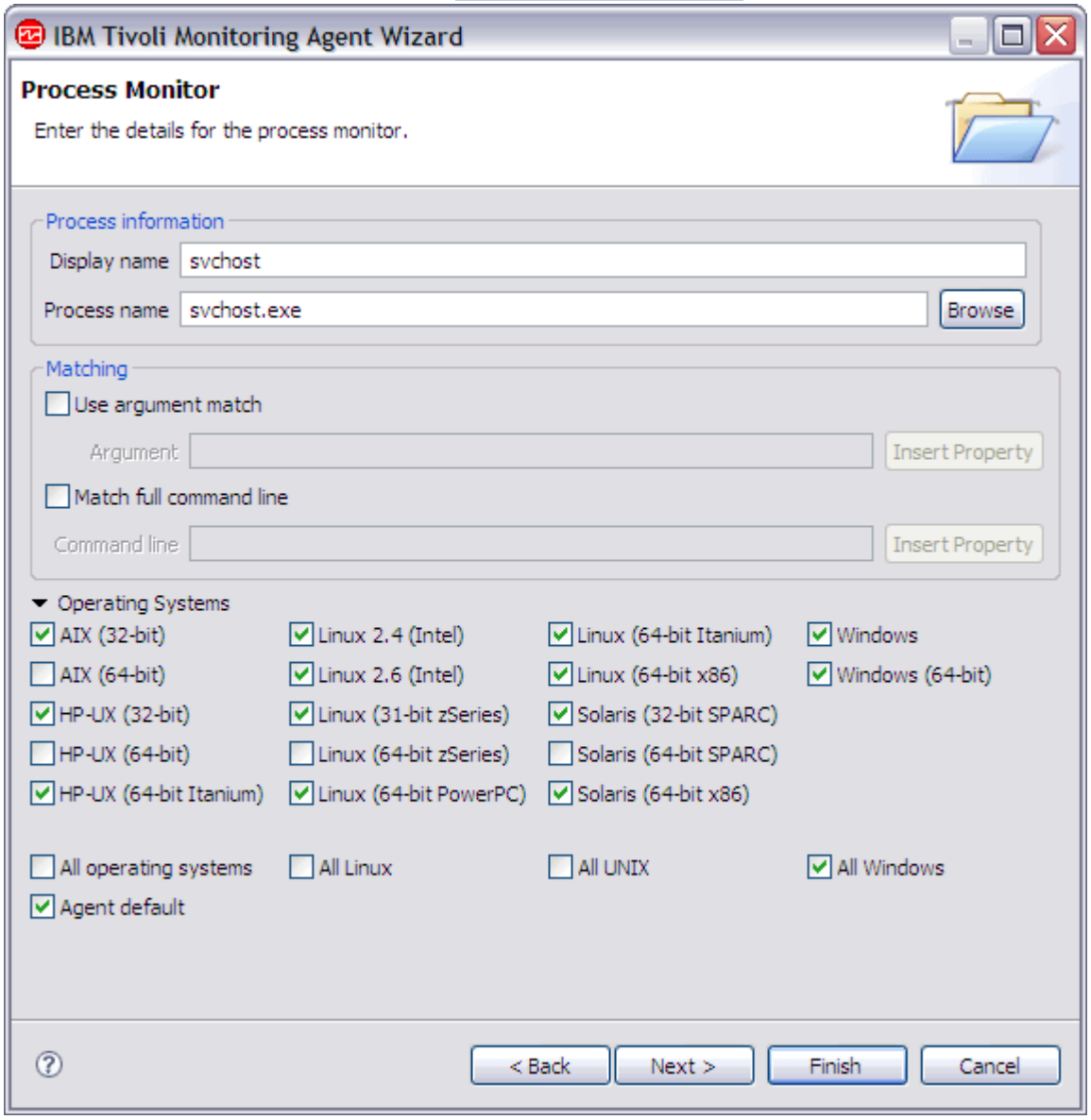


Figura 31. Exemplo da página Monitor de Processo

6. Complete a página **Monitor de Processo** usando as informações em (Tabela 265 na página 1220).

Nota: Se o processo descrito neste monitor for aplicável a somente alguns dos sistemas operacionais nos quais seu aplicativo é executado, você poderá desejar criar um ou mais monitores de processo adicionais com o mesmo nome de exibição para abranger os outros sistemas operacionais. Inclua os monitores de processos um de cada vez. Assegure-se de que o nome de exibição seja o mesmo para

cada monitor, mas que o nome do processo possa ser localizado nos sistemas operacionais selecionados.

7. Execute uma das seguintes etapas:
   - Se estiver usando o assistente de **Agente**, clique em **Avançar**.
   - Clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor.

O que Fazer Depois

Se desejar usar os dados desta origem de dados no painel de resumo para IBM Cloud Application Performance Management, deve-se criar um conjunto de dados filtrado (grupo de atributos) baseado no conjunto de dados Disponibilidade e configurá-lo como fornecendo uma única linha. Use o campo NOME para selecionar a linha para seu processo.

É possível usar o campo Status para status; DOWN significa que o processo não está em execução, enquanto UP significa que ele está em execução. No novo grupo de atributos filtrado, selecione o campo Status e especifique os valores da severidade para ele.

Se várias cópias do processo estiverem em execução, várias linhas com esse nome do processo estarão presentes no conjunto de dados de Disponibilidade, e todos, então, incluirão o status UP. Seu conjunto de dados filtrado deve ser configurados para retornar uma linha, portanto, qualquer uma dessas linhas pode ser retornada, mas o valor de Status será válido em qualquer caso.

Para obter instruções, consulte:

- “Criando um grupo de atributos filtrado” na página 1344
- “Especificando gravidade para um atributo usado como um indicador de status” na página 1200
- “Preparando o agente para Cloud APM” na página 1377

Definindo Conexões para Navegação no Processo

Ao definir uma origem de dados do processo, será possível visualizar e selecionar processos a partir de outros sistemas. No entanto, quando o agente for executado, ele irá monitorar processos executados no mesmo sistema que o agente.

Sobre Esta Tarefa

Você deve ter credenciais para os outros sistemas ou eles deve ser monitorados por um agente do sistema operacional Tivoli Monitoring.

Procedimento

1. Para definir uma conexão, clique em **Incluir** na janela **Navegador de Processo**.

   É possível selecionar um tipo de conexão (Shell Seguro (SSH), Windows ou Tivoli Enterprise Portal Server Managed System) ou selecionar uma conexão existente a ser usada como modelo.

   Para incluir uma conexão do Sistema Gerenciado, é necessário um nome do host do Tivoli Enterprise Server, nome do usuário Tivoli Monitoring e senha. Também é necessário o nome do sistema gerenciado da conexão remota. Quando um sistema gerenciado é selecionado, a tabela lista o processo no sistema remoto.

   Nota: O OS Agent deve estar em execução no sistema que você está tentando procurar. O agente também deve estar conectado a um Tivoli Enterprise Monitoring Server em execução e ao Tivoli Enterprise Portal Server.

   Para incluir o Shell Seguro (SSH) ou as conexões do Windows, é necessário um nome do host, um nome de usuário e uma senha.
2. Quando incluir uma conexão, poderá selecioná-la na lista **Nome da Conexão** na janela **Navegador de Processo**.

   Se todos os campos necessários para estabelecer a conexão não forem salvos (por exemplo, a senha), a janela **Propriedades da Conexão** para essa conexão se abrirá. Insira as informações ausentes. Para

as conexões do Tivoli Enterprise Portal Server Managed System, você deve conectar-se ao Tivoli Enterprise Portal Server antes que seja possível inserir um sistema gerenciado.

3. Insira o nome de usuário e senha e, em seguida, clique no ícone **Atualizar** (raio) a ser conectado antes de selecionar o sistema gerenciado.

O que Fazer Depois

Para excluir uma conexão, selecione-a e clique em **Editar** para abrir a janela **Propriedades da Conexão**. Selecione a caixa de opção **Remover esta Conexão** e clique em **OK**.

Monitorando um Serviço do Windows

É possível definir uma origem de dados que monitora um serviço ou vários serviços que são executados em um sistema Windows. Os serviços devem ser executados no mesmo host que o agente. Para cada serviço, a origem de dados inclui uma linha no conjunto de dados de Disponibilidade.

Procedimento

1. Na página **Origem de Dados Inicial do Agente** ou na página **Local de Origem de Dados**, clique em **Um Processo** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **Um Serviço do Windows**.
3. Clique em **Avançar**.
4. Na página **Monitor de Serviços**, no campo **Nome de Exibição**, digite uma descrição. No campo **Nome do Serviço**, forneça o nome do aplicativo de serviço. É possível digitá-lo manualmente ou clicar em **Procurar** para visualizar uma lista de serviços que estão em execução atualmente no sistema local ou em um sistema remoto.

   Se você clicar em **Procurar**, a janela **Navegador de Serviço** será aberta. Esta janela contém inicialmente informações detalhadas sobre cada serviço no sistema do Agent Builder. As informações incluem o nome do serviço, o nome de exibição, o estado e a descrição para o serviço.

   Nota: Serviços locais não são mostrados quando o Agent Builder não está em execução em um sistema Windows. Um sistema Windows remoto deve ser definido ou selecionado, consulte (“Definindo Conexões para Navegação no Serviço” na página 1224).

   Nota: A descrição do serviço não está disponível ao navegar no Tivoli Enterprise Portal Server ou a partir de um sistema UNIX ou Linux.
5. Selecione um ou mais serviços ou execute uma ou mais das etapas a seguir para trabalhar com a lista na janela **Navegador de Serviço**:
   - Para classificar a lista de serviços, clique no título da coluna.
   - Para atualizar as informações na janela, clique no ícone **Atualizar** (raio brilhante).
   - Para procurar um serviço, clique no ícone **Procurar** (binóculos) para abrir a janela **Procura de Serviço**. É possível procurar por nome do serviço, nome de exibição e descrição.
   - Para visualizar serviços em um sistema diferente, selecione um sistema definidos anteriormente na lista **Nome da Conexão** ou clique em **Incluir** para inserir as informações do sistema. Para obter mais informações, consulte (“Definindo Conexões para Navegação no Serviço” na página 1224). É possível carregar serviços de mais de um sistema de cada vez, e alternar entre conexões enquanto os serviços estiverem sendo carregados para uma ou mais conexões.
6. Após selecionar ou inserir o nome do serviço, conclua uma das etapas a seguir:
   - Se estiver usando o assistente de **Agente**, clique em **Avançar**.
   - Clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor.

O que Fazer Depois

Se desejar usar os dados desta origem de dados no painel de resumo para IBM Cloud Application Performance Management, deve-se criar um conjunto de dados filtrado (grupo de atributos) baseado no

conjunto de dados Disponibilidade e configurá-lo como fornecendo uma única linha. Use o campo NOME para selecionar a linha para seu processo.

No novo grupo de atributos filtrado, selecione o campo Functionality_Test_Status e especifique os valores da severidade para ele.

Para obter instruções, consulte:

- "Criando um grupo de atributos filtrado" na página 1344
- "Especificando gravidade para um atributo usado como um indicador de status" na página 1200
- "Preparando o agente para Cloud APM" na página 1377

Definindo Conexões para Navegação no Serviço
Além de selecionar serviços a partir do sistema no qual o Agent Builder está em execução, é possível selecionar serviços a partir de outros sistemas Windows.

Sobre Esta Tarefa

Para selecionar os serviços a partir de outros sistemas Windows, defina uma conexão para o sistema remoto. Você deve ter credenciais para os sistemas ou eles deve ser monitorados por um agente do sistema operacional Tivoli Monitoring.

Procedimento

1. Para definir uma conexão, clique em **Incluir** na janela **Navegador de Serviço**.

   A janela **Selecionar Tipo de Conexão** é aberta. Para incluir uma conexão do Sistema Gerenciado, é necessário um nome de host do Tivoli Enterprise Server, nome do usuário e senha Tivoli Monitoring, e o nome do sistema gerenciado. Quando um sistema gerenciado é selecionado, a tabela lista o serviço no sistema remoto.

   Nota: O agente do S.O. deve estar em execução no sistema no qual você está tentando procurar e também conectado a um Tivoli Enterprise Monitoring Server e Tivoli Enterprise Portal Server em execução.

   É necessário um nome do host, um nome de usuário e uma senha para incluir uma conexão do Windows.
2. Selecione o tipo de conexão (Windows, ou Tivoli Enterprise Portal Server Managed System) ou selecione uma conexão existente para usar como um modelo.

   A janela **Propriedades de Conexão** é aberta.
3. Conclua as Propriedades da Conexão.
4. Clique em **Concluir**.
5. Quando incluir uma conexão, poderá selecioná-la na lista **Nome da Conexão** na janela **Navegador de Serviço**.

   Se os campos necessários para fazer as conexões não forem salvos (por exemplo, a senha), a janela **Propriedades de Conexão** será aberta e você poderá inserir as informações ausentes.

   a) Para conexões do Tivoli Enterprise Portal Server Managed System, você deve se conectar ao Tivoli Enterprise Portal Server antes que possa inserir um sistema gerenciado. Insira o nome de usuário e senha e, em seguida, clique no ícone **Atualizar** (raio) a ser conectado antes de selecionar o sistema gerenciado.
6. Para excluir uma conexão, siga estas etapas:

   a) Selecione a conexão na janela **Navegador de Serviço**.

   b) Clique em **Editar** para abrir a janela **Propriedades da Conexão**.

   c) Selecione a caixa de opção **Remover esta Conexão**.

   d) Clique em **OK**.

Monitorando Dados a partir do Windows Management Instrumentation (WMI)

É possível definir uma origem de dados para coletar dados do Windows Management Instrumentation (WMI) no sistema no qual o agente é executado ou em um sistema remoto. Uma origem de dados monitora uma classe WMI única e coloca todos os valores dessa classe no conjunto de dados que ela produz. Se a classe fornecer diversas instâncias, o conjunto de dados terá linhas múltiplas; é possível filtrar por nome de instância para garantir que o conjunto de dados tenha uma linha.

Antes de Iniciar

Se seu agente coletar os dados a partir de um sistema remoto usando o Windows Management Instrumentation (WMI), isso requer permissões para acessar os dados WMI no sistema remoto. O agente poderá acessar dados de WMI em um sistema remoto quando você fornecer credenciais de uma conta com permissões para acessar dados de WMI no sistema. A conta do Administrador possui as permissões necessárias. No procedimento a seguir, é possível fornecer as credenciais de Administrador ou as credenciais de outro usuário com as permissões necessárias. Para obter mais informações sobre a criação de uma conta do usuário com permissões para procurar dados WMI, consulte "Criando um Usuário com Permissões do Windows Management Instrumentation (WMI)" na página 1368.

Para coletar métricas por meio das APIs do Windows, o agente deve estar hospedado em um sistema operacional Windows. Administração do registro remoto deve ser ativado nos sistemas remotos.

Procedimento

1. Na página **Origem Inicial de Dados do Agente** ou na página **Local de Origem de Dados**, clique em **Dados de um servidor** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **WMI**.
3. Clique em **Avançar**.
4. Na página **informações do Windows Management Instrumentation (WMI)** , conclua uma das etapas a seguir:
   - Digite um nome para o espaço de nomes do WMI e um nome para a classe do WMI nos campos. Em seguida, acesse a etapa "9" na página 1225
   - Clique em **Procurar** para visualizar todas as classes de WMI no sistema.

     Para procurar um sistema remoto, selecione um sistema da lista (se um estiver definido). Como alternativa, clique em **Incluir** para incluir o nome do host de um sistema Windows. Forneça as credenciais de uma conta do usuário com permissões para acessar dados de WMI no sistema remoto ou forneça credenciais de Administrador para o sistema remoto. A página é atualizada com as informações para o sistema remoto. A procura está disponível somente quando o Agent Builder estiver em execução em um sistema Windows e pode procurar somente em sistemas Windows.
5. Clique no sinal de mais (+) junto a uma classe para expandir a classe e mostrar os atributos.
6. Na lista, selecione a classe com seus atributos associados que deseja especificar e clique em **OK**.

   Nota: Você pode clicar no ícone **Procurar** (binóculos) para localizar sua seleção na lista. Digite uma frase no campo **Procurar frase**; especifique sua preferência clicando nos campos **Procurar por nome**, **Procurar por descrição de classe** ou **Procurar por propriedades de classe** e clique em **OK**. Se localizar o item que está procurando, selecione-o e clique em **OK**.

   A página **Informações de WMI** do assistente é aberta novamente, mostrando as informações da classe de WMI selecionada.
7. Opcional: Você pode testar este grupo de atributos, clicando em **Testar**. Para obter informações adicionais sobre teste, consulte "Testando Grupos de Atributos WMI" na página 1226
8. Opcional: É possível criar um filtro para limitar os dados retornados por esse grupo de atributos clicando em **Avançado**. Para obter informações adicionais sobre filtragem de dados de um grupo de atributos, consulte "Filtrando Grupos de Atributos" na página 1201
9. Clique em **Avançar**.

Nota: Caso tenha digitado o Namespace do WMI e o Nome de Classe do WMI manualmente, você será levado para a página **Informações sobre o Atributo**, em que é possível concluir as informações sobre o atributo. Na página **Informações sobre o Atributo**, é possível selecionar **Incluir atributos adicionais** se deseja incluir mais atributos. Clique em **Concluir** para concluir.

10. Na página **Selecionar Atributos-chave**, selecione os atributos-chave ou indique que esta origem de dados produz somente uma linha de dados. Para obter mais informações, consulte ("Selecionando Atributos-Chaves" na página 1172).
11. Execute uma das seguintes etapas:
    - Se estiver usando o assistente de **Agente**, clique em **Avançar**.
    - Clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor.
12. É possível incluir atributos e fornecer as informações a eles. Para obter mais informações, consulte "Criando Atributos" na página 1192.

    Além dos campos que são aplicáveis a todas as origens de dados (Tabela 261 na página 1196), a página **Informações sobre o Atributo** para a origem de dados WMI possui o campo a seguir:

    Nome da Métrica
    Nome da propriedade da classe que você deseja coletar
13. Se você desejar configurar opções globais para a origem de dados, clique em **Opções Globais**.

    Selecione a caixa de opção **Incluir propriedades de configuração remota do Windows** se desejar incluir esta opção, e clique em **OK**.

    Para obter informações sobre a configuração de conexão remota do Windows para origens de dados Windows, consulte ("Configurando uma conexão remota Windows" na página 1367).

Testando Grupos de Atributos WMI
Se você estiver executando o Agent Builder em um sistema Windows, é possível testar um grupo de atributos WMI dentro do Agent Builder.

Procedimento

1. É possível iniciar o procedimento de Teste das seguintes maneiras:
    - Durante a criação do agente, clique em **Testar** na página **Informações de WMI**.
    - Após a criação do agente, selecione um grupo de atributos no Agent Editor **Definição de Origem de Dados** e clique em **Testar**. Para obter informações adicionais sobre o Agent Editor, consulte "Usando o Agent Editor para modificar o agente" na página 1172.

    Após clicar em **Testar** em uma das duas etapas anteriores, a janela **Teste de WMI** é exibida.
2. Opcional: Antes de iniciar o teste, você pode configurar as variáveis de ambiente e as propriedades de configuração. Para obter mais informações, consulte "Teste de Grupo de Atributos" na página 1380).
3. Clique em **Iniciar Agente**.

    Uma janela indica que o Agente está iniciando.
4. Para simular uma solicitação do ambiente de monitoramento para dados do agente, clique em **Coletar Dados**.

    O agente consulta dados do WMI. A janela **Teste de WMI** coleta e mostra quaisquer dados no cache do agente, desde que ele tenha iniciado por último.
5. Opcional: Clique em **Verificar Resultados**, se os dados retornados não estiverem conforme o esperado.

    A janela **Status de Coleção de Dados** é aberta e mostra informações adicionais sobre os dados. Os dados que são coletados e exibidos pela janela **Status de Coleta de Dados** são descritos em ("Nó de Status do Objeto de Desempenho" na página 1424).
6. Pare o agente, clicando em **Parar Agente**.
7. Clique em **OK** ou **Cancelar** para sair da janela **Teste de WMI**. Clicar em **OK** salva quaisquer mudanças que tiver feito.

Conceitos relacionados

"Testando seu agente no Agent Builder" na página 1380
Depois de usar o Agent Builder para criar um agente, será possível testar o agente no Agent Builder.

Monitorando um Windows Performance Monitor (Perfmon)

É possível definir uma origem de dados para coletar dados a partir do Windows Performance Monitor (Perfmon). Uma origem de dados monitora um objeto Perfmon. Os contadores no objeto são colocados nos atributos no conjunto de dados resultante. Se a classe fornecer diversas instâncias, o conjunto de dados terá linhas múltiplas; é possível filtrar por nome de instância para garantir que o conjunto de dados tenha uma linha.

Procedimento

1. Na página **Origem Inicial de Dados do Agente** ou na página **Local de Origem de Dados**, clique em **Dados de um servidor** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **Perfmon**.
3. Clique em **Avançar**.
4. Na página **Informações sobre Perfmon**, conclua uma das etapas a seguir:
   - Digite o nome do objeto no campo **Nome do Objeto** e clique em **Avançar** para definir o primeiro atributo no grupo de atributos.

     Nota: Se você digitar o nome para o objeto Windows Performance Monitor, ele deve ser o nome em inglês.
   - Clique em **Procurar** para visualizar a lista de objetos Perfmon.

     Quando a janela do Navegador de objetos do Performance Monitor (Perfmon) for inicialmente aberta, a janela será preenchida com as informações do sistema local. Para procurar em um sistema remoto, selecione um sistema a partir da lista (se uma estiver definida) ou clique em **Incluir** para incluir o nome do host de um sistema Windows. Forneça um ID de Administrador e uma senha. A janela é atualizada com as informações para o sistema remoto. A procura está disponível somente quando o Agent Builder estiver em execução em um sistema Windows e pode procurar somente em sistemas Windows. Por exemplo, não será possível incluir o nome do host de um sistema Linux ou Solaris para executar uma procura remota.

     – Ao clicar em um nome de objeto, os contadores disponíveis nesse objeto são mostrados na janela.

       - Para classificar os objetos ou contadores do Windows Performance Monitor, clique no título da coluna.
       - Para atualizar as informações na janela, clique em **Atualizar**.
       - Para procurar objetos ou contadores específicos, clique no ícone **Procurar** (binóculo) para abrir a janela **Procura do Monitor de Desempenho**. É possível procurar nomes do objeto, nomes do contador ou ambos. A operação de procura executa uma correspondência de subsequência e não faz distinção entre maiúsculas e minúsculas.
       - Selecione um objeto e clique em **OK**.
       - O campo **Informações sobre Perfmon** com o nome do objeto selecionado no campo **Nome do Objeto**.
   - Se você deseja configurar opções globais para a origem de dados, clique em **Opções Globais**

     Selecione a caixa de opção **Incluir propriedades de configuração remota do Windows** se desejar incluir esta opção, e clique em **OK**.

     Para obter informações sobre a configuração de conexão remota do Windows para origens de dados Windows, consulte ("Configurando uma conexão remota Windows" na página 1367).
5. Se o objeto Windows Performance Monitor selecionado retornar múltiplas instâncias e você desejar filtrar os resultados com base no nome da instância:

a) Selecione a caixa de opção **Filtrar por Nome da Instância Perfmon** na página **Informações sobre Perfmon**.

b) No campo **Nome da Instância do Perfmon**, digite o nome da instância a ser filtrada ou clique em **Procurar** para listar as instâncias disponíveis.

c) Para navegar um sistema remoto, selecione um a partir da lista ou clique em **Incluir** para incluir o nome do host de um sistema Windows. Após selecionar um host, forneça um ID de Administrador e uma senha. A tabela é atualizada com a lista de instâncias no sistema remoto.

Nota: Também é possível filtrar o grupo de atributos, consulte a etapa "9" na página 1228

6. Se o Objeto Windows Performance Monitor selecionado retornar diversas instâncias e você desejar que o nome da instância seja retornado, selecione **Retornar Nome da Instância** na página **Informações sobre Perfmon**.

   Verificar esta opção inclui um atributo na origem de dados que não é mostrada na lista de atributos. Este atributo contém o nome da instância.

   Nota: Se você procurou o objeto selecionado e esse objeto estiver definido como tendo várias instâncias, esta caixa de opção será selecionada automaticamente.

7. Se você não selecionou a opção para retornar o nome da instância, a página Selecionar Atributos-chave será aberta. Na página Selecionar Atributos-chave, selecione os atributos-chave ou indique que esta origem de dados produz somente uma linha de dados. Para obter mais informações, consulte ("Selecionando Atributos-Chaves" na página 1172).
8. Opcional: Você pode testar este grupo de atributos, clicando em **Testar**. Para obter informações adicionais sobre teste, consulte "Testando Grupos de Atributos Perfmon" na página 1228
9. Opcional: É possível criar um filtro para limitar os dados retornados por esse grupo de atributos clicando em **Avançado**.

   Para obter informações adicionais sobre como filtrar dados de um grupo de atributos, consulte a etapa "Filtrando Grupos de Atributos" na página 1201

   Nota: Também é possível filtrar por nome da instância, consulte "5" na página 1227
10. Execute uma das seguintes etapas:

    - Se você estiver usando o assistente de Novo Agente, clique em **Avançar**.
    - Clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor.

      A página **Definição de Origem de Dados** do **Agent Editor** mostra uma lista que contém o objeto e as informações sobre o objeto.

11. É possível incluir atributos e fornecer as informações a eles. Para obter mais informações, consulte ("Criando Atributos" na página 1192).

    Além dos campos aplicáveis a todas as origens de dados, a página **Informações de Atributo de Perfmon** para a origem de dados possui o campo a seguir:

    Nome da Métrica
    Nome do contador para o objeto específico.

O que Fazer Depois

Para obter informações adicionais sobre a configuração de conexão remota do Windows para origens de dados do Perfmon, consulte "Configurando uma conexão remota Windows" na página 1367.

Testando Grupos de Atributos Perfmon

Se você estiver executando o Agent Builder em um sistema Windows, é possível testar o grupo de atributos Perfmon que você criou.

Procedimento

1. É possível iniciar o procedimento de Teste das seguintes maneiras:

   - Durante a criação do agente, clique em **Testar** na página **Informações sobre Perfmon**.

- Após a criação do agente, selecione um grupo de atributos no Agent Editor **Definição de Origem de Dados** e clique em **Testar**. Para obter informações adicionais sobre o Agent Editor, consulte “Usando o Agent Editor para modificar o agente” na página 1172.

Após clicar em **Testar** em uma das duas etapas anteriores, a janela **Teste de Perfmon** é exibida.

2. Opcional: Antes de iniciar o teste, você pode configurar as variáveis de ambiente e as propriedades de configuração. Para obter mais informações, consulte “Teste de Grupo de Atributos” na página 1380.
3. Clique em **Iniciar Agente**. Uma janela indica que o Agente está iniciando.
4. Para simular uma solicitação a partir do ambiente de monitoramento para dados do agente, clique em **Coletar Dados**.

   O agente consulta dados do Monitor de Desempenho. A janela **Teste de Perfmon** coleta e mostra quaisquer dados no cache do agente, desde a última vez que foi iniciado.

   Nota: Talvez você não veja os dados úteis para todos os atributos até que clique em **Coletar Dados** uma segunda vez. O motivo é que alguns atributos do Monitor de Desempenho retornam valores delta e um valor anterior é necessário para calcular um valor delta.
5. Opcional: Clique em **Verificar Resultados**, se os dados retornados não estiverem conforme o esperado.

   A janela **Status de Coleção de Dados** é aberta e mostra informações adicionais sobre os dados. Os dados coletados e mostrados pela janela **Status de Coleção de Dados** são descritos em “Nó de Status do Objeto de Desempenho” na página 1424
6. Pare o agente, clicando em **Parar Agente**.
7. Clique em **OK** ou **Cancelar** para sair da janela **Teste de Perfmon**. Clicar em **OK** salva quaisquer mudanças que tiver feito.

Conceitos relacionados

“Testando seu agente no Agent Builder” na página 1380
Depois de usar o Agent Builder para criar um agente, será possível testar o agente no Agent Builder.

Dados de monitoramento de um servidor do Protocolo Simples de Gerenciamento de Rede (SNMP)

É possível definir uma origem de dados para monitorar um servidor SNMP. Uma origem de dados monitora todos os dados a partir de um único identificador de objeto (OID) SNMP e um único host. Se selecionar um elemento da árvore do registro do ID do originador em que os objetos estão registrados, um conjunto de dados será criado para cada conjunto distinto de valores escalares ou de tabela. Se um objeto retornar dados escalares, o conjunto de dados terá uma única linha. Se um objeto retornar dados tabulares, o conjunto de dados terá várias linhas.

Sobre Esta Tarefa

Protocolo Simples de Gerenciamento de Rede V1, V2C (observe que a versão é V2C e não somente V2) e V3 são suportados pelos agentes.

Procedimento

1. Na página **Origem Inicial de Dados do Agente** ou na página **Local de Origem de Dados**, clique em **Dados de um servidor** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **SNMP**.
3. Clique em **Avançar**.
4. Na página Informações do Protocolo Simples de Gerenciamento de Rede (SNMP), digite o nome de exibição ou clique em **Procurar** para ver todos os objetos no sistema.

   Depois de definir a origem de dados, é possível incluir um atributo. Os OIDs para esses atributos podem ser longos e difíceis de digitar corretamente. Utilizar a opção Procurar é uma maneira fácil de entrar o OID correto.

Nota: O navegador não procura no sistema ativo, ele lê definições, MIBs (Management Information Bases).

Nota: Clicar no ícone **Atualizar** limpa a versão na memória dos arquivos MIB analisados e reanalisa os arquivos no cache da área de trabalho. O cache está no local a seguir: *workspace_directory* `\.metadata\.plugins\ com.ibm.tivoli.monitoring.agentkit\mibs`

Em que:

workspace_directory
Identifica o diretório da área de trabalho especificado quando você executou o Agent Builder inicialmente, consulte ("Iniciando o Agent Builder" na página 1167).

a) Se o MIB que define o objeto desejado não for carregado, clique em **Gerenciar MIBs Customizados** para abrir o diálogo Gerenciar MIBs Customizados.

b) Clique em **Incluir** para navegar para o arquivo MIB a ser incluído. Para excluir um MIB do cache, selecione-o e clique em **Remover**.

c) Clique em **OK** para atualizar o cache.

Se houver algum erro quando os MIBs forem analisados, o diálogo Gerenciar MIBs Customizados permanece aberto. Este diálogo fornece a oportunidade de incluir ou remover MIBs para eliminar os erros.

Clicar em **Cancelar** retorna o MIB para o estado que estava quando o diálogo foi aberto.

O Agent Builder possui um conjunto de MIBs:

- `hostmib.mib`
- `rfc1213.mib`
- `rfc1243.mib`
- `rfc1253.mib`
- `rfc1271.mib`
- `rfc1286.mib`
- `rfc1289.mib`
- `rfc1315.mib`
- `rfc1316.mib`
- `rfc1381.mib`
- `rfc1382.mib`
- `rfc1443.mib`
- `rfc1461.mib`
- `rfc1471.mib`
- `rfc1493.mib`
- `rfc1512.mib`
- `rfc1513.mib`
- `rfc1516.mib`
- `rfc1525.mib`
- `rfc1573a.mib`
- `rfc1595.mib`
- `rfc1650.mib`
- `rfc1657.mib`
- `rfc1659.mib`
- `rfc1666.mib`
- `rfc1695.mib`

- rfc1747.mib
- rfc1748.mib
- rfc1757.mib
- rfc1903.mib
- rfc1907.mib
- rfc2011.mib
- rfc2021.mib
- rfc2024.mib
- rfc2051.mib
- rfc2127.mib
- rfc2128.mib
- rfc2155.mib
- rfc2206.mib
- rfc2213.mib
- rfc2232.mib
- rfc2233.mib
- rfc2238.mib
- rfc2239.mib
- rfc2320.mib
- rfc3411.mib

Todos esses MIBs são padrão, MIBs definidos pelo IETF. Os MIBs são incluídos porque representam definições comuns que podem ser úteis no monitoramento. Além disso, muitos dos MIBs são necessários para que os MIBs customizados possam resolver os símbolos que importam.

d) Selecione um objeto da lista.

Clique no sinal de mais (+) junto a um objeto para expandir e mostrar os níveis.

e) Na lista, selecione o objeto que deseja especificar e clique em **OK**.

A nova origem de dados é, então, listada na página **Definição de Origem de Dados**.

Nota: Se você selecionar um objeto que define outros objetos (objetos que são aninhados embaixo do primeiro objeto), todos esses objetos se transformam em origens de dados. Se você selecionar um objeto de alto nível, várias origens de dados serão incluídas.

5. Na página **Informações do Protocolo Simples de Gerenciamento de Rede**, selecione os sistemas operacionais.
6. Opcional: É possível testar a origem ou origens de dados clicando em **Testar** na página **Informações do Protocolo Simples de Gerenciamento de Rede**.

   Para obter informações adicionais sobre teste, consulte “Testando Grupos de Atributos SNMP” na página 1233
7. Opcional: É possível criar um filtro para limitar os dados retornados por esse grupo de atributos clicando em **Avançado**. Para obter informações adicionais sobre filtragem de dados de um grupo de atributos, consulte “Filtrando Grupos de Atributos” na página 1201
8. Clique em **Avançar**.
9. Na página **Informações do Atributo**, especifique as informações para o atributo.
10. Execute uma das seguintes etapas:
    - Se você estiver usando o assistente de Novo Agente, clique em **Avançar**.
    - Clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor.

11. Para obter mais informações sobre incluir atributos e fornecer as informações para eles, consulte “Criando Atributos” na página 1192.

    Além de campos que são aplicáveis a todas as origens de dados, a página **Informações do Atributo** para a origem de dados SNMP possui os campos a seguir:

    Nome da Métrica
    Sequência Arbitrária

    Identificador de objeto
    OID completo registrado para o objeto, não incluindo valores de índice

O que Fazer Depois

É possível usar a configuração de tempo de execução do agente para configurar o host monitorado.

Para permitir que o Agent Builder gere tipos de dados de 64 bits e manipule o valor máximo para propriedades MIB não assinadas de 32 bits, consulte “Opções de Análise SNMP MIB” na página 1232.

Erros SNMP MIB
Lidando com erros de SNMP MIBs.

Não é raro encontrar erros durante a inclusão de SNMP MIBs. Clique em **Detalhe>>** na janela **Erro do Agent Builder** para ver qual é o erro do MIB.

Um dos erros mais comuns são definições ausentes que são definidas em outros MIBs. É possível importar vários MIBs simultaneamente para resolver esse problema, ou você pode incluir incrementalmente os MIBs até que todas as definições ausentes sejam resolvidas. O Agent Builder pode usar algumas definições que são resolvidas. Portanto, você pode optar por ignorar um erro que afeta somente a parte do MIB que você não planeja usar. A ordem dos MIBs não importa, pois eles todos são carregados e, em seguida, as referências são resolvidas.

Opções de Análise SNMP MIB
Configure suas preferências para análise do SNMP MIB

Procedimento

1. No Agent Builder, selecione **Janela** > **Preferências** para abrir a janela **Preferências**.
2. Na área de janela de navegação, expanda **IBM Agent Builder**.
3. Clique em **Análise de MIB** para abrir a janela **Análise de MIB**.

   O analisador MIB que é usado pelo Agent Builder usa a gramática que é definida por ASN.1 para analisar os MIBs. Alguns MIBs não seguem a gramática corretamente. O analisador pode afrouxar certas regras para acomodar os erros mais comuns. Ao aliviar essas regras, é possível analisar os MIBs fora de conformidade.

   Permitir que os Tipos Iniciem com Letras Minúsculas
   Permite os tipos que as pessoas gravam em MIBs, tais como valores

   Permite numéricos chamados números
   Permite que os números iniciem com letras maiúsculas

   Permite sublinhado no nome do valor
   Permite caracteres sublinhados

   Permitir que letras comecem com maiúsculas
   Permite valores que iniciam com letras maiúscula.

   Ignorar MIBs duplicados
   Desliga o aviso para módulos MIB duplicados
4. Opcional: Selecionando a caixa de opção **Criar atributos de 64 bits para propriedades MIB não designadas para 32 bits**, o Agent Builder é ativado a gerar tipos de dados de 64 bits para lidar com o valor máximo de propriedades MIB não designadas para 32 bits. Selecionando essa opção não se altera nenhuma definição de campo do agente existente. É necessário navegar para o arquivo MIB para criar novas origens de dados para essas propriedades.

5. Quando você tiver terminado de editar as preferências, clique em **OK**.

Testando Grupos de Atributos SNMP
É possível testar o grupo de atributos SNMP que você criou no Agent Builder.

Procedimento

1. É possível iniciar o procedimento de Teste das seguintes maneiras:
   - Durante a criação do agente, clique em **Testar** na página **Informações do Protocolo Simples de Gerenciamento de Rede**.

     Nota:

     Se o objeto SNMP selecionado contiver mais de um grupo de atributos, você será solicitado a selecionar o grupo de atributos a ser testado.
   - Após a criação do agente, selecione um grupo de atributos na página **Agent Editor Definição de Origem de Dados** e clique em **Testar**. Para obter informações adicionais sobre o Agent Editor, consulte "Usando o Agent Editor para modificar o agente" na página 1172

   Após clicar em **Testar** em uma das duas etapas anteriores, a janela de configurações de Teste SNMP é aberta.
2. Selecione uma conexão existente de **Nome de Conexão** ou clique em **Incluir** e será solicitado que você selecione um tipo de conexão. Como alternativa, selecione uma conexão existente a ser usada como um modelo, usando o **Assistente para Criar Conexão**
3. Depois de selecionar um tipo de conexão ou uma conexão existente, clique em **Avançar** para preencher as propriedades da conexão SNMP. Quando concluir, clique em **Concluir** para retornar para a janela de configurações Teste de SNMP.
4. Opcional: Antes de iniciar o teste, você pode configurar as variáveis de ambiente e as propriedades de configuração. Para obter mais informações, consulte ("Teste de Grupo de Atributos" na página 1380).
5. Clique em **Iniciar Agente**. Uma janela indica que o Agente está iniciando.
6. Para simular uma solicitação a partir do Tivoli Enterprise Portal ou SOAP para dados do agente, clique em **Coletar Dados**. O agente consulta os dados da conexão SNMP configurada.
7. A janela **Testar Configurações** coleta e mostra dados no cache do agente, desde que ele tenha iniciado por último.
8. Opcional: Clique em **Verificar Resultados**, se os dados retornados não estiverem conforme o esperado.

   A janela **Status de Coleção de Dados** é aberta e mostra informações adicionais sobre os dados. Os dados coletados e mostrados pela janela **Status de Coleção de Dados** são descritos em "Nó de Status do Objeto de Desempenho" na página 1424
9. Pare o agente, clicando em **Parar Agente**.
10. Clique em **OK** ou **Cancelar** para sair da janela **Testar Configurações**. Clicar em **OK** salva quaisquer mudanças que tiver feito.

Conceitos relacionados
"Testando seu agente no Agent Builder" na página 1380
Depois de usar o Agent Builder para criar um agente, será possível testar o agente no Agent Builder.

Monitorando eventos a partir de emissores de evento do Simple Network Management Protocol

É possível definir uma origem de dados para coletar dados de eventos de Trap SNMP e de Aviso. Deve-se configurar a porta na configuração de tempo de execução do agente e configurar os servidores para enviar o evento para o host do agente nesta porta. Todos os eventos monitorados são colocados como linhas em um conjunto de dados.

Sobre Esta Tarefa

Protocolo Simples de Gerenciamento de Rede (SNMP) V1, V2C (observe que esse nome de versão é V2C, não somente V2) e V3 são suportadas pelos agentes. Os Traps e Avisos SNMP podem ser recebidos e processados pelo agente. Os dados que são recebidos por esse provedor são passados para o ambiente de monitoramento como eventos.

Para obter mais informações sobre os grupos de atributos para eventos SNMP, consulte ("Grupos de Atributos do Evento SNMP" na página 1451).

Procedimento

1. Na página **Origem Inicial de Dados do Agente** ou na página **Local de Origem de Dados**, clique em **Dados de um servidor** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **Eventos do SNMP**.
3. Clique em **Avançar**.
4. Na janela **Informações de Evento do Protocolo Simples de Gerenciamento de Rede**, execute uma das etapas a seguir:
   - Clique em **Todos os Eventos** para criar um grupo de atributos que envia um evento para qualquer evento SNMP recebido.
   - Clique em **Eventos Genéricos** para criar um grupo de atributos que envia um evento para qualquer evento SNMP genérico recebido, que corresponde a qualquer um dos tipos de evento genérico selecionado.
   - Clique em **Eventos Customizados** para criar um ou mais grupos de atributos que enviam eventos para eventos SNMP específicos da empresa. Clique em **Procurar** para escolher os eventos a serem monitorados.

     Na janela **Simple Network Management Protocol (SNMP) Management Information Base (MIB) Browser**, os eventos na área de janela de seleção são organizados pelo módulo MIB no qual eles foram definidos. Expanda um objeto SNMP para mostrar os eventos nesse módulo MIB. Na lista, clique no objeto que você deseja especificar e clique em **OK**.

     Marque a caixa de seleção **Incluir atributos que mostram as informações definidas no arquivo de configuração de trap** se você tiver um arquivo de configuração de trap que contenha dados estáticos para seus traps. Para obter informações adicionais sobre o arquivo de configuração de trap SNMP, consulte "Configuração de Trap SNMP" na página 1505.

     Selecione a caixa de seleção **Incluir atributo de dados de ligação de variável (VarBind)** se quiser incluir um atributo com todos os dados de ligação de variável (VarBind) recebidos na protocol data unit (PDU) do trap. Para obter informações adicionais sobre este atributo, consulte a definição de atributo ("Grupos de Atributos do Evento SNMP" na página 1451).

     Nota:

     a. O navegador não procura no sistema ativo; ele lê definições e Management Information Bases (MIBs). A lista de MIBs incluídos com o Agent Builder é definida no "Dados de monitoramento de um servidor do Protocolo Simples de Gerenciamento de Rede (SNMP)" na página 1229. Os MIBs carregados por um dos provedores de dados SNMP estão disponíveis em ambos.

     b. Se você selecionar um módulo MIB ou eventos individuais, todos os eventos nesse módulo serão convertidos em origens de dados separadas. Um atributo é incluído para cada uma das variáveis definidas no evento. Se você desejar que todos os eventos para os módulos ou traps selecionados cheguem a uma única origem de eventos, marque a caixa de seleção **Coletar eventos em um único grupo de atributos**. Se você selecionar traps individuais e o sinalizador **Coletar Eventos em um Único Grupo de Atributos** estiver marcado, um atributo será incluído para cada uma das variáveis definidas em cada um dos eventos (as variáveis duplicadas são ignoradas). Se você selecionar um módulo, os atributos variáveis não serão incluídos.

     c. Se você desejar digitar seu próprio filtro, use a seguinte sintaxe:

O valor do elemento OID (identificador de objeto) é usado para determinar quais traps processar para esse grupo de atributos.

- **Correspondência do trap:** O atributo OID do elemento global_snmp_event_settings_for_group pode ser uma lista de tokens delimitada por vírgula. Um único token possui a seguinte sintaxe:

  ```
  [enterpriseOID][-specificType]
  ```

- **Exemplo:** "1.2.3.5.1.4,1.2.3.4.5.6.7.8.9-0" O primeiro token corresponde a qualquer trap com um OID corporativo de 1.2.3.5.1.4. O segundo token corresponde a qualquer trap com um corporativo de 1.2.3.4.5.6.7.8.9 e específico de 0. Como os tokens estão listados juntos em um grupo de atributos, um evento recebido, que corresponde a um dos dois, é processado por esse grupo de atributos.

d. Cada evento que é recebido é processado somente pelo primeiro grupo de atributos que corresponde ao evento recebido. Os grupos de atributos do subnó são processados primeiro e, em seguida, os grupos de atributos base são processados. O desenvolvedor de agente deve garantir que os grupos sejam definidos de maneira que os eventos sejam recebidos no grupo de atributos esperado.

5. Na janela **Informações de Evento SNMP**, selecione a caixa de seleção **Correspondência de Host de Subnó** para corresponder os eventos aos subnós. Se o grupo de atributo do evento SNMP for parte de um subnó, será possível marcar a caixa de seleção **Correspondência de Host do Subnó** para controlar se o evento deve ser proveniente do agente SNMP que é monitorado.

   Por exemplo: Faça um agente monitorar os roteadores, em que cada instância do subnó representa um roteador específico. Você desenvolve um agente para coletar dados de um roteador com o coletor de dados SNMP. Você também define um grupo de atributos para receber eventos SNMP enviados por esse roteador. Cada instância do roteador inclui os mesmos dados definidos para o filtro de eventos. Portanto, você precisa de outra maneira para garantir que eventos de seu roteador sejam mostrados no grupo de atributos para esse roteador.

   Quando a correspondência do host do subnó estiver selecionada, um evento enviado pelo roteador será comparado com o host definido para o coletor de dados do SNMP. Se o host em uso pelo coletor de dados SNMP for o mesmo host que enviou o evento recebido, a instância do subnó processará o evento SNMP. Caso contrário, o evento será transmitido para a próxima instância do subnó. A correspondência de endereço se aplica somente a subnós. Nenhum correspondência de endereço é feita pelos grupos de atributos do evento SNMP no agente de base. Para que a correspondência de endereço funcione, a definição de subnó deverá conter pelo menos um grupo de atributos do SNMP. O host do SNMP usado pelo SNMP para essa instância do subnó é o host usado para correspondência.

   Se a caixa de seleção **Correspondência de Host do Subnó** estiver limpa, suas instâncias de subnó não executarão essa comparação extra. Você deve permitir que o usuário configure um filtro de OID diferente para cada subnó nesse caso. Caso contrário, não precisará incluir grupos de atributos do evento SNMP na definição de subnó.

6. Na janela **Informações de Evento SNMP**, selecione os sistemas operacionais.
7. Opcional: É possível clicar em **Testar** na janela **Informações de Evento SNMP** para iniciar e testar seu agente.

   Para obter mais informações, consulte “Testando Grupos de Atributos de Evento SNMP” na página 1238
8. Opcional:

   Na janela **Informações de Evento SNMP**, clique em **Avançado** para selecionar **Filtragem de Eventos e Opções de Resumo**. Para obter mais informações, consulte “Filtro de eventos e resumo” na página 1408.

   a) Ao concluir a seleção de **Filtragem de Eventos e Opções de Resumo**, retorne à janela **Informações de Evento SNMP**. Se tiver selecionar anteriormente **Eventos Customizados** na janela **Informações de Evento SNMP**, clique em **Avançar**, para selecionar atributos-chave, caso contrário, ignore a próxima etapa.

b) Na página Selecionar atributos-chave, clique em um ou mais atributos-chave para o grupo de atributos, ou clique em **Produz uma única linha de dados**.

9. Clique em **Avançar** ou em **Concluir**, se você estiver usando o assistente de novo agente para salvar o agente e abrir o Agent Editor.
10.

O que Fazer Depois

Para obter informações sobre a inclusão de atributos adicionais, consulte (“Criando Atributos” na página 1192).

Propriedades de Configuração de Eventos SNMP

Certas propriedades de configuração são criadas automaticamente quando um grupo de atributos do Evento SNMP é incluído no agente

Após incluir uma origem de dados, a configuração é exibida na página **Informações de Configuração de Tempo de Execução** do Agent Editor. Por exemplo, Figura 32 na página 1237 mostra as seções de configuração e algumas propriedades de configuração que são criadas automaticamente quando um grupo de atributos de Evento SNMP estiver incluído no agente.

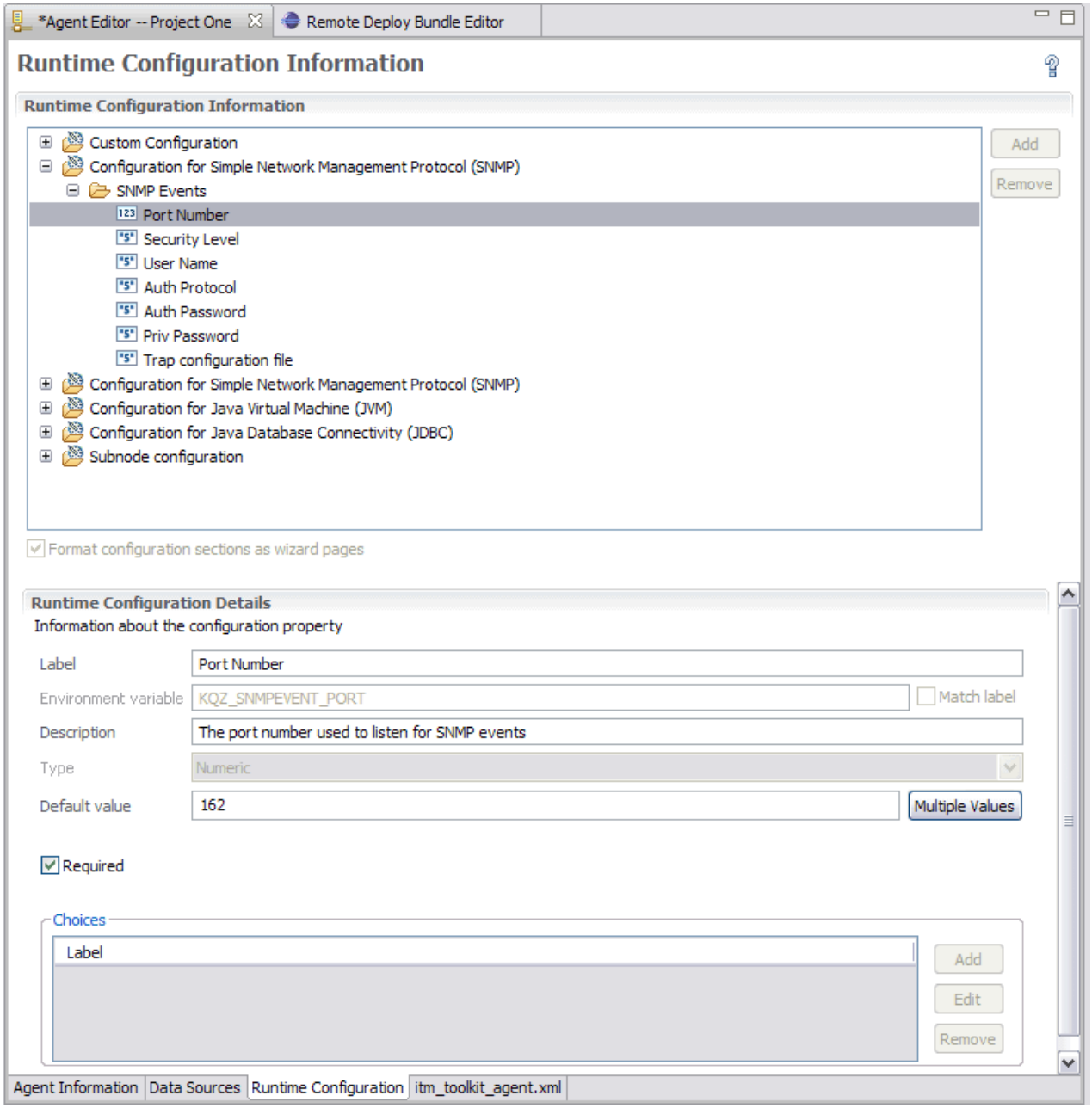


Figura 32. Página Configuração de Tempo de Execução

Os rótulos, descrições e valores padrão de propriedades de configuração predefinidas podem ser alterados, mas os nomes e tipos de variáveis não podem ser alterados. A seção de configuração de Eventos SNMP contém as seguintes propriedades:

Tabela 266. Propriedades de configuração de Eventos SNMP

Nome	Valores Válidos	Obrigatório	Descrição
Número da Porta	Número Inteiro Positivo	Sim	Número da porta necessário usado para atender aos eventos
Nível de Segurança	noAuthNoPriv, authNoPriv, authPriv	Não	Nível de Segurança do SNMP V3
Nome do Usuário	Sequência	Não	Nome de Usuário do SNMP V3

Tabela 266. Propriedades de configuração de Eventos SNMP (continuação)			
Nome	**Valores Válidos**	**Obrigatório**	**Descrição**
Protocolo de Autorização	MD5 ou SHA	Não	Protocolo de Autenticação do SNMP V3
Senha de Autorização	Cadeia	Não	Senha de Autenticação do SNMP V3
Senha Privativa	Cadeia	Não	Senha de Privacidade do SNMP V3
Arquivo de Configuração do Trap	Nome do arquivo que inclui o caminho	Não	Local do Arquivo de Configuração do trap. Se o arquivo não for localizado usando essa propriedade de configuração, será feita uma tentativa de localizar um arquivo `trapcnfg` no diretório bin do agente.

Nenhuma configuração é necessária para os eventos V1 ou V2C. Todos os eventos V1 ou V2C são processados, independentemente da origem ou do nome da comunidade especificado. O único protocolo de privacidade suportado é DES, portanto, não há nenhuma opção para especificar o protocolo de privacidade. As opções de configuração do SNMP V3 não são necessárias (cada uma pode ser especificada opcionalmente). Se você precisar especificá-las deverá especificar os valores apropriados para o nível de segurança selecionado.

Testando Grupos de Atributos de Evento SNMP
É possível testar o grupo de atributos do evento SNMP criado no Agent Builder.

Antes de Iniciar

Para testar o grupo de atributos de evento SNMP, use um programa de teste ou aplicativo para gerar os eventos SNMP.

Procedimento

1. É possível iniciar o procedimento de Teste das seguintes maneiras:
   - Durante a criação do agente, clique em **Testar** na janela **Informação do Evento SNMP**.
   - Após a criação do agente, selecione um grupo de atributos no Agent Editor **Definição de Origem de Dados** e clique em **Testar**. Para obter informações adicionais sobre o Agent Editor, consulte “Usando o Agent Editor para modificar o agente” na página 1172

   Após clicar em **Testar** em uma das duas etapas anteriores, a janela **Testar Configuração de Evento** é aberta.
2. Opcional: Antes de iniciar o teste, você pode configurar as variáveis de ambiente e as propriedades de configuração. Para obter mais informações, consulte “Teste de Grupo de Atributos” na página 1380. Para obter informações adicionais sobre as propriedades de Configuração de Evento SNMP, consulte “Propriedades de Configuração de Eventos SNMP” na página 1236.
3. Clique em **Iniciar Agente**. Uma janela indica que o Agente está sendo iniciado.

   Quando o agente é iniciado, ele recebe eventos SNMP de acordo com sua configuração.

   Nota: O agente que é iniciado é uma versão simplificada que inclui um grupo de atributos que você está testando.

4. Para testar a coleção de dados de seu agente, você gera eventos SNMP que correspondem à configuração do agente. É possível fazer isso usando um aplicativo ou um gerador de evento.

   Quando o agente recebe os eventos SNMP que correspondem à sua configuração, ele inclui os eventos no seu cache interno.

5. Para simular uma solicitação a partir do ambiente de monitoramento para dados do agente, clique em **Coletar Dados**.

   A janela **Testar Configurações de Evento** coleta e mostra quaisquer eventos no cache do agente, desde que ele foi iniciado pela última vez. Uma coleção de dados de exemplo é mostrada em Figura 33 na página 1239

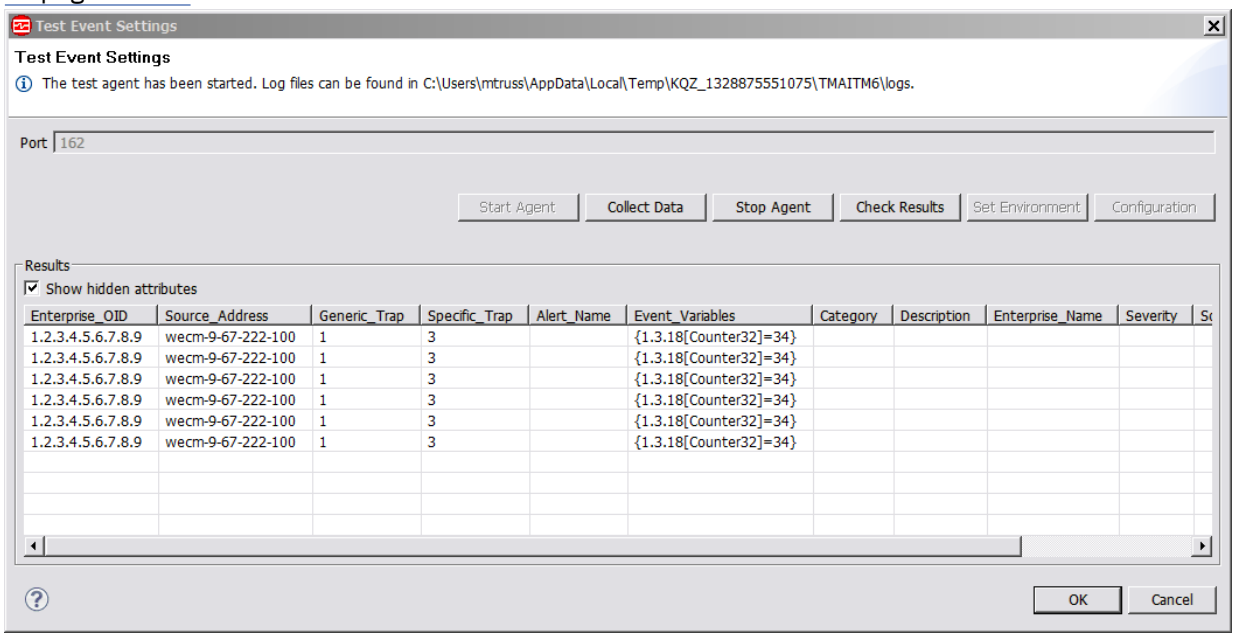


*Figura 33. Janela **Testar Configurações de Evento** que mostra os dados de evento SNMP coletados*

6. Opcional: Clique em **Verificar Resultados**, se os dados retornados não estiverem conforme o esperado.

   A janela **Status de Coleção de Dados** é aberta e mostra informações adicionais sobre os dados. Um exemplo é mostrado em (Figura 34 na página 1239). Os dados coletados e mostrados pela janela **Status de Coleção de Dados** são descritos em “Nó de Status do Objeto de Desempenho” na página 1424

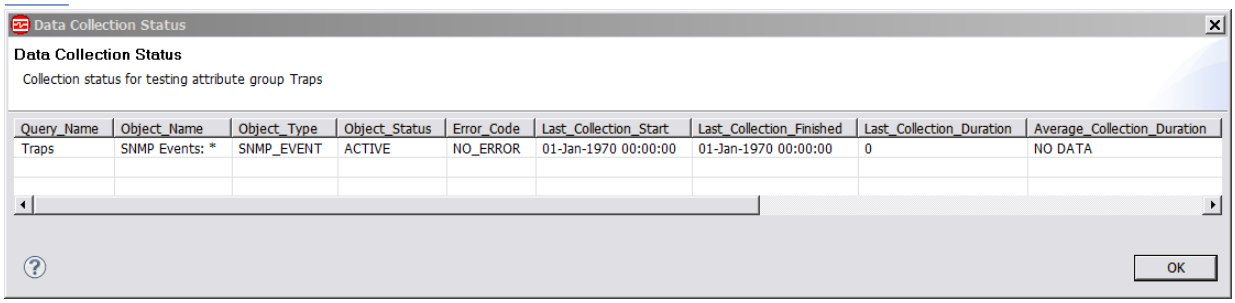


*Figura 34. Janela **Status de Coleta de Dados***

7. Pare o agente, clicando em **Parar Agente**.
8. Clique em **OK** ou **Cancelar** para sair da janela **Testar Configurações de Evento**. Clicar em **OK** salva quaisquer mudanças que tiver feito.

Conceitos relacionados

“Testando seu agente no Agent Builder” na página 1380
Depois de usar o Agent Builder para criar um agente, será possível testar o agente no Agent Builder.

Monitorando MBeans Java Management Extensions (JMX)

É possível definir uma origem de dados para coletar dados de MBeans JMX. Os dados de cada MBean monitorado são posicionados em um conjunto de dados. Dependendo do MBean, o conjunto de dados pode produzir uma única linha ou várias linhas.

Sobre Esta Tarefa

Cada origem de dados JMX que você define deve identificar se um único MBean (única instância) ou um determinado tipo de MBean (diversas instâncias). Você deve saber o nome do Objeto do MBean ou um padrão de Nome do Objeto para um tipo de MBean que contém os dados que você deseja coletar. Use um padrão de nome do objeto para identificar somente um conjunto de MBeans similares. O conjunto de MBeans que corresponde ao padrão deve fornecer todos os dados que você deseja na tabela de monitoramento. Um padrão de Nome de Objeto típico se parece com `*:j2eeType=Servlet,*`. Este Padrão de Nome de Objeto corresponde a todos os MBeans que possuem um j2eeType de servlet. É possível esperar que qualquer MBean correspondente ao padrão tenha um conjunto semelhante de atributos e operações expostos que podem ser incluídos em sua origem de dados. Uma origem de dados que utiliza tal padrão coleta dados de cada MBean correspondente ao padrão. Os atributos que você define para esta origem de dados deve estar disponível para qualquer MBean correspondente ao padrão do Nome de Objeto da origem de dados.

O Java Versão 5 ou mais recente é suportado.

Procedimento

1. Na página **Origem Inicial de Dados do Agente** ou na página **Local de Origem de Dados**, clique em **Dados de um servidor** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **JMX**.
3. Clique em **Avançar**.
4. Na página **Informações de JMX**, clique em **Navegar** para ver todos os MBeans JMX no servidor MBean.

   Depois de definir a origem de dados, é possível usar a função procurar para preencher previamente a lista de atributos. Depois você poderá incluir, remover ou modificar os atributos inseridos pelo navegador. Os nomes para esses atributos podem ser longos e difíceis de digitar corretamente. Utilizar a opção Procurar é uma maneira fácil de inserir o nome correto.

   Nota: Você pode criar manualmente a origem de dados JMX especificando um Nome do Objeto e clicando **Próximo** sem usar o navegador. Criar origens de dados JMX manualmente cria duas origens de dados. Uma origem de dados do evento que contém atributos predefinidos para notificações JMX é criada. Além disso, uma coleção de origem de dados é definida contendo um atributo que é necessário especificar no assistente.

   Padrão MBean
   Mostra o padrão MBean.

   Opções Globais do JMX
   Mostra o nível de suporte.

   O suporte é fornecido para os seguintes servidores JMX:

   - MBean Server do sistema operacional Java 5. Conexão é feita usando o conector JSR-160. As notificações e os monitores são suportados.
   - WebSphere Application Server, versão 6 e posterior. Conectores são fornecidos tanto para os protocolos SOAP quanto RMI. Os Monitores JMX não são suportados porque o MBeans não pode ser criado por um agente remoto.
   - WebSphere Community Edition e outros servidores do aplicativo baseados em Apache Geronimo. A conexão é feita através de conectores JSR-160 padrão. As notificações e os monitores do JMX são suportados nas versões 1.1 e posteriores.
   - JBoss Application Server, versão 4.0 e anterior.

- JBoss Application Server, conexão JSR-160.
- WebLogic Server, versão 9 e mais recente. É fornecido um conector para o protocolo T3.

5. Na primeira vez em que você executar o navegador JMX, não haverá itens no menu de rolagem para baixo **Servidor MBean**. Para incluir conexões, clique no botão **Incluir**).

   Use o botão **Editar** para modificar ou excluir a conexão que você já definiu e selecionou no menu de rolagem para baixo. As definições de conexão são armazenadas no espaço de trabalho assim, quando você criar uma conexão, ela serão relembradas. Conclua as seguintes etapas para criar uma conexão. Se já tiver uma conexão, pule para a próxima etapa.

   a) Para criar uma conexão ao Servidor MBean, clique em **Incluir** para incluir uma conexão ou editar uma conexão existente.

      A janela **Navegador Java Management Extensions (JMX)** é mostrada quando nenhuma conexão está definida.

   b) Após clicar em **Incluir** para incluir uma conexão, a página **Selecionar Tipo de Conexão** é aberta.

   c) Use o assistente de Conexão do Servidor MBean para se conectar a um servidor MBean. As novas conexões listadas na página são seleções que podem ser feitas para criar a conexão. É possível usar a lista de conexões existentes para criar uma nova conexão usando uma conexão existente como um modelo. Selecione um dos novos tipos de conexão e clique em **Avançar** para iniciar a criação de uma conexão.

   d) Depois de selecionar um tipo de conexão, é possível ser solicitado a selecionar um tipo de conexão mais específico. Dois modelos baseados no tipo de conexão **Conexões JMX Padrão (JSR-160)** são mostrados. Selecione o modelo que é mais adequado para seu servidor MBean e clique em **Avançar**.

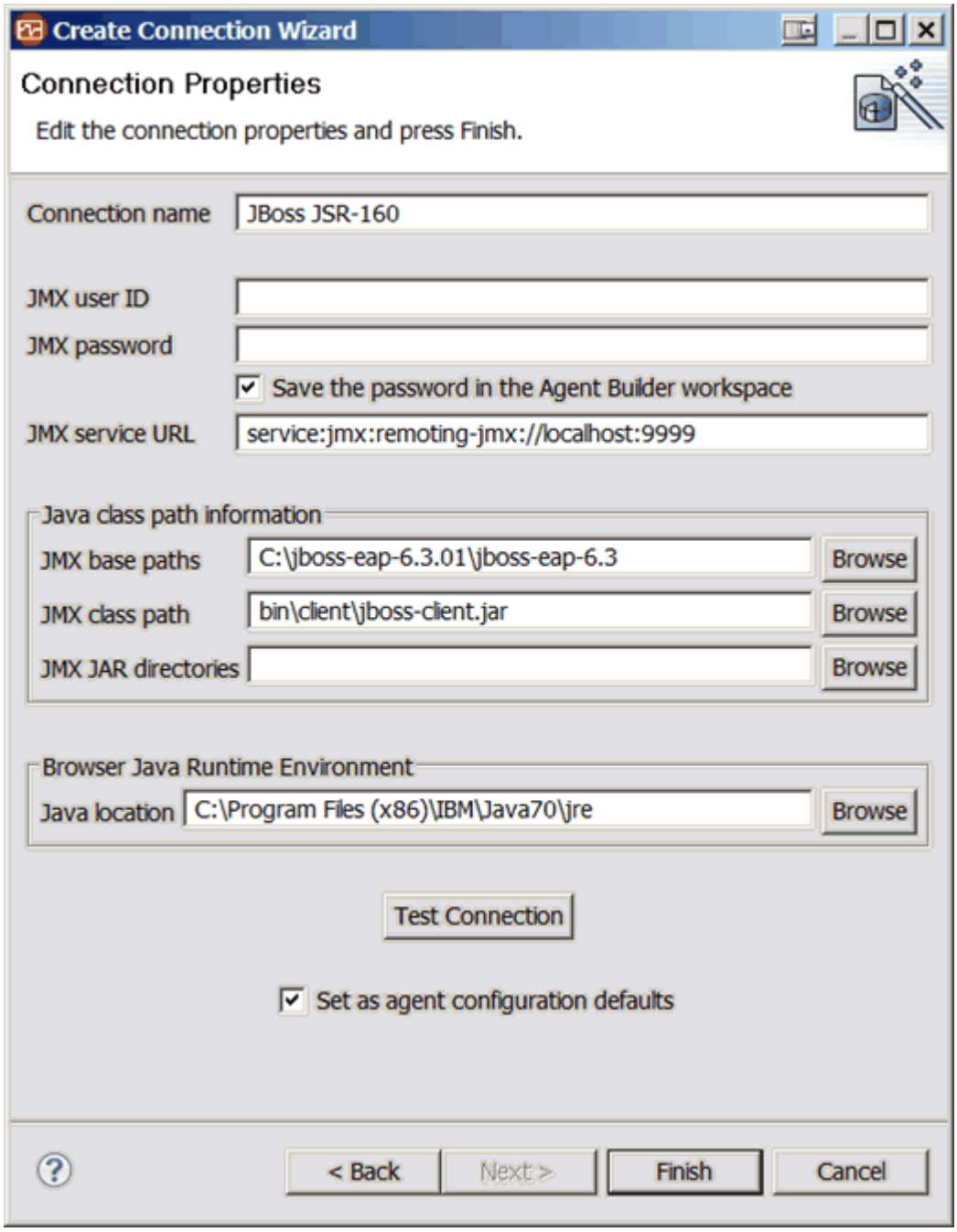


Figura 35. Propriedades de conexão JMX

A página **Propriedades da Conexão** (Figura 35 na página 1242) contém os detalhes sobre como se conectar a um servidor MBean. Você deve concluir a página com detalhes sobre seu servidor MBean.

Importante: Se sua origem de dados se conectar a um WebSphere Application Server remoto, assegure-se de que o WebSphere Application Server também esteja instalado no host que está executando o Agent Builder e configure a definição **Localização do Java** para o Java Runtime Environment que o WebSphere Application Server local usa.

e) Selecione a caixa de opção **Salvar a senha na área de trabalho do Agent Builder** se desejar salvar a senha para esta conexão.

f) Opcional: Selecione **Configurar como Padrões de Configuração do Agente**, se desejar que os padrões para o JMX sejam copiados a partir das propriedades de conexão.

Por exemplo, no Figura 35 na página 1242 o **caminho base JMX** padrão é `C:\jboss-eap-6.3.01\jboss-eap-6.3`, a **URL de serviço JMX** é `service:jmx:remoting-jmx://localhost:9999` e o **local de Java** é `C:\Arquivos de Programas\IBM\Java70\jre`

1) Depois de especificar as propriedades necessárias para conectar, clique em **Testar Conexão** para assegurar que a conexão possa ser estabelecida. Se a conexão não for bem-sucedida, corrija as propriedades necessárias.
2) Quando a conexão é bem-sucedida, clique em **Concluir** para retornar ao navegador e usar a conexão que você configurou.

As informações de caminho de classe Java na página **Propriedades da Conexão** contém três campos. Esses campos devem ser concluídos conforme necessário para conexão a um servidor MBean que requer classes Java que não estejam incluídas no Java Runtime Environment. Normalmente, o servidor MBean ao qual você deseja se conectar deve estar instalado no mesmo sistema que o Agent Builder. Neste caso, especifique o diretório no qual o aplicativo que contém o servidor MBean foi instalado como o campo **Caminhos base do JMX**. O campo **Diretórios Jar do JMX** lista os diretórios relativos ao diretório de Caminhos Base que contém os arquivos JAR que são necessários para se conectar ao servidor MBean. O campo **Caminho da classe do JMX** pode ser usado para incluir arquivos JAR específicos. Os arquivos JAR listados no campo **Diretórios JAR do JMX** não precisam ser listados separadamente no campo **Caminho da classe do JMX**.

Todos os campos podem conter mais de uma referência; separe as entradas por ponto-e-vírgula. Estes valores são os mesmos valores necessários ao configurar o agente. Para obter mais informações, consulte (“Configuração do JMX” na página 1247).

6. Depois de selecionar uma conexão, o Navegador JMX faz o download das informações sobre o MBeans a partir do servidor JMX. Essas informações são mostradas nas quatro áreas a seguir da janela **Navegador JMX** (Figura 36 na página 1244):

   Orientações para telas que iniciam com a janela Navegador Java Management Extensions (JMX) para a guia **Configuração de Tempo de Execução** do Agent Editor: Na página **Informações JMX**, selecione **Procurar**. No navegador (Navegador JMX sem conexão selecionada), selecione **Incluir**. Na página **Seleção de Conexão JMX**, selecione **JBoss** e depois selecione **Avançar**. Na página **Propriedades de Conexão JMX**, customize duas Propriedades de Conexão: Provedor JBoss URL : `jnp://wapwin3.tivlab.raleigh.ibm.com:1099/` e **Diretórios Jar JBoss**: O caminho completo ao diretório que contém os arquivos JAR a seguir: `jbossall-client.jar`, `jboss-jmx.jar`, `jboss-jsr77-client.jar`, `jboss-management.jar`. Selecione **Concluir**. Esta configuração define sua conexão JBoss para que seja possível obter telas semelhantes conforme mostrado aqui.

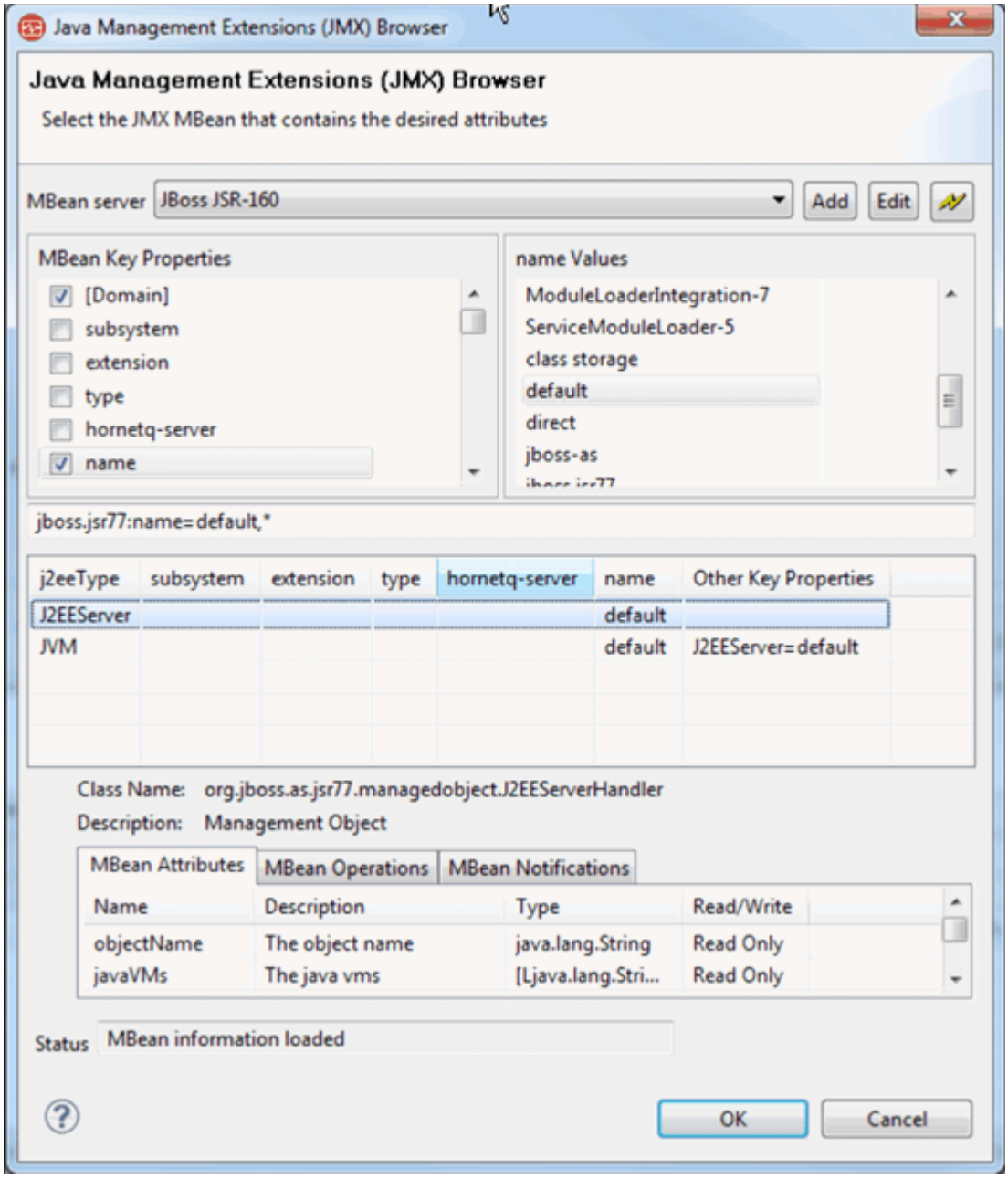


Figura 36. Janela Navegador Java Management Extensions (JMX)

- Área **Propriedades-chave do MBean**: Essa área é uma coleção de cada chave de Nome de Objeto exclusiva localizada em todos os MBeans no servidor. A entrada **[Domain]** é especial porque ela não realmente uma chave. Entretanto, a entrada **[Domain]** é tratada como uma chave implícita para o valor do domínio MBean. Selecione um item dessa lista, e os MBeans que contêm essa propriedade-chave são encontrados. A lista de valores da propriedade-chave é mostrada na lista **Valores da propriedade-chave selecionados**. Quando você verifica uma propriedade-chave, ela é incluída no padrão de Nome de Objeto para a origem de dados.
- Área **Valores da propriedade-chave selecionada**: Essa área mostra os valores da Propriedade-chave MBean atualmente selecionada de todos os MBeans. Selecionando um desses valores, verifica-se a propriedade-chave MBean. A seleção também atualiza o Padrão do Nome do Objeto mostrado no campo da mensagem com o nome da propriedade-chave MBean e o valor.
- Uma tabela lista todos os MBeans que correspondem ao Padrão de Nome de Objeto: Como você selecionou Propriedades-chave e valores a partir das Propriedades-chave MBean e Valores de Propriedade-chave Selecionados, você vê o Padrão de Nome do Objeto atualizar. Também vê a lista

de MBeans nessa tabela mudar para refletir a lista de MBeans que correspondem ao padrão que você selecionou. Se você tem um padrão que não está correspondendo ao MBeans, pode limpar as entradas na lista de Propriedades-chave do MBean. Você limpa as entradas clicando na caixa de seleção próxima à chave que está sendo usada por seu padrão e removendo a marca de seleção. Além disso, é possível editar o padrão para localizar MBeans pelos quais você está procurando. O padrão *:* seleciona todos os MBeans.

Você pode utilizar esta tabela para navegar nos MBeans a partir do servidor e decidir quais contém os dados de você deseja monitorar. Para ajudar a pesquisar um número potencialmente grande de MBeans, você pode classificar por atributo-chave (do menu ou clicando em um cabeçalho da coluna). Também pode mostrar qualquer atributo-chave em qualquer coluna selecionando **Mostrar Propriedade Chave** do menu. Quando você vê um valor de propriedade-chave na tabela que identifica MBeans que você deseja monitorar, clique com o botão direito nesse valor e escolha **Selecionar somente MBeans com Propriedade-chave** no menu.

- Uma tabela que contém detalhes para um MBean selecionado: o Navegador JMX mostra informações sobre um único MBean. Para ver detalhes de um MBean, selecione o MBean da tabela que mostra a lista de MBeans correspondentes ao filtro atual. As informações-chaves sobre o MBean é a lista de Atributos, Operações e Notificações que ele define.

Para criar uma origem de dados a partir do navegador JMX, use os quatro painéis descritos anteriormente para construir um Padrão de Nome de Objeto. Construa Padrão de Nome do Objeto para corresponder a um conjunto de MBeans que contém os dados de monitoramento que você deseja coletar. Por exemplo, se deseja monitorar dados de todos os ThreadPool MBeans, use as etapas a seguir:

a) Selecione o **tipo** no painel **Propriedades-Chaves do MBean**. A seleção de **tipo** faz com que os valores em **Valores de Propriedades-Chave Selecionados** sejam atualizados para listar todos os valores exclusivos a partir da chave de tipo de qualquer MBean.

b) Selecione **ThreadPool** na lista de valores para a chave do tipo. Depois de selecionar **ThreadPool**, o nome da propriedade-chave de tipo é selecionado no painel **Propriedades-Chave do MBean** e o Padrão de Nome do Objeto é atualizado para *:type=ThreadPool,*. A lista de MBeans também é atualizada para mostrar somente o MBeans que corresponde a este padrão.

c) Selecione um dos MBeans na lista de MBeans para ver os atributos, as operações e notificações disponíveis para o MBean. Se suas lista de MBean tiver mais MBeans do que você deseja monitorar, você deve continuar esse procedimento selecionando as propriedades-chave e valores. Continue até ter o Padrão de Nome do Objeto que identifica o conjunto de MBeans que você deseja monitorar. É possível abrir um menu na lista MBean para atualizar o Padrão de Objeto com os valores de propriedade-chave mostrados na tabela.

7. Quando o padrão do nome de objeto estive correto, selecione um MBean na tabela.

   Todos os atributos do MBean são atributos iniciais na nova origem de dados JMX. Alguns atributos podem não conter dados. Depois que a origem de dados JMX é criada, reveja os atributos e remova os que não são significativos. Se o MBean selecionado não tiver atributos, você será avisado de que a origem de dados será criada sem atributos. Se o MBean selecionado tiver notificações, uma origem de dados do evento também é criada para receber as notificações dos MBeans.

   Importante: Para cada atributo MBean, o Agent Builder cria um atributo no novo conjunto de dados. Para um atributo do MBean numérico, o Agent Builder cria um atributo numérico. Para qualquer tipo de objeto, incluindo `String`, o Agent Builder cria um atributo de sequência contendo uma representação em sequência do valor. Se um objeto de um atributo do MBean for do tipo `javax.management.openmbean.CompositeData` e o navegador do Agent Builder puder ler o objeto por si só, ele criará vários atributos, um para cada objeto integrado no objeto `CompositeData`. Para incluir valores internos para um objeto diferente de um objeto `CompositeData` (valores de retorno de arquivos ou de método), é preciso criar um atributo que tenha um nome de métrica mais complexo, conforme descrito em “Campos Específicos para Java Management Extensions (JMX) MBeans” na página 1255.

8. Clique em **Concluir** na página Informações sobre JMX preenchida.

   As origens de dados são criadas com base no MBean que foi selecionado na etapa anterior. Se nenhum MBean foi selecionado, é criado um grupo de atributos sem atributos. Um aviso é mostrado,

oferecendo a você a oportunidade de selecionar um MBean. A origem de dados de notificação possui a palavra **Evento**no início do nome da origem de dados para distingui-la da origem de dados que mostra atributos.

9. Para alterar outras opções do JMX para o agente, clique em **Opções Globais de JMX**. Com essas opções, você pode:
   a) Selecione se os monitores JMX são suportados por este agente. Se desejar que grupos de atributos do monitor JMX e comandos Executar Ação sejam criados, selecione **Incluir grupos de atributos do monitor JMX e execução de ações**

      Consulte a próxima seção para obter uma descrição de monitores JMX.
   b) Selecione os tipos de servidores de MBeans aos quais o seu agente se conecta quando implementado.

      Há diversos tipos específicos de fornecedores de servidores listados, junto com um Servidor Compatível com JSR-160 genérico para servidores baseados em padrões. É possível selecionar tantos quantos forem necessários, mas você deve selecionar somente os tipos de suportam os MBeans que estão sendo monitorados. Você deve selecionar no mínimo um. Se você selecionar mais de um, no momento da configuração do agente, será solicitado que especifique a qual tipo de servidor deseja conectar-se.
10. Clique em **OK** depois de selecionar a opção desejada.
11. Opcional: Você pode testar este grupo de atributos, clicando em **Testar**. Para obter informações adicionais sobre o teste, consulte (“Testando Grupos de Atributos JMX” na página 1258)
12. Opcional: É possível criar um filtro para limitar os dados retornados por esse grupo de atributos clicando em **Avançado**. Para obter informações adicionais sobre filtragem de dados de um grupo de atributos, consulte “Filtrando Grupos de Atributos” na página 1201
13. Clique em **Avançar**.
14. Na página **Selecionar Atributos-chave**, selecione os atributos-chave ou indique que esta origem de dados produz somente uma linha de dados. Para obter mais informações, consulte (“Selecionando Atributos-Chaves” na página 1172).
15. Clique em **Avançar**.

    A janela **Opções Globais do Agente JMX** mostra os tipos de servidores de aplicativos que o Agent Builder suporta. Se você selecionou anteriormente **Configurar como Padrões de Configuração do Agente** na página **Propriedades da Conexão**, o tipo de servidor de aplicativos no qual você navegou será selecionado automaticamente.
16. Na janela **Opções Globais do Agente JMX**, (Figura 37 na página 1247), selecione qualquer outro tipo de servidor de aplicativo ao qual você deseja que seu agente possa se conectar.

    Nota: No exemplo mostrado, escolher **Conexão do JBoss Application Server JSR-160** é o mesmo que escolher **Servidor Compatível com JSR-160**, exceto que valores padrão diferentes são fornecidos.

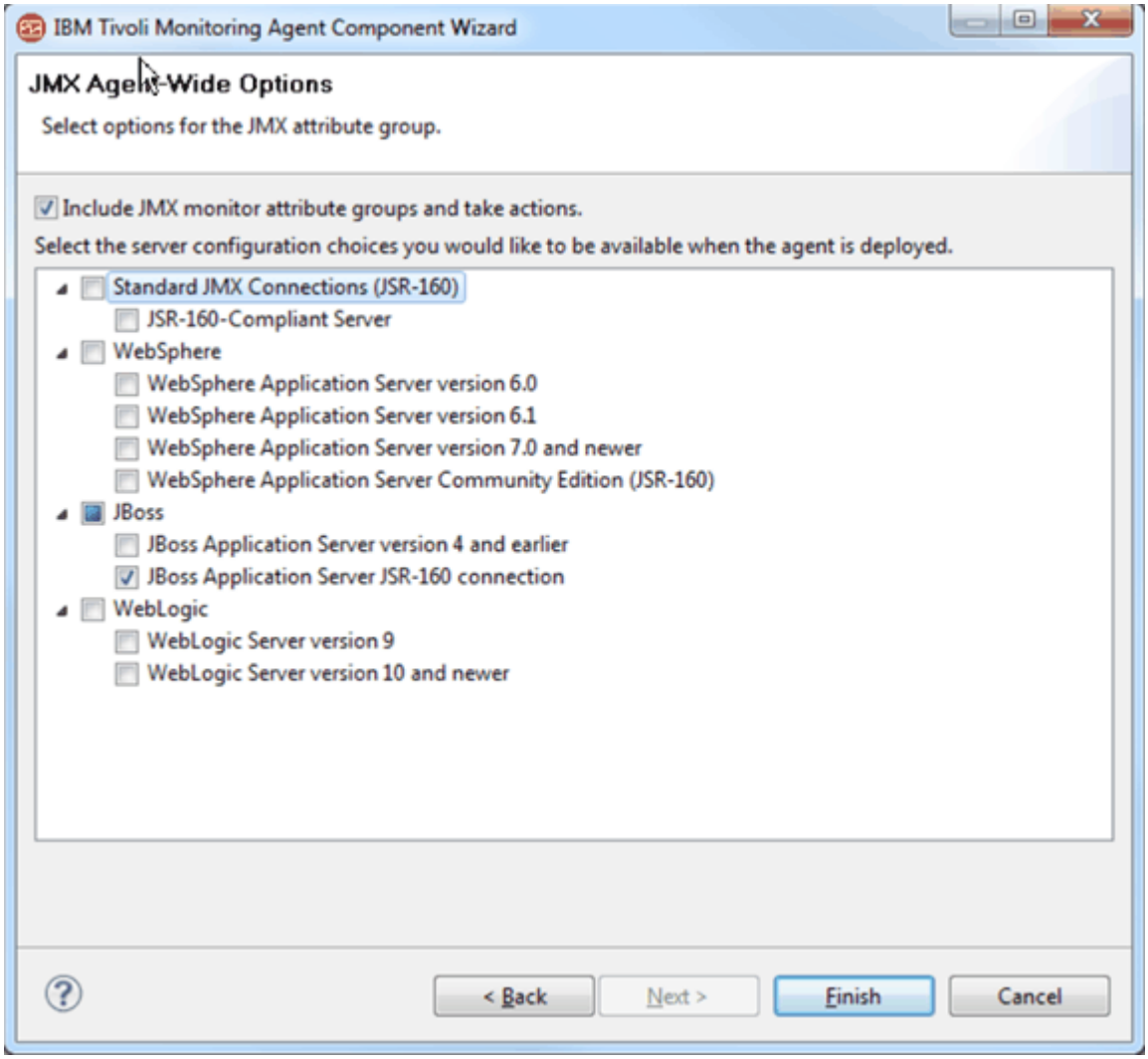


Figura 37. Janela Opções de Todo o Agente JMX

17. Execute uma das seguintes etapas:
    - Se você estiver usando o assistente de Novo Agente, clique em **Avançar**.
    - Clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor.
18. Se desejar mudar os tipos de servidores de aplicativos aos quais você pode se conectar após o agente ser criado, clique em **Opções JMX Globais** na área **Informações da Origem de Dados JMX**.
19. Na página **Opções Globais do Agente JMX**, mude quaisquer seleções que desejar.
20. Clique em **OK**.
21. Para visualizar as seções e propriedades de configuração que foram geradas automaticamente, clique na guia **Configuração de Tempo de Execução** do Agent Editor.

    O valor padrão da propriedade `Caminhos base de JBoss` tem o valor que foi inserido no navegador JMX.

O que Fazer Depois

Para obter informações adicionais sobre os grupos de atributos para eventos do JMX, consulte “Grupos de atributos de eventos JMX” na página 1452,

Configuração do JMX

Quando você define uma origem de dados JMX em seu agente, algumas propriedades de configuração são criadas para você.

A configuração de tempo de execução de JMX é exclusiva porque fornece algum controle sobre a quantidade de configuração exibida. O cliente JMX para o agente pode conectar-se a vários tipos diferentes de servidores de aplicativos. Entretanto, não é necessário suportar todos esses tipos de servidores de aplicativos em nenhum agente. É possível determinar quais tipos de servidores de aplicativos suportar e as seções de configuração desnecessárias não são incluídas no agente.

Na maioria dos casos, um agente é designado para monitorar o tipo de servidor de aplicativos JMX. Ao criar a origem de dados do JMX, é possível usar o Navegador JMX. Ao usar o Navegador JMX, as opções de configuração do servidor JMX usadas para procurar o servidor MBean são incluídas no agente automaticamente. Para mudar os tipos de servidores de aplicativos aos quais você pode se conectar após a criação do agente, clique em **Opções de JMX Globais** na área **Informações de JMX**. Na página **Opções de Todo o Agente JMX**, mude quaisquer seleções que desejar.

É possível projetar um agente genérico que monitora mais de um tipo de servidor de aplicativos JMX. Nesse caso, mais de uma opção de configuração do servidor JMX pode ser selecionada na página **Opções de Todo o Agente JMX**. Quando mais de um tipo de conexão JMX for suportada, a configuração de tempo de execução avisará sobre o tipo de conexão que é usado para essa instância do agente.

Nota: Uma instância de um agente pode conectar-se somente a um tipo de servidor de aplicativos JMX. Os subnós podem ser utilizados para conectar-se a diferentes servidores de aplicativos JMX do mesmo tipo em uma instância do agente. Para conectar-se a mais de um tipo de servidor de aplicativos JMX, é necessário configurar pelo menos uma instância do agente para cada tipo de servidor de aplicativos JMX.

É possível visualizar, incluir e alterar as propriedades de configuração usando o Agent Editor. Para obter instruções, veja "Alterando Propriedades de Configuração Usando o Agent Editor" na página 1367. Se uma origem de dados do JMX estiver definida em um subnó, você também conseguirá de especificar Substituições de Configuração do Subnó. Para obter instruções, veja "Configuração do subnó" na página 1354.

Se você definir uma origem de dados do JMX em seu agente, o agente deverá utilizar Java para conectar-se ao servidor de aplicativos JMX. As propriedades de configuração de Java são incluídas no agente automaticamente.

As seguintes propriedades de configuração de Java são específicas à configuração do tempo de execução do agente:

Início do Java
Caminho completo que aponta para o diretório de instalação Java

Configure o agente para usar o mesmo JVM que o aplicativo que você está monitorando usa, especialmente para o WebLogic Server e o WebSphere Application Server.

Argumentos do JVM
Especifica uma lista opcional de argumentos para a Java virtual machine.

Nível de Rastreio
Define a quantidade de informações a ser gravada no arquivo de rastreio Java. O padrão é somente gravação de dados de erro no arquivo de log.

Nota: O Agent Builder não requer essas propriedades porque usa sua própria JVM e criação de log, que são configurados por meio do plug-in JLog.

Se você definir uma origem de dados do JMX em seu agente, os seguintes campos de configuração necessários comuns serão incluídos no agente automaticamente:

Conexão
O tipo de conexão com o servidor MBean

ID do usuário
O nome de usuário que é usado para autenticar com o servidor MBean.

Password
Senha para o ID do usuário.

Caminhos de Base
Os diretórios que são procurados para arquivos JAR nomeados no **Caminho da Classe** ou diretórios nomeados nos **Diretórios JAR**, que não estão totalmente qualificados. Os nomes de diretório são separados por ponto-e-vírgula (`;`) no Windows, e por ponto e vírgula (`;`) ou dois pontos (`:`) nos sistemas UNIX.

Caminho de Classe
Os arquivos JAR explicitamente nomeados a serem procurados pelo agente. Qualquer um que não esteja totalmente qualificado será anexado a cada um dos Caminhos Base até que o arquivo JAR seja localizado.

Diretórios JAR
Diretórios que são procurados para os arquivos JAR. Os nomes de diretório são separados por ponto-e-vírgula (`;`) no Windows, e por ponto e vírgula (`;`) ou dois pontos (`:`) nos sistemas UNIX. Os arquivos JAR nesses diretórios não precisam ser explicitamente identificados; eles são localizados porque estão em um desses diretórios. Os subdiretórios destes diretórios não são procurados. Qualquer nome de diretório que não esteja totalmente qualificado será anexado em cada Caminho Base até que o diretório seja localizado.

Nota: Ao monitorar remotamente, os arquivos JAR e todos os seus arquivos JAR dependentes devem ser instalados localmente no computador em que o agente está sendo executado. Esses arquivos JAR são os arquivos que são necessários para se conectar ao aplicativo que está sendo monitorado. Esses arquivos JAR devem ser configurados em **diretórios JAR** e em **Caminhos Base** e **Caminho da Classe**. Além disso, instale localmente uma JVM suportada para o aplicativo que você está monitorando e especifique o caminho no campo **Configuração do Java Home**.

Exemplos:

- Para WebLogic 10, o caminho da classe é `server/lib/wlclient.jar;server/lib/wljmxclient.jar`. O caminho base aponta para o diretório do servidor de aplicativos em que o diretório `server/lib` está localizado.
- Para o WebSphere, o caminho base aponta para o local onde o servidor de aplicativo WebSphere está instalado. Múltiplos caminhos base estão listados neste exemplo para fornecer um padrão para oWindows e UNIX. O caminho da classe lista os arquivos JAR relativos ao caminho base. O valor relativo `lib` para o campo **Diretórios JAR** faz com que todos os arquivos JAR neste diretório sob o caminho base sejam carregados.
  - **Caminhos Base**: `C:\Program Files\IBM\WebSphere\AppServer;/opt/IBM/WebSphere/AppServer`
  - **Caminho da Classe**: `runtimes/com.ibm.ws.admin.client_6.1.0.jar;plugins/com.ibm.ws.security.crypto_6.1.0.jar`
  - **Diretórios JAR**: `lib`

Dependendo de quais tipos de servidor JMX estão selecionados na página Opções de Todo o Agente JMX, algumas ou todas as propriedades de conexão a seguir são incluídas. Os valores padrão são fornecidos pelo Agent Builder e podem ser modificados:

Propriedades de configuração específicas da conexão do servidor compatível com JSR-160:

URL de Serviço JMX
A URL de Serviços JMX para conexão para monitoramento.

Propriedades de configuração específicas de conexão do WebSphere Application Server versão 6.0 e mais recente:

Nome de Host
O nome do Host do sistema no qual o servidor de aplicativos que você está monitorando está localizado. Para monitorando local, o nome será o nome do sistema local. Para monitorando remoto, o nome será o nome do host do sistema no qual o servidor de aplicativos está localizado.

Port
Número da porta a ser usado no nome do host a ser monitorado.

Protocolo do conector
O protocolo do conector a ser usado pela conexão de monitoramento. Os protocolos RMI e SOAP são suportados.

Nome do Perfil
O nome do perfil a ser usado para configuração da conexão.

Propriedades de configuração específicas da conexão do JBoss Application Server (não JSR-160):

Nome de JNDI
Nomes JNDI usados para consultar o servidor MBean.

URL do Provedor
URL do provedor de Serviços JMX para conexão para monitoramento.

Propriedades de configuração específicas da conexão do WebLogic Server:

URL do Serviço
A URL do Provedor de Serviços JMX para conexão para monitoramento que inclui o nome JNDI.

Nota: Se a segurança administrativa WebSphere estiver ativada, você deve assegurar-se de que os prompts de login do cliente estejam desativados nos arquivos de propriedades da conexão do cliente apropriados. Para as conexão RMI, para evitar que os clientes exibam prompts ao usuário, você deverá modificar a propriedade *com.ibm.CORBA.loginSource* no arquivo `sas.client.props` no diretório de propriedades do perfil do seu WebSphere Application Server. Para uma conexão SOAP, você deve modificar a *propriedade com.ibm.SOAP.loginSource* no arquivo `soap.client.props` no mesmo diretório. Em ambos os casos, a propriedade *loginSource* deve ser configurada para não conter um valor.

É possível visualizar, incluir e alterar as propriedades de configuração usando o Agent Editor. Consulte ("Alterando Propriedades de Configuração Usando o Agent Editor" na página 1367). Se uma origem de dados do Windows estiver definida em um subnó, também será possível especificar Substituições de Configuração do Subnó. Consulte "Configuração do subnó" na página 1354.

Notificações JMX
Além de fornecer dados de monitoramento quando solicitados, alguns MBeans também fornecem notificações.

Uma notificação é um objeto gerado por um MBean que é transmitido para os listeners registrados quando ocorre um evento.

Os agentes construídos pelo Agent Builder podem definir grupos de atributos que contêm valores de notificações em vez de MBeans.

Quando o aplicativo é iniciado, um `listener de notificação` é registrado com cada MBean que corresponde ao padrão MBean do grupo de atributos. O grupo de atributos então exibe uma linha por notificação recebida. Cada coluna contém um item de dados da notificação. Os dados desejados na notificação são definidos por um valor de coluna semelhante à maneira como os dados da coluna são definidos para MBeans.

Para grupos de atributos não baseados em eventos, os dados são coletados quando necessário. Para grupos de atributos baseados em eventos, o agente mantém um cache dos últimos 100 eventos recebidos. Esses eventos são utilizados para responder aos pedidos do Tivoli Enterprise Portal. Os eventos são redirecionados imediatamente para análise por situações e pelo armazenamento.

Monitores JMX
Além de fornecer dados de monitoramento solicitados, alguns MBeans também fornecem monitores.

O Provedor JMX suporta a capacidade para um agente criar Monitores JMX. Um Monitor JMX é um MBean que o agente JMX cria no Servidor JMX. Ele monitora o valor de um atributo de um outro MBean e envia uma notificação quando esse valor atende a alguns critérios. São definidos limites que possibilitam que o Monitor relate valores de atributos específicos.

Nem todos os servidores de aplicativos suportam a criação de monitores de um cliente JMX, o que é verdadeiro para as liberações atuais do WebSphere Application Server. Monitores JMX e comandos

Executar Ação podem ser incluídos em seu agente selecionando **Incluir grupos de atributos do monitor JMX e executar ações** em **Opções de JMX Globais**.

Qualquer MBean que relate um atributo de um outro MBean pode se considerado um monitor. Na prática, o JMX define três classes de monitor concretas, que são os tipos de monitores que são criados. Os seguintes tipos de monitores concretos são criados:

- Monitor de sequência – observa um atributo de sequência e relata a igualdade ou desigualdade dessa sequência.
- Monitor de calibrador – observa um atributo numérico variável e relata uma movimentação para cima ou para baixo além dos valores limite.
- Monitor de contador – observa um atributo numérico crescente quando ele atinge um valor limite ou aumenta uma certa quantidade.

Os grupos de atributos a seguir podem ser automaticamente incluídos no agente para coleta ou representar notificações do Monitor do JMX:

- `Monitores Registrados`

  Este grupo de atributos exibe todos os Monitores JMX que são incluídos pelo usuário.
- `Notificações de Contador`

  Este grupo de atributos relata todas as notificações recebidas de Monitores de Contador.
- `Notificações de Calibre`

  Este grupo de atributos relata todas as notificações recebidas dos Monitores de Calibre.
- `Notificações de Sequência`

  Este grupo de atributos relata todas as notificações recebidas de Monitores de Sequência.

Comandos Executar Ação para Monitores JMX
Um monitor é criado executando um comando Executar Ação.

Três comandos Executar Ação são definidos, um para criar cada tipo de monitor e um quarto Executar Ação é definido para excluir um monitor existente. Um limite de 256 caracteres se aplica aos comandos Executar Ações.

Os grupos de atributos do monitor são uma parte de cada agente JMX construído, incluindo todos os agentes construídos pelo Agent Builder. Os quatro comandos Executar Ação estão disponíveis para todos os agentes, embora eles não possam ser utilizados, a menos que seja um agente JMX.

Incluir Inspecionador de Métrica de Sequência JMX
Use o comando Executar Ação para criar um monitor para assistir a um atributo de sequência.

Parâmetros

Padrão MBean
Todos os MBeans correspondentes a este padrão são monitorados por esse monitor.

Atributo observado
O nome do atributo de sequência MBean que está sendo inspecionado.

Notificar correspondência
True se uma notificação deve ser enviada quando a sequência monitorada corresponde a um valor de referência, caso contrário é false (o padrão é false).

Notificar diferença
True se uma notificação deve ser enviada quando a sequência monitorada não corresponde ao valor de referência, caso contrário é false (o padrão é true).

Valor de referência
A sequência a ser comparada com o atributo observado.

Um padrão significa que o argumento não está especificado.

Exemplo: Solicitar uma notificação quando um serviço estiver parado.

```
STRING_METRIC_WATCHER [*:type=Service,*] [StateString] [true] [false] [Stopped]
```

Em que:

`*:type=Service,*`
Padrão de MBean: Monitora qualquer MBean com um tipo nomeado de propriedade-chave cujo valor é Serviço.

`StateString`
Atributo observado: Um atributo de sequência que é comum a todos os MBeans de `type=Service`.

verdadeiro
Notificar correspondência: Você deseja que uma notificação seja enviada ao seu agente quando o atributo `StateString` corresponder seu valor de referência Parado.

false
Notificar diferença: Você não deseja ser notificado quando atributo Service não corresponder a Parado.

Interrompido
Valor de referência: Quando o atributo `StateString` for alterado para o valor Parado, uma notificação será enviado.

Incluir Inspecionador de Métrica de Calibre JMX
Use o comando Executar Ação para criar um monitor para assistir a um atributo calibrador.

Parâmetros

Padrão MBean
Todos os MBeans correspondentes a este padrão são monitorados por esse monitor.

Atributo observado
O nome do atributo de sequência MBean que está sendo inspecionado.

Modo de diferença
True, se o valor monitorado for a diferença entre os valores atual e anterior reais do atributo. False, se o valor monitorado for o valor atual real do atributo (o padrão é false).

Notificar alto
True se uma notificação deve ser enviada quando um valor monitorado crescente ultrapassa o limite máximo, caso contrário é false (o padrão é true).

Notificar baixo
True se uma notificação deve ser enviada quando um valor monitorado decrescente ultrapassa o limite mínimo, caso contrário é false (o padrão é true).

Limite alto
Valor sob o qual espera-se que o atributo observado fique.

Limite baixo
Valor sobre o qual espera-se que o atributo observado fique.

Exemplo: Solicitar uma Notificação Quando a Memória Livre Ficar Abaixo de 10 Mb

```
GAUGE_METRIC_WATCHER [ServerInfo] [FreeMemory] [false] [false] [true] [30000000] [10000000]
```

Em que:

`*:type=ServerInfo`
Padrão de MBean: Monitora qualquer MBean cujo nome possua um único tipo de propriedade-chave nomeada cujo valor é ServerInfo.

FreeMemory
Atributo observado: Atributo numérico que flutua acima ou abaixo, indicando a quantidade de memória livre no servidor de aplicativos.

false
Modo de diferença: Monitora o valor de atributo real, não a diferença entre uma observação e outra.

false
Notificação alta: A notificação não é enviada quando a memória livre fica acima.

verdadeiro
Notificação baixa: A notificação não é enviada quando a memória livre fica muito baixa.

30000000
Limite alto: Mesmo se você não estiver preocupado em passar um limite máximo, é necessário um valor de limite alto razoável. Uma segunda notificação de limite baixo não ocorre até que o valor de atributo atinja ou passe o limite máximo.

10000000
Limite baixo: Valor de limite baixo sobre o qual deseja ser notificado.

Incluir Inspecionador de Métrica de Contador JMX
Use o comando Executar Ação para criar um monitor para ver um atributo contador.

Parâmetros

Padrão MBean
Todos os MBeans correspondentes a este padrão são monitorados por esse monitor.

Atributo observado
O nome do atributo de sequência MBean que está sendo inspecionado.

Limite inicial
Valor com o qual o atributo observado é comparado.

Deslocamento
Valor incluído no limite após o limite ser excedido para criar um limite alterado.

Modulus
Valor máximo do contador, após o qual ele muda para 0.

Modo de diferença
True, se o valor monitorado for a diferença entre os valores atual e anterior reais do atributo. False, se o valor monitorado for o valor atual real do atributo (o padrão é false). Este modo ativa efetivamente o monitoramento da taxa de mudança.

Período de granularidade
A freqüência de tomada de medidas (o padrão de 20 segundos). Mais importante, se o modo de diferença for true

Exemplo: Solicitar uma notificação quando qualquer servidor tiver três ou mais erros.

```
COUNTER_METRIC_WATCHER [*:j2eeType=Servlet,*] [errorCount] [3] [4] [] [diff] [gran]
```

Em que:

`*:j2eeType=Servlet,*`
Padrão de MBean: Monitora qualquer MBean do Servlet J2EE cujo nome possua um único tipo de propriedade-chave nomeada cujo valor seja `ServerInfo`

`errorCount`
Atributo observado: Atributo numérico crescente, que indica o número de erros do servlet.

3
Limite inicial: Você quer ser notificado quando c `errorCount` corresponder ou exceder 3.

4
Deslocamento: Ao obter uma notificação para os três erros, 4 é para que o limite anterior de 3 crie um novo limite de 7. Uma segunda notificação será enviada depois que `errorCount` atingir 7; uma terceira em 11; uma quarta em 15, e assim por diante. Zero ou nenhum não é válido, porque espera-

se que o contador sempre aumente e não aumentar o deslocamento não faria sentido para um contador.

Módulo:
O errorCount não possui nenhum valor máximo estruturado, portanto, utilize um valor razoavelmente alto.

false
Modo de diferença: Você está preocupado com as contagens de erros absolutas. A diferença será true se você estiver interessado na taxa de aumento do errorCount.

Período de granularidade: Não configurado, portanto, utilize o período de granularidade padrão de 20 segundos. O período de granularidade está disponível para todos os tipos de monitor. No entanto, ele é mostrado com um monitor de contador, para que uma taxa significativa de mudança (com o modo de monitorar=true) possa ser determinada.

Excluir Inspecionador de Métrica JMX
Use este comando Executar Ação para excluir um monitor.

Parâmetro

Número
O número do monitor conforme mostrado na tabela REGISTERED_MONITORS.

Exemplo: Excluir número de monitor 2

```
DELETE_WATCHER [2]
```

Em que:

2=
Número do monitor a ser excluído.

Operações JMX
Além de fornecer dados de monitoramento quando solicitados, alguns MBeans também fornecem operações.

Os agentes que possuem origens de dados JMX incluem o comando Executar Ação `JMX_INVOKE` que pode ser usado para executar operações JMX no servidor que você está monitorando.

Sintaxe do Comando Executar Ação

A ação possui a seguinte sintaxe:

```
JMX_INVOKE [MBean pattern] [Operation name] [Argument 1] [Argument 2] [Argument 3] [Argument
4]
```

Em que:

Padrão MBean
A consulta MBean que seleciona os MBeans nos quais a operação é executada. Se o padrão corresponder a mais de um MBean, a operação é executada em cada um dos MBeans correspondidos.

Nome da operação
Nome da operação MBean a ser executado.

Argumento 1, Argumento 2, Argumento 3, Argumento 4
Argumentos opcionais que podem ser fornecidos para a operação MBean. Os argumentos devem ser um tipo de dados simples, como uma sequência ou um inteiro.

O comando Executar Ação `JMX invoke` retorna êxito, se a operação for executada com êxito. Se a operação retornar um valor, o valor será gravado no arquivo de log do provedor de dados JMX.

Exemplo: Iniciar uma Operação para Reconfigurar um Contador

Esta ação executa a operação resetPeakThreadCount dos MBeans de Encadeamento:

```
JMX_INVOKE [*:type=Threading,*] [resetPeakThreadCount][] [] [] []
```

Em que:

:type=Threading,
Padrão MBean: Este padrão corresponde a todos os MBeans que possuem um tipo de Passagem.

resetPeakThreadCount
Nome da Operação: A operação que é executada em cada MBean que corresponde ao padrão.

[] [] [] []
Argumento 1, 2, 3, 4: Esses argumentos não são necessários para esta operação. Eles são especificados somente para estar em conformidade com a sintaxe da ação.

Exemplo: Iniciar uma Ação com um Argumento

Esta ação executa a operação getThreadCpuTime dos MBeans de Encadeamento. O resultado é registrado no arquivo de rastreio do provedor de dados JMX.

```
JMX_INVOKE [*:type=Threading,*] [getThreadCpuTime] [1] [] [] []
```

Em que:

:type=Threading,
Padrão de MBean: Este padrão corresponde a todos os MBeans que possuem um tipo de Threading.

getThreadCpuTime
Nome da Operação: A operação que é executada em cada MBean que corresponde ao padrão.

1
Argumento 1: O ID do encadeamento que está sendo consultado.

[] [] []
Argumento 2, 3, 4: Esses argumentos não são necessários para esta operação. Eles são especificados como argumentos vazios para estar em conformidade com a sintaxe de comando Executar Ação.

Executando o Comando Executar Ação `JMX_INVOKE`

O desenvolvedor do agente não pode esperar que o usuário execute o comando Executar Ação `JMX_INVOKE`. Em vez disso, devem ser desenvolvidas ações adicionais que executam a Ação de Execução `JMX_INVOKE`. Se possível nessas condições, oculte os detalhes, como o nome da operação e o padrão MBean do usuário.

Iniciando e Parando os Monitores JMX
Os monitores JMX estão persistentes entres inícios e paradas do agente e do servidor JMX.

Se o agente detectar que o servidor JMX foi reciclado, ele registrará novamente os monitores. Se o agente for reciclado, os monitores tornarão a ser registrados. As definições do monitor são armazenadas em um arquivo chamado `default_`*`instanceName`*`.monitors` em que *instanceName* é o nome da instância do agente ou padrão se ele for um agente de uma única instância. Esse arquivo está no diretório a seguir (observe que *xx* denota o código do produto de dois caracteres):

- Sistemas Windows: `TMAITM6/k`*`xx`*`/config`
- Sistemas UNIX e Linux: *`architecture`*`/`*`xx`*`/config` (consulte “Novos Arquivos em Seu Sistema” na página 1397 para obter informações sobre como determinar o valor da arquitetura)

Se o agente for reiniciado, ele usa o arquivo de definições do monitor para restaurar os monitores.

Campos Específicos para Java Management Extensions (JMX) MBeans
A sintaxe do nome de métrica para um grupo de atributos JMX deve seguir certas regras, quando especificada na janela **Informações de Atributo**.

A sintaxe do nome da métrica para um grupo de Atributos JMX consiste em tokens separados por um ponto final. Os tokens formam valores primários e, opcionalmente, valores secundários:

- **Valor Primário**: um valor obtido diretamente do MBean ou da Notificação em uma linha específica da tabela. Valores primários de um MBean são obtidos a partir de uma chamada ou de uma operação MBean (chamada de método). Os valores primários a partir de uma Notificação são obtidos de um campo ou chamada de um método no objeto da Notificação. Os valores primários podem ser tipos primitivos ou podem ser objetos Java.
- **Valor secundário**: um valor obtido pelo processamento adicional de um valor primário ou outro valor secundário. Valores secundários são processados internamente ao mecanismo e não envolvem chamadas para o servidor JMX. Se o primário (ou outro valor secundário) for um objeto Java, um valor secundário é o resultado da busca de um campo público desse objeto. Um valor secundário também pode ser o resultado de uma chamada de método em tal objeto. Esses valores secundários são obtidos usando a introspecção Java do objeto Java primário (ou outro secundário). Se o valor primário (ou outro secundário) for uma Sequência Java no formato de um nome MBean, o valor secundário pode ser o domínio. O valor secundário também pode ser qualquer uma das propriedades que compõem o nome MBean.

A seguinte sintaxe descreve o formato para o campo **Nome da métrica**:

```
Nome da
Métrica    =    PrimaryValue [ .SecondaryValue ]
PrimaryValue    =    Atributo.attributeName |
        Método.methodName |
        Domain |
        Propriedade.propertyName |
        Campo.fieldName |
        Nome
SecondaryValue    =    Campo.fieldName |
        Método.methodName |
        Domain |
        Propriedade.propertyName |
        Explode |
        ElementCount
```

```
propertyName    =    o nome de uma propriedade chave em um MBean ObjectName attributeName
=    o nome
de um atributo MBean methodName    =    uma operação de argumento zero de um MBean ou um método
de argumento zero
de uma Notificação ou outro objeto Java.
methodName(argument) = Uma operação de argumento único de um MBean ou um
método de argumento único de uma Notificação ou outro objeto Java. A propriedade
argumento será transmitido para o método como uma sequência.
fieldName    =    o nome de uma variável de instância pública em uma Notificação ou outro
objeto Java
notificationMethod    =    o nome de um método público de argumento zero de um objeto de
Notificação
```

Incluindo somente um valor primário na definição do nome da métrica, os dados coletados podem ser qualquer um dos seguintes itens:

- Domínio do MBean
- Valor da sequência do MBean
- Propriedade-chave a partir do nome do MBean
- O valor de atributo numérico ou de sequência em um atributo do MBean (incluindo o nome completo de outro MBean). Um valor de retorno numérico ou de sequência de uma operação de um MBean.
- Valor de uma variável de instância pública numérica ou de sequência em um objeto de Notificação
- O valor de retorno numérico ou de sequência a partir de uma operação de uma Notificação.

Ao incluir um valor secundário na definição de uma métrica, será possível executar drilldown no valor primário de um objeto Java. Além disso, você pode iniciar um método público ou buscar uma variável de instância pública.

Ao incluir um valor secundário em outro valor secundário na definição da métrica, você pode fazer drill down em um objeto de valor secundário. É possível continuar tão detalhadamente quanto os objetos são aninhados dentro de um MBean ou um Notificação.

Os tokens que compõem os valores primários e secundários são as palavras-chaves ou os nomes. Na maioria dos casos, um token de palavra-chave é seguido por um token de nome. A tabela a seguir mostra alguns exemplos:

Amostra de nome de métrica	**Tipo de grupo de atributos**	**Descrição dos dados retornados**
`Domain`	MBean	A parte do domínio do MBean (a parte antes dos dois-pontos).
`Nome`	MBean	A representação de sequência completa do MBean.
`Attribute.serverVendor`	MBean	Atributo serverVendor do MBean.
`Method.getHeapSize`	MBean	O valor retornado pelo getHeapSize() no MBean.
`Property.j2eeType`	MBean	O valor de j2eeType extraído do nome do MBean.
`Field.Message`	Evento (Notificação)	O campo **Mensagem** em uma notificação.

As palavras-chave `Atributo`, `Método` e `Campo` podem retornar objetos Java que contêm outros dados. É possível executar operações nesses objetos, anexando as definições de valor secundário. Mais exemplos:

Amostra de nome de métrica	**Tipo de grupo de atributos**	**Descrição dos dados retornados**
Attribute.deployedObject.Method.getName	MBean	Pega o atributo deployedObject do MBean e obtém o resultados do método getName().
Attribute.eventProvider.Method.getException.Method.getDescription	MBean	Atinge 3 profundidades: um atributo denominado eventProvider é presumido como sendo um objeto que possui um método getException(). Este método retorna um objeto com um método getDescription(). Tal método é chamado e o valor retornado é colocado na coluna.
Attribute.HeapMemoryUsage.Method.get(used)	MBean	Utiliza o atributo HeapMemoryUsage a partir do MBean e obtém o resultado do método get(valor da sequência). A sequência utilizada é passada para o método como o argumento. Somente 1 argumento pode ser fornecido e ele deve ser um valor de sequência literal. Mostra como é possível coletar dados de uma estrutura de dados composta do MBean.

`Domínio` e `Propriedade` podem ser usados como palavras-chave em valores secundários se o valor anterior retornou uma Sequência no formato de um nome MBean. Por exemplo:

Amostra de nome de métrica	Tipo de grupo de atributos	Descrição dos dados retornados
`Attribute.jdbcDriver.Property.name`	MBean	O atributo jdbcDriver retorna um nome MBean, e sua propriedade-chave, nome, é extraída do nome MBean.
`Attribute.jdbcDriver.Domain`	MBean	O atributo jdbcDriver retorna um nome MBean, e o domínio é extraído do nome MBean.

As palavras-chave `ElementCount` e `Explode` executam operações em matrizes ou coleções de dados.

- `ElementCount` – retorna o número de elementos em uma matriz.
- `Explode` – explode uma linha em várias linhas, uma nova linha para cada elemento de uma matriz.

Exemplos de Cada uma das Palavras-Chaves:

Amostra de nome de métrica	Tipo de grupo de atributos	Descrição dos dados retornados
Attribute.deployedObjects.ElementCount	MBean	O atributo MBean deployedObjects é uma matriz e esta coluna contém o número de elementos na matriz.
Attribute.deployedObjects.Explode.MBean.Property.j2eeType	MBean	Faz com que a tabela tenha 1 linha para cada elemento nos objetos implementados. Esta coluna contém j2eeType do Objeto implementado.
Attribute.SystemProperties.Method.values.Explode.Method.get(key)	MBean	Faz você obter uma nova linha para cada entrada em uma estrutura de dados tabular do MBean aberta. Cada estrutura de dados tabular contém uma estrutura de dados composta com um item denominado `chave`, que é retornado.

Testando Grupos de Atributos JMX
É possível testar o grupo de atributos JMX que você criou no Agent Builder.

Procedimento

1. É possível iniciar o procedimento de Teste das seguintes maneiras:
   - Durante a criação do agente, clique em **Testar** na página **Informações de JMX**.
   - Após a criação do agente, selecione um grupo de atributos no Agent Editor **Definição de Origem de Dados** e clique em **Testar**. Para obter informações adicionais sobre o Agent Editor, consulte “Usando o Agent Editor para modificar o agente” na página 1172.

   Após clicar em **Testar** em uma das duas etapas anteriores, a janela **Teste de JMX** é exibida
2. Selecione uma conexão na lista disponível em **Nome de Conexão** ou, alternativamente, clique em **Incluir** para incluir uma conexão e siga o procedimento detalhado em “Monitorando MBeans Java Management Extensions (JMX)” na página 1240.
3. Opcional: Antes de iniciar seu teste, é possível configurar as variáveis de ambiente, as propriedades de configuração e as informações Java.

   Para obter mais informações, consulte “Teste de Grupo de Atributos” na página 1380. Para obter mais informações sobre a configuração de JMX, consulte “Configuração do JMX” na página 1247.
4. Clique em **Iniciar Agente**.

   Uma janela indica que o Agente está iniciando.

5. Clique em **Coletar Dados** para simular uma solicitação a partir do Tivoli Enterprise Portal ou SOAP para os dados do agente.

   O agente monitora os dados do Servidor JMX. A janela **Teste de JMX** coleta e mostra quaisquer dados no cache do agente, desde que ele tenha iniciado por último.
6. Opcional: Clique em **Verificar Resultados**, se os dados retornados não estiverem conforme o esperado.

   A janela **Status de Coleção de Dados** é aberta e mostra informações adicionais sobre os dados. Os dados coletados e exibidos pela janela Status da Coleção de Dados são descritos em "Nó de Status do Objeto de Desempenho" na página 1424
7. Pare o agente, clicando em **Parar Agente**.
8. Clique em **OK** ou **Cancelar** para sair da janela **Teste de JMX**. Clicar em **OK** salva quaisquer mudanças que tiver feito.

Conceitos relacionados

"Testando seu agente no Agent Builder" na página 1380
Depois de usar o Agent Builder para criar um agente, será possível testar o agente no Agent Builder.

Monitorando dados a partir de um Common Information Model (CIM)

É possível definir uma origem de dados para receber dados de uma origem de dados do Modelo de Informação Comum (CIM). Uma origem de dados monitora uma única classe CIM e posiciona todos os valores desta classe no conjunto de dados que ela produz. Se a classe fornecer diversas instâncias, o conjunto de dados terá linhas múltiplas; é possível filtrar por nome de instância para garantir que o conjunto de dados tenha uma linha.

Sobre Esta Tarefa

Essa tarefa descreve as etapas para configurar uma origem de dados do Modelo de Informação Comum (CIM).

Procedimento

1. Na página **Origem de Dados Inicial do Agente** ou na página **Localização de Origem de Dados**, clique em **Dados de um servidor** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **CIM**.
3. Clique em **Avançar**.
4. Na página **Informações do Modelo de Informação Comum (CIM)**, na área **Informações do CIM**, faça uma das opções a seguir:
   - Preencha os campos **Espaço de Nomes** e **Nome da Classe do CIM** para os dados que você deseja coletar.
   - Clique em **Procurar** para procurar um repositório do CIM em um sistema específico.

     A janela **Navegador de Classe do Modelo de Informação Comum (CIM)** é exibida. Esse navegador conecta-se a um servidor CIM e fornece informações sobre as classes que existem nesse servidor.

     Para navegar em um sistema remoto, selecione na lista **Nome do Host** (se um estiver definido). Alternativamente, clique em **Incluir** para incluir o nome do host do sistema em que o servidor CIM está localizado.

     A sintaxe para especificar o nome do host é `http[s]://`*`hostname`*`:`*`port`*. Se você fornecer o nome do host apenas, o Navegador de Classe do Modelo de Informação Comum (CIM) conecta-se usando uma URL padrão de `http://`*`hostname`*`:5988`.

     Se você fornecer um protocolo sem especificar uma porta, 5988 é usado como o padrão para `http` ou 5989 como padrão para `https`.

     Se você fornecer uma porta sem especificar um protocolo, `http` é usado com a porta fornecida.

Forneça um ID do usuário e senha para uma conta com permissão de leitura para objetos no namespace que você deseja navegar. A janela é atualizada com as informações para o sistema remoto.

O Agent Builder tenta descobrir os namespaces disponíveis no Servidor CIM. Os namespaces descobertos são exibidos na lista **Namespace**. No entanto, o Agent Builder talvez não possa descobrir todos os espaços de nomes que estão disponíveis no servidor. Se você deseja navegar por um namespace que não está incluído na lista **Namespace**, clique no ícone de mais (+) próximo à lista **Namespace**. Insira o nome do espaço de nomes no campo e clique em **OK**. Se o namespace estiver presente no servidor CIM, as classes definidas no namespace serão listadas. Os namespaces que você digitar são salvos e colocados na lista **Namespace** na próxima vez que você navegar nesse servidor CIM em particular.

Quando selecionar um namespace da lista **Namespace**, o Agent Builder coleta todas as informações de classe desse namespace em particular. Em seguida, o Agent Builder armazena estas informações em cache para que seja possível comutar entre espaços de nomes rapidamente. Se desejar forçar o Agent Builder a coletar novamente as informações de classe de um determinado namespace, selecione o namespace e clique em **Conectar**. Clicando em **Conectar** elimina-se todas as informações em cache, e faz com que o Agent Builder colete novamente as informações de classe.

Você pode clicar no ícone **Procurar** (binóculos) para localizar sua seleção na lista. Digite uma frase no campo **Procurar frase**; especifique sua preferência clicando nos campos **Procurar pelo nome** ou **Procurar por propriedades de classe**; e clique em **OK**. Se localizar o item que está procurando, selecione-o e clique em **OK**.

5. Na página Informações sobre o Common Information Model (CIM), área **Sistema Operacional**, selecione os sistemas operacionais nos quais a coleta ocorrerá.
6. Se você digitou o Namespace e o nome da classe do CIM na área **Informações do CIM**, execute as etapas a seguir:
   a) Clique em **Avançar** para exibir a página **Informações sobre o Atributo** e definir o primeiro atributo no grupo de atributos.
   b) Especifique as informações sobre a página **Informações sobre o Atributo**, e clique em **Concluir**.
7. Se você procurou as informações sobre o CIM, a página Selecionar Atributos-chave será exibida. Na página Selecionar Atributos-chave, selecione os atributos-chave ou indique que esta origem de dados produz somente uma linha de dados. Para obter mais informações, consulte (“Selecionando Atributos-Chaves” na página 1172).
8. Se você navegou para as informações do CIM, clique em **Concluir**.
9. Opcional: Você pode testar este grupo de atributos, clicando em **Testar**. Para obter informações adicionais sobre teste, consulte “Testando Grupos de Atributos CIM” na página 1261
10. Opcional: É possível criar um filtro para limitar os dados retornados por esse grupo de atributos clicando em **Avançado**. Para obter informações adicionais sobre filtragem de dados de um grupo de atributos, consulte “Filtrando Grupos de Atributos” na página 1201
11. Execute uma das seguintes etapas:
    a) Se estiver usando o assistente de **Agente**, clique em **Avançar**.
    b) Clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor.

Configuração do CIM
Detalhes sobre as propriedades de configuração CIM.

Se você definir uma origem de dados do CIM em seu agente, as propriedades de configuração do CIM serão incluídas no agente automaticamente. É possível visualizar, incluir e alterar as propriedades de configuração usando o Agent Editor. Para obter instruções, consulte “Alterando Propriedades de Configuração Usando o Agent Editor” na página 1367). Se uma origem de dados do CIM for definida em um subnó, especifique Substituições de Configuração do Subnó. Para obter instruções, veja “Configuração do subnó” na página 1354.

As propriedades de configuração específicas de conexão a seguir estão na página de configuração do CIM:

CIM Local ou Remoto
Autenticação local ou remota para o servidor CIM. O valor Padrão Local/Remoto é Remoto

ID do usuário do CIM
O ID do usuário para acesso ao servidor do CIM

Senha do CIM
A senha para acessar o servidor do CIM

Nome do host do CIM
O nome do host a ser acessado para dados do CIM

CIM sobre SSL
Utilize SSL para comunicação com o servidor CIM. As opções são Sim e Não. O valor padrão é Não.

Número da porta CIM
O número da porta usada para comunicação que não é segura.

Número da porta SSL do CIM
O número da porta usada para comunicação segura. O valor padrão é 5989. (O valor padrão para Solaris 8 normalmente é diferente).

Testando Grupos de Atributos CIM
É possível testar o grupo de atributos CIM criado no Agent Builder.

Procedimento

1. Inicie o procedimento de Teste das seguintes maneiras:
   - Durante a criação do agente, clique em **Testar** na página **Informações de CIM**.
   - Após a criação do agente, selecione um grupo de atributos no Agent Editor **Definição de Origem de Dados** e clique em **Testar**. Para obter informações adicionais sobre o Agent Editor, consulte "Usando o Agent Editor para modificar o agente" na página 1172

   Após clicar em **Testar** em uma das duas etapas anteriores, a janela **Testar Configurações** é exibida
2. Opcional: Configure as variáveis de ambiente e as propriedades de configuração antes de iniciar o teste.

   Para obter mais informações, consulte "Teste de Grupo de Atributos" na página 1380.
3. Selecione ou inclua um **Nome do Host**.

   Para obter mais informações sobre a inclusão de um **Nome do Host**, consulte "Monitorando dados a partir de um Common Information Model (CIM)" na página 1259
4. Clique em **Iniciar Agente**.

   Uma janela é aberta indicando que o Agente está iniciando.
5. Para simular uma solicitação a partir do Tivoli Enterprise Portal ou SOAP para dados do agente, clique em **Coletar Dados**.

   O agente consulta os dados do Servidor CIM. A janela **Testar Configurações** coleta e mostra dados no cache do agente, desde que ele tenha iniciado por último.
6. Opcional: Clique em **Verificar Resultados**, se os dados retornados não estiverem conforme o esperado.

   A janela **Status de Coleção de Dados** é aberta e mostra informações adicionais sobre os dados. Os dados que são coletados e exibidos pela janela **Status de Coleção de Dados** são descritos em "Nó de Status do Objeto de Desempenho" na página 1424
7. Pare o agente, clicando em **Parar Agente**.
8. Clique em **OK** ou **Cancelar** para sair da janela **Testar Configurações**. Clicar em **OK** salva quaisquer mudanças que tiver feito.

Conceitos relacionados
"Testando seu agente no Agent Builder" na página 1380

Depois de usar o Agent Builder para criar um agente, será possível testar o agente no Agent Builder.

Monitorando um Arquivo de Log

É possível definir uma origem de dados para receber dados de um arquivo de log de texto. O agente analisa periodicamente as linhas incluídas no arquivo de log e produz as informações de evento com base nessas linhas. É possível configurar a maneira que o agente analisa o log nos eventos. Também é possível configurar o agente para filtrar e resumir os dados. Os eventos resultantes são colocados em um conjunto de dados.

Antes de Iniciar

Nota: O agente monitora os arquivos de log que usam o mesmo código de idioma e página de códigos em que o agente é executado.

Procedimento

1. Na página **Origem de Dados Inicial do Agente** ou na página **Local de Origem de Dados**, clique em **Dados Registrados** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **Um Arquivo de Log**.
3. Clique em **Avançar**.
4. Na página **Informações de Arquivo de Log**, digite o nome do arquivo de log que você deseja monitorar na área **Informações de Arquivo de Log**.

   O nome do arquivo deve ser completo.

   a) Opcional: Parte do nome do arquivo de log pode vir de uma propriedade de configuração do tempo de execução. Para criar um nome do arquivo de log, clique em **Inserir Propriedade de Configuração** e selecione uma propriedade de configuração.

   b) Opcional: O arquivo também pode ser um nome do arquivo dinâmico. Para obter mais informações, consulte (“Suporte ao Nome de Arquivo Dinâmico” na página 1502).
5. Na área **Identificação de Campo**, clique em uma das seguintes opções:

   Número fixo de caracteres
   Quando selecionada, limita o número de caracteres.

   Com essa opção, é designado a cada atributo o número máximo de caracteres que ele pode reter no arquivo de log. Por exemplo, se houver três atributos A, B e C (nessa ordem), e cada atributos for uma Sequência de comprimento máximo 20. Em seguida, os primeiros 20 bytes do registro de log vão para A, os segundos 20 para B e próximos 20 para C.

   Separador de guia
   Quando selecionada, você pode usar separadores de guias.

   Separador de Espaço
   Quando selecionado, diversos espaços simultâneos podem ser usados como um separador único.

   Texto do Separador
   Quando selecionada, digite o texto do separador.

   Iniciar e Encerrar Texto
   Quando selecionada, digite tanto o texto de Início quanto o de Fim.

   XML no elemento
   Quando selecionado, digite o nome do elemento XML para utilizar como o registro ou clique em **Navegar** para definir o elemento.

   Se você clicou em **Procurar**, a janela **Navegador XML** será exibida. Se você usar a função de procura, o Agent Builder identificará todos possíveis atributos do registro examinando as tags filhas e seus atributos.

   Nota: A menos que clique em **Avançado** e preencha as informações nessa janela, são feitas as suposições a seguir sobre as informações que você completa:

- Apenas um arquivo de log é monitorado por vez.
- Cada linha no arquivo de log contém todos os campos necessários para preencher os atributos a serem definidos.

Para obter informações adicionais sobre a análise de arquivo de log e separadores, consulte ("Análise do Arquivo de Log e Separadores" na página 1270).

6. Opcional: Clique em **Avançado** na página **Informações de Arquivo de Log** para executar o seguinte usando a página **Propriedades de Origem de Dados Avançadas**:
   - Monitore mais de um arquivo, ou monitore arquivos com nomes diferentes em sistemas operacionais diferentes ou monitore arquivos com nomes que correspondem a expressões regulares.
   - Extrair um conjunto de campos de mais de uma linha no arquivo de log.
   - Escolha **Filtragem de Eventos e Opções de Resumo**.
   - Produzir informações de resumo de saída. Este resumo produz um grupo de atributos adicional em cada intervalo. Para obter informações adicionais sobre este grupo de atributos, consulte "Resumo do Arquivo de Log" na página 1436. Esta função é reprovada pelas opções disponíveis na guia Informações de Evento.

   a) Para monitorar mais de um arquivo de log, clique em **Incluir** e digite o nome.

      Se mais de um arquivo for listado, um único rótulo deverá ser digitado para cada arquivo. O rótulo pode ser exibido como um atributo para indicar qual arquivo gerou o registro. Ele não deve conter espaços.

   b) Opcional: Para selecionar os sistemas operacionais em que cada arquivo de log deve ser monitorado, siga estas etapas:

      1) Clique na coluna **Sistemas Operacionais** do arquivo de log.
      2) Clique em **Editar**.
      3) Na janela **Sistemas Operacionais**, selecione os sistemas operacionais.
      4) Clique em **OK** para salvar suas mudanças e retornar à página **Propriedades Avançadas da Origem de Dados**.

   c) Opcional: Selecione **Nomes de arquivos correspondem à expressão regular** se o nome do arquivo que você está fornecendo for uma expressão regular que seja usada para localizar o arquivo em vez de ser um nome de arquivo.

      Para obter mais informações, consulte "Expressões Regulares ICU" na página 1492. Se você não verificar esta caixa, o nome deve ser um nome de arquivo real. Como alternativa, ele deve ser um padrão que segue as regras para padrões de nomes de arquivos que são descritos em "Sintaxe do Nome do Arquivo Dinâmico" na página 1503.

   d) Opcional: Selecione **Um elemento de diretório corresponde a expressão regular** para corresponder um subdiretório do caminho do nome de arquivo a uma expressão regular.

      Você pode selecionar essa opção apenas se também selecionou **Nomes de arquivo correspondem a expressão regular** na etapa anterior.

      Se os metacaracteres de expressão regular forem usados no nome do caminho, os metacaracteres poderão ser usados em apenas um subdiretório do caminho. Por exemplo, é possível especificar `/var/log/[0-9\.]*/mylog.*` para ter metacaracteres em um subdiretório. O `[0-9\.]*` resulta na correspondência de qualquer subdiretório do `/var/log` que consiste unicamente em número e pontos `(.)`. O `mylog.*` resulta na correspondência de quaisquer nomes de arquivo nesses subdiretórios `/var/log` que começam com `mylog` e são seguidos por zero ou mais caracteres.

      Como alguns sistemas operacionais usam a barra invertida `(\)` como um separador de diretórios, isto pode ser confundido com um metacaractere de escape de expressão regular. Devido a esta confusão, barras sempre devem ser usadas para indicar os diretórios. Por exemplo, arquivos do Windows que são especificados como `C:\temp\mylog.*` podem significar que o `\t` é um caractere de tabulação de atalho. Portanto, sempre use barras `(/)` em todos os sistemas

operacionais para separadores de diretórios. O exemplo de `C:/temp/mylog.*` representa todos os arquivos no diretório `C:/temp` que iniciam com `mylog`.

e) Na lista **Quando Vários Arquivos Correspondem**, selecione uma das opções a seguir:

- **O arquivo com maior valor numérico no nome do arquivo**
- **O maior arquivo**
- **O arquivo atualizado mais recentemente**
- **O arquivo criado mais recentemente**
- **Todos os arquivos correspondentes**

Nota: Ao selecionar **Todos os Arquivos Correspondentes**, o agente identifica todos os arquivos no diretório que corresponde ao padrão de nome do arquivo dinâmico. O agente monitora atualizações em todos os arquivos em paralelo. Os dados de todos os arquivos são mesclados durante o processo de coleta de dados. É melhor incluir um atributo selecionando **Nome do Arquivo de Log** em **Informações do Campo de Registro** para correlacionar as mensagens de log com os arquivos de log que contêm as mensagens de log. Assegure que todos os arquivos que correspondem ao padrão do nome do arquivo dinâmico possam ser divididos em atributos de uma maneira consistente. Se os arquivos de log selecionados não puderem ser analisados de forma coerente, então, será melhor selecionar **Registro Inteiro** em **Informações do Campo de Registro** para definir um único atributo. Para obter informações adicionais sobre a especificação de **Informações do Campo de Registro** para atributos, consulte a etapa (“8” na página 1266).

f) Escolha como o arquivo é processado.

Com **Processar todos os registros quando o arquivo for amostrado**, você pode processar todos os registros no arquivo inteiro sempre que o intervalo de amostragem definido para o monitor de log expirar. O intervalo padrão é 60 segundos. Este intervalo pode ser modificado usando a variável de ambiente *KUMP_DP_COPY_MODE_SAMPLE_INTERVAL* (especificando um valor em segundos). Os mesmos registros são relatados todas as vezes a menos que sejam removidos do arquivo. Com esta seleção, os dados do evento não são produzidos quando novos registros são gravados no arquivo. Com **Processar novos registros anexados ao arquivo**, é possível processar novos registros anexados ao arquivo enquanto o agente está em execução. Um registro de eventos é produzido para cada registro incluído no arquivo. Se o arquivo for substituído (primeiro registro alterado de alguma maneira), o arquivo será processado e um evento será produzido para cada registro no arquivo.

Nota: Se estiver anexando registros em um arquivo de log XML, os registros de anexo devem conter um conjunto completo de elementos que são definidos no elemento XML que você selecionou como **Identificação de Campo**.

g) Se você escolher processar os novos registros que são anexados ao arquivo, também é possível escolher como novos registros são detectados.

Com **Detectar novos registros quando aumentar a contagem de registros**, novos registros podem ser detectados quando o número de registros no arquivo aumentar, independentemente de o tamanho do arquivo ser alterado. Esse recurso é útil quando um arquivo de log inteiro for pré-alocado antes que qualquer registro seja gravado no arquivo. Esta opção pode ser selecionada para arquivos que não são pré-alocados, mas é menos eficiente do que o monitoramento do tamanho do arquivo. Com **Detectar novos registros quando o tamanho do arquivo aumentar**, você pode determinar quando uma nova entrada é anexada em um arquivo de forma típica. Pode haver um pequeno atraso no reconhecimento de que um arquivo monitorado é substituído.

h) Se você selecionou **Detectar Novos Registros Quando o Tamanho do Arquivo Aumentar**, também é possível escolher como processar um arquivo que existe quando o agente de monitoramento iniciar.

Ignorar registros existentes desativa a produção para todos os registros no arquivo no momento que o agente é iniciado. **Processar ___ registros existentes a partir do arquivo** especifica a produção de um evento para um número fixo de registros do final do arquivo no horário em que o agente for iniciado. **Processar registros não processados anteriormente pelo agente**: Especifica o reinício dos dados a serem mantidos pelo agente de monitoramento para que o agente saiba

quais registros foram processados na última vez que ele foi executado. Eventos são produzidos para todos os registros que forem anexados ao arquivo desde a última vez que o agente foi executado. Esta opção envolve um pouco processamento extra toda vez que um registro é incluído no arquivo.

i) Se você selecionou **Processar Registros Não Processados Anteriormente pelo Agente**, é possível escolher o que fazer quando o agente for iniciado e aparentemente o arquivo existente tiver sido substituído.

Processar todos os registros se o arquivo foi substituído: Se as informações sobre o arquivo monitorado e as informações de dados de reinicialização não corresponderem, os eventos serão produzidos para todos os registros no arquivo. Os exemplos de incompatibilidade incluem: O nome do arquivo é diferente, o tempo de criação do arquivo é diferente, o tamanho do arquivo diminuiu e o horário da última modificação do arquivo é mais recente do que antes. **Não processar registros se o arquivo tiver sido substituído**: Se as informações sobre o arquivo monitorado e as informações de dados de reinicialização não corresponderem, o processamento de registros existentes no arquivo é desativado.

j) Clique na guia **Identificação de Registro** para interpretar diversas linhas no arquivo de log como um único registro lógico.

Nota: Se você selecionar **XML no elemento** como a identificação de campo na página **Informações de Arquivo de Log**, a guia **Identificação de Registro** não será exibida.

- A **Linha Única** interpreta cada linha como um registro lógico único.
- **Linha Separadora**, você pode inserir uma sequência de caracteres que identifica uma linha que separa um registro de outro.

  Nota: A linha separadora não faz parte do registro anterior ou seguinte.
- A **regra** identifica um número máximo de linhas que compõem um registro e, opcionalmente, uma sequência de caracteres que indicam o início ou o término de um registro. Com a **Regra**, é possível especificar as seguintes propriedades:
  - A **linha máxima não em branco** define o número máximo de linhas não em branco que podem ser processadas por uma regra.
  - **Tipo de Regra**: Pode ser um dos seguintes:
    - **Nenhuma comparação de texto** (A Máximo de linhas por registro indica um registro lógico único).
    - **Identificar o Início do Registro** (Marca o início do registro lógico único).
    - **Identificar o Término do Registro** (Marca o término do registro lógico único).
  - **Deslocamento**: Especifica o local dentro de uma linha em que a Sequência de Comparação deve ocorrer.
  - **Teste de Comparação**: Pode ser **Igual a**, solicitando que uma sequência de caracteres seja correspondente no deslocamento específico ou **Não Igual a**, indicando que uma determinada sequência de caracteres não ocorra no deslocamento específico.
  - **Sequência de Comparação** define a sequência de caracteres a serem comparados.
- **Expressão Regular** identifica um padrão usado para indicar o início ou o término de um registro. Usando a **Expressão Regular**, é possível especificar as seguintes propriedades:
  - **Sequência de Comparação** define a sequência de caracteres a serem correspondidos.

    OU
  - Início ou término do registro:
    - **Identificar o início do registro** marca o início do registro lógico único.
    - **Identificar o término do registro** marca o término do registro lógico único.

k) Se você selecionou **Processar todos os registros quando o arquivo estiver amostrado** antes, clique na guia **Expressão do Filtro**. Ao clicar em **Expressão de Filtro**, será possível filtrar os

dados que são retornados como linhas baseadas nos valores de um ou mais atributos, variáveis de configuração ou ambos.

Se você selecionou **Processar Novos Registros Anexados ao Arquivo** anteriormente, não poderá criar uma expressão de filtro. Para obter informações adicionais sobre filtragem de dados de um grupo de atributos, consulte ("Filtrando Grupos de Atributos" na página 1201).

l) Se você selecionou **Processar novos registros anexados ao arquivo** antes, clique na guia **Informações do Evento** para selecionar **Filtragem de Eventos e Opções de Resumo**.

Para obter mais informações, consulte ("Filtro de eventos e resumo" na página 1408).

Nota: A guia Resumo poderá estar presente se o agente foi criado com uma versão anterior do Agent Builder. A guia de resumo agora está descontinuada pela guia Informações de Evento

7. Opcional: Clique em **Testar configurações do arquivo de log** na página **Informações do arquivo de log** para iniciar e testar a origem de dados. . Clique em **Testar Configurações do Arquivo de Log** depois de selecionar as opções para a origem de log. Ao testar a origem de dados do arquivo de log e fornecer conteúdo do arquivo de log, o Agent Builder cria os atributos no grupo automaticamente, com base nos resultados da análise de log. Para obter informações adicionais sobre teste, consulte "Testando Grupos de Atributos do Arquivo de Log" na página 1271.
8. Use as etapas a seguir, se você não usou a função de teste anterior e digitou o nome do arquivo de log na área **Informações de Arquivo de Log** da página **Informações de Arquivo de Log**:
   a) Clique em **Avançar** para exibir a página **Informações sobre o Atributo** e definir o primeiro atributo no grupo de atributos.
   b) Especifique as informações, na página **Informações sobre o Atributo** e clique em **Concluir**.

   Nota: Quando um grupo de atributos do arquivo de log for incluído em um agente na versão mínima padrão do Tivoli Monitoring (6.2.1) ou posterior, um grupo de atributos `Status do Arquivo de Log` será incluído. Para obter informações adicionais sobre o grupo de atributos `Status do Arquivo de Log`, consulte ("Grupo de Atributos de Status do Arquivo de Log" na página 1466).

   Juntamente com os campos aplicáveis a todas as origens de dados, a página **Informações de Atributo** para a origem de dados do arquivo de log possui alguns campos adicionais na área **Informações de Campo de Registro**.

   Os campos **Informações do Campo de Registro** são:

   Próximo campo
   Mostra o próximo campo após a análise, usando os delimitadores do grupo de atributos (ou delimitadores especiais para este atributo a partir do diálogo Avançado).

   Restante do Registro
   Mostra o restante do registro após os atributos anteriores serem analisados. Este atributo é o último atributo, exceto para, possivelmente, o nome do arquivo de log ou o rótulo do arquivo de log.

   Registro inteiro
   Mostra o registro inteiro, o qual pode ser o único atributo, exceto para, possivelmente, o nome do arquivo de log ou o rótulo do arquivo de log.

   Nome do arquivo de registro
   Mostra o nome do arquivo de log.

   Rótulo do arquivo de log
   Mostra o rótulo que é designado ao arquivo no painel avançado.

   Nota: Use a guia **Detalhes de Atributos Derivados** apenas se você deseja um atributo derivado, e não um atributo diretamente do arquivo de log.
9. Clique em **Avançado** na área **Informações do Campo de Registro** para exibir a página **Informações sobre o Atributo do Arquivo de Log Avançado**.
   a) Na seção **Filtros de Atributos**, especifique os critérios para os dados a serem incluídos ou excluídos.

Filtrar atributos pode melhorar o desempenho de sua solução reduzindo a quantidade de dados processada. Clique em um ou mais dos filtros de atributos:

- **Inclusivo** indica que o conjunto de filtros de atributos é um filtro de aceitação, o que significa que se o filtro tiver êxito, o registro passará pelo filtro e será a saída.
- **Exclusivo** indica que o conjunto de filtros do atributo é um filtro de rejeição, o que significa que, se o filtro do atributo tiver êxito, o registro será rejeitado e não será a saída.
- **Corresponder Todos os Filtros** indica que todos os filtros definidos para o filtro devem corresponder ao registro do atributo para que o filtro tenha êxito.
- **Corresponder Qualquer Filtro** indica que, se qualquer um dos filtros definidos para o filtro corresponder ao registro do atributo, o filtro terá êxito.

b) Use **Incluir**, **Editar** e **Remover** para definir os filtros individuais para um conjunto de filtros de atributos.

c) Para incluir um filtro, siga estas etapas:

1) Clique em **Incluir** e conclua as opções na janela **Incluir Filtro**, conforme a seguir:

a) A seção **Critérios de Filtragem** define as características base do filtro, incluindo as seguintes propriedades:

- **Deslocamento Inicial** define a posição na sequência de atributos onde a comparação deve iniciar.
- **Cadeia de Comparação** define a cadeia de padrão na qual o atributo é definido.

  Digite uma sequência, padrão ou expressão regular que seja usado pelo agente para filtrar os dados lidos a partir do arquivo. Os registros que correspondem ao padrão de filtro são eliminados dos registros que são retornados ao ambiente de monitoramento ou são os únicos registros retornados. O resultado depende de você escolher o filtro para ser inclusivo ou exclusivo.
- **Corresponder Valor Inteiro** verifica por uma ocorrência exata da sequência de comparação na sequência de atributos. A verificação inicia da posição de deslocamento inicial.
- **Corresponder Qualquer Parte do Valor** verifica a sequência de comparação em qualquer lugar na sequência de atributos. A verificação inicia da posição de deslocamento inicial.

b) **A sequência de comparação é uma expressão regular** indica que a sequência de comparação é um padrão de expressão regular que pode ser aplicado em relação à sequência de atributos.

O suporte de filtragem de expressão regular é fornecido usando as bibliotecas International Components for Unicode (ICU) para verificar se o valor de atributo examinado corresponde ao padrão especificado.

Para usar de forma efetiva o suporte à expressão regular, você deve estar familiarizado com as especificações de como o ICU implementa as expressões regulares. Esta implementação não é idêntica a como o suporte de expressão regular é implementado em expressões regulares `Perl`, `grep`, `sed`, Java e outras implementações. Consulte o "Expressões Regulares ICU" na página 1492 para obter orientação sobre a criação de filtros de expressão regular.

c) **Definir um Filtro de Substituição** indica que você deseja fornecer uma comparação de filtro mais específica que substitui as características base definidas anteriormente. Essa sequência de comparação adicional é usada para reverter o resultado do filtro. Quando o filtro for **Inclusivo**, a substituição agirá como um qualificador de exclusão para a expressão de filtro. Quando o filtro for **Exclusivo**, a substituição agirá como um qualificador de inclusão para a expressão de filtro. (Para obter mais informações sobre **Inclusivo** e **Exclusivo**, consulte a etapa "9" na página 1266 e os exemplos que seguem). O filtro de substituição possui as seguintes propriedades:

- **Deslocamento Inicial** define a posição na sequência de atributos onde a comparação deve iniciar.
- **Sequência de Comparação** define a sequência padrão em relação a qual o atributo é correspondido.

  Digite uma expressão regular que será usada pelo agente para filtrar os dados lidos a partir do arquivo. Os registros que correspondem ao padrão de filtro são eliminados dos registros que são retornados ao ambiente de monitoramento ou são os únicos registros retornados. O resultado depende de você escolher o filtro para ser inclusivo ou exclusivo.

d) **Valor de Substituição** pode ser usado para alterar a cadeia de atributos brutos com um novo valor. Consulte "Expressões Regulares ICU" na página 1492 para obter mais detalhes sobre os caracteres especiais que podem ser usados.

e) **Substituir Primeira Ocorrência** substitui a primeira ocorrência que correspondida pela sequência de comparação com um novo texto.

f) **Substituir Todas as Ocorrências** substitui todas as ocorrências que são correspondidas pela cadeia de comparação com um novo texto.

2) Clique em **OK**.

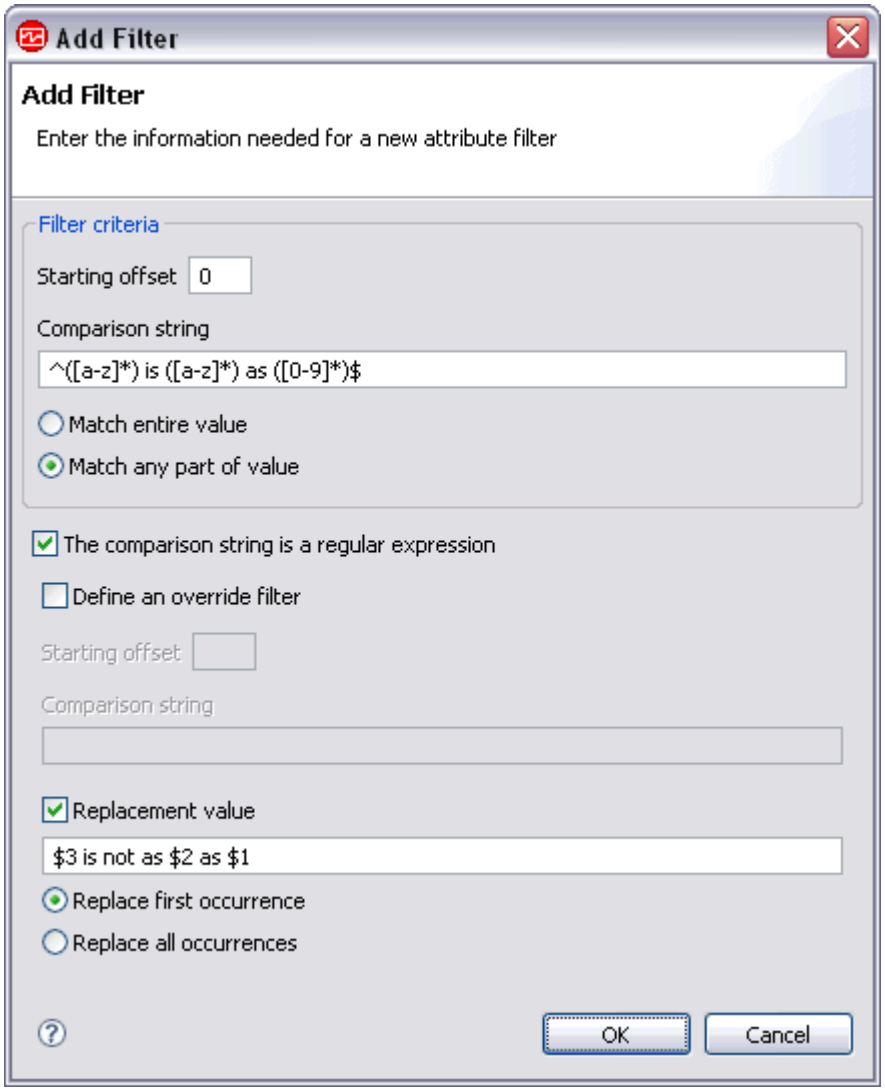


*Figura 38. **Incluir Filtro** - exemplo 1*

Se a sequência de atributos for `abc is easy as 123`, então, a sequência substituída exibida no Tivoli Enterprise Portal ou no console do IBM Cloud Application Performance Management será `123 is not as easy as abc`.

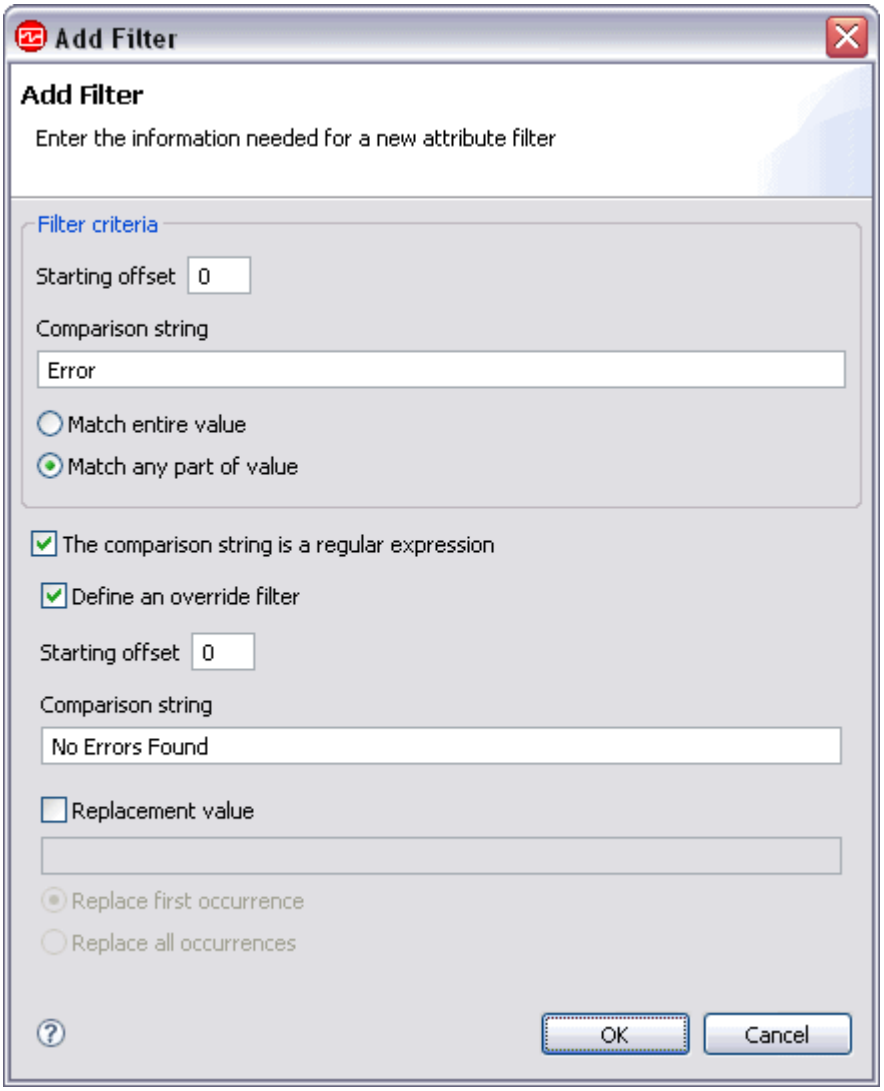


*Figura 39. **Incluir Filtro** - exemplo 2*

Se a sequência de atributos for `Erro Irrecuperável ao ler a partir do disco` e o filtro for **Inclusivo**, o atributo será exibido no console do Tivoli Enterprise Portal ou do IBM Cloud Application Performance Management. Se a sequência de atributos for `Nenhum Erro Localizado durante o backup semanal` e o filtro for **Inclusivo**, o atributo não será exibido.

d) Na seção **Identificação de Campo** da página **Informações sobre o Atributo do Arquivo de Log Avançado**, especifique como substituir os delimitadores de campo do grupo de atributos somente para esse único atributo. Clique em um dos filtros de atributos e preencha os campos necessários para a opção:

- **Número de Caracteres**: Insira o limite para o número de caracteres.
- **Separador de Guias** especifica o uso dos separadores de guias.
- **Texto Separador**: Insira o texto separador que você deseja usar.
- **Texto de Início e Término** Insira o texto de **Início** e o texto de **Término**.

e) Na seção **Resumo** da página **Informações sobre o Atributo do Arquivo de Log Avançado**, clique na caixa de seleção **Incluir atributo no grupo de atributos de resumo** para incluir o atributo no grupo de atributos de resumo.

Este grupo de atributos é produzido quando um usuário ativa a sumarização do atributo de log.

f) Clique em **OK**.

10. Se você usou a função de teste na etapa ("7" na página 1266), a página **Selecionar Atributos-chave** será exibida. Na página **Selecionar Atributos-chave**, selecione os atributos-chave ou indique que esta origem de dados produz apenas uma linha de dados.

    Para obter mais informações, consulte ("Selecionando Atributos-Chaves" na página 1172).

11. Execute uma das seguintes etapas:

    - Se você estiver usando o assistente de Novo Agente, clique em **Avançar**.
    - Clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor.

    Nota: Quando um grupo de atributos do arquivo de log for incluído em um agente na versão mínima padrão do Tivoli Monitoring (6.2.1) ou posterior, um grupo de atributos `Status de Arquivo de Log` será incluído. Para obter informações adicionais sobre o grupo de atributos `Status do Arquivo de Log`, consulte ("Grupo de Atributos de Status do Arquivo de Log" na página 1466).

Análise do Arquivo de Log e Separadores

É possível alterar o separador padrão usado para separar um ou mais atributos em um registro de arquivo de log.

Ao criar um grupo de atributos do arquivo de log, um separador é designado por padrão. O separador padrão é uma guia. O separador é usado pelo agente para analisar e delimitar os dados de cada atributo na linha de dados. Você pode alterar o separador de atributo padrão para ser:

- Um número fixo de caracteres
- Um espaço
- Um caractere diferente ou caracteres
- Um início e final de texto específico
- Um elemento XML.

Você alterar o separador padrão que é utilizado para todos os atributos no grupo das seguintes maneiras:

1. Quando você estiver criando o grupo de atributos, na página **Informações de Arquivo de Log**.
2. Após criar o grupo de atributos, abrindo a guia **Origens de Dados do** > **Agent Editor**, selecionando o grupo de atributos e escolhendo um separador na área **Identificação de Campo** .

Também é possível designar separadores específicos para um ou mais atributos individuais. É possível designar separadores específicos para atributos individuais para usar:

- Um número fixo de caracteres.
- Um separador de guia
- Um separador de espaço
- Um caractere diferente ou caracteres
- Um início e final de texto específico.

Você altera o separador que é utilizado para atributos individuais das seguintes maneiras:

1. Selecionando **Avançado** na página **Informações sobre o Atributo** quando estiver criando um atributo.
2. Abrindo a guia **Agent Editor** > **Origens de Dados**, selecionando o atributo e selecionando **Avançado** na guia **Informações sobre o Atributo do Arquivo de Log**.

Exemplo 1 - Saída de Arquivo de Log Simples

Alguns registros do arquivo de log possuem separadores claros e regulares, por exemplo:

```
um, dois três
```

Aqui, o caractere " , " é um separador claro e regular entre as três partes de dados na linha. Neste caso, selecione **Texto Separador** e especifique " , " como o separador padrão para o grupo de atributos. Não é necessário alterar ou definir outros separadores.

Definindo esse separador para um arquivo de log que contém a linha de dados que é mostrada anteriormente neste exemplo que é mostrado na seguinte saída:

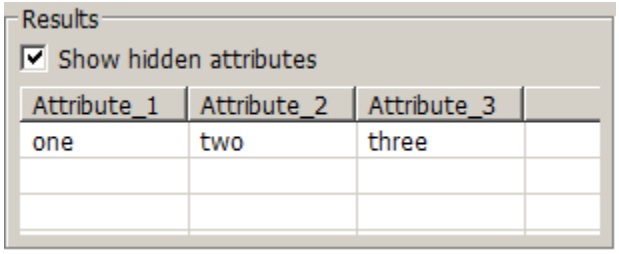


Figura 40. Exemplo de Saída do Valor de Atributo quando o Agent Analisa uma Linha de Dados do Arquivo de Log Simples.

Exemplo 2 - Saída de Arquivo de Log Complexo

Alguns arquivos de log podem conter linhas de dados que possuem separadores irregulares ou em mudança, por exemplo:

```
um, dois três, [quatro]12:42, cinco
```

Neste exemplo, uma designação de separadores a definições de atributos que pode ser usada é:

1. No exemplo anterior você configurou o separador padrão como " , ". Esse separador é usado para todos os atributos, a menos que você o substitua por um separador específico. Neste exemplo o separador padrão de " , " é correto para ser usado novamente para os primeiros três atributos na linha.
2. Para o quarto atributo, suponha que a sequência entre "[" e "]" é um valor que você deseja extrair. Nesse caso, ao definir o quarto atributo, você designa um tipo de separador **Texto de Início e de Término** com valores de texto de início e de término de "[" e "]".
3. Para o quinto atributo, suponha que você deseja extrair os valores entre os "]" e " : ". Neste caso, ao definir o quinto atributo, você designa o tipo de separador **Texto do Separador** configurado como " : ".
4. Para o sexto atributo, o seu separador do grupo de atributos padrão " , " está correto novamente.
5. Para o sétimo atributo, você não precisa especificar um separador, pois ele é o último atributo.

Definindo esse separador em um arquivo de log que contém a linha de dados que é mostrada anteriormente neste exemplo que é mostrado na seguinte saída:

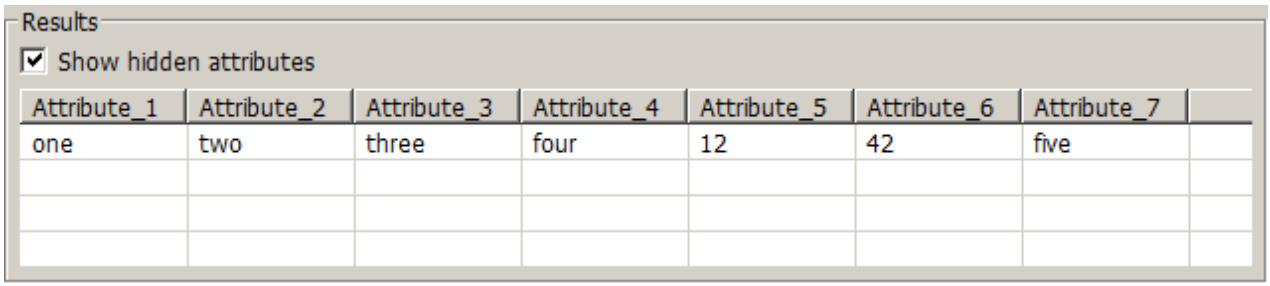


Figura 41. Exemplo de Saída do Valor de Atributo quando o Agent Analisa uma Linha de Dados do Arquivo de Log Complexo

O procedimento para definir os separadores de atributo é descrito na etapa “5” na página 1262 de “Monitorando um Arquivo de Log” na página 1262.

Testando Grupos de Atributos do Arquivo de Log

É possível usar o Agente Builder para testar o conjunto de dados do arquivo de log (grupo de atributos) criado. Se nenhum atributo for definido para o grupo, o processo de teste os definirá automaticamente.

Antes de Iniciar

Se algum atributo já estiver definido para este conjunto de dados e você desejar definir atributos automaticamente durante o teste, use o editor de agente para remover todos os atributos existentes do conjunto de dados. Para obter instruções, veja “Removendo Atributos” na página 1195.

Procedimento

1. É possível iniciar o procedimento de Teste das seguintes maneiras:
   - Durante a criação do agente, clique em **Testar Configurações do Arquivo de Log** na página **Informações de Arquivo de Log**.
   - Após a criação do agente, selecione um grupo de atributos na página **Definição de Origem de Dados** do Agent Editor e clique em **Testar Configurações do Arquivo de Log**. Para obter informações adicionais sobre o Agent Editor, consulte “Usando o Agent Editor para modificar o agente” na página 1172.

   Depois de clicar em **Testar Configurações do Arquivo de Log** em uma das duas etapas anteriores, a janela **Analisar Log** se abre.
2. Selecione a origem dos dados de log para teste:
   - **Usar configurações do grupo de atributos**: use este nome de arquivo e local especificados na origem de dados. Por padrão, a origem de dados processa apenas as informações que são incluídas no arquivo de log depois que o processo de teste é iniciado. É possível usar essa opção quando o arquivo de log está sendo atualizado em tempo real.
   - **Especificar um arquivo de amostra**: fornece um arquivo de log de amostra. Com essa configuração, o procedimento de teste analisa todo o conteúdo do arquivo de log. Com essa opção, é possível testar a origem de dados e criar os atributos para ela imediatamente, com base em uma amostra existente. Especifique o caminho e o nome de arquivo no campo **Nome do arquivo de log** ou use o botão **Procurar** para selecionar o arquivo.
3. Opcional: Antes de iniciar o teste, você pode configurar as variáveis de ambiente e as propriedades de configuração.

   Para obter mais informações, consulte (“Teste de Grupo de Atributos” na página 1380).
4. Clique em **Iniciar Agente**.

   Uma janela é aberta indicando que o Agente está iniciando. Quando o agente é iniciado, ele monitora o arquivo de log configurado para novos registros
5. Para testar a coleção de dados de seu agente, gere novos registros no arquivo de log monitorado.

   Quando novos registros são incluídos no arquivo de log o agente os analisa de acordo com sua configuração e atualiza os valores de atributos correspondentes em seu cache.
6. Para simular uma solicitação a partir do Tivoli Enterprise Portal ou SOAP para dados do agente, clique em **Coletar Dados**.

   A janela **Analisar Log** coleta e mostra todos os novos valores de atributo na cache do agente desde quando ele foi iniciado pela última vez. Uma coleção de dados de exemplo é mostrada na Figura 42 na página 1273

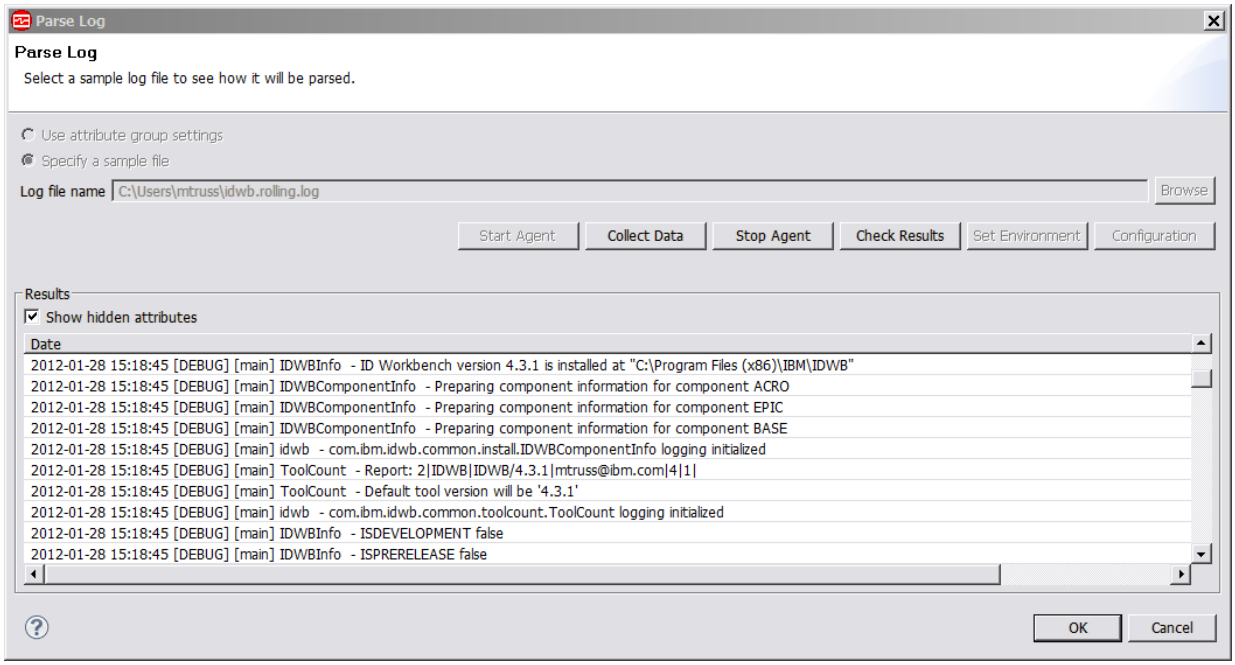


Figura 42. Janela Analisar Log que mostra os valores de atributo de arquivo de log analisado

7. Opcional: Clique em **Verificar Resultados**, se os dados retornados não estiverem conforme o esperado.

   A janela **Status de Coleção de Dados** é aberta e mostra informações adicionais sobre os dados. Os dados coletados e mostrados pela janela Status de Coleta de Dados são descritos em "Nó de Status do Objeto de Desempenho" na página 1424
8. O agente pode ser interrompido clicando em **Parar Agente**.
9. Clique em **OK** ou **Cancelar** para sair da janela **Analisar Log**. Clicar em **OK** salva quaisquer mudanças que tiver feito.

Conceitos relacionados

"Testando seu agente no Agent Builder" na página 1380
Depois de usar o Agent Builder para criar um agente, será possível testar o agente no Agent Builder.

Monitorando um Log Binário do AIX

É possível definir uma origem de dados para monitorar logs de erros binários do AIX por meio do comando `errpt`. Também é possível configurá-la para filtrar e resumir os dados. Os eventos resultantes serão colocados em um conjunto de dados.

Sobre Esta Tarefa

O Monitoramento de Logs suporta o monitoramento dos logs de erros binários do AIX por meio do comando `errpt`. O comando `errpt` gera um relatório de erro a partir das entradas em um log de erro. Ele inclui sinalizadores para selecionar erros que correspondem a critérios específicos. Este suporte para o monitoramento dos logs de erros binários do AIX por meio do comando `errpt` é modelado no suporte para a mesma função no Tivoli Monitoring UNIX Logs Agent (código do produto `kul` ou `ul`).

Ao fornecer o Agent Builder com uma sequência de caracteres de comando **`errpt`**, ele processa os eventos que resultam da execução desse comando. O Agent Builder impinge as mesmas restrições nesse comando que o Monitoring Agent for UNIX Logs impinge. Em particular, você deve usar a opção **`-c`** (modo simultâneo) para que o comando seja executado continuamente e não é possível usar a opção **`-t`** ou as opções a seguir que resultam em saída detalhada: **`-a`**, **`-A`** ou **`-g`**.

Um agente do Agent Builder que monitora o comando AIX **`errpt`** inclui automaticamente as mesmas informações que o Monitoring Agent for UNIX Logs inclui. Para obter mais informações sobre os grupos

de atributos para os log de erros binários do AIX, consulte “Grupo de Atributos de Log Binário do AIX” na página 1438.

Procedimento

1. Na página **Origem de Dados Inicial do Agente** ou na página **Local de Origem de Dados**, clique em **Dados Registrados** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **Log Binário do AIX**.
3. Clique em **Avançar**.
4. Na página **Informações de Log Binário**, insira um comando `errpt`.

   O valor padrão é:

   ```
   errpt -c -smmddhhmmyy
   ```

   O agente procura a sequência 'mmddhhmmaa' e a substitui pela data e hora reais na inicialização. Somente a primeira ocorrência da sequência é substituída.

   É possível fornecer seu próprio comando `errpt`, mas o Agent Builder impinge as mesmas restrições nesse comando que o Monitoring Agent for UNIX Logs impinge. Em particular, você deve usar a opção **`-c`** (modo simultâneo) para que o comando seja executado continuamente e não é possível usar a opção **`-t`** ou as opções a seguir que resultam em saída detalhada: **`-a`**, **`-A`** ou **`-g`**.
5. (Opcional) Clique em **Avançado** para selecionar as opções de filtragem e resumo para eventos. Para obter mais informações, consulte “Controlando eventos duplicados” na página 1408.
6. Execute uma das seguintes etapas:
   - Se estiver usando o assistente de **Agente**, clique em **Avançar**.
   - Clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor.

Referências relacionadas

“Grupo de Atributos de Log Binário do AIX” na página 1438
O grupo de atributos de Log Binário do AIX exibe eventos a partir do Log Binário do AIX conforme selecionados pela sequência de caracteres de comando `errpt`.

Monitorando um Log de Eventos do Windows

É possível definir uma origem de dados para coletar dados de um log de evento do Windows. É possível configurá-la para filtrar os dados. Os eventos resultantes são posicionados no conjunto de dados Log de eventos.

Sobre Esta Tarefa

É possível coletar dados do log de eventos do Windows usando o tipo, a origem ou o ID de eventos. Use esses parâmetros para filtrar os eventos de log que o sistema Windows reuniu. O agente compara cada novo evento no log de eventos monitorados com o filtro especificado. Se o evento corresponder a um dos tipos de eventos, fontes de eventos e IDs de eventos especificados no filtro, ele será transmitido.

Por exemplo, se o filtro de log de Eventos for o log de Aplicativo, especifique **Erro** como o tipo de evento. Esta opção corresponde a todos os eventos registrados no log do Aplicativo com um valor de tipo de evento de `erro`. Se você incluir as fontes de eventos **Diskeeper** e **Symantec AntiVirus**, o agente corresponderá a todos os eventos de erro de qualquer uma dessas fontes. É possível incluir IDs de evento específicos para refinar ainda mais o filtro. Não existe nenhuma associação direta entre o tipo de evento, a fonte de eventos e o ID do evento. Se um dos valores para cada um corresponder a um evento, o evento será correspondido.

Por padrão, somente os eventos gerados após o início do agente são processados. No entanto, será possível ativar o agente quando ele for reiniciado para processar eventos de logs que são gerados enquanto o agente estiver encerrado. Para obter mais informações sobre a ativação do agente para processar eventos gerados enquanto o agente estiver encerrado, consulte a etapa “6” na página 1275.

Procedimento

1. Na página **Origem de Dados Inicial do Agente** ou na página **Local de Origem de Dados**, clique em **Dados Registrados** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **Log de Eventos do Windows**.
3. Clique em **Avançar**.
4. Na página **Log de Eventos do Windows**, selecione o nome a partir de um dos logs na lista **Nome do Log de Eventos do Windows** ou digite um nome para o log de eventos.

   A lista é construída a partir do conjunto de logs no sistema atual, por exemplo:

   ```
   Aplicativo
   Segurança
   Sistema
   ```
5. Na página **Log de Eventos do Windows**, especifique se você deseja filtrar os resultados usando um ou mais dos seguintes mecanismos:

   - "Filtrando pelo Tipo de Evento" na página 1276
   - "Filtrando pela Fonte de Eventos" na página 1276
   - "Filtrando pelo Identificador de Eventos" na página 1276

   Nota: Você deve selecionar pelo menos um destes critérios de filtragem.
6. Para processar os eventos de log gerados enquanto o agente é encerrado, em uma reinicialização de agente, clique em **Configurações de Eventos Offline** na página **Log de Eventos do Windows**.

   A janela **Configurações do Marcador de Log de Eventos Windows** é aberta.
7. Selecione uma das seguintes opções de indicador:

   Nota: Essas opções se aplicam a todos os logs de eventos do Windows que estão sendo monitorados.

   - **Não coletar nenhum evento offline**: os eventos gerados enquanto o agente é encerrado não são processados. Essa opção é a opção padrão.
   - **Coletar todos os objetos offline**: todos os eventos gerados enquanto o agente é encerrado são processados.
   - **Especificar as configurações de coleções customizadas**: é possível inserir um valor para regular o processamento de eventos antigos com base em um valor de tempo ou em um número de eventos, ou em ambos. Usando essa opção, você assegura que o ambiente de monitoramento não seja sobrecarregado com eventos quando o agente for iniciado.

     Por exemplo, se 100 for inserido no campo **O número máximo de eventos a ser coletado** e 30 for inserido no campo **Restringir Coleção Baseada em um Intervalo de Tempo (em segundos)**. O número de eventos processados são os últimos 100 eventos gerados antes que o agente seja iniciado, ou qualquer evento gerado dentro de 30 segundos do início do agente. Qual resultado depende da variável que é correspondida primeiro.

     Ao inserir um valor para o número máximo de eventos a serem coletados, a variável de ambiente *CDP_DP_EVENT_LOG_MAX_ BACKLOG_EVENTS* é incluída. Ao inserir um valor para restringir a coleção baseada em um intervalo de tempo, a variável de ambiente *CDP_DP_EVENT_LOG_MAX_BACKLOG_TIME* é incluída. Quando uma ou ambas essas variáveis forem incluídas, o arquivo *eventlogname_productcode_instancename_subnodename*`.rst` é criado contendo o último registro de evento processado para o log de eventos. Esse arquivo está no diretório *%CANDLE_HOME%*`\tmaitm6\logs` e é usado quando o agente é reiniciado para processar eventos antigos gerados enquanto o agente foi encerrado.
8. Se desejar configurar opções globais para a origem de dados, clique em **Opções Globais** na página **Log de Eventos do Windows**

   A janela **Opções de Origem de Dados Globais do Windows** é aberta.

9. Selecione a caixa de opção **Incluir propriedades de configuração remota do Windows** se desejar incluir esta opção, e clique em **OK**.

   Para obter informações sobre a configuração de conexão remota do Windows para origens de dados do Windows, consulte "Configurando uma conexão remota Windows" na página 1367.
10. Após especificar o filtro e clicar em **OK**, na página **Log de Eventos do Windows**, execute uma das etapas a seguir:
    - Se estiver usando o assistente de **Agente**, clique em **Avançar**.
    - Clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor. O nome do novo Windows Event Log é mostrado na página **Editor de Agente Definição de Origem de Dados**.

O que Fazer Depois

Para obter informações sobre a configuração de conexão do Windows remoto para as origens de dados do Log de Eventos do Windows, consulte "Configurando uma conexão remota Windows" na página 1367.

Filtrando pelo Tipo de Evento
Filtrar resultados do Log de Eventos do Windows por tipo de evento

Procedimento

1. Na página **Log de Eventos do Windows**, selecione **Filtrar por Tipo de Evento**.
2. Selecione um ou mais dos tipos de Evento a seguir:
   - **Informações**
   - **Aviso**
   - **Erro**
   - **Auditoria de Êxito**
   - **Auditoria de Falha**
3. Clique em **Concluir** para concluir.

Filtrando pela Fonte de Eventos
Filtrar resultados do Log de Eventos do Windows por origem de eventos

Procedimento

1. Selecione **Filtrar por origem de eventos** e clique em **Incluir** na área **Origens de Eventos** da página **Log de Eventos do Windows**.

   A janela **Origem de Eventos** é aberta.
2. Faça uma das opções a seguir.
   - Digite o nome da origem de eventos e clique em **OK**.
   - Clique em Procurar **Procurar** para localizar e selecionar uma origem de eventos a partir de uma lista e clique em **OK**.

     O nome que você selecionou é mostrado na janela **Origem de Eventos**.

     Nota:

     a. Para classificar a lista de origens de eventos, clique no título da coluna.

     b. Para atualizar as informações na janela, clique no ícone **Atualizar**.

     c. Para procurar fontes de eventos específicas, clique no ícone **Procurar** (binóculos).
3. Clique em **OK** para ver o novo filtro de origem de eventos na lista de Origens de Eventos na janela **Log de Eventos do Windows**.

Filtrando pelo Identificador de Eventos
Para a origem de dados Windows Event Log, você pode filtrar os eventos pelo identificador de evento.

Sobre Esta Tarefa

Para filtrar pelo identificador de eventos, utilize o procedimento a seguir:

Procedimento

1. Selecione **Filtrar por Identificador de Evento** e clique em **Incluir** na área **Identificadores de Eventos** da janela **Log de Eventos do Windows**.

   A janela **Identifier de Evento** é exibida.
2. Se você souber que deseja monitorar eventos específicos de um aplicativo, especifique os números do evento como o aplicativo o define. Digite um inteiro como o identificador de evento e clique em **OK**.

   O novo filtro de identificador de evento numérico é exibido na lista Identificadores de Evento em **Log de Eventos do Windows**.

   Nota: Cada identificador de evento deve ser definido individualmente.
3. Se desejar modificar um log de eventos do Windows, selecione-o e clique em **Editar**.
4. Se desejar excluir um log de eventos do Windows, selecione-o e clique em **Remover**.
5. Você pode incluir mais logs de eventos na lista ou clicar em **Concluir**.

Monitorando um Código de Retorno de Comando

É possível definir uma origem de dados para monitorar um aplicativo ou sistema usando um *código de retorno de comando*. O agente executa o comando, coleta o código de retorno e inclui o resultado para o conjunto de dados de Disponibilidade.

Sobre Esta Tarefa

Um script, arquivo executável, consulta ou comando do sistema criado pelo usuário pode retornar um código. Um código de retorno de comando é um mecanismo específico de aplicativo para determinar se o aplicativo ou sistema de monitoramento está disponível. O agente executa o comando especificado e determina o estado do aplicativo ou sistema de monitoramento examinando o código de retorno.

O comando deve apresentar um código de retorno exclusivo para cada estado descritivo. O comando também deve definir uma mensagem para ser usada para cada um desses códigos de retorno. O comando pode usar variável de ambiente e de configuração dentro do script criado pelo usuário, arquivo executável, consulte ou comando do sistema. O comando não deve usar variáveis de ambiente ou de configuração na chamada da linha de comandos do comando, com somente as seguintes as exceções disponíveis: *AGENT_BIN_DIR*, *AGENT_ETC_DIR*, *AGENT_LIB_DIR*, *CANDLE_HOME* e *CANDLEHOME*.

Procedimento

1. Na página **Origem de Dados Inicial do Agente** ou página **Local de Origem de Dados**, selecione **Comando ou Script** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **Um código de retorno de comando**.
3. Clique em **Avançar**.
4. Na página **Código de Retorno do Comando**, área **Informações do Código de Retorno do Comando**, digite o nome de exibição.
5. Use as subetapas a seguir para definir e descrever as linhas de comando que deseja que seu código de retorno use.

   Nota: Defina um comando para cada sistema operacional suportado pelo agente. Comandos podem ser compartilhados, mas o conjunto total de sistemas operacionais para todos os comandos deve ser igual ao conjunto sistemas operacionais suportados por agente.

   a) Clique em **Incluir** na área **Comandos** da janela **Código de Retorno de Comando** para abrir a janela **Informações do Comando**.

   b) Digite uma linha de comandos e selecione um sistema operacional da lista na área **Sistemas Operacionais** da janela **Informações de Comando**.

Nota:

1) Para um comando Windows , digite o nome completo do comando. Por exemplo, `command_to_run.bat` e não somente `command_to_run`.
2) Coloque aspas em torno do nome de modo que ele não seja analisado pelo interpretador de comandos. Por exemplo, digite `"este é um test.bat"argument` e não `este é um argumento test.bat`.
3) Você pode clicar em um comando e clicar em **Editar** para modificá-lo ou clicar em **Remover** para excluí-lo.

c) Clique em **Incluir** na área **Códigos de Retorno** da janela **Informações de Comando**.

d) Selecione um tipo de código de retorno na lista que é mostrada na janela **Definição de Código de Retorno**

Você pode designar os seguintes estados para os códigos de retorno de teste:

- `ALREADY_RUNNING`
- `DEPENDENT_NOT_RUNNING`
- `GENERAL_ERROR`
- `NOT_RUNNING`
- `OK`
- `PREREQ_NOT_RUNNING`
- `WARNING`

e) Digite um valor numérico para o tipo de código de retorno selecionado.

O valor do código de retorno é um número inteiro que especifica um código de retorno definido para o código de retorno do comando. Para portabilidade entre sistemas operacionais, use um valor de código de retorno `0 - 255`. Para um comando que é executado somente em Windows, o valor de código de retorno pode ser `-2147483648 - 2147483647`.

f) Defina uma mensagem para cada código de retorno para que a mensagem e o código possam ser mostrados juntos. Clique em **Procurar** para configurar o texto da mensagem.

A janela de mensagens lista mensagens que são definidas no agente. A janela **Mensagens** (lista) é aberta.

Nota:

1) É possível selecionar o texto que foi inserido anteriormente selecionando-o na lista de textos de mensagens em vez de clicar em **Procurar**. Em seguida, continue na Etapa 5k.
2) Até definir as mensagens, a lista permanece em branco. É possível usar **Editar** para alterar uma mensagem definida e **Remover** para excluir uma ou mais mensagens que você definiu.

g) Na janela **Mensagens** (lista), clique em **Incluir**

A janela **Definição de Mensagem** é aberta.

Nota: O identificador de mensagens é automaticamente gerado para você.

h) Insira o texto que descreve o significado da nova mensagem no campo **Texto da Mensagem**.

i) Clique em **OK**.

A janela **Mensagens** (lista) é aberta mostrando a nova mensagem.

j) Para verificar a mensagem e torná-la permanente, selecione-a na lista e clique em **OK**.

O novo tipo do código de retorno, valor e texto são mostrados na janela **Definição de Código de Retorno**.

k) Se desejar que esse código de retorno esteja disponível para outros comandos em outros sistemas operacionais para esse código de retorno de comando, selecione **Código de Retorno Global se aplica a todos os comandos**. Se você desejar que este código de retorno esteja disponível somente para esse comando, deixe **Código de retorno local aplica-se somente a este comando** selecionado.

l) Clique em **OK** na janela **Definição de Código de Retorno**.

m) Defina pelo menos dois códigos de retorno antes de sair da janela **Informações de Comando**. Um código de retorno para indicar nenhum problema com a disponibilidade, outro para indicar se ocorreu problema. Se deseja incluir outro código de retorno, retorne para a etapa c.

n) Opcional: Na janela **Informações de Comando**, na área **Arquivos de Comando**, clique em **Incluir** se desejar selecionar um ou mais scripts ou arquivos executáveis para o agente executar.

O arquivo ou arquivos são copiados na pasta de projeto do agente em `scripts/`*`operating system`*, em que *operating system* é uma variável que depende do que você selecionou na área **Sistemas Operacionais** da janela **Informações de Comando**. Esses arquivos também são fornecidos e distribuídos com o agente. Para editar a definição de um arquivo de comando existente ou o arquivo de comando original desde a cópia no projeto, selecione o arquivo e clique em **Editar**. Consulte ("Editando uma definição de arquivo de comando" na página 1280).

o) Clique em **OK** na janela **Informações de Comando**.

Nota: A tabela de arquivos de comandos é onde você define quaisquer arquivos externos que deseja incluir no pacote do agente. Esses arquivos são copiados no diretório do projeto e são empacotados com o agente para distribuição.

6. Se você tiver outros códigos de retorno que ainda não estejam definidos, defina e descreva os códigos de retorno globais que seu código de retorno do comando pode usar.

a) Clique em **Incluir** na área **Códigos de Retorno Globais** da página **Código de Retorno de Comando**.

Nota: Os códigos de retorno que são definidos aqui são globais. Isto significa que os códigos de retorno são apropriados para todos os comandos definidos para o código de retorno do comando. (Eles não são compartilhados entre os códigos de retorno do comando). Além disso, é possível definir códigos de retorno ao inserir as informações de comando. Os códigos de retorno definidos aqui podem ser globais ou locais. Os códigos de retorno locais são apropriados somente para este comando específico. Essa hierarquia é útil se você tiver um código de retorno que seja o mesmo em todos os sistemas operacionais. (Por exemplo, um código de retorno de 0 significa que tudo está funcionando corretamente. É possível defini-lo para o nível global, e então todos os comandos definidos interpretam 0 dessa forma). Se nenhum dos outros sistemas operacionais retornar um 5, você pode definir o código de retorno 5 somente para o comando Windows. Se você definir um código de retorno no nível do comando local que já está definido no nível global, o nível do comando é usado. É possível usar esse método para substituir códigos de retorno nos sistemas operacionais específicos. Por exemplo, se em todos os sistemas operacionais UNIX, um código de retorno 2 significa uma coisa, mas no Windows, significa algo diferente. Você pode definir um código de retorno 2 no nível global conforme esperado pelos sistemas operacionais UNIX. Em seguida, no comando para o Windows, será possível redefinir o código de retorno 2 para o significado no Windows.

b) Selecione um tipo de código de retorno na lista que é mostrada na janela **Definição de Código de Retorno**.

Você pode designar os seguintes estados para os códigos de retorno de teste:

- `ALREADY_RUNNING`
- `DEPENDENT_NOT_RUNNING`
- `GENERAL_ERROR`
- `NOT_RUNNING`
- `OK`
- `PREREQ_NOT_RUNNING`
- `WARNING`

c) Digite um valor numérico para o tipo de código de retorno selecionado. O valor do código de retorno é um número inteiro que especifica um código de retorno definido para o código de retorno do comando.

d) Clique em **Procurar** para configurar o texto da mensagem e seu significado associado. É necessário definir uma mensagem para cada código de retorno para que a mensagem e o código sejam mostrados juntos.

A janela **Mensagens** lista mensagens definidas no agente.

Nota:

1) Até definir as mensagens, a lista permanece em branco. É possível usar **Editar** para alterar uma mensagem definida e **Remover** para excluir uma ou mais mensagens definidas.
2) É possível selecionar texto que foi inserido anteriormente selecionando-o na lista **Texto de Mensagem** em vez de clicar em **Procurar**. Em seguida, continue na Etapa 6h.

e) Na janela **Mensagens** (lista), clique em **Incluir** para ver uma janela **Definição de Mensagem**, na qual você pode digitar o texto que descreve o significado da nova mensagem.

f) Clique em **OK**.

g) A janela **Mensagens** (lista) é aberta com a nova mensagem. Para verificar a mensagem e torná-la permanente, selecione-a na lista e clique em **OK**.

h) Quando o novo texto, tipo e valor forem mostrados na janela **Definição de Código de Retorno**, clique em **OK**.

i) Na página de código de Retorno do Comando, quando você concluir a definição de códigos de retorno e comandos para todos os sistemas operacionais suportados, execute uma das etapas a seguir:

- Se estiver usando o assistente de Novo Agente, clique em **Avançar** ou clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor.
- Se estiver usando o assistente de componente do Novo Agente, clique em **Concluir** para retornar ao Agent Editor.

O que Fazer Depois

Se desejar usar os dados desta origem de dados no painel de resumo para IBM Cloud Application Performance Management, deve-se criar um conjunto de dados filtrado (grupo de atributos) baseado no conjunto de dados Disponibilidade e configurá-lo como fornecendo uma única linha. Use o campo NOME para selecionar a linha para seu processo.

No novo grupo de atributos filtrado, selecione o campo Status e especifique os valores da severidade para ele.

Para obter instruções, consulte:

- “Criando um grupo de atributos filtrado” na página 1344
- “Especificando gravidade para um atributo usado como um indicador de status” na página 1200
- “Preparando o agente para Cloud APM” na página 1377

Editando uma definição de arquivo de comando

É possível alterar o arquivo de comando no projeto ou importar mudanças no arquivo de comando existente no projeto.

Procedimento

1. Selecione o arquivo na área **Arquivos de Comandos** da janela **Informações de Comando**.
2. Clique em **Editar** para abrir a janela **Importar Arquivo de Comando**.

   Na janela **Importar Arquivo de Comando**, você pode obter o status do arquivo de comando. Também é possível alterar o local do arquivo de origem original e recopiar o arquivo de origem no agente.
3. Escolha uma das seguintes etapas:

   - Clique em **OK** para planejar uma cópia do arquivo para ocorrer na próxima vez que o agente for salvo.

- Clique em **Copiar Imediatamente** para copiar o arquivo sem primeiro salvar o agente.

Nota: A opção **Copiar Imediatamente** não está disponível ao acessar a janela **Importar Arquivo de Comando** do assistente de Novo Agente.

Separação & Consolidação de Arquivo
É possível usar funções Separada e Consolidada para mover arquivos para dentro e fora das pastas específicas do sistema operacional no agente.

Quando um arquivo é incluído pela primeira vez no agente, uma única cópia é incluída na pasta `scripts/all_windows`, na pasta `scripts/all_unix` ou na pasta `scripts/common`. A pasta `scripts/common` é usada se o arquivo for usado em ambos Windows e UNIX.

Para colocar diferentes cópias do arquivo em diferentes sistemas operacionais (por exemplo, um arquivo executável binário), clique em **Editar** e clique em **Separar**. O arquivo é removido da pasta comum e copiado em pastas específicas do sistema operacional. Em seguida, é possível substituir cópias individuais do arquivo por cópias apropriadas para sistemas operacionais específicos.

Nota: Os arquivos de recursos Java devem permanecer na pasta `scripts/common`. Não é possível clicar em **Separada** para criar cópias separadas de arquivos de recursos Java para sistemas operacionais individuais.

Se você separou os arquivos em pastas de sistema operacional, pode usar o **Consolidar** para movê-los de volta em um pasta comum. Se você criou o agente em uma versão de Agent Builder que não suportava pastas comuns, use **Consolidar** para movê-los de volta em uma pasta comum. Se alguma das cópias do arquivo difere-se de outra, será solicitado que você selecione o arquivo a usar como o arquivo comum. Todas as outras cópias são descartadas.

Monitore a Saída de um Script

É possível definir uma origem de dados para coletar dados de um script ou programa externo. Use-a quando os dados do aplicativo não estiverem disponíveis por meio de uma interface de gerenciamento padrão ou quando você precisar fornecer um resumo de dados com diversas linhas em uma única linha. O agente executa o script e coleta sua saída. Cada linha na saída do script ´analisada em uma linha do conjunto de dados resultante.

Os dados podem ser coletados a partir de um sistema local ou remoto. A saída do script ou programa deve conter somente valores para cada atributo dentro do grupo de atributos. Para retornar diversas linhas de dados, os dados de cada linha devem estar separados por uma quebra de linha. Os atributos em cada linha de dados são separados pelos separadores que você define. Para obter informações adicionais sobre separadores, consulte “Análise de Script e Separadores” na página 1282

O comando pode usar variáveis de ambiente e configuração no script criado pelo usuário, arquivo executável, consulta ou comando do sistema. O comando não pode usar variáveis de ambiente ou configuração na chamada da linha de comandos do comando, com somente as seguintes exceções disponíveis: `AGENT_BIN_DIR`, `AGENT_ETC_DIR`, `AGENT_LIB_DIR`, `CANDLE_HOME` e `CANDLEHOME`.

O agente monitora a saída de script gravada usando o mesmo código de idioma e página de códigos em que o agente é executado.

Coletando dados de script de um sistema remoto
Para coletar dados do programa ou do script a partir de um sistema remoto, o Agent Builder usa um Secure Shell (SSH)

Para coletar dados de um sistema remoto, o Agent Builder cria uma sessão de Shell Seguro (SSH) e inicia o script ou programa externo no sistema remoto. O agente estabelece e efetua login em uma sessão de SSH. O agente, então, faz upload dos scripts para o sistema remoto, inicia o script ou o programa externo e recupera a saída. O agente pode ser configurado para manter a sessão aberta ou restabelecer a sessão para cada chamada. Se a sessão for mantida aberta, o script poderá ser reutilizado ou transferido por upload para cada chamada. Por padrão, uma única sessão SSH é usada e os scripts são reutilizados para cada chamada.

O Agent Builder suporta o uso somente do Protocolo SSH Versão 2 com as chaves Rivest, Shamir e Adleman (RSA) ou Digital Signature Algorithm (DSA). O agente é autenticado pelo nome de usuário e senha ou pela autenticação da chave pública. A geração e a distribuição das chaves públicas é uma tarefa administrativa que precisa ser feita fora do agente e Agent Builder.

Para executar um comando Executar Ação escrito com relação a um provedor de dados de script ativado para Shell Seguro (SSH) no sistema remoto, consulte "Ação SSHEXEC" na página 1509.

Restrição: Se seu agente foi construído com uma versão do Agent Builder anterior à 6.3 e ele tiver um provedor de dados de script que usa SSH, o provedor falhará ao ser executado com o IBM Tivoli Monitoring versão 6.3 ou posterior. Para resolver esse problema, reconstrua o agente com a versão atual do Agent Builder.

A restrição é porque o IBM Tivoli Monitoring versão 6.3 usa uma versão mais nova da API do Global Secure ToolKit (GSKit). Você deve reconstruir o agente com o Agent Builder versão 6.3 ou mais recente para executá-lo com o IBM Tivoli Monitoring versão 6.3 ou mais recente. Se você construir o agente com o Agent Builder 6.3, ele também poderá ser executado com versões anteriores do IBM Tivoli Monitoring.

Análise de Script e Separadores
É possível alterar e designar separadores de script específicos para um ou mais atributos.

Ao criar um grupo de atributos de script, um separador de texto de caractere único é designado por padrão. O separador padrão é " ; ". O separador é usado pelo agente para analisar e delimitar os dados de cada atributo na linha de dados. É possível alterar o separador padrão para usar um caractere diferente. Também é possível designar separadores específicos a um ou mais atributos individuais.

É possível designar separadores específicos para atributos individuais que:

- Utilizam um número fixo de bytes da saída.
- Separam um atributo do próximo com um separador customizado, que pode ser mais que um caractere.
- Delimitam um valor de atributo com uma sequência no início e final do valor.
- Retornam o restante do texto como o valor de atributo (contendo separadores integrados ou não).

É possível usar um ou mais desses separadores para extrair valores de atributos das linhas de dados.

Exemplo 1 - Saída de script simples

Alguns scripts podem exibir linhas de dados com separadores claros e regulares, por exemplo:

```
Row One;1;2
Row Two;3;4
Row Three;5;6
```

Aqui, o caractere " ; " é um separador claro e regular entre as três partes de dados em cada linha. Neste caso, o separador padrão é aplicável, portanto, não há necessidade de alterar ou definir outros separadores. Não é difícil imaginar uma saída de script semelhante na qual o separador seja um caractere diferente, como no exemplo a seguir.

```
Row One-1-2
Row Two-3-4
Row Three-5-6
```

Neste exemplo, o separador é alterado de um caractere " ; " para um caractere " - ". Neste caso, ao definir os atributos, altere o separador padrão para usar o caractere " - ".

Exemplo 2 - Saída de Script Complexa

Alguns scripts podem emitir linhas de dados que possuem separadores irregulares ou em mudança, por exemplo:

```
Row One;1;2;[option]Hour:MIN;fourtabby  The end;4
Row Two;3;4;[required]12:30;fourvery tabby the tail;5
Row Three;5;6;[out]March:12;fourline up the rest of the story;6
```

Neste exemplo, uma designação de separadores a definições de atributos que pode ser usada é:

1. Inicialmente, o separador padrão "`;`" é aplicável nos primeiros três atributos de cada linha. Neste caso, você designa o tipo de separador **Texto do Separador** configurado como "`;`" ao definir cada atributo; essa é a configuração padrão.
2. Para o quarto atributo, suponha que a sequência entre "`[`" e "`]`" é um valor que você deseja extrair. Nesse caso, ao definir o quarto atributo, você designa um tipo de separador **Texto de Início e de Término** com valores de texto de início e de término de "`[`" e "`]`".
3. Para o quinto atributo, suponha que você deseja extrair os valores entre os "`]`" e "`:`". Neste caso, ao definir o quinto atributo, você designa o tipo de separador **Texto do Separador** configurado como "`:`".
4. Para o sexto atributo, o separador padrão "`;`" é fino novamente, aceite o padrão.
5. Para o sétimo atributo, você gostaria de extrair a sequência nos próximos quatro caracteres "`four`". Não há um separador claro no final dessa sequência. É possível designar vários caracteres para definir a separação do próximo atributo. Você designa um tipo de separador **Número de Caracteres** e especifica quatro caracteres como o comprimento.
6. Para o oitavo atributo, você gostaria de extrair as sequências `tabby`, `very tabby` e `line up`. Neste caso, é possível supor que todas essas sequências são seguidas por um caractere de tabulação. Neste caso, você designa um separador do tipo **Separador de Tabulação**.
7. Para o nono atributo, você reverte novamente para o tipo de separador padrão para extrair o texto restante para esse atributo.
8. Para o décimo atributo, você especifica **Restante do Registro** para designar o restante da linha de dados a esse atributo

A definição desses separadores em um script que emite como saída as linhas de dados mostradas anteriormente neste exemplo é mostrada na seguinte saída:

Results

Show hidden attributes

Attribute_1	Attribute_2	Attribute_3	Attribute_4	Attribute_5	Attribute_6	Attribute_7	Attribute_8	Attribute_9	Attribute_10 (Remainder of record)
Row One	1	2	option	Hour	MIN	four	tabby	The end	4
Row Two	3	4	required	12	30	four	very tabby	the tail	5
Row Three	5	6	out	March	12	four	line up	the rest of the story	6

Figura 43. Saída de valores de atributo de exemplo quando o Agente analisa a saída de script complexo.

O procedimento para definir os separadores de atributo é descrito na etapa “10” na página 1286 de “Etapas para Monitorar Saída de um Script” na página 1283.

Etapas para Monitorar Saída de um Script
Configurar o agente para receber dados de uma origem de dados do script.

Antes de Iniciar
Consulte o “Monitore a Saída de um Script” na página 1281.

Sobre Esta Tarefa

Use o seguinte procedimento para monitorar a saída de um script:

Procedimento

1. Na página **Origem de Dados Inicial do Agente** ou na página **Local de Origem de Dados**, selecione a opção **Comando ou Script** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **Saída a partir de um script**.
3. Clique em **Avançar**.
4. Na página **Lista de Comandos**, clique em **Incluir** para exibir uma janela **Informações de Comando**.

Nota: Marcando a caixa de seleção **Ativar Coleção de Dados Usando SSH** o SSH é ativado para esse grupo de atributos. Se essa caixa de seleção não estiver marcada, o grupo de atributos será executado localmente.

Nota: Se existir um comando que possa ser executado no sistema operacional no qual o Agent Builder está em execução, a opção **Testar** será ativada. É possível usar **Testar** para testar um comando que você definiu.

5. Na área **Informações de Comando** na janela **Informações de Comando**, digite um nome de comando com os argumentos necessários no campo **Comando** e um separador no campo **Separador**.

   Nota:

   a. Os scripts no Windows geralmente são iniciados sem especificar a extensão `.bat` ou `.cmd` na linha de comandos. Para execução remota, um ambiente de shell deve estar instalado e você deve especificar `.bat` ou `.cmd` no comando da origem de dados do script para que o script seja executado. `Cygwin` é um exemplo de um ambiente shell disponível para Windows. Linux, Red Hat e AIX. Para verificar se um ambiente shell existe, conecte-se por meio de SSH ou efetue logon no host remoto e insira o comando:

   ```
   PATH=$PATH:. <comando>
   ```

   Se o comando for executado, um ambiente shell existirá.

   b. Coloque o nome entre aspas para que ele não seja analisado pelo interpretador de comandos. Por exemplo, `este é um argumento test.bat` se torna:

   ```
   argumento "this is a test.bat"
   ```

   c. Variáveis de ambiente e variáveis de configuração podem ser usadas no script fornecido pelo usuário, mas não podem fazer parte da linha de comandos que inicia o script. As variáveis a seguir são exceções a esta regra:

   AGENT_BIN_DIR
   O diretório em que o agente coloca os arquivos binários ou scripts

   AGENT_ETC_DIR
   O diretório no qual o agente coloca os arquivos de configuração

   AGENT_LIB_DIR
   O diretório no qual o agente coloca as bibliotecas compartilhadas ou bibliotecas de link dinâmico

   CANDLEHOME
   O diretório de instalação do Linux ou UNIX Tivoli Monitoring

   CANDLE_HOME
   O diretório de instalação do Windows Tivoli Monitoring

   d. Se a opção de coleta de dados SSH estiver sendo usada, a linha de comandos será executada em relação ao diretório inicial do usuário no sistema remoto. Se você estiver fazendo upload de scripts ou de executáveis para o sistema remoto, eles serão copiados para o local especificado na variável de ambiente do agente *CDP_SSH_TEMP_DIRECTORY*. O local é padronizado para o diretório inicial do usuário no sistema remoto. Em alguns sistemas, será possível precisar definir a linha de comandos com um caminho relativo, como `./Script.sh`.

6. Na área **Sistemas Operacionais**, selecione um ou mais sistemas operacionais. Ao coletar dados de um sistema remoto usando SSH, Sistemas Operacionais é uma propriedade do sistema no qual o agente está instalado. Ele não é o Sistema Operacional do sistema remoto. É aconselhável que você selecione a caixa de seleção **Todos os Sistemas Operacionais** ao usar os recursos da coleta de dados SSH.
7. Opcional: Se um ou mais arquivos definidos pelo usuário for necessário para executar o comando, clique em **Incluir** na área de arquivos de Comando para especificar os arquivos do seu sistema.

   Os arquivos são copiados para a pasta do projeto do agente sob `scripts/`*`operating system`*, em que *operating system* é uma variável que depende do que você selecionou na janela **Informações de**

Comando. Esses arquivos também são fornecidos e distribuídos com o agente. Se deseja editar a definição de um arquivo de comando que você já incluiu, ou do qual alterou o conteúdo, selecione o arquivo e clique em **Editar**. Consulte "Editando uma definição de arquivo de comando" na página 1280.

8. Clique em **OK**. A página **Lista de Comandos** é exibida.
9. Para testar o comando, use as etapas a seguir:
   a) Clique em **Testar** para abrir as informações de comando e exibir a janela **Testar Comando**. Para testar o script em um sistema remoto, selecione um sistema na lista **Nome da Conexão** ou clique em **Incluir** para incluir o nome do host de um sistema.
   b) Use a janela **Testar Comando** para alterar o comando, o separador padrão e os separadores de atributos e para visualizar como essas mudanças afetam os dados retornados.
      1) Digite o comando e o separados nos campos, se ainda não estiverem inseridos.

         Nota: É possível especificar outros separadores usando a janela **Informações do Atributo** no horário de criação do atributo ou usando o Agent Editor para modificar um atributo existente. Para obter informações adicionais sobre o Agent Editor, consulte "Usando o Agent Editor para modificar o agente" na página 1172; para obter informações adicionais sobre como manipular a origem de dados e os atributos, consulte "Editando as propriedades da origem de dados e do atributo" na página 1191
      2) Antes de iniciar o teste, você pode configurar as variáveis de ambiente e as propriedades de configuração. Para obter mais informações, consulte ("Teste de Grupo de Atributos" na página 1380).
      3) Clique em **OK** para retornar à janela **Testar Configurações**.
      4) Clique em **Iniciar Agente**. Uma janela indica que o Agente está iniciando.
      5) Para simular uma solicitação a partir do Tivoli Enterprise Portal ou SOAP para dados do agente, clique em **Coletar Dados**. O Agent Builder executa seu comando. Se você especificou um sistema remoto, forneça um ID de usuário e senha. Mesmo que o código de retorno não seja 0, o Agent Builder analisará os resultados do comando da mesma maneira que o agente.
      6) A janela **Testar Configurações** coleta e mostra dados no cache do agente desde a última vez que foi iniciado. Os nomes iniciais dos atributos são **Attribute_1, Attribute_2**, e assim por diante; no entanto, é possível modificar as propriedades dos atributos clicando nos títulos da coluna apropriados.
      7) Clique em **Verificar Resultados** para visualizar o código de retorno do comando, os dados não analisados e quaisquer mensagens de erro que foram retornadas.
      8) O agente pode ser interrompido clicando em **Parar Agente**.
      9) Clique em **OK** para retornar à janela **Informações de Comando**.

         Se você alterar o comando ou o separador, o comando apropriado será atualizado para refletir essas mudanças.

         Se essa janela foi aberta ao criar a origem de dados do script, os atributos foram incluídos na nova origem de dados do script.

         Se esta janela foi aberta a partir de uma origem de dados do script existente, quaisquer mudanças nos atributos serão feitas na origem de dados do script. Quaisquer atributos adicionais são incluídos, mas quaisquer atributos extras não são removidos. Essas opções afetam somente os atributos analisados a partir da saída do script. Os atributos derivados não são afetados. Se qualquer um desses atributos se tornar inválido com base nos atributos que eles referenciam, você pode precisar atualizar ou remover atributos derivados manualmente. A fórmula do atributo derivado é exibida e não o valor do resultado real.

Nota: Se o grupo de atributos existir, para iniciar um teste, conclua o procedimento a seguir

a. Selecione o grupo de atributos na página **Definição de Origem de Dados** do **Agent Editor**.
b. Selecione o script a ser testado a partir da Lista de Comandos.

c. Clique em **Testar** e siga o procedimento na etapa "9" na página 1285

10. Se você ignorou o teste do comando na etapa ("9" na página 1285), use as etapas a seguir:
    a) Na página **Lista de Comandos** com as informações de comandos concluídas, clique em **Avançar**.
    b) Na página **Informações do Atributo**, preencha as informações de nome e tipo de atributo usando (Tabela 261 na página 1196). Selecione **Incluir Atributos Adicionais** para incluir atributos adicionais
    c) Na página **Informações sobre o Atributo**, use a guia **Informações sobre o Atributo de Script** para escolher um separador de dados específico para este atributo.

       O separador padrão `;` está selecionado por padrão. É possível escolher uma série de outros separadores como uma sequência, uma série de caracteres, uma guia ou um espaço. Também é possível usar um separador de sequência diferente para o início e o fim dos dados. Por último, também é possível escolher **Restante do Registro** para designar o restante do registro ao atributo. Para obter informações adicionais sobre análise de script e separadores, consulte "Análise de Script e Separadores" na página 1282.
11. Execute uma das seguintes etapas:
    - Se estiver usando o assistente de **Agente**, clique em **Avançar**.
    - Clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor.
12. É possível incluir atributos e fornecer as informações a eles. Para obter mais informações, consulte "Criando Atributos" na página 1192.

    Além dos campos aplicáveis a todas as origens de dados (descrito em "Campos e Opções para Definir Atributos" na página 1195), a página **Definição de Origens de Dados** para a origem de dados de Script possui as opções a seguir:

    Lista de Comandos
    Fornece acesso para os comandos e scripts a serem iniciados durante a coleta de dados.

    Incluir
    Permite que o usuário inclua um a ser iniciado por este grupo de atributos.

    Editar
    Permite que o usuário edite uma entrada de comando existente.

    Remover
    Permite que o usuário exclua uma entrada de comando existente.

    Testar
    Permite que o usuário acesse o ambiente de teste para esse grupo de atributos.

    Ativar Coleção de Dados Usando SSH
    Marcando essa caixa de seleção o SSH é ativado para esse grupo de atributos. Se essa caixa de seleção não estiver marcada, o grupo de atributos será executado localmente.

    Para obter informações sobre a configuração de conexão remota do SSH para origens de dados de script, consulte "Configurando uma Conexão Remota de Secure Shell (SSH)" na página 1370.

Dados de Monitoramento do Java Database Connectivity (JDBC)

É possível definir uma origem de dados para receber dados de um banco de dados JDBC. O agente executa uma consulta SQL para coletar os dados do banco de dados. Cada coluna que é retornada pela consulta é um atributo no conjunto de dados resultante.

Sobre Esta Tarefa

O provedor de dados JDBC suporta os seguintes servidores de banco de dados:

- IBM DB2 9.x e 8.x
- Microsoft SQL Server 2008, 2005 e 2000
- Banco de dados Oracle 11g e 10g

O Agent Builder não inclui os drivers JDBC para esses bancos de dados. Os drivers JDBC são um conjunto de arquivos JAR fornecidos pelo fornecedor que são necessários para estabelecer uma conexão JDBC com o banco de dados. Para conveniência, aqui há links para onde esses drivers podem ser transferidos por download:

- IBM DB2: Os drivers JDBC são incluídos na instalação de servidor de banco de dados em um subdiretório chamado `java` localizado no diretório de instalação principal do DB2.
- Website do Microsoft SQL Server em www.microsoft.com
- Banco de Dados Oracle: Oracle Database JDBC (http://www.oracle.com/technetwork/database/features/jdbc/index.html)

Nota: É importante lembrar-se de que o provedor de dados JDBC pode monitorar remotamente seus servidores de banco de dados. Um Java Runtime Environment e os arquivos JAR de driver JDBC para o servidor de banco de dados ao qual você está se conectando devem estar no sistema no qual o agente é executado.

As seguintes versões Java são suportadas:

- Oracle Corporation Java Versão 5 ou mais recente
- IBM Corporation Java Versão 5 ou posterior

Procedimento

1. Na página **Origem Inicial de Dados do Agente** ou na página **Local de Origem de Dados**, clique em **Dados de um servidor** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **JDBC**.
3. Clique em **Avançar**.
4. Na área **Informações de JDBC** na página **Informações de JDBC**, clique em **Procurar** para conectar-se a um banco de dados e construa sua Consulta SQL.

   Use o navegador JDBC para conectar-se a um banco de dados e visualizar suas tabelas, para que você possa construir uma consulta SQL que coleta os dados que você precisa. Ao selecionar uma tabela e colunas, uma consulta será gerada para você e atributos serão incluídos para cada uma das colunas retornadas pela consulta. É possível modificar e testar a consulta que é gerada para verificar se os dados que forem retornados são os dados necessários.

   Nota: Você também pode criar manualmente a origem de dados JDBC sem clicar em **Procurar**. Se desejar criar manualmente a origem de dados, especifique a consulta e clique em **Avançar**. Deve-se definir um atributo para cada coluna retornada pela consulta, na ordem em que as colunas são retornadas.

   Com o provedor de dados JDBC, é possível executar consultas SQL e procedimentos armazenados com relação a um banco de dados para coletar dados de monitoramento. Ao especificar uma consulta SQL para coletar dados, é possível incluir uma cláusula where em sua instrução SQL para filtrar os dados retornados. A instrução SQL também pode unir dados a partir de várias tabelas. Além das instruções select SQL, o provedor de dados JDBC pode executar procedimentos armazenados. Para obter informações sobre como executar procedimentos armazenados, consulte “Procedimentos armazenados” na página 1292.
5. A primeira vez em que o Navegador for aberto, a janela Navegador de Java Database Connectivity (JDBC) indica que nenhuma conexão está selecionada. Você deve incluir uma conexão. Clique em **Incluir** e siga as Etapas para incluir uma conexão.

   Se você já definiu uma conexão, essa conexão é usada e é possível continuar para a Etapa “6” na página 1288.

   Nota: O campo **Status** mostra o status da conexão atual.

   Use as etapas a seguir para incluir uma conexão:

   a) Na página **Conexões JDBC**, clique em **Conexão JDBC** e clique em **Avançar**.

   b) Na página **Propriedades da Conexão**, preencha os campos da seguinte forma:

Nome de Conexão
Nome da conexão do JDBC. Digite um nome exclusivo para essa conexão. Use esse nome para referenciar a conexão no navegador.

Database Type
O tipo do banco de dados. Selecione o produto de banco de dados para o qual você está conectando. Por exemplo, para se conectar ao banco de dados IBM DB2, selecione **DB2**.

Nome do Usuário
Deve ser definido com pelo menos acesso de leitura ao banco de dados, mas não tem de ser o administrador de banco de dados

Password
Deve ser definido com pelo menos acesso de leitura ao banco de dados, mas não tem de ser o administrador de banco de dados

Nome de Host
Nome do host em que o servidor de banco de dados está em execução. Com JDBC, é possível monitorar bancos de dados remotos, assim você não está restrito a monitorar bancos de dados no sistema local.

Port
Porta no nome do host em que o servidor de banco de dados está atendendo.

Banco de Dados
Nome do banco de dados a ser conectado.

Diretório Jar
Diretório contendo os arquivos JAR JDBC usados para conectar-se ao banco de dados. Digite o nome do caminho ou clique em **Procurar** para localizar o diretório.

c) Opcional: Selecione a caixa de opção **Salvar a senha na área de trabalho do Agent Builder** se desejar salvar a senha para esta conexão.

d) Opcional: Selecione a caixa de opção **Configurar como Padrões de Configuração do Agente**, se desejar que os padrões para este tipo de servidor de aplicativos sejam copiados destas propriedades.

Se você estiver construindo o agente em um sistema que é semelhante a seus sistemas monitorados, é aconselhável verificar essa caixa. Se essa caixa não for marcada, o usuário que configura o agente vê um campo vazio. O usuário deve então determinar os valores para todas as informações sem valores padrão.

e) Clique em **Conexão de Teste** para criar uma conexão com o banco de dados que usa os parâmetros de configuração que você especificou.

Uma mensagem na página **Propriedades de Conexão** indica se a conexão é bem-sucedida.

f) Quando tiver uma conexão ativa, clique em **Concluir**.

6. Na janela **Navegador do Java Database Connectivity (JDBC)**, é feita uma conexão com o banco de dados configurado. As tabelas contidas no banco de dados são mostradas na área **Tabelas de Banco de Dados**. Selecione a tabela de banco de dados para ver as colunas contidas nessa tabela na área **Colunas na tabela selecionada**.

Nota:

a. Clique no ícone de binóculos para procurar por uma tabela na lista **Tabelas de Banco de Dados**.

b. Todas as tabelas são mostradas por padrão. É possível filtrar as tabelas mostradas selecionando uma opção de filtro diferente. As opções de filtro disponíveis são mostradas em Tabela 267 na página 1288.

Tabela 267. Opções de filtro

Opção de filtro	Descrição
Todos	Mostrar todas as tabelas
Usuário	Mostrar somente tabelas de usuários

Tabela 267. Opções de filtro (continuação)	
Opção de filtro	**Descrição**
Sistema	Mostrar somente tabelas de sistemas
Visualizar	Mostrar somente visualizações do banco de dados

Nota: Se você deseja recuperar colunas específicas, selecione somente essas colunas. Se você selecionar a tabela, o Agent Builder constrói automaticamente uma consulta que reúne todas as colunas a partir da tabela e cria atributos para todas as colunas que estiverem na tabela no momento.

É possível selecionar as colunas nas seguintes formas:

- Selecione a tabela e obtenha a consulta padrão para todas as colunas.
- Selecione as colunas para obter somente essas colunas.

7. Opcional: Modifique os valores de enumeração que são configurados para Erro, Dados ausentes e Sem valor na página **Informações sobre o Atributo**.

   Modifique os valores para evitar qualquer sobreposição com valores legitimados que podem ser retornados de colunas da tabela de banco de dados.

8. Opcional: Clique em **Testar** na janela do navegador **Java Database Connectivity (JDBC)** para testar e modificar a instrução SQL.

   A janela **Executar a instrução SQL** é aberta.

   a) Digite ou modifique a instrução SQL no campo **Instrução SQL**.

   b) Clique em **Executar** para executar a instrução SQL.

      Os resultados são exibidos na área **Resultados**. Continue a modificar e testar a instrução até estar satisfeito com os dados que são retornados.

   c) Clique em **OK** para salvar a instrução, crie os atributos corretos e retorne à janela **Informações de JDBC**.

9. Opcional: Clique em **Testar** na janela **Informações de JDBC** para testar o grupo de atributos em um ambiente de agente mais realista. Para obter informações adicionais sobre como testar grupos de atributos de JDBC, consulte “Testando Grupos de Atributos JDBC” na página 1293. Se você mudar a instrução JDBC durante esse teste, também deve ajustar os atributos de forma que haja um atributo por coluna retornado pela instrução JDBC, na ordem correta.
10. Opcional: É possível criar um filtro para limitar os dados retornados por esse grupo de atributos clicando em **Avançado**. Para obter informações adicionais sobre filtragem de dados de um grupo de atributos, consulte “Filtrando Grupos de Atributos” na página 1201
11. Na página **Informações de JDBC**, na seção **Sistemas Operacionais**, selecione os sistemas operacionais e clique em **Avançar**. Consulte “Especificando Sistemas Operacionais” na página 1213 para obter informações sobre quais sistemas operacionais devem ser selecionados.

    Nota: Clique em **Inserir Propriedade de Configuração** para selecionar uma propriedade a ser inserida. Para obter mais informações, consulte (“Customizando configuração do agente” na página 1364).
12. Na página **Selecionar Atributos-chave**, selecione os atributos-chave ou indique que esta origem de dados produz somente uma linha de dados. Para obter mais informações, consulte “Selecionando Atributos-Chaves” na página 1172.
13. Se você deseja testar uma origem de dados que definiu anteriormente, na janela do Agent Editor, selecione **Origens de Dados** e selecione uma origem de dados JDBC. Na área **Informações do Grupo de Atributos JDBC**, clique em **Testar**. Para obter informações adicionais sobre teste, consulte “Testando Grupos de Atributos JDBC” na página 1293.
14. Se desejar visualizar as seções de configuração que foram geradas automaticamente, clique na guia **Inserir Propriedade de Configuração** do Agent Editor.

É possível alterar os rótulos ou valores padrão para essas propriedades para corresponder aos padrões que o usuário vê quando configuram inicialmente o agente.

15. Opcional: Conclua a página **Informações do Atributo** ; para obter detalhes, consulte "Campos e Opções para Definir Atributos" na página 1195. Execute essa etapa se optou por criar manualmente a origem de dados JDBC sem clicar em Procurar na etapa "4" na página 1287.

    A origem de dados do Agent Builder JDBC suporta coletar dados da maioria dos tipos SQL. As informações da Tabela 268 na página 1290 descrevem o tipo de atributo que é criado pelo Navegador do JDBC quando ele detecta uma coluna de um desses tipos. Esses tipos de dados são os tipos suportados para uso com o agente de monitoramento.

Tabela 268. Tipos de dados SQL suportados para uso com um agente de monitoramento

Tipo de dados SQL	**IBM Tivoli Monitoring atributo que é criado**
BIGINT	Esse tipo de dado é um valor de calibrador de 64 bits no IBM Tivoli Monitoring. Se você selecionar a compatibilidade IBM Tivoli Monitoring V6.2, ela terá um calibrador de 32 bits.
DECIMALDOUBLEFLOATNUMERICREAL	Esses Tipos de SQL são criados como atributos de calibrador de 64 bits no IBM Tivoli Monitoring. Se os metadados do banco de dados contiverem um valor escalar, esse valor será usado, caso contrário, a escala será configurada como 1. Se você selecionar a compatibilidade IBM Tivoli Monitoring V6.2, o atributo será um calibrador de 32 bits.
BITINTEGERSMALLINTTINYINT	Os tipos de SQL a seguir são criados como atributos de calibrador de 32 bits no IBM Tivoli Monitoring.
BOOLEAN	Este valor é um calibrador de 32 bits em IBM Tivoli Monitoring com enumerações para TRUE e FALSE.
TIMESTAMP	Os dados nas colunas desse tipo são convertidos em um atributo de registro de data e hora do IBM Tivoli Monitoring de 16 bits.
TIMEDATECHARLONGVARCHARVARCHAR	Esses tipos SQL são todos tratados como atributos de cadeia pelo navegador. O tamanho da coluna é usado como o tamanho do atributo até 256, que é o tamanho padrão do atributo de cadeia para o navegador do JDBC.

    Nota: Se você coletar dados a partir de um tipo de dados que não estiver listado, um atributo de cadeia será usado por padrão. O agente também tenta coletar os dados a partir do banco de dados como uma cadeia.

    Modifique os valores de enumeração que são configurados para Erro, Dados ausentes e Sem valor na página **Informações sobre o Atributo**, se necessário. Modifique os valores para evitar qualquer sobreposição com valores legitimados que podem ser retornados de colunas da tabela de banco de dados.

Configuração JDBC

Quando você define uma origem de dados JDBC em seu agente, algumas propriedades de configuração são criadas para você.

Se você definir uma origem de dados JDBC em seu agente, o agente deverá usar Java para se conectar ao servidor de banco de dados JDBC. As propriedades de configuração de Java são incluídas no agente

automaticamente. As seguintes propriedades de configuração de Java são específicas à configuração do tempo de execução do agente:

- *Java Home*: Um caminho completo que aponta para o diretório de instalação Java
- *JVM Arguments*: Use este parâmetro para especificar uma lista opcional de argumentos para a Java virtual machine.
- *Trace Level*: Este parâmetro define a quantidade de informações a serem gravadas no arquivo de log de rastreio Java. O padrão é gravar somente dados de erros no arquivo de log.

Nota: O Agent Builder não requer as propriedades Java porque usa a sua própria JVM e criação de log, que são configurados por meio do plug-in JLog.

Se você definir uma origem de dados do JDBC em seu agente, os seguintes campos de configuração necessários comuns serão incluídos no agente automaticamente:

- *Tipo de banco de dados JDBC*: Tipo de banco de dados ao qual você está se conectando, IBM DB2, Microsoft SQL Server ou Oracle Database Server.
- *Nome do usuário JDBC*: Nome do usuário que é usado para autenticar-se com o servidor de banco de dados.
- *Senha do JDBC*: Senha que é utilizada para autenticar-se com o servidor de banco de dados.
- *Caminhos Base*: Lista de diretórios que são procurados por arquivos JAR denominados no campo de *Caminho de Classe*, ou diretórios denominados no campo *Diretórios JAR*, que não estão totalmente qualificados. Os nomes de diretório são separados por ponto-e-vírgula (`;`) no Windows, e por ponto e vírgula (`;`) ou dois pontos (`:`) nos sistemas UNIX.
- *Caminho de Classe*: Arquivos JAR explicitamente nomeados para serem procurados pelo agente. Todos os arquivos que não estão totalmente qualificados são anexados em cada um dos Caminhos Base até que o arquivos JAR seja encontrado.
- *Diretórios JAR*: Lista de diretórios que são procurados por arquivos JAR. Os nomes de diretório são separados por ponto-e-vírgula (`;`) no Windows, e por ponto e vírgula (`;`) ou dois pontos (`:`) nos sistemas UNIX. Os arquivos JAR nesses diretórios não precisam ser explicitamente identificados; eles são localizados porque estão em um desses diretórios. Os subdiretórios destes diretórios não são procurados. Quaisquer diretórios não totalmente qualificados são anexados em cada Caminho de Classe até que o diretório seja localizado.

A configuração do tempo de execução também requer especificar alguns detalhes adicionais para conectar-se com o banco de dados. Você pode escolher como especificar os itens de configuração restantes, seja como uma URL JDBC ou como propriedades de configuração básica (o padrão):

- Opção de configuração de URL
  - URL de conexão JDBC: URL de conexão específica do fornecedor que fornece detalhes sobre em qual host o banco de dados está localizado e o número da porta no qual conectar. O formato da URL normalmente se parece com o seguinte:

    ```
    jdbc:identificador://servidor:porta/banco de dados
    ```

    Consulte a documentação do fornecedor do driver JDBC para obter formatos de URL diferentes.
- Opção de Propriedades Básicas do JDBC (padrão)

  Nome do servidor JDBC: Nome do host no qual o servidor do banco de dados está em execução.
  Nome do banco de dados JDBC: Nome do banco de dados no host em que a conexão é realizada.
  Número da porta JDBC: O número da porta na qual o servidor de banco de dados está atendendo.

Nota: Com o provedor de dados JDBC, é possível monitorar vários tipos de banco de dados no mesmo agente usando os subnós. Para monitorar dessa maneira, você deve definir cuidadosamente as Substituições de Configuração de Subnós. Se você monitorar múltiplos tipos de banco de dados, as seguintes definições de configuração provavelmente serão diferentes:

- tipo de banco de dados JDBC
- nome de usuário JDBC

- senha JDBC

Se você estiver usando a opção de configuração básica, deverá definir também as substituições para as seguintes propriedades na página **Substituições de Configuração do Subnó**:

- nome do servidor JDBC
- número da porta JDBC
- nome do banco de dados JDBC

Para definir as substituições de configuração para seu subnó, consulte "Usando subnós" na página 1347 para obter detalhes adicionais sobre o acesso à página **Substituições de Configuração do Subnó**. Quando configurar o agente no tempo de execução, todas essas propriedades devem ser configuradas para cada nova instância de subnó criada.

Além das substituições da configuração, seu agente também deve apontar para drivers JDBC para cada tipo de banco de dados que você pretende conectar-se a partir de seus subnós. O parâmetro *Diretórios JAR* é a maneira mais conveniente de apontar para seus drivers JDBC. Lista de diretórios que contêm os drivers JDBC, usando ponto-e-vírgula para separar cada diretório. Por exemplo, se estiver se conectando aos bancos de dados DB2 e Oracle com o agente, você deve especificar um valor *JAR directories* semelhante a este exemplo: `C:\Program Files\IBM\SQLLIB\java;C:\oracle\jdbc`.

Procedimentos armazenados
Exemplo de procedimentos armazenados do SQL e do DB2 que podem ser usados com o provedor de dados JDBC.

O provedor de dados JDBC pode processar os conjuntos de resultados retornados por um procedimento armazenado. Parâmetros de entrada de sequência ou número inteiro podem ser transmitidos ao procedimento armazenado. A seguinte sintaxe executa um procedimento armazenado:

```
call[:index] procedureName [argument] ...
```

Em que:

índice
Um número inteiro opcional que especifica qual conjunto de resultados deve ser utilizado pelo provedor de dados. Esse parâmetro é útil quando o procedimento armazenado retorna múltiplos conjuntos de resultados e você deseja somente coletar os valores de um dos conjuntos de resultados. Se um índice não for especificado, os dados de cada conjunto de resultados são coletados e retornados.

procedureName
O nome do procedimento armazenado que deve ser executado pelo provedor de dados JDBC.

argument
Um argumento de entrada para o procedimento armazenado. Múltiplos argumentos devem ser separados por um espaço. Se o argumento contiver um caractere de espaço, coloque todo o argumento entre aspas duplas. Se o argumento puder ser analisado como um número inteiro ele é transmitido ao procedimento armazenado como um argumento de número inteiro. Qualquer argumento colocado entre aspas duplas é transmitido como um argumento de sequência.

Amostras do SQL Server
`call sp_helpdb`

Executa o procedimento `call sp_helpdb` que requer nenhum argumento. Os dados de todos os conjuntos de resultados retornados são incluídos nos dados retornados pelo provedor de dados.

`call:2 sp_helpdb master`

Executa o procedimento `sp_helpdb` com o argumento principal. Este argumento é um argumento de entrada de sequência. Somente os dados do segundo conjunto de resultados retornado pelo procedimento armazenado são incluídos nos dados retornados pelo provedor de dados.

Quando o índice não é especificado, os dados de todos os conjuntos de resultados retornados são coletados. Você deve se certificar de que os dados retornados nesses casos são compatíveis com os

atributos que você define. O Agent Builder cria atributos a partir do primeiro conjunto de resultados retornado, e para quaisquer conjuntos de resultados adicionais esperados, espera-se que sejam compatíveis com o primeiro conjunto.

Procedimento Armazenado do DB2

Aqui está uma função do DB2 de amostra que está escrita em SQL. Essa função demonstra como retornar resultados que podem ser processados pelo provedor de dados JDBC do Agent Builder:

```
-- Execute este script como a seguir:
-- db2 -td# -vf db2sample.sql

-- Procedimento para demonstrar como retornar uma consulta de
-- um procedimento armazenado DB2, que pode então ser usado por
-- um provedor JDBC do Agent Builder. O procedimento armazenado
-- retorna as colunas a seguir:
-- Nome      Descrição         Tipo de Dados
-- current_timestamp A hora atual do sistema registro de data e hora
-- lock_timeout    Tempo limite do bloqueio escala numérica 0
-- user        O usuário da sessão    Sequência de 128 caracteres de comprimento
DROP procedure db2sample#

CREATE PROCEDURE db2sample()
  RESULT SETS 1
  LANGUAGE SQL
BEGIN ATOMIC

  -- Defina o SQL para a consulta
  DECLARE c1 CURSOR WITH HOLD WITH RETURN FOR
  SELECT CURRENT TIMESTAMP as current_timestamp,
CURRENT LOCK TIMEOUT as lock_timeout, CURRENT USER as user
  FROM sysibm.sysdummy1;

  -- Emita a consulta e retorne os dados
  OPEN c1;
END#
```

Esta função pode ser chamada a partir do Agent Builder usando a mesma sintaxe definida para outros procedimentos armazenados. Neste caso, você define `call db2sample` como sua instrução JDBC para executar esse procedimento armazenado.

Procedimentos armazenados Oracle

Os procedimentos armazenados Oracle não retornam conjuntos de resultados. Em vez disso, você deve gravar uma função que retorne um cursor de referência Oracle. Veja a seguir uma função Oracle de amostra gravada em PL/SQL que demonstra como retornar resultados que podem ser processados pelo provedor de dados JDBC do Agent Builder:

```
CREATE OR REPLACE FUNCTION ITMTEST
RETURN SYS_REFCURSOR
IS
       v_rc SYS_REFCURSOR;
BEGIN
  OPEN v_rc FOR SELECT * FROM ALL_CLUSTERS;
  RETURN v_rc;
END;
```

Esta função pode ser chamada a partir do Agent Builder usando a mesma sintaxe definida para outros procedimentos armazenados. Nesse caso, você define `call ITMTEST` como sua instrução JDBC para executar esse procedimento armazenado. Como a função Oracle deve retornar uma referência de cursor, somente um conjunto de resultados pode ser processado pelas funções Oracle. Isto significa que a opção de índice não é suportada para Oracle porque não há como retornar vários conjuntos de resultados.

Testando Grupos de Atributos JDBC

É possível testar o grupo de atributos JDBC criado no Agent Builder.

Procedimento

1. É possível iniciar o procedimento de Teste das seguintes maneiras:
   - Durante a criação do agente, clique em **Testar** na página **Informações de JDBC**.
   - Após a criação do agente, selecione um grupo de atributos no Agent Editor **Definição de Origem de Dados** e clique em **Testar**. Para obter informações adicionais sobre o Agent Editor, consulte "Usando o Agent Editor para modificar o agente" na página 1172.

   Após clicar em **Testar** em uma das duas etapas anteriores, a janela **Testar Instrução JDBC** é exibida.
2. Opcional: Antes de iniciar seu teste, é possível configurar as variáveis de ambiente, as propriedades de configuração e as informações Java.

   Para obter mais informações, consulte "Teste de Grupo de Atributos" na página 1380. Para obter informações adicionais sobre as propriedades de configuração JDBC, consulte ("Configuração JDBC" na página 1290).
3. Clique em **Iniciar Agente**.

   Uma janela indica que o Agente está iniciando.
4. Para simular uma solicitação a partir do Tivoli Enterprise Portal ou SOAP para dados do agente, clique em **Coletar Dados**.

   O agente consulta o banco de dados com a consulta SQL especificada. A janela **Testar Instrução JDBC** coleta e mostra dados no cache do agente, desde que ele tenha iniciado por último.

   Nota: A ordem dos dados retornados é significativa; por exemplo, o valor dos dados na primeira coluna retornada sempre é designado ao primeiro atributo. Se você alterar a instrução JDBC, deve-se incluir, remover ou reordenar os atributos para corresponder às colunas retornadas pela instrução.
5. Opcional: Clique em **Verificar Resultados**, se os dados retornados não estiverem conforme o esperado.

   A janela **Status de Coleção de Dados** é aberta e mostra informações adicionais sobre os dados. Os dados coletados e exibidos pela janela Status da Coleção de Dados são descritos em "Nó de Status do Objeto de Desempenho" na página 1424
6. Pare o agente, clicando em **Parar Agente**.
7. Clique em **OK** ou **Cancelar** para sair da janela **Testar Instrução JDBC**. Clicar em **OK** salva quaisquer mudanças que tiver feito.

Conceitos relacionados

"Testando seu agente no Agent Builder" na página 1380
Depois de usar o Agent Builder para criar um agente, será possível testar o agente no Agent Builder.

Monitorando a disponibilidade do sistema usando Ping

É possível definir uma origem de dados para testar uma lista de dispositivos de rede usando o ping de repetição do Internet Control Message Protocol (ICMP). O nome do host ou o endereço IP dos dispositivos que você deseja testar estão listados em um ou mais arquivos de listas de dispositivos. Um arquivo de configuração de Ping separado especifica o caminho para cada arquivo de lista de dispositivos. Em seguida, o nome do arquivo de configuração de Ping é definido na configuração de tempo de execução do agente. Os resultados incluem o status de cada dispositivo de rede.

Antes de Iniciar

Crie arquivos de lista de dispositivos e um arquivo de configuração de ping (consulte "Arquivos de configuração" na página 1295).

Sobre Esta Tarefa

Parte do gerenciamento de rede envolve a capacidade de determinar se os sistemas respondem a um ping do Internet Control Message Protocol (ICMP). Use esta origem de dados para monitorar o status básico online e offline para um conjunto de servidores ou outros dispositivos críticos em seu ambiente. O

monitoramento com ping é simples e pouco sobrecarregado. Para monitorar uma lista de dispositivos, inclua o coletor de dados de Ping no agente.

Procedimento

1. Na página **Origem de Dados Inicial do Agente** ou na página **Local de Origem de Dados**, clique em **Dados de Gerenciamento de Rede** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **Ping**.
3. Clique em **Avançar**.
4. Na área **Sistemas Operacionais** na janela **Informações de Ping**, selecione os sistemas operacionais.
5. Opcional: Você pode testar este grupo de atributos, clicando em **Testar**. Para obter informações adicionais sobre teste, consulte “Testando grupos de atributos de Ping” na página 1296
6. Opcional: É possível criar um filtro para limitar os dados retornados por esse grupo de atributos clicando em **Avançado**. Para obter informações adicionais sobre filtragem de dados de um grupo de atributos, consulte “Filtrando Grupos de Atributos” na página 1201
7. Execute uma das seguintes etapas:
   a) Se estiver usando o assistente de **Agente**, clique em **Avançar**.
   b) Clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor.
8. Para obter informações adicionais sobre a inclusão dos atributos, consulte (“Criando Atributos” na página 1192).

Resultados

Para obter mais informações sobre os grupos de atributos para Ping, consulte “Grupo de Atributos de Ping” na página 1454.

Arquivos de configuração

Forneça ao agente a lista de dispositivos dos quais executar ping usando arquivos de configuração.

O agente requer dois tipos de arquivos de configuração.

Arquivo de lista de dispositivos

Inclui uma lista de dispositivos dos quais executar ping. Se você possuir muitos dispositivos, poderá dividi-los em múltiplos arquivos de lista de dispositivos. O agente inicia um encadeamento separado para cada arquivo de lista de dispositivos e executa ciclos por meio dos arquivos em paralelo. Ele executa ciclos por meio de cada arquivo a cada 60 segundos ou a cada 30 segundos mais o tempo que leva para executar ping na lista, o que levar mais tempo.

A sintaxe do arquivo de lista de dispositivos é a seguinte:

```
LISTNAME=list_name
device_name or host_name
device_name or host_name
device_name or host_name device_name or host_name
```

em que *list_name* é uma descrição para os dispositivos nesse arquivo. Se nenhum nome de lista estiver definido, o nome do arquivo de lista de dispositivos será usado. O nome da lista não precisa ser a primeira entrada no arquivo. No entanto, se o arquivo tiver múltiplas definições de nomes da lista, a última definição será usada.

Não há limite para o número de dispositivos que é possível incluir em um arquivo de lista de dispositivos. No entanto, a inclusão de muitas entradas vai contra o propósito de ter uma lista destinada de dispositivos críticos e aumenta a carga de trabalho geral. Pode ser mais difícil recuperar o status de cada dispositivo dentro do intervalo de monitoramento de 60 segundos.

No início de cada ciclo, o agente verifica a hora da última modificação do arquivo de lista de dispositivos. Se o horário da última modificação do arquivo for mais recente que o último horário que o agente leu o arquivo, o agente lerá novamente o arquivo sem exigir uma reinicialização.

Arquivos de configuração de Ping
Especifica o local de cada arquivo de lista de dispositivos. Use o caminho completo ou um caminho relativo ao local do arquivo de configuração de ping. O arquivo de configuração de ping é transmitido como um parâmetro de configuração de tempo de execução para o agente.

Exemplo

No exemplo a seguir, os dispositivos são divididos em dois arquivos.
O arquivo `/data/retailList.txt` contém as entradas a seguir:

```
LISTNAME=Retail
frontend.mycompany.com
productdb.mycompany.com
```

O arquivo `/data/manufacturingList.txt` contém as entradas a seguir:

```
LISTNAME=Manufacturing systems
manufloor.mycompany.com
stats.supplier.com
```

O arquivo de ping, `/data/pinglists.txt`, contém as entradas a seguir:

```
/data/retailList.txt
/data/manufacturingList.txt
```

Propriedade de configuração de gerenciamento de rede

Depois que uma origem de dados de ping é incluída, a configuração é exibida na página **Informações de Configuração de Tempo de Execução** do Agent Editor.

A seção de configuração **Gerenciamento de Redes** da página **Informações de Configuração de Tempo de Execução** contém a propriedade a seguir:

Tabela 269. Propriedades de configuração de Gerenciamento de Rede

Nome	Valores Válidos	Obrigatório	Descrição
`Arquivo de configuração de Ping`	Caminho para um arquivo	Não. Se este arquivo não for fornecido, o arquivo `KUMSLIST` será usado a partir do diretório bin do agente.	O caminho para o arquivo que contém uma lista de arquivos, cada uma contendo uma lista de hosts para monitorar usando pings ICMP.

Testando grupos de atributos de Ping
É possível testar o grupo de atributos de Ping que você criou no Agent Builder.

Procedimento

1. É possível iniciar o procedimento de Teste das seguintes maneiras:
   - Durante a criação do agente, clique em **Testar** na página **Informações de Ping**.
   - Após a criação do agente, selecione um grupo de atributos no Agent Editor **Definição de Origem de Dados** e clique em **Testar**. Para obter informações adicionais sobre o Agent Editor, consulte "Usando o Agent Editor para modificar o agente" na página 1172.

   Depois de clicar em **Testar** em uma das duas etapas anteriores, a janela **Configurações de Teste** será aberta.
2. Opcional: Antes de iniciar o teste, você pode configurar as variáveis de ambiente e as propriedades de configuração. Para obter mais informações, consulte "Teste de Grupo de Atributos" na página 1380.

3. Clique em **Procurar** para selecionar um arquivo de configuração de Ping. Para obter informações adicionais sobre arquivos de configuração de Ping, consulte “Arquivos de configuração” na página 1295
4. Clique em **Iniciar Agente**. Uma janela indica que o Agente está iniciando.
5. Para simular uma solicitação a partir do ambiente de monitoramento para dados do agente, clique em **Coletar Dados**. O agente executa ping dos dispositivos especificados no arquivo de lista de dispositivos, que é referenciado a partir do arquivo de configuração de Ping.
6. A janela **Testar Configurações** coleta e mostra dados no cache do agente, desde que ele tenha iniciado por último.
7. Opcional: Clique em **Verificar Resultados**, se os dados retornados não estiverem conforme o esperado.

   A janela **Status de Coleção de Dados** é aberta e mostra informações adicionais sobre os dados. Os dados que são coletados e mostrados pela janela Status de Coleta de Dados são descritos em “Nó de Status do Objeto de Desempenho” na página 1424.
8. Pare o agente, clicando em **Parar Agente**.
9. Clique em **OK** ou **Cancelar** para sair da janela **Testar Configurações**. Clicar em **OK** salva quaisquer mudanças que tiver feito.

Conceitos relacionados

“Testando seu agente no Agent Builder” na página 1380
Depois de usar o Agent Builder para criar um agente, será possível testar o agente no Agent Builder.

Monitorando a Disponibilidade de HTTP e o Tempo de Resposta

É possível configurar uma origem de dados para monitorar a disponibilidade e o tempo de resposta de URLs selecionadas. Use um arquivo de configuração para definir uma lista de URLs. Configure o nome do arquivo na configuração de tempo de execução do agente. No IBM Tivoli Monitoring, também é possível usar comandos Executar ação para incluir e remover URLs monitoradas. O status de cada URL é incluído como uma linha no conjunto de dados resultante.

Sobre Esta Tarefa

Para cada URL que você monitora, os resultados fornecem informações gerais sobre a resposta de HTTP à solicitação de HTTP. Os resultados incluem se ela pode ser recuperada, quanto tempo leva para recuperar e o tamanho da resposta. Se o conteúdo da resposta for HTML, as informações sobre os objetos da página dentro da URL também serão fornecidas.

É possível monitorar URLs que usam os protocolos HTTP, HTTPS, FTP e File. As URLs são especificadas para serem monitoradas no arquivo de URLs de HTTP ou por meio das opções Executar Ação.

Importante: No momento da liberação, os comandos Executar ação não estavam disponíveis em um ambiente IBM Cloud Application Performance Management. Eles estão disponíveis somente em um ambiente Tivoli Monitoring.

Essa origem de dados requer um Java Runtime Environment. As seguintes versões Java são suportadas:

- Oracle Corporation Java Versão 5 ou mais recente
- IBM Corporation Java Versão 5 ou posterior

Use o seguinte procedimento para criar um grupo de atributos para monitorar uma lista de URLs:

Procedimento

1. Na página **Origem Inicial de Dados do Agente** ou na página **Local de Origem de Dados**, clique em **Dados de um servidor** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **HTTP**.
3. Clique em **Avançar**.
4. Na página **Informações de HTTP**, selecione um ou mais sistemas operacionais na área **Sistemas Operacionais**.

5. Opcional: Clique em **Testar** para testar esse grupo de atributos. Para obter informações adicionais sobre teste, consulte "Testando Grupos de Atributos HTTP" na página 1304
6. Opcional: Clique em **Avançado** para criar um filtro para limitar os dados que são retornados por este grupo de atributos. Para obter informações adicionais sobre filtragem de dados de um grupo de atributos, consulte "Filtrando Grupos de Atributos" na página 1201
7. Execute uma das seguintes etapas:
   a) Se estiver usando o assistente de **Agente**, clique em **Avançar**.
   b) Clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor.

Resultados

A origem de dados de HTTP cria dois grupos de atributos: URLs Gerenciadas e Objetos da URL. É possível incluir, modificar ou excluir atributos.

Tarefas relacionadas

"Criando Atributos" na página 1192

É possível incluir novos atributos em um conjunto de dados.

Referências relacionadas

"Grupos de Atributos HTTP" na página 1456

Os dois grupos de atributos HTTP, `URLs Gerenciadas` e `Objetos de URL`, são usadas para receber informações das URLs e os objetos dentro dessas URLs.

Tabelas de HTTP

Informações de referência sobre os grupos de atributos HTTP padrão.

Os dois grupos de atributos que são criados pela origem de dados HTTP são:

`URLs Gerenciadas`
A tabela de URLs Gerenciadas fornece dados de disponibilidade e de tempo de resposta sobre cada URL que está sendo monitorada.

`Objetos da URL`
A tabela de objetos de URL contém uma entrada de URL separada para cada objeto incorporado. Por exemplo, os arquivos `.gif` e `.jpg` que podem ser usados no website que está listado no relatório de URL gerenciado.

Para obter informações sobre a sintaxe usada nas URLs Gerenciadas e nas tabelas de Objetos da URL, consulte ("Campos Específicos para Atributos HTTP" na página 1299).

Quando desejar monitorar o tempo de resposta e a disponibilidade de objetos específicos em um website, revise o conteúdo da tabela Objetos de URL. A tabela Objetos de URL monitora uma lista específica de objetos que são detectados em arquivos HTML transferidos por download. A tabela a seguir lista os elementos HTML que são procurados por objetos a serem monitorados, e os atributos dentro desses elementos que fazem referência aos objetos:

Tabela 270. Elementos HTML procurados por objetos a serem monitorados

Elemento HTML	**Atributo que Contém o Objeto a Ser Monitorado**
`img`	`src`
`script`	`src`
`integrar`	`src`
`object`	`código base` ou `dados`
`corpo`	`plano de fundo`
`entrada`	`src`

No extrato de HTML de exemplo a seguir, o objeto que é monitorado é a imagem que é referenciada pelo atributo `src` do elemento `img`.

```
<img src="/v8/images/id-w3-sitemark-simple.gif" alt="" width="54" height="33" />
```

Uma URL completa para a imagem é calculada com base na URL para o documento de origem.

Nota: Se você não precisar monitorar os objetos localizados em uma página da web, na seção Configuração do Monitoramento de URL, configure a propriedade **Coleção de objetos de páginas** 6como **Não**.

Campos Específicos para Atributos HTTP

Na página **Informações do Atributo**, existem dois campos para atributos HTTP que definem como os dados são coletados a partir da URL. O campo **Tipo de Atributo** pode ser qualquer valor a partir de uma lista que controla as informações sobre a URL que é retornada. Alguns tipos de atributos requerem um valor no campo **Valor de Tipo**.

A tabela a seguir descreve todos os tipos de atributos para o grupo de atributos de URLs Gerenciadas, e o valor de tipo quando um for necessário:

Tabela 271. Informações sobre o Atributo de HTTP - URLs Gerenciadas

Tipo de Atributo	Descrição	Valor de tipo	Tipo de dados retornados	Diferenças com protocolos FTP e de arquivos
`Consulta XPath`	Executa uma consulta XPath no conteúdo que é retornado de uma conexão de URL. A consulta deve ser gravada para retornar dados úteis para um atributo, não uma lista de nós.	A consulta XPath para ser executada no conteúdo que é obtido de uma conexão de URL.	Os dados retornados podem ser uma sequência, um valor numérico ou de registro de data e hora. Se os dados estiverem no formato XML DateTime, é possível especificar registro de data e hora como um tipo de atributo. O agente converte o valor para Registro de Data e Hora Candle.	none
`Tempo de Resposta`	A quantidade de tempo em milissegundos que demorou para fazer download do conteúdo a partir da URL solicitada.	Nenhum	Número inteiro (número em milissegundos)	Nenhum
`Mensagem de Resposta`	A mensagem de resposta de HTTP que é retornada pelo servidor.	Nenhum	Cadeia	A mensagem de resposta somente será aplicada se a URL usar os protocolos HTTP ou HTTPS.

Tabela 271. Informações sobre o Atributo de HTTP - URLs Gerenciadas (continuação)

Tipo de Atributo	Descrição	Valor de tipo	Tipo de dados retornados	Diferenças com protocolos FTP e de arquivos
`Código de Resposta`	O código de resposta de HTTP que é retornado pelo servidor.	none	Integer	O código de resposta somente será aplicado se a URL usar os protocolos HTTP ou HTTPS. É sempre 0 para URLs de arquivos ou de FTP.
`Comprimento da Resposta`	O tamanho do conteúdo em bytes que é transferido por download da URL solicitada	none	Número inteiro (tamanho em bytes)	Nenhum
`Cabeçalho da Resposta`	O cabeçalho da resposta pode ser usado para recuperar um valor de um dos campos de cabeçalho de resposta da URL. O argumento especifica qual campo é solicitado.	O cabeçalho de resposta para coletar.	Cadeia	Geralmente, os protocolos de arquivos e FTP não possuem nenhum cabeçalho que possa ser coletado.
`URL da Solicitação`	A conexão é feita com esta URL. Todas as palavras-chave de resposta fornecem informações sobre a conexão com essa URL. A Consulta XPath pode ser usada para obter informações a partir do conteúdo retornado acessando esta URL.	none	Cadeia	Nenhum
`Objetos da Página`	O número de objetos que são descobertos na página HTML monitorada que são monitorados pelo grupo de atributos Objetos de URL.	Nenhum	Integer	Nenhum

Tabela 271. Informações sobre o Atributo de HTTP - URLs Gerenciadas (continuação)				
Tipo de Atributo	**Descrição**	**Valor de tipo**	**Tipo de dados retornados**	**Diferenças com protocolos FTP e de arquivos**
`Total do tamanho do objeto`	O tamanho total dos objetos monitorados no grupo de atributos Objetos de URL para esta página da web.	Nenhum	Número inteiro (em bytes)	Nenhum
`Alias`	O alias especificado pelo usuário para esta URL.	Nenhum	Cadeia	Nenhum
`Usuário`	Os dados especificados pelo usuário para esta URL.	Nenhum	Cadeia	Nenhum

A tabela a seguir descreve os tipos de atributos para o grupo de atributos dos Objetos da URL:

Tabela 272. Informações sobre o Atributo de HTTP - Objetos da URL				
Tipo de Atributo	**Descrição**	**Valor de tipo**	**Tipo de dados retornados**	**Diferenças com protocolos FTP e de arquivos**
`URL`	A URL que é monitorada na tabela de URLs Gerenciadas.	none	Cadeia	Nenhum
`Nome do Objeto`	A URL para o objeto que é monitorado na página **HTML**.	Nenhum	Sequência	Nenhum
`Tamanho do Objeto`	O tamanho em bytes do conteúdo que é transferido por download a partir da URL de Nome do Objeto.	Nenhum	Numérico	Nenhum
`Tempo de Resposta do Objeto`	O tempo em milissegundos que demorou para fazer download do objeto da página.	Nenhum	Numérico	Nenhum

Monitorando uma URL

É possível iniciar o monitoramento de qualquer URL incluindo-a no arquivo de URLs ou usando a opção Executar ação Incluir URL HTTP.

Arquivos das URLs

O arquivo de URLs especificado na configuração pode estar em qualquer diretório. Se esse arquivo não existir ou estiver vazio, será possível iniciar o monitoramento da URL usando Executar Ações. Para obter mais informações, consulte "Take Action option" na página 1302. Se você já possui um Tivoli Universal Agent que usa o Provedor de Dados HTTP do Tivoli Universal Agent, é possível reutilizar o arquivo KUMPURLS. Quando estiver configurando o agente, aponte para seu arquivo KUMPURLS.

A tabela a seguir fornece exemplos de como as URLs são inseridas no arquivo de URLs, dependendo do método no qual elas foram incluídas.

Tabela 273. Entradas de arquivos de URLs

URLs	Incluídas por

`www.bbc.co.uk`
`http://weather.com`
`www.ibm.com`
	Incluindo Entradas no Arquivo Manualmente. Se nenhum protocolo estiver especificado, como no exemplo `www.ibm.com`, o http será assumido.

`ftp://userid:password@ftpserver/index.html`	Incluídas manualmente usando o Protocolo de Transferência de Arquivos (FTP)
`http://www.ibm.com USER=ibm ALIAS=ibm`	Usando Executar ação Incluir URL HTTP
`file:/tmp/samples.html USER=samples \` `ALIAS=samples`	Usando Executar ação Incluir URL HTTP que usa FTP
`http://google.com INTERVAL=60 CACHE=50 \` `USER=google ALIAS=search`	Exemplo de arquivo KUMPURLS do Tivoli Universal Agent

Ao editar diretamente o arquivo de URLs, suas mudanças serão implementadas quando o agente fizer sua próxima coleção de dados.

Take Action option

Também é possível especificar URLs para monitorar por meio de uma opção Executar ação chamada `Incluir URL HTTP`.

Restrição: Essa opção não está disponível na liberação atual do IBM Cloud Application Performance Management, pois não é possível iniciar comandos Executar ação manualmente.

Quando esta opção está selecionada, é exibida uma janela na qual é possível especificar os parâmetros a seguir:

URL
Um parâmetro necessário que representa a própria URL. É possível digitar esse parâmetro com ou sem o prefixo `http://` ou `https://`.

Alias
Um parâmetro opcional que pode ser especificado para associar um nome mais significativo a uma URL. Nenhum espaço é permitido nesse parâmetro. Se esse parâmetro não for concluído, o Nome Alternativo será padronizado como em branco.

User_Data
Um parâmetro opcional que é possível especificar para inserir dados sobre a URL. Se esse parâmetro não estiver concluído, o `User_Data` padroniza para `INITCNFG`.

Após concluir as informações e fechar a janela, designe a ação `Inclusão de URL de HTTP` no sistema gerenciado de destino associado ao agente. O monitoramento é iniciado imediatamente para a nova URL. A URL também é incluída no arquivo de URLs, para que continue a ser monitorada por meio do reinício do agente.

Uma opção de Executar Ação correspondente é denominada Remoção de URL HTTP. Use a ação Remoção de URL HTTP para parar imediatamente o monitoramento de uma URL em particular. A URL removida também é excluída do arquivo de URLs. A janela **Remoção da URL HTTP** solicita somente os valores URL e User_Data. Os valores URL e User_Data devem corresponder aos valores vistos no Tivoli Enterprise Portal ou a ação Remover falha. Por exemplo, se você omitiu o http:// no campo URL da ação Incluir, você deve incluí-lo no campo URL da ação Remover. Se não especificar User_Data, deverá especificar INITCNFG como visto no Tivoli Enterprise Portal.

Se uma URL for incluída manualmente no arquivo de URLs, é possível excluí-la com Executar Ação. Se excluir com Executar Ação, você deve especificar os valores conforme visto no Tivoli Enterprise Portal. Por exemplo, se você incluiu www.ibm.com em seu arquivo de URLs, o Tivoli Enterprise Portal exibirá http://www.ibm.com como a URL e INITCNFG como User_Data. Para remover a URL com Executar Ação, você deve usar os valores vistos no Tivoli Enterprise Portal.

Após preencher as informações e fechar a janela, designe a ação Remover URL HTTP ao sistema gerenciado pelo destino associado ao agente.

Monitorar URLs https://
A origem de dados HTTP pode monitorar somente URLs seguras https:// que não precisam de acesso de script ou prompt interativo.

Se a URL https:// pode ser recuperada com uma chamada HTTP Get padrão, então ela pode ser monitorada.

Servidor Proxy
Se o sistema no qual o agente está em execução exigir um proxy para acessar o provedor de dados SOAP, você deve especificar as propriedades de configuração do servidor proxy.

Para obter mais informações, consulte "Configuração do Servidor Proxy" na página 1303.

Configuração de HTTP
Informações de referência sobre a configuração HTTP.

Após ser incluída uma origem de dados HTTP, a configuração é exibida na página **Configuração de Tempo de Execução** do Agent Editor. As seções de configuração são incluídas para Monitoramento de URL, para autenticação de Servidor Proxy e para Java.

Configuração de Monitoramento da URL

A seção de configuração de Monitoramento da URL contém as seguintes propriedades:

Tabela 274. Propriedades de configuração de monitoramento da URL

Nome	Valores Válidos	Obrigatório	Descrição
Arquivo de URLs de HTTP	Caminho para um arquivo	Sim	O caminho para o arquivo que contém uma lista de URLs.
Coleta de Objeto de Página	Sim, Não O valor padrão é Sim.	Não	Se fizer download dos objetos localizados em uma página da web e coletar dados a partir deles.

Configuração do Servidor Proxy

A seção de configuração do Servidor Proxy contém as seguintes propriedades:

Tabela 275. Propriedades de configuração do Servidor Proxy			
Nome	**Valores Válidos**	**Obrigatório**	**Descrição**
Nome de host de proxy	Cadeia	Não	O nome do host do proxy a ser usado para conexões de HTTP.
Nome do Usuário de Proxy	Cadeia	Não	O nome de usuário para o servidor proxy.
Porta do Proxy	Número inteiro positivo O valor padrão é 80.	Não	O número da porta HTTP do servidor proxy.
Senha de Proxy	Senha	Não	A senha para o servidor proxy.

Nota: Se a propriedade **Nome do Host do Proxy** estiver em branco, nenhum proxy será usado.

Configuração do Java

Se você definir uma origem de dados HTTP no seu agente, ele deverá usar Java para conectar-se ao servidor HTTP. As propriedades de configuração de Java são incluídas no agente automaticamente. As seguintes propriedades de configuração de Java são específicas à configuração do tempo de execução do agente. O Agent Builder não requer as propriedades Java porque usa sua própria JVM e criação de log, que são configurados por meio do plug-in JLog):

Tabela 276. Propriedades de configuração do Java			
Nome	**Valores Válidos**	**Obrigatório**	**Descrição**
Início do Java	Caminho completo para um diretório	Não	Um caminho completo que aponta para o diretório de instalação do Java.
Nível de Rastreio	Opção (O valor padrão é Erro)	Sim	Use essa propriedade para especificar o nível de rastreio usado pelos provedores Java.
Argumentos do JVM	Cadeia	Não	Use essa propriedade para especificar uma lista opcional de argumentos para a Java virtual machine.

Testando Grupos de Atributos HTTP

É possível testar o grupo de atributos HTTP criado no Agent Builder.

Procedimento

1. Inicie o procedimento de Teste das seguintes maneiras:
   - Durante a criação do agente, clique em **Testar** na página **Informações de HTTP**.
   - Após a criação do agente, selecione um grupo de atributos no Agent Editor **Definição de Origem de Dados** e clique em **Testar**. Para obter informações adicionais sobre o Agent Editor, consulte "Usando o Agent Editor para modificar o agente" na página 1172

   Após clicar em **Testar** em uma das duas etapas anteriores, a janela **Teste de HTTP** é exibida.

2. Clique em **Procurar** para selecionar o arquivo HTTP URLs. Para obter mais informações sobre arquivos de URLs, consulte "Arquivos das URLs" na página 1302.
3. Opcional: Antes de iniciar seu teste, é possível configurar as variáveis de ambiente, as propriedades de configuração e as informações Java.

   Para obter mais informações, consulte "Teste de Grupo de Atributos" na página 1380. Para obter mais informações sobre a configuração de HTTP, consulte "Configuração de HTTP" na página 1303.
4. Clique em **Iniciar Agente**.

   Uma janela indica que o Agente está iniciando.
5. Para simular uma solicitação a partir do Tivoli Enterprise Portal ou SOAP para dados do agente, clique em **Coletar Dados**.

   O agente monitora as URLs definidas no arquivo de URLs de HTTP. A janela **Teste de HTTP** exibe quaisquer dados retornados.
6. Opcional: Clique em **Verificar Resultados**, se os dados retornados não estiverem conforme o esperado.

   A janela **Status de Coleção de Dados** é aberta e mostra informações adicionais sobre os dados. Os dados coletados e exibidos pela janela Status da Coleção de Dados são descritos em "Nó de Status do Objeto de Desempenho" na página 1424
7. Pare o agente, clicando em **Parar Agente**.
8. Clique em **OK** ou **Cancelar** para sair da janela **Teste de HTTP**. Clicar em **OK** salva quaisquer mudanças que tiver feito.

Conceitos relacionados

"Testando seu agente no Agent Builder" na página 1380
Depois de usar o Agent Builder para criar um agente, será possível testar o agente no Agent Builder.

Monitorando dados a partir de uma origem de dados SOAP ou HTTP

É possível definir uma origem de dados para receber dados de um servidor HTTP (por exemplo, usando o protocolo SOAP). A origem de dados envia uma solicitação de HTTP para uma URL e analisa a resposta (nos formatos XML, HTML ou JSON) nos atributos do conjunto de dados resultante. É possível selecionar os dados que são recuperados da solicitação.

Sobre Esta Tarefa

Ao usar a origem de dados SOAP, é possível especificar uma URL HTTP e enviar uma solicitação GET, POST ou PUT. Para solicitações POST ou PUT, é possível especificar os dados POST associados. Uma resposta XML, HTML ou JSON é recuperada e analisada e os dados são expostos para o ambiente de monitoramento nos atributos. É possível definir os atributos como todos os valores dentro de um elemento específico. Ou é possível definir valores XPath customizados para especificar como preencher atributos individuais. Também é possível combinar os dois mecanismos.

Use o procedimento a seguir para coletar e analisar respostas XML, HTML ou JSON em uma URL:

Procedimento

1. Na página **Origem Inicial de Dados do Agente** ou na página **Local de Origem de Dados**, clique em **Dados de um servidor** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **SOAP**.
3. Clique em **Avançar**.
4. Na página **Informações de SOAP**, insira uma URL.

   O valor padrão é:

   ```
   http://${KQZ_HTTP_SERVER_NAME}:${KQZ_HTTP_PORT_NUMBER}
   ```

   Nota: É possível usar uma variável de configuração ou diversas variáveis de configuração que são resolvidas para uma URL. Clique em **Inserir Propriedade de Configuração** para selecionar uma

propriedade a ser inserida. Para obter mais informações, consulte “Customizando configuração do agente” na página 1364.

5. Selecione um tipo de solicitação. O tipo de solicitação padrão é Get. Para solicitações Post e Put, insira os dados a serem processados.

   Nota: Para solicitações Post e Put, a opção **Inserir Propriedade de Configuração** é ativada. Clique em **Inserir Propriedade de Configuração** para incluir uma variável de configuração nos dados a serem processados. Para obter mais informações, consulte (“Customizando configuração do agente” na página 1364).

6. Clique em **Procurar**

   Nota: Se depois de inserir uma URL e selecionar um tipo de solicitação, você não desejar usar o navegador SOAP para construir a definição, insira um **XPath de Seleção de Linha**. Insira **XPath de Seleção de Linha** na janela **Informações de SOAP**. Em seguida, defina todos os atributos para o grupo de atributos.

7. Na janela **Navegador SOAP**, execute as etapas a seguir:
   a) Insira uma URL e selecione um tipo de solicitação, se ainda não fez isso.
   b) Clique em **Configuração** para configurar quaisquer propriedades de configuração que sejam referenciadas na URL ou outros campos.
   c) Clique em **Conectar** para obter dados do provedor SOAP.

      Ao se conectar à URL, uma lista de elementos XML para esta URL é mostrada em uma árvore Modelo de Objeto de Documento (DOM). Uma resposta HTML ou JSON é convertida em XML e exibida como uma árvore DOM. Para obter detalhes sobre a conversão de uma resposta JSON em XML, consulte “Representação XML de dados JSON” na página 1309. No exemplo WebSphere Application Server em (Figura 44 na página 1307), a URL a seguir foi inserida:

      ```
      http://nc053011.tivlab.raleigh.ibm.com:9080/wasPerfTool/servlet
      /perfservlet?module= \threadPoolModule
      ```

      O elemento XML `PerformanceMonitor` é mostrado. Este elemento é o elemento XML de nível superior no documento XML retornado pelo provedor SOAP.

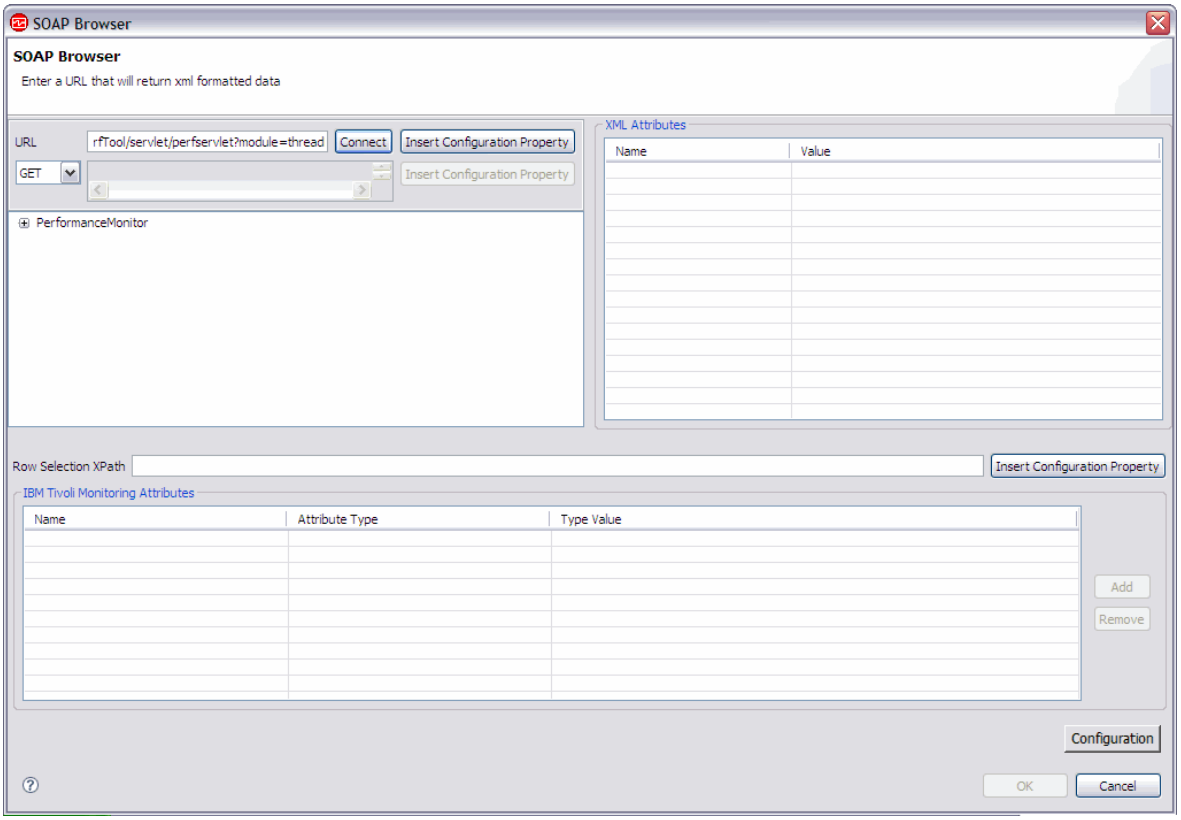


*Figura 44. Janela **Navegador SOAP***

d) Na árvore DOM, localize e selecione o nó XML que deseja configurar como o **XPath de Seleção de Linha**.

No exemplo WebSphere Application Server em (Figura 45 na página 1308), o nó `PerformanceMonitor/Node/Server/Stat/Stat/Stat` é selecionado. Esse nó representa uma linha de dados no grupo de atributos. Ao selecionar um nó na árvore DOM e clicar em **Incluir**, você obtém todos os atributos e elementos definidos nesse nó da árvore. (Você clica em **Incluir** na área **Atributos do agente**).

Quando um nó é selecionado, a área **Atributos XML** mostra quaisquer atributos XML definidos para o nó selecionado. Selecione um atributo XML e clique em **Incluir** para incluir esse atributo na lista de Atributos de agente.

Nota: Se mais de uma linha de dados for esperada, o XPath deverá ser mapeado para um conjunto de nós. Em que o XPath de Seleção de Linha retornar um nó que é configurado com somente um item, o grupo de atributos conterá somente uma linha.

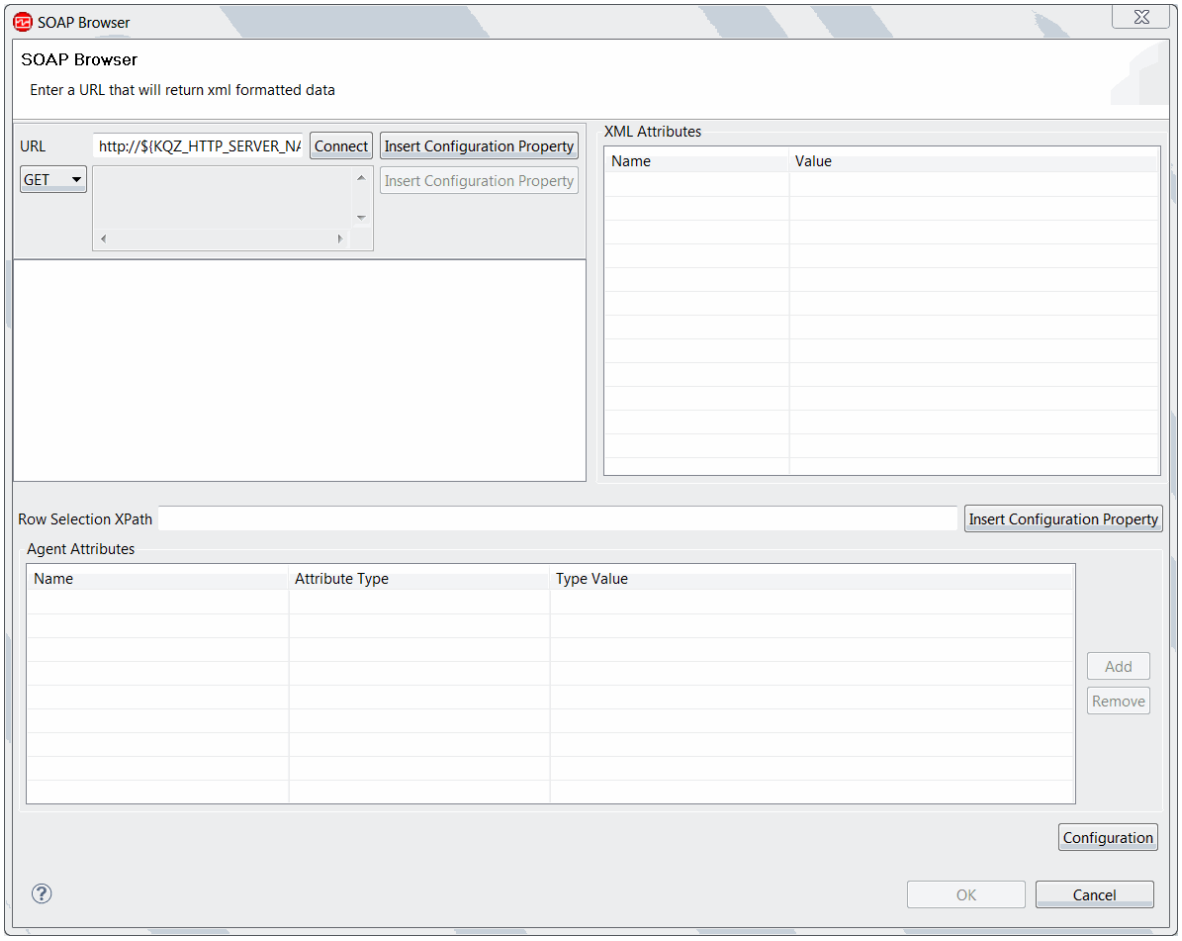


*Figura 45. Janela **Navegador SOAP***

e) Clique em **Incluir** na área Atributos de Agente.

A lista de atributos de agente é mostrada e o campo **XPath de seleção de linha** é preenchido.

O XPath para cada atributo de agente é usado para mapear os nós XML ou elementos para atributos do agente. No exemplo do WebSphere Application Server no Figura 46 na página 1309, o primeiro atributo na lista de atributos do agente, `Stat`, não é usado e seria removido.

É possível editar o nome e o XPath para um atributo de agente no campo **Valor de tipo**. Para obter mais informações sobre o uso de XPaths, consulte “Opções de XPath” na página 1312

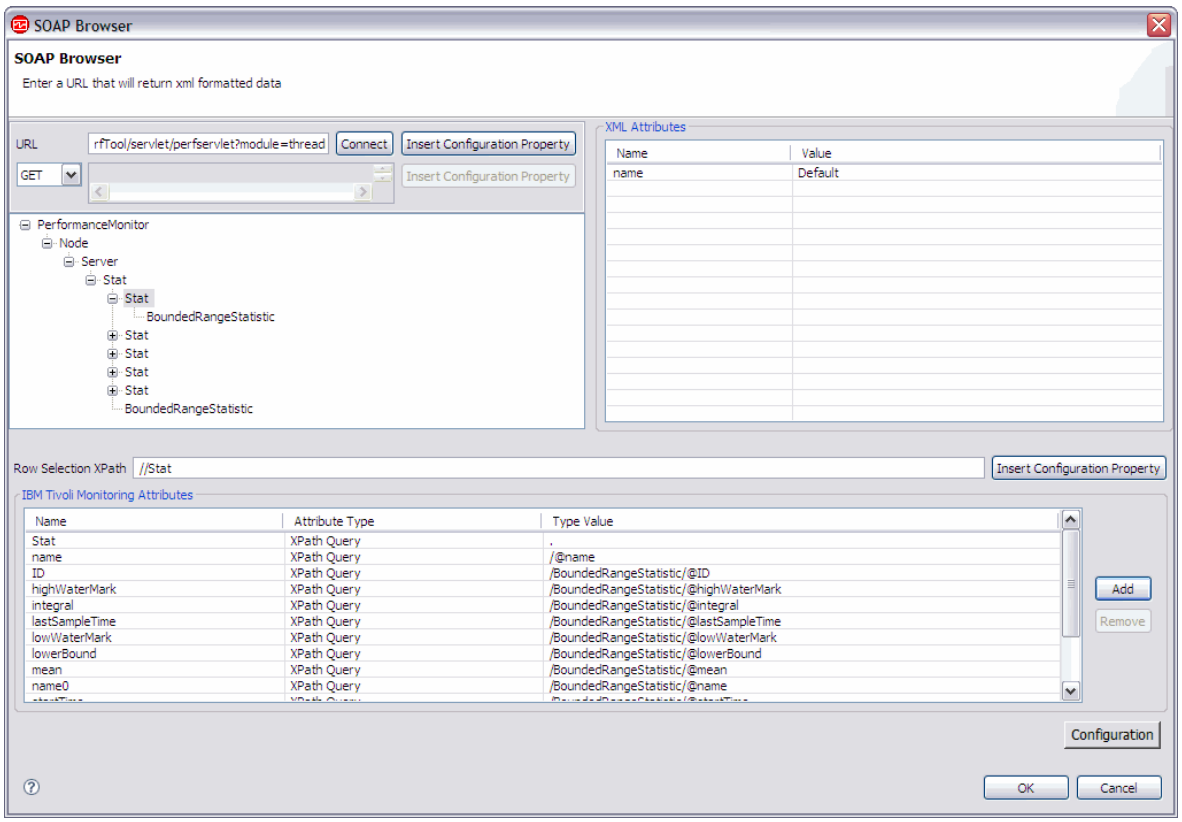


*Figura 46. Janela **Navegador SOAP***

f) Na janela **Navegador SOAP**, clique em **OK** para salvar suas alterações e retornar à janela **Informações de SOAP**.

8. Na janela **Informações de SOAP**, clique em **Avançar**.
9. Se você não usou **Procurar** antes e inseriu a **URL** e o **XPath de Seleção de Linha** na janela **Informações de SOAP**, a página **Informações do Atributo** será mostrada. Especifique as informações para o primeiro atributo na página **Informações do Atributo**, e clique em **Concluir**. É possível especificar atributos adicionais usando o Agent Editor. Para obter informações adicionais sobre a criação dos atributos, consulte (“Criando Atributos” na página 1192).
10. Se você usou a função **Procurar** na etapa “6” na página 1306, a página **Selecionar atributos-chave** será mostrada. Na página **Selecionar Atributos-chave**, selecione os atributos-chave ou indique que esta origem de dados produz somente uma linha de dados. Para obter mais informações, consulte “Selecionando Atributos-Chaves” na página 1172.
11. Opcional: Você pode testar este grupo de atributos, clicando em **Testar**. Para obter informações adicionais sobre teste, consulte “Testando Grupos de Atributo SOAP” na página 1313
12. Opcional: É possível criar um filtro para limitar os dados retornados por esse grupo de atributos clicando em **Avançado**. Para obter informações adicionais sobre filtragem de dados de um grupo de atributos, consulte “Filtrando Grupos de Atributos” na página 1201
13. Execute uma das seguintes etapas:
    a) Se estiver usando o assistente de **Agente**, clique em **Avançar**.
    b) Clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor.

Representação XML de dados JSON

Se a solicitação de HTTP retornar dados JSON, o provedor de dados converterá os dados em XML.

O provedor de dados converte o nome de um atributo JSON no nome do elemento. Para um atributo JSON de um tipo simples, ele converte o valor nos dados de texto dentro do elemento. Os objetos JSON integrados são convertidos em elementos XML integrados. Qualquer atributo subordinado é convertido em elemento subordinado.

O elemento XML raiz é `JSON_document`.

Se o nome de um atributo JSON contém caracteres que são inválidos em um nome de elemento, o provedor de dados o modifica para produzir um nome de elemento válido. O provedor de dados também inclui um atributo `JSON_name` no elemento. O valor do atributo é o nome do atributo JSON original.

Para cada elemento de uma matriz JSON, o provedor de dados cria um elemento XML `JSON_`*xxx*`_array_element`, em que *xxx* é o nome da matriz. O valor do elemento de matriz é convertido em texto dentro do elemento XML. Um atributo `JSON_index` é incluído em cada elemento XML; o valor do atributo é o índice do elemento de matriz dentro da matriz.

O provedor de dados inclui os atributos a seguir em cada elemento:

- `JSON_level`: o nível do nó dentro do arquivo JSON. A raiz da árvore representada pela tag `JSON_document` é de nível `1`.
- `JSON_type`: o tipo do nó JSON (objeto, matriz, sequência ou número).

Campos específicos para atributos SOAP
Na janela **Informações do Atributo**, existem dois campos para os atributos SOAP que definem como os dados são coletados a partir da resposta SOAP.

O campo **Tipo de Atributo** pode ser qualquer valor a partir de uma lista que controla as informações sobre a resposta que é retornada. Alguns tipos de atributos requerem um valor no campo **Valor de Tipo**. O tipo de atributo padrão é XPath Query, que executa uma consulta XPath com relação ao conteúdo da resposta do servidor SOAP. O valor de tipo é a consulta XPath que é executada. A tabela a seguir descreve todos os tipos de atributos e o valor de tipo quando um for necessário:

Tabela 277. Informações sobre o Atributo SOAP

Tipo de Atributo	Descrição	Valor de tipo	Tipo de dados retornado	Diferenças com protocolos FTP e de arquivos
`Consulta XPath`	Executa uma consulta XPath no conteúdo que é retornado de uma conexão de URL. A consulta deve ser gravada para retornar dados úteis para um atributo, não uma lista de nós.	A consulta XPath para ser executada no conteúdo que é obtido de uma conexão de URL. Se uma consulta de seleção de linha foi definida, esta consulta XPath deve ser relativa à consulta de seleção de linha.	Os dados retornados podem ser uma sequência, um valor numérico ou de registro de data e hora. O navegador Agent Builder para SOAP geralmente detecta o tipo de dados correto para o atributo dos dados que está sendo procurado. Se os dados estiverem no formato DateTime XML, você pode especificar o registro de data e hora como o tipo de atributo e o agente converterá o valor para um Registro de Data e Hora Candle.	none

Tabela 277. Informações sobre o Atributo SOAP (continuação)

Tipo de Atributo	Descrição	Valor de tipo	Tipo de dados retornado	Diferenças com protocolos FTP e de arquivos
`Tempo de Resposta`	A quantidade de tempo em milissegundos que demorou para fazer download do conteúdo a partir da URL solicitada.	Nenhum	Número inteiro (número em milissegundos)	Nenhum
`Mensagem de Resposta`	A mensagem de resposta de HTTP que é retornada pelo servidor.	Nenhum	Cadeia	A mensagem de resposta somente será aplicada se a URL usar os protocolos HTTP ou HTTPS.
`Código de Resposta`	O código de resposta de HTTP que é retornado pelo servidor.	none	Integer	O código de resposta somente será aplicado se a URL usar os protocolos HTTP ou HTTPS. É sempre 0 para URLs de arquivos ou de FTP.
`Comprimento da Resposta`	O tamanho do conteúdo em bytes, que foi transferido por download a partir da URL solicitada	none	Número inteiro (tamanho em bytes)	Nenhum
`Cabeçalho da Resposta`	O cabeçalho da resposta pode ser usado para recuperar um valor de um dos campos de cabeçalho de resposta da URL. O argumento especifica qual campo é solicitado.	O campo de cabeçalho de resposta a ser coletado.	Cadeia	Geralmente, os protocolos de arquivos e FTP não possuem nenhum cabeçalho que possa ser coletado.

Tabela 277. Informações sobre o Atributo SOAP (continuação)				
Tipo de Atributo	**Descrição**	**Valor de tipo**	**Tipo de dados retornado**	**Diferenças com protocolos FTP e de arquivos**
URL da Solicitação	A conexão foi feita com essa URL. Todas as palavras-chave de resposta fornecem informações sobre a conexão com essa URL. A Consulta XPath pode ser usada para obter informações a partir do conteúdo retornado acessando esta URL.	none	Cadeia	Nenhum

Opções de XPath

Usando o XML Path Language, é possível selecionar os nós de um documento XML. Alguns dos possíveis usos de XPaths para as origens de dados SOAP incluem:

- O uso de predicados no XPath para identificar os elementos XML que correspondem às linhas de dados no grupo de atributos do IBM Tivoli Monitoring. É possível usar predicados no XPath que mapeia elementos ou atributos XML para os atributos do Tivoli Monitoring, como no exemplo a seguir:

  ```
  Stat[@name="URLs"]/CountStatistic[@name="URIRequestCount"]/@count
  ```

  Em que há diversas etapas de local no XPath, cada etapa de local pode conter um ou mais predicados. Os predicados podem ser complexos e conter valores booleanos ou operadores de fórmulas. Exemplo:

  ```
  //PerformanceMonitor/Node/Server[@name="server1"]/Stat/Stat/Stat[@name="Servlets"]/Stat
  ```

- Incluindo as funções de conjunto de nós no XPath, se uma linha contiver diversos elementos XML do mesmo tipo. E se a posição de um elemento XML na lista de nós determinar o atributo Tivoli Monitoring para o qual o elemento é mapeado. Os exemplos de funções do conjunto de nós são `position()`, `first()`, `last()` e `count()`.
- Fazer transformação de dados simples, como subsequência. Se você especificar a seguinte subsequência:

  ```
  substring(myXMLElement,1,3)
  ```

  o XPath retornará os três primeiros caracteres do elemento XML, myXMLElement.

É possível especificar elementos fora do contexto do XPath de seleção de linha usando dois pontos, `(..`, como no exemplo a seguir:

```
/../OrganizationDescription/OrganizationIdentifier
```

Configuração de SOAP

Após uma origem de dados SOAP ser incluída, a configuração será exibida na página **Configuração de Tempo de Execução** do Agent Editor.

As seções de configuração são incluídas para o servidor HTTP, para o servidor Proxy e para Java. Para obter informações sobre a configuração de servidor Proxy, consulte (“Configuração do Servidor Proxy” na

página 1303). Para obter mais informações sobre a configuração Java, consulte “Configuração do Java” na página 1304.

Servidor HTTP

A seção de configuração do Servidor HTTP contém as seguintes propriedades:

Tabela 278. Propriedades de configuração do Servidor HTTP

Nome	Valores Válidos	Obrigatório	Descrição
Nome de usuário de HTTP	Cadeia	Não	O usuário de HTTP
Senha de HTTP	Senha	Não	A senha do servidor HTTP
Nome do servidor HTTP	Sequência (O valor padrão é localhost)	Não	O host ou o endereço IP do servidor HTTP
Número da porta HTTP	Numérico (O valor padrão é 80)	Não	O host ou o endereço IP do servidor HTTP
Validação de Certificado Ativada	True, False (O valor padrão é True)	Sim	Desativar a validação do certificado é potencialmente inseguro.
Arquivo trust store de HTTP	Caminho para um arquivo	Não	O arquivo trust store de HTTP
Senha do trust store de HTTP	A senha do trust store de HTTP	Não	A senha do trust store de HTTP

Servidor Proxy

Se o sistema no qual o agente está em execução exigir um proxy para acessar o provedor de dados SOAP, você deve especificar as propriedades de configuração do servidor proxy. Para obter mais informações, consulte “Configuração do Servidor Proxy” na página 1303.

Testando Grupos de Atributo SOAP

É possível testar o grupo de atributos SOAP criado no Agent Builder

Procedimento

1. É possível iniciar o procedimento de Teste das seguintes maneiras:
   - Durante a criação do agente, clique em **Testar** na página **Informações de SOAP**.
   - Após a criação do agente, selecione um grupo de atributos no Agent Editor **Definição de Origem de Dados** e clique em **Testar**. Para obter informações adicionais sobre o Agent Editor, consulte “Usando o Agent Editor para modificar o agente” na página 1172

   Após clicar em **Testar** em uma das duas etapas anteriores, a janela **Testar Coleção de SOAP** é exibida.
2. Opcional: Antes de iniciar seu teste, é possível configurar as variáveis de ambiente, as propriedades de configuração e as informações Java.

   Para obter mais informações, consulte “Teste de Grupo de Atributos” na página 1380. Para obter mais informações sobre a configuração SOAP, consulte “Configuração de SOAP” na página 1312.
3. Altere a URL, o XPath de Seleção de Linha e o tipo de solicitação.

4. Clique em **Iniciar Agente**.

   Uma janela indica que o Agente está iniciando.
5. Para simular uma solicitação a partir do Tivoli Enterprise Portal ou SOAP para dados do agente, clique em **Coletar Dados**. Essa ação preenche a tabela de Resultados e você pode visualizar como os dados são analisados e mostrados nas colunas no Tivoli Enterprise Portal.

   Na área Resultados, você pode alterar as definições de atributos e recarregar os dados para ver como suas mudanças afetam o grupo de atributos. Você pode clicar com o botão direito em uma área de resultados da coluna para exibir opções para editar o atributo. As opções de edição do atributo são:

   - **Editar Atributo**
   - **Ocultar Atributo**
   - **Inserir Atributo Antes**
   - **Inserir Atributo Após**
   - **Remover**
   - **Remover Atributos Subsequentes**
   - **Remover Tudo**
6. Opcional: Clique em **Verificar Resultados**, se os dados retornados não estiverem conforme o esperado.

   A janela **Status de Coleção de Dados** é aberta e mostra informações adicionais sobre os dados. Os dados coletados e mostrados pela janela **Status de Coleção de Dados** são descritos em "Nó de Status do Objeto de Desempenho" na página 1424
7. Pare o agente, clicando em **Parar Agente**.
8. Clique em **OK** ou **Cancelar** para sair da janela **Testar Coleção de SOAP**. Clicar em **OK** salva quaisquer mudanças que tiver feito.

Conceitos relacionados

"Testando seu agente no Agent Builder" na página 1380
Depois de usar o Agent Builder para criar um agente, será possível testar o agente no Agent Builder.

Monitorando dados usando um soquete

É possível definir uma origem de dados para coletar dados a partir de um aplicativo externo usando um soquete TCP. O aplicativo deve iniciar a conexão TCP com o agente e enviar dados em um formato XML estruturado. Dependendo do aplicativo, a origem de dados pode produzir um conjunto de dados com uma única linha, com várias linhas, ou com dados do evento.

Sobre Esta Tarefa

Use a origem de dados do soquete para fornecer dados para o agente a partir de um aplicativo externo, sendo executado no mesmo sistema que o agente. O aplicativo externo pode enviar dados para o agente no momento que desejar. Por exemplo, você pode desenvolver uma interface da linha de comandos que permita a um usuário postar dados para um grupo de atributos quando ele é executado. Uma outra opção é modificar um aplicativo monitorado para enviar atualizações para o agente. O agente não inicia ou para o aplicativo que está enviando dados para o soquete; essa ação é controlado pelo usuário.

Existem algumas limitações com a origem de dados do soquete:

- Por padrão, somente as conexões ao host local (127.0.0.1) são possíveis. Para obter informações adicionais sobre como configurar seu agente para aceitar as conexões de um host remoto, consulte "Conexão da porta do soquete remoto" na página 1322.
- Não há nenhum mecanismo na API do soquete para o cliente determinar quais subnós estão disponíveis. O cliente pode enviar dados para um determinado subnó, mas ele já precisa saber o nome do subnó.

Use o procedimento a seguir para criar um grupo de atributos para coletar dados usando um soquete Transmission Control Protocol socket (TCP).

Procedimento

1. Na página **Origem de Dados Inicial do Agente** ou na página **Local da Origem de Dados**, clique em **Programas Customizados** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **Soquete**.
3. Clique em **Avançar**.
4. Na página **Informações do Soquete**, insira um nome de grupo de Atributos.
5. Insira um texto de ajuda para o grupo de atributos.
6. Selecione se o grupo de atributos **Produz uma única linha de dados**, **Pode produzir mais de uma linha de dados** ou **Produz eventos**. Para obter mais informações, consulte “Enviando Dados” na página 1317.
7. Na seção Informações do Soquete, selecione uma **Página de Códigos**. Para obter mais informações, consulte “Conjuntos de Caracteres” na página 1320.
8. Opcional: Clique em **Avançado** para modificar as propriedades avançadas para o grupo de atributos. A opção **Avançado** é ativada quando voê seleciona o grupo de atributo **Pode produzir mais de uma linha de dados** ou **Produz eventos**.
9. Clique em **Avançar**.
10. Na página **Informações do Atributo**, especifique o primeiro atributo para o grupo de atributos. Para obter mais informações sobre a criação de atributos, consulte “Criando Atributos” na página 1192.
11. Clique em **Avançar**.
12. Opcional: Na página **Informações Globais de Origem de Dados de Soquete**, na seção **Códigos de Erro**, é possível definir os códigos de erros que o cliente de soquete pode enviar quando não pode coletar dados. Para obter mais informações, consulte (“Enviando Erros em Vez de Dados” na página 1318). Para definir um código de erro, use as etapas a seguir:
    a) Na seção **Códigos de Erro**, clique em **Incluir**. Um código de erro possui um limite de 256 caracteres. Somente letras, dígitos e sublinhados ASCII são permitidos. Não são permitidos espaços.
    b) Na janela **Definição de Código de Erro de Soquete**, insira um valor de exibição que é mostrado no grupo de atributos **Status do Objeto de Desempenho**.
    c) Insira um valor de interno. O valor interno deve ser um número inteiro de 1.000 a 2.147.483.647.
    d) Você deve definir um texto de mensagem para cada erro. É possível usar o texto de mensagem que foi inserido anteriormente selecionando-o da lista. Clique em **OK** para retornar à página **Informações Globais de Origem de Dados de Soquete**. O texto da mensagem é usado no arquivo de log do agente.

       Se nenhum texto de mensagem adequado estiver disponível, clique em **Procurar** para configurar o texto da mensagem. A janela Mensagens (lista) é aberta. A janela de mensagens lista mensagens que são definidas no agente. Até definir as mensagens, a lista permanece em branco. É possível usar **Editar** para alterar uma mensagem definida e **Remover** para excluir uma ou mais mensagens que você definiu.
    e) Na janela Mensagens (lista), clique em **Incluir** para ver uma janela **Definição de Mensagem**. No tipo de janela **Definição de Mensagem**, o texto que descreve o significado da nova mensagem e selecione o tipo de mensagem.

       Nota: O identificador de mensagens é automaticamente gerado para você.
    f) Clique em **OK**.
    g) A janela Mensagens (lista) se abre, com uma nova mensagem. Para verificar a mensagem e retornar à página **Informações Globais de Origem de Dados de Soquete**, clique em **OK**.
13. Opcional: Na seção **Arquivos Suplementares** da página **Informações Globais da Origem de Dados do Soquete**, é possível incluir os arquivos que são compactados com o agente. Estes arquivos são copiados para o sistema de agente quando o agente é instalado.

    A coluna **Tipo de Arquivo** descreve como é esperado que cada arquivo seja usado. Três possíveis usos são descritos na tabela a seguir:

Tabela 279. Tipos de arquivos para arquivos complementares	
Tipo de Arquivo	**Descrição**
Executável	Selecione esta opção se desejar incluir um arquivo executável com o agente. O agente não usa esses arquivos.
Biblioteca	Selecione esta opção se você incluir uma biblioteca com o agente. O agente não usa esses arquivos.
Recurso Java	Selecione esta opção para incluir recursos Java com o agente. O agente não usa esses arquivos.

Para obter informações sobre onde os Arquivos Suplementares estão instalados com o agente, consulte ("Novos Arquivos em Seu Sistema" na página 1397).

Clique em **Editar** para editar o arquivo de importado. Para obter mais informações, consulte ("Editando uma definição de arquivo de comando" na página 1280).

14. Opcional: Você pode testar este grupo de atributos, clicando em **Testar**. Para obter informações adicionais sobre teste, consulte "Testando Grupos de Atributos do Soquete" na página 1324
15. Opcional: Se a origem de dados for amostrada, você poderá criar um filtro para limitar os dados retornados por esse grupo de atributos, clicando em **Avançado**. A origem de dados é amostrada quando você não seleciona "Produz Eventos" na página **Informações do Soquete**. Para obter informações adicionais sobre filtragem de dados de um grupo de atributos, consulte "Filtrando Grupos de Atributos" na página 1201
16. Execute uma das seguintes etapas:

    a) Se estiver usando o assistente de **Agente**, clique em **Avançar**.

    b) Clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor.

    Selecione os sistemas operacionais nos quais o agente atende dados dos clientes do soquete na seção **Sistemas Operacionais** da página **Configurações do Provedor do Soquete**. Para abrir esta página, clique em **Configurações do Provedor do Soquete** na visualização da estrutura de tópicos ou clique em **Configurações Globais** no Agent Editor em qualquer página do grupo de atributos do soquete.

    Nota: Códigos de erros e arquivos complementares podem ser atualizados nas seções **Códigos de Erros** e **Arquivos Complementares** da página **Configurações do Provedor do Soquete**.

Enviando informações do soquete para o agente

Quando o seu agente contém um ou mais grupos de atributos do soquete, o agente abre um soquete e atende dados dos clientes.

O aplicativo que envia dados do soquete para o agente conecta-se a uma porta definida no agente. A porta é o valor configurado por uma propriedade de configuração do agente ou uma porta temporária alocada automaticamente por TCP/IP. Para obter informações adicionais sobre as portas de soquete e configuração, consulte "Configuração do Soquete" na página 1321.

Os dados recebidos devem seguir um formato XML estruturado. Os fluxos de informações XML a seguir são possíveis usando a origem de dados de soquete:

- Enviar uma ou mais linhas de dados para o agente para um grupo de atributos amostrados
- Enviar uma linha de dados para o agente para um grupo de atributos que Produz eventos
- Enviar um código de erro para o agente em vez de dados.
- Enviar um registro de prefixo de tarefa para o agente
- Receber uma solicitação de tarefa do agente
- Enviar uma resposta de tarefa para o agente

Enviando Dados

Um grupo de atributos é definido para receber dados de amostra ou dados de evento. Quando você cria o grupo de atributos, você especifica uma opção que indica se os dados que serão recebidos:

- Produz uma única linha de dados
- Produzem mais de uma linha de dados
- Produzem eventos

Se você selecionar **Produz uma única linha de dados** ou **Pode produzir mais de uma linha de dados**, que é um grupo de atributos exemplificado. Se você selecionar **Produz eventos**, seu grupo de atributos enviará um evento para o ambiente de monitoramento cada vez que uma linha for recebida.

Ao visualizar dados de amostra no Tivoli Enterprise Portal ou no console do IBM Cloud Application Performance Management, você vê o conjunto mais recente de linhas coletadas. Os dados exibidos para um grupo de atributos de evento são o conteúdo de um cache local mantido pelo agente. Para dados de eventos, o agente inclui a nova entrada no cache, até que o tamanho seja atingido quando a entrada mais antiga é excluída. Para dados amostrados, o agente substitui o conteúdo do cache sempre que você envia dados.

Se selecionar **Produz Eventos** ou **Produz uma Única Linha de Dados**, você deve enviar somente uma linha de dados para o agente para esse o grupo de atributo em cada mensagem. É possível enviar quantos eventos você desejar, enviar cada evento em uma mensagem separada.

Normalmente, os dados de amostra são coletados pelo agente por encomenda, mas o cliente de soquete fornece amostras atualizadas em seu próprio planejamento. Você pode atualizar um grupo de atributos de amostra (linha única ou diversas linhas) sempre que precisar. Quando os dados forem solicitados pelo Tivoli Monitoring ou IBM Cloud Application Performance Management, o agente fornecerá os dados mais recentes.

Se linhas de dados estiverem ausentes para o grupo de atributos do soquete no Tivoli Enterprise Portal ou no console do IBM Cloud Application Performance Management, verifique os erros no arquivo de log. Além disso, se os dados no grupo de atributos não for o esperado, verifique os erros no arquivo de log. A origem de dados do soquete tenta processar tudo o que puder da entrada. Por exemplo, se o cliente enviar três linhas bem formatadas e uma que não seja válida (por exemplo, XML mal formado), você verá:

- Três linhas de dados no grupo de atributos
- Um erro é registrado para a linha malformada no arquivo de log do agente
- Como as linhas válidas foram retornadas, o Status do Objeto de Desempenho mostra um status de `NO_ERROR`

Para os dados de eventos e os dados amostrados, os dados são enviados para o agente como um único fluxo de dados XML a partir do cliente do soquete. Os dados enviados a partir de um cliente do soquete sempre devem ser terminados com um caractere de nova linha: `'\n'`. O agente lês dados até encontrar o caractere de nova linha e, em seguida, é realizada uma tentativa de processar o que foi recebido. Quaisquer dados recebidos que não podem ser processados são descartados. A seguir é um exemplo de como você enviaria duas linhas de dados para o agente para um grupo de atributos chamado `abc`:

```
<socketData><attrGroup name="abc"><in><a v="1"/><a v="no"/><a v="5"/></in><in> \
<a v="3"/><a v="yes"/><a v="5"/></in></attrGroup></socketData>\n
```

Esta amostra envia duas linhas de dados para o agente em que cada linha contém três atributos. A ordem dos atributos é importante e deve seguir a ordem definida em seu grupo de atributos. A única exceção para isso é que os atributos derivados devem ser ignorados, independentemente de onde eles estão no grupo de atributos.

Se o grupo de atributos for definido em um subnó, então o ID da instância de subnó deve ser identificado quando os dados foram enviados para o agente O ID da instância do subnó é identificado usando o atributo de subnó no elemento `socketData`. A convenção deve ser adotada para configuração de IDs de instâncias de subnós para uso pelo cliente do soquete, pois o cliente não pode consultar IDs de instâncias ou propriedades de configuração. Os dados enviados para um subnó que não está configurado são ignorados.

Veja a seguir uma amostra:

```
<socketData subnode="app1"><attrGroup name="abc"><in><a v="1"/><a v="no"/><a v="5"/>
</in><in> \<a v="3"/><a v="yes"/><a v="5"/></in></attrGroup></socketData>\n
```

Nesta amostra, os dados são enviados para o subnó com um ID de instância igual a "app1". "app1" não é o nome do sistema gerenciado, mas o identificador da instância especificado quando a instância do subnó é configurada.

Os seguintes elementos XML formam os dados do soquete:

socketData
O elemento raiz. Ele possui um atributo opcional chamado subnó que especifica o ID da instância do subnó.

attrGroup
Este elemento identifica o grupo de atributos para o qual são destinados os dados do soquete. O atributo name é necessário e é usado para especificar o nome do grupo de atributos.

in
Este elemento é necessário para identificar uma nova linha de dados. Todos os valores de atributos para uma linha de dados devem ser filhos do mesmo elemento in.

a
O elemento a identifica um valor de atributo. O atributo v é necessário e é usado para especificar o valor do atributo.

Enviando Erros em Vez de Dados

Às vezes, o aplicativo que posta os dados do soquete pode não conseguir coletar os dados necessários para um grupo de atributos. Neste caso, em vez de enviar dados para o agente, um código de erro pode ser retornado. O código de erro fornece uma maneira de informar o ambiente de monitoramento sobre seu problema. Um erro de exemplo é o seguinte:

```
<socketData><attrGroup name="abc"/><error rc="1000"/></attrGroup></socketData>\n
```

O código de erro pode ser definido no agente em uma lista que é comum para todos os grupos de atributos de soquete. Quando o agente recebe um código de erro, a mensagem de erro definida é registrada no arquivo de log do agente. Além disso, o grupo de atributos denominado Status do Objeto de Desempenho possui um atributo de Código de Erro é atualizado com o Tipo de Código de Erro. O Tipo de Código de Erro é definido para o código de erro que você envia.

Para o exemplo anterior, você deve definir o Valor do Código de Erro de 1000 no agente. Consulte a seguinte definição de código de erro de amostra:

Tabela 280. Código de erro de amostra

Valor de Código de Erro	Tipo de Código de Erro	Mensagem
1000	APP_NOT_RUNNING	O aplicativo não está em execução

Quando o código de erro é enviado, uma mensagem semelhante à seguinte é registrada no arquivo de log do agente:

```
(4D7FA153.0000-5:customproviderserver.cpp,1799,"processRC") Received error code 1000
 from client. \Message: K1C0001E The application is not running
```

Se você selecionar a consulta do Status do Objeto de Desempenho a partir do Tivoli Enterprise Portal, a coluna **Código de Erro** para a o grupo de atributos **abc** da linha mostrará o valor APP_NOT_RUNNING nessa tabela.

Enviar um erro para um grupo de atributos amostrados elimina quaisquer dados que foram recebidos anteriormente para esse grupo de atributos. O envio de dados para o grupo de atributos faz com que o

código de erro não seja mais exibido no grupo de atributos Status do Objeto de Desempenho. Também é possível enviar um código de erro 0 para limpar o código de erro dessa tabela.

O envio de um erro para um grupo de atributos que produz eventos não limpa o cache de eventos que foram anteriormente enviados.

Manipulando Solicitações `take action`

O cliente do soquete pode ser registrado para receber solicitações `take action` a partir do agente quando o comando de ação corresponder a um certo prefixo. Qualquer ação que não for correspondida será manipulada pelo agente. O prefixo não deve conflitar com ações que se espera que o agente manipule, portanto, use o código de produto do agente como o prefixo. `Take actions` fornecido com o Agent Builder é nomeado após a origem de dados que `take action` usa. Por exemplo, o `JMX_INVOKE take action` opera na origem de dados JMX. Outro exemplo é o `SSHEXEC take action` que usa o provedor de dados de script SSH. Como essas ações não usam o código do produto, o código do produto é um prefixo seguro a ser usado como o prefixo `take action`.

O cliente de soquete deve estar em execução há muito tempo e deixar o soquete aberto. Ele deve enviar uma solicitação de registro para o prefixo e receber solicitações do soquete. O agente assegura que um tempo limite não ocorra no soquete de um cliente de longa execução, mesmo se nenhum dado estiver fluindo. A seguir é uma solicitação de registro de amostra:

```
<taskPrefix value="K42"/>\n
```

Neste exemplo, qualquer comando `executar ação` recebido pelo agente que inicia com `"K42"` é encaminhado para o cliente de soquete que iniciou o registro. A seguir é apresentada uma amostra de solicitação `take action` que o cliente de soquete pode receber:

```
<taskRequest id="1"><task command="K42 refresh" user="sysadmin"/></taskRequest>\n
```

O `id` é um identificador exclusivo que o agente usa para controlar solicitações que são enviadas aos clientes. Quando o cliente do soquete responder à tarefa, ele deverá fornecer este identificador no atributo `id` do elemento `taskResponse`.

O cliente do soquete deve processar a ação e enviar uma resposta. Uma resposta de amostra é:

```
 <taskResponse id="1" rc="1"/>\n
```

Se a ação for concluída com êxito, um valor de atributo `rc` igual a `0` será retornado. O valor de `rc` deve ser um número inteiro, em que qualquer valor diferente de 0 é considerado uma falha. O valor do código de retorno da tarefa é registrado no arquivo de log do agente e é mostrado na consulta do Status da Execução de Ação que é incluído com o agente. O diálogo que é exibido no Tivoli Enterprise Portal após a execução de uma ação não mostra o código de retorno. Esse diálogo indica se o comando `take action` retornou sucesso ou falha. O log do agente ou a consulta do Status da Execução da Ação deve ser visualizado para determinar o código de retorno real se uma falha ocorreu.

É responsabilidade do desenvolvedor do agente documentar, criar e importar qualquer ação que seja suportada pelos clientes de soquete usados com um agente. Se os usuários enviarem ações não suportadas para o cliente do soquete, o cliente deverá ser desenvolvido para manipular esses cenários de uma forma apropriada. Se os usuários definirem ações adicionais que são iniciadas com o prefixo registrado, elas serão passadas para o cliente. O cliente deve ser desenvolvido para manipular esses cenários de uma maneira apropriada.

Existe um tempo limite que controla quanto tempo o agente aguarda por uma resposta do cliente de soquete. A configuração é uma variável de ambiente que é definida no agente chamado `CDP_DP_ACTION_TIMEOUT` e o valor padrão é 20 segundos.

Nota: As mensagens de códigos de erros definidas para os grupos de atributos da origem de dados do soquete não são usadas para `executar ações`. É possível retornar os mesmos valores de código de retorno. No entanto, o agente não registra a mensagem definida ou afeta o campo `Código de Erro` no grupo de atributos Status do Objeto de Desempenho.

Codificação dos dados de soquete
O cliente de soquete codifica os dados que são enviados para o agente.

É importante estar ciente de como seu cliente de soquete está codificando os dados que estão sendo enviados para o agente.

Caracteres Especiais

Os dados enviados para o agente não devem conter nenhum caractere de nova linha, exceto ao final de cada evento ou amostra de dados. Os caracteres de nova linha que ocorrem dentro dos valores de atributos devem ser substituídos por um caractere diferente ou codificados conforme mostrado em (Tabela 281 na página 1320). Você também deve ter cuidado para não quebrar a sintaxe XML com seus valores de atributos. A tabela a seguir mostra os caracteres que ocorrem nos valores de atributo que você codifica:

Tabela 281. Caracteres para codificar nos valores de atributos

Caractere	**Cabeçalho**
&	&
<	<
>	>
“	"
'	'
\n

Nota: O agente usa o caractere de nova linha para separar respostas recebidas de um cliente. Os caracteres de nova linha inesperados evitam que os dados sejam analisados corretamente.

O agente não contém um analisador XML completo, portanto você não deve usar codificação especial para os caracteres que não estão em (Tabela 281 na página 1320). Por exemplo, não codifique ¢ ou &cent no lugar de um sinal de centavo ¢.

Conjuntos de Caracteres

Além dos caracteres especiais de codificação, o agente deve saber qual página de códigos foi usado para codificar seus dados. Defina cada grupo de atributos no soquete para indicar se está enviando os dados ao agente como dados **UTF-8** ou como **Página de código local**. Esteja ciente de como o seu cliente está enviando dados. Se usar um cliente escrito em Java, especifique **UTF-8** como a codificação no gravador que você usa para enviar os dados para o agente. Especifique **UTF-8** como **Página de Códigos** para seu grupo de atributos. **Página de código local** signiica a página de códigos local do agente. Se os dados forem enviados por um soquete remoto, eles devem estar em conformidade com a página de códigos local do agente ou usar UTF-8.

Dados Numéricos

Esteja ciente de como você está formatando seus valores de atributos numéricos. Os valores numéricos que enviar ao agente não devem conter caracteres especiais. Um exemplo é o caractere do separador de milhares. Outros exemplos são símbolos monetários ou caracteres que descrevem as unidades do valor. Se o agente encontrar um problema quando estiver analisando dados numéricos, ele registrará um erro que indica o problema. O Código de Erro do Status do Objeto de Desempenho não é configurado quando um atributo falhar na análise. A seguir é uma mensagem de erro de exemplo do log do agente:

```
(4D3F1FD6.0021-9:utilities.cpp,205,"parseNumericString") Caracteres inválidos :00:04 \
localizados ao obter valor numérico de 00:00:04, retornando 0.000000
```

Nota: Para obter mais informações sobre como um atributo de registro de data e hora deve ser formatado, consulte (“Registro de Data e Hora” na página 1198).

Erros de Soquete
Erros são gravados no arquivo de log do agente para problemas que ocorrem com dados recebidos de um cliente de soquete.

Outros erros que são registrados são ações de execução que retornam um valor diferente de 0. Os valores de erros enviados pelo cliente do soquete são registrados juntamente com a mensagem associada ao código de erro.

O Status do Objeto de Desempenho para o grupo de atributos é configurado quando o cliente do soquete envia um código de retorno de erro para o agente. Alguns outros valores podem ser vistos além daqueles definidos pelo agente. A tabela a seguir descreve outros valores "Error Code" que você provavelmente encontrará com os grupos de atributos de soquete:

Tabela 282. Valores de Status do Objeto de Desempenho

Código de Erro	**Descrição**
NO_ERROR	Não ocorreu nenhum erro. Indica que não existem problemas com o grupo de atributos. Os problemas com uma linha de dados exemplificados não fazem com que o estado mude de NO_ERROR. Você deve validar o número de linhas mostrado e os valores de atributo mesmo quando encontrar NO_ERROR como o código de erro.
NO_INSTANCES_RETURNED	Um cliente do soquete não enviou nenhuma linha de dados para um grupo de atributos amostrados. Não é um erro. Indica que não existem instâncias dos recursos que estejam sendo monitorados por este grupo de atributos.
XML_PARSE_ERROR	O agente falhou em analisar os dados recebidos do cliente. Consulte o log do agente para obter mais detalhes.
OBJECT_CURRENTLY_UNAVAILABLE	O cliente enviou ao agente um código de erro que não foi definido na lista global de códigos de erros.
GENERAL_ERROR	Ocorreu um problema ao coletar dados do cliente, geralmente porque o cliente não respondeu à solicitação dentro do intervalo de tempo limite. Consulte o log de rastreio do agente para obter mais detalhes. O cliente também pode especificar GENERAL_ERROR como um código de erro, mas é melhor se um código de erro mais detalhado for definido.

Configuração do Soquete
Após incluir uma origem de dados do soquete em seu agente, é possível configurar o agente para aceitar dados de uma porta de soquete especificada.

Sobre Esta Tarefa

Após incluir uma origem de dados de soquete, a configuração será exibida na página **Configuração de Tempo de Execução** do Agent Editor. A seção Configuração do Soquete contém a seguinte propriedade:

Tabela 283. Propriedade de configuração do soquete			
Nome	**Valores Válidos**	**Obrigatório**	**Descrição**
Número da Porta	0 ou qualquer número inteiro positivo O valor padrão é 0	Sim	A porta que o agente usa para atender dados dos clientes do soquete. Um valor 0 indica que uma porta temporária deve ser usada.

O agente grava o valor da porta que está sendo usado para um arquivo. Os clientes de soquete que são executados no computador agente podem ler este arquivo posteriormente para determinar a qual porta se conectar. O arquivo em que a porta é gravada é chamado de *kxx_instanceName*_cps.properties, em que: *kxx* é o código do produto de três caracteres do agente e *instanceName* é o nome da instância do agente para um agente de diversas instâncias. Se o agente não for um agente de diversas instâncias, esta parte do nome não será incluída e, portanto, o nome do arquivo será *kxx*_cp.properties.

No Windows, o arquivo é gravado no diretório %CANDLE_HOME%\TMAITM6 para instalações de 32 bits ou no %CANDLE_HOME%\TMAITM6_x64 para instalações de 64 bits. No UNIX, o arquivo é gravado para /tmp.

Procedimento

1. Opcional: Configure a variável de ambiente CDP_DP_HOSTNAME para o nome do host ou endereço IP de sua interface de rede, se seu sistema possui várias interfaces:
   a) Acesse a visualização **Informações do Agente** do Agent Editor e selecione **Variáveis de Ambiente**.
   b) Clique em **Incluir** e selecione CDP_DP_HOSTNAME a partir da lista de variáveis de ambiente usando o campo Nome.
   c) Configure o nome do host ou endereço IP no campo Valor.
2. Inicie o seu agente.

   Quando o agente for iniciado, ele se ligará à interface que é definida pela variável de ambiente CDP_DP_HOSTNAME. Se CDP_DP_HOSTNAME não estiver configurado, o agente se ligará ao nome do host padrão.

   Se desejar que o agente ligue-se a uma porta definida em vez de uma porta efêmera, é possível configurar a propriedade de configuração **Número de Porta** (CP_PORT).

   Para configurar a propriedade de configuração de número da porta, use as etapas a seguir:

   a) Acesse o a visualização **Configuração de Tempo de Execução** do Agent Editor.
   b) Na área de janela **Informações de Configuração de Tempo de Execução**, selecione **Configuração para Soquete** > **Soquete** > **Número da Porta**
   c) Insira um valor de número da porta em **Valor Padrão**.

      Se você não inserir um valor, um valor 0 será usado. Um valor 0 indica que uma porta temporária é usada.

Conexão da porta do soquete remoto

É possível configurar seu agente para que aceite dados de uma porta de soquete remota. O agente deve ser executado em um sistema que possua uma conexão de interface de rede com um sistema remoto.

Procedimento

1. Configure o valor da variável de ambiente CDP_DP_ALLOW_REMOTE para YES, concluindo as etapas a seguir.
   a) Acesse a página **Informações do Agente** do Agent Editor e selecione **Variáveis de Ambiente**.

b) Clique em **Incluir** e selecione CDP_DP_ALLOW_REMOTE na lista de variáveis de ambiente usando o campo **Nome**.

c) Configure o campo **Valor** como SIM.

2. Siga o procedimento detalhado em "Configuração do Soquete" na página 1321.

Restrição:

- Os dados enviados entre o aplicativo de soquete e o agente:
  - Os dados devem estar em conformidade com a sintaxe XML definida para um provedor de dados do soquete. Para obter mais informações, consulte " Codificação dos dados de soquete" na página 1320.
  - Deve ser codificado em UTF-8.
  - É enviado em texto limpo (não criptografado). Se houver informações sensíveis nos dados, a comunicação deverá ser assegurada através de um túnel SSH ou outro mecanismo fora do agente.
- O agente processará os dados recebidos de qualquer host remoto de modo que o ambiente deve ser protegido com o firewall apropriado ou filtros de tráfego de rede.

Resultados

É possível executar o código que implementa um provedor de dados do soquete em qualquer sistema que pode se conectar ao sistema em que o agente está executando.

Script de Amostra para Soquete

Este script de amostra demonstra como um cliente de soquete pode ser gravado.

Amostra Perl

O script Perl de amostra a seguir se conecta a um soquete e envia dados. Esta amostra foi escrita para um agente em execução no UNIX, com código do produto k00 e um grupo de atributos chamado SocketData.

```
#!/usr/bin/perl -w
# SocketTest.pl
# A simple Agent Builder Socket client using IO:Socket
#------------------------

use strict;
use IO::Socket;

# Inicializar conexão do soquete com o agente
#-----------------------
my $host = '127.0.0.1';
my $port = 0;
# Essa amostra é para um agente com o código do produto k00.  O código do produto é
# usado na linha a seguir para localizar o arquivo que contém o número da porta a ser usado.
open PORTFILE, "/tmp/k00_cps.properties" || die "Port file not found $!\n";
while (<PORTFILE>) {
    if (/^CP_PORT=([0-9]+)/) {
        $port = $1;
    }
}

if ($port == 0) {
    die "Could not find port to use to connect to agent.\n";
}

my $sock = new IO::Socket::INET( PeerAddr => $host, PeerPort => $port,
Proto => 'tcp'); $sock or die "no socket :$!";

# The following call sends 2 rows of data to the agent.  Each row contains 1
# atributo de Sequência e 3 atributos numéricos.
syswrite $sock, "<socketData><attrGroup name=\"SocketData\"><in><a v=\"A message
from perl\"/>  \<a v=\"1\"/><a v=\"2\"/><a v=\"123\"/></in><in><a v=\"More from
perl\"/><a v=\"456\"/>  \<a v=\"123\"/><a v=\"789\"/></in></attrGroup>
</socketData>\n";

close $sock;
```

Testando Grupos de Atributos do Soquete

É possível testar o grupo de atributos do soquete criado no Agent Builder.

Antes de Iniciar

Para testar o grupo de atributos, é necessário um cliente de soquete para enviar dados. Um cliente de soquete de exemplo escrito com script perl pode ser visualizado em "Script de Amostra para Soquete" na página 1323

Restrição: Diferentemente da maioria dos outros grupos de atributos, não é possível testar o grupo de atributos do soquete enquanto ele está sendo criado. É possível testar o grupo de atributos ao concluir sua criação.

Procedimento

1. Selecione um grupo de atributos na página **Definição de Origem de Dados** do Agent Editor após a criação do agente e clique em **Testar**. Para obter informações adicionais sobre o Agent Editor, consulte "Usando o Agent Editor para modificar o agente" na página 1172.

   Após clicar em **Testar** em uma das duas etapas anteriores, a janela **Testar Cliente de Soquete** é exibida.
2. Opcional: Configure as variáveis de ambiente e as propriedades de configuração antes de iniciar o teste.

   Para obter mais informações, consulte "Teste de Grupo de Atributos" na página 1380.
3. Clique em **Iniciar Agente**. Uma janela indica que o Agente está iniciando.
4. Quando o agente é iniciado, ele recebe dados de soquete de acordo com sua configuração.
5. Para testar a coleta de dados do seu agente, gere agora dados do soquete que correspondam à configuração dos agentes.

   É possível gerar os dados de soquete usando um cliente de soquete.

   Quando o agente recebe dados de soquete que correspondem à sua configuração, ele inclui os dados em seu cache interno.
6. Para simular uma solicitação do Tivoli Enterprise Portal para dados do agente, clique em **Coletar Dados**.

   A janela **Testar Cliente de Soquete** coleta e exibe quaisquer dados no cache do agente desde que foi iniciada pela última vez.
7. Clique em **Verificar Resultados** se algo não parecer estar funcionando conforme esperado.

   A janela **Status de Coleção de Dados** é aberta e mostra informações adicionais sobre os dados. Os dados coletados e exibidos pela janela Status da Coleção de Dados são descritos em "Nó de Status do Objeto de Desempenho" na página 1424
8. Pare o agente, clicando em **Parar Agente**.
9. Clique em **OK** ou **Cancelar** para sair da janela **Testar Cliente de Soquete**. Clicar em **OK** salva quaisquer mudanças que tiver feito.

Conceitos relacionados

"Testando seu agente no Agent Builder" na página 1380
Depois de usar o Agent Builder para criar um agente, será possível testar o agente no Agent Builder.

Usar a API Java para monitorar dados

É possível definir uma origem de dados para usar a API Java para interagir com um aplicativo de longa execução na plataforma Java. O agente inicia o aplicativo na inicialização e interage periodicamente com ele. Ao construir o agente, o Agent Builder cria o código-fonte para o aplicativo. Deve-se customizar o código para reunir os dados corretos. Dependendo do código, o código-fonte pode produzir vários conjuntos de dados que podem contém uma única linha, várias linhas ou dados de evento.

Sobre Esta Tarefa

Use a origem de dados da API Java e a linguagem de programação Java para coletar os dados que não podem ser coletados usando outras origens de dados do Agent Builder. O agente inicia o aplicativo Java e envia uma solicitação de encerramento no momento de encerrar. O aplicativo Java deve sair apenas quando for solicitado que isso seja feito.

Um agente contendo os grupos de atributos da API Java faz interface com o processo de aplicativo Java. O aplicativo Java usa a API do Cliente de Provedor Java para fazer interface com o agente. Para obter informações sobre a API, consulte o Javadoc no Tivoli Monitoring Knowledge Center. Usando a API Java, você pode:

- Conecte-se ao processo do agente e registre para grupos de atributos suportados pelo aplicativo Java
- Receber e responder uma solicitação de dados amostrados
- Enviar dados no modo assíncrono para um grupo de atributos que produz eventos
- Enviar um erro para um grupo de atributos em que a coleção de dados é falha
- Suportar grupos de atributos em subnós com instâncias de subnós configurados
- Receber e responder uma solicitação "Executar Ação"

Use o procedimento a seguir para criar um grupos de atributos que coleta dados em um aplicativo Java e o envia usando a API Java. O procedimento mostra como criar um aplicativo Java de amostra a ser usado como um ponto de início para o seu aplicativo Java.

Procedimento

1. Na página **Origem de Dados Inicial do Agente** ou na página **Local da Origem de Dados**, clique em **Programas Customizados** na área **Categorias de Dados de Monitoramento**.
2. Na área **Origens de Dados**, clique em **API Java**.
3. Clique em **Avançar**.
4. Na página **Informações da API Java**, insira um nome de grupo de atributos.
5. Insira um texto de ajuda para o grupo de atributos.
6. Selecione se o grupo de atributos **Produz uma única linha de dados**, **Pode produzir mais de uma linha de dados** ou **Produz eventos**. Essa escolha afeta o aplicativo Java de amostra criado ao final do assistente. Para obter mais informações, consulte “Enviando Dados” na página 1317.
7. Opcional: Clique em **Avançado** para modificar as propriedades avançadas para o grupo de atributos. **Avançado** está disponível ao selecionar que o grupo de atributos **Pode produzir mais de uma linha de dados** ou **Produz eventos**.
8. Clique em **Avançar**.
9. Na página **Informações do Atributo**, especifique o primeiro atributo para o grupo de atributos. Para obter informações adicionais sobre a criação dos atributos, consulte (“Criando Atributos” na página 1192).
10. Selecione **Incluir Atributos Adicionais** e clique em **Avançar** para incluir outros atributos no agente. Referências aos atributos são incorporadas no aplicativo Java de amostra que é criado no final do assistente.
11. Clique em **Avançar**.
12. Na página **Informações Globais da Origem de Dados da API Java**, insira um nome de Classe e um nome de arquivo JAR.

    O nome de classe é um nome de classe completo cujo método main é chamado quando o Java é iniciado. O aplicativo Java de amostra é criado com o método Java principal nessa classe.

    O arquivo JAR é o archive que contém as classes Java que constituem o aplicativo Java. O arquivo JAR é empacotado e instalado com o agente.
13. Opcional: Na página **Informações Globais da Origem de Dados da API Java**, seção **Códigos de Erro**, defina os códigos de erro que o aplicativo Java pode enviar. Esses códigos de erro são enviados pelo aplicativo Java quando não puder coletar os dados.

Restrição: Um código de erro possui um limite de 256 caracteres. Apenas letras, dígitos e sublinhados ASCII são permitidos. Não são permitidos espaços.

a) Clique em **Incluir** na seção Códigos de Erros.

b) Na janela **Definição de Código de Erro da API Java**, insira um valor de exibição.

c) Insira um valor de interno. O valor interno deve ser um número inteiro de 1.000 a 2.147.483.647.

d) Defina um texto de mensagem para cada erro. É possível usar o texto de mensagem que foi inserido anteriormente selecionando-o da lista. Clique em **OK** para retornar à página **Informações Globais de Fonte de Dados Java API**.

A mensagem é registrada no arquivo de log do agente.

e) Se nenhum texto de mensagem adequado estiver disponível, clique em **Procurar** para configurar o texto da mensagem.

A janela Mensagens (lista) é exibida. A janela de mensagens lista mensagens que são definidas no agente. Até definir as mensagens, a lista permanece em branco. É possível usar **Editar** para alterar uma mensagem definida e **Remover** para excluir uma ou mais mensagens que você definiu.

f) Na janela Mensagens (lista), clique em **Incluir** para ver uma janela **Definição de Mensagem**. Na janela **Definição de Mensagem**, você pode digitar o texto que descreve o significado da nova mensagem e selecionar o tipo de mensagem.

Nota: O identificador de mensagens é automaticamente gerado para você.

g) Clique em **OK**.

h) A janela Mensagens (lista) é exibida com a nova mensagem. Para verificar a mensagem e retornar à página **Informações Globais de Fonte de Dados Java API**, clique em **OK**.

14. Opcional: Na seção **Arquivos Suplementares** da página **Informações Globais da Origem de Dados da API Java**, você pode incluir os arquivos que são compactados com o agente e copiados para o sistema de agente na instalação do agente. O arquivo JAR da API do cliente do provedor Java não é listado aqui; ele é copiado automaticamente para o sistema do agente. A coluna **Tipo de Arquivo** descreve como é esperado que cada arquivo seja usado. Três possíveis usos são descritos na tabela a seguir: (Tabela 284 na página 1326). Clique em **Editar** para editar o arquivo de importado. Para obter mais informações, consulte (“Editando uma definição de arquivo de comando” na página 1280).

Tabela 284. Tipos de arquivos para arquivos complementares

Tipo de arquivo	**Descrição**
Executável	Selecione esta opção se desejar incluir um arquivo executável com o agente. O agente não usa esse arquivo, mas ele está no caminho para que o aplicativo Java use.
Biblioteca	Selecione esta opção se você incluir uma biblioteca com o agente. O agente não usa esse arquivo, mas está no caminho da biblioteca para que o aplicativo Java use.
Recurso Java	Selecione esta opção para incluir recursos Java com o agente. O agente não usa esse arquivo, mas ele está no caminho da classe para que o aplicativo Java use.

Nota: Quando um arquivo complementar de recursos Java é incluído no Agent Builder, o arquivo é incluído automaticamente no caminho de classe do projeto. O compilador Java usa o arquivo complementar para resolver quaisquer referências que seu código possua para as classes no recurso.

Para obter informações sobre onde os Arquivos Suplementares estão instalados com o agente, consulte ("Novos Arquivos em Seu Sistema" na página 1397).

15. Opcional: Crie um filtro para limitar os dados retornados por este grupo de atributos, se os dados são amostrados. Crie um filtro clicando em **Avançado**.

    Nota: Os dados são de amostra se você não selecionou **Produz eventos** na página de **Informações de API Java**.

    Para obter informações adicionais sobre filtragem de dados de um grupo de atributos, consulte "Filtrando Grupos de Atributos" na página 1201

16. Opcional: Inclua propriedades de configuração para o subnó.

    Se estiver incluindo esta origem de dados em um subnó, a página **Substituições de Configuração de Subnó** é mostrada para que seja possível incluir propriedades de configuração no subnó. Pelo menos uma propriedade de configuração é necessária sob o subnó para que o aplicativo Java de amostra a ser criado. Pelo menos uma propriedade de configuração é necessária, pois a amostra usa uma propriedade de configuração para distinguir uma instância de subnó da outra.

17. Execute uma das seguintes etapas:

    a) Se estiver usando o assistente de **Agente**, clique em **Avançar**. Complete o assistente conforme necessário.

    b) Caso contrário, clique em **Concluir** para salvar a origem de dados e abrir o Agent Editor. Em seguida, no menu principal, selecione **Arquivo** > **Salvar**.

    Neste ponto, o Agent Builder cria o código-fonte para o aplicativo de monitoramento. O código está localizado no subdiretório `src` do diretório do projeto. Edite este código para criar seu aplicativo de monitoramento.

O que Fazer Depois

Selecione os sistemas operacionais na página **configurações de API Java**. Faça essa seleção se este grupo de atributos e o aplicativo Java forem executados em sistemas diferentes do sistema operacional definido para o agente. Para abrir esta página, clique em **Configurações API Java** na visualização da estrutura de tópicos ou clique em **Configurações Globais** no Agent Editor em qualquer página do grupo de atributos API Java.

Nota: Os códigos de erro e arquivos complementares podem ser atualizados posteriormente nas seções **Códigos de Erro** e **Arquivos Complementares** da página **Configurações da API Java**.

Executando o Aplicativo Java

Informações sobre a inicialização do aplicativo Java e suas dependências

Inicialização do Aplicativo Java

O agente inicia o aplicativo Java enquanto está iniciando e inicializando. As definições de configuração são usadas para controlar qual tempo de execução Java é usado para iniciar o processo. Os argumentos da Java virtual machine e o nível de criação de log Java também podem ser especificados na configuração. Para obter mais informações sobre a configuração da API Java, consulte "Configuração de API Java" na página 1337. O processo Java herda as variáveis de ambiente definidas para o agente. As definições de configuração do tempo de execução também são colocadas no ambiente e podem ser consultadas usando as chamadas de API.

O aplicativo Java deve ser um processo de execução longa. Não deve finalizar a menos que ele receba uma solicitação de encerramento da API. Se o aplicativo Java finalizar depois de ter se registrado no agente, o agente tentará reiniciar o aplicativo Java até três vezes. Se a coleção de dados for retomada de forma bem-sucedida, essa contagem de reinicialização será reconfigurada. O agente registra um erro quando um aplicativo Java finaliza e quanto uma reinicialização é iniciada.

Nota: Se o aplicativo Java finalizar antes de o registro do grupo de atributos ser concluído, não será feita nenhuma tentativa reinicialização.

Dependências

Um aplicativo Java deve usar um Java Runtime Environment. As seguintes versões Java são suportadas:

- Oracle Corporation Java Versão 5 ou mais recente
- IBM Corporation Java Versão 5 ou posterior

O Java já deverá estar instalado no sistema de agente quando o agente for configurado e iniciado. O arquivo JAR que contém a API usada para se comunicar com o agente é incluída com o `tempo de execução` do agente e incluída com o `caminho de classe` da JVM. Quaisquer arquivos JAR adicionais necessários a seu aplicativo Java devem ser definidos como Arquivos Complementares para os grupos de atributos da API Java. Qualquer arquivo suplementar que tenha um *Tipo de Arquivo* de *Recurso Java* será automaticamente incluído no `classpath` base do aplicativo Java, juntamente com o arquivo JAR da API Java.

Quaisquer arquivos JAR necessários para a operação de tempo de execução do aplicativo Java que não forem incluídos com o agente deverão ser incluídos na definição de configuração *Caminho da classe para jars externos*.

Aplicativo Java de Amostra Gerado

Uma referência que descreve o código que o Agent Builder gera e o código que deve incluir ou substituir para os recursos que deseja monitorar.

Ao criar um agente com uma ou mais origens de dados da API Java, o Agent Builder gera o código de origem do aplicativo Java. O código é gerado no projeto do agente e acompanha a estrutura de seu agente. Você deve incluir seu próprio código Java no aplicativo gerado. Seu código coleta dados para grupos de atributos, manipula eventos para serem postados em grupos de atributos baseados em eventos, reporta erros se forem encontrados problemas, e executa tarefas. O aplicativo gerado fornece ao agente dados, mas são dados de amostra, para serem substituídos pelos dados obtidos dos recursos que você deseja monitorar.

Um agente de amostras é presumido conter as características a seguir:

- Código de produto: `K91`
- Classe Principal da API Java: `agent.client.MainClass`
- Estrutura da origem de dados do agente, conforme mostrado em (Figura 47 na página 1329):

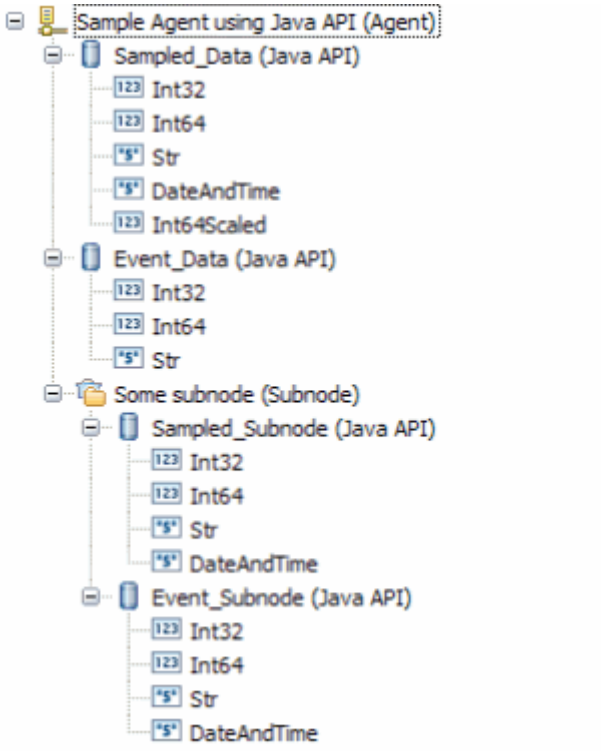


Figura 47. Estrutura do agente de amostra

- Propriedades de configuração de *alguns subnós*: `K91_INSTANCE_KEY`

Estrutura de Classes

O aplicativo Java gerado separa, em um grau elevado, o código que faz interface com o agente do código que faz interface com os recursos que você está monitorando. Contém arquivos que você modifica e arquivos que não podem ser modificados.

As seguintes classes Java são criadas pelo Agent Builder:

`MainClass` (pacote `agent.client`)
A classe que especificou na página **Informações de Origem de Dados da API Java Global**. Essa classe contém um método main e um método que manipula solicitações *take action* . Esta classe é herdada da classe auxiliar descrita a seguir. Você deve modificar essa classe para fazer interface com recursos que você deseja monitorar e as ações que deseja tomar.

`MainClassBase` (pacote `agent.client`)
Uma classe auxiliar que inicializa a conexão com o servidor, registra os grupos de atributos e aguarda por solicitações do servidor. Não modifique esta classe.

Classes `Sampled_Data`, `Sampled_Subnode`, `Event_Data` e `Event_Subnode` (pacote `agent.client.attributeGroups`)
Há uma classe para cada grupo de atributos da API Java que trata solicitações de coleção de dados para o grupo de atributos ou gera eventos para o grupo de atributos. Cada uma dessas classes é herdada de uma das classes auxiliares descritas a seguir. Você deve modificar essas classes para reunir dados dos recursos que deseja monitorar.

Classes `Sampled_DataBase`, `Sampled_SubnodeBase`, `Event_DataBase` e `Event_SubnodeBase` (pacote `agent.client.attributeGroups`)
As classes auxiliares, uma para cada grupo de atributos API Java, que definem a estrutura dos atributos do grupo em uma classe interna. Não modifique essas classes.

Interface `ICustomAttributeGroup` (pacote `agent.client.attributeGroups`)
Uma interface que defina os métodos públicos em cada classe de grupo de atributos. Não modifique esta interface.

As classes que você deseja modificar nunca são substituídas pelo Agent Builder. O Agent Builder as cria somente se elas não existirem.

As classes auxiliares e a interface são sobrescritas sempre que o Agent Builder é salvo. Conforme você modifica e salva o agente, as classes auxiliares são atualizadas para refletir quaisquer mudanças estruturais nos grupos de atributos da API Java. A interface e as classes auxiliares contêm um aviso no cabeçalho que lembra você para não modificar o arquivo.

Inicialização e limpeza

O método main em `MainClass` é chamado quando o agente é iniciado. Ele cria uma instância `MainClass` e então cria um método de execução longa para receber e manipular solicitações do agente.

A maior parte da inicialização e código de limpeza deve ser incluída em `MainClass`. No construtor, inclua a inicialização que é necessária para criar ou acessar seus recursos. Pode ser necessário abrir conexões para remover recursos, criar manipulação ou inicializar estruturas de dados.

Antes que o agente finalize, o método `stopDataCollection` é chamado. Se você precisar fechar as conexões ou limpar antes que o aplicativo Java seja encerrado, inclua esse código no método `stopDataCollection`.

Se a inicialização for necessária somente para um grupo de atributos em particular, essa inicialização pode ser incluída no construtor da classe do grupo de atributos. Do mesmo modo, se alguma limpeza for necessária comente para um grupo de atributos em particular, esse código de limpeza pode ser incluído no método `stopDataCollection` do grupo de atributos.

Qualquer código no aplicativo Java pode usar o objeto criador de logs para gravar entradas de log. (A classe auxiliar principal cria um objeto criador de logs protegido em seu construtor. Os objetos auxiliares do grupo de atributos criam uma referência protegida para esse criador de logs em seus construtores). O objeto do criador de logs utiliza o utilitário de log de rastreio Java. Erros e informações de rastreio detalhadas podem ser obtidas no log de rastreio que é criado pelo criador de logs. As informações de rastreio são importantes para resolução de problemas com o provedor.

Quando `stopDataCollection` é chamado, se passar o trabalho de limpeza para outro encadeamento, aguarde até que ele termine antes de retornar do método `stopDataCollection`. Caso contrário, o trabalho de limpeza poderá ser finalizado abruptamente quando o processo finalizar, pois o encadeamento principal foi concluído.

Uma das definições de configuração do agente é para o nível de rastreio Java. A tabela a seguir mostra os valores que podem ser definidos na propriedade de configuração JAVA_TRACE_LEVEL. Se a API criou o criador de logs para você, a tabela mostrará o Nível que é usado pelo criador de logs.

Tabela 285. Opções de nível de rastreio Java

Nível de rastreio configurado	**Nível de rastreio de criação de log de Java**	**Descrição**
Desativado	DESLIGADO	Nenhuma criação de log é feita.
Erro	GRAVE	Problemas de rastreio que ocorreram no aplicativo Java.
Aviso	Aviso	Erros de rastreio e erros em potencial.
Informações	INFORMAÇÕES	Rastrear informações importantes sobre o aplicativo Java.
Depuração Mínima	BOM	Rastrear detalhes de alto nível necessários para analisar o comportamento do aplicativo Java.

Tabela 285. Opções de nível de rastreio Java (continuação)		
Nível de rastreio configurado	**Nível de rastreio de criação de log de Java**	**Descrição**
Depuração Média	MELHOR	Rastrear detalhes sobre o fluxo do programa do aplicativo Java.
Depuração Máxima	EXCELENTE	Rastrear todos os detalhes sobre o aplicativo Java.
Todos	TODOS	Rastrear todas as mensagens.

O nome do arquivo de log que é criado pelo aplicativo Java neste exemplo é `k91_trace0.log`. Se o agente for um agente de diversas instâncias, o nome da instância será incluído no nome do arquivo de log.

Nota: Não escreva mensagem para erro padrão ou para saída do padrão. Nos sistemas Windows, essas mensagens serão perdidas. Nos sistemas UNIX e Linux, esses dados serão gravados em um arquivo que não é quebrado.

Coletando Dados do Grupo de Atributos Amostrados

A classe de um grupo de atributos de amostra (um que coleta um ou mais linhas de dados) contém um método `collectData`, por exemplo, `Sampled_Data.collectData`. Este método é chamado sempre que dados são solicitados pelo agente.

A classe auxiliar do grupo de atributos define uma classe interna chamada Atributos. Essa classe possui um campo para cada atributo que é definido em seu grupo de atributos. Atributos derivados não são incluídos pois são calculados pelo agente. Os tipos de dados de campos de atributo são equivalentes Java para os tipos de atributo do Tivoli Monitoring, conforme mostrado em (Tabela 286 na página 1331).

Tabela 286. Os tipos de dados de campos de atributo e seus equivalentes de tipo de atributo do IBM Tivoli Monitoring	
Tipo do Tivoli Monitoring	**Tipo de dados do campo de atributo**
Sequência	Sequência
Numérico, 32 bits, sem ajuste decimal	int
Numérico, 64 bits, sem ajuste decimal	long
Numérico, ajuste decimal diferente de zero	duplo
Registro de Data e Hora	Calendário

O método `collectData` deve:

1. Coletar os dados apropriados do recurso que está sendo monitorado.
2. Criar um objeto Atributos.
3. Incluir os dados nos campos do objeto Atributos.
4. Chamar o método `Attributes.setAttributeValues` para copiar os dados para um buffer interno.
5. Repita as etapas 1 - 4 conforme necessário para cada linha de dados. É possível ignorar as etapas de 1 a 4 juntas e não ter retorno de linha. Nesse caso, a coluna de código de erro da tabela de Status do Objeto de Desempenho possui um valor de NO_INSTANCES_RETURNED. Para obter informações adicionais sobre os códigos de erro, consulte (“Códigos de Erros” na página 1334).
6. Chame `AgentConnection.sendData` para enviar os dados ao agente ou chame `sendError` para descartar dados copiados de chamadas para `setAttributeValues` e envie um código de erro em vez disso.

Você deve coletar os dados de seu recurso (Etapa 1), substituindo os dados de amostra usados no aplicativo gerado.

Para preencher o objeto Atributos, é possível passar os dados usando o construtor de Atributos (como é feito no aplicativo gerado). Alternativamente, use o construtor de argumento zero para criar um objeto Atributos e, em seguida, designar os campos do objetos Atributos aos valores dos atributos coletados. Os campos possuem o mesmo nome que os atributos, embora iniciem com uma letra minúscula.

Coletando Dados Amostrados para um Subnó

Se um grupo de atributos amostrados estiver em um subnó, presumivelmente há vários recursos que você esteja monitorando (um recurso diferente para cada subnó). Você deve determinar de qual recurso coletar dados. Deve haver uma ou mais propriedades de configuração que identifiquem qual recurso está sendo monitorado.

Para este exemplo, assume-se que uma propriedade de configuração, `K91_INSTANCE_KEY`, contém um valor que identifica o recurso a partir do qual dados devem ser coletados.

Use as etapas a seguir para localizar o recurso correto:

1. Obtenha o ID da instância de todos os subnós configurados chamando `AgentConnection.getConfiguredSubnodeInstanceIDs`. Cada subnó que é configurado possui um ID de instância exclusivo.
2. Para cada ID de instância, obtenha a propriedade de configuração `K91_INSTANCE_KEY` chamando `AgentConnection.getSubnodeConfigurationProperty`.
3. Localize o recurso que é representado pelo valor em `K91_INSTANCE_KEY`.

Essas etapas podem ser executadas no método `collectData`, antes das séries de etapas detalhadas em (“Coletando Dados do Grupo de Atributos Amostrados” na página 1331).

Alternativamente, você pode desejar executar essas etapas no construtor de classe do grupo de atributos e estabelecer um mapeamento direto do ID da instância para o recurso. Um construtor de classe de grupo de atributos de exemplo é o construtor `Sampled_Subnode`. Esse procedimento oferece a oportunidade de criar identificadores ou abrir conexões que podem ser usadas durante a vida do agente. Criar identificadores ou abrir conexões podem deixar seu acesso aos recursos mais eficiente.

O código gerado cria objetos de recurso de amostra do tipo `MonitoredEntity` no construtor, e os inclui em um mapa `configurationLookup`. Você deve remover a classe interna de `MonitoredEntity`, e substituis os objetos `MonitoredEntity` com objetos que acessam seus próprios recursos. Se você escolher fazer todos o procedimento de consulta no método `collectData`, pode remover o mapa `configurationLookup` da classe.

Se escolher usar o construtor para mapear o ID da instância do subnó para seu recurso, as etapas no método `collectData` são:

1. Recuperar o ID da instância do subnó a partir do parâmetro de solicitação, chamando `Request.getSubnodeInstanceID`.
2. Recupere o objeto de recurso do mapa que é criado no construtor.
3. Execute as séries de etapas detalhadas em “Coletando Dados do Grupo de Atributos Amostrados” na página 1331 para enviar dados ao agente.

Uma propriedade de subnó arbitrária é escolhida no exemplo do Agent Builder, nesse caso `K91_INSTANCE_KEY`. Se não for a propriedade correta, ou mais de uma propriedade for necessária para identificar o recurso correto, você deverá escolher as propriedades para identificar o recurso.

Enviando Eventos

Para grupos de atributos que geram eventos, não há chamada periódica para um método `collectData`. Os eventos são enviados pelo aplicativo enquanto são postados pelo recurso.

Como um exemplo de eventos de produção, o código gerado para um grupo de atributos baseado em eventos cria e inicia um encadeamento que executa a partir de uma classe interna chamada

SampleEventClass. O grupo de atributos baseado em evento que é usado no exemplo é a classe Event_Data. O encadeamento, periodicamente, se torna ativo e envia um evento. Se desejar pesquisar seu recurso para eventos periodicamente, é possível usar a estrutura da classe Event_Data como foi gerada:

1. Do construtor Event_Data, crie e inicie um encadeamento.
2. No método de execução do encadeamento, realize um loop até o agente ser finalizado.
3. Fique inativo por um tempo antes de verificar eventos. Você talvez deseje alterar o intervalo de pesquisa de 5.000 milissegundos para um número que faça sentido para o seu agente.
4. Determine se um ou mais eventos ocorreram. O aplicativo gerado não verifica, mas sempre posta um único evento.
5. Para cada evento que deve ser postado, obtenha os dados a serem postados.
6. Crie e preencha o objeto de Atributo (como o método collectData realizou para um grupo de atributos amostrado).
7. Chame o método Attributes.sendEventData. Os eventos consistem em uma única linha, portanto, somente um único evento pode ser enviado por vez.

Como alternativa, se você estiver trabalhando com uma API Java que relata eventos a partir de seu próprio encadeamento, você poderá inicializar esse encadeamento no construtor Event_Data. Também é possível registrar seu próprio objeto de manipulação de evento com o mecanismo de manipulação de evento de seu recurso. Em seu manipulador de eventos, use as etapas a seguir:

1. Obtenha os dados de eventos a serem postados.
2. Crie e preencha o objeto Atributos.
3. Chame o método Attributes.sendEventData.

Neste caso, você não tem de criar seu próprio encadeamento na classe Event_Data nem seria necessária a classe SampleEventClass.

Enviando Eventos em um Subnó

Quando um evento é detectado para um grupo de atributos de subnó, o aplicativo Java deve postar o evento no subnó correto.

Para este exemplo, assume-se que uma propriedade de configuração, K91_INSTANCE_KEY, contém um valor que identifica uma instância de um recurso que pode produzir eventos. Também é assumido que o valor da propriedade K91_INSTANCE_KEY é recuperado juntamente com os dados a serem postados no evento. Para executar a recuperação da propriedade e dos dados, o aplicativo Java executa as etapas a seguir:

1. Obtém dos dados do evento a serem postados, juntamente com a “chave da instância”.
2. Cria e preenche o objeto Atributos.
3. Obtém uma lista de IDs de subnós configurados chamando AgentConnection.getConfiguredSubnodeInstanceIDs.
4. Para cada instância de subnó, busque o valor K91_INSTANCE_KEY chamando AgentConnection.getSubnodeConfigurationProperty.
5. Quando o valor K91_INSTANCE_KEY for localizado, o que corresponde ao valor que é obtido com os dados do evento, lembra-se do ID da instância do subnó correspondente.
6. Chama Attributes.sendSubnodeEventData, passando o ID da instância de subnó lembrado.

O aplicativo gerado não realiza a consulta descrita nas etapas 4 e 5, mas, em vez disso, posta um evento para o grupo de atributos de cada subnó. Provavelmente, este não é o comportamento correto para um agente de produção.

Comandos Executar ação

Os comandos Executar Ação são definidos no Tivoli Enterprise Portal e usando o comando tacmd createaction. As ações podem ser importadas no projeto Agent Builder do agente, de modo que elas sejam criadas quando o agente é instalado. Para obter informações adicionais sobre a importação dos comandos take action, consulte ("Importando Arquivos de Suporte do Aplicativo" na página 1406).

O aplicativo Java gerado registra-se para quaisquer ações que iniciam com o código do produto do agente, por exemplo, K91Refresh. Esse registro é feito na classe auxiliar principal (MainClassBase) a partir do método registerActionPrefix. Se desejar registrar outros prefixos, ou não registrar para ação nenhuma, substitua o registerActionPrefix em (MainClassBase).

Quando o agente deseja executar uma ação que inicia com um prefixo que seu agente registrou, o método MainClass.takeAction é chamado. Você inclui o código para chamar Request.getAction(), execute a ação apropriada e então chame AgentConnection.sendActionReturnCode para enviar o código de retorno de sua ação. Um código de retorno de 0 significa que a ação é bem-sucedida, qualquer outro código de retorno significa que a ação falhou.

Manipulando Exceções

Os métodos collectData e takeAction podem lançar qualquer exceção Java; portanto, você pode permitir que seu código de coleção lance as exceções sem capturá-las. O método handleException (para collectData) ou o método handleActionException (para takeAction) é chamado quando a classe auxiliar obtém a exceção.

Para exceções collectData, você deve chamar AgentConnection.sendError quando ocorre uma exceção ou quando há um problema na coleta de dados. O aplicativo gerado passa um código de erro de GENERAL_ERROR. Entretanto, você deve substituir este código de erro por um definido pelo seu agente que melhor descreva o problema que foi encontrado. Para obter informações adicionais sobre a inclusão dos códigos de erro, consulte a Etapa ("13" na página 1325).

Para exceções takeAction, você deve chamar AgentConnection.sendActionReturnCode com um código de retorno diferente de zero.

Alguns do métodos AgentConnection lançam exceções que são derivadas de com.ibm.tivoli.monitoring.agentFactory.customProvider.CpciException. O método handleException não é chamado se uma CpciException for lançada durante a coleta de dados, já que a classe auxiliar lida com a exceção.

Nota: Se você optar por capturar suas exceções dentro do método collectData em vez de usar o método handleException, assegure-se de que qualquer CpciException seja lançado novamente. Assegure que CpciException seja lançada novamente assim ela pode ser manipulada pela classe base.

Códigos de Erros

Uma resposta típica para uma exceção ou outro erro de recurso é enviar um código de erro para o agente chamando o método AgentConnection.sendError. Um erro para um grupo de atributos com base em eventos pode ser enviado em qualquer momento. Um erro para o grupo de atributos de amostra pode ser enviado somente em resposta a uma solicitação de dados de coleção, e em lugar de uma chamada sendData.

Se você enviar um erro para o agente, ocorrerá o seguinte:

1. Uma mensagem de erro é registrada no log de rastreio do agente. Esta mensagem de erro inclui o código de erro e a mensagem definidos para esse código de erro.
2. Há uma consulta de Status do Objeto de Desempenho que pode ser visualizada para obter informações de status sobre os seus grupos de atributos. A coluna Código de Erro é configurada para o tipo de Código de Erro definido para o erro que você enviou. O status de erro é eliminado após os dados serem recebidos de forma bem-sucedida pelo agente para o grupo de atributos. Se você responder a uma solicitação de dados de coleção com uma chamada sendData mas você não tiver incluído linhas de dados, você obterá NO_INSTANCES_RETURNED na coluna de Código de Erro.

A tabela a seguir descreve alguns códigos de erros que são internos para o agente e que você poderá ver em determinadas situações:

Tabela 287. Códigos de erros internos para o agente

Código de Erro	Descrição
NO_ERROR	Não há problemas com o grupo de atributos atualmente.
NO_INSTANCES_RETURNED	O aplicativo Java respondeu a uma solicitação de coleção de dados mas não forneceu dados. Não fornecer dados não é um erro. Isso geralmente indica que não há instâncias do recurso que esteja sendo monitorado pelo grupo de atributos.
OBJECT_NOT_FOUND	O agente tentou coletar dados de um grupo de atributos que não é registrado por meio de API do cliente. Esse erro pode significar que o aplicativo falhou ao iniciar ou não iniciou o registro do grupo de atributos quando o agente tentou coletar dados.
OBJECT_CURRENTLY_UNAVAILABLE	O aplicativo enviou ao agente um código de erro que não está definido na lista global de códigos de erro.
GENERAL_ERROR	Ocorreu um problema ao coletar dados do aplicativo, geralmente porque o aplicativo não respondeu à solicitação dentro do intervalo de tempo limite. Consulte o log de rastreio do agente para obter mais detalhes. O aplicativo também pode especificar GENERAL_ERROR como um código de erro, mas é melhor se um código de erro mais detalhado for definido.

Alterações para o Agente

Para determinadas mudanças no agente serão necessárias mudanças correspondentes no aplicativo Java. Se as mudanças estruturais forem complexas, é possível excluir algum ou todos os arquivos de origem Java antes de salvar o agente. Também é possível excluir os arquivos se desejar iniciar sem as customizações que você fez.

A tabela a seguir descreve as modificações necessárias nos arquivos de origem do aplicativo Java depois que determinadas mudanças forem feitas no Agent Builder quando o agente for salvo.

Tabela 288. Mudanças em um Agente que Precisam de Modificações na Origem Java

Alteração do agente	O que o Agent Builder executa	Mudanças manuais necessárias na origem Java
Alteração do nome do pacote da classe principal	• Gerar todas as classes na nova estrutura de pacotes. • Remove todas as classes auxiliares do pacote antigo.	• Transportar o conteúdo da classe principal e do grupo de atributos a partir das classes no antigo pacote para as classes no novo pacote. • Remover as classes do antigo pacote após a conclusão da migração.

Tabela 288. Mudanças em um Agente que Precisam de Modificações na Origem Java (continuação)

Alteração do agente	**O que o Agent Builder executa**	**Mudanças manuais necessárias na origem Java**
Alteração do nome da classe principal	• Cria novas classes principais. • Remove a antiga classe auxiliar principal.	• Transportar o conteúdo da classe principal para a nova classe. • Atualizar referências para o nome da classe a partir das classes do grupo de atributos.
Adição de um grupo de atributos da API Java	• Cria classes para o novo grupo de atributos. • Inclui o registro para o novo grupo de atributos na classe auxiliar principal.	Sobrescrever o código de amostra com lógica customizada na classe do grupo de atributos.
Remoção de um grupo de atributos da API Java	Remove o registro da classe auxiliar principal.	• Remover a classe de grupo de atributos ou transportar a lógica customizada para alguma outra classe. • Remover a classe auxiliar do grupo de atributos.
Renomeação de um grupo de atributos da API Java	• Cria classes para o novo nome do grupo de atributos. • Atualiza o registro para o grupo de atributos renomeado na classe auxiliar principal.	• Transportar lógica customizada na classe do grupo de atributos com o nome antigo para a classe do grupo de atributos com o novo nome. • Remover a classe do grupo de atributos com o antigo nome. • Remover a classe auxiliar do grupo de atributos com o antigo nome.
Adição de um atributo em um grupo de atributos da API Java	Atualiza a classe interna Atributos na classe auxiliar do grupo de atributos.	Coletar dados para o novo atributo na classe do grupo de atributos.
Remoção de um atributo de um grupo de atributos da API Java	Atualiza a classe Atributos na classe auxiliar do grupo de atributos.	Remover coleção de dados para o atributo antigo na classe do grupo de atributos.
Renomeação de um atributo em um grupo de atributos da API Java	Atualiza o nome do atributo na classe Atributos na classe auxiliar do grupo de atributos.	Atualizar quaisquer referências para o nome do atributo na classe Atributos (geralmente, não há referências, pois o construtor Atributos, com argumentos posicionais, é usado).
Reordenação de atributos em um grupo de atributos da API Java	Atualiza a ordem de atributos na classe Atributos na classe auxiliar do grupo de atributos.	Atualizar a ordem dos argumentos em quaisquer chamadas para o construtor Atributos.

Algumas das mudanças que são mencionadas na tabela anterior podem ser aperfeiçoadas se usar a ação Eclipse Refactor - Rename action. Use esta ação em todos os nomes afetados (incluindo nomes de classe auxiliar) antes de salvar o conteúdo alterado.

Uso da API Java

A API Java é usada em todo o aplicativo Java gerado para a comunicação com o agente. Frequentemente, sua única interação direta com a API Java é modificar um parâmetro de uma chamada de método existente. Por exemplo, alterando um código de erro postado de GENERAL_ERROR para um código de erro definido em seu agente.

Se você precisar executar codificação mais intensiva com a API Java, poderá visualizar o Javadoc a partir do editor de texto do Eclipse. É possível visualizar o Javadoc ao editar código Java executando as etapas a seguir:

1. Destaque um nome de pacote, classe ou método na API.
2. Pressione **F1** para abrir a visualização Ajuda do Eclipse.
3. Selecione o link Javadoc.

Também é possível ver uma breve descrição a partir do Javadoc passando o ponteiro do mouse sobre um nome de classe ou método. O Javadoc para a API também pode ser localizado no Tivoli Monitoring Knowledge Center, consulte Javadoc.

As classes para a API Java estão em `cpci.jar`. O arquivo `cpci.jar` é incluído automaticamente no Java Build Path do projeto quando um agente que contém um grupo de atributos da API Java é criado. O arquivo também é incluído quando um agente que contém um grupo de atributos API Java é importado. O arquivo também é incluído quando um grupo de atributos de API Java for incluído em um agente existente. O `cpci.jar` também é compactado automaticamente com cada agente que contém um grupo de atributos da API Java e incluído no CLASSPATH do aplicativo Java.

Configuração de API Java

Ao definir uma origem de dados de API Java em seu agente, algumas propriedades de configuração são criadas para você.

Se você definir uma origem de dados da API Java no seu agente, o agente deverá usar o Java para conectar-se ao servidor da API Java. As propriedades de configuração de Java são incluídas no agente automaticamente. As seguintes propriedades de configuração de Java são específicas à configuração do tempo de execução do agente:

Tabela 289. Propriedades de configuração do Java

Nome	Valores Válidos	Obrigatório	Descrição
Início do Java	Caminho completo para um diretório	Não	Um caminho completo que aponta para o diretório de instalação do Java.
Nível de rastreio Java	Opção	Sim	Use esta propriedade para especificar o nível de rastreio usado pelos provedores Java.
argumentos do JVM	Cadeia	Não	Use essa propriedade para especificar uma lista opcional de argumentos para a Java virtual machine.

Tabela 289. Propriedades de configuração do Java (continuação)			
Nome	**Valores Válidos**	**Obrigatório**	**Descrição**
Caminho da classe para JARs externos	Cadeia	Não	Caminho contendo quaisquer arquivos JAR que não estão incluídos com o agente, mas são necessários para a operação do cliente de tempo de execução.

Essas variáveis de configuração estão disponíveis na página **Informações de Configuração de Tempo de Execução** do Agent Editor em **Configuração para Java Virtual Machine (JVM)** e **Configuração para API Java**.

Testando Grupos de Atributos de Aplicativo Java
É possível testar o grupo de atributos do aplicativo Java criado no Agent Builder.

Antes de Iniciar

Restrição: Diferentemente da maioria dos outros grupos de atributos, não é possível testar o grupo de atributos do aplicativo Java enquanto ele está sendo criado. É possível testar o grupo de atributos quando é incluso no agente e o agente é salvo. Salvar o agente faz com que o código Java seja gerado para o grupo de atributos.

Procedimento

1. Selecione um grupo de atributos na página **Definição de Origem de Dados** do **Agent Editor** após a criação do agente e clique em **Testar**.

   Para obter informações adicionais sobre o Agent Editor, consulte "Usando o Agent Editor para modificar o agente" na página 1172

   Após clicar em **Testar** em uma das duas etapas anteriores, a janela **Testar Cliente Java** é exibida.
2. Opcional: Antes de iniciar seu teste, é possível configurar as variáveis de ambiente, as propriedades de configuração e as informações Java. Para obter mais informações, consulte "Teste de Grupo de Atributos" na página 1380. Para obter mais informações sobre as propriedades de configuração do Java Runtime padrão, consulte "Configuração de API Java" na página 1337.
3. Clique em **Iniciar Agente**. Uma janela indica que o Agente está iniciando.
4. Para simular uma solicitação a partir do Tivoli Enterprise Portal ou SOAP para dados do agente, clique em **Coletar Dados**.

   O agente monitora os dados do Cliente Java. A janela **Testar Cliente Java** exibe quaisquer dados que são retornados.
5. Opcional: Clique em **Verificar Resultados**, se os dados retornados não estiverem conforme o esperado.

   A janela **Status de Coleção de Dados** é aberta e mostra informações adicionais sobre os dados. Os dados coletados e exibidos pela janela Status da Coleção de Dados são descritos em "Nó de Status do Objeto de Desempenho" na página 1424
6. Pare o agente, clicando em **Parar Agente**.
7. Clique em **OK** ou **Cancelar** para sair da janela **Testar Cliente Java**. Clicar em **OK** salva quaisquer mudanças que tiver feito.

Conceitos relacionados
"Testando seu agente no Agent Builder" na página 1380
Depois de usar o Agent Builder para criar um agente, será possível testar o agente no Agent Builder.

Criando conjuntos de dados a partir de origens existentes

Quando existe pelo menos um conjunto de dados, é possível criar um novo conjunto de dados usando os dados de um conjunto de dados existente.

A opção para criar um novo conjunto de dados está disponível na página **Origem de dados inicial do agente** e na página **Local da origem de dados**. É possível criar um conjunto de dados usando origens de dados existentes nas seguintes formas:

1. Juntando dados de dois conjuntos de dados existentes (grupos de atributos). Para obter mais informações, consulte “Juntando Dois Grupos de Atributos” na página 1339.
2. Filtrando dados a partir de um conjunto de dados existente (grupo de atributos). Para obter mais informações, consulte “Criando um grupo de atributos filtrado” na página 1344.

Dica: A opção para associar dois conjuntos de dados está disponível somente após a criação de dois ou mais conjuntos de dados.

Juntando Dois Grupos de Atributos

Criar um grupo de atributos a partir de dois outros grupos de atributo.

Sobre Esta Tarefa

Unir grupos de atributos é mais útil quando o agente coleta dados de dois tipos diferentes de origens de dados. Por exemplo, o agente pode coletar dados WMI e PerfMon, ou SNMP e origens de dados de script. Cada conjunto de atributos pode ser mais útil quando usados juntos em uma visualização Tivoli Enterprise Portal.

Por exemplo, presumam que seus grupos de atributos estejam definidos como segue:

```
First_Attribute_Group
    index integer
    trafficRate    integer
    errorCount    integer
```

```
Second_Attribute_Group
    index2    integer
    name string
    traffic string
```

Uma definição lhe fornece os contadores (como Perfmon) e a outra lhe fornece as informações de informação. Nenhum grupo de atributos é útil a você por si próprio. Contudo, se você puder combinar dois grupos de atributos usando o índice para corresponder as linhas apropriadas de cada, terá um grupo de atributos mais útil. É possível usar grupo de atributos combinado para exibir o nome, tipo, e métricas juntos.

Esse mesmo mecanismo pode ser usado para incluir tags nas informações coletadas por meio dos grupos de atributos normais. As informações podem então ser mais facilmente correlacionadas em um sistema de eventos quando um problema for detectado. Por exemplo, uma empresa deseja gerenciar todos os seus servidores coletando dados comuns e usando situações comuns para monitorar o funcionamento dos servidores. Ela também deseja poder identificar os servidores com informações adicionais que informem qual aplicativo está em execução em um determinado servidor. Ela deseja ter o controle dos valores usados em cada servidor, mas não deseja criar agentes diferentes para cada aplicativo. Ele pode conseguir esse controle criando um grupo de atributos adicional em seu agente único, como segue:

```
Application_Information
    application_type     integer
    application_name    string
    application_group    string
```

Esse grupo de atributos seriam definidos como um grupo de atributos de script que reúne seus valores a partir da configuração do agente. É possível especificar valores diferentes para cada instância do agente e usar um agente para gerenciar todos os seus sistemas. Esse grupo de atributos poderia então ser unido a

todos os grupos de atributos de origem em que essas informações do aplicativo pudessem ser necessárias. As informações então ficam disponíveis no Tivoli Enterprise Portal, situações, eventos e dados em warehouse.

Quando você junta dois grupos de atributos, um terceiro grupo de atributos é criado. Este grupo de atributos contém todos os atributos contidos nos grupos de atributos de origem.

Os resultados de uma operação de junção variam, dependendo do número de linhas que cada grupo de atributos de origem suporta. Se ambos os grupos de atributos fossem definidos para retornar somente uma linha única de dados, então o grupo de atributos unidos resultante teria uma linha de dados. O única linha teria todos os atributos de ambos os grupos de atributos de origem de dados.

Tabela 290. grupo um de atributos de origem (linha única)

Atributo1	**Atributo2**	**Atributo3**
16	algum texto	35

Tabela 291. grupo 2 de atributos de origem (linha única)

Atributo4	**Atributo5**	**Atributo6**	**Atributo7**
5001	mais dados	56	35

Tabela 292. Junção resultante

Atributo1	**Atributo2**	**Atributo3**	**Atributo4**	**Atributo5**	**Atributo6**	**Atributo7**
16	algum texto	35	5001	mais dados	56	35

Suponha que um grupo de atributos de origem for definido para retornar somente uma linha (linha única) enquanto outro pode retornar mais de uma linha (linhas múltiplas). O grupo de atributos unido resultante contém o mesmo número de linhas que o grupo de atributos de origem com várias linhas. Os dados do grupo de atributo de linha única é incluído em cada linha do grupo de atributos de múltiplas linhas.

Tabela 293. grupo um de atributos de origem (linha única)

Atributo1	**Atributo2**	**Atributo3**
16	algum texto	35

Tabela 294. grupo dois de atributos de origem (mais de uma linha)

Atributo4	**Atributo5**	**Atributo6**	**Atributo7**
user1	path1	56	35
user2	path2	27	54
user3	path3	44	32

Tabela 295. Junção resultante

Atributo1	**Atributo2**	**Atributo3**	**Atributo4**	**Atributo5**	**Atributo6**	**Atributo7**
16	algum texto	35	user1	path1	56	35
16	algum texto	35	user2	path2	27	54
16	algum texto	35	user3	path3	44	32

Finalmente, presuma que ambos os grupos de atributos de origem sejam definidos para retornar mais de uma linha. Você deve identificar um atributo de cada um dos grupos de atributos de origem nos quais

executar a junção. O grupo de atributos resultante contém linhas de dados em que o valor de atributo no primeiro grupo de atributos corresponde ao valor de atributo do segundo grupo de atributos.

Tabela 296. grupo um de atributos de origem (mais de 1 linha)

Atributo1	**Atributo2**	**Atributo3**
16	algum texto	35
27	mais texto	54
39	outra cadeia	66

Tabela 297. grupo 2 de atributos de origem (mais de 1 linha)

Atributo4	**Atributo5**	**Atributo6**	**Atributo7**
user1	path1	56	35
user2	path2	27	54
user3	path3	44	32

Tabela 298. Junção resultante (juntando Atributo3 e Atributo7)

Atributo1	**Atributo2**	**Atributo3**	**Atributo4**	**Atributo5**	**Atributo6**	**Atributo7**
16	algum texto	35	user1	path1	56	35
27	mais texto	54	user2	path2	27	54

Com o Agent Builder, também é possível juntar grupos de atributos definidos pelo usuário com o grupo de atributos de Disponibilidade, se houver quaisquer filtros de disponibilidade definidos no agente. Para obter informações adicionais sobre os dados contidos no grupo de atributos de Disponibilidade, consulte (“Nó de Disponibilidade” na página 1419).

É possível criar esse tipo de grupo de atributos acessando o menu na árvore de origens de dados clicando com o botão direito do mouse e, em seguida, selecionando **Juntar Grupos de Atributos**.

Procedimento

1. Na página **Definição de Origem de Dados**, clique com o botão direito em um dos grupos de atributo no qual gostaria de ingressar e selecione **Ingressar nos Grupos de Atributos**.

   Essa opção somente será visível, se houver pelo menos dois grupos de atributos definidos. Ter um filtro de disponibilidade definido, leva-se em conta como tendo um grupo de atributos definido.

   A página **Informações de Grupo de Atributos** é exibida.

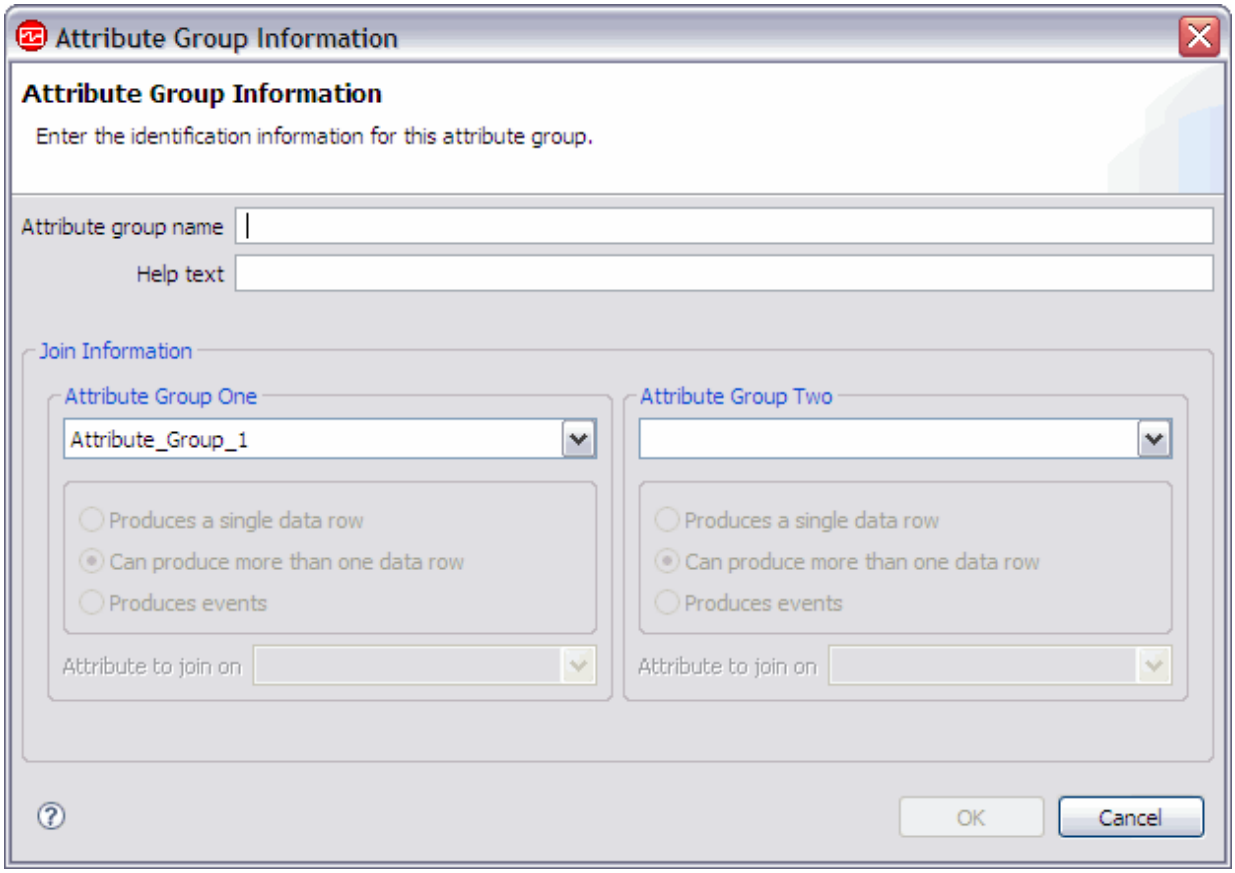


*Figura 48. Página **Informações do Grupo de Atributos**Janela Informações sobre Grupo de Atributos*

2. Na janela **Informações de Junção**, selecione os dois grupos de atributos que você gostaria de juntar. Selecione os grupos de atributos escolhendo entre os grupos disponíveis nas listas **Grupo de Atributos Um** e **Grupo de Atributos Dois**.

   Para cada grupo de atributos, ou **Produz uma única linha de dados** ou **Pode produzir mais de uma linha de dados** está selecionado para você. Essa seleção é bloqueada e depende de como os grupos de atributos de origem foram originalmente definidos.

   Nota: Existem restrições às quais os grupos de atributos podem ser unidos:

   - Não é possível unir um grupo de atributos em um tipo de subnó a um grupo de atributos em outro tipo de subnó.
   - É possível unir somente um grupo de atributos de evento a um grupo de atributos não de evento de linha única.

   a) Selecione o atributo que deseja unir para cada grupo de atributos quando ambos os grupos de atributos mostrarem **Pode produzir mais de uma linha de dados**, em **Atributo para unir**.

   Os campos **Nome do grupo de atributo** e **Ajuda** são preenchidos para você usar informações dos grupos de atributos escolhidos. Se desejar, pode alterar essas entradas.
3. Clique em **OK**.

Resultados
O grupo de atributos unido que criou é incluído na área **Informações do Grupo de Atributos** da página **Definição de Origem de Dados**

Manipulando atributos em grupos de atributos unidos

Usar atributos em grupos de atributos unidos pode impor regras sobre como esses atributos são manipulados.

Excluindo um Grupo de Atributos

Um grupo de atributos não poderá ser excluído, se ele for referido em um grupo de atributos unidos, a não ser que o grupo de atributos unidos também esteja sendo excluído.

Excluindo um Atributo

Um atributo não poderá ser excluído, se seu grupo de atributos pai for referido em um grupo de atributos unidos e uma dessas instruções for verdadeira:

- O atributo é definido como um atributo de junção no grupo de atributos unidos.
- O atributo é usado em qualquer atributo derivado no grupo de atributos unidos.

Os atributos unidos não podem ser excluídos. Somente atributos derivados, se algum for incluído, podem ser excluídos do grupo de atributos unido.

Reordenando Atributos

A ordem dos atributos unidos é fixada pela ordem dos atributos de origem. A lista de atributos unidos não pode ser reordenada. Somente atributos derivados, se houver, podem ser reordenados.

Quando a versão de um agente é confirmada, os atributos de origem e derivados não podem ser reordenados ou removidos. Os atributos incluídos em uma nova versão do agente, se forem atributos derivados ou de origem, virão depois de todos os atributos confirmados. Para obter mais informações, consulte "Confirmando a Versão do Agente" na página 1189.

Incluindo um Atributo

Os novos atributos unidos não podem ser incluídos explicitamente. Somente atributos derivados podem ser criados explicitamente.

Removendo Filtros de Disponibilidade

O último filtro de disponibilidade não poderá ser removido, se o grupo de atributos de Disponibilidade estiver referido em um grupo de atributos unidos.

Atributos Unidos

Manipular informações que estão relacionadas aos atributos unidos.

Procedimento

- Mude o nome do atributo e o texto de ajuda do atributo unido pode ser alterado de forma que fiquem diferentes do atributo de origem:
  a) Selecione o atributo no grupo de atributos associados na área de janela **Informações do Grupo de Atributos** da página **Definição de Origem de Dados**.
  b) Insira o novo nome e o texto de ajuda.
- O atributo associado pode ser mostrado ou não mostrado no Tivoli Enterprise Portal selecionando ou limpando a caixa de opção **Exibir Atributo no Tivoli Enterprise Portal**. A caixa de seleção está na seção **Informações de Atributo Unido** da página **Definição de Origem de Dados**. Essa opção é sem restrição se o atributo de origem for mostrado no Tivoli(r) Enterprise Portal.
- Qualquer atributo ou combinação de atributos (que é mostrado no Tivoli Enterprise Portal) pode ser marcado como atributo-chave, ao selecionar a caixa de seleção **Atributo-chave**. Essa opção não depende dos atributos serem ou não atributos-chave nos grupos de atributos de origem. A opção também não depende dos atributos de origem serem mostrados ou não no Tivoli(r) Enterprise Portal.
- As informações sobre tipo de atributo para atributos unidos são obtidas dos atributos de origem e não podem ser alteradas no atributo unido. Na seção **Informações do Grupo de Atributos Associados** do Agent Editor (Figura 49 na página 1344), clique em **Localizar Atributo de Origem** para acessar o atributo de origem.

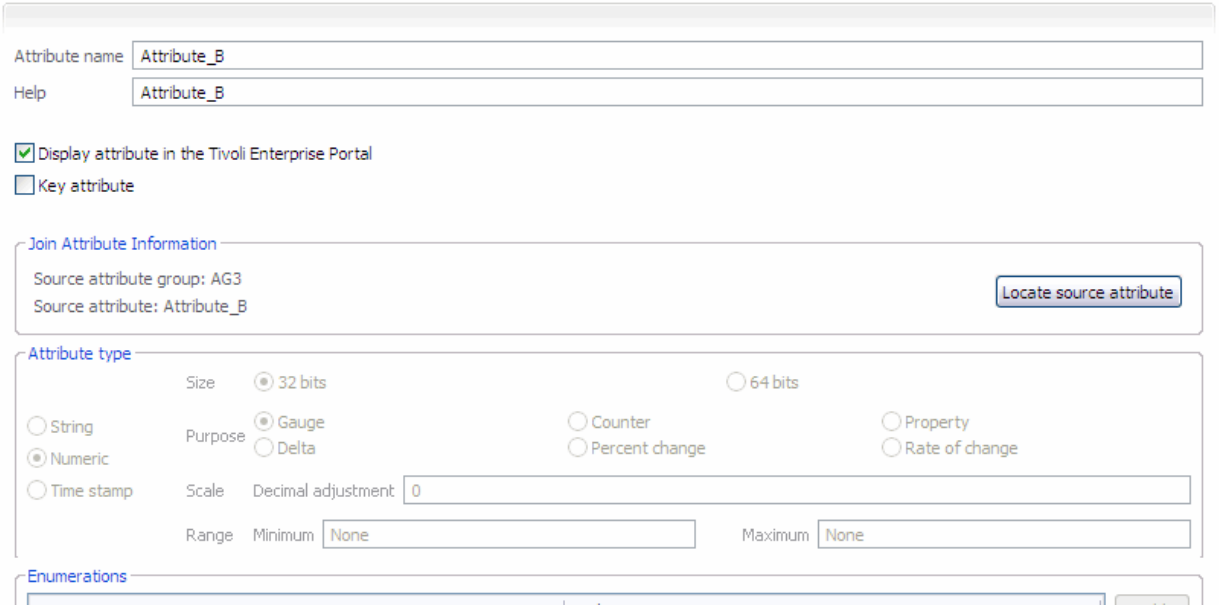


Figura 49. Localizando Informações sobre o Atributo de Origem

Quaisquer alterações nos grupos de atributos de origem são refletidas nos atributos unidos. Se os grupos de atributos de origem forem alterados, eles serão automaticamente atualizados sob o grupo de atributos unido. Essa atualização automática também ocorre se um grupo de atributos diferente for configurado como o grupo de atributos de origem. As mudanças em um tipo de atributo de origem são copiadas no atributo unido. As mudanças em um nome do atributo de origem ou no texto de ajuda são copiadas no atributo unido. Entretanto, essas alterações no atributo de origem não são copiadas depois que você alterar o nome ou o texto de ajuda de um atributo unido.

Criando um grupo de atributos filtrado

Crie um grupo de atributos filtrado (conjunto de dados) filtrando linhas de dados a partir de um grupo de atributos existente. Se um conjunto de dados existente retornar diversas linhas, é possível criar um grupo filtrado retornando uma linha para uso com IBM Cloud Application Performance Management.

Sobre Esta Tarefa

Um grupo de atributos filtrado tem as mesmas colunas que o grupo de atributos de origem, mas pode excluir algumas das linhas. Ele usa uma fórmula de seleção para determinar quais linhas incluir.

Para fornecer informações de resumo e status para o Cloud APM, você precisa usar um conjunto de dados que retorne uma única linha. Para obter detalhes, consulte “Preparando o agente para Cloud APM” na página 1377. Se as informações de origem estiverem em um conjunto de dados que retorna várias linhas, você poderá criar um grupo de atributos filtrado que retorna uma única linha.

Por exemplo, o processo, o serviço do Windows e as origens de dados do código de retorno do comando fornecem informações como linhas no conjunto de dados de Disponibilidade único. É possível criar um grupo de atributos filtrado, usando o campo NOME na fórmula de seleção. O grupo inclui o status para o aplicativo necessário. Defina-o como retornando uma linha. Então é possível usar esse grupo de atributos como o conjunto de dados de resumo para Cloud APM.

Um grupo de atributos filtrado também é útil quando uma consulta de origem de dados base retorna dados que você prefere dividir em grupos separados. Os exemplos dessas origens de dados são Windows Performance Monitor, SNMP e WMI.

Por exemplo, presuma que uma origem de dados possa retornar os dados a seguir:

```
Nome Tipo Tam. Usado Livre
Memória MEM  8  4  4
Disk1 DISK 300 200 100
Disk2 DISK 500 100 400
```

Essa é uma tabela que relata sobre o armazenamento que existe no sistema e inclui memória e espaço em disco. Você pode preferir dividir a tabela em memória e disco como tabelas separadas. É possível dividir a tabela criando dois grupos de atributos base. Cada um desses grupos de atributos base coleta os mesmos dados e filtros das linhas que você não deseja. Entretanto, essa não é a forma mais eficiente de fazer as coisas. Em vez disso, você define um grupo de atributos de base que retorna os dados de uso de memória e disco juntos. Em seguida, defina dois grupos de atributos filtrados. Cada um deles usa a mesma tabela base que sua origem. Um inclui um filtro, em que `Type=="MEM"` e o outro inclui um filtro, em que `Type=="DISK"`.

No exemplo, para o grupo de atributos filtrado em que `Type=="MEM"`, os dados retornados são:

```
Nome Tipo Tam. Usado Livre
Memória MEM  8  4  4
```

e em que `Type=="DISK"`, os dados retornados são:

```
Nome Tipo Tam. Usado Livre
Disk1 DISK 300 200 100
Disk2 DISK 500 100 400
```

Nota: Os grupos de atributos cujos dados são baseados em eventos não podem ser usados para criar grupos de atributos filtrados. Somente os grupos de atributos cujos dados são amostrados podem ser usados.

Procedimento

1. Clique em **Origens de dados existentes** na área **Monitorando Categorias de Dados** na página **Origem de Dados Iniciais do Agente** ou na página **Local da Origem de Dados**

   Nota:

   - Você chega à página **Origem de Dados Iniciais de Agente** usando o novo assistente de agente. Para obter mais informações, consulte “Criar um agente” na página 1169.
   - É possível chegar à página **Local da Origem de Dados** clicando com o botão direito do mouse em um agente na página **Definição de Origem de Dados** do **Agent Editor** e selecionando **Incluir Origem de Dados**.
2. Selecione **Filtrar linhas de dados de um grupo de atributos** na área **Origens de Dados**.
3. Clique em **Avançar**

   A página **Informações de Filtro** é exibida.
4. Selecione um **Grupo de Atributos de Origem** a partir da lista.
5. Insira uma **Fórmula de Seleção** para filtrar os dados do grupo de atributos selecionado.
   Por exemplo, na página **Informações de Filtro** que é mostrada, a fórmula de seleção filtra linhas de dados em que o atributo `Tipo` é igual a `"DISK"`. Linhas de dados cujo atributo `Tipo` não corresponde com `"DISK"` são descartadas. A fórmula de seleção que inserir deve avaliar para um resultado booleano, true ou false.

   Nota: Na página **Informações de Filtro**, é possível clicar em **Editar** para inserir ou modificar a fórmula usando o Editor de Fórmula. Para obter mais informações sobre o Editor de fórmula, consulte “Editor de Fórmula” na página 1201.
6. Clique em **Avançar**.
7. Selecione **Produz uma única linha de dados** ou **Pode produzir mais de uma linha de dados**.
   a) Se você selecionou **Pode produzir mais de uma linha de dados**, selecione um atributo-chave ou atributos a partir da lista.
8. Clique em **Concluir**.

Criando um Grupo de Navegadores

Em um ambiente do IBM Tivoli Monitoring, use grupos Navegadores para agrupar várias origens de dados relacionadas (grupos de atributos), de modo que possam ser criadas áreas de trabalho que mostrem visualizações que combinem as origens de dados. É possível criar um grupo navegador enquanto você cria um agente usando o assistente Novo agente no nível do agente base. Também é possível criar um grupo navegador enquanto você define um subnó usando o assistente Novo componente do agente.

Sobre Esta Tarefa

Por exemplo, você pode coletar dados do sistema de arquivos de mais de uma origem de dados. Pode ser útil criar uma área de trabalho que mostre visualizações de todos os dados do sistema de arquivos a partir de diferentes origens de dados.

Os grupos Navegadores também são uma boa maneira de ocultar origens de dados no Tivoli Enterprise Portal. Você pode decidir que métricas coletadas de duas origens de dados são mais úteis se as origens de dados forem associadas para criar uma nova origem de dados combinada. Você deseja ver somente os dados combinados na origem de dados Juntada. Você pode criar um grupo de navegadores que contenha todas as três origens de dados e criar uma área de trabalho que contenha visualizações para exibir somente a origem de dados combinada. As duas origens de dados originais ficam efetivamente ocultas na visualização no Tivoli Enterprise Portal. Consulte “Criando conjuntos de dados a partir de origens existentes” na página 1339 para obter informações sobre juntar origens de dados.

Nota: Quando você agrupar as origens de dados em um grupo de navegador, o Tivoli Monitoring não associará uma consulta ao grupo de navegador. Presume-se que você tenha definido uma área de trabalho padrão para o grupo de navegadores para exibir as origens de dados em um formato útil.

Um grupo de navegadores pode ser definido no agente base ou em um subnó. Um grupo de navegadores não pode conter outro grupo de Navegadores.

Os grupos Navegadores não têm efeito em um ambiente IBM Cloud Application Performance Management.

Procedimento

1. Execute uma das seguintes etapas:
   - Ao criar um novo agente usando o assistente de **Agente**, na página **Origem de Dados Inicial do Agente**, clique em **Agrupamentos de origens de dados** na área **Categorias de Dados de Monitoramento**.
   - Com um agente existente, execute as seguintes etapas no Agent Editor:
     a. Clique na guia **Origens de Dados** para abrir a página **Definição de Origem de Dados**.
     b. Selecione o agente e clique em **Incluir em selecionado**.
     c. Na página **Localização da Origem de Dados**, na área **Categorias de Dados de Monitoramento**, clique em **Agrupamentos de origem de dados**.
2. Na área **Origens de Dados**, clique em **Um Grupo de Navegadores**.
3. Clique em **Avançar**.
4. Na página **Informações do Grupo Navegador**, digite o nome do grupo navegador e o texto para a Ajuda que deseja associar ao nome e clique em **Avançar**.

   Nota: O Agent Builder automaticamente cria grupos navegadores em determinadas situações. O seguinte nome do grupo de navegadores é reservado:

   - Disponibilidade

   .
5. Na página **Primeira Origem de Dados do Grupo Navegador**, selecione a primeira origem de dados de monitoramento para o novo grupo de navegadores. Clique em uma categoria na lista **Categorias de**

Dados de Monitoramento e em uma origem de dados na lista **Origens de Dados**. Em seguida, clique em **Avançar**.

Dica: É possível criar a origem de dados como de costume. Como alternativa, clique em **Origens de Dados Existentes** e escolha para mover uma ou mais origens de dados que já foram criadas no grupo de navegadores.

6. Se você deseja criar uma origem de dados em um grupo navegador, na página **Definição de Origem de Dados**, selecione o grupo navegador e clique em **Incluir em Selecionado**.
7. Se desejar mover origens de dados existentes para o grupo navegador, na página **Definição de Origem de Dados**, selecione o grupo navegador e clique em **Incluir em Selecionados** e, na página **Origem de Dados do Grupo Navegador**, selecione **Origens de Dados Existentes**. Na página **Origens de Dados Atualmente Definidas**, selecione as origens de dados.
8. Se deseja remover uma origem de dados de um grupo navegador, execute uma das etapas a seguir na página **Definição de Origem de Dados**:
   - Selecione a origem de dados e arraste-a para a raiz da árvore de origens de dados.
   - Selecione a origem de dados e clique em **Remover**.
9. Se você desejar criar um grupo de navegadores, execute uma das seguintes etapas na página **Definição de Origem de Dados**:
   - Clique em **Incluir no Agente**.
   - Selecione um subnó e clique em **Incluir em Selecionados**.

Usando subnós

É possível usar subnós para monitorar vários componentes de aplicativo a partir de uma instância de agente única.

Você pode construir um único agente que realize as seguintes tarefas utilizando subnós:

- Monitora cada instância de um servidor de software que está sendo executado em um sistema em vez de fazer com que use instâncias separadas do agente, um por cada instância do servidor de software.
- Monitora vários sistemas remotos diferentes em vez de precisar utilizar instâncias separadas do agente, uma para cada sistema remoto.
- Monitora vários tipos diferentes de recursos a partir de um agente em vez de precisar construir e implementar vários agentes diferentes.
- No IBM Tivoli Monitoring, é exibido um nível adicional na árvore de Navegação física do Tivoli Enterprise Portal que permite agrupamento e customização adicionais. Além disso, é possível definir Grupos de Sistemas Gerenciados para um outro nível de granularidade com situações.
- No IBM Cloud Application Performance Management, fornece vários recursos diferentes, exibindo diferentes painéis de resumo e detalhes. Os recursos do subnó podem ser exibidos como peers ou subcomponentes do recurso do agente. É possível incluir esses recursos em aplicativos independentemente.

É possível criar tipos de subnó no Agent Builder. Cada tipo deve corresponder a um tipo diferente de recurso que um agente pode monitorar. Inclua origens de dados e conjuntos de dados no tipo de subnó para um determinado recurso monitorado.

Quando você implementa o agente em um host monitorado e o configura, é possível criar uma ou mais instâncias de cada tipo de subnó. Cada instância de um subnó deve corresponder a uma instância de um servidor, um sistema remoto ou qualquer recurso que o tipo de subnó foi projetado para monitorar. Todas as instâncias do subnó de um único tipo de subnó possuem grupos de atributos e áreas de trabalho que possuem um formato idêntico. Entretanto, cada instância de subnó tem dados provenientes do recurso específico que está sendo monitorado.

Ao configurar o agente no host monitorado, é possível determinar o número de instâncias de subnó. Alguns dados de configuração podem aplicar-se ao agente como um todo, mas outros dados de configuração se aplicam a uma instância de subnó única. Configure cada instância do subnó de maneira

diferente das outras instâncias do subnó para que elas não monitorem o mesmo recurso exato e exibam exatamente os mesmos dados.

Em um ambiente do IBM Tivoli Monitoring, uma instância de subnó é exibida dentro do agente na visualização Navegação Física no Tivoli Enterprise Portal. As áreas de trabalho exibem os dados que são produzidos por uma instância do subnó e as situações podem ser distribuídas para uma ou mais instâncias de um subnó. É automaticamente criada uma lista de sistemas gerenciados que contém todas as instâncias do subnó, da mesma forma que a Lista de Sistemas Gerenciados criada para um agente.

Em um ambiente do IBM Cloud Application Performance Management, é possível exibir instâncias de agente e subnó como recursos monitorados. Cada instância do subnó se torna um recurso separado. Para obter detalhes, consulte “Subnós no IBM Cloud Application Performance Management” na página 1353.

Como os agentes construídos com o Agent Builder criam instâncias de subnó com base nos valores de configuração, esses subnós possuem o mesmo tempo de vida que o agente. Ainda existe somente uma pulsação pronta para o agente, não uma pulsação separada para cada subnó. Portanto, usando subnós é possível aumentar significativamente a escala potencial do ambiente de monitoramento. A alternativa é usar diversas instâncias de agente, que podem limitar a escala potencial do ambiente IBM Tivoli Monitoring ou IBM Cloud Application Performance Management.

Incluir ou remover um subnó requer a reconfiguração do agente. Para reconfigurar o agente, é necessário parar e reiniciá-lo, envolvendo todos os subnós. É possível definir o agente como um agente de várias instâncias; nesse caso, é possível iniciar e parar uma única instância, e deixar as outras instâncias em execução.

Junto a conjuntos de dados em subnós, um agente pode definir conjuntos de dados de nível de agente que estão localizados fora de um subnó.

Na árvore do Tivoli Enterprise Portal Navigator, um tipo de subnó é exibido sob o nome do agente e instâncias do subnó são exibidas em um tipo de subnó. Os subnós são identificados por um Managed System Name (MSN) assim como os agentes, por exemplo, `94:Hill.cmn`.

Por exemplo, na árvore do Navegador em Figura 50 na página 1349, **Cuidando de Nossos Amigos** há um agente com três recursos (**Pensionistas**, **Áreas Comuns**e **Execuções do Kennel**) e dois tipos de subnó (**Área Comum** e **Execução do Kennel**). Dois desses recursos têm tipos de subnós que são definidos para eles (**Área Comum** e **Execução do Kennel**). Um subnó não é necessário para o terceiro recurso (**Pensionista**), que é representado por uma única linha em uma tabela no nível do agente base. O tipo de subnó Área Comum possui três instâncias de subnó: `94:Hill:cmn`, `94:Meadow:cmn` e `94:Tree:cmn` que representam três áreas comuns no kennel. O tipo de subnó Execução de Kennel possui quatro instâncias de subnó: `94:system1:run`, `94:system2:run`, `94:system4:run` e `94:system5:run` que representam quatro execuções de kennel.

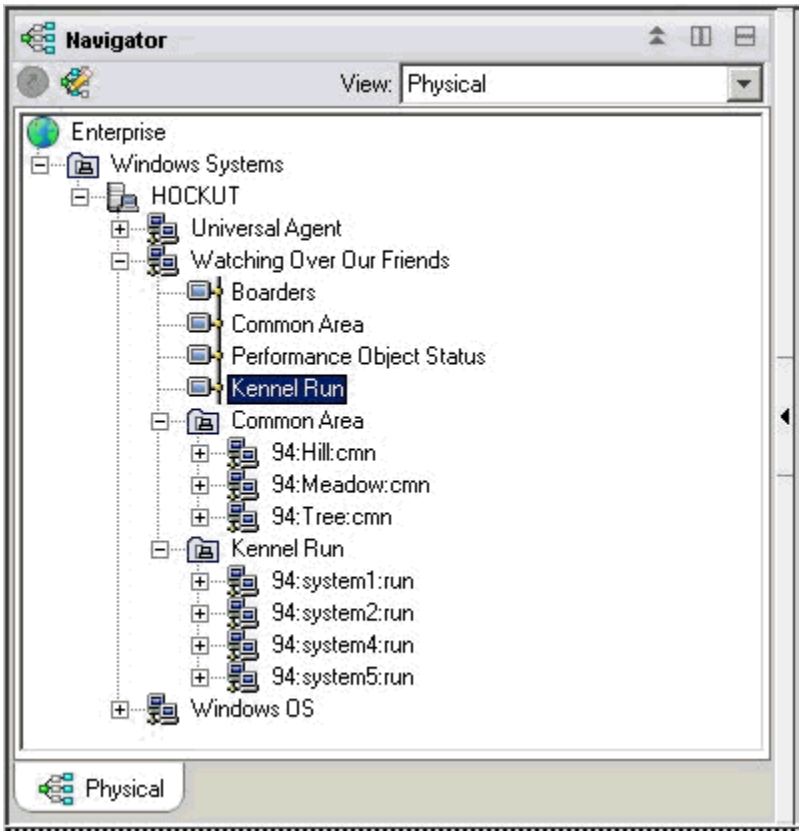


Figura 50. Subnós na árvore do Navegador

Existem duas maneiras nas quais um único agente pode utilizar subnós:

- O agente pode ter diferentes subnós do mesmo tipo.
- O agente pode ter subnós de diferentes tipos.

Subnós para os mesmos dados a partir de diferentes fontes

É possível usar subnós do mesmo tipo para representar várias instâncias de um tipo de recurso monitorado. Cada subnó do mesmo tipo inclui os mesmos grupos de atributos e os valores corretos para a instância de recurso monitorada específica. O número de subnós varia com base na configuração do agente. O exemplo na Figura 51 na página 1350 mostra o monitoramento de sistemas diferentes.

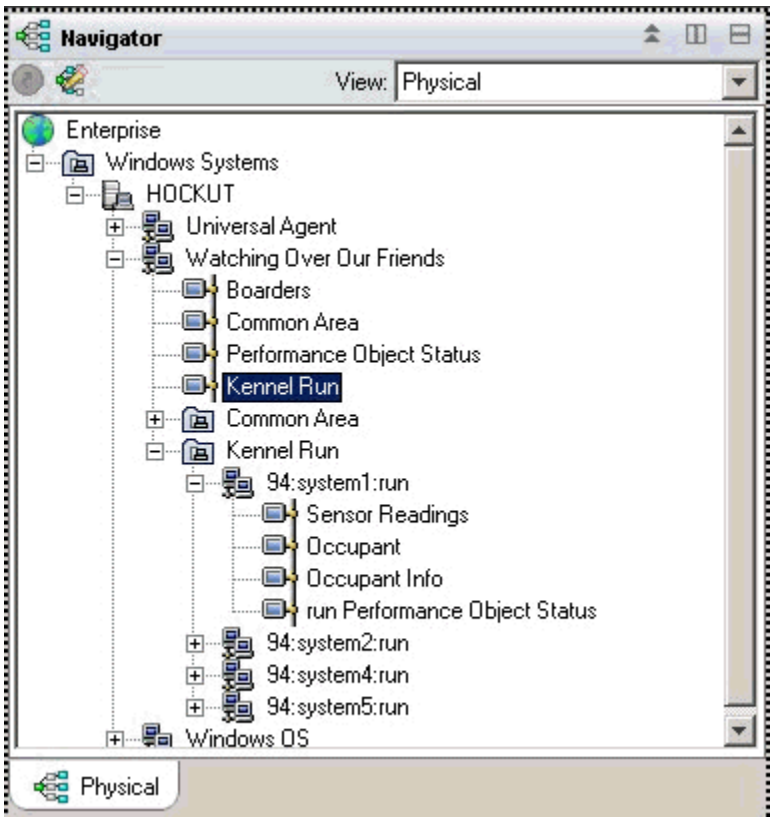


Figura 51. Subnós Monitorando Diferentes Sistemas

Subnós para vários tipos de dados

Quando um agente monitora vários tipos de recursos monitorados, é possível criar um tipo de subnó para cada um dos tipos de recurso. Cada subnó inclui as informações definidas nesse tipo de subnó. O exemplo a seguir mostra dois tipos de subnós. Cada tipo está monitorando um tipo de recurso diferente, com diferentes tipos de dados disponíveis para cada recurso:

- Área Comum
- Execução do Kennel

O agente em Figura 52 na página 1351 executa uma cópia de cada tipo de subnó. Um agente específico pode criar qualquer subconjunto dos agentes definidos. Os subnós podem ser usados para imitar os perfis do Tivoli Monitoring V5.

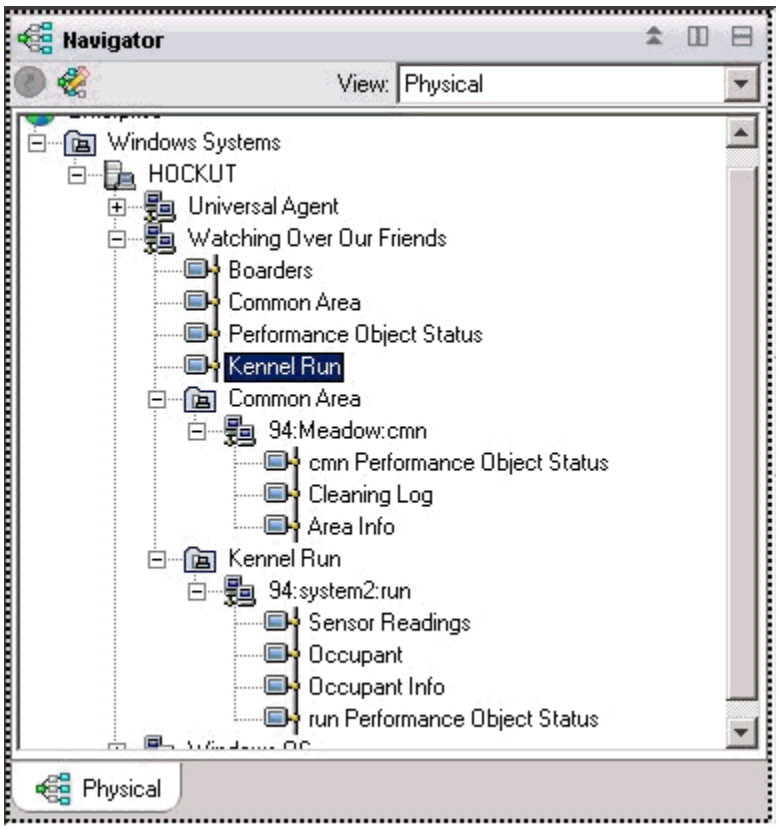


Figura 52. Tipos de Subnós na Árvore do Navegador

Ambas as maneiras de usar os subnós podem ser usadas no mesmo agente, em que cada tipo pode ter mais de uma instância de subnó.

O Figura 52 na página 1351 mostra dois tipos de subnós que monitoram dois tipos de recursos: Áreas Comuns e Execuções de Kennel. Além disso, existem vários subnós definidos para cada tipo. Há três subnós do tipo Área Comum; esses subnós possuem os seguintes IDs: Meadow, Hill e Tree. Também existem quatro subnós de tipo Kennel (cada um coletando dados a partir de um sistema diferente dedicado a uma Execução Kennel); esses subnós possuem os seguintes IDs: system1, system2, system4 e system5.

Nota: Os primeiros 24 caracteres dos IDs do subnó devem ser exclusivos para todas as instâncias do tipo de subnó na instalação do IBM Tivoli Monitoring.

Provedores de Dados em Subnós

Um subnó pode conter qualquer combinação de dados dos diferentes tipos de provedores de dados. A maioria dos provedores de dados atuais do Agent Builder podem ser utilizados em um subnó, incluindo os seguintes provedores de dados:

- WMI
- Perfmon
- Log de Eventos do Windows
- SNMP
- Eventos do SNMP
- JMX
- Ping ICMP
- Script

- Registro
- CIM
- JDBC
- HTTP
- SOAP
- Soquete
- API Java

Um subnó pode conter também um grupo de atributos unidos que combina dados de dois outros grupos de atributos no mesmo subnó ou nos grupos de atributos no nível do agente.

Status de Subnós

Existem duas maneiras de determinar o status para um agente do subnó. A primeira maneira é consultar os dados exibidos no grupo de atributos de Status do Objeto de Desempenho. Este grupo de atributos exibe o status para cada um dos outros grupos de atributos no mesmo nível no agente. O grupo de atributos Status do Objeto de Desempenho no nível de agente exibe o status de coleta para outros grupos de atributos no nível de agente. O grupo de atributos Status do Objeto de Desempenho em cada subnó exibe o status de coleta para os grupos de atributo nesse subnó.

O Agent Builder também cria um grupo de atributos para cada tipo de subnó, que exibe uma linha para cada subnó configurado desse tipo. No exemplo em (Figura 53 na página 1352), quatro subnós estão em execução para coletar dados.

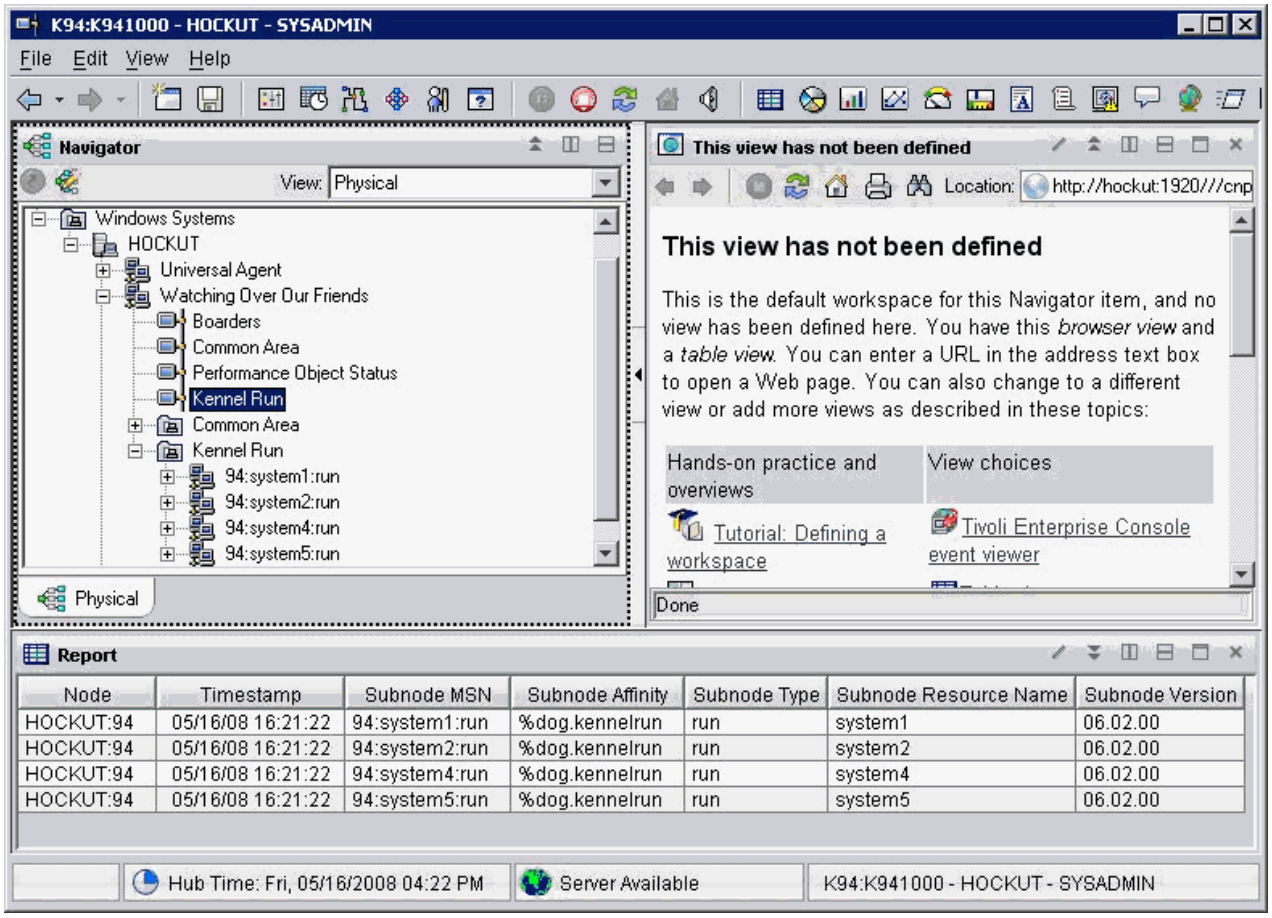


Figura 53. Monitorando instâncias de vários subnós do mesmo tipo de subnó

No ambiente do IBM Tivoli Monitoring, o subnó **Status do Objeto de Desempenho** contém dados visíveis na árvore do Navegador e pode ter situações que monitoram o status das outras coletas de dados.

No ambiente do IBM Cloud Application Performance Management, é possível criar limites para monitorar os dados de **Status do Objeto de Desempenho**.

O exemplo em Figura 54 na página 1353 mostra um caso em que a coleta de dados falhou (o comando script shell não foi localizado). Geralmente, qualquer valor diferente de NO_ERROR indica que há um problema. Para cada um dos coletores de dados definidos no subnó, há uma linha na tabela.

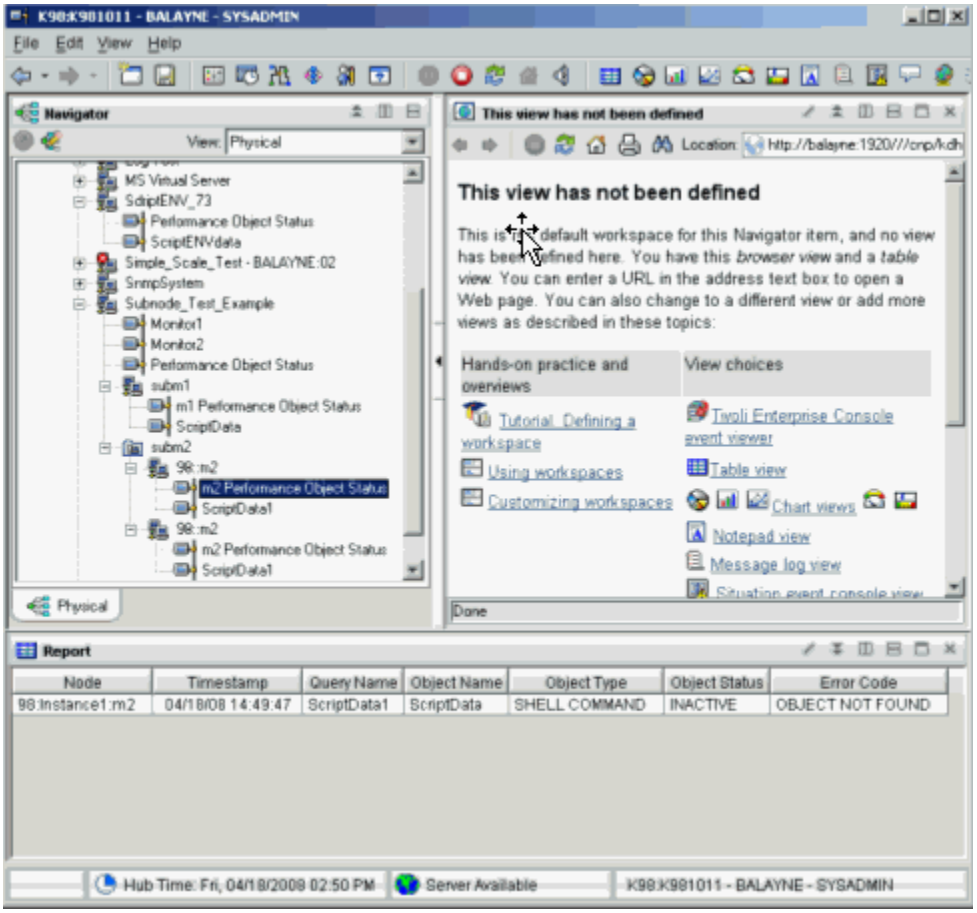


Figura 54. Exemplo: Coleta de Dados em um Subnó

Subnós no IBM Cloud Application Performance Management

No IBM Cloud Application Performance Management, é possível definir a instância do agente, ou uma instância do subnó ou ambas como recursos monitorados, e cada recurso corresponde a um painel de resumo.

Os painéis de subnó não podem exibir dados no nível do agente. Para exibir dados de nível de agente nesse ambiente, defina um painel de resumo para o agente.

Dependendo das configurações que você selecionar, os recursos do agente e do subnó poderão aparecer no mesmo nível, sem distinção hierárquica, ou recursos do subnó poderão ser listados como filhos para recursos do agente.

Para obter instruções sobre como configurar recursos de agente e subnó, consulte “Preparando o agente para Cloud APM” na página 1377.

Criando Subnós

É possível criar um subnó ao criar ou editar um agente.

Procedimento

1. Execute uma das seguintes etapas:
   - Ao criar um novo agente usando o assistente de **Agente**, na página **Origem de Dados Inicial do Agente**, clique em **Agrupamentos de origens de dados** na área **Categorias de Dados de Monitoramento**.
   - Com um agente existente, execute as seguintes etapas no Agent Editor:
     a. Clique na guia **Origens de Dados** para abrir a página **Definição de Origem de Dados**.
     b. Selecione o agente e clique em **Incluir em selecionado**.
     c. Na página **Localização da Origem de Dados**, na área **Categorias de Dados de Monitoramento**, clique em **Agrupamentos de origem de dados**.
2. Na área **Origens de Dados**, clique em **Uma Definição do Subnó**
3. Clique em **Avançar**.
4. Preencha a página **Informações do Subnó** da forma a seguir para definir o novo subnó:
   a) No campo **Nome**, digite o nome do subnó que está sendo criado.
   b) No campo **Tipo**, digite 1 a 3 caracteres (usando número, letras ou ambos) para identificar o tipo do subnó que você está criando.
   c) No campo **Descrição**, digite uma descrição para o subnó que está sendo criado.
   d) Clique na caixa de seleção **Mostrar grupo de atributos de nós para este tipo de subnó** para ocultar ou exibir o grupo de atributos de disponibilidade. Para obter mais detalhes sobre esse grupo de atributos, consulte "Nó de Disponibilidade" na página 1419.
   e) Clique em **Avançar**.
5. Conclua a página **Origem de Dados do Subnó Inicial** para selecionar uma origem de dados como o primeiro item no novo subnó. Clique em uma categoria na lista **Categorias de Dados de Monitoramento** e em uma origem de dados na lista **Origens de Dados**. Em seguida, clique em **Avançar**.

   Dica: É possível criar a origem de dados como de costume. Como alternativa, você pode mover uma ou mais origens de dados que já foram criadas para o grupo de navegadores. Para mover origens de dados, clique em **Origens de Dados Existentes** e, na página **Origens de Dados Definidas Atualmente**, selecione as origens de dados.

   Importante: Não é possível incluir origens de dados de processo, de serviço do Windows ou de código de retorno de comando em um subnó. Como uma solução alternativa, é possível gravar um script que determine as informações de processo ou de serviço necessárias e usar uma origem de dados de saída do script.
6. Se o seu agente contiver propriedades de configuração customizadas ou se a origem de dados selecionada precisar de configuração, use a página **Substituições de Configuração de Subnó** para escolher as propriedades de configuração.

   Na janela **Substituições da Configuração do Subnó**, escolha as propriedades de configuração que deseja para o subnó no nível do agente. Em seguida, escolha as propriedades de configuração que deseja variar para cada subnó.

   Utilize **Mover**, **Copiar** e **Remover** para especificar as propriedades de configuração conforme descrito em "Configurando um Subnó" na página 1355.
7. Clique em **Avançar**.
   A página **Definição de Origem de Dados** é exibida.

Configuração do subnó

Quando um tipo de subnó é definido, uma única seção de configuração é definida especificamente para esse subnó.

Existem várias maneiras nas quais uma seção de configuração do subnó é diferente de outras seções de configuração:

- O conjunto de propriedades em uma seção do subnó pode ser duplicado, portanto, existem vários conjuntos de propriedades. Cada conjunto de propriedades forma sua própria seção. O layout de todas as seções é idêntico, mas podem ser digitados valores diferentes em cada seção.

  Em contraste, as propriedades em outras seções (que são referidas como seções em nível do agente) são mostradas somente uma vez durante a configuração de tempo de execução. Elas não foram subseções e não podem ser duplicadas ou removidas.

  Consulte "Exemplo de configuração de subnó" na página 1358 para obter exemplos da GUI e da linha de comandos de configuração de subnós.
- Para cada cópia de uma seção do subnó criada na configuração de tempo de execução, o agente cria uma instância do subnó separada. Todas essas instâncias do subnó são do mesmo tipo.
- Os nomes das propriedades em seções do subnó podem ser duplicatas de nomes das propriedades em seções em nível do agente. Quando isto ocorre, o valor da propriedade do subnó substitui o valor da propriedade em nível do agente.
- No IBM Tivoli Monitoring V6.2.1 e posterior, um seção do subnó pode ter os valores da propriedade padrão que se aplicam a todas as instâncias de subnós desse tipo. Isto permite ter uma consulta de três níveis de um único valor da propriedade, conforme a seguir:
  1. O agente obtém o valor da propriedade da subseção da instância do subnó.
  2. Se nenhum valor estiver configurado no nível da instância do subnó, o valor da propriedade será obtido do nível padrão do subnó.
  3. Se nenhum valor estiver configurado em nenhum destes dois níveis, o valor da propriedade será obtido de uma seção em nível do agente.

Consulte "Exemplo de configuração de subnó" na página 1358 para obter exemplos da GUI e da linha de comandos de configuração de subnós.

Configurando um Subnó
Use a página **Substituições de Configuração de Subnó** para configurar uma origem de dados de subnó.

Antes de Iniciar

Utilize as etapas do "Criando Subnós" na página 1353 para criar um subnó.

Sobre Esta Tarefa

Quando você incluir uma origem de dados para um subnó, a página **Substituições de Configuração do Subnó** será apresentada se a origem de dados requerer configuração. Ela mostra as propriedades de configuração customizadas e quaisquer outras propriedades de configuração que são aplicáveis ao tipo de subnó.

Procedimento

- Na janela **Substituições da Configuração do Subnó**, escolha as propriedades de configuração que deseja para o subnó no nível do agente. Em seguida, escolha as propriedades de configuração que deseja variar para cada subnó.
- Use **Copiar >>** para copiar propriedades de configuração para que elas possam ficar no nível do agente e no nível do subnó.

  O agente procura um valor primeiro no nível do subnó e, se não localizar um valor, ele procurará no nível do agente. Se uma propriedade em ambos os níveis for uma propriedade necessária, ela será necessária somente no nível do agente, é opcional no nível do subnó.
- Utilize **Mover >>** para mover propriedades do nível do agente para o nível do subnó. **Mover>>** não está disponível para propriedades requeridas por uma origem de dados de nível de agente ou por um subnó de um tipo diferente.
- Utilize **Remover** para remover uma das duas listas. As propriedades podem ser removidas somente se estiverem listadas no nível do agente e no nível de subnó. Esta função não pode ser utilizada para remover totalmente uma propriedade.

- Utilize **<< Copiar** para copiar uma propriedade do nível do subnó para o nível do agente.
- Utilize **<< Mover** para mover uma propriedade do subnó para o nível do agente.

O que Fazer Depois

É possível alterar a configuração para um subnó existente usando o Agent Editor.

Substituições de Configuração de Subnó
Utilize Substituições de Configuração do Subnó para substituir propriedades de configuração do agente por propriedades específicas do subnó.

O procedimento em "Configurando um Subnó" na página 1355 descreve como gerenciar a configuração de subnó para propriedades geradas automaticamente. O gerenciamento de propriedades de configuração customizada é semelhante. Qualquer propriedade de configuração customizada definida será exibida na janela **Substituições de Configuração de Subnó**.

Ao copiar ou mover uma propriedade customizada do nível de subnó para o nível de agente, a seção na qual colocar a propriedade é solicitada. Você pode selecionar uma seção customizada existente, ou digitar o nome de uma nova seção customizada.

Selecionando Propriedades de Configuração do Subnó

Sem subnós, todas as instâncias de um tipo de origem de dados compartilham os parâmetros de configuração. Por exemplo, todos os grupos de atributo SNMP se conectam ao mesmo host usando o mesmo nome de comunidade. Com subnós, cada instância de um subnó pode se conectar a um host diferente se a propriedade SNMP_HOST for colocada no nível de subnó.

Selecionar propriedades a serem substituídas no nível do subnó é uma consideração importante ao desenvolver um agente. Se muitas propriedades forem selecionadas, a seção de configuração do subnó ficará desorganizada e difícil de gerenciar. Se muito poucas propriedades forem selecionadas, as funções do agente podem ser limitadas quando alguém desejar modificar uma propriedade de um subnó para a próxima.

As propriedades a seguir não podem ser copiadas para o nível de subnó. (Todos os grupos de atributos em todos os subnós e no agente base devem usar a mesma versão SNMP e tipo de conexão JMX):

- Versão do SNMP
- Tipo de Conexão do Servidor JMX MBean
- Diretório inicial Java
- Nível de rastreio de Java
- argumentos da JVM
- Caminho de classe para arquivos JAR externos
- Número da porta de origem de dados do soquete
- Configurações do caminho da classe JMX ou JDBC

Configuração de Subnó Avançada
Use a configuração de subnó avançada para substituir uma propriedade de configuração do agente em um subnó.

Sobre Esta Tarefa

Existe uma opção em IBM Tivoli Monitoring V6.2.1 e agentes posteriores que você pode ativar para substituir as propriedades a partir de qualquer seção de configuração de nível de agente em uma instância de subnó. Na página **Substituições de Configuração de Subnó**, existe uma caixa de seleção rotulada **Permitir que qualquer propriedade de configuração seja substituída em qualquer subnó**. Para obter mais informações, consulte ("Substituições de Configuração de Subnó" na página 1356). Para esta opção ser ativada, você deve selecionar **6.2.1** como **Versão Mínima do ITM** ao nomear seu agente

(“Nomeando e configurando o agente” na página 1169). Se você escolher esta opção, cada instância do subnó poderá substituir qualquer propriedade a partir de qualquer seção de configuração em nível do agente. Mas esta propriedade pode ser substituída somente a partir da GUI e não a partir da linha de comandos **itmcmd**.

Procedimento

A opção **Permitir que qualquer propriedade de configuração seja substituída em qualquer subnó** faz com que um campo **Avançado** que contém uma lista seja exibido em cada painel de configuração do subnó. A seleção inicial no campo **Avançado** fornece as direções breves: **Selecione uma seção para substituir os valores**.

- Ao clicar na lista, você vê uma lista de todas as seções não subnó que contêm as propriedades de configuração.
- Selecione uma seção.

  As propriedades dessa seção são incluídas temporariamente no painel do subnó. O valor de qualquer propriedade que você altere é incluído ao conjunto de propriedades definidas para o subnó. Uma origem de dados em um subnó procura valores da propriedade no subnó antes de procurar nas seções no nível do agente. .

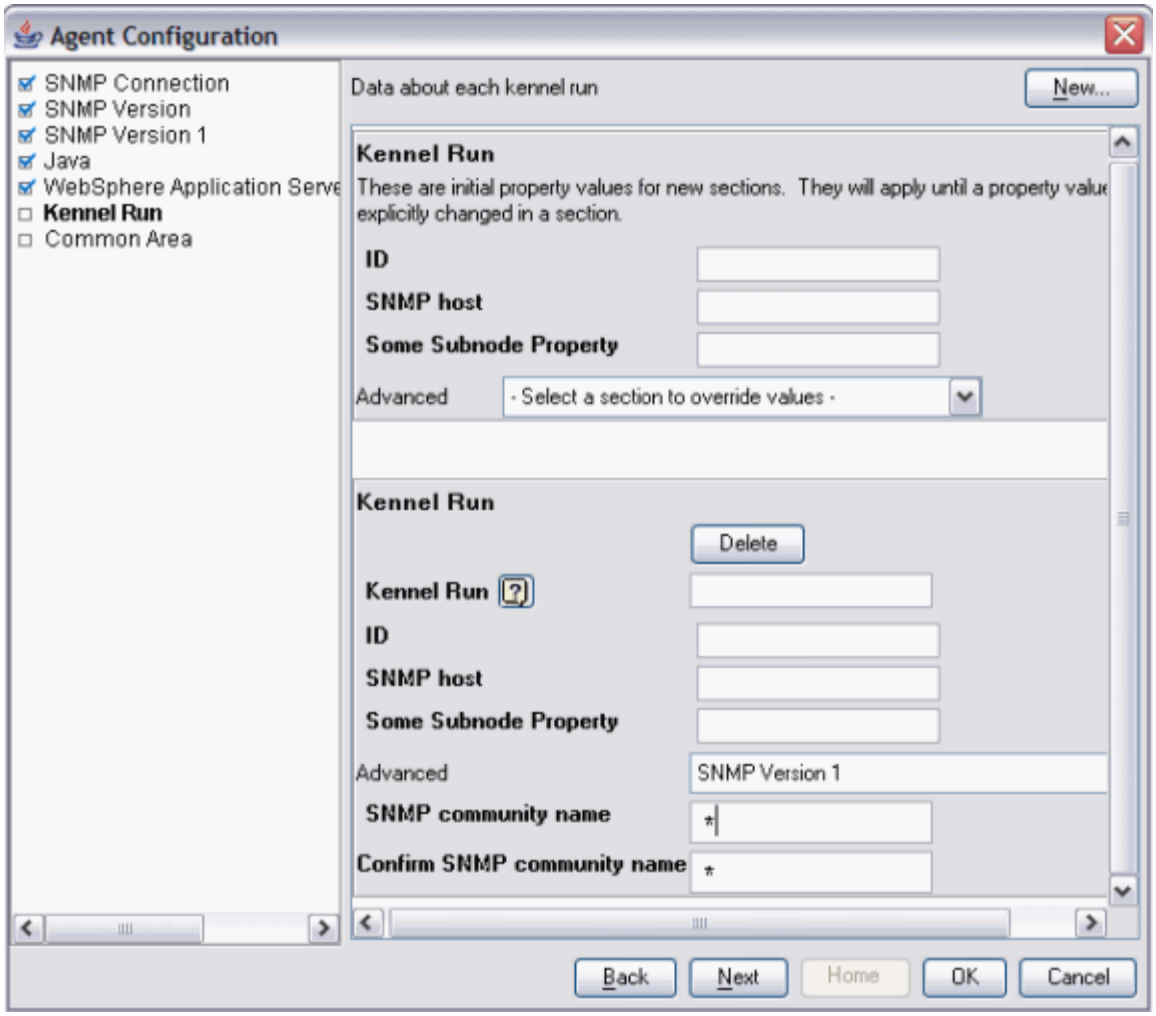


Figura 55. SNMP Versão 1 Propriedades expandidas

As seguintes informações adicionais se aplicam a propriedades de substituição das seções do nível do agente:

– As propriedades que foram copiadas para a seção do subnó não são mostradas quando a seção de nível do agente estiver selecionada na lista **Avançado**. Por exemplo, em Figura 55 na página 1357,

host SNMP não é exibido após a lista **Avançado** porque foi copiado nas propriedades do subnó e já é exibido.

- As seções que não contêm nenhuma propriedade de substituição não possuem uma seleção na lista **Avançada**.
- Valores substituídos que você insere em uma seção são retidos mesmo se você seleciona uma seção diferente para exibir propriedades diferentes.
- Selecione **Permitir que qualquer propriedade de configuração seja substituída em qualquer subnó** para ativar esse recurso em seu agente.

Configurando um Subnó a partir da Linha de Comandos
No ambiente IBM Tivoli Monitoring, também é possível configurar um subnó usando a linha de comandos.

Antes de Iniciar

Para obter informações adicionais sobre a configuração de subnó, consulte "Configuração do subnó" na página 1354

Sobre Esta Tarefa

Procedimento

- Para configurar uma instância de subnó a partir da linha de comandos, use o seguinte comando:

```
tacmd configureSystem -m HOSTNAME:00 -p
section_name:subnode_instance_id.property_name=value
```

Em que:

section_name
O mesmo que o tipo de subnó

subnode_instance_id
ID para o subnó definido durante a configuração.

property_name
Nome da propriedade de configuração

value
Valor da propriedade

Exemplo de configuração de subnó
Como configurar um agente de amostra com um subnó definido.

Por exemplo:

Este exemplo mostra como configurar um agente de amostra que possui um subnó denominado Subnó de Exemplo do tipo `exs` e as três propriedades de configuração a seguir:

- O `Agent Cfg` (nome da propriedade real é `K00_AGENT_CFG`) é definido somente no nível de agente.
- O `Subnode Cfg` (nome real da propriedade é `K00_SUBNODE_CFG`) é definido somente no subnó de exemplo
- `Overridable Cfg` (o nome real da propriedade é `K00_OVERRIDABLE_CFG`) é definido no nível do agente e foi copiado para o subnó de exemplo.

(Figura 56 na página 1359) mostra essas propriedades de configuração na página **Informações de Configuração de Tempo de Execução** do Agent Editor.

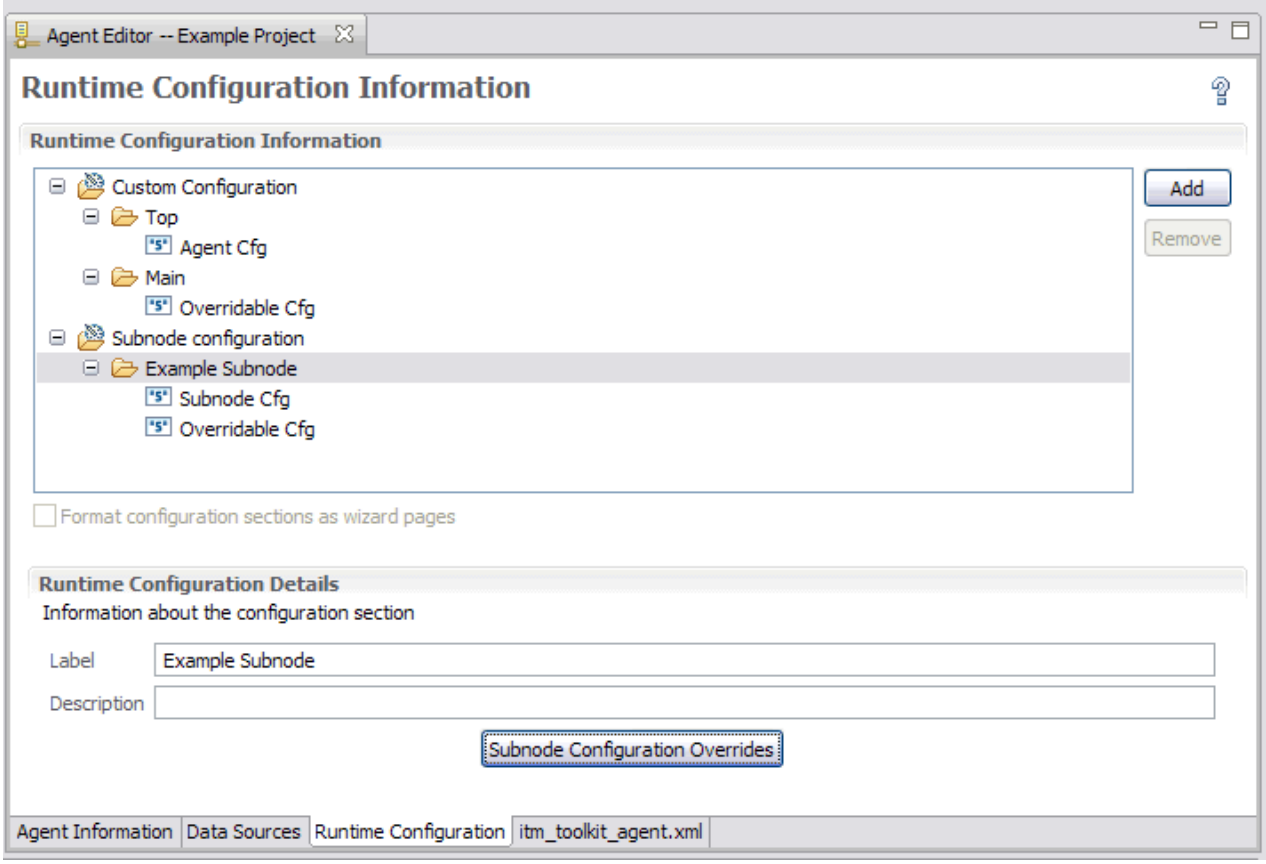


Figura 56. Definições de propriedade de configuração no Agent Builder

Ao configurar esse agente de exemplo, a primeira página que é exibida é a seção **Parte Superior**, que contém a propriedade **Cfg de Agente** conforme mostrado em (Figura 57 na página 1360). Como essa propriedade é uma propriedade de nível de agente, ela é mostrada uma vez durante a configuração do agente. Qualquer instância do Subnó de Exemplo pode ver esse valor de propriedade, mas todas as instâncias veem o mesmo valor.

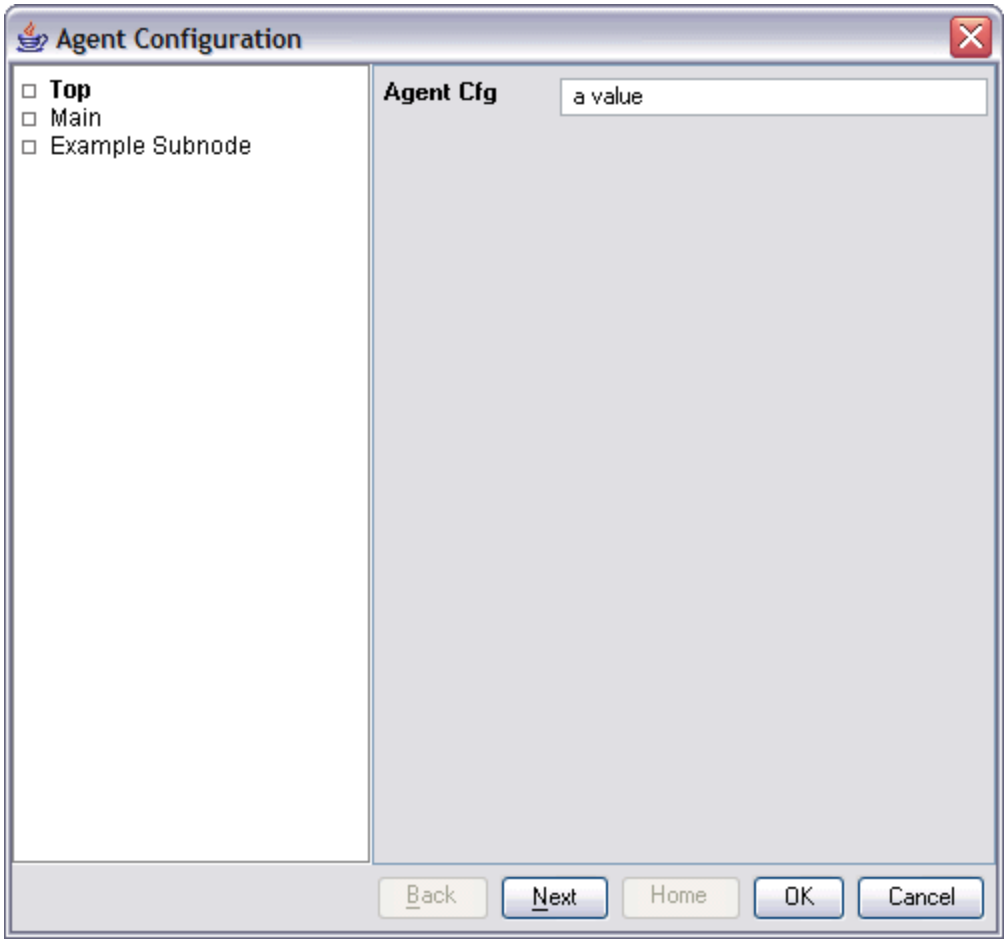


*Figura 57. Seção **Parte Superior** com configuração no nível de agente para a propriedade **Agent Cfg***

Se você estiver configurando a partir da linha de comandos Tivoli Enterprise Monitoring Server, a propriedade **Cfg de Agente** pode ser configurada usando o comando a seguir:

```
tacmd configureSystem -m HOSTNAME:00 -p "TOP.K00_AGENT_CFG=a value"
```

A próxima seção exibida é a seção **Principal**, conforme mostrado na Figura 58 na página 1361. Ela também é uma seção de nível de agente e contém a propriedade **Configuração Substituível** de nível de agente. Esta propriedade é diferente da propriedade **Agent Cfg** porque essa propriedade foi copiada do Subnó de Exemplo no Agent Builder. Isso significa que um valor padrão para a propriedade pode ser inserido na página **Principal**. No entanto, qualquer instância do Subnó de Exemplo pode substituir o valor inserido aqui por um valor diferente.

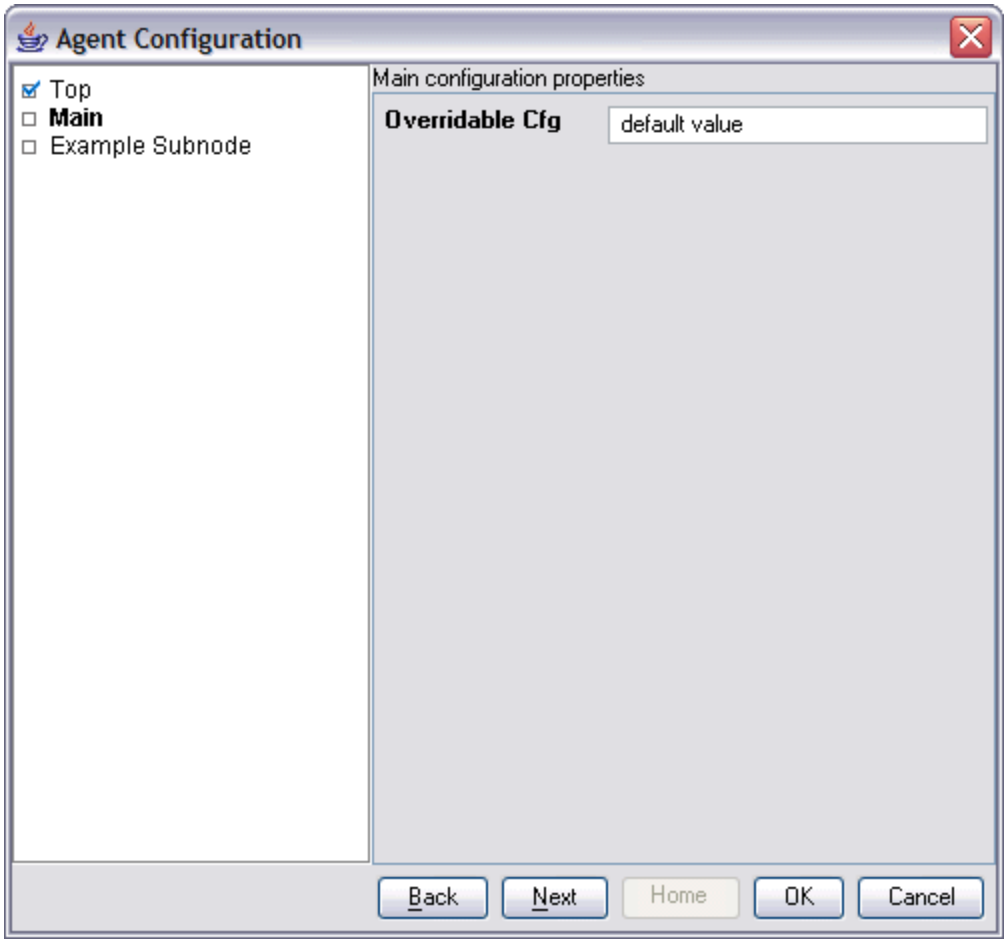


*Figura 58. Seção **Principal** com o valor-padrão do agente para a propriedade **Overridable Cfg***

Se você estiver configurando a partir da linha de comandos do Tivoli Enterprise Monitoring Server, essa propriedade pode ser configurada usando o comando a seguir:

```
tacmd configureSystem -m HOSTNAME:00 -p "MAIN.K00_OVERRIDABLE_CFG=default value"
```

Você pode colocar essas duas propriedades na mesma seção de nível do agente. Você pode decidir quantas seções de nível do agente customizadas serão criadas e como as propriedades customizadas serão distribuídas entre elas.

A próxima seção exibida é a seção **Subnó de Exemplo**, conforme mostrado na Figura 59 na página 1362. Como esse agente está sendo configurado pela primeira vez, não existem instâncias de subnó definidas e nenhuma subseção de instância de subnó é mostrada. A subseção de valores de propriedade inicial é mostrada, embora ela seja opcional e alguns tipos de subnós podem não mostrá-la. Como a subseção os valores da propriedade inicial são mostrados, os valores padrão podem ser inseridos para quaisquer propriedades de configuração. A propriedade **Overridable Cfg** já possui um valor padrão que foi obtido da propriedade de nível do agente do mesmo nome.

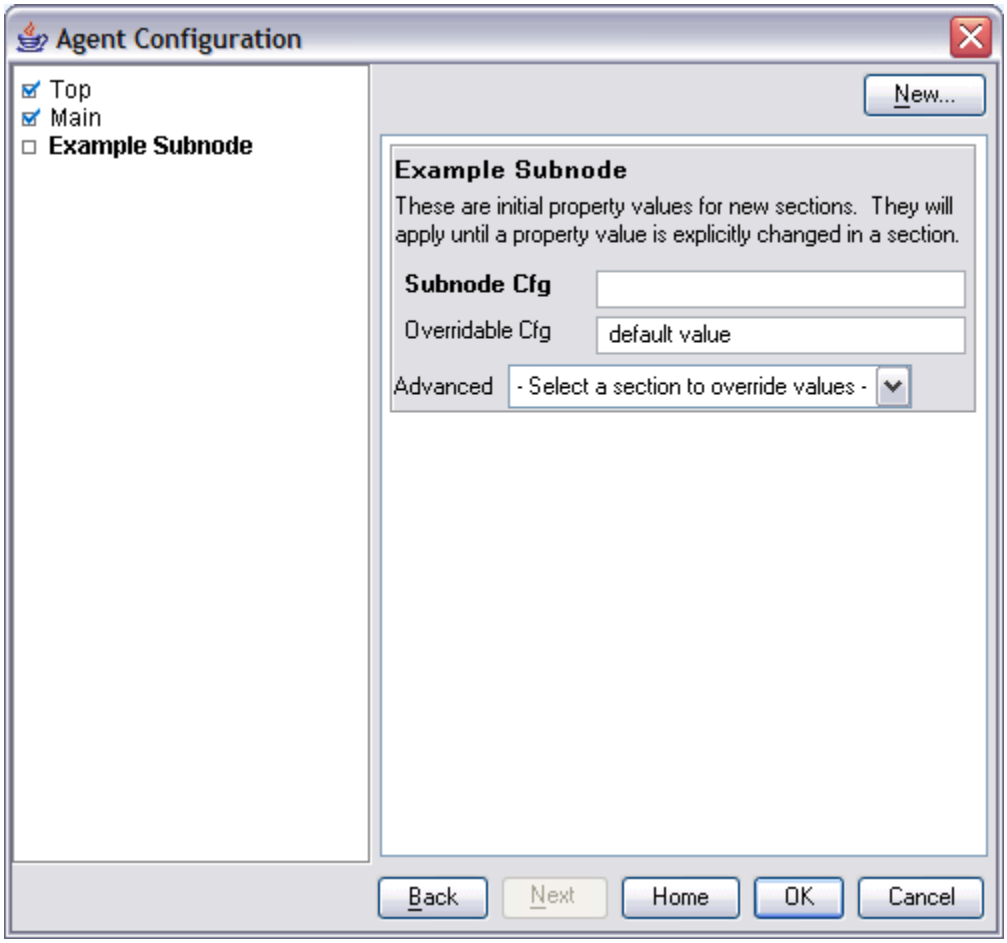


*Figura 59. Página de seção **Subnó de Exemplo** sem nenhum subnó*

As instâncias de subnó são definidas executando as ações a seguir na página da seção vazia **Subnó de Exemplo** (Figura 60 na página 1363):

1. Na seção **Subnó de Exemplo** inicial, no campo **Subnode Cfg.**, digite a seguinte sequência padrão para a propriedade: `valor sub-padrão`.
2. Clique em **Novo**. Uma subseção **Subnó de Exemplo** é exibida após a subseção de propriedades iniciais.
3. No campo **Subnó de Exemplo**, digite o seguinte ID da instância de subnó: do.
4. Clique em **Novo**. Uma segunda subseção **Subnó de Exemplo** é mostrada após a primeira.
5. No segundo campo **Subnó de Exemplo**, digite o seguinte ID da instância de subnó: `re`.
6. No campo **Subnode Cfg**, digite o valor a seguir para a propriedade **Subnode Cfg**: `sc override`.
7. No campo **Overridable Cfg**, digite o valor a seguir para a propriedade **Overridable Cfg**: `oc override`.

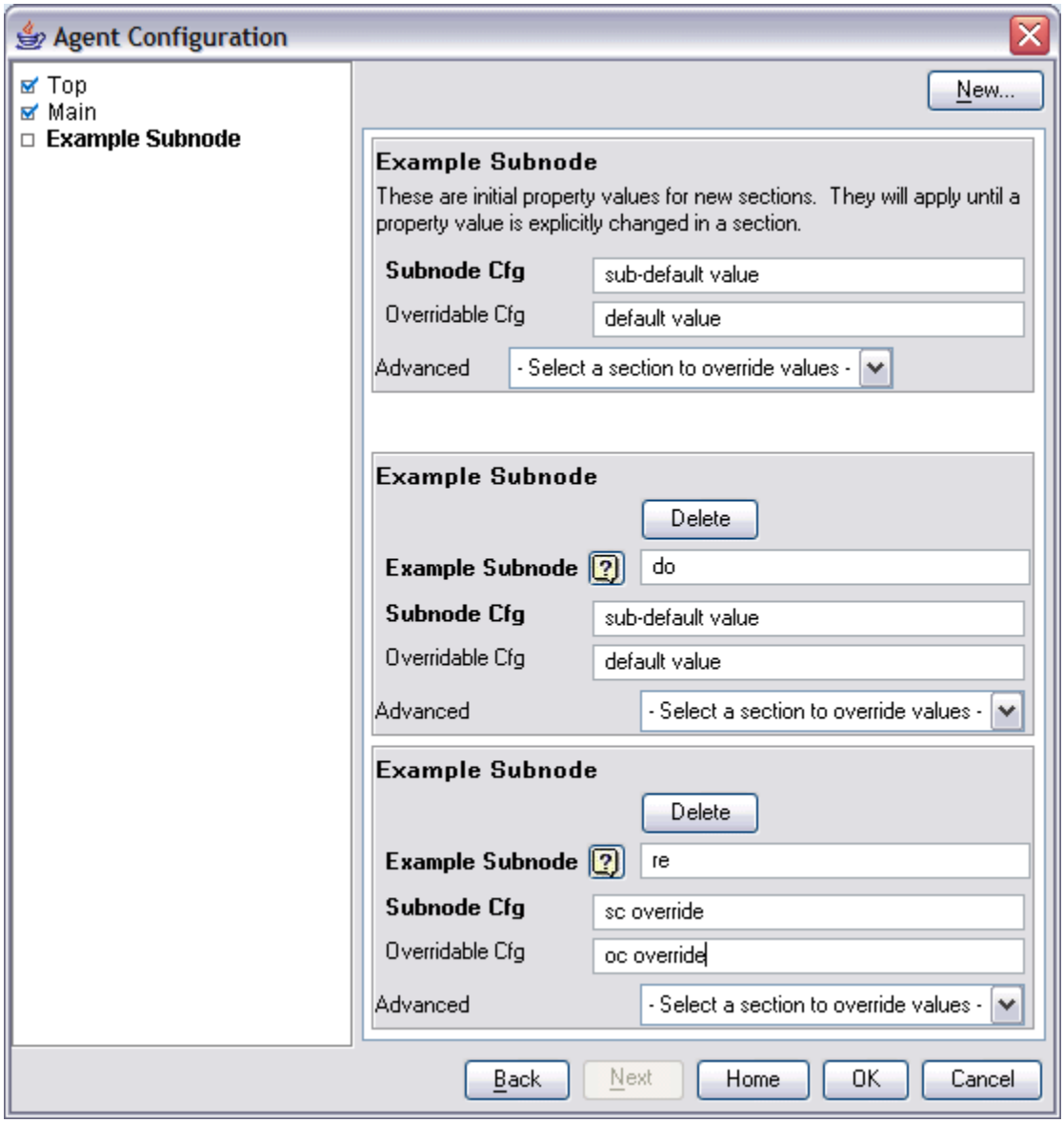


*Figura 60. Página da seção **Subnó de Exemplo** com duas instâncias de subnó definidas*

As duas novas subseções fazem com que o agente crie duas instâncias de subnó quando ele for iniciado. Como as propriedades da subseção do subnó **do** não foram alteradas, os valores da propriedade padrão são usados por essa instância de subnó. Como valores diferentes foram digitados para as propriedades na subseção **re**, a instância de subnó **re** usa esses valores que foram digitados.

Você pode configurar um valor-padrão a partir da linha de comandos do Tivoli Enterprise Monitoring Server com o seguinte comando:

```
tacmd configureSystem -m HOSTNAME:00 -p "exs.K00_SUBNODE_CFG=sub-default value"
```

O formato para configurar os valores padrão do subnó é exatamente igual ao formato para configurar as propriedades de nível do agente, exceto que o nome da seção identifica uma seção de subnó.

Você pode criar as instâncias de subnós a partir da linha de comandos do Tivoli Enterprise Monitoring Server com o seguinte comando:

```
tacmd configureSystem -m HOSTNAME:00 -p "exs:do.K00_OVERRIDABLE_CFG=default value" \
 "exs:re.K00_SUBNODE_CFG=sc override" "exs:re.K00_OVERRIDABLE_CFG=oc override"
```

O ID da instância de subnó é inserido entre o nome da seção e o nome da propriedade. Ao usar a linha de comandos para criar uma instância de subnó, pelo menos uma propriedade deve ser especificada,

mesmo se todas as propriedades usarem valores padrão. Caso contrário, os valores padrão não precisam ser especificados na linha de comandos ao definir as instâncias de subnó.

Todas as propriedades de configuração do agente podem ser configuradas com um único comando. O comando a seguir é equivalente a todos os comandos individuais anteriores:

```
tacmd configureSystem -m HOSTNAME:00 -p "TOP.K00_AGENT_CFG=a value" \
 "MAIN.K00_OVERRIDABLE_CFG=default value" \
 "exs.K00_SUBNODE_CFG=sub-default value" \
 "exs:do.K00_OVERRIDABLE_CFG=default value" \
 "exs:re.K00_SUBNODE_CFG=sc override" "exs:re.K00_OVERRIDABLE_CFG=oc override"
```

Subnós e Origens de Dados do Windows
Escolha incluir as propriedades de Conexão Remota do Windows no agente ou não.

Sobre Esta Tarefa

Se um agente tiver as origens de dados do Windows no nível de agente e não nos subnós, a inclusão das propriedades de configuração de Conexão Remota do Windows no agente será opcional. As origens de dados do Windows são Windows Event Log, Windows Management Instrumentation, Windows Performance Monitor. Se as propriedades de configuração não forem incluídas, essas origens de dados irão monitorar o sistema local do Windows, por padrão, e não vão precisar de configuração. Por padrão, nenhuma origem de dados do Windows é incluída em nenhum subnó.

Para escolher se as propriedades de Conexão Remota do Windows devem ser incluídas no agente, execute as etapas a seguir:

Procedimento

1. Na página **Informações de Windows Management Instrumentation (WMI)**, clique em **Opções Globais** ao exibir as propriedades da origem de dados. Selecione **Opções Globais**, enquanto você estiver criando a origem de dados ou a partir da página **Origens de Dados** do Agent Editor.
2. Na janela **Opções de Origens de Dados Globais do Windows**, selecione **Incluir Configuração do Windows Remote Connection**, se desejar incluir essas propriedades no agente.

Origens de Dados de Subnós e de Script
As propriedades de configuração da instância do subnó são acessadas em scripts do subnó da mesma forma que são acessadas em scripts em nível do agente.

Os scripts possuem acesso a todas as propriedades de configuração em nível do agente e a todas as propriedades de configuração da instância do subnó. Se uma propriedade em nível do agente for substituída no nível do subnó, o script terá acesso somente ao valor da propriedade no nível do subnó.

Customizando configuração do agente

Customizar a configuração do processo, arquivo de log e origens de dados de script

Antes de Iniciar

Se você estiver incluindo origens de dados SNMP, JMX, CIM, JDBC, HTTP e SOAP em seu agente, configure essas origens de dados conforme descrito nas seguintes seções:

- “Dados de monitoramento de um servidor do Protocolo Simples de Gerenciamento de Rede (SNMP)” na página 1229
- “Monitorando MBeans Java Management Extensions (JMX)” na página 1240
- “Monitorando dados a partir de um Common Information Model (CIM)” na página 1259
- “Dados de Monitoramento do Java Database Connectivity (JDBC)” na página 1286
- “Monitorando a Disponibilidade de HTTP e o Tempo de Resposta” na página 1297
- “Monitorando dados a partir de uma origem de dados SOAP ou HTTP” na página 1305

Sobre Esta Tarefa
Use esta tarefa para customizar a configuração do processo, arquivo de log e origens de dados de script para que um agente possa acessar o aplicativo que está monitorando.

Todos os agentes devem ser configurados antes que possam ser iniciados. Todos os agentes devem ter informações de configuração básica como o método de conectar ao Tivoli Enterprise Monitoring Server. Muitas vezes, um agente deve ter mais informações de configuração para que tenha acesso a informações específicas ao sistema no qual está em execução. Por exemplo, se você souber o local de instalação de um produto de software, inclua as propriedades de configuração para solicitar essas informações. Outro exemplo de informações que você pode solicitar é o ID do usuário e senha para acessar uma interface.

A configuração customizada é definida pelo desenvolvedor do agente. Ela não é necessária para todos os agentes, mas pode ser utilizada nas seguintes áreas de coleta de dados:

- Corresponder um argumento em um Monitor de Processos
- Corresponder a linha de comandos em um Monitor de Processos
- Formar um caminho ou nome do arquivo de log
- Definir uma variável de ambiente em um script

Nota: Determinadas origens de dados como JMX e SNMP incluem essa configuração automaticamente.

Nota: Quando uma configuração específica da origem de dados é incluída automaticamente pelo Agent Builder, ela é incluída somente em inglês.

Se durante a definição de origem de dados seu agente precisar de informações específicas do sistema para uma área de coleta de dados, **Inserir Propriedade** ou **Inserir Propriedade de Configuração** são mostrados.

Por exemplo, quando se cria um grupo de atributos que monitora um arquivo de log, é mostrado **Inserir Propriedade de Configuração**.

Procedimento

1. Clique em **Inserir Propriedade de Configuração** para exibir a janela **Propriedades de Configuração**,
2. Na janela **Propriedades de Configuração**, clique em uma propriedade e clique em **Incluir**.

   Nota: Inicialmente, não existem propriedades de configuração definidas para o agente.
3. Na janela **Propriedade de Configuração de Tempo de Execução**, preencha os campos a seguir:
   a) Na área **Seção**, preencha os seguintes campos:

      Etiqueta
      Texto que descreve as propriedades

      Descrição
      (opcional) Descrição das propriedades

   b) Na área **Propriedade**, preencha os seguintes campos:

      Etiqueta
      Texto que é exibido no painel de configuração do agente que identifica as informações que você deve inserir.

      Variável de ambiente
      A variável de ambiente é exibida no campo **Variável de Ambiente** e é atualizada conforme você digita no campo do rótulo. O Agent Builder automaticamente constrói o nome da variável de ambiente a partir do código do produto e do rótulo. Se desejar alterar a variável de ambiente independentemente do rótulo, é possível limpar **Corresponder Rótulo**.

      Descrição
      (opcional) Descrição da propriedade que está sendo definida.

      Type
      Tipo de informações coletadas, uma das opções a seguir:

Sequência
Para qualquer informação alfabética que precise ser coletada (por exemplos, locais de instalação, nomes de usuário e nomes de host).

Password
Para quaisquer informações que devam ser criptografadas quando armazenadas. Além de fornecer a criptografia dos dados, os dados que são digitados na caixa de texto são substituídos por asteriscos. Adicionalmente, é necessário digitar esta informação duas vezes para validar os dados.

Numérico
Para quaisquer informações numéricas (por exemplo, números de portas).

Opção
Para uma lista de valores específicos. Esta opção ativa a tabela Opções. É possível definir valores específicos clicando em **Incluir**. Os valores inseridos são exibidos no painel de configuração do agente como um grupo de seleções, é possível fazer somente uma seleção no grupo.

Texto Somente Leitura
Exibe texto ao configurar o agente, mas nenhuma informação é coletada.

Separador
Exibe um separador horizontal, mas nenhuma informação é coletada.

Navegador de Arquivo
Coleta uma sequência, que é um nome de arquivo. Clique em **Navegar** para navegar pelo sistema de arquivos para o arquivo desejado.

Valor Padrão
(Opcional) Especifique o valor que é mostrado no painel de configuração no tempo de execução quando o agente é configurado pela primeira vez. Se você quiser um valor-padrão para UNIX/Linux que seja diferente de um valor-padrão para Windows, clique em **Valores Múltiplos**.

Na janela **Valores Padrão da Propriedade de Configuração**, especifique os valores padrão que você deseja para sistemas Windows e para sistemas UNIX e Linux.

Nota: O suporte para vários valores-padrão é um recurso suportado somente no IBM Tivoli Monitoring V6.2.1 e superior. Se o seu agente for compatível com IBM Tivoli Monitoring V6.2, um aviso avisará sobre este requisito e você poderá cancelar ou continuar com a compatibilidade V6.2.1 ativada.

Obrigatório
Marque este campo se o usuário dever inserir um valor quando o agente for configurado. Desmarque este campo se for opcional para o usuário inserir um valor.

c) Para incluir uma opção, clique em **Incluir**

4. Na janela **Valor da Propriedade de Configuração**, preencha os campos **Rótulo** e **Valor**.

   O rótulo é exibido como uma das opções. Se esta opção for feita, o valor se tornará o valor de propriedade.
5. Clique em **OK**.

   A propriedade e seção da nova configuração são exibidas na janela **Propriedades de Configuração** em **Configuração Customizada**.
6. Opcional: Para incluir outra propriedade em uma seção existente, selecione a seção ou uma propriedade existente na seção e clique em **Incluir**. Você faz a seleção na árvore de configuração de tempo de execução da janela **Propriedades de Configuração**.
7. Preencha os campos para a nova propriedade (Preencha os mesmos campos que na etapa “3” na página 1365).
8. Clique em **OK**. É selecionada a propriedade que foi incluída mais recentemente.
9. Mantenha a seleção ou selecione a propriedade que deseja inserir no nome do arquivo de log.
10. Clique em **OK**. A propriedade é inserida no nome do arquivo de log.

Você pode então continuar no assistente para concluir a definição do grupo de atributos do arquivo de log.

Nota: Mesmo que uma propriedade de configuração esteja definida no contexto do nome de um arquivo de log, ela poderá ser usada em outros locais. Por exemplo, outro local que aceita uma propriedade de configuração é uma origem de dados de script. Essa flexibilidade significa que você pode acessar o valor do elemento de configuração **Informações do arquivo** com a variável do script *$K00_APPLICATION_LOG_FILE* se o código do produto for K00. Também é possível usar a variável de arquivo de lote do Windows, *%K00_APPLICATION_LOG_FILE%*.

Alterando Propriedades de Configuração Usando o Agent Editor

Use o Agent Editor para alterar as propriedades de configuração de seu agente.

Sobre Esta Tarefa

Esta tarefa fornece informações sobre como visualizar, incluir e alterar propriedades de configuração usando o Agent Editor.

Procedimento

1. Clique na guia **Configuração de Tempo de Execução**.
2. Selecione uma seção de configuração e clique em **Incluir**.

   Incluir funciona simplesmente como em "Customizando configuração do agente" na página 1364. Não há seleção **Editar**, porque uma seção ou propriedade de configuração é editada quando é selecionada.
3. Selecione uma propriedade de configuração para exibir a área **Detalhes da Configuração de Tempo de Execução**.
4. Na área **Detalhes da Configuração de Tempo de Execução**, edite os campos para configurar a propriedade.

Configurando uma conexão remota Windows

Informações sobre a Configuração de uma Conexão Remota do Windows

Sobre Esta Tarefa

As origens de dados do Windows Management Instrumentation (WMI), Windows Performance Monitor (Perfmon) e Windows Event Log podem monitorar os dados no sistema em que o agente é instalado. Essas origens de dados também podem monitorar os dados nos sistemas remotos do Windows. Esses três tipos de origem de dados são conhecidos como origens de dados do Windows. Se essas origens de dados do Windows estiverem monitorando os dados remotamente, todos eles compartilharão as propriedades de configuração da Conexão Remota do Windows para o nível de agente em que estão definidos.

Se você definir uma origem de dados do Windows no nível base do seu agente, as propriedades de configuração da Conexão Remota do Windows não serão incluídas no agente automaticamente. Elas não serão incluídas, para manter compatibilidade com versões anteriores de agentes que possam usar o provedor de dados do Windows antes que o monitoramento remoto tenha sido ativado. A origem de dados do Windows no seu agente, monitora os dados no sistema Windows local no qual o agente está instalado.

Se você definir uma origem de dados do Windows em um subnó em seu agente, as propriedades de configuração da Conexão Remota Windows serão incluídas no agente automaticamente. A origem de dados do Windows deve suportar a Conexão Remota do Windows, se estiver em um subnó. Não é possível limpar a opção até que todas as origens de dados do Windows sejam removidas de todos os subnós no agente. Cada instância de um subnó pode ser configurada para monitorar um sistema remoto diferente do Windows. Todas as origens de dados do Windows no subnó compartilham as propriedades de configuração da Conexão Remota do Windows.

Para configurar um agente base para monitorar remotamente um único sistema remoto do Windows, use o procedimento a seguir.

Procedimento

1. Na janela **Definição de Origem de Dados** do Agent Editor, clique em **Opções Globais**.
   A janela **Opções de Origem de Dados Globais do Windows** é aberta.
2. Selecione **Incluir Configuração da Conexão Remota do Windows**.
3. Clique em **OK**.

Resultados

As propriedades de configuração específicas da conexão a seguir podem ser acessadas a partir da página **Informações de Configuração de Tempo de Execução** do Agent Editor selecionando **Configuração para Acesso Remoto do Windows** > **Conexão Remota do Window**

Host Remoto do Windows
O nome do host do computador com Windows remoto

Senha Remota do Windows
Senha para o Windowsremoto

Windows `DOMAIN\user name` remoto
Nome de usuário para o host do Windows remoto

O que Fazer Depois

É possível visualizar, incluir e alterar as propriedades de configuração usando o Agent Editor. Para obter instruções, veja "Alterando Propriedades de Configuração Usando o Agent Editor" na página 1367. Se uma origem de dados do Windows estiver definida em um subnó, também será possível especificar Substituições de Configuração do Subnó. Para obter instruções, veja "Configuração do subnó" na página 1354.

Criando um Usuário com Permissões do Windows Management Instrumentation (WMI)

É possível incluir e configurar um usuário em um sistema Windows com permissões para navegação WMI.

Sobre Esta Tarefa

Se seu agente coletar os dados a partir de um sistema remoto usando o Windows Management Instrumentation (WMI), isso requer permissões para acessar os dados WMI no sistema remoto. O agente poderá acessar dados de WMI em um sistema remoto quando você fornecer credenciais de uma conta com permissões para acessar dados de WMI no sistema. O procedimento se aplica ao Windows 7, Windows 2008 Server e Windows Vista.

Nota: agente também pode acessar os dados em um sistema Windows remoto usando as origens de dados do Windows Performance Monitor (Perfmon), e do Windows Event Log. No entanto, no caso das origens de dados do Windows Performance Monitor (Perfmon), e do Windows Event Log, você deve fornecer credenciais de Administrador para o sistema remoto.

Procedimento

1. Crie uma conta do usuário:
   a. Acesse Windows **Iniciar** > **Ferramentas Administrativas** > **Gerenciamento de Computadores**. A janela **Gerenciamento de Computadores** é aberta.
   b. Expanda **Usuários e Grupos Locais**.
   c. Clique com o botão direito do mouse na pasta **Usuários** e selecione **Novo Usuário**.
   d. Conclua os detalhes do usuário e clique em **Criar** e em **Fechar**.
2. Configure a associação ao grupo para a nova conta de usuário:

a. Na janela **Gerenciamento de Computadores**, selecione a pasta **Usuários**.
b. Clique com o botão direito do mouse na nova conta do usuário e selecione **Propriedades**.
c. Clique na guia **Membro de**.
d. Clique em **Incluir**.
e. Clique em **Avançado**.
f. Clique em **Localizar Agora**.
g. Selecione os grupos a seguir:
   - Usuários COM Distribuídos
   - Usuários de Log de Desempenho
   - Usuários de Desktop Remoto

   Dica: Pressione Ctrl e clique para selecionar múltiplos grupos.
h. Clique em **OK** até retornar para a janela **Gerenciamento de Computadores**.
i. Selecione **Arquivo** > **Sair** para sair da janela **Gerenciamento de Computador**.

3. Designar direitos Assign Distributed Component Object Model (DCOM):
   a. Acesse Windows **Iniciar** > **Ferramentas Administrativas** > **Serviços de Componente**. A janela **Serviços de Componentes** é aberta.
   b. Expanda **Serviços de Componente** > **Computadores** > **Meu Computador**.
   c. Dê um clique com o botão direito do mouse em **Meu Computador** e selecione **Propriedades**. A janela **Propriedades de Meu Computador** é aberta.
   d. Clique na guia **Segurança de COM**.
   e. Na área **Permissões de Acesso**, clique em **Editar Limites**
   f. Em **Usuários COM Distribuídos**, verifique se **Acesso Local** e **Acesso Remoto** estão selecionados.
   g. Clique em **OK** para salvar as configurações.
   h. Na janela **Propriedades de Meu Computador**, área **Permissões de Ativação**, clique em **Editar Limites**
   i. Em **Usuários COM Distribuídos**, verifique se **Lançamento Local**, **Lançamento Remoto**, **Ativação Local** e **Ativação Remota** estão selecionados.
   j. Clique em **OK** para salvar as configurações e clique em **OK** novamente para fechar a janela **Propriedades de Meu Computador**.
   k. Selecione **Arquivo** > **Sair** para sair da janela **Serviços de Computador**.
4. Configure as designações de segurança de namespace WMI
   a. Acesse Windows **Iniciar** > **Executar...**.
   b. Insira `wmimgmt.msc` e clique em **OK**.
   c. Clique com o botão direito do mouse em **Controle de WMI (Local)** e selecione **Propriedades**.
   d. Clique na guia **Segurança**.
   e. Clique em **Segurança**.
   f. Clique em **Incluir**.
   g. Clique em **Avançado**.
   h. Clique em **Localizar Agora**.
   i. Selecione a nova conta do usuário e clique em **OK** até retornar para a janela **Segurança para Raiz**.
   j. Clique em **Avançado** e selecione a conta do usuário incluída recentemente.
   k. Clique em **Editar**.
   l. Na seleção do menu **Aplicar a:**, selecione **Este namespace e subnamespaces**.

m. Em **Executar Métodos**, verifique se **Ativar Conta**, **Ativação Remota** e **Segurança de Leitura** estão selecionados.

n. Clique em **OK** até retornar para a janela **wmimgmt**.

o. Selecionar **Arquivo** > **Sair** para sair da janela **wmimgmt**.

O que Fazer Depois

Para obter informações adicionais sobre a coleta de dados WMI a partir de um sistema remoto, consulte "Monitorando Dados a partir do Windows Management Instrumentation (WMI)" na página 1225.

Configurando uma Conexão Remota de Secure Shell (SSH)

Informações sobre como configurar uma conexão remota SSH

Sobre Esta Tarefa

As origens de dados de script podem monitorar dados no sistema no qual o agente está instalado e também nos sistemas remotos. Se as origens de dados de script estiverem monitorando dados remotamente, todas elas compartilham as propriedades de configuração da conexão remota SSH para o nível do agente em que estão definidas. Versões anteriores de um agente podem usar o provedor de dados antes do monitoramento remoto ter sido ativado. Para manter a compatibilidade com versões anteriores dos agentes, as propriedades de configuração da conexão remota SSH não são incluídas automaticamente no agente. A origem de dados de script no agente monitora dados no sistema local no qual o agente está instalado.

Se você definir uma origem de dados de script em um subnó e selecionar **Ativar coleta de dados usando SSH**, poderá configurar cada instância do subnó para monitorar um sistema remoto diferente. Todas as origens de dados de script no subnó compartilham as propriedades de configuração de conexão remota SSH.

Se você deseja que o agente monitore remotamente um sistema remoto, use o procedimento a seguir.

Procedimento

Na janela **Definição de Origem de Dados** do Agent Editor para a origem de dados de script, selecione **Ativar coleta de dados usando SSH**.

Resultados

As propriedades de configuração específica de conexão a seguir podem ser acessadas a partir da página **Agent Editor**, **Informações de Configuração de Tempo de Execução**, selecionando **Configuração para Shell Seguro (SSH)** > **Conexão Remota de SSH**

Endereço de Rede
O endereço IP ou o nome do host do computador remoto.

Número da Porta do SSH
O número da porta do protocolo da Internet no qual o servidor SSH está em execução. O valor padrão é 22.

Tipo de Autenticação
Tipo de autenticação a ser usada quando estiver efetuando login no servidor SSH remoto. É possível escolher Senha ou Chave Pública.

Desconectar-se do Sistema Remoto Depois de Cada Intervalo de Coleta
Uma opção para determinar se o provedor de dados de script elimina a sessão de login para o sistema remoto após ele coletar dados. Por padrão, o valor é No.

Remover o Script do Sistema Remoto Depois de Cada Intervalo de Coleta
Uma opção para excluir o script do sistema remoto depois de cada intervalo de coleta de dados. Por padrão, o valor é No.

Se o Tipo de Autenticação for configurado para a Senha, as propriedades de configuração a seguir podem ser acessadas da página **Agent Editor**, **Informações de Configuração de Tempo de Execução**, selecionando **Configuração para Shell Seguro (SSH)** > **Senha**:

Nome do Usuário
Nome de usuário para o sistema remoto

Password
Senha para o sistema remoto

Se o Tipo de Autenticação for configurado para a Chave Pública, as propriedades de configuração a seguir podem ser acessadas da página **Agent Editor**, **Informações de Configuração de Tempo de Execução**, selecionando **Configuração para Shell Seguro Shell (SSH)** > **Chave Pública**:

Nome do Usuário
O nome de usuário associado ao arquivo da chave pública

Arquivo-chave Público
O arquivo da chave pública associado ao usuário

Arquivo-chave Privado
O arquivo de chave privado associado ao usuário

Password
Senha usada para desbloquear o arquivo de chave privado

O que Fazer Depois

É possível visualizar, incluir e alterar as propriedades de configuração usando o Agent Editor. Para obter instruções, veja "Alterando Propriedades de Configuração Usando o Agent Editor" na página 1367. Se as propriedades de configuração de Conexão Remota do SSH estiverem incluídas em um subnó, será possível especificar também as Substituições de Configuração do Subnó. Para obter instruções, veja "Configuração do subnó" na página 1354.

Criando Espaços de Trabalho, Comandos Executar Ação e Situações

Após a instalação de um agente em um ambiente IBM Tivoli Monitoring, será possível criar áreas de trabalho, consultas, comandos Executar ação e situações para sua solução de monitoramento.

As situações, espaços de trabalho, comandos Executar Ação e consultas criados podem ser incluídos no pacote de instalação. Para ter uma imagem de instalação para situações, áreas de trabalho e o agente em si, a situação e os arquivos da área de trabalho devem estar no mesmo projeto que o agente. O Agent Builder fornece um assistente para criar os arquivos apropriados no projeto do agente. Para obter informações sobre a importação de arquivos de suporte ao aplicativo, consulte "Importando Arquivos de Suporte do Aplicativo" na página 1406.

Criando Situações, Comandos Executar Ação e Consultas

Localizar informações para ajudar a criar situações, comandos Executar Ação e consultas.

Para criar situações, comandos Executar Ação e consultas, use o Tivoli Enterprise Portal e o editor de Situação integrado. Para obter informações detalhadas sobre como criar situações, consulte o Tivoli Enterprise Portal: Guia do Usuário. Também é possível usar a documentação da ajuda que está instalada com seu Tivoli Enterprise Portal Server. Um agente de monitoramento do Agent Builder pode reconhecer e executar processamento especial para um conjunto de comandos executar ação específicos. Para obter mais informações sobre esses comandos especiais Executar Ação, consulte "Referência dos Comandos Executar Ação" na página 1508.

Situações para agentes de monitor do sistema são criadas de forma diferente das situações Corporativas que são criadas com o editor Tivoli Enterprise Portal Situation ou o comando **`tacmd createSit`**. Para agentes system monitor, situações privadas são criadas em um arquivo de configuração de situação privada local XML para o agente. Para obter maiores informações sobre a criação de situações para

agentes de system monitor, consulte "Situações privadas" no capítulo "Agent Autonomy" do Guia do Administrador de Monitoramento *IBM Tivoli'*.

Criando Espaços de Trabalho

Coloque o Tivoli Enterprise Portal no modo de Administrador para criar áreas de trabalho que você possa exportar e incluir em sua solução.

Sobre Esta Tarefa

Construir as áreas de trabalho no ambiente no qual elas são usadas. Ao criar áreas de trabalho, altere as configurações de exibição em seu computador para construir áreas de trabalho na resolução mínima que é usada normalmente em seu ambiente. A construção de espaços de trabalho em uma resolução maior pode criar visualizações que são muito confusas para serem razoavelmente utilizadas em resoluções menores.

Para criar áreas de trabalho que possam ser exportadas e incluídas em sua solução, o Tivoli Enterprise Portal deverá ser colocado no modo "Administrador". Para colocar o Tivoli Enterprise Portal no modo "Administrador", use as etapas a seguir:

Procedimento

1. Acesse o diretório *ITM_INSTALL*/CNP e abra o arquivo `cnp.bat`.

   Se você usou a instalação padrão, o diretório é `C:\IBM\ITM\CNP`. No arquivo `cnp.bat`, é necessário atualizar a linha `set _CMD= %_JAVA_CMD%` para incluir a opção `-Dcnp.candle.mode="$_KCJ_$"`.

   Para criar extensões em sistemas Linux ou AIX, use o seguinte caminho:

   ```
   /opt/IBM/ITM/li263/cj/bin/cnp.sh
   ```

   Em que *li263* é o sistema operacional em que o Tivoli Enterprise Portal está sendo executado.

   O `set _CMD= %_JAVA_CMD%` atualizado se parece com o exemplo a seguir:

   ```
   set _CMD= %_JAVA_CMD% -Dcnp.candle.mode="$_KCJ_$" -Xms64m -Xmx256m -showversion -noverify
    -classpath %CPATH% -Dkjr.trace.mode=LOCAL -Dkjr.trace.file=C:\IBM\ITM\CNP\LOGS\kcjras1.log
   -Dkjr.trace.params=ERROR -DORBtcpNoDelay=true -Dibm.stream.nio=true
   -Dice.net.maxPersistentConnections=16 -Dice.net.persistentConnectionTimeout=1
   -Dcnp.http.url.host=SKINANE -Dvbroker.agent.enableLocator=false -Dnv_inst_flag=%NV_INST_FLAG
   %
   -Dnvwc.cwd=%NVWC_WORKING_DIR% -Dnvwc.java=%NVWC_JAVA% candle.fw.pres.CMWApplet
   ```

   Nota: O comando é mostrado aqui em várias linhas somente para motivos de formatação.
2. Abra um novo Tivoli Enterprise Portal Client e efetue login com o ID do usuário `sysadmin`.
3. Configure o ID do usuário "sysadmin" no modo "Administrador". No Tivoli Enterprise Portal, selecione **Editar** > **Administrar Usuários**. Selecione **sysadmin** e, em seguida, na guia **Permissões**, selecione **Administração de Espaço de Trabalho**. Selecione a caixa de opções **Modo de Administração da Área de Trabalho**.

   Se você fizer a seleção corretamente, ***ADMIN MODE*** será exibido na barra de título da área de trabalho.

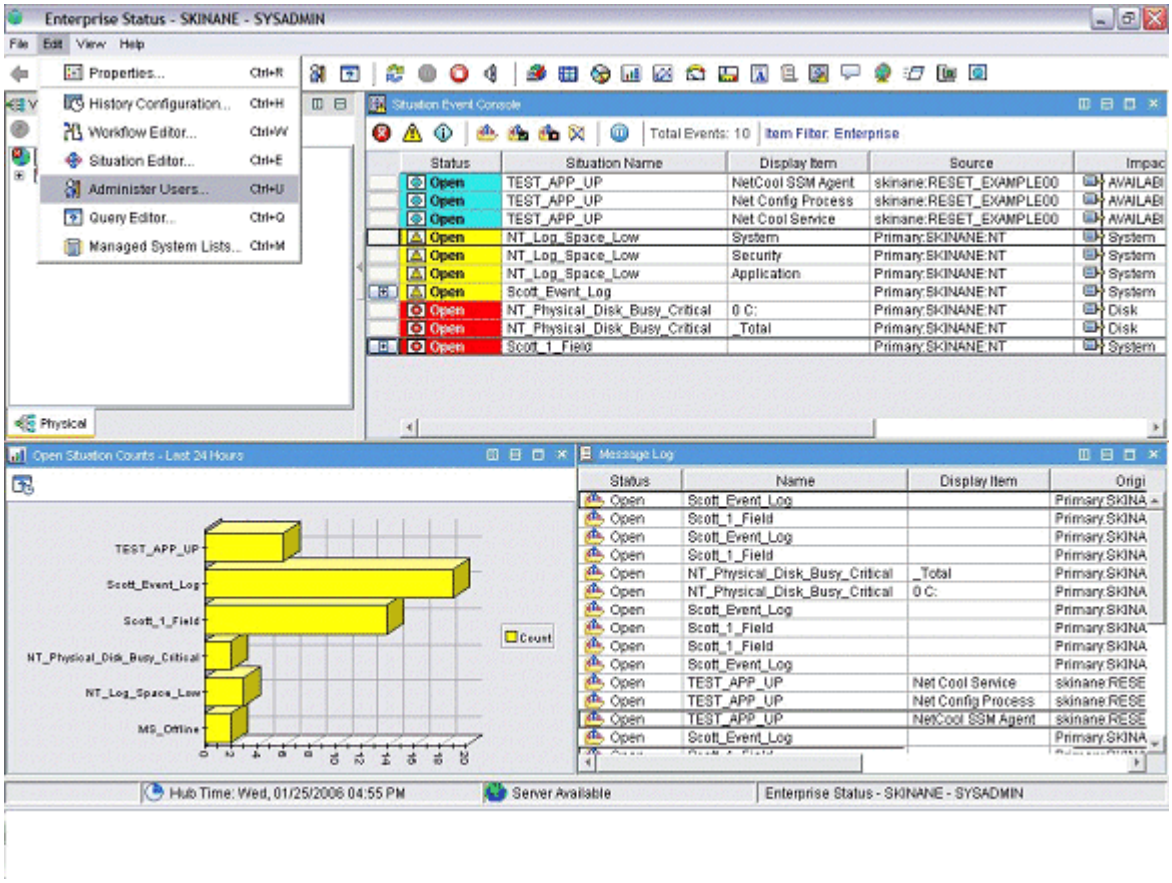


Figura 61. Configurando o ID do usuário `sysadmin`

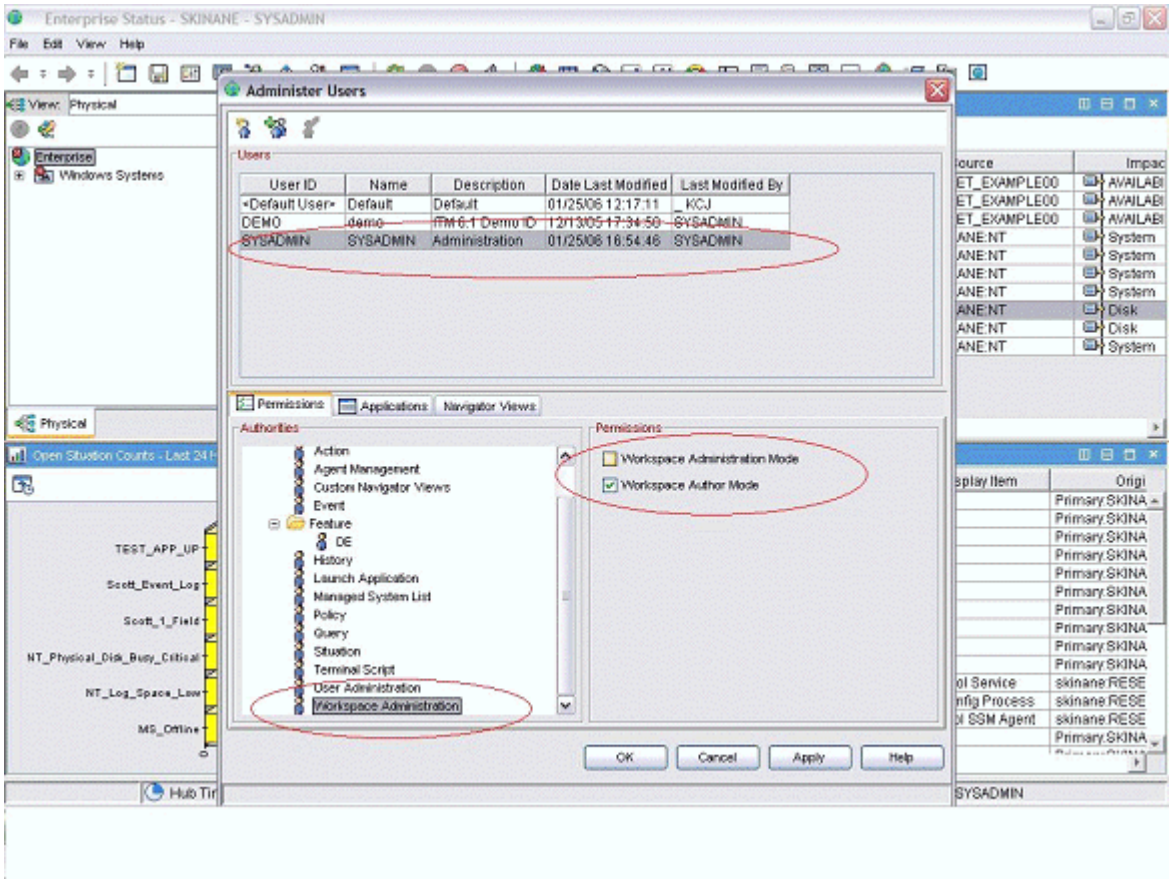


Figura 62. Configurando o ID do usuário `sysadmin` (continuado)

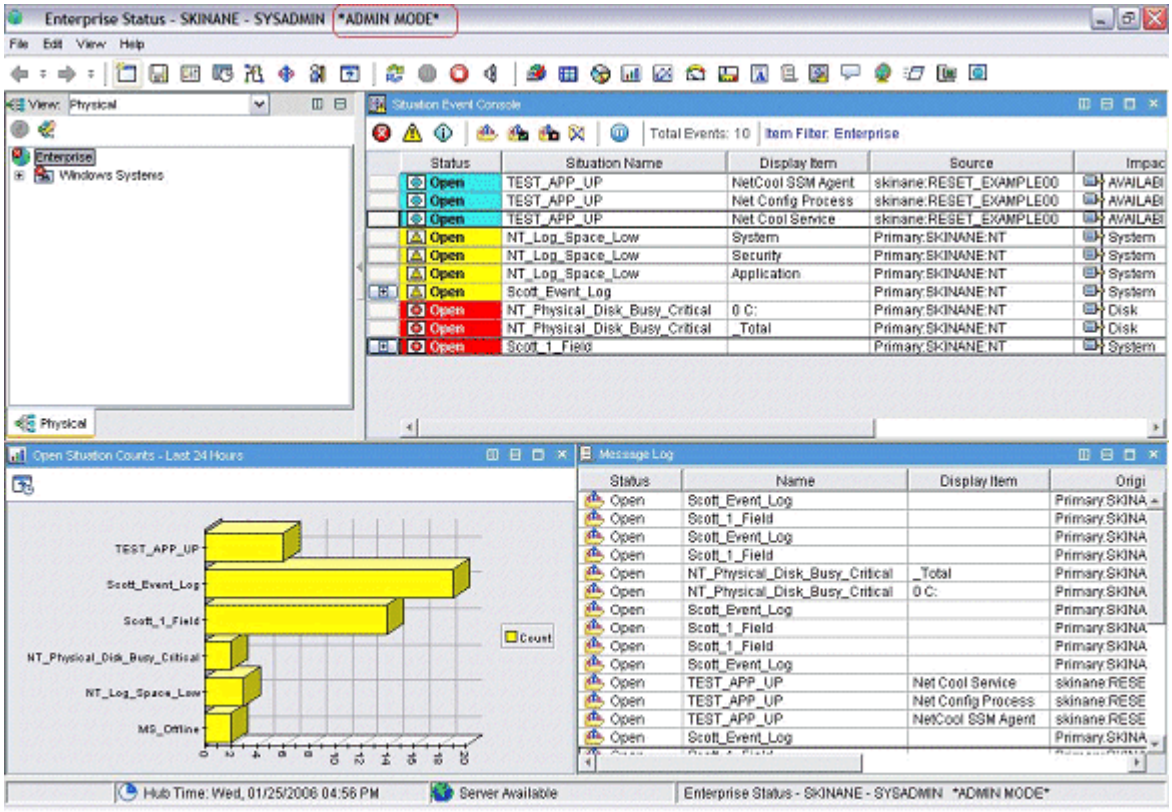


Figura 63. Configurando o ID do usuário `sysadmin` (continuado)

O que Fazer Depois

Depois que estiver no modo "Administrador", conforme descrito em (Figura 63 na página 1375), você estará pronto para criar áreas de trabalho para seu aplicativo. Para obter informações sobre como customizar e criar áreas de trabalho, consulte o Tivoli Enterprise Portal: Guia do Usuário. Como alternativa, use a documentação da ajuda que é instalada com seu componente Tivoli Enterprise Portal.

Se desejar que as áreas de trabalho sejam "somente leitura" e que não sejam excluídas por um cliente, configure as propriedades "not-editable" e "non-deletable" para cada área de trabalho. Nas propriedades do espaço de trabalho, é necessário selecionar as seguintes propriedades:

- **Não Permitir Modificações**
- **Produto Fornecido pela IBM (Marcar como Não Podendo Ser Excluído)**

Você pode ir para propriedades visualizando uma área de trabalho ou clicando no ícone com os controles nele. Também pode ir para uma das páginas de propriedade de visualização e então ir para o nível da área de trabalho na árvore de propriedades. Se tiver mais de uma área de trabalho para cada item do navegador, lembre-se de configurar as propriedades para cada área de trabalho. Conforme indicado na captura de tela do exemplo a seguir:

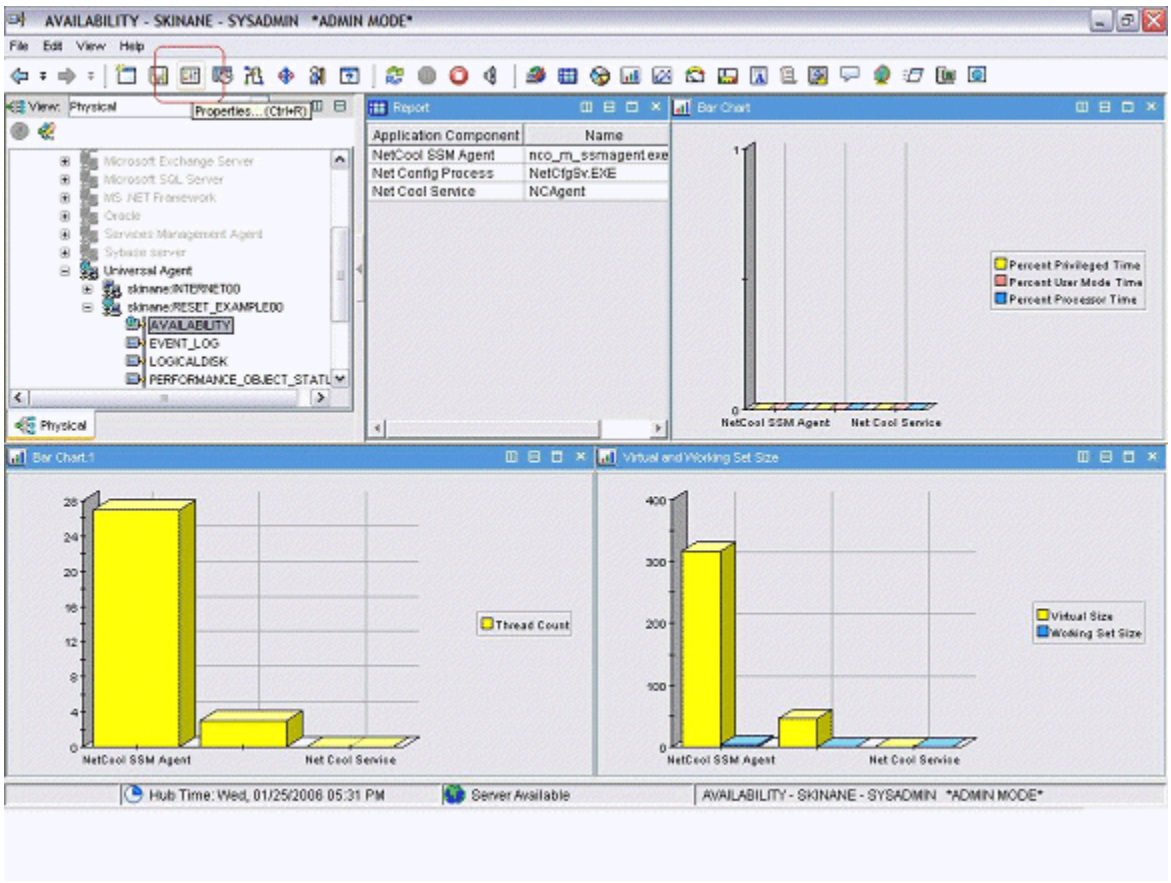


Figura 64. Configurando propriedades do espaço de trabalho

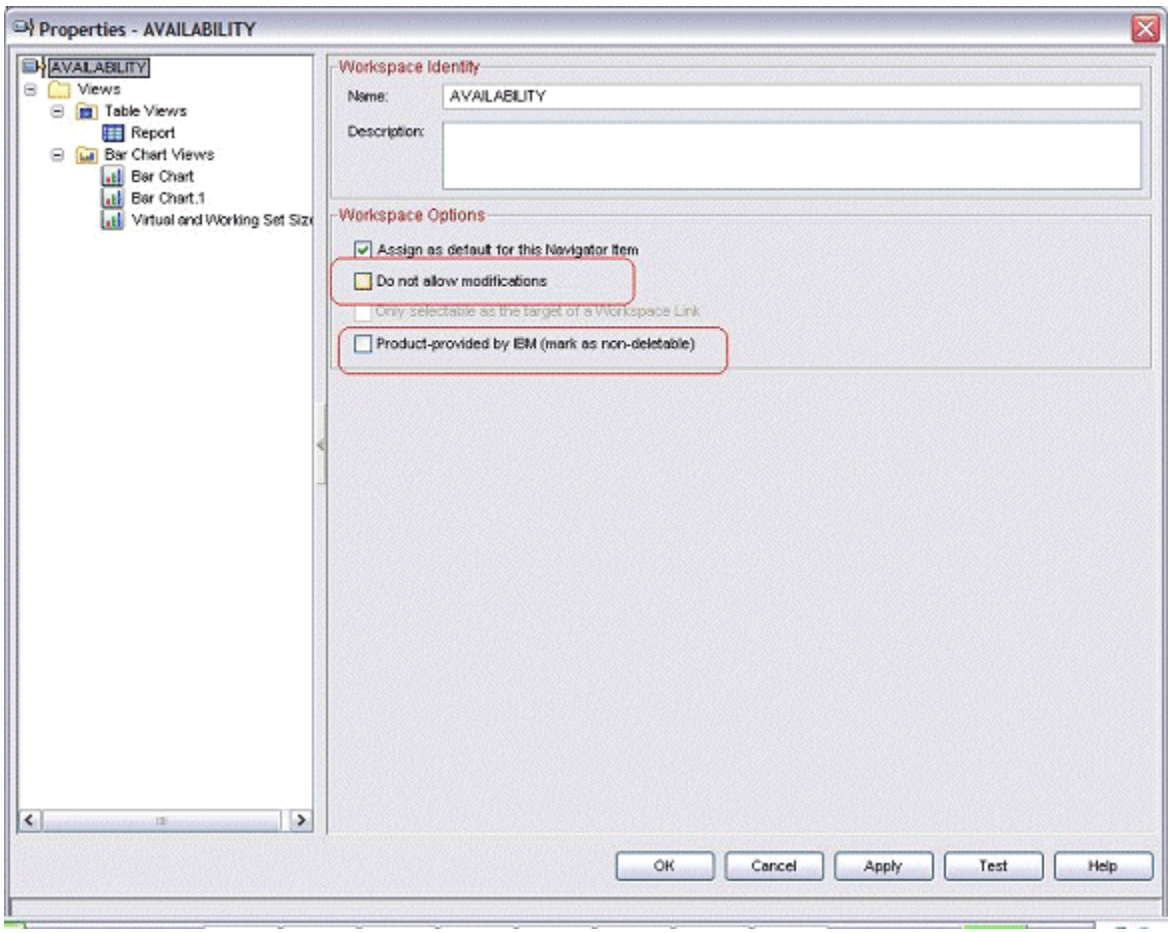


Figura 65. Configurando propriedades do espaço de trabalho (continuação)

Preparando o agente para Cloud APM

Se desejar usar seu agente com o IBM Cloud Application Performance Management, será necessário prepará-lo usando o assistente do **Configuração do Painel**. Este assistente configura as informações que você pode ver nos painéis de resumo e detalhes em Cloud APM. Ele também configura as informações de recurso que o Cloud APM requer para o agente.

Antes de Iniciar

A fim de preparar o agente para o Cloud APM com êxito, é necessário assegurar-se de que o agente forneça os dados a seguir:

- Um ou mais conjuntos de dados (grupos de atributos) que produzem uma linha de dados. É possível usar os atributos a partir desses conjuntos de dados para preencher o painel de resumo.

  Importante: Para incluir quaisquer informações no painel de resumo, é necessário fornecê-las no conjunto de dados que produz uma linha única de dados. Algumas origens de dados criam conjuntos de dados que produzem várias linhas de dados; por exemplo, o processo, o serviço do Windows e as origens de dados do código de retorno do comando colocam dados no conjunto de dados de Disponibilidade único, que produz várias linhas. Em tais casos, é necessário criar um conjunto de dados filtrado produzindo uma linha a fim de incluir os dados em um painel de resumo. Para obter instruções, veja “Criando um grupo de atributos filtrado” na página 1344.
- Um atributo numérico dentro de um desses conjuntos de dados que indica o status do serviço monitorado (normal, aviso, crítico ou outros valores de status similares). Você deve definir os valores da gravidade do status para este atributo. Para obter instruções sobre como definir os valores da gravidade

de status, consulte “Especificando gravidade para um atributo usado como um indicador de status” na página 1200.

- Se o número da porta no qual o aplicativo monitorado fornece serviço for fixo, você deverá conhecer a porta. Se a porta puder ser mudada entre diferentes implementações, um dos conjuntos de dados que produzem uma linha de dados deverá conter um campo numérico indicando a porta.
- Se o agente puder ser instalado em um host para monitorar um servidor que está em execução em um host diferente, um atributo de sequência dentro de um desses conjuntos de dados que indica o endereço IP do servidor. Se o agente sempre monitora o host no qual ele está em execução, um atributo desse tipo não é necessário.

  Dica: Se um atributo que fornece o nome do host estiver disponível, será possível criar um atributo derivado para o endereço IP usando a função `nameToIpAddress`. Para obter informações sobre a criação de um atributo derivado, consulte “Criando Atributos Derivados” na página 1193. Para obter informações sobre a função, consulte “ipAddressToName” na página 1207.

Se o agente tiver subnós, esses requisitos se aplicarão a cada subnó para o qual você deseja criar um painel.

Sobre Esta Tarefa

Cloud APM monitora *recursos*. Um recurso corresponde à instância do agente ou, às vezes, a um subnó. Para definir um recurso, é necessário fornecer um nome do tipo de recurso, nome do servidor, endereço IP e número da porta que se aplicam ao serviço monitorado.

Cloud APM exibe um painel de resumo para cada recurso monitorado. O painel de resumo inclui um indicador de status; com este indicador (geralmente verde, amarelo ou vermelho para status normal, aviso ou crítico) o usuário pode ter uma visão rápida do status do recurso. O mesmo painel pode conter algumas outras métricas de funcionamento de alto nível.

No painel de resumo, os dados são exibidos como itens únicos. Portanto, o conjunto de dados com estes dados deve produzir somente uma linha.

Opcionalmente, um painel de detalhe pode estar disponível para o agente. O usuário pode clicar no painel de resumo para visualizar o painel de detalhes. O painel de detalhes pode exibir tabelas, portanto, os dados de qualquer conjunto de dados podem ser usados nesse painel.

Você deve selecionar os atributos que são exibidos no painel de resumo (incluindo o indicador de status) e no painel de detalhes.

Importante: Os dados nos atributos que você seleciona são transmitidos automaticamente do agente para o servidor Cloud APM a cada minuto. A especificação de dados em excesso pode levar à sobrecarga da rede, do servidor ou do host monitorado. Selecione somente os atributos necessários. Por exemplo, se um conjunto de dados associados ou um atributo derivado precisar ser exibido, não especifique os atributos de origem também.

Importante: Nenhum dado diferente desses atributos é transmitido para o Cloud APM. Não é possível visualizar ou usar outros dados no Cloud APM, exceto para limites, que são monitorados no nível do agente. Se você usar outros dados nos limites, poderá não ser capaz de visualizar o status de limite no console do Cloud APM.

Procedimento

1. Na visualização **Informações do Agente**, clique no link **Painéis**.
2. Sob **Componentes do Painel**, selecione **Mostrar Componentes do Agente no Painel**.

   Dica: Alternativamente, se você estiver criando um agente para usar exclusivamente com IBM Tivoli Monitoring, é possível selecionar **Nenhuma Presença de Painel para este Agente**. Neste caso, não conclua as etapas subsequentes desse procedimento. Não é possível instalar esse tipo de agente em um ambiente do Cloud APM.
3. Clique no link **Assistente de Configuração de Painel**.
4. Se o agente tiver subnós, defina as disposições dos recursos do agente e do subnó no Cloud APM:

- Selecione **Instâncias do Agente Base** para exibir o agente base (dados fora de subnós) como um recurso.
- Para cada subnó, selecione **Instâncias de "*nome*" do Subnó** para exibir este subnó como um recurso.
- Opcionalmente, para qualquer um dos subnós selecionados, selecione **Mostrar como filho do agente**. Nesse caso, o recurso do subnó é exibido como um filho sob o recurso do agente nas listas no console do Cloud APM.

O Cloud APM exibirá um painel de resumo e detalhes para cada um dos componentes que você selecionou.

Importante: Se você executar o assistente novamente e desmarcar o agente ou subnó, os recursos para o agente ou subnó não serão removidos automaticamente. Para remover os recursos, expanda **Recursos** na visualização Esboço, selecione os recursos a serem excluídos e pressione a tecla Delete no teclado.

5. Na página **Seleção de Atributo - Status**, selecione o atributo que indica o status do serviço monitorado. Atributos numéricos a partir de grupos que retornam uma única linha de dados estão disponíveis.

   Dica: Alternativamente, se você não desejar exibir status no painel, desmarque **Fornecer Status para este Agente**.
6. Na mesma página, é possível selecionar se você deseja exibir dados adicionais nos painéis de resumo e detalhes:
   - Para exibir métricas de funcionamento de alto nível adicionais no painel de resumo, assegure que a caixa **Selecionar atributos adicionais para exibir nas informações de resumo deste agente** esteja selecionada. Caso contrário, desmarque a caixa.
   - Para exibir dados adicionais no painel de detalhes, assegure que a caixa **Selecionar atributos adicionais para exibir nas informações detalhadas deste agente** esteja selecionada. Caso contrário, desmarque a caixa. (Em geral, selecione esta caixa, pois um painel de detalhes é necessário para exibir dados suficientes para tornar um agente de monitoramento significativo).

   Clique em **Avançar**.
7. Se você selecionou **Selecionar atributos adicionais para exibir nas informações de resumo deste agente**, na página **Seleção de Atributo - Resumo**, selecione até quatro atributos adicionais para incluir no painel de resumo. Atributos de grupos que retornam uma única linha de dados estão disponíveis. Clique em **Avançar**.
8. Se você selecionou **Selecionar atributos adicionais para exibir nas informações detalhadas deste agente**, na página **Seleção de Atributo - Detalhes**, selecione o atributo para incluir no painel de detalhes. Todos os atributos no agente estão disponíveis; para evitar problemas de desempenho, inclua o mínimo de atributos possível. Clique em **Avançar**.
9. Na página **Tipo de Recurso**, insira o tipo de servidor que você está monitorando, por exemplo, `Servidor de E-mail` ou `SampleCo Database Server`. Clique em **Avançar**.
10. Na página **Seleção de Atributo - Nome do Servidor de Software**, insira um nome de servidor de software fixo no campo **Nome Fixo** ou selecione um atributo a partir de seu agente que forneça o nome do servidor de software. Esse nome é exibido para o usuário para esta instância monitorada específica, por exemplo, o nome da instância do servidor de aplicativos JBoss. Clique em **Avançar**.

    Importante: Não execute dois ou mais agentes de monitoramento, instâncias do agente ou subnós com o mesmo nome do servidor de software no mesmo host monitorado. Se seu agente tiver subnós ou instâncias, assegure que um nome de servidor de software exclusivo seja gerado para cada instância ou subnó. Se dois agentes diferentes produzirem o mesmo nome do servidor de software, não os instale no mesmo host monitorado.
11. Na página **Seleção de Atributo - Endereço IP**, selecione um atributo a partir de seu agente que especifique o endereço IP (não o nome do host) da conexão de interface primária que o servidor monitorado ou aplicativo usa. Por exemplo, a conexão HTTP para um servidor HTTP ou a conexão do cliente de banco de dados para um servidor de banco de dados. Como alternativa, selecione **Usar o**

endereço IP do agente para usar o endereço do host no qual o agente é executado. Clique em **Avançar**.

12. Na página **Seleção de Atributo - Porta**, insira a porta na qual o aplicativo monitorado fornece serviço ou selecione um atributo numérico a partir de seu agente que especifique essa porta. Clique em **Concluir**.
13. Se você selecionou o agente e um subnó ou mais de um subnó como recursos, clique em **Avançar** para inserir informações do painel e recurso para o próximo componente (agente ou subnó). Se o botão **Avançar** estiver desativado, você inseriu as informações para todos os componentes necessários; clique em **Concluir** para concluir o assistente.

Resultados

Ao instalar o agente em um host monitorado, é possível visualizar os painéis de resumo e detalhes na guia **Visão Geral do Status**.

Importante: Pode haver um atraso de até 30 minutos entre a instalação do agente e a disponibilidade dos painéis, principalmente se essa for a primeira vez que este tipo e esta versão do agente são instalados em seu ambiente.

Clique no painel de resumo para o agente para visualizar o painel de detalhes. Por padrão, todas as informações no painel de detalhes são exibidas como tabelas.

É possível usar a guia **Detalhes do Atributo** para configurar a exibição customizada destas informações como tabelas e gráficos.

Testando seu agente no Agent Builder

Depois de usar o Agent Builder para criar um agente, será possível testar o agente no Agent Builder.

Teste o agente para assegurar que os dados de monitoramento que você está esperando são os dados que estão sendo exibidos. Ao testar o seu agente, você aprenderá a modificar ou ajustar as configurações no agente para assegurar que os dados exibidos sejam proveitosos. e precisos.

É possível testar seu agente no Agent Builder usando os métodos a seguir:

1. Inicie usando a função de teste de grupo de atributo do Agent Builder para testar os grupos de atributos individuais um por vez. Para obter mais informações, consulte “Teste de Grupo de Atributos” na página 1380.
2. Depois de concluir o teste do grupo de atributos, você pode usar a função de teste do agente do Agent Builder para testar todos os grupos de atributos em seu agente juntos. Para obter mais informações, consulte “Teste integral de agente” na página 1384.

Importante: Ao testar seu agente no Agent Builder, será possível ver os valores especiais a seguir para atributos numéricos:

- -1: um erro geral
- -2: dados ausentes
- -3: nenhum valor (por exemplo, NULL foi retornado por um banco de dados)

Teste de Grupo de Atributos

Você pode utilizar grupo de atributos de teste para testar os grupos de atributos do agente criado com Agent Builder, um grupo de atributos por vez. É possível testar muitos grupos de atributo antes de concluir a definição do grupo de atributos. Por exemplo, você pode iniciar o teste a partir do **Assistente do IBM Tivoli Monitoring Agent** quando você estiver definindo os grupos de atributos de um novo agente. Também é possível iniciar o teste a partir do **Assistente do Componente IBM Tivoli Monitoring Agent** quando estiver incluindo grupos de atributos para um agente existente.

Antes de Iniciar

Antes de iniciar o teste de um grupo de atributos, opcionalmente, é possível:

- Configurar preferências de teste do grupo de atributos. Para obter mais informações, consulte “Teste de Grupo de Atributos - Preferências” na página 1382.
- Configurar variáveis de ambiente, propriedades de configuração e, onde aplicável, informações de Java. Para obter mais informações, consulte “Teste de Grupo de Atributos - Configuração” na página 1383.

Sobre Esta Tarefa

O Agent Builder suporta uma função de teste de grupo de atributos para a maioria das origens de dados

Procedimento

- Inicie o procedimento de Teste das seguintes maneiras:
  1. Durante a criação do agente ou do grupo de atributos, clique em **Testar** na página Informações da origem de dados relevantes.
  2. Após a criação do agente, selecione um grupo de atributos no Agent Editor **Definição de Origem de Dados** e clique em **Testar**. Para obter informações adicionais sobre o Agent Editor, consulte “Usando o Agent Editor para modificar o agente” na página 1172.

  Após clicar em **Testar** em uma das duas etapas anteriores, a janela Teste do Grupo de Atributos é exibida. Essa janela é diferente para diferentes origens de dados,

  O Agent Builder suporta uma função de teste de grupo de atributos para a maioria das origens de dados.

  Para obter informações adicionais sobre os procedimentos de teste para grupos de atributo específicos, consulte as seções de Teste a seguir:

  - Windows Management Instrumentation (WMI), para obter informações adicionais sobre o procedimento de teste WMI, consulte “Testando Grupos de Atributos WMI” na página 1226
  - Windows Performance Monitor (Perfmon), para obter informações adicionais sobre o procedimento de teste Perfmon, consulte “Testando Grupos de Atributos Perfmon” na página 1228
  - Protocolo Simples de Gerenciamento de Rede (SNMP), para obter informações adicionais sobre o teste SNMP, consulte “Testando Grupos de Atributos SNMP” na página 1233
  - Emissor de eventos do Protocolo Simples de Gerenciamento de Rede (SNMP), para obter informações adicionais sobre o procedimento de teste de evento SNMP, consulte “Testando Grupos de Atributos de Evento SNMP” na página 1238
  - Java Management Extensions (JMX), para obter informações adicionais sobre o procedimento de teste JMX, consulte “Testando Grupos de Atributos JMX” na página 1258
  - Modelo de Informação Comum (CIM), para obter informações adicionais sobre o procedimento de teste CIM, consulte “Testando Grupos de Atributos CIM” na página 1261
  - Arquivo de log, para obter informações adicionais sobre o procedimento de teste do arquivo de log, consulte “Testando Grupos de Atributos do Arquivo de Log” na página 1271
  - Script, para obter informações adicionais sobre o procedimento de teste de script, consulte “Etapas para Monitorar Saída de um Script” na página 1283
  - Java Database Connectivity (JDBC), para obter informações adicionais sobre o procedimento de teste JDBC, consulte “Testando Grupos de Atributos JDBC” na página 1293
  - Ping do Internet Control Message Protocol (ICMP), para obter informações adicionais sobre o procedimento de teste ICMP, consulte “Testando grupos de atributos de Ping” na página 1296
  - Disponibilidade do Hypertext Transfer Protocol (HTTP), para obter informações adicionais sobre o procedimento de teste HTTP, consulte “Testando Grupos de Atributos HTTP” na página 1304
  - SOAP, para obter informações adicionais sobre o procedimento de teste SOAP, consulte “Testando Grupos de Atributo SOAP” na página 1313
  - Soquete do Protocolo de Controle de Transmissões (TCP), para obter informações adicionais sobre o procedimento de teste de soquete, consulte “Testando Grupos de Atributos do Soquete” na página 1324

– Java application programming interface (API), para obter informações adicionais sobre o procedimento de teste de API Java, consulte “Testando Grupos de Atributos de Aplicativo Java” na página 1338

Algumas origens de dados não possuem uma função de teste de grupo de atributos, por exemplo:

– Quando for possível usar o navegador do Agent Builder para visualizar os dados ativos em um sistema. Por exemplo, é possível visualizar os processos que estão atualmente em execução no sistema (processos). Outros exemplos ocorrem quando você pode visualizar os serviços que são instalados no sistema (serviços do Windows) e os Logs de Eventos do Windows que estão presentes.
– Há pouca ou nenhuma customização que pode ser realizada no agente (Log Binário do AIX, código de retorno de comando).
– Os grupos de atributos Associados e Filtrados não podem ser testados usando a função de teste do grupo de atributos porque esses grupos são baseados em diversos grupos de atributos.

Nota:

1. Use o teste de agente integral para testar as origens de dados que não podem ser testadas usando a função de teste do grupo de atributos. Para obter mais informações sobre o teste de agente integral, consulte “Teste integral de agente” na página 1384.
2. Ao testar as origens de dados depois de clicar em **Coletar Dados** os dados podem não ser exibidos ou podem não ser atuais após o primeiro clique. Nesses casos, clique em **Coletar Dados** uma segunda vez para exibir os dados atuais.

- Depurando:

  Cada origem de dados testada possui um diretório de teste criado para ela pelo Agent Builder. Esse diretório é usado para o ambiente de tempo de execução de teste da origem de dados. Os arquivos de log que estão relacionados aos testes executados na origem de dados estão armazenados neste diretório. Os arquivos de log podem ser úteis para ajudar a depurar problemas localizados durante o teste.

  Nota:

  1. O local do arquivo de log de teste é mostrado como uma mensagem de status na janela **Testar** depois de clicar em **Iniciar Agente** e também depois de clicar em **Parar Agente**.
  2. Todos os diretórios da origem de dados de teste são excluídos quando o Agent Builder é encerrado.

Teste de Grupo de Atributos - Preferências
Configurar preferências antes de testar um grupo de atributos.

Sobre Esta Tarefa
Antes de iniciar o teste de um grupo de atributos, opcionalmente, é possível configurar algumas preferências que determinam como os atributos serão tratados durante o teste.

Procedimento

1. Selecione **Janela** > **Preferências** da barra de menus do Agent Builder.
   A janela **Preferências** é aberta.
2. Selecione **Agent Builder**.

   As preferências associadas ao teste dos grupos de atributos são mostradas:

   Diálogo Mostrar Tipos de Dados Alterados ao Testar
   Quando selecionado, o Agent Builder sugere mudanças no tipo de dados de um atributo. O Agent Builder sugere mudanças quando o tipo de dados de um atributo não corresponde aos dados retornados por um teste para esse atributo. Por exemplo, se o comprimento da sequência definido para um atributo for muito curto para conter um valor retornado por um teste. Neste exemplo, o Agent builder sugere a redefinição do atributo para ter um comprimento de sequência mais longo.

Quando esta opção estiver desmarcada, o Agent Builder não verificará ou sugerirá tipos de dados durante o teste. Esta opção é selecionada por padrão.

Máximo de Atributos de Script ou de Log Criados
O valor inserido neste campo determina o número máximo de atributos que o Agent Builder analisa durante um teste inicial de um arquivo de log ou de um grupo de atributos de script. O valor padrão é 25.

3. Quando concluir a configuração de suas preferências, clique em **OK** para salvar suas configurações e fechar a janela **Preferências**.

   Se desejar restaurar as configurações padrão, clique em **Restaurar Padrões** antes de clicar em **OK**

Teste de Grupo de Atributos - Configuração
Configurar variáveis de ambiente, propriedades de configuração e informações de Java antes de testar um grupo de atributos.

Sobre Esta Tarefa
Antes de iniciar o teste de um grupo de atributos, opcionalmente, é possível configurar variáveis de ambiente, propriedades de configuração e, onde aplicável, informações de Java a partir da janela Teste da origem de dados. As informações de Java são um subconjunto dos dados de configuração. Algumas variáveis de ambiente possuem valores especiais que são configurados por padrão para o teste de grupo de atributos. Para obter informações adicionais sobre variáveis de ambiente com valores especiais para o teste de grupo de atributos, consulte “Variáveis de Ambiente de Teste” na página 1388.

Procedimento

1. Opcional: Clique em **Configurar Ambiente** a partir da janela **Teste** da origem de dados.
   A janela **Variáveis de Ambiente** se abre. Quando preenchida, a janela **Variáveis de Ambiente** lista todas as variáveis de ambiente que são usadas durante a execução do teste. A visualização inicial da janela de variável de Ambiente contém as variáveis de ambiente existentes definidas no agente. Ela também contém quaisquer variáveis de ambiente que você incluiu nos testes anteriores deste agente.
   a) Clique em **Incluir** ou em **Editar** para incluir ou editar variáveis individuais.
   b) Clique em **Remover** para remover as variáveis individuais ou **Restaurar Padrão** para restaurar as variáveis padrão e remover todas as outras.
   c) Clique em **OK** para salvar suas mudanças e retornar à janela **Teste**.
2. Opcional: Clique em **Configuração** a partir da janela **Teste** da origem de dados. A janela **Configuração de Tempo de Execução** se abre.
   a) Clique em **Editar Configuração do Agente** para incluir uma propriedade de configuração ou para editar propriedades de configuração do agente existentes utilizando a janela **Propriedades de Configuração**.
   b) Selecione uma propriedade de configuração e clique em **Editar** para editar uma propriedade de configuração existente que está relacionado para o grupo de atributos você estiver testando.
   c) Selecione uma propriedade de configuração e clique em **Restaurar Padrão** para restaurar uma propriedade de configuração para seu valor padrão.

   Importante: Se uma origem de dados JMX se conectar a um WebSphere Application Server remoto, assegure que um WebSphere Application Server local esteja instalado e que o local de Java esteja configurado para o JRE que esse servidor usa. Para obter detalhes sobre a configuração da conexão, consulte “Monitorando MBeans Java Management Extensions (JMX)” na página 1240.
3. Clique em **OK** para salvar suas mudanças e retornar à janela **Teste**.
4. **Nota:** É possível configurar informações de Java para os seguintes tipos de grupos de atributos:
   - Java Management Extensions (JMX)
   - Java Database Connectivity (JDBC)
   - Disponibilidade de Protocolo de Transporte de Hipertexto (HTTP)
   - SOAP

- Java Application Programming Interface (API)

As informações do Java são um subconjunto dos dados de configuração descritos na etapa “2” na página 1383

Opcional: Clique em **Informações de Java** a partir da janela **Teste** da origem de dados.

A janela **Informações de Java** se abre.

a) Insira as Informações de Java.
Por exemplo, navegue para ou digite o local do Java Runtime Environment (JRE), selecione um **nível de rastreio de Java** ou insira **argumentos da JVM**

b) Clique em **OK** para salvar suas mudanças e retornar à janela **Teste**.

Teste integral de agente

Use o teste de agente integral para testar todos os grupos de atributos juntos de seu agente. Você também pode usar o teste de agente integral para testar as origens de dados que não podem ser testadas usando a função de teste do grupo de atributos.

Sobre Esta Tarefa

É possível usar o teste do agente integral para executar o agente da mesma maneira que executa no IBM Tivoli Monitoring sem precisar de uma instalação do IBM Tivoli Monitoring.

Importante: Em sistemas Windows, se quiser executar um teste completo do agente dentro do Agent Builder (consulte “Teste integral de agente” na página 1384), assegure-se de que a versão de 32 bits do sistema operacional no qual você está executando o Agent Builder, ou seja, Windows de 32 bits, esteja selecionada na janela Informações do Agente. Em sistemas Linux, a versão de 64 bits deve ser selecionada.

Procedimento

1. Abra a perspectiva **Teste do Agente**:
   a) No editor de agente, abra a guia **Informações do Agente**.
   b) Clique em **Testar o agente**.

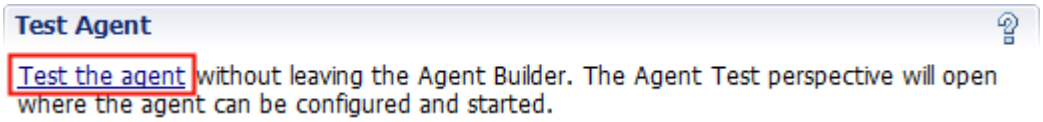


*Figura 66. Seção **Testar o Agente** do **Agent Editor**, página **Informações do Agente**.*

   Como alternativa, no menu Agent Builder, selecione **Janela** > **Abrir Perspectiva** > **Outro**, selecione **Teste de Agente** e clique em **OK**

A perspectiva **Teste do Agente** se abre (Figura 68 na página 1386). A visualização **Teste do Agente** mostra agentes que foram abertos no editor do agente; é possível testar qualquer um desses agentes. Uma visualização **Teste do Grupo de Atributos** também é exibida; essa visualização inicialmente está vazia. A visualização **Teste do Grupo de Atributos** mostra os dados que são coletados a partir de um grupo de atributos selecionado quando o agente estiver em execução.

Dica: Se nenhum agente estiver sendo editado, a perspectiva **Teste do Agente** está vazia. Para preencher a visualização, acesse a perspectiva do **IBM Tivoli Monitoring** e abra um agente no **Agent Editor**. Quando um agente for aberto no **Agent Editor**, retorne para a perspectiva de **Teste do Agente** para testar o agente.

2. Opcional: Configure as variáveis de ambiente e as propriedades de configuração antes de iniciar o teste.

   Você pode acessar as janelas **Variáveis de Ambiente** e **Configuração de Tempo de Execução** de duas maneiras a partir da visualização **Teste do Agente**:

   - Clique com o botão direito no agente na visualização **Teste do agente** para abrir um menu de seleção. É possível selecionar **Configurar Ambiente** no menu para abrir a janela **Variáveis de**

Ambiente. É possível selecionar **Configuração** no menu para abrir a janela **Configuração de Tempo de Execução**.

- Clique no ícone de menu Visualizar na barra de ferramentas da visualização **Teste do Agente** para acessar os itens de menu **Configurar Ambiente** e **Configuração** como na opção anterior.

Para obter informações sobre o uso das janelas **Variáveis de Ambiente** e **Configuração de Tempo de Execução**, consulte "Teste de Grupo de Atributos" na página 1380.

Importante:

a. O agente é preenchido automaticamente com o último conjunto de configuração que se relaciona a cada grupo de atributos testado.

b. Algumas variáveis de ambiente podem ter diferentes valores padrão para o teste de grupo de atributo e para teste de agente integral. Para obter informações adicionais sobre as variáveis de ambiente com valores especiais para o teste de grupo de atributos, consulte, ("Variáveis de Ambiente de Teste" na página 1388).

c. Se uma origem de dados JMX se conectar a um WebSphere Application Server remoto, assegure que um WebSphere Application Server local esteja instalado e que o local de Java esteja configurado para o JRE que esse servidor usa. Para obter detalhes sobre a configuração da conexão, consulte "Monitorando MBeans Java Management Extensions (JMX)" na página 1240.

d. Em uma API Java, JDBC, JMX, HTTP ou origem de dados SOAP, é possível usar a configuração **Java** > **Argumentos da JVM** para controlar a criação de logs de rastreio de agente. Defina o seguinte valor:

```
-DJAVA_TRACE_MAX_FILES=files -DJAVA_TRACE_MAX_FILE_SIZE=size
```

em que *files* é a quantidade máxima de arquivos de log de rastreio que são mantidos (o valor padrão é 4) e *size* é o tamanho máximo do arquivo de log em kilobytes (o valor padrão é 5000). Por exemplo, é possível configurar o valor a seguir:

```
-DJAVA_TRACE_MAX_FILES=7 -DJAVA_TRACE_MAX_FILE_SIZE=100
```

Neste caso, o agente grava 100 kilobytes no primeiro arquivo de log, em seguida, alterna para o segundo arquivo de log, e assim por diante. Após gravar sete arquivos de log de 100 kilobytes cada, ele sobrescreve o primeiro arquivo de log.

e. Se o seu agente tiver subnós, em uma versão instalada, será possível definir valores de configuração diferentes para diferentes subnós e separadamente para os grupos de atributos do agente base. No entanto, na configuração do teste do agente completo, é possível definir cada valor de configuração somente uma vez; a configuração se aplica ao agente base e a quaisquer subnós. É possível testar apenas uma instância de cada subnó.

3. Na visualização **Teste de Agente**, selecione o agente que deseja testar e clique no ícone  **Iniciar Agente**.

Uma janela indica que o agente está iniciando. Quando o agente é iniciado, seus grupos de atributos são mostrados como filhos do agente na visualização **Teste do Agente**. Os grupos de atributos são indicados pelo ícone de grupo de atributos  .

Os grupos de atributos de status que fornecem informações sobre o agente (**Status do Objeto de Desempenho**, **Status do Conjunto de Encadeamentos** e **Status de Executar Ação**) também são mostrados como filhos do agente na visualização **Teste do Agente**. Os grupos de atributos de status são indicadas pelo ícone de informações.

É possível iniciar e executar mais de um agente por vez.

O ícone  **Parar Agente** fica disponível quando o agente é iniciado.

Se o agente tiver subnós ou grupos navegadores, eles serão mostrados como nós na visualização **Teste do Agente**. Definições de subnó são mostradas sob o agente. Um nó da instância do subnó é

mostrado sob o nó de definição do subnó. Grupos de atributos e grupos navegadores são mostrados sob o nó da instância do subnó. Por exemplo:

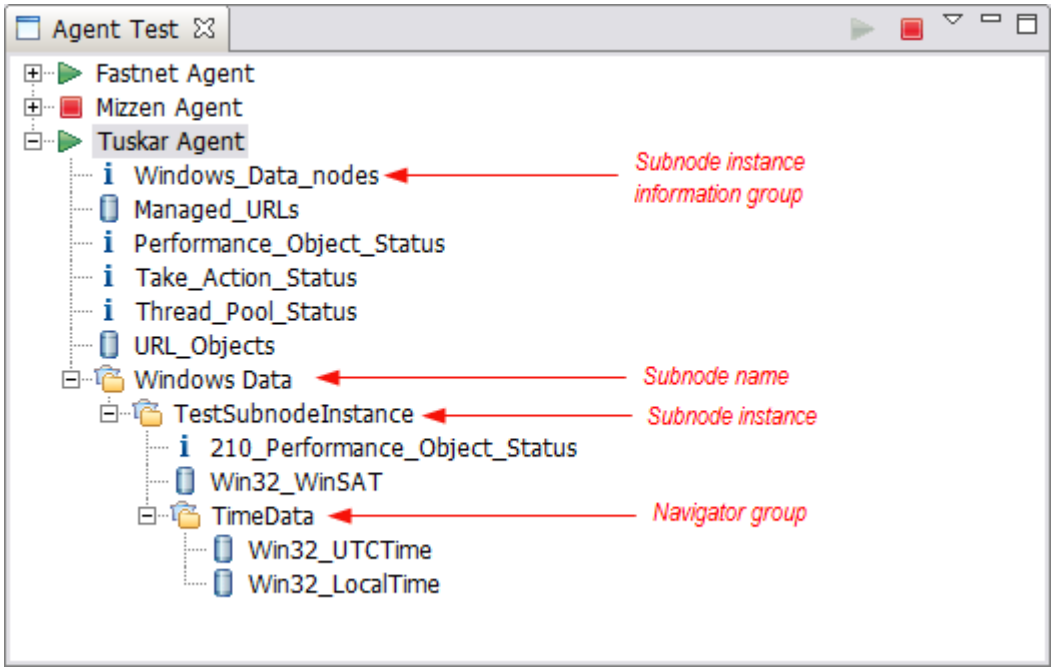


*Figura 67. Visualização **Teste do Agente** com o subnó de exemplo e o grupo de navegador destacado.*

É possível clicar com o botão direito em qualquer um dos nós na visualização **Teste do Agente** para acessar as seleções de menu, como **Editar** e **Parar Agente**. **Editar** abre a **Definição de Origem de Dados** para o nó selecionado no **Agent Editor**.

Nota: As mudanças que você efetua com o **Agent Editor** não são visíveis no agente de execução até que pare e reinicie o agente.

4. Na visualização **Teste do Agente**, selecione o primeiro grupo de atributos que deseja testar.

   Ao selecionar um grupo de atributos, uma coleta de dados é iniciada para o grupo de atributos selecionados. Se a coleta levar algum tempo, uma janela indicará que a coleta de dados está em andamento. Quando a coleta de dados for concluída, os dados coletados serão exibidos na visualização **Teste do Grupo de Atributos**, por exemplo:

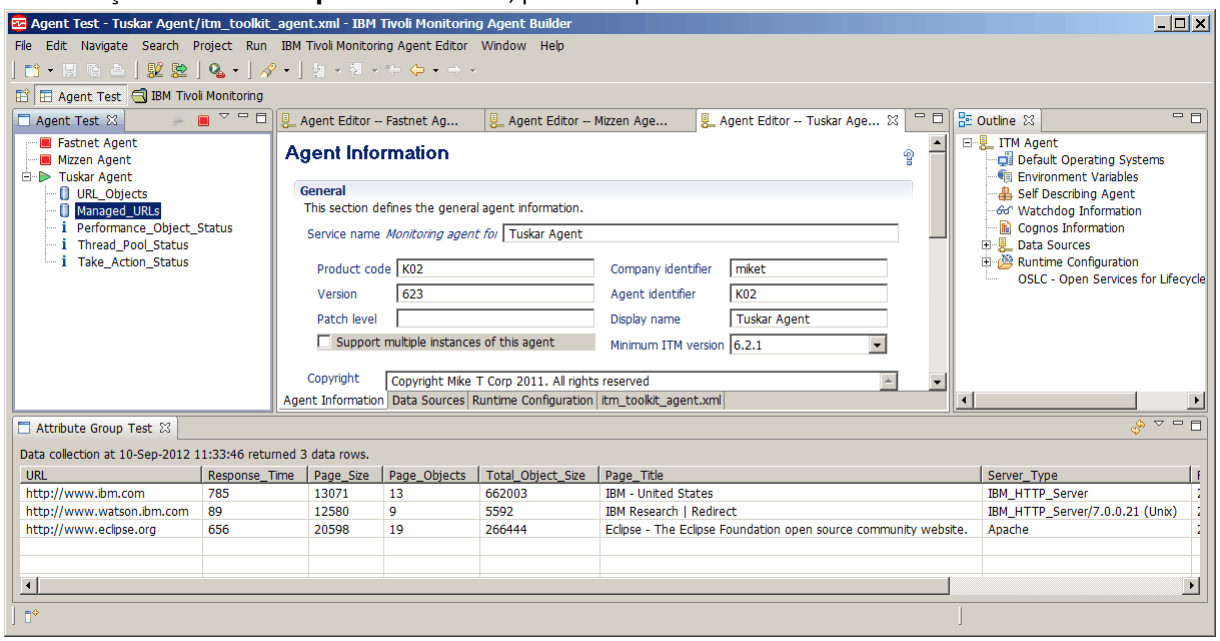


*Figura 68. Perspectiva **Teste do Agente***

Se nenhum dado for exibido, uma mensagem `0 linhas de dados retornados` é mostrada na visualização **Teste do Grupo de Atributos**. Existem vários motivos pelos quais o agente pode não retornar os dados. Esses motivos incluem:

- Não existem dados
- Definição incorreta
- Configuração incorreta

É possível verificar o motivo pelo qual nenhum dado é retornado, examinando o valor do **Error_Code** no grupo de atributos **Status do Objeto de Desempenho**. Para obter informações adicionais sobre a visualização do grupo de atributos **Status do Objeto de Desempenho**, consulte a etapa "9" na página 1387

Para coletar dados para outro grupo de atributos no agente em execução, selecione o grupo de atributos requerido.

Ao selecionar um grupo de atributos na visualização **Teste do Agente**, o grupo de atributos correspondentes é exibido na visualização **Agent Editor**.

5. Opcional: Execute uma segunda coleta de dados, após a coleta de dados inicial, para determinados tipos de grupo de atributos, para obter valores de dados úteis.

   Para executar uma coleta de dados, clique no ícone Coletar dados  na visualização **Teste de Grupo de Atributos**.

   Se a coleta levar algum tempo, uma janela indicará que uma coleta de dados está em andamento. Quando a coleta de dados estiver concluída, os dados recém-coletados serão exibidos na visualização **Teste de Grupo de Atributos**.

6. Opcional: Clique em um título da coluna do atributo na visualização **Teste do Grupo de Atributos** para abrir as **Informações de Atributo** na guia **Definição de Origem de Dados** do **Agent Editor**. Também é possível acessar as mesmas **Informações sobre o Atributo**, clicando com o botão direito em qualquer célula de dados na tabela e escolhendo **Editar** no menu.

   É possível editar propriedades do atributo de maneira anormal. As mudanças que você efetua não são visíveis no agente de execução até que pare e reinicie o agente.

7. Opcional: Você pode abrir diversas visualizações **Teste do Grupo de Atributos** ao mesmo tempo.

   Para abrir uma visualização adicional **Teste de Grupo de Atributos**, clique no ícone de menu de visualização na barra de ferramentas de visualização **Teste de Grupo de Atributos** e, em seguida, selecione **Abrir Visualização para Grupo de Atributos**.

   Nota: Quando uma visualização adicional **Teste de Grupo de Atributos** estiver aberta, ela exibirá as mesmas informações de atributo que a visualização original **Teste do Grupo de Atributos**. Em seguida, é possível selecionar outro grupo de atributos na visualização **Teste do Agente** para exibir informações diferentes do grupo de atributos na visualização **Teste do Grupo de Atributos** original. Na primeira vez em que outra visualização **Teste do Grupo de Atributos** é aberta, ele abre no mesmo local como a visualização original, mas com sua própria guia. Se desejar ver as duas visualizações simultaneamente, é possível arrastar a guia para outro local na área de trabalho.

8. Opcional: Se o seu agente tiver subnós, selecione o grupo de atributos de informações de instância do subnó para ver como os subnós são listados em seu agente (Figura 67 na página 1386). A seleção do grupo de atributos de informações da instância do subnó mostra as informações da instância do subnó na visualização **Teste do Grupo de Atributos** (para todos os subnós online do tipo selecionado).

9. Opcional: Para ver informações adicionais sobre a operação do agente, é possível selecionar os grupos de atributos **Status do Objeto de Desempenho** e **Status do Conjunto de Encadeamento** na visualização **Teste do Agente**. Esses grupos de atributos são indicados pelo ícone de informações **i**. Selecione esses grupos para ver informações de status sobre coletas de dados anteriores de seus grupos de atributos.

   Por exemplo:

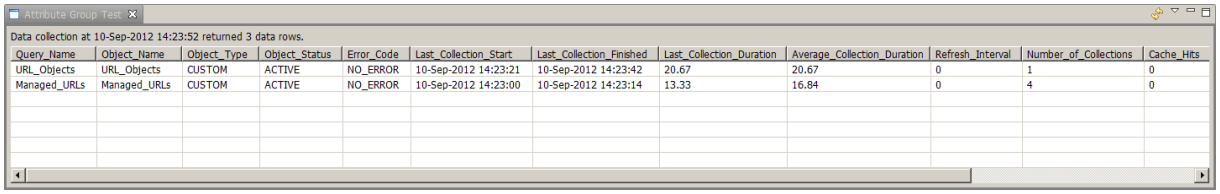


*Figura 69. A visualização **Teste do Grupo de Atributos** que mostra informações adicionas (Status do Objeto de Desempenho) sobre as coletas de dados para os grupos de atributos **Managed_URLs** e **Managed_Nodes***

10. Quando tiver terminado de testar seu agente, clique no ícone Parar agente 

Variáveis de Ambiente de Teste

Use essas variáveis de ambiente para controlar o comportamento do agente durante o teste.

As variáveis de ambiente são valores nomeados dinâmicos que determinam como o agente é executado. Para teste de grupo de atributos, algumas variáveis de ambiente do agente são configuradas para os valores especiais. Os valores especiais são usados para que o agente responda de maneira que ajuste o teste de um único grupo de atributos. Para o teste de gente integral, os valores especiais não são usados e, em vez disso, os valores padrão são usados. Os valores padrão significam que o agente se comporta normalmente, o que é mais apropriado para o teste de agente integral.

As variáveis de ambiente que possuem os valores especiais para teste de grupo do atributo são resumidos na tabela a seguir. Para obter informações adicionais sobre todas as variáveis de ambiente de agente, consulte ("Lista de variáveis de ambiente" na página 1175). Para obter informações adicionais sobre a configuração das variáveis de ambiente, consulte ("Variáveis de ambiente" na página 1175).

Tabela 299. Variáveis de ambiente

Variável de ambiente	Valor padrão (teste de agente integral)	Valor de teste do grupo de atributos	Motivo para valor alterado para o teste de grupo de atributos
CDP_DP_INITIAL_COLLECTION_DELAY	varies	1	Este valor se aplica a um agente com um conjunto de encadeamentos. Esse valor é o tempo em segundos que o conjunto de encadeamentos espera antes que a solicitação de coleta de dados inicial seja enviada a um provedor de dados. **Nota:** Se CDP_DP_INITIAL_COLLECTION_DELAY não é configurado, o conjunto de encadeamentos aguarda por um tempo que é especificado pelo CDP_DP_REFRESH_INTERVAL ou CDP_ATTRIBUTE_GROUP_REFRESH_INTERVAL. Esse tempo de espera é o mesmo tempo o conjunto de encadeamento aguarda entre coletas de dados, e pode ser muito longo para aguardar a primeira coleta de dados.
CDP_DP_CACHE_TTL	55	1	Quando configurado como 1, uma solicitação Coletar Dados tem muita probabilidade de fazer com que o provedor de dados colete os dados imediatamente. Caso contrário, pode retornar dados em cache que tem até 60 segundos de idade.

Instalando o agente em uma infraestrutura de monitoramento para teste e uso

Depois de testar o agente no Agent Builder, é possível instalar o agente em um ambiente existente do IBM Tivoli Monitoring ou do IBM Cloud Application Performance Management para fazer mais testes e para uso.

A instalação e o teste do agente em uma infraestrutura de monitoramento apresenta os seguintes benefícios:

- É possível configurar e testar diversas instâncias de um agente que são executadas simultaneamente.
- É possível configurar e testar diversas instâncias de subnós que são executadas simultaneamente.
- Em um Tivoli Monitoring de ambiente, você pode construir espaços, situações, ações e consultas no Tivoli Enterprise Portal .

Importante: Implemente versões iniciais de seu agente em uma versão de teste da infraestrutura de monitoramento. No Tivoli Monitoring, use um servidor de monitoramento e um servidor de portal separado. No Cloud APM, use uma conta de nuvem de teste ou uma implementação de teste separada do servidor de monitoramento no local. Implemente a versão final do seu agente em uma infraestrutura de produção.

Se você implementar uma versão do agente na infraestrutura de monitoramento de produção e, em seguida, mudar quaisquer conjuntos de dados no agente, a nova versão poderá conflitar com a versão mais antiga do servidor. Neste caso, pode ser impossível usar qualquer versão do agente.

Instalando um agente

Há dois métodos para instalar os agentes criados com o Agent Builder.

1. Para testar o agente com uma infraestrutura de monitoramento que está em execução no mesmo sistema que o Agent Builder, é possível instalar o agente na instalação local do Tivoli Monitoring ou Cloud APM.
2. Para testar ou usar o agente com um sistema Tivoli Monitoring ou Cloud APM que não esteja em execução no mesmo sistema que o Agent Builder, é possível gerar um arquivo compactado (*pacote de agente*) que pode ser transferido para outros sistemas e ser implementado.

Nota:

1. Com o Tivoli Monitoring, após instalar um agente, será possível ver métricas de desempenho nas tabelas do Tivoli Enterprise Portal. Para o suporte de situações ou áreas de trabalho, consulte “Importando Arquivos de Suporte do Aplicativo” na página 1406.
2. Com o Tivoli Monitoring, após instalar o agente, será possível usar o Tivoli Enterprise Portal para verificar os dados do agente. Para obter mais informações, consulte “Mudanças no Tivoli Enterprise Portal” na página 1400. Se após visualizar os dados no Tivoli Enterprise Portal, você quiser modificar o agente, consulte “Usando o Agent Editor para modificar o agente” na página 1172.
3. Para um agente que suporte Linux ou UNIX, gere a imagem do instalador em um sistema Linux ou UNIX, pois um sistema Linux ou UNIX cria os arquivos com as permissões apropriadas.

Instalando um agente localmente

Instale o agente em um ambiente de monitoramento no sistema local no qual o Agent Builder está em execução.

Sobre Esta Tarefa

Conclua as etapas a seguir para instalar o agente em um ambiente de monitoramento no sistema local:

1. Clique no arquivo `itm_toolkit_agent.xml`, na árvore de navegação do Explorador de Projetos do Agent Builder, usando um dos métodos a seguir:
   a. Clique com o botão direito no arquivo `itm_toolkit_agent.xml` e selecione **IBM** > **Gerar agente**.

b. Selecione o arquivo `itm_toolkit_agent.xml` e selecione o ícone  **Gerar Agente** na barra de ferramentas.

c. Dê um clique duplo no arquivo `itm_toolkit_agent.xml` e selecione **Agent Editor** > **Gerar Agente**.

2. Na janela **Assistente Gerar Agente**, na seção **Instalar o Agente Localmente**, insira o diretório de instalação para a infraestrutura de monitoramento. O Agent Builder completa o valor que está localizado na variável de ambiente `CANDLE_HOME`. Se esta variável não for configurada, o valor padrão para Windows, `C:\IBM\ITM`, será exibido.

   As caixas de seleção são ativadas como a seguir:

   Instalar o agente
   Ativado se o Agent Builder detectar um Tivoli Enterprise Monitoring Agent apropriado ou um agente IBM Cloud APM no local especificado. Um agente apropriado é aquele que suporta o sistema operacional local e tem a versão mínima correta.

   Instalar o Suporte do TEMS
   Ativado em um ambiente do Tivoli Monitoring se o Agent Builder detectar um Tivoli Enterprise Monitoring Server no local especificado.

   Instalar o Suporte do TEPS
   Ativado em um ambiente do Tivoli Monitoring se o Agent Builder detectar um Tivoli Enterprise Portal Server no local especificado.

3. Selecione os componentes para instalação (agente, suporte do Tivoli Enterprise Monitoring Server, suporte do Tivoli Enterprise Portal Server).

4. Em um ambiente Tivoli Monitoring, se o Tivoli Enterprise Monitoring Server ou o Tivoli Enterprise Portal Server estiver instalado no computador local e você estiver instalando os arquivos de suporte para esses servidores, será possível escolher se reiniciar os servidores.

   Neste caso, as caixas de seleção **Reiniciar o TEMS sem credenciais** e **Reiniciar TEPS** ficam ativas na seção **Instalar o Agente Localmente** do assistente Gerar Agente. É possível desmarcar as caixas de seleção para instalar o suporte sem reciclar os servidores.

   Ao desmarcar a caixa de seleção **Reiniciar o TEMS sem credenciais**, será solicitado o ID do usuário e a senha do Tivoli Enterprise Monitoring Server. Insira esses detalhes e clique em **Logon**. Se você estiver usando o Tivoli Monitoring com a segurança desligada, insira "sysadmin" para o ID do usuário, deixe a senha em branco e clique em **Logon**.

   Como alternativa, para continuar sem inserir credenciais, clique em **Logon** sem especificar um ID de usuário e senha ou clique em **Cancelar**. Se você concluir essas etapas, o Tivoli Enterprise Monitoring Server será reciclado.

   Importante: Para instalar arquivos de suporte sem reciclar o Tivoli Enterprise Monitoring Server, certifique-se de que o Tivoli Enterprise Monitoring Server esteja em execução.

5. Selecione os componentes do agente para gerar. É possível selecionar **Agente base**, **Relatório Cognos** ou ambos.

6. Em um ambiente do IBM Cloud APM, é possível fornecer assinatura de segurança para agentes autoexplicativos. Clique em **Editar todas as preferências de assinatura do JAR**. É possível incluir um registro de data e hora em arquivos JAR assinados e especificar a autoridade do registro de data e hora. Especifique os detalhes sobre Arquivo Keystore do Java.

   Nota: Deve-se criar o arquivo keystore Java usando as ferramentas Java. Por exemplo, para gerar uma chave privada e um certificado com uma chave pública correspondente em um Arquivo keystore Java, é possível executar este comando:

   - *ab_install_path*`/jre/bin/keytool -genkeypair -keystore` *keystore_file_path* `-storepass` *key_store_password* `-alias` *key_store_alias* `-dname "CN=`*common_name*`, OU=`*organizational_unit*`, L=`*city_or_locality*`, ST=`*state_or_province*`, C=`*country*`" -keypass` *key_password*

   Em que:

- *ab_install_path* é o local no qual o Agent Builder está instalado
- *keystore_file_path* é o caminho em que um keystore JKS existente está localizado ou onde um será criado
- *key_store_password* é a senha que é necessária para acessar quaisquer itens nesse keystore
- *key_store_alias* é um nome que identifica esta chave dentro do keystore (padronizado para `"mykey"`)
- *key_password* a senha que é necessária para acessar essa determinada chave (padronizado para `key_store_password`)

O certificado deve ser incluído no keystore para o servidor.

7. Ao concluir os detalhes de **Assinatura do JAR**, clique em **OK**.
8. Clique em **Concluir**.
9. Configure e inicie o agente. Para obter mais informações, consulte "Configurando e iniciando o agente em um ambiente IBM Tivoli Monitoring" na página 1394 ou "Configurando o agente" na página 1395 e "Iniciando e parando o agente" na página 1396 em um ambiente do IBM Cloud APM.

   Para o Tivoli Monitoring v6.2 FP1 ou mais recente, será possível instalar o suporte do Tivoli Enterprise Monitoring Server e do Tivoli Enterprise Portal Server sem reiniciar os servidores. Neste caso, as caixas de seleção **Reiniciar o TEMS sem credenciais** e **Reiniciar TEPS** ficam ativas na seção **Instalar o Agente Localmente** do assistente Gerar Agente. É possível desmarcar as caixas de seleção para instalar o suporte sem reciclar os servidores. Ao desmarcar a caixa de seleção **Reiniciar o TEMS sem credenciais**, será solicitado o ID do usuário e a senha do Tivoli Enterprise Monitoring Server. Insira o ID de usuário e a senha do Tivoli Enterprise Monitoring Server e clique em **Logon**. Se você estiver usando o Tivoli Monitoring com a segurança desligada, insira "sysadmin" para o ID do usuário, deixe a senha em branco e clique em **Logon**. Você também pode continuar sem inserir as credenciais (clique em **Logon** sem especificar um ID de usuário e uma senha ou clique em **Cancelar**. Isso faz com que o Tivoli Enterprise Monitoring Server seja reciclado).

   Nota: O Tivoli Enterprise Monitoring Server deve estar em execução para poder instalar os arquivos de suporte sem reciclar o Tivoli Enterprise Monitoring Server.

Criando o pacote de agente

É possível usar o Agent Builder para criar um pacote de instalação do agente compactado.

Sobre Esta Tarefa

Um pacote de agente contém todas as multas necessárias para executar o agente, bem como os scripts de instalação e configuração. O pacote também inclui arquivos de suporte para o ambiente de monitoramento.

É possível usar um pacote de agente para instalar o agente em ambientes IBM Tivoli Monitoring e IBM Cloud Application Performance Management.

Procedimento

1. Clique no arquivo `itm_toolkit_agent.xml` na árvore de navegação **Explorador de Projetos** do Agent Builder usando um dos seguintes métodos:
   - Clique com o botão direito no arquivo `itm_toolkit_agent.xml` e selecione **IBM** > **Gerar agente**.
   - Selecione o arquivo `itm_toolkit_agent.xml` e selecione o ícone  **Gerar Agente** na barra de ferramentas.
   - Dê um clique duplo no arquivo `itm_toolkit_agent.xml` e selecione **Editor do agente** > **Gerar agente**.
2. Insira o nome do diretório no qual você deseja colocar a saída (um pacote compactado ou expandido arquivos) no **Gerar Imagem do Agente** seção.
3. Selecione **Manter arquivos intermediários** caixa para manter os arquivos separados expandidos gerados a partir do arquivo zip ou tar.

4. Selecione a caixa de opção **Criar um Arquivo ZIP** para criar um arquivo compactado no diretório especificado. O arquivo zip compactado é chamado `smai-agent_name-version.zip` para Windows sistemas por padrão.
5. Selecione a caixa de opção **Criar um Arquivo TAR** para criar um arquivo tar no diretório especificado. Por padrão, o arquivo tar compactado é denominado `smai-agent_name-version.tgz` para sistemas UNIX e Linux.
6. Selecione os componentes do agente para gerar. É possível selecionar **Agente base**, **Relatório Cognos** ou ambos.

   Importante: Para o ambiente do IBM Cloud Application Performance Management , não selecione **Cognos Reporting**, porque os relatórios são Atualmente não suportado e incluindo os relatórios aumenta o tamanho do Pacote .
7. Como opção, é possível fornecer assinatura de segurança para arquivos de aplicativo do agente. Se desejar fornecer assinatura de segurança, selecione **Assinar JAR de suporte autoexplicativo**. Clique em **Editar todas as preferências de assinatura do JAR**. É possível incluir um registro de data e hora em arquivos JAR assinados e especificar a autoridade do registro de data e hora. Especifique os detalhes sobre Arquivo Keystore do Java.

   Importante: É possível criar o Arquivo keystore Java usando as ferramentas Java. Por exemplo, para gerar uma chave privada e um certificado com uma chave pública correspondente em um Arquivo keystore Java, é possível executar este comando:

   - `ab_install_path/jre/bin/keytool -genkeypair -keystore keystore_file_path -storepass key_store_password -alias key_store_alias -dname "CN=common_name, OU=organizational_unit, L=city_or_locality, ST=state_or_province, C=country" -keypass key_password`

   Em que:

   - *ab_install_path* é o local no qual o Agent Builder está instalado
   - *keystore_file_path* é o caminho no qual um armazenamento de chaves JKS existente reside ou onde um será criado
   - *key_store_password* é a senha necessária para acessar quaisquer itens neste armazenamento de chaves
   - *key_store_alias* é um nome que identifica essa chave dentro do armazenamento de chaves (padrão é `"mykey"`)
   - *key_password* é a senha necessária para acessar essa chave específica (é padronizado para `key_store_password`)

   Inclua esse certificado no armazenamento de chaves do servidor.
8. Clique em **Concluir**.

Instalando o pacote em um ambiente do IBM Tivoli Monitoring
Para testar ou usar o agente no ambiente do IBM Tivoli Monitoring , use o pacote gerado para instalar o agente nos sistemas monitorados, hub Sistemas Monitoring Server e Portal Server Sistema .

Antes de Iniciar
Antes de instalar o agente em um sistema monitorado, certifique-se de que o Tivoli Monitoring agente do sistema operacional está presente e funcionando. Para obter informações sobre como instalar os agentes Tivoli Monitoring, consulte Instalando agentes de monitoramento no Knowledge Tivoli Monitoring Centro Tivoli Monitoring Centro.

Importante: Para exibir informações do agente no Tivoli Enterprise Portal, deve-se instalar os seguintes componentes:

- O agente em todos os sistemas monitorados
- Tivoli Enterprise Monitoring Server suporta arquivos no hub Tivoli Enterprise Monitoring Servers
- Tivoli Enterprise Portal Server suporta arquivos no Tivoli Enterprise Portal Server

- Arquivos de suporte do Tivoli Enterprise Portal no Tivoli Enterprise Portal Server e, se aplicável, nos clientes de desktop do Tivoli Enterprise Portal

Procedimento

1. Copie o arquivo compactado, que é denominado *product_code*.zip para Windows sistemas ou *product_code*.tgz para UNIX e Linux sistemas por padrão, no sistema em que você Quer instalar o Agente .
2. Extraia o arquivo para um local provisório.

   Nota: Linux AIX Para UNIX e Linux sistemas, esse local temporário não pode ser /tmp/*product_code*, em que o código do produto é em minúscula.

   Você pode instalar o agente remotamente usando o arquivo compactado.

   - Linux Em um sistema Linux, use o comando a seguir para extrair o arquivo .tgz:

     ```
     tar -xvzf filename
     ```

   - UNIX Em um sistema AIX, use o comando a seguir para extrair o arquivo .tgz:

     ```
     gunzip filename
     tar -xvf filename
     ```

3. Execute o script de instalação apropriado.
   - Para instalar o suporte do agente, do Tivoli Enterprise Monitoring Server, do Tivoli Enterprise Portal Server e do Tivoli Enterprise Portal todos ao mesmo tempo:

     ```
     InstallIra.bat/.sh itm_install_location [[-h Hub_TEMS_hostname] -u
     HUB_TEMS_username -p Hub_TEMS_password]
     ```

   - Para instalar o agente sem instalar arquivos de suporte:

     ```
     installIraAgent.bat/.sh itm_install_location
     ```

   - Para instalar o suporte do Tivoli Enterprise Monitoring Server:

     ```
     installIraAgentTEMS.bat/.sh itm_install_location [[-h Hub_TEMS_hostname] -u
     HUB_TEMS_username -p Hub_TEMS_password]
     ```

   - Para instalar o suporte Tivoli Enterprise Portal Server e Tivoli Enterprise Portal:

     ```
     installIraAgentTEPS.bat/.sh itm_install_location
     ```

   O local da instalação *itm_install_location* deve ser o primeiro argumento e é obrigatório em todos os scripts: installIra.bat/.sh, installIraAgent.bat/.sh, installIraAgentTEMS.bat/.sh e installIraAgentTEPS.bat/.sh. Este é o local onde os componentes Tivoli Monitoring estão instalados neste sistema.

   Outros argumentos são opcionais.

   Se você instalar o Monitoring Server suporta arquivos e não fornecer um ID do usuário não for fornecido, o Tivoli Enterprise Monitoring Server seja reciclado.
4. Configure e inicie o agente; consulte “Configurando e iniciando o agente em um ambiente IBM Tivoli Monitoring” na página 1394.

O que Fazer Depois

Se você alterou o layout do agente de uma maneira que faz com que os itens do navegador sejam movidos ou removidos, reinicie o Tivoli Enterprise Portal Server e o Tivoli Enterprise Portal. A reinicialização assegura que suas alterações sejam corretamente reconhecidas.

Configurando e iniciando o agente em um ambiente IBM Tivoli Monitoring
Depois de instalar um agente em um sistema monitorado no IBM Tivoli Monitoring, configure e inicie o agente.

Procedimento

1. Abra **Gerenciar Tivoli Monitoring Service**.
   A nova entrada **Monitorando Agente para *agent_name*** é exibido.
2. Clique com o botão direito do mouse na entrada e selecione **Configurar Utilizando Padrões**. Clique em **OK** para aceitar os padrões, se solicitado.

   Importante:

   a. Em sistemas UNIX , a opção a ser selecionada é **Configurar**.
   b. Para agentes de várias instâncias, quando estiver configurando, será solicitado um nome da instância.

   Dica: Se seu agente usar uma origem de dados JMX para se conectar a um WebSphere Application Server remoto, assegure-se de que o WebSphere Application Server também esteja instalado no host que está executando o agente e defina a configuração `Início do Java` para o Java Runtime Environment usado pelo WebSphere Application Server local.

   Dica: Para uma API Java, JDBC, JMX, HTTP ou origem de dados SOAP, é possível usar a configuração **Java** > **Argumentos da JVM** para controlar a criação de logs de rastreio de agente. Defina o seguinte valor nesta configuração:

   ```
   -DJAVA_TRACE_MAX_FILES=files -DJAVA_TRACE_MAX_FILE_SIZE=size
   ```

   Em que *files* é o número máximo de arquivos de log de rastreio que são mantidos (o valor padrão é 4) e *size* é o tamanho máximo do arquivo de log em kilobytes (o valor padrão Estado Islâmico 5000) . Por exemplo, é possível configurar o valor a seguir:

   ```
   -DJAVA_TRACE_MAX_FILES=7 -DJAVA_TRACE_MAX_FILE_SIZE=100
   ```

   Neste caso, o agente grava 100 kilobytes no primeiro arquivo de log, em seguida, alterna para o segundo arquivo de log, e assim por diante. Após gravar sete arquivos de log de 100 kilobytes cada, ele sobrescreve o primeiro arquivo de log.

   Se você incluiu elemento de configuração de tempo de execução em seu agente, ou se você selecionou uma origem de dados, então serão apresentados os painéis de configuração. Utilize esses painéis para coletar as informações necessárias para seu agente.
3. Clique com o botão direito na entrada do agente e selecione **Iniciar**
4. Abra o Tivoli Enterprise Portal e acesse o novo agente.

Instalando e usando um agente em um ambiente do IBM Cloud Application Performance Management
Para testar ou usar o agente no ambiente do IBM Cloud Application Performance Management, use o pacote gerado para instalar o agente em todos os sistemas monitorados. Em alguns casos, é necessário configurar o agente antes que ele possa ser iniciado. Você pode iniciar e parar o agente conforme necessário.

Instalando o agente
Use o pacote de instalação preparado pelo Agent Builder para instalar o agente em todos os sistemas monitorados.

Antes de Iniciar
Assegure que um agente para o IBM Cloud Application Performance Management, geralmente o agente do sistema operacional, já esteja presente no sistema monitorado e funcionando.

Windows Em sistemas Windows, use um shell de linha de comandos do Administrador para instalar e configurar agentes. Para iniciar um shell de Administrador, selecione **Prompt de Comandos** a partir do menu Programas do Windows, clique com o botão direito e clique em **Executar como Administrador**.

Procedimento

1. Extraia o pacote para um diretório temporário e mude para esse diretório.
2. Instale o agente usando o comando a seguir, dependendo de seu sistema operacional:
   - Windows Em sistemas Windows, `installIraAgent.bat` *`agent_install_location`*
   - Linux AIX Em sistemas Linux e UNIX, `./installIraAgent.sh` *`agent_install_location`*

   Em que *agent_install_location* é o local de instalação do agente existente. O local padrão é:
   - Windows Nos sistemas Windows, `C:\IBM\APM`
   - Linux Nos sistemas Linux, `/opt/ibm/apm/agent`
   - AIX Em sistemas AIX, `/opt/ibm/apm/agent`

   Importante: Se você tiver incluído quaisquer propriedades de configuração customizadas no **Configuração de Tempo de Execução** janela do Agent Editor, se o agente suportar diversas instâncias, ou se o agente usa qualquer Origem de dados predefinida que precisa de configuração (por exemplo, um ID do usuário e senha), você deve configurar o agente antes de poder Início . Se um agente não precisar de configuração, ele será iniciado automaticamente após a instalação.

Configurando o agente

Se você tiver incluído quaisquer propriedades de configuração customizadas na janela Configuração de tempo de execução do Agent Editor, se o agente suportar várias instâncias, ou se o agente usar qualquer origem de dados predefinida que precise de configuração (por exemplo, um ID de usuário e senha), deve-se configurar o agente antes que ele possa ser iniciado.

Antes de Iniciar

Windows Em sistemas Windows, use um shell de linha de comandos do Administrador para instalar e configurar agentes. Para iniciar um shell de Administrador, selecione **Prompt de Comandos** a partir do menu Programas do Windows, clique com o botão direito e clique em **Executar como Administrador**.

Sobre Esta Tarefa

No processo de configuração, é possível:

- Configurar o nome da instância para criar ou alterar uma instância, se o agente suportar diversas instâncias.
- Configure qualquer propriedade de configuração que esteja disponível para o agente.
- Criar e configurar sobnós, se o agente suportar subnós.

Windows Em sistemas Windows, para configurar qualquer propriedade de configuração ou criar qualquer subnó, deve-se usar o procedimento de configuração silenciosa. Um arquivo de resposta de configuração silenciosa de amostra está localizado no diretório *`install_dir`*`\samples` e é denominado *`agentname`*`_silent_config.txt`. Crie uma cópia desse arquivo e configure as variáveis de configuração conforme necessário.

Linux AIX Em sistemas Linux e UNIX, é possível usar opcionalmente o procedimento de configuração silenciosa. Alternativamente, é possível usar o procedimento interativo. Se você iniciar o comando de configuração sem um nome de arquivo de resposta, o utilitário de configuração solicita os valores de configuração.

Procedimento

1. Mude para o diretório *install_dir*/bin.
2. Execute o comando a seguir para configurar o agente:
   - Se o agente não suporta várias instâncias:
     - Windows Em sistemas Windows, *name*-agent.bat config [*response_file*]
     - Linux AIX Em sistemas Linux e UNIX, ./*name*-agent.sh config [*response_file*]
   - Se o agente suporta várias instâncias:
     - Windows Em sistemas Windows, *name*-agent.bat config *instance_name* [*response_file*]
     - Linux AIX Em sistemas Linux e UNIX, ./*name*-agent.sh config *instance_name* [*response_file*]

   Em que:

   - *instance_name* é o nome da instância. Se uma instância com esse nome não existe, a instância é criada. Se a instância já existe, ela é reconfigurada. Deve-se criar pelo menos uma instância para usar o agente.
   - *response_file* é o nome do arquivo de resposta de configuração silenciosa.

   Dica: Se seu agente usar uma origem de dados JMX para se conectar a um WebSphere Application Server remoto, assegure-se de que o WebSphere Application Server também esteja instalado no host que está executando o agente e defina a configuração Início do Java para o Java Runtime Environment usado pelo WebSphere Application Server local.

   Dica: Para uma API Java, JDBC, JMX, HTTP ou origem de dados SOAP, é possível usar a configuração **Java** > **Argumentos da JVM** para controlar a criação de logs de rastreio de agente. Defina o seguinte valor nesta configuração:

   ```
   -DJAVA_TRACE_MAX_FILES=files -DJAVA_TRACE_MAX_FILE_SIZE=size
   ```

   Em que *files* é o número máximo de arquivos de log de rastreio que são mantidos (o valor padrão é 4) e *size* é o tamanho máximo do arquivo de log em kilobytes (o valor padrão Estado Islâmico 5000) . Por exemplo, é possível configurar o valor a seguir:

   ```
   -DJAVA_TRACE_MAX_FILES=7 -DJAVA_TRACE_MAX_FILE_SIZE=100
   ```

   Neste caso, o agente grava 100 kilobytes no primeiro arquivo de log, em seguida, alterna para o segundo arquivo de log, e assim por diante. Após gravar sete arquivos de log de 100 kilobytes cada, ele sobrescreve o primeiro arquivo de log.

Iniciando e parando o agente

Para monitorar um sistema, certifique-se de que o agente esteja iniciado no sistema. É possível iniciar e parar o agente a qualquer momento. Se o agente suportar várias instâncias, é possível iniciar e parar cada instância independentemente.

Procedimento

1. Mude para o diretório *install_dir*/bin.
2. Execute o comando a seguir para iniciar o agente:
   - Se o agente não suporta várias instâncias:
     - Windows Em sistemas Windows, *name*-agent.bat start
     - Linux AIX Em sistemas Linux e UNIX, ./*name*-agent.sh start
   - Se o agente suporta várias instâncias:

- Windows Em sistemas Windows, *name*`-agent.bat start` *instance_name*
- Linux AIX Em sistemas Linux e UNIX, `./`*name*`-agent.sh start` *instance_name*

3. Execute o comando a seguir para parar o agente:
   - Se o agente não suporta várias instâncias:
     - Windows Em sistemas Windows, *name*`-agent.bat stop`
     - Linux AIX Em sistemas Linux e UNIX, `./`*name*`-agent.sh stop`
   - Se o agente suporta várias instâncias:
     - Windows Em sistemas Windows, *name*`-agent.bat stop` *instance_name*
     - Linux AIX Em sistemas Linux e UNIX, `./`*name*`-agent.sh stop` *instance_name*

Resultados de Pós-geração e Instalação do Agente

A instalação de um agente do Agent Builder cria e muda alguns arquivos no sistema. Em um ambiente do IBM Tivoli Monitoring , você também pode ver as mudanças no Tivoli Enterprise Portal.

Novos Arquivos em Seu Sistema

Após gerar e instalar o agente criado com o Agent Builder, será possível ver os novos arquivos a seguir em seu sistema de agente:

Nota: *xx* denota o código do produto de dois caracteres.

Windows

Sistemas Windows:

TMAITM6\k*xx*agent.exe
Binário do agente

TMAITM6\K*xx*ENV
Configurações da variável de ambiente

TMAITM6\K*xx*.ref
Configuração do Agent Provider

TMAITM6\SQLLIB\k*xx*.his
Descrição SQL de informações sobre o atributo do agente

TMAITM6\SQLLIB\k*xx*.atr
Informações sobre o atributo do agente

TMAITM6*xx*_dd_*version*.xmll
Descrição do produto

TMAITM6*xx*_dd.properties
Nome do produto

TMAITM6\kxxcma.ini
Arquivo de definição de serviço do agente

TMAITM6*seus arquivos*
Arquivos suplementares incluídos a partir da API Java ou das origens de dados do Soquete com um tipo de arquivo *executable* ou *library*. Scripts incluídos a partir das origens de dados de código de retorno do Script ou do Comando.

Linux AIX

Sistemas UNIX/Linux:

registry/*xx*architecture.ver
Versões internas e arquivos de pré-requisito

***architecture*/*xx*/bin/*xx*_dd_*version*.xml**
Descrição do produto

***architecture*/*xx*/bin/k*xx*agent**
Binário do agente

***architecture*/*xx*/bin/*xx*_dd.properties**
Nome do produto

***architecture*/*xx*/work/k*xx*.ref**
Configuração do Agent Provider

***architecture*/*xx*/tables/ATTRLIB/k*xx*.atr**
Informações sobre o atributo do agente

***architecture*/*xx*/hist/k*xx*.his**
Descrição SQL de informações sobre o atributo do agente

architecture*/*xx*/bin/*your files
Arquivos Complementares incluídos a partir da Java API ou origens de dados do Soquete com um tipo de arquivo de *executable*. Scripts incluídos a partir das origens de dados de código de retorno do Script ou do Comando.

architecture*/*xx*/lib/*your files
Arquivos Complementares incluídos a partir da Java API ou origens de dados do Soquete com um tipo de arquivo de Biblioteca.

config/.*xx*.rc
Arquivo de configuração interna

config/*xx*.environment
Configurações do ambiente

config/*xx*_dd_*version*.xml
Descrição do produto

config/*xx*_dd.properties
Nome do produto

config/.ConfigData/k*xx*env
Configurações da variável de ambiente

Nota: Execute o comando a seguir para descobrir a arquitetura do sistema:

```
cinfo -p xx
```

em que *xx* é o código do produto de dois caracteres.

Por exemplo, para um sistema Solaris 8 de 64 bits que está executando um agente com código do produto 19, aqui está a saída:

```
# /opt/ibm/apm/agent/bin/cinfo -p 19

*********** Fri Aug 17 11:23:58 EDT 2007 ******************
User : root Group: other
Host name : guadalajara Installer Lvl:06.20.00.00
CandleHome: /opt/IBM/ITM
***********************************************************
Platform codes:
sol286 : Current machine
sol286 : Product (19)
tmaitm6/sol286 : CT Framework (ax)
```

A linha em negrito é a relevante. A sequência antes dos dois pontos, `sol286`, indica a arquitetura em uso para esse agente. Essa sequência é diferente das combinações de sistema operacional e tipo de hardware do computador. O agente deve ser instalado anteriormente para este recurso funcione.

Os arquivos a seguir são para origens de dados baseadas em Java. Estes arquivos são criados somente se o agente contiver origens de dados JMX, JDBC, HTTP ou SOAP:

- `cpci.jar`

- `jlog.jar`
- `common/jatlib-1.0.jar`

Os arquivos a seguir são para o suporte de tempo de execução de JMX. Estes arquivos são criados somente se o agente contiver origens de dados JMX:

- `common/jmx-1.0.jar`
- `common/connectors/jboss/connJboss-1.0.jar`
- `common/connectors/jsr160/connJSR160-1.0.jar`
- `common/connectors/was/connWas-1.0.jar`
- `common/connectors/weblogic/connWeblogic-1.0.jar`

O arquivo a seguir oferece suporte para o tempo de execução JDBC. Estes arquivos são criados somente se o agente contiver origens de dados JDBC:

- `common/jdbc-1.0.jar`

O arquivo a seguir oferece suporte para o tempo de execução HTTP ou SOAP. Estes arquivos são criados somente se o agente contiver origens de dados HTTP ou SOAP:

- `http-1.0.jar`

Os arquivos a seguir são para suporte de tempo de execução da API Java. Estes arquivos são criados somente se o agente contiver uma origem de dados da API Java:

- `cpci.jar`
- `custom/`*`your JAR file`* O nome desse arquivo JAR é especificado nas **Configurações Globais** de uma origem de dados da API Java.
- `custom /`*`your JAR file`* Arquivos Suplementares com um tipo de arquivo Java do recurso.

Os mesmos arquivos existem em sistemas Windows, UNIX e Linux para origens de dados baseada em Java, mas eles estão em diretórios diferentes:

- Windows Caminho do Windows: `TMAITM6\kxx\jars`
- Linux AIX Caminho do UNIX/Linux: *`architecture`*`/`*`xx`*`/jars`

Os arquivos a seguir são para suporte a monitoramento de arquivo de log no tempo de execução. Estes arquivos são criados somente se o agente tiver origens de dados de arquivo de log:

- Windows Nos sistemas Windows: TMAITM6\kxxudp.dll
- Linux Nos sistemas Solaris/Linux: *architecture*/*xx*/lib/libkxxudp.so
- Nos sistemas HP-UX: *architecture*/*xx*/lib/libkxxudp.sl
- UNIX Nos sistemas AIX: *architecture*/*xx*/lib/libkxxudp.a

Os arquivos a seguir são para suporte a monitoramento de script SSH no tempo de execução. Estes arquivos são criados somente se o agente contiver uma origem de dados de script ativada para da coleção de SSH:

- Windows Em sistemas Windows: `TMAITM6\kxxssh.dll`
- Linux Em sistemas Solaris/Linux: *`architecture`*`/`*`xx`*`/lib/libkxxssh.so`
- Em sistemas HP-UX: *`architecture`*`/`*`xx`*`/lib/libkxxssh.sl`
- UNIX Em sistemas AIX: *`architecture`*`/`*`xx`*`/lib/libkxxssh.a`

Mudanças na janela Gerenciar Serviços do Tivoli Enterprise Monitoring

Depois de instalar um agente em um ambiente do IBM Tivoli Monitoring , você pode ver uma entrada para o agente no **Gerenciar Tivoli Enterprise Monitoring Services** Janela . O nome da entrada é **Monitoring Agent para *agent_name***.

Importante: Gerenciar Tivoli Enterprise Monitoring Services não é suportado no ambiente do IBM Cloud Application Performance Management.

Windows Em sistemas Windows, esta entrada contém uma coluna **Tarefa/Subsistema** que identifica se seu agente suporta diversas instâncias:

- Um único agente da instância exibe um novo aplicativo no **Gerenciar Tivoli Enterprise Monitoring Services** janela. O nome do aplicativo é **Monitoring Agent for *agent_name***. Um serviço é criado para o agente (Figura 70 na página 1400). A **Tarefa / Subsistema** coluna contém o valor **Primário**.
- Um agente de diversas instâncias exibe um novo modelo de aplicativo no **Gerenciar Tivoli Enterprise Monitoring Services** janela. O nome do modelo é **Monitoring Agent para *agent_name***. Um serviço não será criado para o agente até que você crie uma instância do agente a partir deste modelo. A coluna **Tarefa/subsistema** contém o valor **Modelo** para indicar que essa entrada é um modelo usado para criar instâncias do agente.

Linux AIX No Linux e UNIX sistemas, a entrada para o agente é o mesmo se seu agente suporta várias instâncias ou não.

Nota: As telas a seguir são para um sistema Windows. Os sistemas UNIX e Linux têm janelas semelhantes.

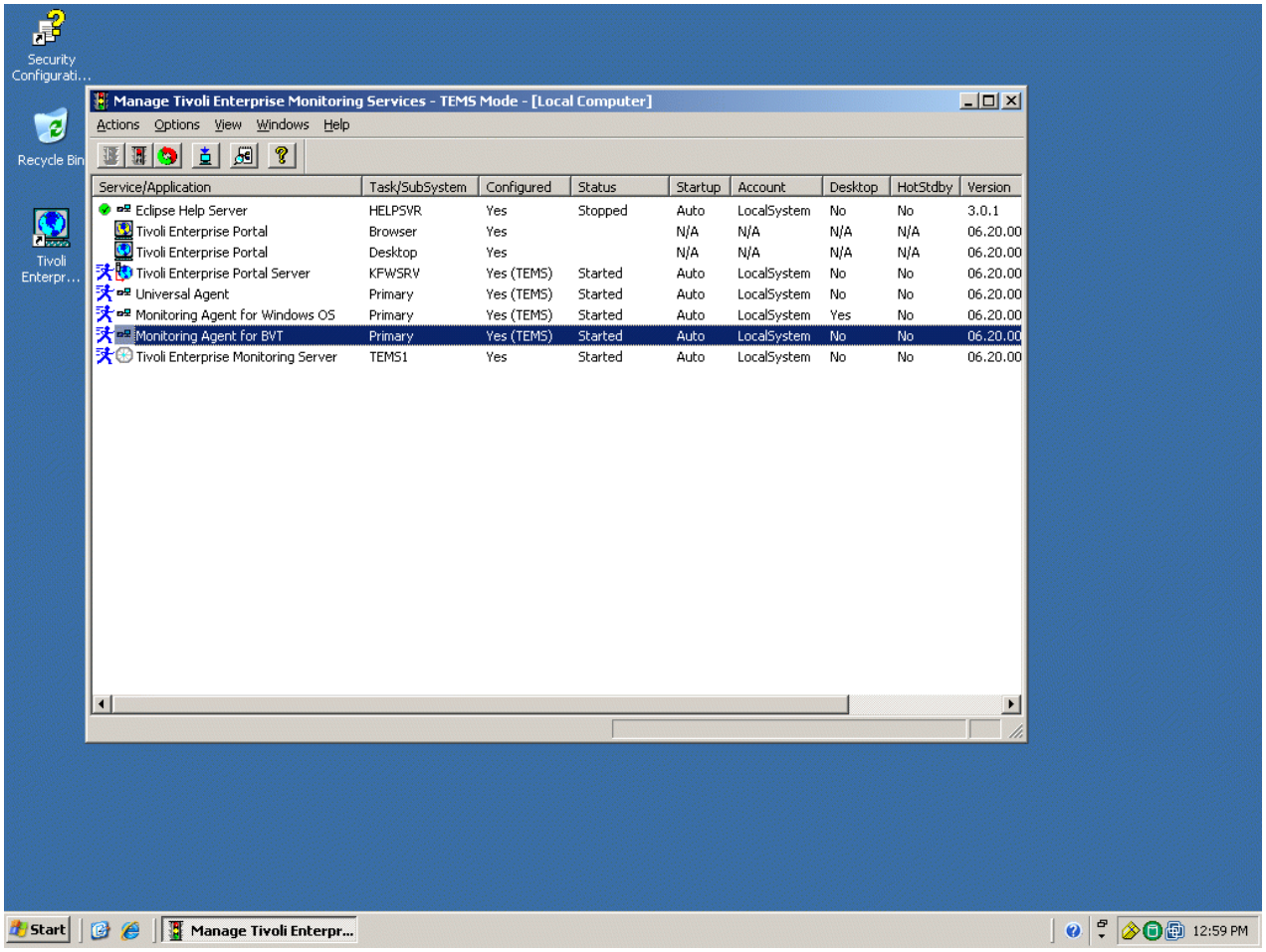


Figura 70. Janela Gerenciar o Tivoli Enterprise Monitoring Services

Mudanças no Tivoli Enterprise Portal

Em um ambiente IBM Tivoli Monitoring , depois de instalar e iniciar o agente, clique no verde **Atualizar** no ícone Tivoli Enterprise Portal . Depois disso, é possível visualizar o novo agente. É possível ver as seguintes mudanças no portal:

- Um novo subnó para o agente na visualização física do Tivoli Enterprise Portal .

- Nós para cada grupo navegador e origem de dados definida usando o Agent Builder (Figura 71 na página 1401).

  Nota: Para cada item do navegador, você deve definir uma consulta padrão.

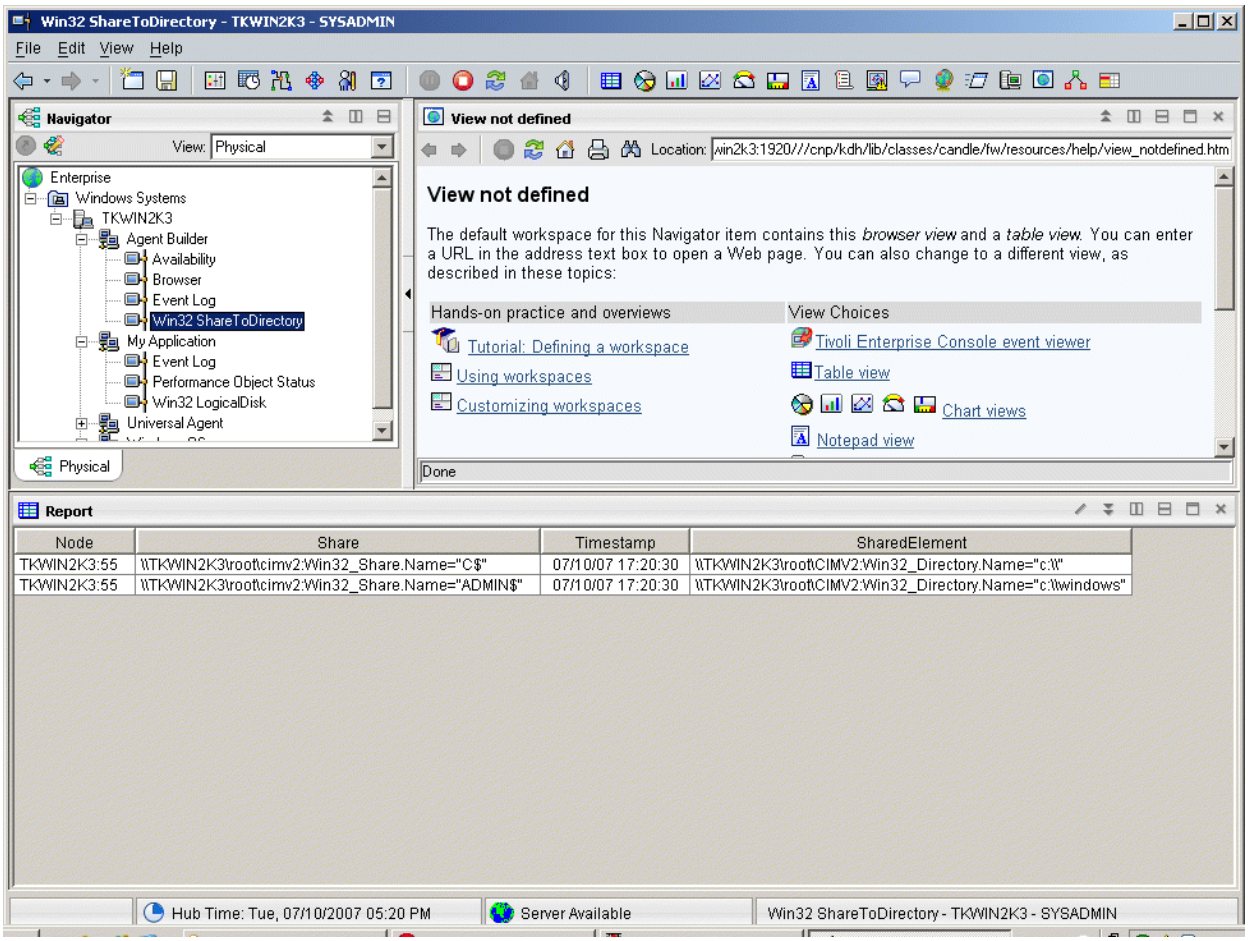


Figura 71. Nós para grupos de atributos no novo agente.

- Se o seu agente contiver subnós, um nó expansível estará presente para cada subnó que estiver definido em seu agente. Os nós a seguir são mostrados sob o nó expansível:
  - xxx status do objeto de desempenho, em que xxx é o tipo de subnó de três letras.
  - Nós para cada grupo de navegadores e origem de dados que você definiu no subnó
  - xxx nó do log de eventos se houver logs de eventos
  - xxx Nós de monitores JMX se você tiver o JMX e tiver incluído monitores JMX
- O seguinte nó automático:
  - Um nó de disponibilidade se seu agente contiver uma origem de dados de disponibilidade (Figura 72 na página 1402)

    Nota: Este nó se comporta de forma diferente dependendo do conteúdo do agente. Se o agente monitora somente a disponibilidade, o nó de disponibilidade representa a origem de dados de disponibilidade. Se o agente monitorar disponibilidade e desempenho, o nó de disponibilidade torna-se o item do navegador que representa as origens de dados de status do objeto de disponibilidade e desempenho.

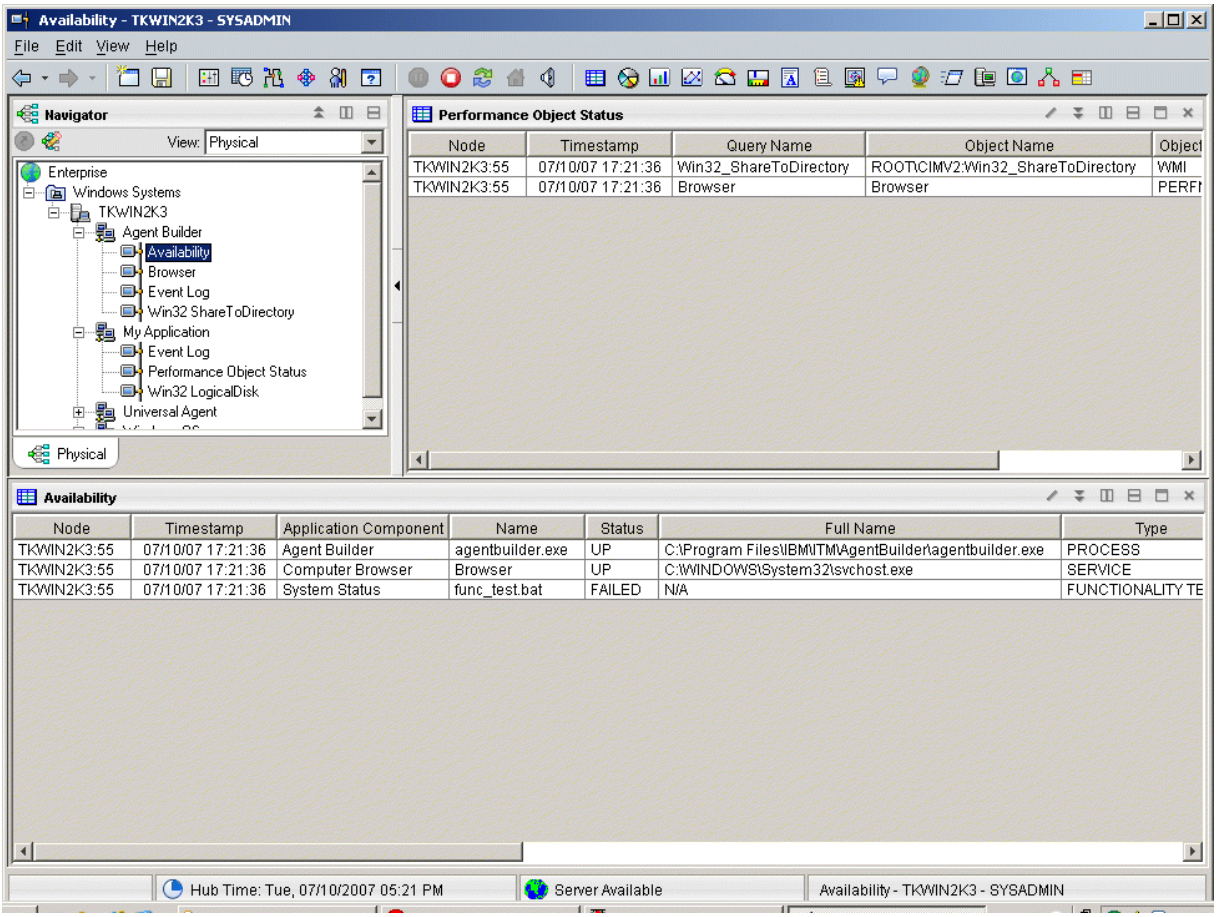


Figura 72. Nó de Disponibilidade

– Status do Objeto de Desempenho, se o agente inclui monitoramento de desempenho (não disponibilidade) origens de dados (Figura 73 na página 1403)

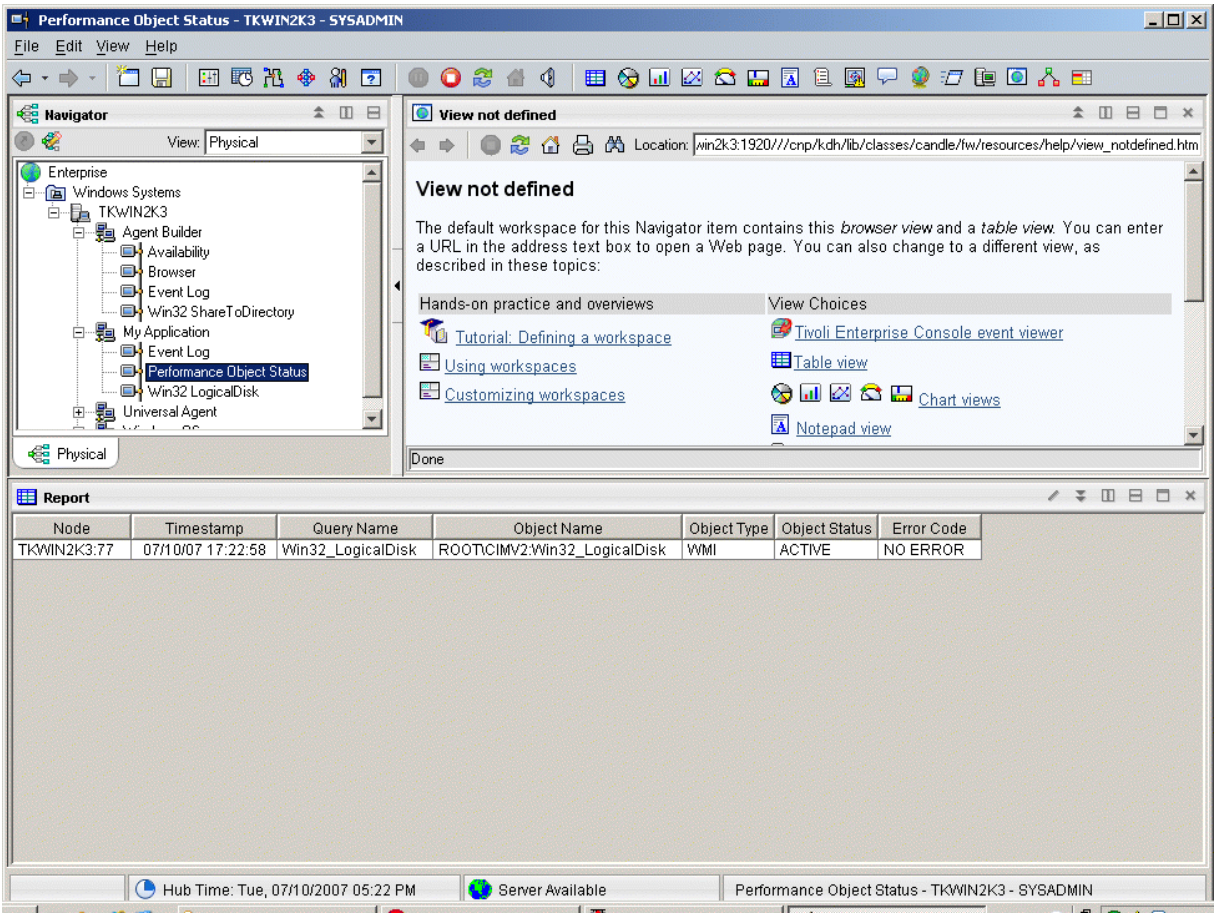


Figura 73. Nó de Status do Objeto de Desempenho

– Log de eventos, caso o agente contenha origens de dados que produzem dados de log (Figura 74 na página 1404)

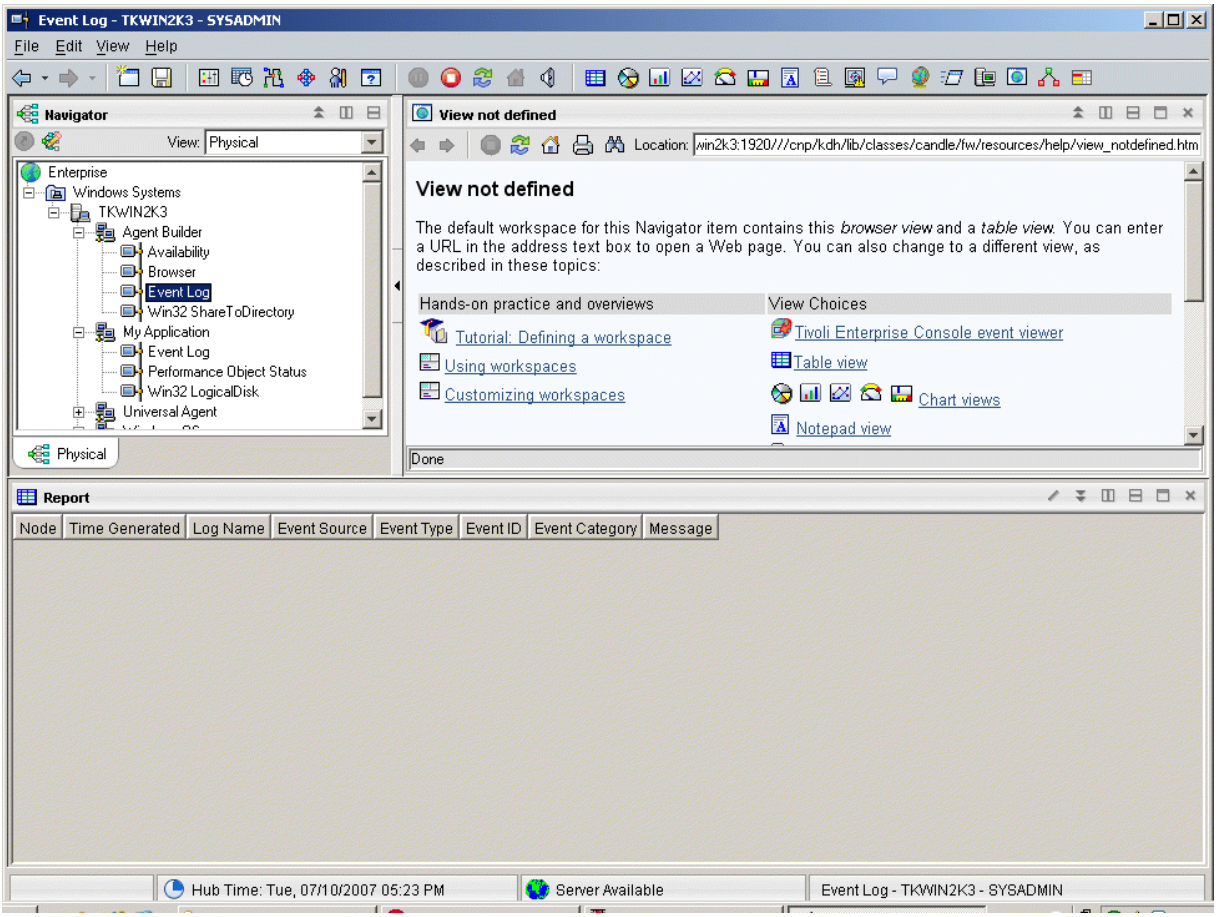


Figura 74. Nó do log de eventos

Consulte o "Referência de Atributo" na página 1419 para obter descrições dos grupos de atributos e atributos do Agent Builder.

Desinstalando um Agente

É possível remover um agente que o Agent Builder gerou a partir de um host monitorado.

Sobre Esta Tarefa

O processo de desinstalação somente desinstala o agente do sistema de agente. Esse processo não desinstala nenhum outro agente ou qualquer infraestrutura de monitoramento.

Em um ambiente IBM Tivoli Monitoring, é possível usar um dos procedimentos a seguir para remover um agente que o Agent Builder gerou:

- "Removendo um agente Tivoli Monitoring usando o Tivoli Enterprise Portal" na página 1404
- "Removendo um agente Tivoli Monitoring sem usar o Tivoli Enterprise Portal" na página 1405

Após remover o agente usando qualquer um desses procedimentos, limpe-o do Tivoli Enterprise Portal usando o procedimento a seguir: "Limpando um agente Tivoli Monitoring a partir do Tivoli Enterprise Portal" na página 1405.

Em um ambiente IBM Cloud Application Performance Management, use o procedimento a seguir: "Desinstalando um agente do IBM Cloud Application Performance Management" na página 1406.

Removendo um agente Tivoli Monitoring usando o Tivoli Enterprise Portal

Em um ambiente IBM Tivoli Monitoring, é possível usar o Tivoli Enterprise Portal para remover um agente.

Antes de Iniciar
O agente de seu sistema operacional deve estar em execução para remover seu agente criado.

Procedimento

Para usar o Tivoli Enterprise Portal para remover um agente, conclua as seguintes etapas:

- Na árvore de navegação do Tivoli Enterprise Portal, clique com o botão direito no agente e selecione **Remover**.

Removendo um agente Tivoli Monitoring sem usar o Tivoli Enterprise Portal
Se um Tivoli Enterprise Portal não está disponível em seu IBM Tivoli Monitoring ambiente, Você pode utilizar scripts e comandos do sistema operacional para remover um Agente .

Procedimento

Para remover um agente que o Agent Builder gerou a partir do sistema de destino sem usar um Tivoli Enterprise Portal, você pode concluir qualquer um dos seguintes Etapas :

- Windows
  Em sistemas Windows, use os comandos:

  ```
  cd ITM_INSTALL/TMAITM6
  kxx_uninstall.vbs ITM_INSTALL
  ```

  em que *xx* é o código do produto para o agente
- Windows
  Como alternativa, Em sistemas Windows, você pode utilizar o comando `cscript.exe` para executar o script de desinstalação. Este comando é o analisador de interface da linha de comandos para scripts vbs e não exibe uma janela; em vez disso, uma mensagem será exibida no console:

  ```
  cd ITM_INSTALL/TMAITM6
  cscript.exe kxx_uninstall.vbs
  ITM_INSTALL
  ```

- Linux AIX
  Em sistemas Linux ou UNIX, use o arquivo `uninstall.sh` que é localizado no *ITM_INSTALL*`/bin`:

  ```
  uninstall.sh [-f] [-i] [-h ITM_INSTALL] [product platformCode]
  ```

Limpando um agente Tivoli Monitoring a partir do Tivoli Enterprise Portal
Em um IBM Tivoli Monitoring após você remover o agente, campos vazios para informações do agente pode permanecer no Tivoli Enterprise Portal. Para remover os campos, limpe o agente do Tivoli Enterprise Portal.

Procedimento

1. Assegure-se de que o Tivoli Enterprise Monitoring Server e o Tivoli Enterprise Portal Server estejam ativos e em execução.
2. Efetue logon no cliente do Tivoli Enterprise Portal.
3. Na visualização do Navegador Físico do cliente Tivoli Enterprise Portal, clique com o botão direito em **Corporativo** e selecione **Área de Trabalho** > **Status do Sistema Gerenciado**.
   A área de trabalho Status do Sistema Gerenciado é exibida.
4. Selecione todos os Sistemas Gerenciados do IBM Tivoli para o seu agente.
5. Clique com o botão direito do mouse e selecione **Limpar Entrada Off-line**, que limpa todas as entradas dessa tabela.

Desinstalando um agente do IBM Cloud Application Performance Management

Você pode desinstalar o agente de qualquer sistema monitorado em um ambiente IBM Cloud Application Performance Management .

Procedimento

1. No sistema em que o agente está instalado, inicie uma linha de comandos e altere para o *install_dir*/bin no diretório, em que *install_dir* o Diretório de instalação do monitoramento Agentes .
2. Para desinstalar um agente de monitoramento específico, insira o nome do script do agente e a opção de desinstalação, em que *name* é o nome do script do agente:
   - No Windows sistemas, *name*-agent.bat uninstall
   - Em sistemas Linux ou AIX, ./*name*-agent.sh uninstall

Importando Arquivos de Suporte do Aplicativo

Se um agente precisar ser usado em um ambiente IBM Tivoli Monitoring, situações customizadas, áreas de trabalho, comandos Executar ação e consultas podem ser incluídos no pacote de instalação.

Sobre Esta Tarefa

Para ter uma única imagem de instalação para situações, áreas de trabalho, e o agente, a situação, e arquivos de espaços de trabalho devem estar no mesmo projeto que o agente. O Agent Builder fornece um assistente para criar os arquivos apropriados no projeto do agente.

Definições associadas com um agente também podem ser incluídas no pacote de instalação. O conteúdo dessas definições é diferente para um agente usado em um ambiente de monitoramento corporativo e em um ambiente do System Monitor. Uma imagem de agente de monitoramento corporativo pode incluir situações customizadas, áreas de trabalho, comandos Executar Ação e consultas. Uma imagem de agente system monitor pode incluir situações privadas, definição de trap, e agente de informações de configuração.

Para ter um único pacote de instalação que inclua as definições apropriadas e o próprio agente, os arquivos devem estar no mesmo projeto que o agente. O Agente Construtor fornece um assistente para criar os arquivos apropriados para uma instalação de monitoramento corporativo. Os arquivos para um ambiente de agente de monitoramento de sistema são criados usando o processo descrito no capítulo *Anatomia do Agente* no *IBM Tivoli Monitoring Administrator's Guide*. Os arquivos resultantes são copiados na raiz do projeto Eclipse para o agente.

Exportando e Importando Arquivos para Agentes do Tivoli Enterprise Monitoring

Sobre Esta Tarefa

Depois de criar situações, áreas de trabalho, consultas e comandos Executar Ação no Tivoli Enterprise Portal, é possível exportá-los e importá-los em outro ambiente do Tivoli Monitoring Versão 6.2. Para obter informações adicionais sobre a criação de situações e áreas de trabalho, consulte (“Criando Espaços de Trabalho, Comandos Executar Ação e Situações” na página 1371). Utilize as etapas a seguir para extrair as situações, áreas de trabalho, comandos Executar Ação e consultas:

Procedimento

1. Na guia **Explorador de Projetos**, clique com o botão direito na pasta do projeto do agente.
2. Selecione **IBM Corporation** > **Importar arquivos de suporte do aplicativo**.
3. Insira o nome do host do Servidor Tivoli Enterprise Portal.
4. Insira o nome do usuário e a senha para o ambiente do Tivoli Monitoring ao qual você está se conectando e clique em **Concluir**.

5. Se você definiu situações para o seu agente, uma caixa de diálogo será apresentada listando as situações definidas para o agente.
6. Selecione as situações que deseja exportar da lista e clique em **<<** para incluí-las na tabela de situações selecionada e clique em **OK**.

   A importação pode levar alguns instantes. Quando a tarefa for concluída, você verá os arquivos SQL nas pastas apropriadas no projeto do agente.
7. Se você definiu comandos Executar Ação para seu agente, um diálogo exibe os comandos Executar Ação definidos. Escolha os comandos executar ação que você deseja exportar da lista, clique em **>>** para incluí-los na tabela Executar Ação Selecionados e clique em **OK**.

   A importação pode levar alguns instantes. Quando a tarefa for concluída, você verá os arquivos SQL nas pastas apropriadas no projeto do agente.
8. Se você definiu consultas customizadas para seu agente, um diálogo apresenta as Consultas definidas. Selecione as consultas que deseja exportar da lista e clique em **<<** para incluí-las na tabela Consultas Selecionadas e clique em **OK**.

   A importação pode levar alguns instantes. Quando a tarefa for concluída, você verá os arquivos SQL nas pastas apropriadas no projeto do agente. Os espaços de trabalho são importados automaticamente.

O que Fazer Depois
Recrie o agente customizado, instale seu agente no host monitorado e instale o suporte do Tivoli Enterprise Portal.

Exportando e Importando Arquivos para Agentes Tivoli System Monitor

Sobre Esta Tarefa
As definições do agente system monitor estão contidas em três tipos de arquivos:

- Situações particulares são definidas em um arquivo nomeado *xx*`_situations.xml`, em que *xx* é o código do produto de dois caracteres
- Informações de configuração de trap são definidas em um arquivo nomeado *xx*`_trapcnfg.xml`, em que *xx* é o código do produto de dois caracteres
- Para agentes que requerem configuração, a configuração é definida em um arquivo para cada instância do agente. Quando o agente for um agente de instância única, o arquivo será denominado *xx*`.cfg`. Quando o agente for um agente de múltiplas instâncias, haverá um arquivo presente para cada instância. Os nomes dos arquivos são *xx*`_instance name.cfg`, em que *xx* é o código do produto de dois caracteres e *instance name* é o nome da instância do agente.

Procedimento

- Crie os arquivos usando o processo descrito no capítulo *Anatomia do Agente* no *IBM Tivoli Monitoring Administrator's Guide*. Copie os arquivos na raiz do diretório do projeto manualmente ou use a função de importação do Eclipse para selecionar os arquivos a serem importados: **Arquivo** > **Importar** > **Geral** > **Sistema de Arquivos**.

  Esses arquivos são incluídos na imagem do agente e instalados pelo instalador.

  Quando o agente é instalado, a instalação:

  – Copia os arquivos incluídos nos locais apropriados.
  – Quaisquer situações particulares definidas no arquivo `pc_situations.xml` são executadas no agente.
  – As definições de trap definidas no `pc_trapcnfg.xml` são utilizadas para encaminhar traps baseados nas situações.
  – O agente é configurado automaticamente e iniciado se:
    - O agente é um agente de instância única sem configuração definida como parte do agente.

- O agente for um agente de única instância com configuração definida como parte do agente e a imagem incluir um arquivo `pc.cfg`.
- O agente for um agente de múltiplas instâncias (todos os agentes de múltiplas instâncias requerem configuração): o instalador inicia uma instância do agente para cada arquivo `pc_inst.cfg`.

Filtro de eventos e resumo

Um grupo de atributos é definido como sendo *evento puro* ou *amostrado*. Os grupos de atributos de evento puro contêm linhas de dados que ocorrem assincronicamente. Conforme cada nova linha de dados chega, ela é processada imediatamente pelo Tivoli Monitoring. Os grupos de atributos de amostra coletam o conjunto atual de linhas de dados cada vez que os dados forem solicitados. Os seguintes grupos de atributos ilustram a diferença:

- É criado um grupo de atributos `SNMPEvent` que representa todos os Traps SNMP e informa que são enviados para o agente. Os traps ou as informações chegam assincronicamente, conforme são enviados pelos sistemas monitorados. Conforme cada evento chega, ele é passado para Tivoli Monitoring.
- Um grupo de atributos `Disco` é criado para representar as informações sobre todos os discos em um sistema. As informações do disco são coletadas periodicamente. Cada vez que as informações de disco são coletadas, o agente retorna várias linhas de dados, uma para cada disco.

A diferença entre o evento puro e os grupos de atributos de amostra afeta vários aspectos do Tivoli Monitoring. Esses aspectos incluem: visualizações de situações, de dados do armazém e do Tivoli Enterprise Portal.

Cada situação é designada (ou *distribuída*) para um ou mais sistemas gerenciados a serem monitorados para uma condição específica de um condições e condições. Quando a determinação do evento precisa ser feita com base em observações feitas em intervalos específicos, o evento é conhecido como um *evento de amostra*. Quando um evento é baseado em uma ocorrência espontânea, o evento é conhecido como um *evento puro*. Portanto, as situações para eventos de amostra têm um intervalo associado a elas, enquanto as situações para eventos puros não têm. Outra característica de eventos de amostra é que a condição que causou o evento pode alterar, fazendo, assim, com que ele não seja mais verdadeiro. Eventos puros não podem ser alterados. Portanto, os alertas surgidos para eventos de amostra podem ser alterados de true para false, enquanto um evento puro permanece true quando ocorre.

Um exemplo de um evento exemplificado é `número de processos > 100`. Um evento torna-se verdade quando o número de processos excede 100 e posteriormente torna-se falso novamente quando essa conta caia para 100 ou menos. Uma situação que monitora a `tentativa de logon inválida pelo usuário` é um evento puro; o evento ocorre quando uma tentativa de logon inválida é detectada e não se torna um evento Falso. Enquanto é possível criar situações que são avaliadas em um intervalo específico para grupos de atributos de amostra, tais avaliações não são possíveis para grupos de atributos de evento puro.

Do mesmo modo, para dados históricos, você pode configurar com que frequência os dados de amostra são coletados. No entanto, quando você ativa a coleção para dados de evento puro, você obtém cada linha como ele acontece.

Os dados exibidos no Tivoli Enterprise Portal para dados amostrados são o conjunto de linhas coletadas mais recente. Os dados exibidos para grupos de atributos de evento puro são o conteúdo de um cache local mantido pelo agente. Eles não correspondem necessariamente aos dados que são transmitidos ao Tivoli Monitoring para avaliação de situação e coleção histórica.

Controlando eventos duplicados

Use as opções de resumo e filtragem de evento para controlar como os eventos duplicados são enviados para o Tivoli Monitoring.

Antes de Iniciar

Para obter informações adicionais sobre o resumo e a filtragem de evento, consulte "Filtro de eventos e resumo" na página 1408.

Sobre Esta Tarefa

O Agent Builder define grupos de atributos que representam dados do evento como *evento puro* em Tivoli Monitoring. Esses grupos de atributos incluem arquivo de log, Log Binário do AIX, eventos SNMP e notificações JMX. Esses grupos de atributos podem produzir vários eventos duplicados. É possível controlar como esses eventos duplicados são enviados ao Tivoli Monitoring. É possível ativar esses controles para o arquivo de log, eventos SNMP e grupos de atributos de notificações JMX na guia **Informações de Evento** em **Propriedades Avançadas da Origem de Dados** na janela **Avançado**.

Se um evento é tratado como uma duplicata de outros eventos, isso é determinado pelos atributos-chave que você define no grupo de atributos. Um evento duplicado ocorre quando os valores de todos os atributos-chave no evento correspondem aos valores para os mesmos atributos-chave em um evento existente. Quando filtro de eventos e o resumo estiverem ativados, os atributos para as funções `isSummary`, `occurrenceCount`, `summaryInterval` e `eventThreshold` serão incluídos automaticamente.

Procedimento

- Na área **Opções de filtro de eventos e resumo**, selecione uma das seguintes opções:
  - **Nenhum filtro de eventos ou resumo**: Envia todos os eventos sem qualquer filtro de eventos ou resumo. Essa opção é a opção padrão.
  - **Filtrar e resumir eventos**: Cria um registro de resumo para cada evento com duplicatas e cada evento exclusivo baseado nos atributos-chave. Selecione também a opção filtro de eventos. Na área **Opções de resumo**, digite o intervalo de resumo. É possível inserir um valor em segundos ou inserir uma propriedade de configuração.

    As opções de filtro de eventos serão:

    - **Somente enviar eventos de resumo**: Envia somente os registros de resumo para o intervalo especificado.
    - **Enviar todos os eventos**: Envia todos os eventos e registros de resumo.
    - **Enviar o Primeiro Evento**: para cada evento, envia somente o primeiro evento recebido no intervalo de resumo especificado e nenhum evento duplicado. Essa opção também envia os registros de resumo.
    - **Limite de Evento**: Envia um evento para Tivoli Monitoring quando o número de eventos duplicados recebidos no intervalo for uniformemente divisível pelo limite. Por exemplo, se você configurar o limite do evento como 5 e receber menos de cinco duplicatas (incluindo o primeiro evento) no intervalo, nenhum evento será enviado ao Tivoli Monitoring. Se você receber 5, 6, 7, 8, ou 9 duplicatas, um evento é enviado. Se receber 10 duplicatas, 2 eventos são enviados. No campo **Limite do Evento**, pode digitar um número ou inserir uma propriedade de configuração. Essa opção também envia os registros de resumo.

Visualizando a Filtragem e o Resumo de Eventos no Tivoli Enterprise Portal

Exemplos de como os dados são tratados, dependendo de suas opções de filtragem e resumo de eventos.

O agente mantém um cache dos últimos eventos recebidos. Por padrão, essa cache é 100 em tamanho. Se você ativar a filtragem de evento do agente e o resumo, as diferenças podem ocorrer entre o número de eventos no cache e o número enviado ao IBM Tivoli Monitoring. Os eventos adicionais no cache podem não atingir o limite designado para envio. Ou você pode ter menos eventos no cache, se você selecionou a opção **Enviar todos os eventos**. Se a opção **Enviar todos os eventos** estiver configurada, um evento é enviado cada vez que uma duplicata ocorrer. No entanto somente uma cópia do evento é mantida no cache e a contagem de ocorrências é incrementada cada vez que o evento ocorre. Para visualizar os eventos que são enviados ao IBM Tivoli Monitoring, crie uma visualização de histórico. Para obter informações sobre como criar visualizações históricas, consulte *Historical Reporting* no Tivoli Enterprise

Portal: Guia do Usuário. É possível comparar essa visualização com a visualização de cache em tempo real no Tivoli Enterprise Portal. Também é possível usar situações para fazer a mesma comparação.

Os exemplos a seguir indicam como os mesmos dados do log são tratados, dependendo de sua opção, se houver, da filtragem de eventos e resumo. O agente de exemplo foi criado para ilustrar comportamentos diferentes. Cada grupo de atributos foi definido para monitorar o mesmo arquivo de log. Em cada exemplo, uma visualização histórica e visualização em tempo real (cache) são mostradas. Os nomes dos nós no Tivoli Enterprise Portal refletem as configurações selecionadas. Por padrão, a visualização histórica exibe os eventos mais últimos. A visualização em tempo real padrão do cache exibe os eventos mais novos recentes. Nesses exemplos, a visualização histórica mostra a última hora.

Como novos eventos ativos, é possível vê-los na visualização de cache. Na media em que duplicatas de um evento chegam, os dados são atualizados na linha existe. Na media em que um intervalo de resumo passa, os eventos existentes são convertidos em eventos de resumo e enviados. Novas linhas são então incluídas para o próximo intervalo de resumo.

(Figura 75 na página 1411) mostra a visualização histórica e a visualização de cache, se você não ativou o filtro de eventos ou resumo. Ambas as visualizações exibem os mesmos dados, mas em ordem reversa. Para exibir os eventos correspondentes, a visualização histórica é rolada para baixo e a visualização de tempo real (cache) é rolada para cima.

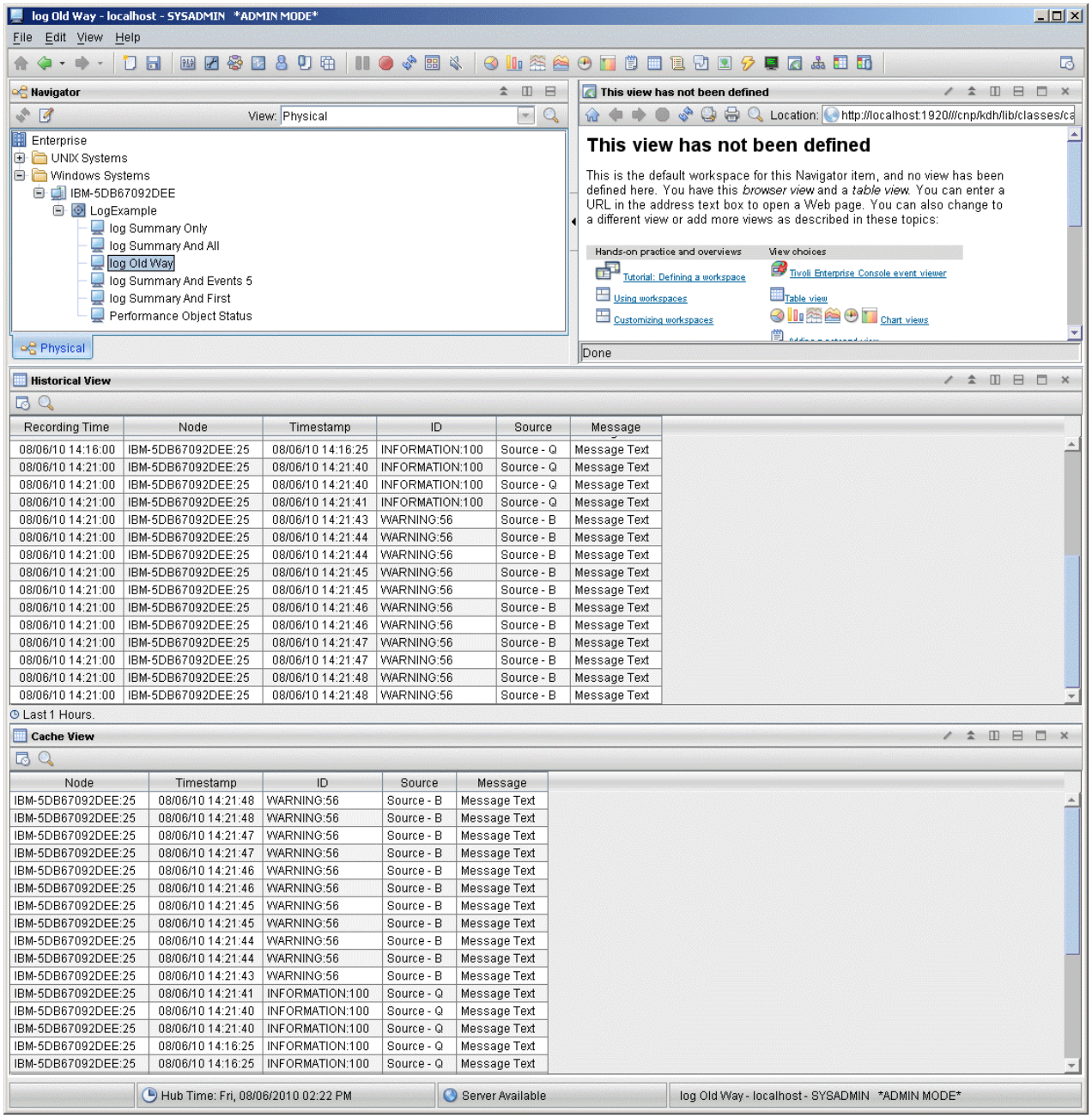


Figura 75. Visualização histórica e visualização de cache quando o filtro de eventos ou resumo não estiverem ativados

(Figura 76 na página 1412) mostra a visualização histórica e a visualização de cache, se você selecionou a opção **Enviar Somente Eventos de Resumo** na guia **Informações de Evento**. Os eventos de resumo são exibidos nas duas visualizações, mas os novos eventos são exibidos somente na visualização em tempo real (cache).

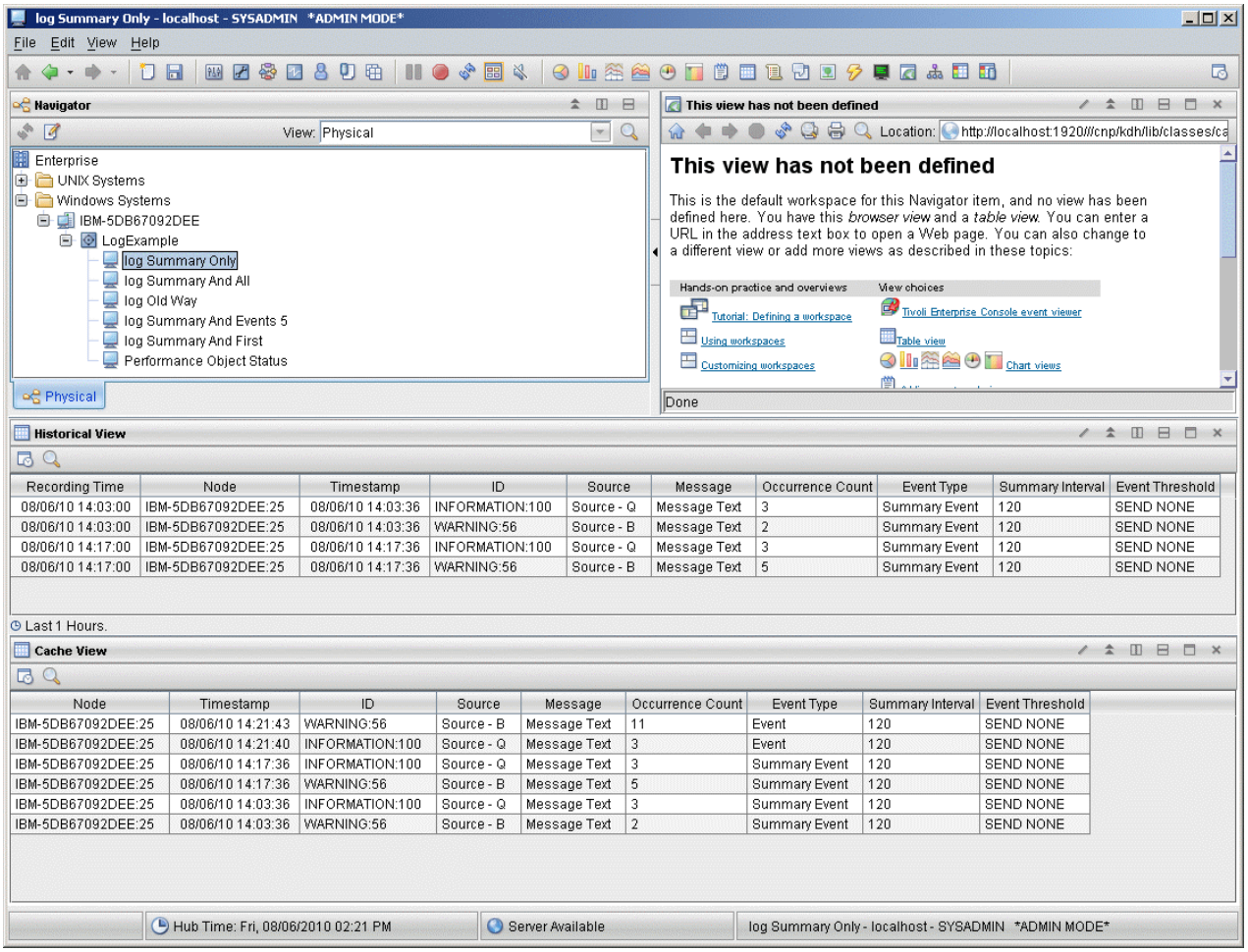


*Figura 76. Visualização de Histórico e Visualização de Cache Quando **Somente Enviar Eventos de Resumo** Estiver Selecionado*

(Figura 77 na página 1413) mostra a visualização histórica e a visualização de cache, se você selecionou a opção **Enviar Todos os Eventos** na guia **Informações de Evento**. Todos os eventos são mostrados em ambas as visualizações, mas você também pode ser os eventos de resumo que são criados no final de cada intervalo. A visualização em tempo real será alterada quando o intervalo for decorrido. Os exentos existentes são convertidos em registros de resumo e então os novos eventos são incluídos. A inclusão dos outros dois atributos de eventos disponíveis, que são usados para exibir o intervalo de resumo (120 segundos neste exemplo) e o limite *SEND ALL*.

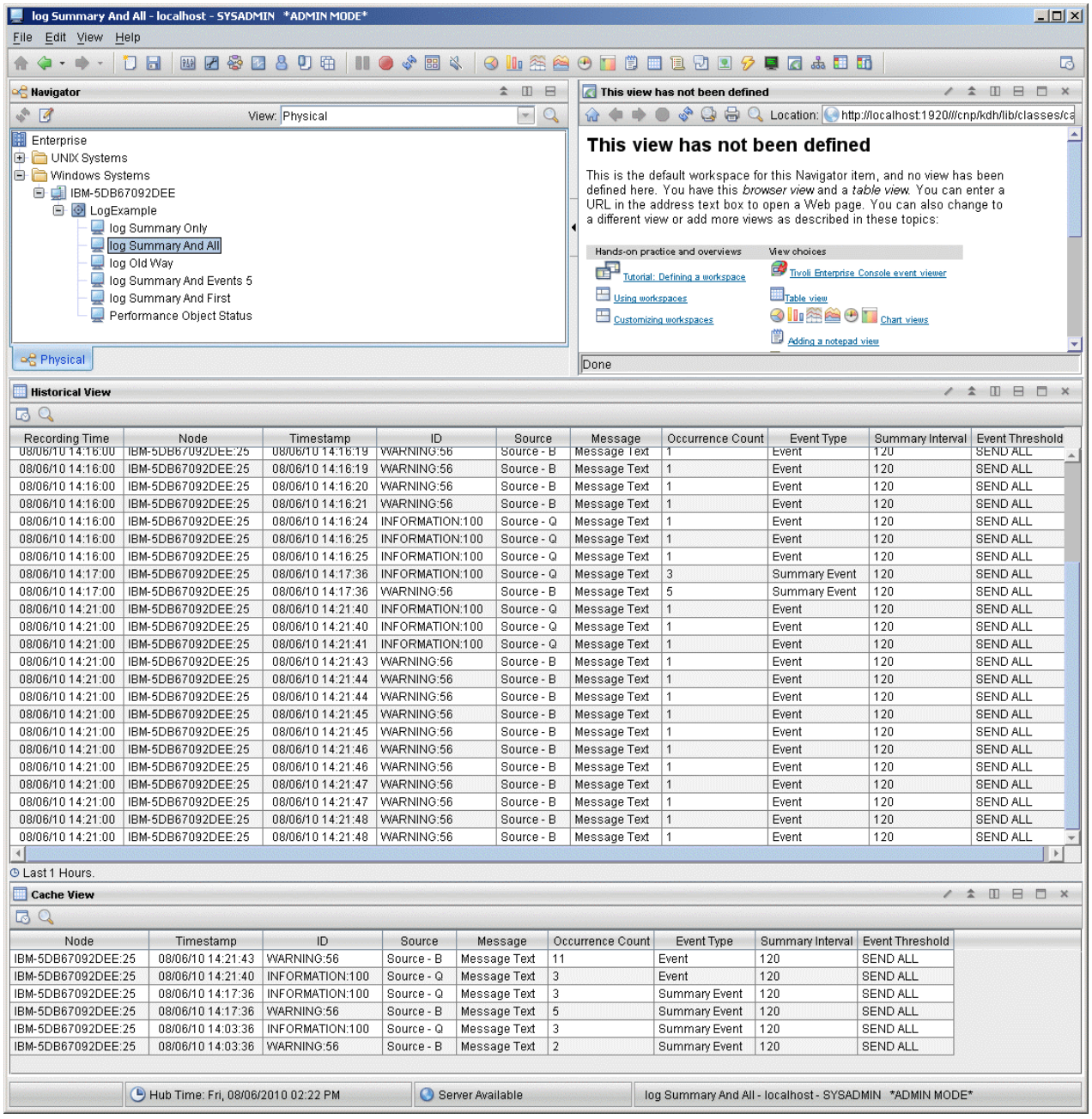


*Figura 77. Visualização de Histórico e Visualização de Cache Quando **Enviar Todos os Eventos** Estiver Selecionado*

(Figura 78 na página 1414) mostra a visualização histórica e a visualização de cache, se você selecionou a opção **Enviar Primeiro Evento** na guia **Informações de Evento**. Os eventos de resumo são exibidos nas duas visualizações, mas todos os eventos novos são exibidos somente na visualização em tempo real (cache). Para cada evento, a visualização histórica exibe somente o primeiro evento recebido no intervalo e nenhum evento duplicado.

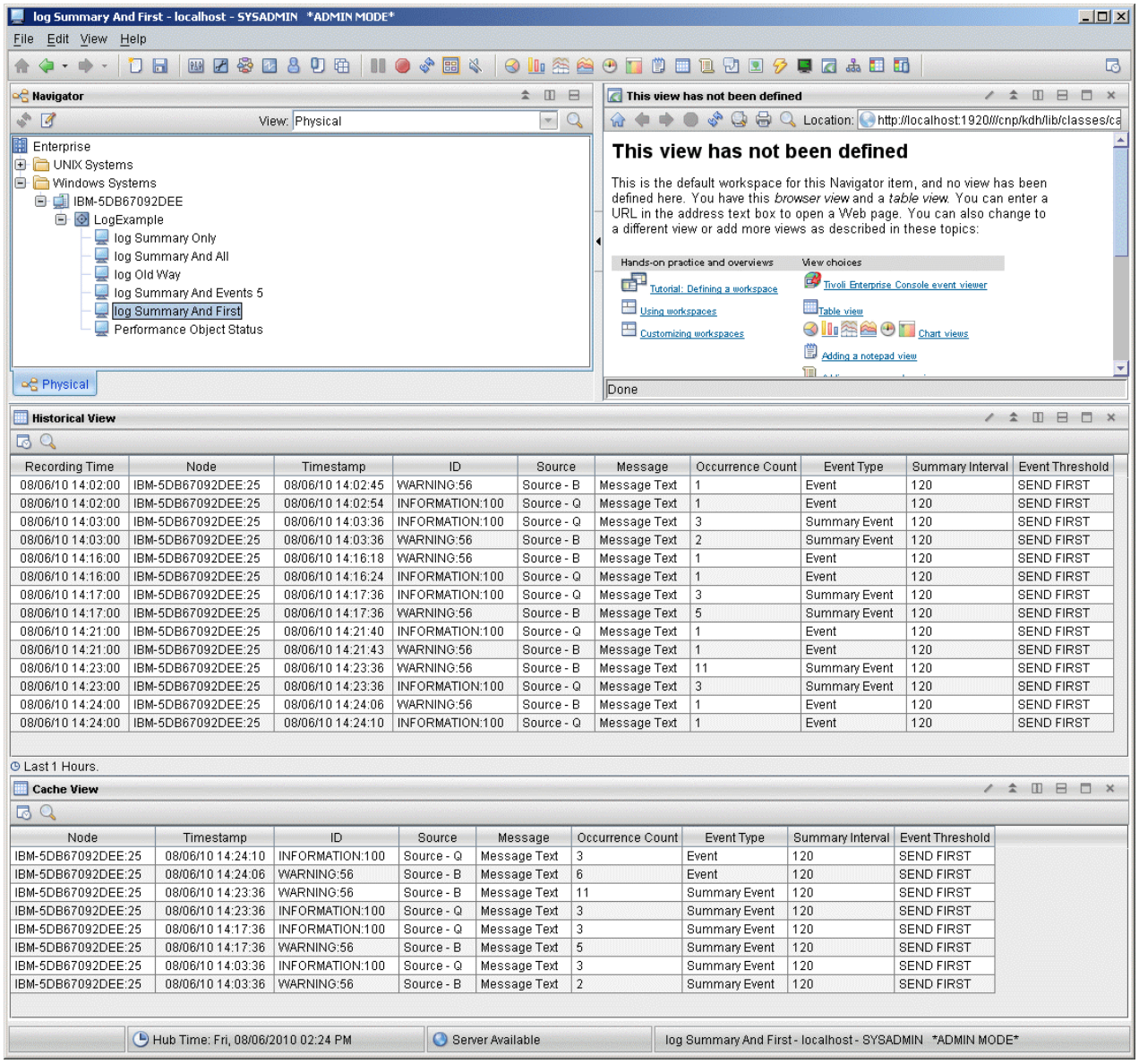


*Figura 78. Visualização de Histórico e Visualização de Cache Quando **Enviar Primeiro Evento** Estiver Selecionado*

(Figura 79 na página 1415) a visualização histórica e a visualização de cache se foi selecionada a opção **Limite de Evento** e inserido um valor de 5. Os eventos de resumo são exibidos em ambas as visualizações, mas todos os novos eventos são exibidos somente na visualização em tempo real (cache). Neste exemplo, um limite de 5 está especificado. A visualização histórica exibe um evento somente quando cinco duplicatas de um evento (incluindo o primeiro evento) são recebidas no intervalo. Se menos de 5 forem recebidas, nenhum evento será exibido. Se 6, 7, 8, ou 9 duplicatas forem recebidas no intervalo, um evento será exibido. Se 10 duplicatas forem recebidas, 2 eventos serão exibidos.

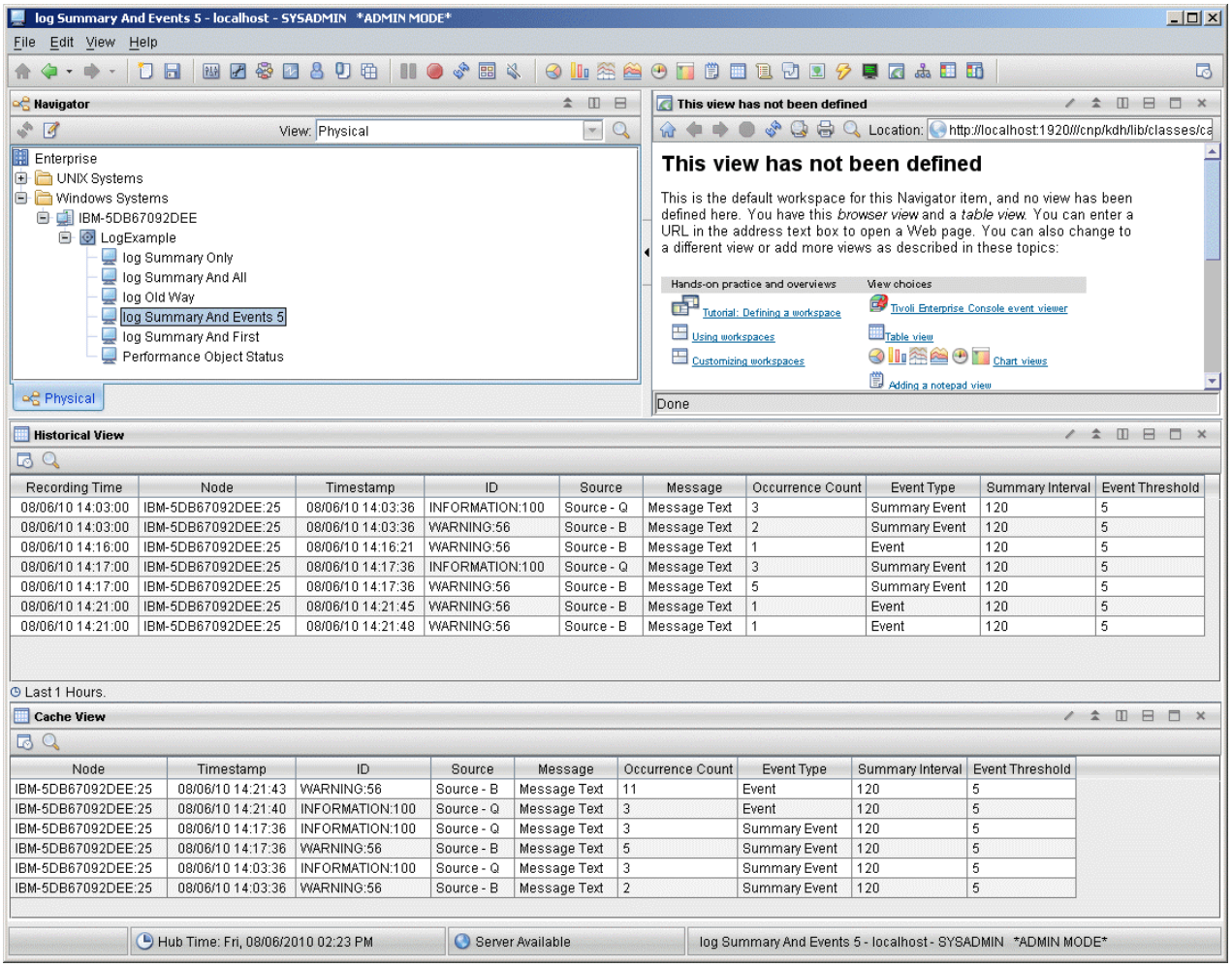


*Figura 79. Visualização de Histórico e Visualização de Cache Quando **Limite de Evento** Estiver Selecionado*

Conceitos relacionados

"Filtro de eventos e resumo" na página 1408

Resolução de Problemas e Suporte

Revise as informações de resolução de problemas para problemas que possam ocorrer ao instalar, configurar ou usar o IBM Agent Builder.

Para obter ajuda na resolução de problemas durante o desenvolvimento, a instalação ou utilizando de agentes customizados no ambiente do IBM Cloud Application Performance Management, consulte o Fórum do Cloud Application Performance Management no developerWorks. É possível procurar pela tag "agent_builder", responder a uma entrada para fazer uma pergunta relacionada ou criar uma nova entrada com sua questão.

Para informações de referência de log e mensagem e para obter ajuda na resolução de problemas relacionados ao ambiente do IBM Tivoli Monitoring, consulte a referência de resolução de problemas do IBM Agent Builder.

Compartilhando Arquivos do Projeto

Compartilhe um projeto de agente IBM Tivoli Monitoring com alguém.

Procedimento

1. Obtenha os arquivos. Você precisa de todo o conteúdo do diretório com o mesmo nome que o projeto no diretório do espaço de trabalho.
   Por exemplo, se seu diretório da área de trabalho for `c:\Documents and Settings\User1\workspace` e você desejar compartilhar seu projeto denominado `TestProject`. Você deve tornar o diretório `c:\Documents and Settings\User1\workspace\TestProject Installer` e todo o seu conteúdo acessível ao sistema.
2. Selecione **Arquivo** > **Importar**.
3. Abra o **IBM Tivoli Monitoring**.
4. Selecione **IBM Tivoli Monitoring Agent** e clique em **Avançar**.
5. Digite o caminho completo até o arquivo xml do agente ou clique em **Procurar** para procurar no arquivo.
6. Clique em **Concluir**.

Resultados
Quando o assistente for concluído, você verá o novo projeto de agente IBM Tivoli Monitoring na área de trabalho.

Compartilhar um Projeto do Instalador de Solução

Compartilhar um Projeto do Instalador de Solução com alguém

Procedimento

1. Obtenha os arquivos. Você deve ter todo o conteúdo do diretório com o mesmo nome que o projeto do Solution Installer em seu diretório do espaço de trabalho.
   Por exemplo, se seu diretório da área de trabalho for `c:\Documents and Settings\User1\workspace` e você desejar compartilhar o projeto do Instalador de Solução denominado `Instalador do TestProject`. Você deve tornar o diretório `c:\Documents and Settings\User1\workspace\TestProject Installer` e todo o seu conteúdo acessível ao sistema.
2. Clique em **Arquivo** > **Importar**.
3. Abra **Geral**.
4. Selecione **Projetos Existentes no Espaço de Trabalho** e clique em **Avançar**.
5. Digite o caminho completo para o diretório-raiz do projeto do Solution Installer ou clique em **Procurar** para procurar no diretório-raiz do projeto do Solution Installer. (Neste exemplo, o diretório `TestProject Installer`.) O Projeto nesse diretório é exibido na lista Projetos e é selecionado por padrão.
6. Opcional: Clique em **Copiar Projetos na Área de Trabalho**.
7. Clique em **Concluir**.

Opções de Linha de Comandos

Comandos disponíveis a partir da interface da linha de comandos (CLI) do Agent Builder.

O Tivoli Monitoring Agent Builder contém uma interface da linha de comandos (CLI) que pode ser usada para gerar o Tivoli Monitoring Agent sem iniciar a interface gráfica com o usuário (GUI) do Eclipse. É possível gerar o agente como parte de uma construção, por exemplo:

Nos sistemas Windows, é possível usar um arquivo em lote no seguinte diretório para acessar a CLI:

```
install_location\agenttoolkit.bat
```

Nos sistemas UNIX e Linux, é possível usar um script no seguinte diretório para acessar a CLI:

```
install_location/agenttoolkit.sh
```

Os comandos descritos nesta documentação são formatados para sistemas Windows systems, que usam uma barra invertida (\) para caminhos de diretório.

Para sistemas UNIX® ou Linux®, use os mesmos comandos que para sistemas Windows, mas com as seguintes mudanças:

- Use uma barra (/) para caminhos de diretório em vez de uma barra invertida (\).
- Use o script `agenttoolkit.sh` em vez do script `agenttoolkit.bat`.

Comandos

A Tabela 300 na página 1417 lista o nome e a declaração de objetivo para cada opção de comando para o comando de texto:

Tabela 300. Tabela de referência rápida de comandos

Comando	Objetivo
generatelocal	Carrega e valida o arquivo `itm_toolkit_agent.xml` e gera os arquivos que executam o Tivoli Monitoring Agent. A instalação é em um ambiente local do Tivoli Monitoring.
generatemappingfile	Cria o arquivo de mapeamento para portar modelos de recursos customizados IBM Tivoli Monitoring v5.x para agentes IBM Tivoli Monitoring v6.
generatezip	Gera um arquivo compactado denominado *productcode*`.zip` ou *productcode*`.tgz`.

As descrições de comando que são referidas na tabela descrevem como executar os comandos, incluindo as seguintes informações:

Objetivo
Lista o objetivo do comando.

Formato
Especifica a sintaxe digitada na linha de comandos. A sintaxe contém o nome do comando e uma lista dos parâmetros para o comando. Uma definição de cada parâmetro segue o nome do comando.

Exemplos
O exemplo para o comando contém uma breve descrição do exemplo e um exemplo da sintaxe.

Uso
Fornece uma explicação do comando e seu objetivo.

Comentários
Fornece comandos ou texto que podem fornecer mais informações.

Comando - `generatelocal`

Use este comando para carregar e validar o XML e para gerar os arquivos para executar o Tivoli Monitoring Agent.

Objetivo

Carrega e valida o arquivo `itm_toolkit_agent.xml` e gera os arquivos para executar o Tivoli Monitoring Agent. A instalação é em um ambiente local do Tivoli Monitoring.

Formato

Para sistemas Windows :

```
install_location\agenttoolkit.bat  project_dir -generatelocal
itm_install_dir
```

em que:

install_location
Diretório no qual o Agent Builder está instalado

project_dir
Nome do diretório que contém o arquivo `itm_toolkit_agent.xml`

itm_install_dir
Local no qual o Tivoli Monitoring está instalado (por exemplo, `c:\IBM\ITM`)

Exemplos

O exemplo a seguir para Windows, a definição de agente no `C:\ABCAgent` é validada e os arquivos que são necessários para executar o `ABCAgent` são gerados em `C:\IBM\ITM`:

```
install_location\agenttoolkit.bat C:\ABCAgent -generatelocal C:\IBM\ITM
```

Comando - `generatemappingfile`

Use este comando para migrar os modelos de recursos customizados do IBM Tivoli Monitoring v5.x para agentes do IBM Tivoli Monitoring v6.

Objetivo

Este comando cria o arquivo de mapeamento para migração de modelos de recursos customizados do IBM Tivoli Monitoring v5.x para agentes do IBM Tivoli Monitoring v6.

Formato

Para sistemas Windows :

```
install_location\agenttoolkit.bat project_dir -generatemappingfile output_dir
   itm5_interp_list
```

Em que:

install_location
Diretório no qual o Agent Builder está instalado

project_dir
Nome do diretório que contém `itm_toolkit_agent.xml`

output_dir
Nome do diretório no qual o arquivo de mapeamento é gravado

itm5_interp_list
Lista separada por vírgulas dos sistemas operacionais ITM 5x nos quais o modelo de recurso customizado é executado. Os seguintes valores são permitidos:

- `aix4-r1`
- `hpux10`
- `linux-ix86`
- `linux-ppc`
- `linux-s390`
- `os2-ix86`
- `os400`
- `solaris2`
- `solaris2-ix86`
- `w32-ix86`

Exemplos

Para sistemas Windows

```
install_location\agenttoolkit.bat c:\ABCAgent -generatemappingfile c:\output linux-ix86,linux-
ppc,linux-s390
```

Comando - generatezip

Use esse comando para carregar um XML de validação para gerar um arquivo compactado que pode ser usado para instalar o agente em outro sistema.

Objetivo

Carrega e valida o arquivo `itm_toolkit_agent.xml` e gera um arquivo compactado denominado *productcode*`.zip` ou *productcode*`.tgz`. O arquivo compactado gerado pode ser usado para instalar o agente em outro sistema. Dependendo de seu ambiente, os dois tipos de arquivo podem ser gerados.

Formato

Para sistemas Windows :

```
install_location\agenttoolkit.bat  project_dir -generatezip
output_dir
```

Em que:

project_dir
Nome de um diretório que contém o arquivo `itm_toolkit_agent.xml`

output_dir
Nome de um diretório no qual o arquivo compactado é gravado

Exemplos

No exemplo a seguir para Windows, a definição de agente no `C:\ABCAgent` é validada e um arquivo compactado que contém os arquivos necessários para executar `ABCAgent` é gerado no `C:\Output`:

```
install_location\agenttoolkit.bat\ C:\ABCAgent -generatezip C:\Output
```

Referência de Atributo

Contém descrições dos atributos para cada grupo gerado por atributo incluído no Agent Builder.

Nó de Disponibilidade

O grupo de atributos Disponibilidade contém dados de disponibilidade para o aplicativo.

A tabela fornece um formato comum para representar disponibilidade de aplicativo, que inclui informações relevantes para três aspectos de um aplicativo: serviços (Windows somente), processos e códigos de retorno de comando.

A seguinte lista contém informações sobre cada atributo no grupo de atributos Disponibilidade:

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente

Type
Sequência

Nomes

Nome do Atributo
Nó

Nome da Coluna
ORIGINNODE

atributo Time stamp

Descrição
O horário local no agente quando os dados foram coletados

Type
Hora

Nomes

Nome do Atributo
Registro de Data e Hora

Nome da Coluna
TIMESTAMP

Atributo de componente de aplicativo - Esse atributo é um atributo-chave

Descrição
O nome descritivo de uma parte do aplicativo

Type
Sequência

Nomes

Nome do Atributo
Application_Component

Nome da Coluna
COMPONENT

atributo Nome

Descrição
O nome do processo, serviço ou teste funcional. Este nome corresponde ao nome do executável do processo, o nome abreviado do serviço ou o nome do processo que é usado para testar o aplicativo.

Type
Sequência

Nomes

Nome do Atributo
Nome

Nome da Coluna
NOME

Atributo Status

Descrição
O status do componente do aplicativo.

- Para processos, os valores são UP, DOWN, WARNING ou PROCESS_DATA_NOT_AVAILABLE. PROCESS_DATA_NOT_AVAILABLE é exibido para um processo quando o processo correspondente está executando, mas o recurso que utiliza informações não pode ser coletado para esse processo.

- Para serviços, os valores são UP, DOWN ou UNKNOWN. UNKNOWN é exibido quando o serviço não está instalado.
- Para código de retorno de comando, os valores são PASSED ou FAILED.

Type
Sequência

Nomes

Nome do Atributo
Estado

Nome da Coluna
STATUS

Atributo Nome Completo

Descrição
O nome completo do processo que inclui informações que são dependentes do processo. O nome do pode incluir o caminho completo se o processo foi iniciado dessa forma. O nome também pode incluir um caminho parcial ou até mesmo um caminho que é alterado pelo processo.

Type
Sequência

Nomes

Nome do Atributo
Full_Name

Nome da Coluna
FULLNAME

Atributo Tipo

Descrição
Identifica o tipo de componente de aplicativo. Componentes são processos, serviços ou códigos de retorno de comandos.

Type
Número inteiro (calibrador)

Nomes

Nome do Atributo
Type

Nome da Coluna
TYPE

atributo Tamanho Virtual

Descrição
O tamanho virtual (em MB) do processo

Type
Número inteiro (calibrador)

Nomes

Nome do Atributo
Virtual_Size

Nome da Coluna
VIRTSIZE

atributo Falhas de Página por Seg

Descrição
A taxa de falhas de página para o processo que é medido em falhas por segundo. Esse valor contém somente dados válidos para processos.

Type
Número inteiro (calibrador)

Nomes

Nome do Atributo
Page_Faults_Per_Sec

Nome da Coluna
PAGEFAULTS

atributo Tamanho do Conjunto de Tarefas

Descrição
O tamanho do conjunto de trabalho do processo em MB. Esse valor contém somente dados válidos para processos.

Type
Número inteiro (calibrador)

Nomes

Nome do Atributo
Working_Set_Size

Nome da Coluna
WORKSET

Atributo Contagem de Encadeamentos

Descrição
O número de encadeamentos atualmente alocados por este processo. Esse valor contém somente dados válidos para processos.

Type
Número inteiro (calibrador)

Nomes

Nome do Atributo
Thread_Count

Nome da Coluna
THREADS

atributo PID

Descrição
O ID do processo associado ao processo. Esse valor contém somente dados válidos para processos.

Type
Número inteiro (calibrador)

Nomes

Nome do Atributo
PID

Nome da Coluna
PID

atributo Porcentagem de Tempo Privilegiado

Descrição
A porcentagem do tempo de processador disponível que está sendo utilizada por este processo para operação privilegiada

Type
Número inteiro (calibrador)

Nomes

Nome do Atributo
Percent_Privileged_Time

Nome da Coluna
PERCPRIV

atributo Porcentagem de Tempo no Modo de Usuário

Descrição
A porcentagem do tempo de processador disponível que está sendo utilizada por este processo para operação do modo de usuário

Type
Número inteiro (calibrador)

Nomes

Nome do Atributo
Percent_User_Mode_Time

Nome da Coluna
PERCUSER

atributo Porcentagem de Tempo do Processador

Descrição
A porcentagem de tempo decorrido em que este processo utilizou o processador para executar instruções

Type
Número inteiro (calibrador)

Nomes

Nome do Atributo
Percent_Processor_Time

Nome da Coluna
PERCPROC

atributo Linha de Comandos

Descrição
O nome do programa e quaisquer argumentos especificados na linha de comandos quando o processo foi iniciado. Este atributo possui o valor *N/D* se estiver executando um teste de Serviço ou Funcionalidade.

Type
Sequência

Nomes

Nome do Atributo
Command_Line

Nome da Coluna
CMDLINE

atributo Status do Teste de Funcionalidade

Descrição
O código de retorno do teste de funcionalidade. Quando o aplicativo monitorado está executando corretamente, SUCCESS é retornado. NOT_RUNNING é retornado quando o aplicativo não está executando corretamente. N/A é retornado quando a linha não representa um teste de funcionalidade.

Type
Inteiro com valores enumerados. As sequências são exibidas no Tivoli Enterprise Portal, o warehouse e as consultas retornam os números. Os valores definidos são: N/A(1), SUCCESS (0), GENERAL_ERROR (2), WARNING (3), NOT_RUNNING (4), DEPENDENT_NOT_RUNNING (5), ALREADY_RUNNING (6), PREREQ_NOT_RUNNING (7), TIMED_OUT (8), DOESNT_EXIST (9), UNKNOWN (10), DEPENDENT_STILL_RUNNING (11) ou INSUFFICIENT_USER_AUTHORITY (12). Quaisquer outros valores exibirão o valor numérico no Tivoli Enterprise Portal.

Nomes

Nome do Atributo
Functionality_Test_Status

Nome da Coluna
FUNCSTATUS

atributo Mensagem do Teste de Funcionalidade

Descrição
A mensagem de texto que corresponde ao Status do Teste de Funcionalidade. Esse atributo é válido somente para códigos de retorno de comando.

Type
Sequência

Nomes

Nome do Atributo
Functionality_Test_Message

Nome da Coluna
FUNCMSG

Nó de Status do Objeto de Desempenho

Use o grupo de atributos Status do Objeto de Desempenho para ver o status de todos os grupos de atributos que constituem o agente. Cada um dos grupos de atributos é representado por uma linha nesta tabela ou outro tipo de visualização. O status de um grupo de atributos reflete o resultado da última tentativa de coleta de dados, ou evento de recepção de dados, para o grupo de atributos. Ao verificar as informações de status, é possível ver se o agente está operando corretamente. Quando o seu agente não coleta os dados, mas o recebe (dados de evento), os atributos que se relacionam aos dados de amostra não contêm dados úteis. Somente os sete primeiros atributos que são listados são relevantes para os dados de evento.

Grupo Histórico
Este grupo de atributos é elegível para uso com o Tivoli Data Warehouse.

Descrições do Atributo
A seguinte lista contém informações sobre cada atributo no grupo de atributos Status do Objeto de Desempenho:

Atributo do nó: Este atributo é um atributo-chave.

Descrição
O nome do sistema gerenciado do agente.

Type
Sequência

Nome do Warehouse
NODE

atributo Time stamp

Descrição
A hora local no agente quando os dados foram coletados.

Type
Sequência

Nome do Warehouse
TIMESTAMP

Atributo de Nome da Consulta: Este atributo é um atributo-chave.

Descrição
O nome do grupo de atributos.

Type
Sequência

Nome do Warehouse
QUERY_NAME ou ATTRGRP

Atributo Nome do Objeto

Descrição
O nome do objeto de desempenho.

Type
Sequência

Nome do Warehouse
OBJECT_NAME ou OBJNAME

Atributo Tipo de Objeto

Descrição
O tipo do objeto de desempenho.

Type
Inteiro com valores enumerados. As sequências são exibidas no Tivoli Enterprise Portal. O warehouse e as consultas retornam os valores mostrados em parênteses. Os seguintes valores são definidos:

- WMI (0)
- PERFMON (1)
- WMI ASSOCIATION GROUP (2)
- JMX (3)
- SNMP (4)
- SHELL COMMAND (5)
- JOINED GROUPS (6)
- CIMOM (7)
- CUSTOM (8)
- ROLLUP DATA (9)
- WMI REMOTE DATA (10)
- LOG FILE (11)
- JDBC (12)

- CONFIG DISCOVERY (13)
- NT EVENT LOG (14)
- FILTER (15)
- SNMP EVENT (16)
- PING (17)
- DIRECTOR DATA (18)
- DIRECTOR EVENT (19)
- SSH REMOTE SHELL COMMAND (20)

Qualquer outro valor é o valor retornado pelo agente no Tivoli Enterprise Portal.

Nome do Warehouse
OBJECT_TYPE ou OBJTYPE

Atributo Status do Objeto

Descrição
O status do objeto de desempenho.

Type
Inteiro com valores enumerados. As sequências são exibidas no Tivoli Enterprise Portal. O warehouse e as consultas retornam os valores mostrados em parênteses. Os seguintes valores são definidos:

- ACTIVE (0)
- INACTIVE (1)

Qualquer outro valor é o valor retornado pelo agente no Tivoli Enterprise Portal.

Nome do Warehouse
OBJECT_STATUS ou OBJSTTS

Atributo Código de Erro

Descrição
O código de erro associado à consulta.

Type
Inteiro com valores enumerados. As sequências são exibidas no Tivoli Enterprise Portal. O warehouse e as consultas retornam os valores mostrados em parênteses. Os seguintes valores são definidos:

- NO ERROR (0)
- GENERAL ERROR (1)
- OBJECT NOT FOUND (2)
- COUNTER NOT FOUND (3)
- NAMESPACE ERROR (4)
- OBJECT CURRENTLY UNAVAILABLE (5)
- COM LIBRARY INIT FAILURE (6)
- SECURITY INIT FAILURE (7)
- PROXY SECURITY FAILURE (9)
- NO INSTANCES RETURNED (10)
- ASSOCIATOR QUERY FAILED (11)
- REFERENCE QUERY FAILED (12)
- NO RESPONSE RECEIVED (13)
- CANNOT FIND JOINED QUERY (14)

- CANNOT FIND JOIN ATTRIBUTE IN QUERY 1 RESULTS (15)
- CANNOT FIND JOIN ATTRIBUTE IN QUERY 2 RESULTS (16)
- QUERY 1 NOT A SINGLETON (17)
- QUERY 2 NOT A SINGLETON (18)
- NO INSTANCES RETURNED IN QUERY 1 (19)
- NO INSTANCES RETURNED IN QUERY 2 (20)
- CANNOT FIND ROLLUP QUERY (21)
- CANNOT FIND ROLLUP ATTRIBUTE (22)
- FILE OFFLINE (23)
- NO HOSTNAME (24)
- MISSING LIBRARY (25)
- ATTRIBUTE COUNT MISMATCH (26)
- ATTRIBUTE NAME MISMATCH (27)
- COMMON DATA PROVIDER NOT STARTED (28)
- CALLBACK REGISTRATION ERROR (29)
- MDL LOAD ERROR (30)
- AUTHENTICATION FAILED (31)
- CANNOT RESOLVE HOST NAME (32)
- SUBNODE UNAVAILABLE (33)
- SUBNODE NOT FOUND IN CONFIG (34)
- ATTRIBUTE ERROR (35)
- CLASSPATH ERROR (36)
- CONNECTION FAILURE (37)
- FILTER SYNTAX ERROR (38)
- FILE NAME MISSING (39)
- SQL QUERY ERROR (40)
- SQL FILTER QUERY ERROR (41)
- SQL DB QUERY ERROR (42)
- SQL DB FILTER QUERY ERROR (43)
- PORT OPEN FAILED (44)
- ACCESS DENIED (45)
- TIMEOUT (46)
- NOT IMPLEMENTED (47)
- REQUESTED A BAD VALUE (48)
- RESPONSE TOO BIG (49)
- GENERAL RESPONSE ERROR (50)
- SCRIPT NONZERO RETURN (51)
- SCRIPT NOT FOUND (52)
- SCRIPT LAUNCH ERROR (53)
- CONF FILE DOES NOT EXIST (54)
- CONF FILE ACCESS DENIED (55)
- INVALID CONF FILE (56)
- EIF INITIALIZATION FAILED (57)

- CANNOT OPEN FORMAT FILE (58)
- FORMAT FILE SYNTAX ERROR (59)
- REMOTE HOST UNAVAILABLE (60)
- EVENT LOG DOES NOT EXIST (61)
- PING FILE DOES NOT EXIST (62)
- NO PING DEVICE FILES (63)
- PING DEVICE LIST FILE MISSING (64)
- SNMP MISSING PASSWORD (65)
- DISABLED (66)
- URLS FILE NOT FOUND (67)
- XML PARSE ERROR (68)
- NOT INITIALIZED (69)
- ICMP SOCKETS FAILED (70)

Qualquer outro valor é o valor retornado pelo agente no Tivoli Enterprise Portal.

Nome do Warehouse
ERROR_CODE ou ERRCODE

atributo Início da Última Coleta

Descrição
O horário mais recente de início da coleção de dados deste grupo.

Type
Registro de data e hora com valores enumerados. As sequências são exibidas no Tivoli Enterprise Portal. O warehouse e as consultas retornam os valores mostrados em parênteses. Os seguintes valores são definidos:

- NOT COLLECTED (0691231190000000)
- NOT COLLECTED (0000000000000001)

Qualquer outro valor é o valor retornado pelo agente no Tivoli Enterprise Portal.

Nome do Warehouse
LAST_COLLECTION_START ou COLSTRT

Atributo Última Coleta Concluída

Descrição
O horário mais recente de conclusão da coleção de dados deste grupo.

Type
Registro de data e hora com valores enumerados. As sequências são exibidas no Tivoli Enterprise Portal. O warehouse e as consultas retornam os valores mostrados em parênteses. Os seguintes valores são definidos:

- NOT COLLECTED (0691231190000000)
- NOT COLLECTED (0000000000000001)

Qualquer outro valor é o valor retornado pelo agente no Tivoli Enterprise Portal.

Nome do Warehouse
LAST_COLLECTION_FINISHED ou COLFINI

Atributo Duração da Última Coleta

Descrição
A duração da coleção de dados concluída mais recentemente para este grupo em segundos.

Type
Número real (contador de 32 bits) com duas casas decimais de precisão.

Nome do Warehouse
LAST_COLLECTION_DURATION ou COLDURA

Atributo Média de Duração da Coleta

Descrição
A duração média de todas as coleções de dados para este grupo em segundos.

Type
Número real (contador de 32 bits) com duas casas decimais de precisão com valores enumerados. As sequências são exibidas no Tivoli Enterprise Portal. O warehouse e as consultas retornam os valores mostrados em parênteses. Os seguintes valores são definidos:

- `NO DATA (-100)`

Qualquer outro valor é o valor retornado pelo agente no Tivoli Enterprise Portal.

Nome do Warehouse
AVERAGE_COLLECTION_DURATION ou COLAVGD

Atributo Intervalo de Atualização

Descrição
O intervalo no qual este grupo é atualizado em segundos.

Type
Número inteiro (contador de 32 bits)

Nome do Warehouse
REFRESH_INTERVAL ou REFRINT

Atributo Número de Coletas

Descrição
O número de vezes que este grupo é coletado desde o início do agente.

Type
Número inteiro (contador de 32 bits)

Nome do Warehouse
NUMBER_OF_COLLECTIONS ou NUMCOLL

Atributo Ocorrências de Cache

Descrição
O número de vezes que uma solicitação de dados externos para este grupo é atendida a partir do cache.

Type
Número inteiro (contador de 32 bits)

Nome do Warehouse
CACHE_HITS ou CACHEHT

atributo Ausências de Cache

Descrição
O número de vezes que uma solicitação de dados externos para este grupo não estava disponível no cache.

Type
Número inteiro (contador de 32 bits)

Nome do Warehouse
CACHE_MISSES ou CACHEMS

atributo Porcentagem de Ocorrência de Cache

Descrição
A porcentagem de solicitações de dados externos para este grupo que são atendidas a partir do cache.

Type
Número real (contador de 32 bits) com duas casas decimais de precisão.

Nome do Warehouse
CACHE_HIT_PERCENT ou CACHPCT

Atributo Intervalos Ignorados

Descrição
O número de vezes em que uma coleta de dados de plano de fundo foi ignorada porque a coleta anterior ainda estava executando quando a coleta seguinte estava para começar.

Type
Número inteiro (contador de 32 bits)

Nome do Warehouse
INTERVALS_SKIPPED ou INTSKIP

Grupo de atributos do Status do Conjunto de Encadeamentos

O grupo de atributos Status do Conjunto de Encadeamentos contém informações que refletem o status do conjunto de encadeamentos interno que é usado para coletar dados de forma assíncrona.

A seguir há uma lista dos atributos para este grupo de atributos. O nome com texto em negrito mostra como o atributo é exibido no Tivoli Enterprise Portal.

A lista a seguir contém informações sobre cada atributo no grupo de atributos de Status do Conjunto de Encadeamentos:

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente

Type
Sequência

Nomes

Nome do Atributo
Nó

Nome da Coluna
ORIGINNODE

atributo Time stamp

Descrição
O horário que é coletado do sistema de agente quando a linha de dados é criada e enviada do agente para o Tivoli Enterprise Monitoring Server. Ou armazenada para propósitos históricos. Representa o fuso horário local do sistema do agente.

Type
Hora

Nomes

Nome do Atributo
Registro de Data e Hora

Nome da Coluna
TIMESTAMP

Atributo Tamanho do Conjunto de Encadeamentos

Descrição
O número de encadeamentos atualmente existentes no conjunto de encadeamentos.

Type
Integer

Nomes

Nome do Atributo
Thread_Pool_Size

Nome da Coluna
THPSIZE

Atributo Tamanho Máx do Conjunto de Encadeamentos

Descrição
O número máximo de encadeamentos que são permitidos a existir no conjunto de encadeamentos.

Type
Integer

Nomes

Nome do Atributo
Thread_Pool_Max_Size

Nome da Coluna
TPMAXSZ

Atributo Encadeamentos Ativos do Conjunto de Encadeamentos

Descrição
O número de encadeamentos no conjunto de encadeamentos que atualmente estão ativos e em operação.

Type
Integer

Nomes

Nome do Atributo
Thread_Pool_Active_Threads

Nome da Coluna
TPACTTH

Atributo Média de Encadeamentos Ativos do Conjunto de Encadeamentos

Descrição
O número médio de encadeamentos no conjunto de encadeamentos que estão ativos e em operação simultaneamente.

Type
Integer

Nomes

Nome do Atributo
Thread_Pool_Avg_Active_Threads

Nome da Coluna
TPAVGAT

Atributo Mínimo de Encadeamentos Ativos do Conjunto de Encadeamentos

Descrição
O número mínimo de encadeamentos no conjunto de encadeamentos que estão ativos e em operação simultaneamente.

Type
Integer

Nomes

Nome do Atributo
Thread_Pool_Min_Active_Threads

Nome da Coluna
TPMINAT

Atributo Máx. de Encadeamentos Ativos do Conjunto de Encadeamentos

Descrição
O número de pico de encadeamentos no conjunto de encadeamentos que estão ativos e em operação simultaneamente.

Type
Integer

Nomes

Nome do Atributo
Thread_Pool_Max_Active_Threads

Nome da Coluna
TPMAXAT

Atributo de Comprimento da Fila do Conjunto de Encadeamentos

Descrição
O número de tarefas que estão aguardando na fila do conjunto de encadeamentos.

Type
Integer

Nomes

Nome do Atributo
Thread_Pool_Queue_Length

Nome da Coluna
TPQLGTH

Atributo de Comprimento Médio da Fila do Conjunto de Encadeamentos

Descrição
O comprimento médio da fila do conjunto de encadeamentos durante esta execução.

Type
Integer

Nomes

Nome do Atributo
Thread_Pool_Avg_Queue_Length

Nome da Coluna
TPAVGQL

Atributo Comprimento Mín. da Fila do Conjunto de Encadeamentos

Descrição
O comprimento mínimo que a fila do conjunto de encadeamentos atingiu.

Type
Integer

Nomes

Nome do Atributo
Thread_Pool_Min_Queue_Length

Nome da Coluna
TPMINQL

atributo Comprimento Máximo da Fila do Conjunto de Encadeamentos

Descrição
O comprimento de pico que a fila do conjunto de encadeamentos alcançou.

Type
Integer

Nomes

Nome do Atributo
Thread_Pool_Max_Queue_Length

Nome da Coluna
TPMAXQL

Atributo Média de Espera de Tarefa do Conjunto de Encadeamentos

Descrição
O tempo médio gasto por uma tarefa aguardando na fila do conjunto de encadeamentos.

Type
Integer

Nomes

Nome do Atributo
Thread_Pool_Avg_Job_Wait

Nome da Coluna
TPAVJBW

Atributo de Total de Tarefas do Conjunto de Encadeamentos

Descrição
O número de tarefas que são concluídas por todos os encadeamentos no conjunto desde a inicialização do agente.

Type
Integer

Nomes

Nome do Atributo
Thread_Pool_Total_Jobs

Nome da Coluna
TPTJOBS

Nó do Atributo de Log de Eventos

O grupo de atributos Log de eventos contém todas as entradas de logs de eventos recentes que pertencem ao aplicativo.

Por padrão, o agente exibe somente eventos que ocorrem após o agente ser criado. Os eventos são removidos da visualização Log de Eventos 1 hora após ocorrerem.

A lista a seguir contém informações sobre cada atributo no grupo de atributos Log de Eventos:

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente

Type
Sequência

Nomes

Nome do Atributo
Nó

Nome da Coluna
ORIGINNODE

atributo Nome do Log

Descrição
O log de eventos - Aplicação, Sistema, Segurança ou um log específico do aplicativo

Type
Sequência

Nomes

Nome do Atributo
Log_Name

Nome da Coluna
LOGNAME

atributo Fonte de Eventos

Descrição
A origem de eventos definida pelo aplicativo

Type
Sequência

Nomes

Nome do Atributo
Event_Source

Nome da Coluna
EVTSOURCE

atributo Tipo de Evento

Descrição
Tipo de Evento - Error(0), Warning(1), Informational(2), Audit_Success(3), Audit_Failure(4), Unknown(5)

Type
Integer

Nomes

Nome do Atributo
Event_Type

Nome da Coluna
EVTTYPE

atributo ID do Evento

Descrição
O ID do evento

Type
Integer

Nomes

Nome do Atributo
Event_ID

Nome da Coluna
EVTID

atributo Categoria do Evento

Descrição
A categoria do evento

Type
Sequência

Nomes

Nome do Atributo
Event_Category

Nome da Coluna
EVTCATEG

atributo Mensagem

Descrição
A mensagem do evento

Type
Sequência

Nomes

Nome do Atributo
Mensagem

Nome da Coluna
MESSAGE

atributo Hora de Geração

Descrição
A hora em que o evento foi gerado

Type
Hora

Nomes

Nome do Atributo
Time_Generated

Nome da Coluna
TIMESTAMP

Resumo do Arquivo de Log

Os atributos desse grupo de atributos são incluídos nos grupos de atributo de resumo quando essa opção é selecionada nas propriedades avançadas da origem de dados.

Um nó Resumo é criado para cada origem de dados Arquivo de Log quando **Incluir atributo no grupo de atributos de resumo** é selecionado nas propriedades avançadas da origem de dados. O nome do nó de resumo é o nome da origem de dados com Resumo incluído no final.

A lista a seguir contém informações sobre cada um dos atributos padrão no grupo de atributos de Resumo de Arquivo de Log. Esses atributos são sempre incluídos nos grupos de atributos de resumo. Se você selecionar **Incluir atributo no grupo de atributos de resumo**, consulte a etapa “9” na página 1266 em (“Monitorando um Arquivo de Log” na página 1262), depois o grupo de atributos de resumo para esse grupo de atributos do log também conterá cada um dos atributos que você selecionou. Os valores são uma cópia do atributo correspondente no grupo de atributos de arquivo de log.

Todos os atributos incluídos juntos se tornam uma chave e a tabela de resumo inclui uma linha por conjunto de chaves exclusivo. A linha indica quantos registros são recebidos durante o intervalo em que todas as chaves fornecidas correspondiam ao valor relatado nos atributos correspondentes.

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente

Type
Sequência

Nomes

Nome do Atributo
Nó

Nome da Coluna
ORIGINNODE

atributo Time stamp

Descrição
O horário local no agente quando os dados foram coletados

Type
Hora

Nomes

Nome do Atributo
Registro de Data e Hora

Nome da Coluna
TIMESTAMP

atributo Unidade de Intervalo

Descrição
O número de segundos entre a geração do atributo de resumo

Type
Número inteiro (calibrador)

Nomes

Nome do Atributo
_Interval_Unit

Nome da Coluna
IU

atributo Intervalo

Descrição
Deslocamento do intervalo atual dentro da próxima unidade de tempo maior (por exemplo, minutos dentro de uma hora)

Type
Número inteiro (calibrador)

Nomes

Nome do Atributo
_Interval

Nome da Coluna
INV

atributo Ocorrências

Descrição
O número de ocorrências registradas durante o intervalo

Type
Número inteiro (calibrador)

Nomes

Nome do Atributo
_Occurrences

Nome da Coluna
OCC

atributo LocalTimeStamp

Descrição
A hora em que os dados do resumo foram gerados

Type
Registro de Data e Hora

Nomes

Nome do Atributo
_LocalTimeStamp

Nome da Coluna
LTS

atributo DateTime

Descrição
A hora em que os dados do resumo foram gerados

Type
Sequência

Nomes

Nome do Atributo
_Date_Time

Nome da Coluna
DT

atributo Nome da Unidade de Intervalo

Descrição
A descrição da unidade de intervalo

Type
Sequência

Nomes

Nome do Atributo
_Interval_Unit_Name

Nome da Coluna
IUN

Grupo de Atributos de Log Binário do AIX

O grupo de atributos de Log Binário do AIX exibe eventos a partir do Log Binário do AIX conforme selecionados pela sequência de caracteres de comando `errpt`.

A lista a seguir contém informações sobre cada atributo no Grupo de Atributos de Log Binário do AIX:

Nota: O Agent Builder evita a remoção, a reordenação ou a mudança do tamanho dos atributos `Identifier`, `ErrptTimestamp`, `Type`, `Class`, `ResourceName` e `Description`. O agente analisa os dados que voltam de um comando `errpt` que é baseado em colunas com a linha de texto. Essas colunas são definidas pela ordem e tamanho dos atributos `Identificador`, `ErrptTimestamp`, `Tipo`, `Classe`, `ResourceName` e `Descrição`. Remover, reordenar ou alterar o tamanho destes atributos altera o atributo em que as várias colunas entram. A linha resultante, conforme visto no Tivoli Monitoring, está, portanto, incorreta.

No entanto, é possível renomear esses atributos.

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente

Type
Sequência

Nomes

Nome do Atributo
Nó

Nome da Coluna
ORIGINNODE

Atributo do Identificador - Esse atributo é um atributo-chave

Descrição
O identificador de evento reportado pelo `errpt`

Type
Sequência

Nomes

Nome do Atributo
Identificador

Nome da Coluna
IDENTIFIER

Atributo ErrptTimestamp

Descrição
O horário em que o evento é registrado, conforme relatado por `errpt`.

Nota: Este atributo está oculto no tempo de execução. Esse atributo contém um valor bruto. Outros atributos que são derivados deste atributo exibem o valor de uma forma mais utilizável. Esse atributo está disponível no Agent Builder para esse propósito, mas, por padrão, não está visível no ambiente Tivoli Monitoring no tempo de execução. Se desejar torná-lo visível, selecione o atributo na página **Definição de Origem de Dados** no Agent Editor e selecione **Exibir atributo no Tivoli Enterprise Portal**.

Type
Sequência

Nomes

Nome do Atributo
ErrptTimestamp

Nome da Coluna
ERRPTTIMES

Type

Descrição
O tipo de evento de caractere único reportado pelo `errpt`, um de `I(NFO)`, `P(END/ERF/ERM)`, `T(EMP)` e `U(NKN)`

Type
Sequência

Nomes

Nome do Atributo
Type

Nome da Coluna
TYPE

Atributo de Classe - Esse atributo é um atributo-chave

Descrição
A classe de eventos reportada pelo `errpt`, um de `Hardware`, `Software`, `Operador eIndeterminado`. Esses valores são numerados. Os valores brutos para uso com situações são H, S, O e U.

Type
Sequência

Nomes

Nome do Atributo
Classe

Nome da Coluna
CLASS

ResourceName

Descrição
O nome do recurso reportado pelo `errpt`, identifica a origem do registro de erro

Type
Sequência

Nomes

Nome do Atributo
ResourceName

Nome da Coluna
RESOURCENA

Atributo Description

Descrição
A descrição reportada pelo `errpt`, normalmente uma pequena mensagem de texto que descreve a natureza do erro.

Type
Sequência

Nomes

Nome do Atributo
Descrição

Nome da Coluna
DESCRIPTIO

Atributo LogFile

Descrição
O nome completo do log binário `errpt` incluindo o caminho.

Nota: Este atributo está oculto no tempo de execução. Esse atributo contém um valor bruto. Outros atributos que são derivados deste atributo exibem o valor de uma forma mais utilizável. Esse atributo está disponível no Agent Builder para esse propósito, mas, por padrão, não está visível no ambiente Tivoli Monitoring no tempo de execução. Se desejar torná-lo visível, selecione o atributo na página **Definição de Origem de Dados** no Agent Editor e selecione **Exibir atributo no Tivoli Enterprise Portal**.

Type
Sequência

Nomes

Nome do Atributo
LogFile

Nome da Coluna
LOGFILE

Atributo System

Descrição
O nome do host do sistema em que o erro foi coletado

Type
Sequência

Nomes

Nome do Atributo
Sistema

Nome da Coluna
SYSTEM

Atributo LogName

Descrição
O nome base do log binário `errpt` a partir do qual o registro foi coletada

Type
Sequência

Nomes

Nome do Atributo
LogName

Nome da Coluna
LOGNAME

Atributo LogPath

Descrição
O nome de diretório que contém o log binário `errpt` a partir do qual o registro foi coletado

Type
Sequência

Nomes

Nome do Atributo
LogPath

Nome da Coluna
LOGPATH

Atributo EntryTime

Descrição
A hora em que o evento foi registrado como relatado por `errpt` no formato do Registro de Data e Hora do Tivoli. Esse horário não é necessariamente idêntico ao horário em que o agente recebeu o evento, conforme registrado no campo **`Registro de data e hora`**.

Type
Registro de Data e Hora

Nomes

Nome do Atributo
EntryTime

Nome da Coluna
ENTRYTIME

Grupos de Atributos do Monitor e de Notificação

Definições dos grupos de atributos Monitor e Notificação

Os primeiros 4 são específicos para monitores e o último é para notificações (todos estão relacionados ao JMX).

Cada um está listado com uma indicação se é ou não baseado em evento. Para grupos de atributos não baseados em eventos, os dados são coletados quando necessário. Para grupos de atributos baseados em eventos, o agente mantém um cache dos últimos 100 eventos recebidos. Esses eventos são utilizados para responder aos pedidos do Tivoli Enterprise Portal. Os eventos são redirecionados imediatamente para análise por situações e pelo armazenamento.

Notificações de Contador
O grupo de atributos Notificações de Contador é um grupo de atributos baseado em não evento que envia eventos que são recebidos por todos os monitores de contador.

A lista a seguir contém informações sobre cada atributo no grupo de atributos de Notificações do Contador:

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente

Type
Sequência

Nomes

Nome do Atributo
Nó

Nome da Coluna
ORIGINNODE

atributo Time stamp

Descrição
O horário local no agente quando os dados foram coletados

Type
Hora

Nomes

Nome do Atributo
Registro de Data e Hora

Nome da Coluna
TIMESTAMP

Atributo de Tipo de Notificação

Descrição
O tipo de notificação recebida. Descreve como o atributo observado do MBean acionou a notificação.

Type
Sequência

Nomes

Nome do Atributo
Notification_Type

Nome da Coluna
NOTIFICATI

Atributo do ID do Monitor

Descrição
O ID do Monitor do monitor que gerou esta notificação

Type
Integer

Nomes

Nome do Atributo
Monitor_ID

Nome da Coluna
MONITOR_ID

Atributo MBean Observado

Descrição
O MBean cujo atributo está sendo monitorado

Type
Sequência

Nomes

Nome do Atributo
Observed_MBean

Nome da Coluna
OBSERVED_M

Atributo Atributo Observado

Descrição
Nome do atributo que é monitorado no MBean Observado

Type
Sequência

Nomes

Nome do Atributo
Observed_Attribute

Nome da Coluna
OBSERVED_A

Atributo de Limite

Descrição
O limite atual do monitor

Type
Sequência

Nomes

Nome do Atributo
Limite

Nome da Coluna
THRESHOLD

Atributo de deslocamento

Descrição
O valor incluído no limite toda vez que o atributo exceder o limite. Esta valor forma uma novo limite.

Type
Sequência

Nomes

Nome do Atributo
Deslocamento

Nome da Coluna
OFFSET

Atributo de módulo

Descrição
O valor máximo do atributo. Quando ele atinge este valor, ele reinicie e começa a contagem do zero novamente.

Type
Integer

Nomes

Nome do Atributo
Modulus

Nome da Coluna
MODULUS

Atributo Valor do Contador

Descrição
O valor do contador que acionou a notificação

Type
Integer

Nomes

Nome do Atributo
Counter_Value

Nome da Coluna
COUNTER_VA

Atributo de Registro de Data e Hora da Notificação

Descrição
Hora em que a notificação foi acionada

Type
Hora

Nomes

Nome do Atributo
Notification_Time_Stamp

Nome da Coluna
NOTIFICAT0

Atributo da Mensagem de Notificação

Descrição
A mensagem na notificação

Type
Sequência

Nomes

Nome do Atributo
Notification_Message

Nome da Coluna
NOTIFICAT1

Notificações de Calibre
O grupo de atributos Notificações de Calibre é um atributo de base baseado em não evento que envia eventos que são recebidos por todos os monitores de calibre.

A lista a seguir contém informações sobre cada atributo no grupo de atributos das Notificações de Calibre:

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente

Type
Sequência

Nomes

Nome do Atributo
Nó

Nome da Coluna
ORIGINNODE

atributo Time stamp

Descrição
O horário local no agente quando os dados foram coletados

Type
Hora

Nomes

Nome do Atributo
Registro de Data e Hora

Nome da Coluna
TIMESTAMP

Atributo de Tipo de Notificação

Descrição
O tipo de notificação recebida. Descreve como o atributo observado do MBean acionou a notificação.

Type
Sequência

Nomes

Nome do Atributo
Notification_Type

Nome da Coluna
NOTIFICATI

Atributo do ID do Monitor

Descrição
O ID do Monitor do monitor que gerou esta notificação

Type
Integer

Nomes

Nome do Atributo
Monitor_ID

Nome da Coluna
MONITOR_ID

Atributo MBean Observado

Descrição
O MBean cujo atributo está sendo monitorado

Type
Sequência

Nomes

Nome do Atributo
Observed_MBean

Nome da Coluna
OBSERVED_M

Atributo Atributo Observado

Descrição
Nome do atributo que é monitorado no MBean Observado

Type
Sequência

Nomes

Nome do Atributo
Observed_Attribute

Nome da Coluna
OBSERVED_A

Atributo de Limite Baixo

Descrição
O limite que o monitor está observando para que o atributo observado ultrapasse

Type
Sequência

Nomes

Nome do Atributo
Low_Threshold

Nome da Coluna
LOW_THRESH

Atributo de Limite Alto

Descrição
O limite que o monitor está observando para que o atributo observado ultrapasse

Type
Sequência

Nomes

Nome do Atributo
High_Threshold

Nome da Coluna
HIGH_THRES

Atributo de Valor de Calibre

Descrição
Valor do calibre que acionou a notificação

Type
Sequência

Nomes

Nome do Atributo
Gauge_Value

Nome da Coluna
MODULUSGAUGE_VALU

Atributo de Registro de Data e Hora da Notificação

Descrição
Hora em que a notificação foi acionada

Type
Hora

Nomes

Nome do Atributo
Notification_Time_Stamp

Nome da Coluna
NOTIFICAT0

Atributo da Mensagem de Notificação

Descrição
A mensagem na notificação

Type
Sequência

Nomes

Nome do Atributo
Notification_Message

Nome da Coluna
NOTIFICAT1

Monitores Registrados
O atributo de monitor Monitores Registrados é um grupo de atributos baseado em evento que mostra uma lista de todos os Monitores JMX que são criados pelo agente.

A lista a seguir contém informações sobre cada atributo no grupo de atributos de Monitores Registrados:

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente

Tipo
Cadeia

Nomes

Nome do Atributo
Node

Nome da Coluna
ORIGINNODE

atributo Time stamp

Descrição
O horário local no agente quando os dados foram coletados

Tipo
Hora

Nomes

Nome do Atributo
Registro de data e hora

Nome da Coluna
TIMESTAMP

Atributo de ID de monitor - Este atributo é um atributo-chave

Descrição
O identificador inteiro exclusivo para um monitor

Tipo
Integer

Nomes

Nome do Atributo
Monitor_ID

Nome da Coluna
MONITOR_ID

Atributo de Parâmetros do Monitor

Descrição
Os parâmetros que são usados para criar o monitor

Tipo
Cadeia

Nomes

Nome do Atributo
Monitor_Parameters

Nome da Coluna
MONITOR_PA

Atributo de Nome do Monitor

Descrição
O Nome do Objeto do JMX do MBean do monitor

Tipo
Cadeia

Nomes

Nome do Atributo
Monitor_Name

Nome da Coluna
MONITOR_NA

Notificações de Sequência
O grupo de atributos Notificações de Sequência é um grupo de atributos baseado em não evento que envia eventos que são recebidos por todos os monitores de sequência.

A lista a seguir contém informações sobre cada atributo no grupo de atributos de Notificações de Cadeia:

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente

Type
Sequência

Nomes

Nome do Atributo
Nó

Nome da Coluna
ORIGINNODE

atributo Time stamp

Descrição
O horário local no agente quando os dados foram coletados

Type
Hora

Nomes

Nome do Atributo
Registro de Data e Hora

Nome da Coluna
TIMESTAMP

Atributo de Tipo de Notificação

Descrição
O tipo de notificação recebida. Descreve como o atributo observado do MBean acionou a notificação.

Type
Sequência

Nomes

Nome do Atributo
Notification_Type

Nome da Coluna
NOTIFICATI

Atributo de ID de monitor - Este atributo é um atributo-chave

Descrição
O identificador inteiro exclusivo para um monitor

Type
Integer

Nomes

Nome do Atributo
Monitor_ID

Nome da Coluna
MONITOR_ID

Atributo MBean Observado

Descrição
O MBean cujo atributo está sendo monitorado

Type
Sequência

Nomes

Nome do Atributo
Observed_MBean

Nome da Coluna
OBSERVED_M

Atributo Atributo Observado

Descrição
Nome do atributo que é monitorado no MBean Observado

Type
Sequência

Nomes

Nome do Atributo
Observed_Attribute

Nome da Coluna
OBSERVED_A

Atributo Comparar Cadeia

Descrição
A sequência que é usada na operação de comparação

Type
Sequência

Nomes

Nome do Atributo
Compare_String

Nome da Coluna
COMPARE_ST

Atributo de Valor de Cadeia

Descrição
O valor do atributo que acionou a notificação

Type
Sequência

Nomes

Nome do Atributo
String_Value

Nome da Coluna
STRING_VAL

Atributo de Registro de Data e Hora da Notificação

Descrição
Hora em que a notificação foi acionada

Type
Hora

Nomes

Nome do Atributo
Notification_Time_Stamp

Nome da Coluna
NOTIFICAT0

Atributo da Mensagem de Notificação

Descrição
A mensagem na notificação

Type
Sequência

Nomes

Nome do Atributo
Notification_Message

Nome da Coluna
NOTIFICAT1

Grupos de Atributos do Evento SNMP

Os grupos de atributos do evento SNMP são usados para receber traps e informs. Esses grupos de atributos são grupos de atributos baseados em evento

A lista a seguir contém informações sobre cada atributo nos Grupos de Atributos do Evento SNMP:

Nota: É possível alterar o nome de exibição padrão desses atributos. Esses nomes de exibição são distintos do ID interno de cada atributo.

Enterprise_OID
O OID corporativo que gerou o trap.

Source_Address
O nome do host ou o endereço IP do agente SNMP que enviou o trap.

Generic_Trap
Número de trap genérico que é extraído do trap recebido. Possíveis valores:

```
0 ColdStart
1 WarmStart
2 LinkDown
3 LinkUp
4 Authentication Failure
5 EGPNeighborLoss
```

Specific_Trap
Número de trap específico da empresa que é extraído do trap recebido. Aplica-se somente quando Generic_Trap = 6.

Alert_Name
Nome do trap conforme especificado na definição no arquivo de configuração do trap.

Categoria
Categoria do trap conforme especificado na definição no arquivo de configuração do trap.

Descrição
Descrição do trap conforme especificado na definição no arquivo e configuração do trap. O comprimento máximo da descrição é de 256 caracteres.

Enterprise_Name
Nome do Corporativo do Trap conforme especificado no arquivo de configuração do trap e determinado por meio do identificador de objeto do trap.

Source_Status
Status do agente que originou o trap após o trap ser enviado conforme especificado na definição de trap no arquivo de configuração de trap.

Source_Type
Tipo do agente que originou o trap, conforme especificado na definição do trap no arquivo de configuração do trap.

Event_Variables
Os dados da ligação de variável (VarBind) que são recebidos na unidade de dados de protocolo de trap (PDU). A sequência é construída da seguinte forma:

```
{OID[type]=value}{OID[type]=value}{oid[type]=value}...
```

Em que:

oid
Identificador de objeto da variável MIB

tipo
Tipo de dados SMI

value
Valor da variável

{}
Cada trio é cercado por chaves ({}).

Nota: Os atributos Alert Name, Category, Description, Enterprise_Name, Source_Status e Source_Type fornecem informações adicionais. Na janela **Navegador MIB SNMP**, selecione a caixa de seleção **Incluir atributos que mostram informações definidas no arquivo de configuração de trap** para incluir esses atributos.

Grupos de atributos de eventos JMX

Os grupos de atributos de eventos do JMX são utilizados para receber notificações a partir de um servidor MBean.

Estes grupos de atributos não baseados em eventos e são gerados com os seguintes atributos que podem ser editados pelo desenvolvedor do agente.

A lista a seguir contém informações sobre cada atributo nos Grupos de Atributos de Eventos do JMX:

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente

Type
Sequência

Nomes

Nome do Atributo
Nó

Nome da Coluna
ORIGINNODE

atributo Time stamp

Descrição
O horário local no agente quando os dados foram coletados

Type
Hora

Nomes

Nome do Atributo
Registro de Data e Hora

Nome da Coluna
TIMESTAMP

Atributo Tipo

Descrição
O tipo de notificação

Type
Sequência

Nomes

Nome do Atributo
Type

Nome da Coluna
TYPE

Atributo de origem

Descrição
O MBean que causou a notificação a ser enviada

Type
Sequência

Nomes

Nome do Atributo
Origem

Nome da Coluna
SOURCE

Atributo de Número de Seqüência

Descrição
O número de seqüência a partir do objeto de notificação

Type
Sequência

Nomes

Nome do Atributo
Sequence_Number

Nome da Coluna
SEQUENCE_N

atributo Mensagem

Descrição
A mensagem de notificação

Type
Sequência

Nomes

Nome do Atributo
Mensagem

Nome da Coluna
MESSAGE

Atributo de Dados do Usuário

Descrição
O objeto de dados do usuário a partir da notificação

Type
Sequência

Nomes

Nome do Atributo
User_Data

Nome da Coluna
USER_DATA

Grupo de Atributos de Ping

O grupo de atributos de ping contém os resultados dos pings de ICMP que são enviados às listas de dispositivos.

A lista a seguir contém informações sobre cada atributo no Grupo de Atributos de Ping:

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente.

Type
Sequência

Nomes

Nome do Atributo
Nó

Nome da Coluna
ORIGINNODE

atributo Time stamp

Descrição
O horário que é coletado do sistema de agente quando a linha de dados é criada e enviada do agente para o Tivoli Enterprise Monitoring Server. Ou armazenada para propósitos históricos. Representa o fuso horário local do sistema do agente.

Type
Hora

Nomes

Nome do Atributo
Registro de Data e Hora

Nome da Coluna
TIMESTAMP

Atributo de endereço - Esse atributo é um atributo-chave

Descrição
O endereço IP do host que é monitorado.

Type
Sequência com valor enumerado. O valor UNKNOWN_ADDRESS será exibido, se o endereço IP for desconhecido. O armazém e as consultas retornam 0.0.0.0 para essa enumeração. Quaisquer outros valores do endereço IP são exibidos no estado em que se encontram.

Nomes

Nome do Atributo
Endereço

Nome da Coluna
PNGADDR

Atributo de Entrada do Dispositivo - Esse atributo é um atributo-chave

Descrição
A entrada no arquivo de lista de dispositivos para este nó.

Type
Sequência

Nomes

Nome do Atributo
Device_Entry

Nome da Coluna
PINGDEVC

Atributo de tempo de resposta atual

Descrição
O tempo de resposta de rede atual para pedidos de ICMP para o nó gerenciado em milissegundos.

Type
Inteiro com valores enumerados. As sequências são exibidas no Tivoli Enterprise Portal. O armazém e as consultas retornam os números. Os valores definidos são `TIMEOUT(-1)` e `SEND_FAILURE(-2)`. Quaisquer outros valores mostram o valor numérico.

Nomes

Nome do Atributo
Current_Response_Time

Nome da Coluna
PINGRSTM

atributo Nome

Descrição
O nome do host do nó gerenciado. Se o endereço do nó não puder ser resolvido por meio de DNS, o endereço IP decimal com pontos será mostrado.

Type
Sequência com valor enumerado. Um valor UNKNOWN_HOSTNAME será exibido, se o nome do host for desconhecido. O armazém e as consultas retornam 0.0.0.0 para essa enumeração. Quaisquer outros valores de nome do host são exibidos como estão.

Nomes

Nome do Atributo
Nome

Nome da Coluna
PNGNAME

Atributo de Descrição do Nó

Descrição
A descrição do nó gerenciado.

Type
Sequência

Nomes

Nome do Atributo
Node_Description

Nome da Coluna
PNGDESC

Atributo de Status do Nó

Descrição
O status operacional atual do nó gerenciado.

Type
Inteiro com valores enumerados. As sequências são exibidas no Tivoli Enterprise Portal. O armazém e as consultas retornam os números. Os valores definidos são `INVALID(-2)`, `UNKNOWN(-1)`, `INACTIVE(0)` e `ACTIVE(1)`.

Nomes

Nome do Atributo
Node_Status

Nome da Coluna
PNGSTAT

Atributos de Tipo de Nó

Descrição
O tipo do nó gerenciado. Se o nó estiver on-line, ele será um Nó IP. Se ele estiver off-line, o tipo será Desconhecido.

Type
Inteiro com valores enumerados. As sequências são exibidas no Tivoli Enterprise Portal. O armazém e as consultas retornam os números. Os valores definidos são `UNKNOWN(0)` e `IP NODE(1)`.

Nomes

Nome do Atributo
Node_Type

Nome da Coluna
PNGTYPE

Registro de Data e Hora do Status

Descrição
A data e hora em que o nó foi verificado pela última vez.

Type
Hora

Nomes

Nome do Atributo
Status_Timestamp

Nome da Coluna
PNGTMSP

Grupos de Atributos HTTP

Os dois grupos de atributos HTTP, `URLs Gerenciadas` e `Objetos de URL`, são usadas para receber informações das URLs e os objetos dentro dessas URLs.

Para obter informações sobre a sintaxe usada nas URLs Gerenciadas e nas tabelas de Objetos da URL, consulte (“Campos Específicos para Atributos HTTP” na página 1299).

URLs Gerenciadas

A lista a seguir contém informações sobre cada atributo no Grupo de Atributos URL Gerenciada:

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente

Type
Sequência

Nomes

Nome do Atributo
Nó

Nome da Coluna
ORIGINNODE

atributo Time stamp

Descrição
O horário local no agente quando os dados foram coletados

Type
Hora

Nomes

Nome do Atributo
Registro de Data e Hora

Nome da Coluna
TIMESTAMP

Atributo URL - Esse atributo é um atributo-chave

Descrição
A URL que está sendo monitorada.

Type
Sequência

Nomes

Nome do Atributo
URL

Nome da Coluna
HTTPURL

Atributo Response Time

Descrição
A quantidade de tempo que demora para fazer download da resposta em milissegundos.

Type
Número inteiro com valor enumerado. A sequência é exibida no Tivoli Enterprise Portal, o warehouse e as consultas retornarão o número. O valor definido é `TIMEOUT (-1)`.

Nomes

Nome do Atributo
Response_Time

Nome da Coluna
HTTPURL

Atributo Page Size

Descrição
O tamanho da página que é retornada pela solicitação de HTTP.

Type
Número inteiro com valor enumerado. A sequência é exibida no Tivoli Enterprise Portal, o warehouse e as consultas retornarão o número. O valor definido é `NO_RESPONSE_RECEIVED(-1)`.

Nomes

Nome do Atributo
Page_Size

Nome da Coluna
PAGESZ

Atributo Page Objects

Descrição
O número total de objetos associados à página monitorada.

Type
Número inteiro com valor enumerado. A sequência é exibida no Tivoli Enterprise Portal, o warehouse e as consultas retornarão o número. O valor definido é `NOT_COLLECTED(-1)`.

Nomes

Nome do Atributo
Page_Objects

Nome da Coluna
PGOBJS

Atributo Total Object Size

Descrição
O tamanho da página que é retornada pela solicitação de HTTP.

Type
Número inteiro com valor enumerado. A sequência é exibida no Tivoli Enterprise Portal, o warehouse e as consultas retornarão o número. O valor definido é `NOT_COLLECTED(-1)`.

Nomes

Nome do Atributo
Total_Object_Size

Nome da Coluna
TOTOSZ

Atributo Page Title

Descrição
O título da página da URL recebida.

Type
Sequência

Nomes

Nome do Atributo
Page_Title

Nome da Coluna
PAGETTL

Atributo Server Type

Descrição
O tipo de servidor que é usado no website da URL de destino.

Type
Sequência

Nomes

Nome do Atributo
Server_Type

Nome da Coluna
SRVTYP

Atributo Response Code

Descrição
O código de resposta da solicitação de HTTP.

Type
Número inteiro com valor enumerado. A sequência é exibida no Tivoli Enterprise Portal, o warehouse e as consultas retornarão o número. O valor definido é `NO_RESPONSE_RECEIVED(-1)`.

Nomes

Nome do Atributo
Response_Code

Nome da Coluna
CODE

Atributo Status

Descrição
O status atual da URL gerenciada (OK ou descrição do status).

Type
Sequência

Nomes

Nome do Atributo
Estado

Nome da Coluna
STATUS

Atributo URL Alias

Descrição
O alias especificado pelo usuário para a URL.

Type
Sequência

Nomes

Nome do Atributo
URL_Alias

Nome da Coluna
ALIAS

Atributo de Dados do Usuário

Descrição
Os dados do usuário especificados com a URL.

Type
Sequência

Nomes

Nome do Atributo
User_Data

Nome da Coluna
USER

Objetos da URL

A lista a seguir contém informações sobre cada atributo no Grupo de Atributos de Objetos de URL:

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente

Type
Sequência

Nomes

Nome do Atributo
Nó

Nome da Coluna
ORIGINNODE

atributo Time stamp

Descrição
O horário local no agente quando os dados foram coletados

Type
Hora

Nomes

Nome do Atributo
Registro de Data e Hora

Nome da Coluna
TIMESTAMP

Atributo URL - Esse atributo é um atributo-chave

Descrição
A URL que está sendo monitorada.

Type
Sequência

Nomes

Nome do Atributo
URL

Nome da Coluna
HTTPURL

Atributo Nome do Objeto

Descrição
O nome do objeto da página dentro da URL de destino.

Type
Sequência

Nomes

Nome do Atributo
Object_Name

Nome da Coluna
ONAME

Atributo Object Size

Descrição
O tamanho (bytes) do objeto da página dentro da URL de destino.

Type
Inteiro com valores enumerados. As sequências são exibidas no Tivoli Enterprise Portal. O armazém e as consultas retornam os números. Os valores definidos são `NOT_COLLECTED (-1)`, `OBJECT_NOT_FOUND (-2)`. Quaisquer outros valores mostram o valor numérico.

Nomes

Nome do Atributo
Object_Size

Nome da Coluna
SIZE

Atributo Object Response Time

Descrição
A quantidade de tempo que demora para fazer download do objeto em milissegundos.

Type
Inteiro com valores enumerados. As sequências são exibidas no Tivoli Enterprise Portal. O armazém e as consultas retornam os números. Os valores definidos são `NOT_COLLECTED (-1)`, `NO_RESPONSE_RECEIVED (-2)`, `STATUS_CODE_ERROR (-3)`. Quaisquer outros valores mostram o valor numérico.

Nomes

Nome do Atributo
Object_Response_Time

Nome da Coluna
ORTIME

Grupos de Atributos de Descoberta

Um grupo de atributos que representa o conjunto de instâncias de subnó que está definido para um tipo de subnó.

Ao criar um tipo de subnó, é criado um grupo de atributos que representa o conjunto de instâncias do subnó que estão definidas para esse tipo de subnó. Cada um destes grupos de atributos inclui o mesmo conjunto de atributos.

A lista a seguir contém informações sobre cada atributo em um Grupo de atributos de descoberta. O nome com texto em negrito mostra como o atributo é exibido no Tivoli Enterprise Portal:

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente

Type
Sequência

Nomes

Nome do Atributo
Nó

Nome da Coluna
ORIGINNODE

atributo Time stamp

Descrição
O horário do sistema de agente quando a linha de dados foi construída e enviada para o Tivoli Enterprise Monitoring Server (ou armazenada para propósitos históricos). Representa o fuso horário local do sistema do agente.

Type
Hora

Nomes

Nome do Atributo
Registro de Data e Hora

Nome da Coluna
TIMESTAMP

Atributo de MSN do Subnó

Descrição
O Nome do Sistema Gerenciado do agente do subnó.

Type
Sequência

Nomes

Nome do Atributo
Subnode_MSN

Nome da Coluna
SN_MSN

Atributo de Afinidade do Subnó

Descrição
A afinidade para o agente do subnó.

Type
Sequência

Nomes

Nome do Atributo
Subnode_Affinity

Nome da Coluna
SN_AFFIN

Atributo de Tipo de Subnó

Descrição
O tipo de nó desse subnó.

Type
Sequência

Nomes

Nome do Atributo
Subnode_Type

Nome da Coluna
SN_TYPE

Atributo de Nome de Recurso do Subnó

Descrição
O nome do recurso do agente do subnó.

Type
Sequência

Nomes

Nome do Atributo
Subnode_Resource_Name

Nome da Coluna
SN_RES

Atributo de Versão do Subnó

Descrição
A versão do agente do subnó.

Type

Nomes

Nome do Atributo
Subnode_Version

Nome da Coluna
SN_VER

Grupo de Atributos de Status de Execução de Ação

O atributo de status de Status de Executar Ação contém o status de ações que o agente processou.

Este grupo de atributos é baseado em evento e contém informações sobre cada atributo no grupo de atributos Status de Execução de Ação:

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente.

Type
Sequência

Nomes

Nome do Atributo
Nó

Nome da Coluna
ORIGINNODE

atributo Time stamp

Descrição
O horário que é coletado do sistema de agente quando a linha de dados é criada e enviada do agente para o Tivoli Enterprise Monitoring Server. Ou armazenada para propósitos históricos. Representa o fuso horário local do sistema do agente.

Type
Hora

Nomes

Nome do Atributo
Registro de Data e Hora

Nome da Coluna
TIMESTAMP

Atributo de Nome da Ação

Descrição
O nome da ação que foi executada

Type
Sequência

Nomes

Nome do Atributo
Action_Name

Nome da Coluna
TSKNAME

Atributo de Status da Ação

Descrição
O status da ação.

Type
Inteiro com valores enumerados. Os valores são: OK (0), NOT_APPLICABLE (1), GENERAL_ERROR (2), WARNING (3), NOT_RUNNING (4), DEPENDENT_NOT_RUNNING (5), ALREADY_RUNNING (6), PREREQ_NOT_RUNNING (7), TIMED_OUT (8), DOESNT_EXIST (9), UNKNOWN (10), DEPENDENT_STILL_RUNNING (11), INSUFFICIENT_USER_AUTHORITY (12)

Nomes

Nome do Atributo
Action_Status

Nome da Coluna
TSKSTAT

Atributo de Código de Retorno da Ação do Aplicativo

Descrição
O código de retorno do aplicativo em que a ação foi iniciada.

Type
Integer

Nomes

Nome do Atributo
Action_App_Return_Code

Nome da Coluna
TSKAPRC

Atributo de Mensagem da Ação

Descrição
A mensagem associada ao código de retorno da ação.

Type
Sequência

Nomes

Nome do Atributo
Action_Message

Nome da Coluna
TSKMSGE

Atributo da Instância da Ação

Descrição
A instância associada à saída produzida executando a ação. Se a ação for um comando do sistema, a instância será a número da linha da saída do comando.

Type
Sequência

Nomes

Nome do Atributo
Action_Instance

Nome da Coluna
TSKINST

Atributo de Resultados da Ação

Descrição
A saída produzida executando a ação.

Type
Sequência

Nomes

Nome do Atributo
Action_Results

Nome da Coluna
TSKOUTP

Atributo de Comando de Ação

Descrição
O comando que foi executado pela ação.

Type
Sequência

Nomes

Nome do Atributo
Action_Command

Nome da Coluna
TSKCMND

Atributo de Nó de Ação

Descrição
O nó em que a ação foi executada.

Type
Sequência

Nomes

Nome do Atributo
Action_Node

Nome da Coluna
TSKORGN

Atributo de Subnó de Ação

Descrição
O subnó em que a ação foi executada.

Type
Sequência

Nomes

Nome do Atributo
Action_Subnode

Nome da Coluna
TSKSBND

Atributo do ID da Ação

Descrição
O ID da ação.

Type
Integer

Nomes

Nome do Atributo
Action_ID

Nome da Coluna
TSKID

Atributo de Tipo de Ação

Descrição
O tipo da ação.

Type
Inteiro com valores enumerados. As sequências são exibidas no Tivoli Enterprise Portal, o warehouse e as consultas retornam os números. Os valores definidos são: UNKNOWN (0), AUTOMATION (1).

Nomes

Nome do Atributo
Action_Type

Nome da Coluna
TSKTYPE

Atributo de Proprietário da Ação

Descrição
O nome da situação ou usuário que iniciou a ação.

Type
Sequência

Nomes

Nome do Atributo
Action_Owner

Nome da Coluna
TSKOWNR

Grupo de Atributos de Status do Arquivo de Log

O grupo de atributos Status do Arquivo de Log contém informações que refletem o status dos arquivos de log que este agente está monitorando.

O grupo de atributos Status do Arquivo de Log será incluído se você tiver um grupo de atributos de log e o agente estiver na versão mínima padrão do Tivoli Monitoring de 6.2.1 ou mais recente. O grupo de atributos Status de Arquivo de Log inclui dois atributos que são definidos como números de 64 bits para que eles possam lidar com arquivos grandes. O suporte do atributo numérico de 64 bits é fornecido pelo Tivoli Monitoring versão 6.2.1 ou mais recente.

A lista a seguir contém informações sobre cada atributo no grupo de atributos Status do Arquivo de Log:

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente.

Type
Sequência

Nomes

Nome do Atributo
Nó

Nome da Coluna
ORIGINNODE

atributo Time stamp

Descrição
O valor é o tempo coletado a partir do sistema do agente quando a linha de dados foi construída e enviada a partir do agente para Tivoli Enterprise Monitoring Server. Ou armazenada para propósitos históricos. Representa o fuso horário local do sistema do agente.

Type
Hora

Nomes

Nome do Atributo
Registro de Data e Hora

Nome da Coluna
TIMESTAMP

Atributo de Nome de Tabela - Este atributo é um atributo-chave

Descrição
O nome da tabela na qual este log está sendo monitorado

Type
Sequência

Nomes

Nome do Atributo
Table_Name

Nome da Coluna
TBLNAME

Atributo de Nome de Arquivo - Este atributo é um atributo-chave

Descrição
Nome do arquivo que está sendo monitorado

Type
Sequência

Nomes

Nome do Atributo
File_Name

Nome da Coluna
FILNAME

Atributo de Padrão RegEx - Este atributo é um atributo chave

Descrição
O padrão de expressão regular (se houver) que fez com que este arquivo seja monitorado

Type
Sequência

Nomes

Nome do Atributo
RegEx_Pattern

Nome da Coluna
REPATRN

Atributo Tipo de Arquivo

Descrição
O tipo deste arquivo (arquivo regular ou canal)

Type
Inteiro com valores enumerados. As sequências são exibidas no Tivoli Enterprise Portal. Os valores definidos são UNKNOWN(0), REGULAR FILE(1) e PIPE(2)

Nomes

Nome do Atributo
File_Type

Nome da Coluna
FILTYPE

Atributo Status do Arquivo

Descrição
O status do arquivo que está sendo monitorado

Type
Inteiro com valores enumerados. As sequências são exibidas no Tivoli Enterprise Portal. Os valores definidos são: OK(0), PERMISSION DENIED(1), FILE DOES NOT EXIST(2), INTERRUPTED SYSTEM CALL(4), I/O ERROR(5), NO SUCH DEVICE(6), BAD FILE NUMBER(9), OUT OF MEMORY(12), ACCESS DENIED(13), RESOURCE BUSY(16), NOT A DIRECTORY(20), IS A DIRECTORY(21), INVALID ARGUMENT(22), FILE TABLE OVERFLOW(23), TOO MANY OPEN FILES(24), TEXT FILE BUSY(26), FILE TOO LARGE(27), NO SPACE LEFT ON DEVICE(28), ILLEGAL SEEK ON PIPE(29), READ-ONLY FILE SYSTEM(30), TOO MANY LINKS(31), BROKEN PIPE(32)

Nomes

Nome do Atributo
File_Status

Nome da Coluna
FILSTAT

Atributo Número de Registros Correspondidos

Descrição
O número de registros processados deste log que corresponderam com um dos padrões especificados

Type
Integer

Nomes

Nome do Atributo
Num_Records_Matched

Nome da Coluna
RECMTCH

Atributo Número de Registros Não Correspondidos

Descrição
O número de registros processados enviados para o UnmatchLog; que não corresponderam com nenhum padrão

Type
Integer

Nomes

Nome do Atributo
Num_Records_Not_Matched

Nome da Coluna
RECUNMT

Atributo Número de Registros Processados

Descrição
O número de registros processados deste log desde o início do agente (incluindo aqueles que não são correspondências/eventos)

Type
Integer

Nomes

Nome do Atributo
Num_Records_Processed

Nome da Coluna
RECPROC

Atributo de Posição do Arquivo Atual

Descrição
A posição atual em bytes no arquivo monitorado. Os dados até esta posição são processados, os dados após esta posição não são processados. Não aplicável para canais.

Type
Integer

Nomes

Nome do Atributo
Current_File_Position

Nome da Coluna
OFFSET

Atributo Tamanho do Arquivo Atual

Descrição
O tamanho atual do arquivo monitorado. Não aplicável para canais.

Type
Integer

Nomes

Nome do Atributo
Current_File_Size

Nome da Coluna
FILESIZE

Atributo Horário da Última Modificação

Descrição
O horário quando o arquivo monitorado foi gravado pela última vez. Não aplicável para canais.

Type
Registro de Data e Hora

Nomes

Nome do Atributo
Last_Modification_Time

Nome da Coluna
LASTMOD

Atributo Página de Códigos

Descrição
A página de códigos de idioma do arquivo monitorado

Type
Sequência

Nomes

Nome do Atributo
Página de códigos

Nome da Coluna
CODEPG

Grupo de Atributos Estatísticas de RegEx do Arquivo de Log

O grupo de atributos Estatísticas de RegEx do Arquivo de Log contém informações que mostram as estatísticas das expressões de procura de expressão regular de arquivo de log.

As expressões regulares podem ser usadas para filtrar registros ou para definir registros. Esse grupo de atributos mostra informações sobre ambos os tipos. Quando o atributo de Tipo de Resultado contém um `INCLUDE` ou `EXCLUDE`, o filtro é usado para filtrar registros. Se o atributo de Tipo de Resultado contiver `BEGIN` ou `END`, o filtro é usado para definir registros. As medidas de CPU são aproximações que são baseadas na granularidade dos dados expostos pelo sistema operacional. Essas medições podem resultar em valores de `0,00` quando uma expressão regular demorar um tempo pequeno para avaliar. Utilize os tempos de CPU para determinar o custo relativo de expressões regulares e otimizar o comportamento de expressões regulares específicas.

O grupo de atributos Estatísticas RegEx de Arquivo de Log será incluído se você tiver um grupo de atributos de log e o agente estiver no Tivoli Monitoring versão de 6.2.1 ou mais recente. A versão mínima do Tivoli Monitoring é selecionada na página **Informações do Agente**. Para obter mais informações, consulte (“Nomeando e configurando o agente” na página 1169). O grupo de atributos de Estatísticas de RegEx de Arquivo de Log inclui atributos que são definidos como números de 64 bits para que eles possam tratar longas durações. O suporte para atributos numéricos de 64 bits é fornecido pelo Tivoli Monitoring versão 6.2.1 ou mais recente.

A lista a seguir contém informações sobre cada atributo no grupo de atributos Estatísticas de RegEx do Arquivo de Log:

Atributo de nó - Este atributo é um atributo-chave

Descrição
O nome do sistema gerenciado do agente.

Type
Sequência

Nomes

Nome do Atributo
Nó

Nome da Coluna
ORIGINNODE

atributo Time stamp

Descrição
A hora local no agente quando os dados foram coletados.

Type
Hora

Nomes

Nome do Atributo
Registro de Data e Hora

Nome da Coluna
TIMESTAMP

Atributo de Nome de Tabela - Este atributo é um atributo-chave

Descrição
O nome o grupo de atributos do arquivo de log.

Type
Sequência

Nomes

Nome do Atributo
Table_Name

Nome da Coluna
TBLNAME

Atributo de Nome de Atributo - Este atributo é um atributo-chave

Descrição
O nome do grupo de atributos no qual o filtro é aplicado.

Type
Sequência

Nomes

Nome do Atributo
Attribute_Name

Nome da Coluna
ATRNAME

Número do Filtro

Descrição
O número de sequência, iniciando com zero, do filtro que está sendo utilizado para o atributo.

Type
Número Inteiro (Propriedade Numérica)

Nomes

Nome do Atributo
Filter_Number

Nome da Coluna
FLTRNUM

Atributo Tipo de Resultados

Descrição
O tipo de resultado pode ser INCLUDE ou EXCLUDE para aceitar ou rejeitar o atributo se o filtro corresponde. O tipo de resultado pode ser BEGIN ou END para especificar o início e o término de um registro para registros de multilinhas.

Type
Inteiro com valores enumerados. As sequências são exibidas no Tivoli Enterprise Portal. Se o filtro for usado para filtrar os registros, os valores definidos serão `INCLUDE(1)` ou `EXCLUDE(2)`. Se o filtro for usado para definir registros, os valores definidos serão `BEGIN(3)` ou `END(4)` .

Nomes

Nome do Atributo
Result_Type

Nome da Coluna
RSTTYPE

Atributo de Média de Tempo do Processador

Descrição
O número médio de segundos do processador usados para processar o filtro para este atributo. O tempo médio do processador é o total de segundos do processador dividido pela contagem do filtro.

Type
Inteiro (Calibre)

Nomes

Nome do Atributo
Average_Processor_Time

Nome da Coluna
CPUTAVG

Atributo de Tempo do Processador

Descrição
O número total de segundos do processador usados para processar o filtro para este atributo. O tempo do processador é acumulativo e é truncado, não arredondado. Semelhante a Linux `/proc/<pid>/task/`*`thread`*`/stat file`.

Type
Integer (Counter)

Nomes

Nome do Atributo
Processor_Time

Nome da Coluna
CPUTIME

Atributo Máx. de Tempo do Processador

Descrição
O número máximo de segundos do processador usados para o processamento de um único filtro. É possível que o máximo seja zero caso o filtro nunca tenha sido usado ou se caso cada processamento de filtro tenha demorado menos de 0,01 segundo.

Type
Número inteiro (Calibre)

Nomes

Nome do Atributo
Max_Processor_Time

Nome da Coluna
CPUTMAX

atributo Min de Tempo do Processador

Descrição
O número mínimo de segundos do processador usados para um único processamento de filtro. É possível que o mínimo seja zero caso um processamento de filtro tenha demorado menos de 0,01 segundo.

Type
Número inteiro (Calibre)

Nomes

Nome do Atributo
Min_Processor_Time

Nome da Coluna
CPUTMIN

Atributo de Contagem de Filtro

Descrição
O número de vezes que o filtro é executado. Usado com o tempo total do processador para calcular o tempo médio do processador.

Type
Integer (Counter)

Nomes

Nome do Atributo
Filter_Count

Nome da Coluna
COUNT

Atributo Correspondido de Contagem de Filtro

Descrição
O número de vezes que o filtro é executado e o atributo correspondido.

Type
Integer (Counter)

Nomes

Nome do Atributo
Filter_Count_Matched

Nome da Coluna
COUNTMA

Atributo Não Correspondido de Contagem de Filtro

Descrição
O número de vezes que o filtro é executado e o atributo não correspondeu.

Type
Integer (Counter)

Nomes

Nome do Atributo
Filter_Count_Unmatched

Nome da Coluna
COUNTUN

Atributo de Padrão RegEx - Este atributo é um atributo chave

Descrição
A expressão regular usada para a correspondência.

Type
Sequência

Nomes

Nome do Atributo
RegEx_Pattern

Nome da Coluna
REGXPAT

Atributo do Último Horário Correspondido

Descrição
A última vez que o filtro foi usado e o resultado correspondeu.

Type
Hora

Nomes

Nome do Atributo
Last_Matched_Time

Nome da Coluna
LASTMAT

Atributo Último Horário Não Correspondido

Descrição
A última vez que o filtro foi usado e que o resultado não foi correspondido.

Type
Hora

Nomes

Nome do Atributo
Last_Unmatched_Time

Nome da Coluna
LASTUMA

Criando Extensões de Suporte de Aplicativo para Agentes Existentes

Para o ambiente IBM Tivoli Monitoring, é possível construir um pacote instalável para distribuir áreas de trabalho, situações, consultas e comandos Executar ação customizados que você criou, como uma extensão de suporte de aplicativo para um agente existente.

Antes de Iniciar

Para obter mais informações sobre como criar situações, áreas de trabalho, comandos Executar Ação e consultas customizadas, consulte ("Criando Espaços de Trabalho, Comandos Executar Ação e Situações" na página 1371).

Sobre Esta Tarefa

Importante: Essa tarefa não é a maneira como se inclui o suporte do aplicativo em um agente que está sendo construído. Para incluir um suporte de aplicativo em um agente que está criando, consulte ("Importando Arquivos de Suporte do Aplicativo" na página 1406).

Procedimento

1. No Agent Builder, selecione **Arquivo** > **Novo** > **Outro**.
2. Selecione **Extensão de Suporte de Aplicativo do Agent Builder** em **Agent Builder**.
3. Clique em **Avançar** para obter a página de boas-vindas do assistente **IBM Tivoli Monitoring Application Support Extension**.
4. Clique em **Avançar** na página de boas-vindas.
5. Insira um nome para o projeto e clique em **Concluir**

Criando um Projeto de Extensão de Suporte de Aplicativo

Criar um projeto de Extensão de Suporte de Aplicativo usando o construtor de Agente.

Procedimento

1. No Agent Builder, selecione **Arquivo** > **Novo** > **Outro**.
2. Selecione **Extensão de Suporte de Aplicativo do Agent Builder** em **Agent Builder**.
3. Clique em **Avançar** para acessar a página de boas-vindas para o **Assistente de Extensão de Suporte de Aplicativo IBM Tivoli Monitoring**.

4. Clique em **Avançar** na página de boas-vindas.
5. Insira um nome para o projeto e clique em **Concluir**

Incluindo Arquivos de Suporte a um Projeto

Incluir seus arquivos de suporte em um projeto de Extensão de Suporte de Aplicativo

Antes de Iniciar

Crie um Projeto de Extensão de Suporte de Aplicativo. Para obter mais informações, consulte "Criando um Projeto de Extensão de Suporte de Aplicativo" na página 1474.

Procedimento

1. Clique com o botão direito do mouse em um projeto Extensão de Suporte de Aplicativo e selecione **IBM Tivoli** > **Importar Extensões de Suporte de Aplicativo**
2. Na janela **Importar Informações**, selecione o nome do host no qual o Tivoli Enterprise Portal Server está localizado ou clique em **Incluir** para incluir um.
3. No campo **Aplicativo**, insira o código do produto do agente.
4. Insira a afinidade do agente para o qual está criando o suporte de aplicativo customizado.

   A afinidade do agente é um identificador interno do Tivoli Monitoring que associa as áreas de trabalho, consulta e outros itens, com o agente. Isso deve ser exclusivo na instalação do Tivoli Monitoring. Clique em **Pesquisar** para abrir a janela **Tipos de Nó** e selecione essa informação da lista ao invés de digitá-la.
5. Quando estiver satisfeito com as informações de importação, clique em **Concluir**.
6. Na janela **Situações**, selecione as situações que deseja importar a partir da lista Situações Disponíveis.

   Clique em **<<** para inseri-los na lista de situações selecionadas e clique em **OK**. Uma nova pasta é criada sob o projeto e ela contém os arquivos necessários para instalar os espaços de trabalho, situações e consultas.
7. Na janela **Consultas**, selecione as consultas que deseja importar a partir da lista Consultas Disponíveis.

   Clique em **<<** para inseri-los na lista de consultas selecionadas e clique em **OK**.
8. Na janela **Executar Ações**, escolha os comandos Executar Ação que você deseja importar na lista Executar Ações Disponíveis.

   Clique em **<<** para inseri-los na lista Executar Ações Selecionadas e clique em **OK**. Os arquivos de suporte para o agente são colocados no projeto sob a pasta apropriada.

O que Fazer Depois

É possível repetir esse processo por quantos agentes diferentes você desejar. O Agente Builder cria uma única imagem de instalação de todos os arquivos de suporte no projeto de Extensão de Suporte de Aplicativo.

Gerando a Imagem de Instalação da Extensão de Suporte de Aplicativo

Gerar uma imagem de instalação da Extensão de Suporte de Aplicativo.

Procedimento

1. Clique com o botão direito no projeto Extensão de Suporte de Aplicativo e selecione **IBM Tivoli** > **Criar Imagem de Instalação da Extensão de Suporte de Aplicativo**.
2. Na janela **Informações de Extensão de Suporte de Aplicativo**, insira o diretório no qual a imagem deve ser colocada.
3. Sua Extensão de Suporte de Aplicativo deve ter seu próprio código de produto. Insira o código de produto registrado para o seu novo agente. É possível usar um dos códigos de produto reservados para uso com o Agent Builder. Os valores permitidos são `K00-K99`,`K{0-2}{A-Z}` e `K{4-9}{A-Z}`.

Nota: Estes valores destinam-se somente a uso interno e não são destinados a agentes que serão compartilhados ou vendidos. Se estiver criando um agente a ser compartilhado com outros, envie uma nota para toolkit@us.ibm.com para reservar um código do produto. O pedido para um código do produto deve incluir uma descrição do agente a ser montado. Um código do produto é então designado, registrado e retornado a você. Ao receber o código de três letras do produto, você é informado sobre como ativar o Agent Builder para usar o código de produto designado.

4. Insira o nome da Extensão de Suporte de Aplicativo.
5. Insira uma descrição da Extensão de Suporte de Aplicativo.
6. Insira uma versão para a Extensão de Suporte de Aplicativo no formato VVRRMMFF em que `vv` = número da versão; `rr` = número da liberação; `mm` = número da modificação (número do fix pack); e `ff` = número da correção temporária.
7. Clique em **Concluir**.

Instalando Sua Extensão de Suporte de Aplicativo

Instalar sua Extensão de Suporte de Aplicativo

Procedimento

1. Transfira sua imagem para o Tivoli Enterprise Monitoring Server e os servidores Tivoli Enterprise Portal Server.
2. Para instalar o suporte do Tivoli Enterprise Monitoring Server, execute um dos comandos a seguir:
   - No Windows: `install`*`KXX`*`TEMSSupport.bat`
   - No UNIX: `install`*`KXX`*`TEMSSupport.sh`

   O formato para o comando é o seguinte:

   ```
   installKXXTEMSSupport[.bat | .sh] <Diretório de Instalação do ITM> [-s tems_host]
    [-u tems_user] \[-p tems_password]
   ```
3. Para instalar o suporte do Tivoli Enterprise Portal Server, execute um dos comandos a seguir:
   - No Windows: `install`*`KXX`*`TEPSSupport.bat`
   - No UNIX: `install`*`KXX`*`TEPSSupport.sh`

   O formato para o comando é o seguinte:

   ```
   installKXXTEPSSupport[.bat | .sh] <ITM Install Directory> [-r]
   ```

   em que `-r` indica que o Tivoli Enterprise Portal Server deve ser reiniciado após a instalação

Convertendo um Projeto de Instalação de Solução em um Projeto de Extensão de Suporte de Aplicativo

Converter um **Projeto de Instalação de Solução** existente em um projeto de Extensão de Suporte de Aplicativo

Sobre Esta Tarefa

Se você tiver um **Projeto de Instalação de Solução** existente que deseja converter em um projeto de Extensão de Suporte de Aplicativo, conclua as etapas a seguir:

Nota: No **Projeto de Instalação de Solução** somente os arquivos de Suporte são migrados.

Procedimento

1. Clique com o botão direito no **Projeto de Instalação de Solução** e selecione **IBM Tivoli** > **Converter Projeto de Instalação de Solução**.
2. Insira o nome de um novo projeto de Extensão de Suporte de Aplicativo ou selecione um projeto existente na lista

3. Clique em **Concluir**.

Geração de Modelo de Dados Cognos

O Agent Builder pode gerar um modelo de dados Cognos para cada agente. Use o modelo de dados para importar as informações do agente no Cognos Framework Manager para criação de relatório.

Este modelo de dados Cognos pode ser aberto e visualizado no Framework Manager, que construirá um pacote de modelo a ser publicado no Tivoli Common Reporting. O modelo de dados também pode ser customizado ou modificado dentro do Framework Manager antes da publicação

Quando um relatório é criado, o Agent Builder também permite que um pacote de relatórios final seja importado no projeto do Agent Builder. Esse recurso permite que projetos futuros do agente sejam gerados com os relatórios que já fazem parte do pacote de agente. Os relatórios que são empacotados como parte da imagem de instalação do agente podem ser importados no relatório do Tivoli Common em seu ambiente de produção.

Nota: Nesta documentação, observe a convenção a seguir:

- K*xx* ou k*xx* refere-se ao código do produto fornecido ao agente, por exemplo k99.
- *dbType* refere-se ao banco de dados que está sendo usado pelo Tivoli Data Warehouse, por exemplo, DB2.

Pré-requisitos para Gerar um Modelo de Dados do Cognos

Conclua estas tarefas antes de poder gerar um modelo de dados do Cognos

Sobre Esta Tarefa

Nota:

- Estas etapas devem ser concluídas somente uma vez, pois todos os modelos de dados futuros gerados com o Agent Builder usarão este ambiente.
- É aconselhável criar um ambiente de desenvolvimento isolado para criação de relatório e teste do agente.

Procedimento

1. Instalar e configurar um (“ Tivoli Data Warehouse” na página 1477).
2. Criar tabelas e Procedimentos no Tivoli Data Warehouse.
   a) “Criar Tabelas e Procedimentos no Tivoli Data Warehouse” na página 1477.
   b) “Preenchendo o Tivoli Data Warehouse com Tivoli Reporting and Analytics Model” na página 1480.
3. Instalar e configurar (“Tivoli Common Reporting” na página 1480).
4. Instalar e configurar o (“Framework Manager” na página 1481).

Tivoli Data Warehouse

Sobre o Tivoli Data Warehouse.

Para criar relatórios, é necessário um Tivoli Data Warehouse, um Warehouse Proxy Agent e um Summarization and Pruning Agent instalados e configurados no seu ambiente. Para obter informações adicionais, consulte o *IBM Tivoli Monitoring Installation and Setup Guide*.

Criar Tabelas e Procedimentos no Tivoli Data Warehouse

Crie ou altere o Procedimento Armazenado e Tabela `ManagedSystem` no Tivoli Data Warehouse

Sobre Esta Tarefa

O modelo de dados Cognos gerado inclui uma tabela `ManagedSystem` que é usada para definir uma dimensão `ManagedSystem`. A dimensão `ManagedSystem` permite que relatórios sejam criados e que

possam se correlacionar com sistemas gerenciados. Por exemplo, se o agente for um agente do subnó, a dimensão pode ser usada para determinar os subnós existentes para uma instância do agente específica.

A tabela `ManagedSystem` não é criada pelo Tivoli Data Warehouse. Portanto, quando um agente é gerado no Agent Builder, os scripts SQL são gerados para cada plataforma de banco de dados que:

- Cria a tabela `ManagedSystem`. Use este script, se a tabela não existir no Tivoli Data Warehouse.
- Edite a tabela `ManagedSystem`. Use este script se a tabela existir no Tivoli Data Warehouse. Outros produtos de relatórios podem criar a tabela `ManagedSystem`, mas eles não a criarão com todas as colunas necessárias.
- Crie um procedimento armazenado que preenche a tabela `ManagedSystem` das tabelas no Tivoli Data Warehouse.

Execute estes scripts somente uma vez.

Executando os Scripts DB2 para Criar Tabelas e Procedimentos no Tivoli Data Warehouse
Para um banco de dados DB2, use estes scripts para criar tabelas no Tivoli Data Warehouse

Antes de Iniciar

Os scripts para DB2 estão no diretório a seguir:

```
reports/db2/Kxx/reports/cognos_reports/itmkxx/db_scripts
```

Procedimento

1. Todos os scripts gerados (`create_table.sql`, `alter_table.sql` e `create_procedure.sql`) usam *`itmuser`* como o ID de usuário do Tivoli Data Warehouse. Se *`itmuser`* não for o ID do usuário Tivoli Data Warehouse em seu ambiente, altere todas as ocorrências de *`itmuser`* para o ID do usuário correto.
2. Conecte-se ao Tivoli Data Warehouse como o usuário do Tivoli Data Warehouse:

   ```
   db2 connect to <Tivoli Data Warehouse alias name> user
   <Tivoli Data Warehouse user id> using  <password>
   ```

3. Determine se a tabela ManagedSystem existe:

   ```
   db2 "select count(*) from sysibm.systables where name = 'MANAGEDSYSTEM'
   and creator=upper ('<Tivoli Data Warehouse user id>')"
   ```

4. Crie ou altere a tabela.
   - Se a consulta retornar 1, a tabela existe. Execute o script de alteração:

     ```
     db2 -tvf alter_table.sql
     ```

   - Se a consulta retornar 0, a tabela não existe. Execute o script de criação:

     ```
     db2 -tvf create_table.sql
     ```

5. Execute o script para criar o procedimento armazenado:

   ```
   db2 -td@ -f create_procedure.sql
   ```

Executando Scripts Oracle para Criar Tabelas e Procedimentos no Tivoli Data Warehouse
Para um banco de dados Oracle, use esses scripts para criar tabelas no Tivoli Data Warehouse

Antes de Iniciar

Os scripts para Oracle estão no diretório a seguir:

```
reports/oracle/Kxx/reports/cognos_reports/itmkxx/db_scripts
```

Procedimento

1. Todos os scripts gerados (`create_table.sql`, `alter_table.sql` e `create_procedure.sql`) usam *`itmuser`* como o ID de usuário do Tivoli Data Warehouse. Se *`itmuser`* não for o ID do usuário Tivoli Data Warehouse em seu ambiente, altere todas as ocorrências de *`itmuser`* para o ID do usuário correto.
2. Inicie o `sqlplus`:

```
sqlplus <IBM Tivoli Monitoring user ID>/<password>@
<Tivoli Data Warehouse SID>
```

3. Determine se a tabela ManagedSystem existe:

```
select count(*) from user_tables where table_name = 'MANAGEDSYSTEM';
```

4. Crie ou altere a tabela.
   - Se a consulta retornar 1, a tabela existe. Execute o script de alteração:

     ```
     @<path to alter_table.sql>;
     ```

   - Se a consulta retornar 0, a tabela não existe. Execute o script de criação:

     ```
     @<path to create_table.sql>;
     ```

5. Execute o script para criar o procedimento armazenado:

```
@<path to create_procedure.sql>;
```

Executando os Scripts SQL Server 2005 e 2008 para Criar tabelas e Procedimentos no Tivoli Data Warehouse

Antes de Iniciar

Os scripts para SQL Server estão no diretório a seguir:

```
reports/mssql/Kxx/reports/cognos_reports/itmkxx/db_scripts
```

Procedimento

1. Todos os scripts gerados (`create_table.sql`, `alter_table.sql` e `create_procedure.sql`) usam *`itmuser`* como o ID de usuário do Tivoli Data Warehouse. Se *`itmuser`* não for o ID do usuário Tivoli Data Warehouse em seu ambiente, altere todas as ocorrências de *`itmuser`* para o ID do usuário correto.
2. Determine se a tabela `ManagedSystem` existe:

```
osql -S <Server> -U <Tivoli Data Warehouse user ID> -P <password> -d
<Tivoli Data Warehouse database name> -Q "Select count(*)
from INFORMATION_SCHEMA.TABLES where table_name = 'ManagedSystem'"
```

3. Crie ou altere a tabela.
   - Se a consulta retornar 1, a tabela existe. Execute o script de alteração:

     ```
     osql -S <Server> -U <Tivoli Data Warehouse user ID> -P <password> -d
     <Tivoli Data Warehouse database name> -I -n -i <path to alter_table.sql>
     ```

   - Se a consulta retornar 0, a tabela não existe. Execute o script de criação:

     ```
     osql -S <Server> -U <Tivoli Data Warehouse user ID> -P <password> -d
     <Tivoli Data Warehouse database name> -I -n -i <path to create_table.sql>
     ```

4. Execute o script para criar o procedimento armazenado:

```
osql -S <Server> -U <Tivoli Data Warehouse user ID> -P
<password> -d <Tivoli Data Warehouse database name>
-I -n -i <path to create_procedure.sql>
```

Preenchendo o Tivoli Data Warehouse com Tivoli Reporting and Analytics Model
Use os scripts de banco de dados fornecidos para preencher o Tivoli Data Warehouse

Sobre Esta Tarefa

O Tivoli Reporting and Analytics Model (TRAM) contém o conjunto básico de conhecimento que é comum para todos os pacotes de relatórios. O TRAM é instalado por um conjunto de scripts exclusivos a cada banco de dados. Os scripts necessários para preenchimento de cada banco de dados suportado são incluídos na imagem de instalação do agente, dentro do diretório de relatórios. Use o procedimento a seguir para criar Dimensões Comuns do Tivoli Reporting and Analytics Model no Tivoli Data Warehouse.

Procedimento

1. Navegue para os scripts do banco de dados do Tivoli Reporting and Analytics Model.
2. Extraia o pacote de agente.
   - Nos sistemas Windows, o pacote de agente é k*xx*.zip.
   - Nos sistemas Linux e UNIX, o pacote de agente é k*xx*.tgz.
3. Acesse os scripts do banco de dados apropriados.
   - Os scripts DB2 estão no pacote de Agente em:

     ```
     reports/db2/Kxx/reports/cognos_reports/itmkxx/db_scripts
     ```

   - Os scripts Oracle estão no pacote de Agente em:

     ```
     reports/oracle/Kxx/reports/cognos_reports/itmkxx/db_scripts
     ```

   - Os scripts Microsoft SQL Server estão no pacote de Agente em:

     ```
     reports/mssql/Kxx/reports/cognos_reports/itmkxx/db_scripts
     ```

4. Execute os scripts do banco de dados para gerar as dimensões comuns no Tivoli Data Warehouse. Cada conjunto de scripts fornece um arquivo leia-me com instruções de uso.
5. Verifique se os scripts incluíram as tabelas a seguir no Tivoli Data Warehouse:

   ```
   "Sistema de Computador", WEEKDAY_LOOKUP, MONTH_LOOKUP, TIMEZONE_DIMENSION, TIME_DIMENSION
   ```

Tivoli Common Reporting
O Tivoli Common Reporting contém o mecanismo do Cognos Business Intelligence, que contém elementos para ajudar na criação de relatórios do agente.

O Tivoli Common Reporting deve ser instalado e configurado com uma origem de dados que se conecta ao Tivoli Data Warehouse.

Instalando o Tivoli Common Reporting

Você deve instalar o Tivoli Common Reporting. As versões 1.3, 2.1 e 2.1.1 ou posteriores são suportadas. Para obter informações sobre como instalar o Tivoli Common Reporting, consulte Instalando o Tivoli Common Reporting.

Configurando o Tivoli Common Reporting

Você deve configurar o Tivoli Common Reporting. Para obter informações sobre como configurar o Tivoli Common Reporting, consulte Configurando o IBM Tivoli Common Reporting.

Crie uma origem de dados entre o Tivoli Data Warehouse e o Tivoli Common Reporting. Para obter mais informações, consulte Configurando a conexão com o banco de dados. Clique no tipo de banco de dados apropriado. Observe o nome fornecido para a origem de dados. O padrão é **TDW**.

Nota: O nome da origem de dados deve corresponder ao campo **Origem de dados** da página **Informações do Cognos**. Para obter informações adicionais sobre a página **Informações do Cognos**, consulte "Informações do Cognos" na página 1186.

Framework Manager

O Framework Manager é um aplicativo enviado com o aplicativo Tivoli Common Reporting, mas deve ser instalado e configurado separadamente.

O Framework Manager é usado para visualizar e modificar modelos de dados e publicar modelos de dados para o Tivoli Common Reporting

Instalando o Framework Manager

Você deve instalar o Framework Manager. As versões 8.4, 8.4.1 ou posteriores são suportadas.

O Framework Manager é enviado com o Tivoli Common Reporting, mas deve ser instalado manualmente. O Tivoli Common Reporting 1.3 é enviado com o Framework Manager 8.4. O Tivoli Common Reporting 2.1 e 2.1.1 são enviados com o Framework Manager 8.4.1. Para obter informações sobre como instalar o Framework Manager, consulte Installing Framework Manager no *Tivoli Common Reporting: Guia do Usuário*.

Configurando o Framework Manager

Você deve configurar o Framework Manager. Para obter informações sobre como configurar o Framework Manager, consulte Configuring Framework Manager no *Tivoli Common Reporting: Guia do Usuário*.

Criando relatórios

Use o Framework Manager para publicar o modelo de agente e o Report Studio para começar a criar relatórios.

Antes de Iniciar

Quando o agente for concluído, ele deve ser instalado no ambiente Tivoli Monitoring. Além disso, a coleção histórica para o agente deve ser configurada e o agente deve ser executado por pelo menos um intervalo de upload do warehouse. O resumo deve ser configurado e as opções de configuração de resumo que são feitas no Tivoli Monitoring devem ser idênticas às opções de resumo feitas no Agent Builder. O agente de Resumo e Remoção deve executar pelo menos uma vez depois que os dados do agente tiverem sido transferidos por upload para o warehouse.

1. Instale, configure e inicie o agente.
2. Crie e distribua para o agente uma coleção histórica para cada grupo de atributos para o qual deseja criar um relatório.

   Nota: O intervalo de upload do armazém é padronizado como diariamente. Entretanto, você pode desejar reduzir esse intervalo.

   Para obter informações sobre como configurar a coleta histórica, consulte Managing historical data no *IBM Tivoli Monitoring: Guia do Administrador*.
3. No Tivoli Monitoring, configure o resumo para todos os grupos de atributos para os quais você criou coleções históricas na Etapa 2.

   Nota: Ao configurar a coleção de histórico e o resumo, você deve esperar tempo suficiente para que os dados sejam encerrados nas tabelas de resumo.

   Nota: Por padrão, o agente Summarization and Pruning é configurado para ser executado uma vez por dia às 2h. Talvez você queira alterar esta configuração. Por exemplo, é possível configurá-lo para ser

executado de hora em hora. Para obter informações sobre como configurar o Tivoli Data Warehouse, consulte Setting up data warehousing no *IBM Tivoli Monitoring Installation and Setup Guide*.

Sobre Esta Tarefa

A geração de um agente no Agent Builder cria um projeto inteiro do Framework Manager, que inclui o modelo de dados e o arquivo de projeto do Framework Manager. O Framework Manager pode abrir o arquivo do projeto diretamente, que abre o modelo de dados para modificação, customização ou publicação.

Procedimento

Nota: O modelo de dados gerado para o agente contém todas as dimensões de tempo de resumo para cada grupo de atributos: por hora, diariamente, semanalmente, mensalmente, trimestralmente e anualmente. As dimensões existem somente no Tivoli Data Warehouse para o agente se o resumo e a limpeza estiverem configurados para o agente. E também se as dimensões estiverem selecionadas e se o agente Summarization and Pruning tiver criado e preenchido as tabelas. Os relatórios podem ser definidos e publicados no Tivoli Common Reporting que usam as dimensões que não existem. Tais relatórios não funcionam até que as tabelas de resumo sejam criadas pelo agente de Resumo e Remoção.

1. Abra o Modelo de Dados de Agente no Framework Manager:
   a) Abra o Framework Manager.
   b) Na página **Bem-vindo**, clique em **Abrir um Projeto**.

      Dica: Se você estiver no Framework Manager, clique em **Abrir** no menu **Arquivo**.
   c) Navegue até o modelo de dados do Agente.
      - Para DB2:

        ```
        reports/db2/Kxx/model/
        ```

      - Para o Oracle:

        ```
        reports/oracle/Kxx/model/
        ```

      - For Microsoft SQL Server:

        ```
        reports/mssql/Kxx/model/
        ```

   d) Selecione o arquivo de projeto do agente, K*xx*`.cpf`.

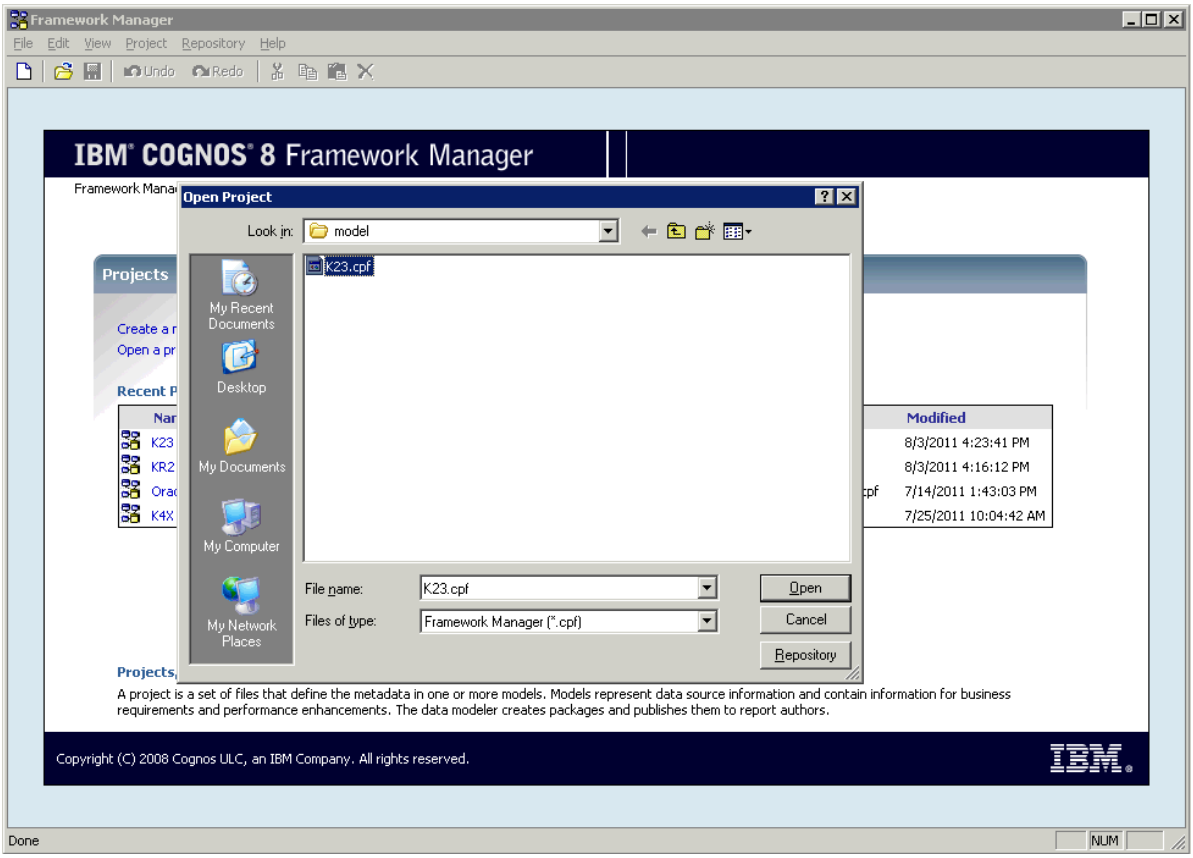


Figura 80. Selecionando o arquivo de projeto do agente

Nota: Quando um projeto do agente é aberto no Framework Manager, o nome do agente é listado nos Projetos Recentes.

2. Preencha a Tabela do Sistema Gerenciado. Para obter mais informações, consulte "Preenchendo a Tabela ManagedSystem" na página 1487
3. Use o Framework Manager para publicar o Modelo de Agente no Tivoli Common Reporting
   a) Abra o Framework Manager.
   b) Abra o projeto do Agente.
   c) Expanda **Pacotes** na árvore de navegação.
   d) Clique com o botão direito do mouse no pacote de agente e selecione **Pacotes de Publicação**.

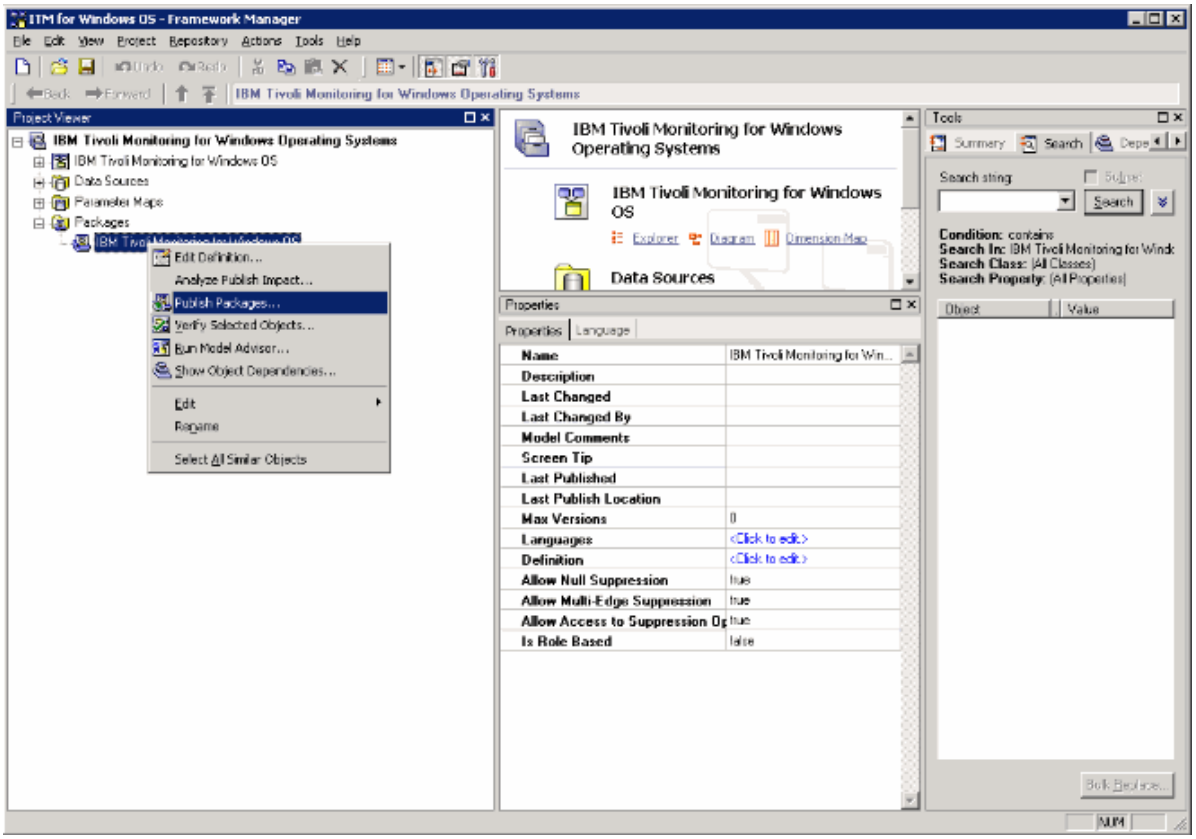


Figura 81. Selecionando os Pacotes de Publicação

4. Use o Report Studio para criar novos relatórios ou modelos.
   a) Efetue logon no Tivoli Common Reporting.
   b) Navegue nas Pastas Públicas, expanda **Relatório** no painel de navegação e selecione **Relatório Comum**.

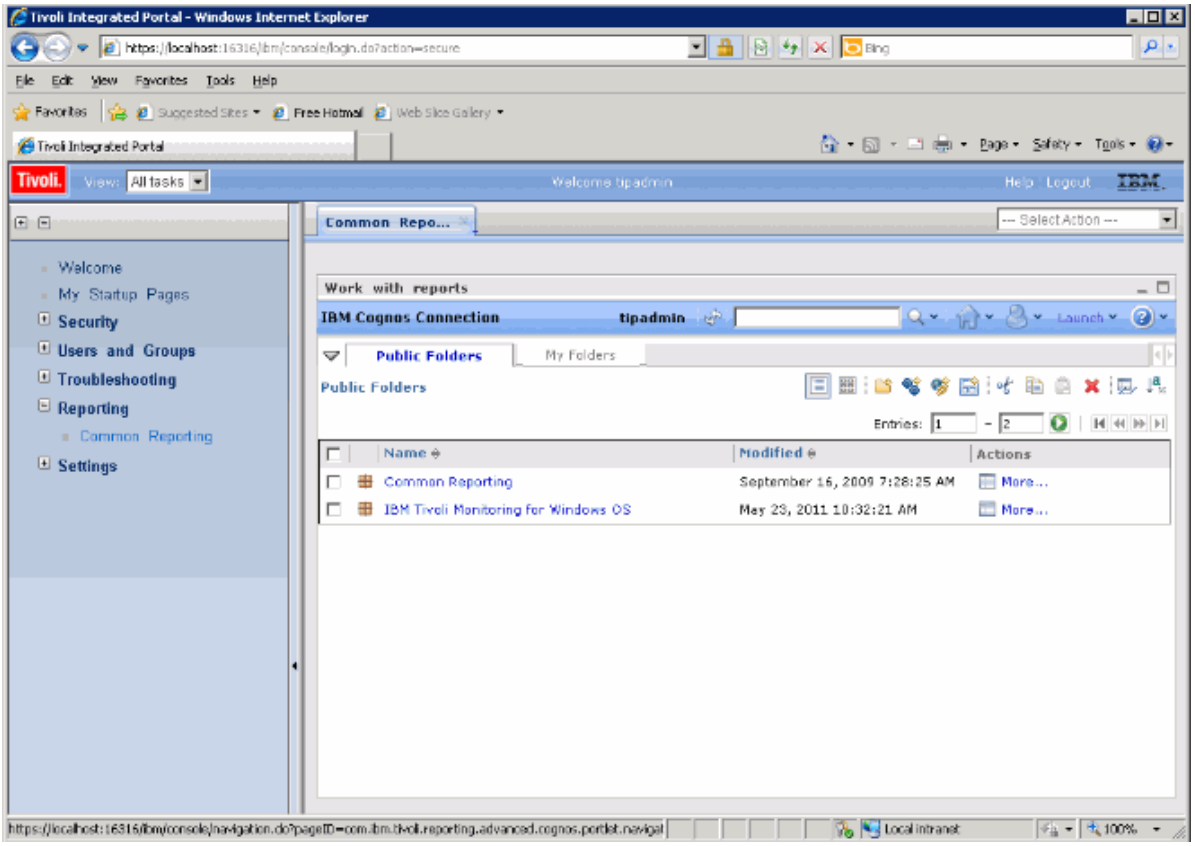


Figura 82. Selecting Common Reporting

c) Selecione seu agente Tivoli Monitoring da lista fornecida.

d) Abra a ferramenta de criação de relatório clicando no menu Ativar e selecionando **Report Studio** ou **Query Studio**.

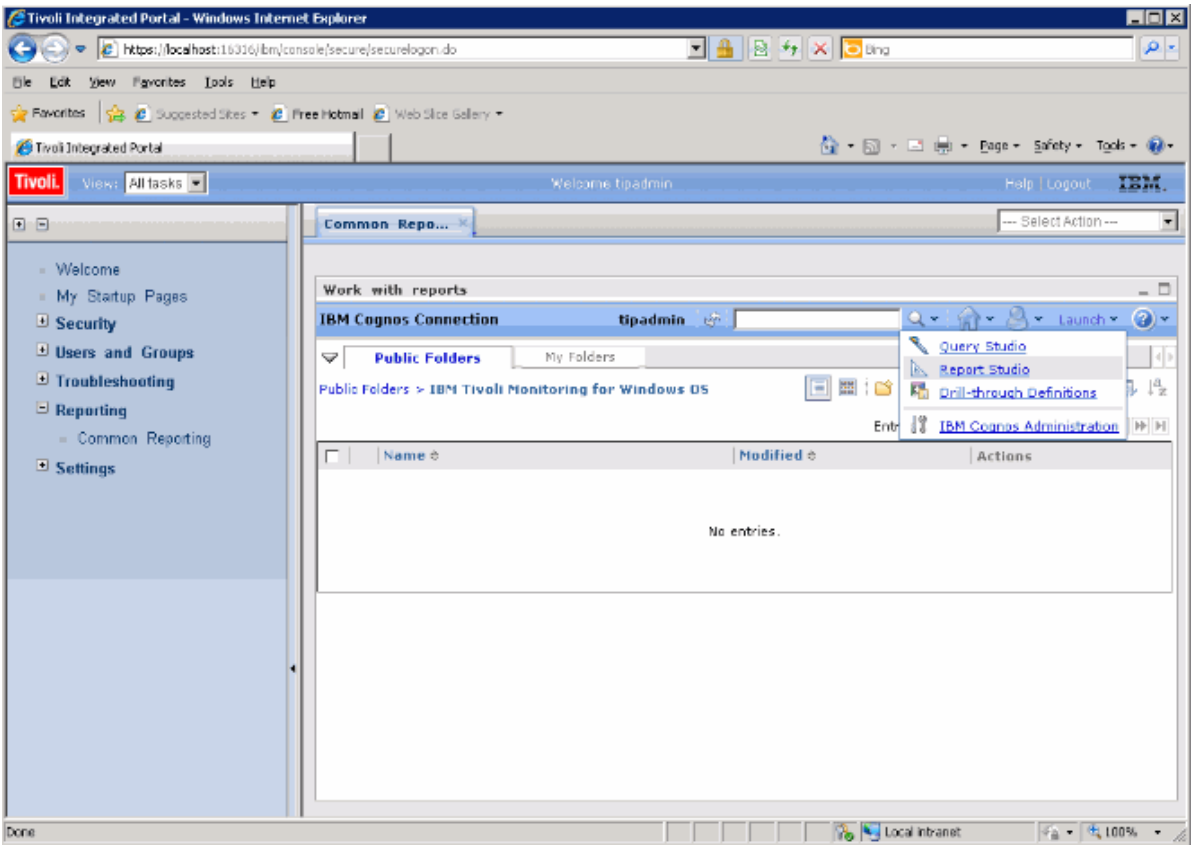


Figura 83. Selecionando Report Studio

O que Fazer Depois

É possível usar o Report Studio para criar novos relatórios ou modelos ou é possível modificar um relatório ou modelo existente.

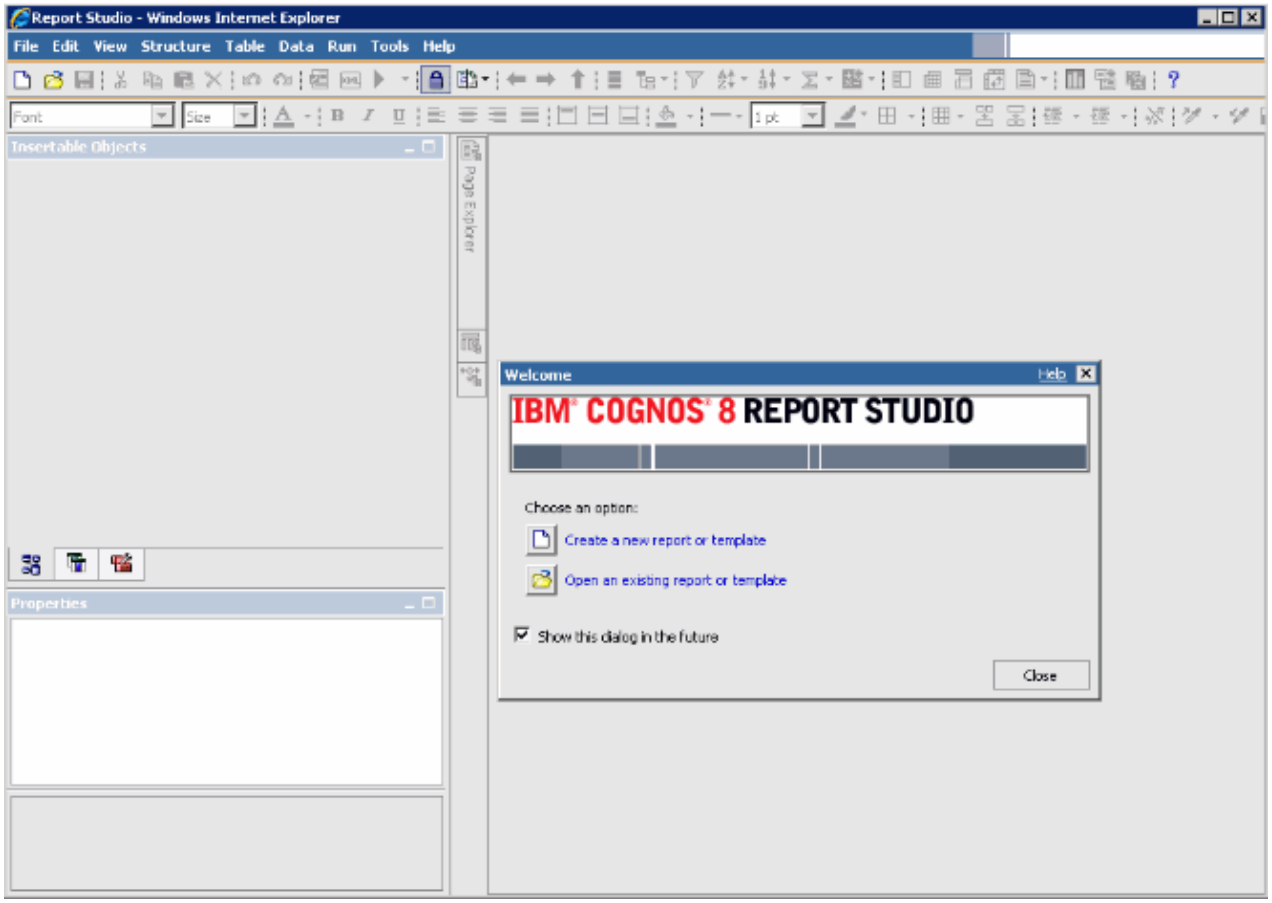


Figura 84. Report Studio

Para obter informações adicionais, consulte a coleção de tópicos do Tivoli Common Reporting no IBM Knowledge Center.

Preenchendo a Tabela ManagedSystem

A tabela `ManagedSystem` é preenchida usando o procedimento armazenado `kqz_populate_msn`.

Para obter mais informações, consulte "Executando o Procedimento Armazenado DB2" na página 1489. Este procedimento deve ser executado periodicamente para que a tabela `ManagedSystem` contenha a lista atual de nomes de sistema gerenciado.

O procedimento armazenado lê as seguintes tabelas de históricos no Tivoli Data Warehouse se elas existirem:

- A tabela de status do Objeto de Desempenho do agente
- A tabela de disponibilidade do agente. Agentes que monitoram processos ou serviços possuem uma tabela de disponibilidade.
- As tabelas de descoberta do agente. Os agentes de subnó criam tabelas de descoberta.

A coleta de históricos deve ser iniciada em um determinado conjunto de grupos de atributos. Um conjunto de scripts é gerado para criar e iniciar a coleta de históricos para esses grupos de atributos. Se você não deseja usar os scripts, a lista de grupos de atributos é relacionada no bloco de cabeçalho de comentário do script.

São criados scripts de amostra que mostram quais tabelas devem ter coleta de histórico ativada:

- `reports/configuretdw.sh`
- `reports/configuretdw.bat`

A seguinte tabela descreve os argumentos necessários:

Nota: Você deve especificar `-n` ou `-m`, mas não ambos.

Tabela 301. Argumentos Obrigatórios	
Argumento	**Descrição**
`-h` *candle_home*	O caminho da instalação do Tivoli Monitoring.
`-u` *teps_user*	O usuário do Tivoli Enterprise Portal Server para efetuar login como quando você cria as coletas de históricos.
`-n` *tems_name*	O Tivoli Enterprise Monitoring Server onde as coleções devem ser iniciadas. Mais de um Tivoli Enterprise Monitoring Server pode ser especificado usando uma lista separada por espaços. Se você especificar mais de um Tivoli Enterprise Monitoring Server, coloque a lista entre aspas. Por exemplo, `-n "tems1 tems2"`
`-m` *managed_system_group_or_managed_system*	O grupo de sistema gerenciado ou nome do sistema gerenciado com relação ao qual a coleção deve ser iniciada. Mais de um grupo de sistema gerenciado ou sistema gerenciado pode ser especificado usando uma lista separada por espaço. Se você especificar mais de um grupo de sistema gerenciado ou sistema gerenciado, coloque a lista entre aspas. Por exemplo, `-m "msg1 msg2"`

A tabela a seguir descreve os argumentos opcionais:

Tabela 302. Argumentos opcionais	
Argumento	**Descrição**
`-s` *teps_host*	O nome do host ou endereço IP do Tivoli Enterprise Portal Server. Se não especificado, o padrão será localhost.
`-p` *teps_password*	A senha para o usuário do Tivoli Enterprise Portal Server que é especificada com a opção `-u`. Se não especificado, o script solicita senha.
`-c` *historical_collection_interval*	O intervalo de coleta de histórico a ser usado ao iniciar as coletas de histórico. Se não especificado, o padrão é `1h` (1 hora). Os valores válidos são: `15m`, `30m`, `1h`, `12hou 1d`, em que `m` é minuto, `h` é hora e `d` dia.
`-r` *pruning_interval*	O intervalo de remoção a ser usado para os dados históricos. Os dados históricos devem ser removidos para que as tabelas não continuem crescendo em tamanho. Se não especificado, o padrão será `2d`(2 dias). Use `d` para dias, `m` para meses, `y` para anos.

Depois de iniciada a coleção histórica, o procedimento armazenado `kqz_populate_msn` deve ser executado periodicamente. O procedimento armazenado é executado periodicamente para que a tabela `ManagedSystem` contenha a lista mais atual dos sistemas gerenciados no ambiente Tivoli Monitoring.

Executando o Procedimento Armazenado DB2
Execute um procedimento armazenado em DB2.

Sobre Esta Tarefa

Execute as seguintes etapas para executar o procedimento armazenado em DB2:

Procedimento

1. Conecte-se ao banco de dados do Tivoli Data Warehouse como o usuário do armazém:

```
connect to <Tivoli Data Warehouse database alias> user
<Tivoli Data Warehouse user id> using <password>
```

2. Execute o procedimento armazenado:

```
db2 "call <Tivoli Data Warehouse schema>.kqz_populate_msn
('<código do produto de três letras para o agente>')"
```

Executando o procedimento armazenado de Oracle
Execute um procedimento armazenado no Oracle.

Sobre Esta Tarefa

Siga estas etapas para executar o procedimento armazenado no Oracle:

Procedimento

1. Inicie o `sqlplus`:

```
sqlplus <Tivoli Data Warehouse user id>/<password>@
<Oracle SID>
```

2. Execute o procedimento armazenado:

```
execute kqz_populate_msn('<código do produto de três
letras para o agente>');
```

Executando o Procedimento Armazenado no SQL Server 2005 e 2008
Execute um procedimento armazenado no SQL Server.

Sobre Esta Tarefa

Siga estas etapas para executar o procedimento armazenado no SQL Server 2005 e 2008:

Procedimento

Execute o procedimento armazenado:

```
osql -S <server> -U <Tivoli Data Warehouse id> -P
<Tivoli Data Warehouse password> -d
<Tivoli Data Warehouse database name> -Q "EXEC
[<Tivoli Data Warehouse schema>].[kqz_populate_msn]
@pv_productcode = N'<three letter product code>'"
```

Exportando Relatórios e Modelos de Dados do Tivoli Common Reporting
Exporte os relatórios e modelos de dados do Tivoli Common Reporting.

Procedimento

1. Efetue login no Tivoli Common Reporting.
2. Acesse as Pastas Públicas e em **Relatório** no painel de navegação selecione **Relatório Comum**.
3. Na seção Trabalhar com Relatórios, clique no menu **Ativar** e selecione **IBM Cognos Administration**.

4. Clique na guia **Configuração**.
5. Clique em **Administração de Conteúdo**.

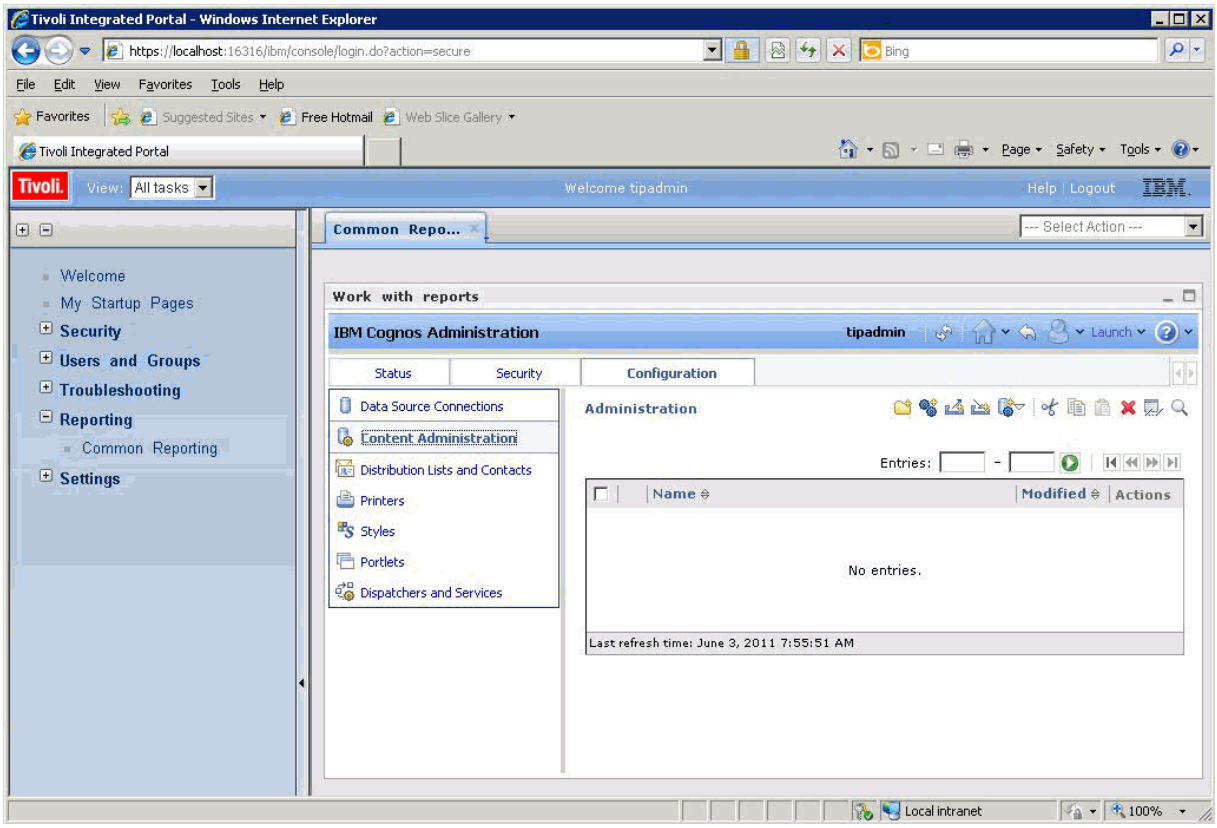


Figura 85. A guia Administração de Conteúdo

6. Clique no ícone **Nova Exportação** para exportar um novo pacote.
7. Nomeie o pacote. Opcionalmente, é possível incluir uma dica de tela e a descrição.
8. Selecione **Selecionar pastas públicas e conteúdo de diretório**.
9. No diálogo Pastas Públicas, clique no link **Incluir**.
10. Mova seu pacote de agente para **Entradas selecionadas**.
11. Na última página do assistente, selecione **Salvar Apenas**. Quando o assistente for concluído, o pacote de relatórios é listado na guia Administração de Conteúdo.
12. Na guia Administração de Conteúdo, clique na seta verde (Executar) para criar o arquivo `.zip` compactado.

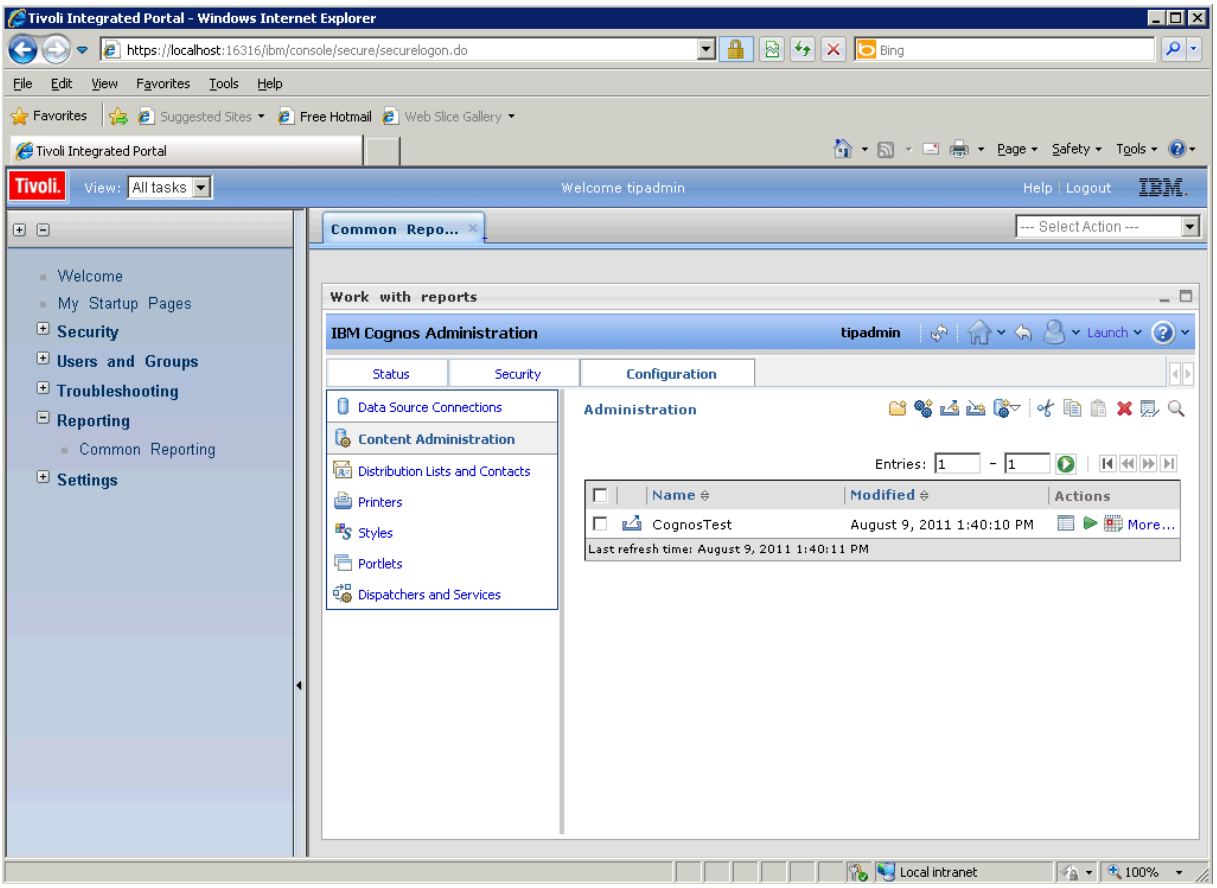


Figura 86. A guia Administração de Conteúdo com o pacote de agente listado

Resultados
O arquivo `.zip` compactado criado pelo processo de exportação é colocado no diretório de implementação.

- O caminho do diretório para o Tivoli Common Reporting versão 1.3 é:

```
C:\IBM\tivoli\tip\products\tcr\Cognos\c8\deployment
```

- O caminho do diretório para o Tivoli Common Reporting versão 2.1 ou posterior é:

```
C:\IBM\tivoli\tipv2Components\TCRComponent\cognos\deployment
```

O que Fazer Depois
Para obter informações adicionais sobre como exportar relatórios, consulte Exporting Cognos report packages no *Tivoli Common Reporting: Guia do Usuário*.

Importando relatórios no Agent Builder
Quando o pacote de relatórios for exportado do Tivoli Common Reporting, ele poderá ser importado no projeto Agent Builder. O pacote de relatórios podem então ser incluído na imagem de instalação do agente.

Procedimento

1. Clique com o botão direito no projeto do agente no Agent Builder.
2. Selecione **IBM** > **Importar Pacote de Relatórios**.
3. Na janela **Importar Pacote de Relatórios**, selecione o **Tipo de Banco de Dados** no qual o pacote de relatórios foi criado.

4. Insira o caminho completo para o pacote de relatórios ou clique em **Procurar** para selecioná-lo.
5. Clique em **OK**.
6. O pacote de relatório agora é mostrado no projeto de agente no diretório `reports/`*`dbtype`*.

   Nota: Se você criar pacotes de relatórios que são específicos do banco de dados, é necessário importar cada pacote no Agent Builder.

Instalando relatórios de um pacote de agente no Tivoli Common Reporting
Importe um pacote de relatórios a partir do agente para Tivoli Common Reporting

Procedimento

1. Siga as etapas no assistente para importar um novo pacote de imagens do agente.

   Na imagem do agente, os relatórios são localizados em: `reports/`*`dbType`*`/K`*`xx`*`/reports/cognos_reports/itmk`*`xx`*`/packages`
2. Copie o arquivo `zip` compactado por relatórios no diretório de implementação do Tivoli Common Reporting.
   - O caminho do diretório para Tivoli Common Reporting versão 1.3 é: `C:\IBM\tivoli\tip\products\tcr\Cognos\c8\deployment`
   - O caminho do diretório para Tivoli Common Reporting versão 2.1 ou posterior é: `C:\IBM\tivoli\tipv2Components\TCRComponent\cognos\deployment`
3. Efetue login no Tivoli Common Reporting.
4. Acesse as Pastas Públicas e em **Relatório** no painel de navegação selecione **Relatório Comum**.
5. Na seção Trabalhar com Relatórios, clique no menu **Ativar** e selecione **IBM Cognos Administration**.
6. Acesse a guia **Configuração** e abra a seção **Administração de Conteúdo**.
7. Clique em **Nova Importação** para criar uma importação de pacote.
8. Selecione o pacote de relatórios do agente.
9. Selecione as pastas públicas que você deseja importar.
10. Selecione Salvar.
11. Clique na seta verde (executar) para importar.

Resultados

Para obter informações adicionais, consulte Logging in to the reporting interface no *Tivoli Common Reporting: Guia do Usuário*.

Expressões Regulares ICU

Uma descrição dos específicos da implementação de expressão comum de ICU.

Este conteúdo de referência é extraído do *Guia do Usuário do ICU*. O conteúdo descreve os específicos da implementação de expressão comum de ICU. Essas informações são essenciais se você estiver usando o recurso de expressão regular do Agent Builder porque linguagens de programação diferentes implementam expressões regulares de formas um pouco diferentes.

Tabela 303. Meta-caracteres de Expressão Comum

Caractere	**Descrição**
\a	Corresponder um BELL, \u0007
\A	Corresponder no início da entrada. Difere de ^ em que \A não corresponde após uma nova linha na entrada.

Tabela 303. Meta-caracteres de Expressão Comum (continuação)	
Caractere	**Descrição**
\b, fora de um [Set]	Corresponder se a posição atual for um limite de palavra. Limites ocorrem nas transições entre caracteres de palavras (\w) e não palavras (\W), com marcas de combinação ignoradas. Para obter informações adicionais sobre limites de palavras, consulte Análise de Limite de ICU.
\b, em um [Set]	Corresponder um BACKSPACE, \u0008.
\B	Corresponder se a posição atual não for um limite de palavra.
\cX	Corresponder um caractere Ctrl-X.
\d	Corresponder qualquer caractere com Unicode General Category de Nd (Número, Dígito Decimal.)
\D	Corresponder qualquer caractere que não é um dígito decimal.
\e	Corresponder um ESCAPE, \u001B.
\E	Termina uma sequência citada \Q ... \E.
\f	Corresponder um FEED DE FORMULÁRIO, \u000C.
\G	Corresponder se a posição atual está no final da correspondência anterior.
\n	Corresponder um FEED DE LINHA, \u000A.
\N{UNICODE CHARACTER NAME}	Corresponder o caractere denominado.
\p{UNICODE PROPERTY NAME}	Corresponder qualquer caractere à Propriedade Unicode especificada.
\P{UNICODE PROPERTY NAME}	Corresponder qualquer caractere que não tenha a Propriedade Unicode especificada.
\Q	Colocar aspas em torno de todos os caracteres seguintes até \E.
\r	Corresponder um RETORNO DE LINHA, \u000D.
\s	Corresponder um caractere de espaço em branco. Espaço em branco é definido como [\t\n\f\r \p{Z}].
\S	Corresponder um caractere de não espaço em branco.
\t	Corresponder uma TABULAÇÃO HORIZONTAL \u0009.
\uhhhh	Corresponder o caractere com valor hexadecimal hhhh.
\Uhhhhhhhh	Corresponder o caractere com valor hexadecimal hhhhhhhh. Exatamente oito dígitos hexadecimais devem ser fornecidos, mesmo que o maior ponto de código Unicode seja \U0010ffff.

Tabela 303. Meta-caracteres de Expressão Comum (continuação)	
Caractere	**Descrição**
\w	Corresponder um caractere de palavra. Caracteres de palavra são [\p{Ll}\p{Lu}\p{Lt}\p{Lo}\p{Nd}].
\W	Corresponder um caractere não palavra.
\x{hhhh}	Corresponder o caractere com valor hexadecimal hhhh. De 1 a 6 dígitos hexadecimais podem ser fornecidos.
\xhh	Corresponder o caractere com valor hexadecimal de 2 dígitos hh.
\X	Corresponder um Grapheme Cluster.
\Z\	Corresponder se a posição atual está no final da entrada, mas antes do terminador de linha final, se existir um.
\z	Corresponder se a posição atual estiver no final da entrada.
\n	Referência Retroativa. Corresponder a qualquer coisa correspondente ao enésimo grupo de captura. n deve ser um número > 1 e < o número total de grupos de captura no padrão. **Nota:** Escapes octais, como \012, não são suportados em expressões regulares de ICU.
[pattern]	Corresponder qualquer caractere do conjunto. Consulte UnicodeSet para obter uma descrição completa do que pode aparecer no padrão
.	Corresponder qualquer caractere.
^	Corresponder no início de uma linha.
$	Corresponder no final de uma linha.
\	Colocar aspas em todos do caractere a seguir. Os caracteres que devem ter aspas ao seu redor para ser tratados como literais são * ? + [( ) { } ^ $ | \ . /

Tabela 304. Operadores de Expressão Comum	
Operador	**Descrição**
|	Alternação. A | B corresponde a A ou B.
*	Corresponder 0 ou mais vezes. Corresponder o maior número de vezes possível.
+	Corresponder 1 ou mais vezes. Corresponder o maior número de vezes possível.
?	Corresponder zero ou 1 hora. Preferir um.
{n}	Corresponder exatamente n vezes.

Tabela 304. Operadores de Expressão Comum (continuação)	
Operador	**Descrição**
{n,}	Corresponder pelo menos n vezes. Corresponder o maior número de vezes possível.
{n,m}	Corresponder entre n e m vezes. Corresponder o maior número de vezes possível, mas não mais do que m.
*?	Corresponder 0 ou mais vezes. Corresponder o menor número de vezes possível.
+?	Corresponder 1 ou mais vezes. Corresponder o menor número de vezes possível.
??	Corresponder zero ou 1 hora. Preferir zero.
{n}?	Corresponder exatamente n vezes.
{n,}?	Corresponder pelo menos n vezes, mas não mais do que o necessário para uma correspondência de padrão geral
{n,m}?	Corresponder entre n e m vezes. Corresponder o menor número de vezes possível, mas não menos do que n.
*+	Corresponder 0 ou mais vezes. Corresponder o maior número de vezes possível quando encontrado pela primeira vez, não tentar novamente com menos mesmo se a correspondência geral falhar (Correspondência Possessiva)
++	Corresponder 1 ou mais vezes. Correspondência possessiva.
?+	Corresponder zero ou 1 hora. Correspondência possessiva.
{n}+	Corresponder exatamente n vezes.
{n,}+	Corresponder pelo menos n vezes. Correspondência Possessiva.
{n,m}+	Corresponder entre n e m vezes. Correspondência Possessiva.
(...)	Parêntese de captura. Intervalo de captura que correspondeu a expressão entre parênteses está disponível após a correspondência.
(?: ...)	Parêntese de não captura. Agrupa o padrão incluído, mas não fornece captura do texto de correspondência. Mais eficiente do que o parêntese de captura.

Tabela 304. Operadores de Expressão Comum (continuação)	
Operador	**Descrição**
`(?> ... )`	Parêntese de correspondência atômica. Primeira correspondência da subexpressão entre parênteses é a única tentada. Se ele não levar a uma correspondência de padrões geral, faça backup da procura por uma correspondência para uma posição anterior a "`(?>`".
`(?# ... )`	Comentário de formato livre `(?# comentário)`.
`(?= ... )`	Asserção lookahead. Verdadeiro se o padrão entre parênteses corresponder na posição de entrada atual, mas não avança a posição de entrada.
`(?! ... )`	Asserção lookahead negativa. Verdadeiro se o padrão entre parênteses não corresponder na posição de entrada atual. Não avança a posição de entrada.
`(?<= ... )`	Asserção lookbehind. Verdadeiro se o padrão entre parênteses corresponder ao texto que precede a posição de entrada atual. O último caractere da correspondência é o caractere de entrada logo antes da posição atual. Não altera a posição de entrada. O comprimento de possíveis sequências correspondidas pelo padrão lookbehind não deve ser sem ligação (sem operadores * ou +.)
`(?<!...)`	Asserção lookbehind negativa. Verdadeiro se o padrão entre parênteses não corresponder ao texto que precede à posição de entrada atual. O último caractere da correspondência é o caractere de entrada logo antes da posição atual. Não altera a posição de entrada. O comprimento de possíveis sequências correspondidas pelo padrão lookbehind não deve ser sem ligação (sem operadores * ou +.)
`(?ismx-ismx: ... )`	Configurações de sinalizador. Avaliar a expressão entre parênteses com os sinalizadores especificados ativados ou desativados.
`(?ismx-ismx)`	Configurações de sinalizador. Alterar as configurações do sinalizador. As mudanças se aplicam à parte do padrão após a configuração. Por exemplo, `(?i)` altera para uma correspondência sem distinção de maiúsculas e minúsculas.

Texto de Substituição

O texto de substituição para operações localizar e substituir pode conter referências ao texto do grupo de captura da localização. As referências são no formato $n, onde n é o número do grupo de capturas.

Tabela 305. Caracteres do Texto de Substituição	
Caractere	**Descrição**
$n	O texto do grupo de captura de posição n é substituído por $n. n deve ser >= 0, e não maior que o número de grupos de capturas. Um $ não seguido por um dígito não tem nenhum significado especial e é exibido no texto de substituição como ele mesmo, um $.
\	Trate esse caractere como um literal, suprimindo qualquer significado especial. O escape como barra invertida em texto de substituição é necessário somente para '$' e '\', mas pode ser usado por qualquer outro caractere sem efeitos adversos.
$@n	O texto do grupo de captura n será substituto para a expressão regular correspondente ao grupo de captura n. n deve ser >= 0, e não maior que o número de grupos de captura. Um $@ não seguido por um dígito não tem significado especial e é exibido no texto de substituição como ele mesmo, um $@.
$#n	O texto do grupo de captura correspondido n é substituído por $#n. n deve ser >= 0, e não maior que o número de grupos de captura correspondidos. Um $# não seguido por um dígito não tem significado especial e é exibido no texto de substituição como ele mesmo, um $#.

Opções de Sinalizador

Os sinalizadores a seguir controlam diversos aspectos de correspondência de expressão comum. Os valores do sinalizador podem ser especificados no momento que uma expressão é compilada em um objeto RegexPattern. Ou, eles podem ser especificado no próprio padrão utilizando as opções de padrão (?ismx-ismx).

Tabela 306. Opções de Sinalizador		
Sinalizador (padrão)	**Sinalizador (constante de API)**	**Descrição**
i	UREGEX_CASE_INSENSITIVE	Se configurado, a correspondência ocorre sem distinção de maiúsculas e minúsculas.
x	UREGEX_COMMENTS	Se configurado, o espaço em branco e #comments podem ser usados nos padrões.

Tabela 306. Opções de Sinalizador (continuação)		
Sinalizador (padrão)	**Sinalizador (constante de API)**	**Descrição**
s	UREGEX_DOTALL	Se configurado, um "." em um padrão corresponde a um terminador de linha no texto de entrada. Por padrão, não. Um par retorno de carro /feed de linha no texto se comporta como um único terminador de linha e corresponde a um único "." no padrão RE.
m	UREGEX_MULTILINE	Controlar o comportamento de "^" e "$" em um padrão. Por padrão, esses padrões correspondem somente no início e no fim, respectivamente, do texto de entrada. Se esse sinalizador estiver configurado, "^" e "$" também correspondem no início e no fim de cada linha no texto de entrada.

Criando Pacotes Configuráveis de Arquivo Não Agente

Você pode criar os pacotes configuráveis do arquivo que podem ser colocados no depósito do Tivoli Monitoring. Em seguida, esses pacotes configuráveis do arquivo podem ser implementados para sistemas de destino em seu ambiente.

Sobre Esta Tarefa

Com essa função, é possível configurar remotamente produtos para os quais não há opção de configuração remota. Para usar essa função, você coloca arquivos de configuração pré-preenchidos no depósito e os envia para os sistemas desejados.

Procedimento

1. No Agent Builder, selecione **Arquivo** > **Novo** > **Outro**.
2. No **Agent Builder**, selecione **Pacote Configurável de Implementação Remota de Não Agente**.
3. Clique em **Avançar**.
4. No campo **Nome do Projeto**, insira um nome para o projeto.
5. Clique em **Avançar**.
6. Preencha as informações na janela **Informações de Pacote Configurável de Implementação Remota**:
   a) No campo **Identificador de Pacote Configurável**, digite um identificador que seja uma sequência alfanumérica exclusiva de 3 a 31 caracteres. Essa sequência pode conter um hífen. A sequência deve iniciar com uma letra, mas não pode iniciar com um K ou um hífen.
   b) No campo **Descrição do Pacote Configurável**, digite uma descrição do pacote configurável.
   c) No campo **Versão**, digite uma versão para o pacote configurável no formato VVRRMMFFF. Em que `vv`= número da versão; `rr`= número da liberação; `mm`= número da modificação (número do fix pack) e `fff` = número da correção temporária.

7. Na área **Sistemas Operacionais**, selecione os sistemas operacionais nos quais o pacote configurável pode ser implementado.
8. Clique em **Concluir** para criar um projeto na área de trabalho e abrir o **Editor de Pacote Configurável de Implementação Remota**.

Editor de Pacotes Configuráveis de Implementação Remota

O Editor de Pacote Configurável de Implementação Remota é usado para gerar comandos para ajudar a implementar seu pacote configurável do arquivo.

O Editor de Pacote Configurável de Implementação Remota fornece informações sobre o pacote configurável para um projeto.

A seção **Informações de Identificação do Pacote Configurável** contém as seguintes informações:

Identificador do pacote configurável
ID exclusivo do pacote configurável

Descrição do pacote configurável
Descrição do pacote configurável

Versão do pacote configurável
Versão do pacote configurável

Compilação
Construir Identificador para o pacote configurável. Insira um número da construção aqui. Se nenhum número da construção estiver especificado, será gerado um número a partir da data e hora em que o pacote configurável for gerado.

Caixa de opção Criar Comandos de Cópia para os Arquivos no Pacote Configurável
Clique na caixa de opção para gerar um conjunto de comandos de cópia padrão, que são executados quando o pacote configurável é implementado. Os arquivos são copiados no local especificado na caixa de texto **Local da Cópia**. O local padrão é *INSTALLDIR*. Especifique essa variável de implementação remota a partir da implementação da linha de comandos, configurando KDY.*INSTALLDIR*=...

A seção **Sistemas Operacionais** mostra os sistemas operacionais para os quais o pacote configurável pode ser implementado.

A seção **Comandos** mostra os comandos a serem executados quando o pacote configurável for implementado.

A seção **Pacotes Configuráveis de Pré-requisitos** mostra os pacotes configuráveis que devem estar presentes para que esse pacote configurável funcione.

Use o Editor de Pacote Configurável de Implementação Remota para optar por um conjunto de comandos de cópia padrão que copiam os arquivos de seu pacote configurável em um local definido. Se essa opção estiver selecionada, um comando de cópia será gerado para cada arquivo no projeto do pacote configurável. O local da cópia padrão é *INSTALLDIR*. Uma variável de implementação remota especial que, se não configurada na linha de comandos de implementação, é padronizada como *CANDLEHOME*. Para alterar o local especificado por *INSTALLDIR*, especifique a propriedade **KDY.INSTALLDIR** ao executar o comando **addSystem**.

A mesma estrutura de diretório especificada em seu projeto de pacote configurável é replicada em *INSTALLDIR*. Por exemplo, se houver uma pasta denominada `config` em seu projeto de pacote configurável com um arquivo denominado `myprod.config`, então o comando de cópia gerada copiará o arquivo para *INSTALLDIR*`/config/myprod.config` quando o pacote configurável for implementado.

Incluindo Comandos no Pacote Configurável

É possível especificar mais comandos para execução durante a implementação.

Sobre Esta Tarefa

É possível especificar mais comandos para execução durante a implementação usando o **Editor de Pacote Configurável de Implementação Remota**.

Procedimento

1. Para especificar mais comandos para execução durante a implementação, clique em **Incluir** na seção **Comandos** do **Editor de Pacote Configurável de Implementação Remota**.
2. Na janela **Comando**, selecione o tipo de comando **Pré-Instalação**, **Instalação**, **Pós-Instalação**, ou **Desinstalação** e, então, especifique o comando a executar.

   Você deve especificar o caminho completo para o comando que deseja executar. Por conveniência, a implementação remota fornece um conjunto definido de variáveis predefinidas. Para fazer referência à variável de um comando, cerque a variável com barras verticais, por exemplo `|DEPLOYDIR|`. Para obter informações adicionais sobre as variáveis predefinidas para os comandos, consulte (Tabela 307 na página 1500).

Tabela 307. Variáveis Predefinidas para os Comandos

Variável	Descrição
DEPLOYDIR	O diretório temporário no terminal em que o pacote configurável é armazenado durante a implementação. Por exemplo, se desejar executar `myscript.sh`, um script incluso em seu pacote configurável, especifique o comando a seguir: `|DEPLOYDIR|/myscript.sh`
INSTALLDIR	Ou *CANDLEHOME* ou o valor de *KDY.INSTALLDIR* se especificado no comando **addSystem**.
CANDLEHOME	O diretório de instalação do Tivoli Monitoring.

3. Finalmente, selecione os **Sistemas Operacionais** nos quais o comando deve ser executado.

Incluindo Pré-requisitos no Pacote Configurável

Use o **Editor de Pacote Configurável de Implementação Remota** para especificar pré-requisitos do pacote configurável.

Procedimento

1. Para incluir um pré-requisito, clique em **Incluir** na seção **Pacotes Configuráveis de Pré-requisito** da página **Editor de Pacote Configurável de Implementação Remota**, **Informações de Pacote Configurável**.
2. Na janela **Novo Pré-requisito**, insira o identificador de pacote configurável do qual esse pacote configurável depende e a versão mínima necessária.
3. Selecione os sistemas operacionais para os quais esse pré-requisito é necessário.
4. Clique em **OK** para concluir e sair.

Incluindo Arquivos no Pacote Configurável

Inclua arquivos em um pacote configurável de arquivo usando o **Editor de Pacote Configurável de Implementação Remota**.

Procedimento

1. Para incluir arquivos no pacote configurável de implementação remota, execute um dos seguintes procedimentos:
   - No Editor de Pacote Configurável, clique em **Incluir Arquivos no Pacote Configurável**.
   - Clique com o botão direito no projeto na árvore do navegador, clique em **Implementação Remota do IBM Tivoli Monitoring** > **Incluir Arquivos no Pacote Configurável**

   Ambas as ações são exibidas na janela **Importar Arquivos de Pacote Configurável**:
2. Especifique arquivos individuais ou diretórios que contêm arquivos na área **Informações de Arquivo**.

3. Clique em **Concluir**.

   Os arquivos ou diretórios que estão especificados são copiados no diretório do projeto. A estrutura de diretório no projeto é mantida ao criar o pacote configurável de implementação remota. Se desejar que o Agent Builder gere comandos de cópia padrão, assegure-se de que os arquivos estejam na estrutura de diretório correta para a implementação.

Gerando o Pacote Configurável

Use o Agent Builder para gerar um pacote configurável para implementação remota de um agente.

Procedimento

1. Para gerar o pacote configurável de implementação remota, use um dos procedimentos a seguir para exibir a janela **Gerar Pacote Configurável de Implementação Remota Final**
   - No **Editor de Pacote Configurável de Implementação Remota**, clique em **gerar o pacote configurável de implementação remota final**.
   - Clique com o botão direito no projeto na árvore do navegador e clique em **Implementação Remota do IBM Tivoli Monitoring** > **Gerar Pacote Configurável de Implementação Remota**
2. Agora é possível gerar o pacote configurável de duas maneiras:
   - Se houver um Tivoli Enterprise Monitoring Server no sistema no qual o Agent Builder está em execução, clique em **Instalar o pacote configurável de Implementação Remota em um depósito local do TEMS**.

     O Agent Builder tenta determinar o local da instalação do Tivoli Monitoring e inseri-lo no campo **Diretório**. Se *CANDLE_HOME* não estiver configurado, o local padrão de `C:\IBM\ITM` ou `/opt/IBM/ITM` será utilizado. Assegure-se de que o local da instalação esteja correto antes de continuar.

     Você deve fornecer as informações de login do Tivoli Enterprise Monitoring Server para instalar o pacote configurável.
   - Para gerar o pacote configurável em um diretório em seu sistema, clique em **Gerar o Pacote Configurável de Implementação Remota em um diretório local**

     Após a conclusão do processo, você deverá transferir esse diretório para um sistema do Tivoli Enterprise Monitoring Server e usar o comando `tacmd addbundles` para incluir o pacote configurável no depósito.

O que Fazer Depois

Ao implementar o pacote configurável, você deve usar o comando `tacmd addSystem`. Exemplo:

```
tacmd addsystem -t MONITORINGCOLLECTION -n Primary:ITMAGT:NT
```

Em que `-t` (tipo) é o Código do Produto conforme retornado pelo comando `tacmd viewDepot`:

```
>tacmd viewDepot
Product Code : MONITORINGCOLLECTION
Version : 010000003
Description : MonitoringCollectionScripts
Host Type : WINNT
Host Version : WINNT
Prerequisites:
```

Nota: Não é possível implementar remotamente a partir da Área de Trabalho ou Navegador do Tivoli Enterprise Portal. A implementação remota a partir da Área de Trabalho ou do Navegador Tivoli Enterprise Portal resulta na mensagem KFWITM219E.

Consulte a documentação do Tivoli Monitoring para obter mais detalhes.

Criando Pacotes Configuráveis Implementáveis para as Análises Tivoli Netcool/OMNIbus

É possível usar o Agent Builder para criar pacotes configuráveis de pacote e de configuração que podem ser usados para implementar as análises do Tivoli Netcool/OMNIbus em computadores remotos.

Sobre Esta Tarefa

Para suportar a implementação remota de análises, também é possível criar pacotes configuráveis do Tivoli Netcool/OMNIbus que podem ser implementados em computadores remotos antes da implementação das análises.

Procedimento

1. No Agent Builder, selecione **Arquivo** > **Novo** > **Outro**.
2. Em **Assistentes do IBM Tivoli OMNIbus**, selecione **Pacote Configurável do Pacote**.
3. Clique em **Avançar**.

O que Fazer Depois

Em seguida, use o assistente do **OMNIbus Install Bundle** para criar os pacotes configuráveis. Para obter informações sobre o uso desse assistente, consulte a documentação do Tivoli Netcool/OMNIbus.

Suporte ao Nome de Arquivo Dinâmico

Usar o suporte de nome do arquivo dinâmico para especificar um padrão de nome do arquivo em vez de um nome do arquivo real.

Alguns programas aplicativos criam um nome do arquivo de saída que está sujeito a mudança. O nome muda com base nos critérios específicos, como o dia atual, mês, ano, ou um nome de arquivo que inclui uma incrementação do número de sequência. Nesses casos, é possível especificar o padrão de nome do arquivo em vez do nome do arquivo real. Há dois formatos padrão que são reconhecidos ao especificar o padrão de nome do arquivo:

- Expressões Regulares (preferencial).
- Sintaxe do nome do arquivo dinâmico do IBM Tivoli Universal Agent (descontinuado).

Padrões de nome do arquivo de expressão regular

Para especificar padrões de nome de arquivo, é possível usar expressões regulares de acordo com a sintaxe de International Components for Unicode (ICU) que está documentada em (“Expressões Regulares ICU” na página 1492). Para esse recurso, você deve selecionar a caixa de seleção **Nomes de arquivo correspondem a expressão regular** na página **Informações de Grupo de Atributos de Arquivo de Log Avançado**. Ao especificar padrões de expressão regular, você também deve selecionar uma opção da lista **Quando Vários Arquivos Correspondem** na página **Informações do Grupo de Atributos de Arquivo de Log Avançadas** para especificar as diretrizes para selecionar o arquivo correspondente mais atual.

Nota: As expressões regulares são o método preferencial para especificar padrões de nome de arquivo.

Para obter mais informações sobre como configurar as propriedades de grupo de atributos de arquivo de log avançado, consulte (“Monitorando um Arquivo de Log” na página 1262), Etapa (“6” na página 1263). Por exemplo, se você especificou um padrão de nome do arquivo:

```
d:\program files\logs\tivoli.*
```

Esse padrão corresponde aos nomes de arquivo que começam com `tivoli` no diretório `d:\program files\logs`. As expressões regulares podem ser especificadas somente para a parte do nome do arquivo e não para o nome do caminho.

Sintaxe do Nome do Arquivo Dinâmico

Com a sintaxe do nome do arquivo dinâmico, somente um arquivo de cada vez pode ser monitorado. O Provedor de Dados do Arquivo inspeciona todos os arquivos no local do caminho designado, buscando arquivos que correspondem ao padrão definido. O Provedor de Dados do Arquivo sempre monitora o arquivo correspondente mais atual, baseado em qualquer nome do arquivo correspondente que tenha o número ou o valor de data/hora mais alto. O arquivo apropriado a ser monitorado é determinado pelo nome do arquivo, em vez de pela criação do arquivo ou outros critérios.

Os padrões podem ser especificados para nomes do arquivo com qualquer número de partes. Por exemplo, `Log{###}` corresponde a nomes de arquivos de uma parte, como `Log010` ou `Log456`. Em nomes do arquivo de múltiplas partes, os caracteres padrão podem ser especificados em qualquer parte do nome do arquivo ou em múltiplas partes. Por exemplo, `aaa.bbb{???}.ccc` é um padrão válido e `aaa.bbb{???}.ccc{###}` também é válido.

Nota: As expressões regulares em vez da sintaxe de nome de arquivo dinâmico são o método preferencial para especificar padrões de nome de arquivo; para obter informações adicionais sobre expressões regulares, consulte "Padrões de nome do arquivo de expressão regular" na página 1502

Os exemplos a seguir ilustram a especificação de padrão de nome do arquivo:

`{#########}.abc`
Corresponde a nome do arquivo numérico de comprimento 8 e a extensão do arquivo *`.abc`*, como `10252006.abc` ou `10262006.abc`. O arquivo `10262006.abc` é monitorado porque `10262006` é maior do que `10252006`.

`{#########}.*`
Corresponde aos nomes do arquivo numérico de comprimento 8 e ignora a extensão do arquivo. Exemplos incluem `20061025.log`, `20061101.log` e `10252006.abc`. O arquivo `20061101.log` é monitorado porque `20061101` é o número maior.

`{######??}.abc`
Corresponde a nome do arquivo numérico de comprimento 8 e extensão do arquivo `.abc`, e ignora as duas últimas posições na porção de nome. Exemplos incluem `02110199.abc`, `02110200.abc` e `021101AZ.abc`. O arquivo `02110200.abc` é monitorado porque `021102` é o número maior.

`Console.{######}`
Corresponde a nomes de arquivo que contêm *`Console`* na parte de nome e um número de seis dígitos na porção de extensão. Exemplos incluem `Console.000133`, `Console.000201` e `Console.000134`. O arquivo `Console.000201`é monitorado.

`IN{######}.log`
Corresponde a nomes do arquivo que começam com `IN` seguidos por seis numerais e a extensão do arquivo `.log`. Exemplos incluem `IN021001.log`, `IN021002.log` e `IN021004.log`. O arquivo `IN021004.log` é monitorado.

`PS{###}FTP.txt`
Corresponde a nomes do arquivo que começam com PS seguidos por três numerais, seguidos por FTP, e a extensão `.txt`. Exemplos incluem `PS001FTP.txt`, `PS005FTP.txt` e `PS010FTP.txt`. O arquivo `PS010FTP.txt`é monitorado.

Siga essas diretrizes para estabelecer os padrões de nome do arquivo:

- Use chaves {} para fechar os caracteres padrão em um nome do arquivo. A presença de caracteres padrão dentro das chaves indica que um padrão de nome do arquivo está sendo usado.
- Use um asterisco (*) como um curinga para ignorar extensões do arquivo ou quaisquer caracteres à direita no nome do arquivo. Por exemplo, `Myapp{###}.log*` especifica que qualquer nome do arquivo que começa com `Myapp`, seguido por esses três dígitos, e seguido por `.log`, é uma correspondência, independentemente do que vem depois.

  O asterisco deve ser especificado após as chaves (`{ }`) e não pode ser usado no início de um nome do arquivo. Ao usar o asterisco em uma extensão do nome do arquivo, o asterisco deverá ser usado sozinho.

  Exemplos desse uso correto de curinga (`*`):

err{??}.*

error{$}.*

Exemplos de uso incorreto de curinga (*):

error.20*
Nenhuma chave precede o asterisco (*).

error*.{###}
O asterisco não é usado no final do nome do arquivo.

error.*
Nenhuma chave precede o asterisco (*).

- Se uma extensão do arquivo específico estiver definida, somente os arquivos com a mesma extensão serão considerados.
- Use um sinal de número para indicar cada elemento numérico de um nome do arquivo.
- Use um ponto de interrogação para excluir cada elemento da convenção de nomenclatura que não serve como critérios de procura na determinação do nome do arquivo apropriado.
- Use um cifrão ($) para representar qualquer caractere ou nenhum caractere. Por exemplo, se deseja corresponder a dois arquivos chamados Log e LogA, especifique Log{$}. O sinal de dólar tem várias restrições de uso. Ao usar um ou mais cifrões como prefixo de um nome do arquivo como em {$$$$$}_abc.log, o número de cifrões deve corresponder exatamente ao número de caractere nessa posição no nome do arquivo. Também, não é possível especificar cifrões em diversos locais em um padrão de nome do arquivo, por exemplo, {$$$}b{$$$}.log não corresponde a abc.log. Dadas essas restrições de cifrão, utilize padrões de nome de arquivo de expressão regular se houver um número indeterminado de caracteres nos nomes do arquivo.
- O número total de sinais de número e pontos de interrogação entre chaves é significativo. Ele deve corresponder exatamente à parte do nome do arquivo. Por exemplo, o padrão AA{####} instrui ao Provedor de Dados de Arquivo a procurar arquivos como AA0001. Nomes de arquivo, como AA001 ou AA00001, não são considerados.
- O padrão de nome do arquivo exato, a constante e as parte numéricas devem corresponde exatamente ao nome do arquivo. Por exemplo, o padrão AA{###} instrui ao Provedor de Dados de Arquivo a verificar o arquivo AA101. Nomes de arquivo, como XAA101, AA222X e AA55555, não são considerados.
- Use a sequência padrão reservada {TIVOLILOGTIME} a ser substituída pelo registro de data e hora hexa e o número de sequência do arquivo em um agente do Tivoli Monitoring ou arquivo de log do servidor. Essa sequência padrão é útil ao executar o automonitoramento de componentes do Tivoli Monitoring. Por exemplo, se você deseja monitorar o último log do servidor de monitoramento no diretório /opt/IBM/ITM/logs, pode especificar um padrão de nome do arquivo:

```
/opt/IBM/ITM/logs/Host1_ms_{TIVOLILOGTIME}.log
```

Se Host1_ms_452053c0-01.log, Host1_ms_451f11f4-01.log, Host1_ms_45205946-01.log e Host1_ms_451f11f4-02.log estiverem presentes no diretório /logs, o arquivo Host1_ms_45205946-01.log será selecionado para monitoramento.

Para especificar precisamente um nome do arquivo que consiste de componentes de data (ano, mês e dias), use as letras maiúsculas Y, M e D. Essas letras devem ser especificadas entre chaves; caso contrário, elas serão tratadas como caracteres literais no nome de arquivo.

Veja os seguintes exemplos:

{YYYYMMDD}.log
Especifica nomes do arquivo como 20060930.log ou 20061015.log.

{MMDDYY}.log
Especifica nomes do arquivo como 101106.log ou 110106.log.

{DDMMYYYY}.log
Especifica nomes do arquivo como 01092006.log ou 15082006.log.

{DDMMMAA}.log
Especifica nomes do arquivo como 24Jan07 ou 13Sep06.

{MM-DD-AA}.log
Especifica nomes do arquivo, como 11-02-06 ou 04-29-07. O caractere separador (-) é ignorado no campo de data e não requer um padrão de ponto de interrogação para ser ignorado.

MY{YYDDD}.log
Especifica nomes do arquivo como MY06202.log, MY06010.log ou MY04350.log.

Casos complexos existem, em que um campo de data é integrado dentro de um nome do arquivo mais longo, e os padrões de data nos exemplos anteriores não são suficientes. Para casos complexos, crie padrões que combinem sinais de número e pontos de interrogação e ainda execute comparações numéricas que selecionem o arquivo mais atual para monitoramento. Por exemplo, o padrão ABC{?#####?##?##?##?##?##?}XYZ.TXT pode ser usado para nomes de arquivo, como ABC 2006-04-20 11_22_33 XYZ.TXT. Nesse exemplo, você está interessado somente em dígitos marcados #- e os pontos de interrogação servem como marcadores que ignoram outros caracteres no nome do arquivo.

O Provedor de Dados do Arquivo verifica periodicamente novos arquivos que correspondem ao padrão do arquivo definido no local do caminho de destino. Quando um arquivo que nunca corresponde ao padrão for detectado, o Provedor de Dados do Arquivo alternará automaticamente o monitoramento de aplicativo para o novo arquivo. O Provedor de Dados do Arquivo procura o melhor arquivo correspondente quando:

- O Provedor de Dados do Arquivo inicia pela primeira vez.
- O arquivo monitorado atualmente não existe mais em razão de possível renomeação ou exclusão.
- O conteúdo do arquivo existente foi alterado em razão de possível regravação.
- O intervalo de verificação expirou. O intervalo padrão é 10 minutos. É possível alterar o intervalo para um valor de intervalo mais longo ou mais curto especificando a variável de ambiente.

```
KUMP_DP_FILE_SWITCH_CHECK_INTERVAL=número-de-segundos
```

Configuração de Trap SNMP

Descrição do arquivo de configuração usado pelo SNMP Provedor de Dados para renderizar informações de trap de uma forma mais facilmente legível. O arquivo também é usado para designar categorias, severidades, status e IDs de origem para traps.

Ele também contém instruções para modificar o arquivo padrão ou substituir seu próprio arquivo de configuração.

arquivo de configuração de trap SNMP, trapcnfg

Na inicialização, o SNMP Provedor de Dados lê um arquivo de configuração denominado trapcnfg. Um propósito deste arquivo é converter as informações sobre do trap SNMP em uma forma mais legível. Outro é designar as categorias, severidades, status e IDs de origem para os traps específicos, porque essas categorias não estão definidas por SNMP.

É possível modificar o arquivo trapcnfg para que ele se ajuste às necessidades específicas do site incluindo novo trap ou definições corporativas ou alterando as existentes. É possível usar também seu próprio arquivo de configuração.

Use o arquivo trapd.conf HP OpenView

O arquivo trapcnfg é semelhante no formato, mas não é idêntico, ao arquivo de configuração de trap trapd.conf do HP OpenView Network Node Manager. É possível copiar o arquivo OpenView e reutilizar várias das instruções de definição, se necessário.

Tipos de Registros

O trapcnfg contém três tipos de registros ou blocos de registros:

comentários
Registros de comentário são iniciados com um sinal de número (#).

definições corporativas
As definições corporativas consistem em dois tokens delimitados por branco, em que o primeiro token é um nome e o segundo é um identificador de objeto (OID) circundado por chaves ({ }).

definições de trap
As definições de trap consistem em oito tokens delimitados por branco. As definições de trap são registros de blocos, porque cada definição poderá consistir em múltiplos registros.

O primeiro tipo é auto-explicativo. (Figura 87 na página 1506) mostra exemplos do segundo e terceiro tipos.

O primeiro exemplo em Figura 87 na página 1506 mostra um registro de definição corporativa que define a empresa OID 1.3.6.1.4.1.311.1.1.3.1.1 como sendo Microsoft Windows NT.

O segundo exemplo mostra um registro de definição de trap que define `trapName MSNTCOLD` como sendo associado à empresa OID `1.3.6.1.4.1.311.1.1.3.1.1`, número de trap genérico 0 e número de trap específico 0. Observe que a severidade está em formato decimal embora a categoria esteja no formato textual. As gravidades são convertidas em seu formato textual antes de serem exibidas. O próximo registro no bloco de registros do tipo 3 é a descrição curta, que o Agent Builder não usa. O Agent Builder usa a descrição detalhada dentro dos delimitadores SDESC e EDESC.

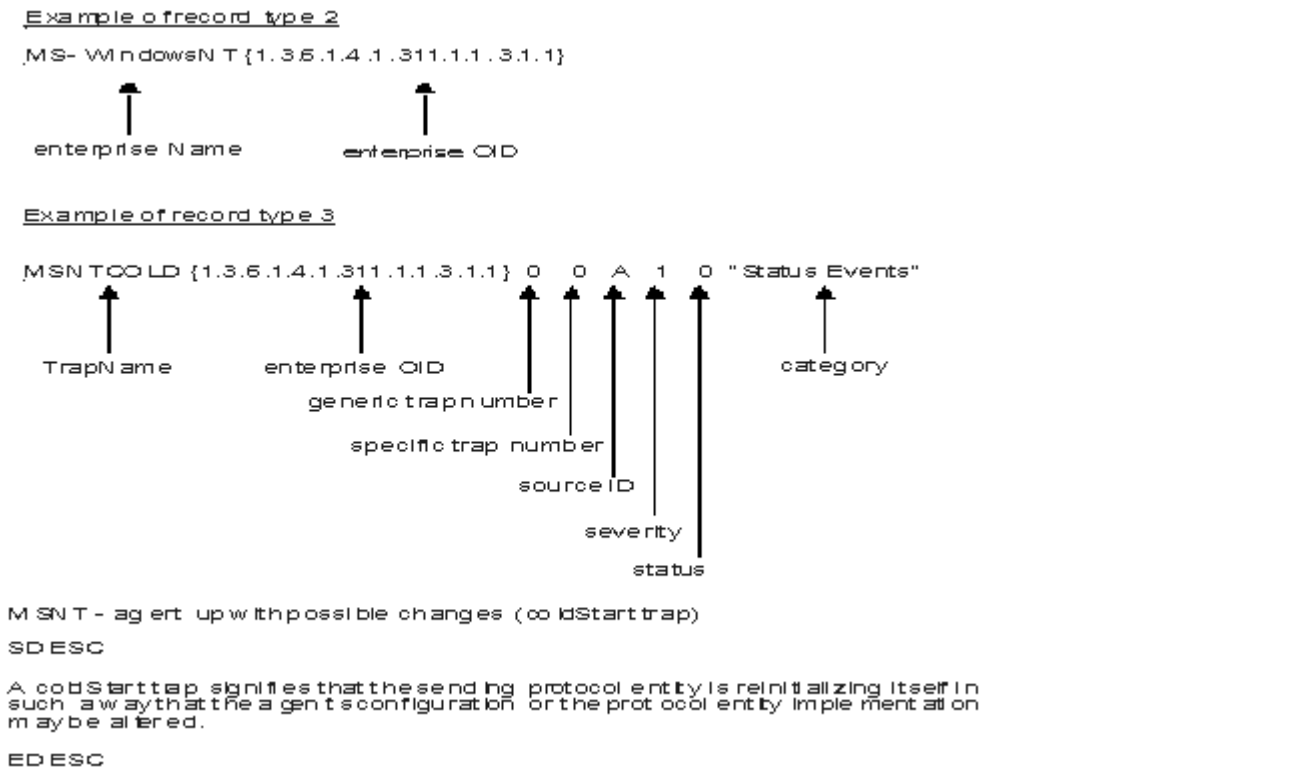


Figura 87. Exemplos de Tipos de Registros de Configuração 2 e 3

Padrões para o arquivo `trapcnfg`

Tabelas que listam os padrões que são suportados pelo SNMP Provedor de Dados.

Categorias Suportadas

(Tabela 308 na página 1507) mostra as categorias suportadas pelo Agent Builder.

Tabela 308. Categorias suportadas pelo SNMP Provedor de Dados	
Categoria	**Representação textual**
0	Eventos de Limites
1	Eventos de Topologia de Rede
2	Eventos de Erros
3	Eventos de Status
4	Eventos de Configuração de Nó
5	Eventos de Alertas de Aplicativos
6	Eventos de Todas as Categorias
7	Eventos Somente de Log
8	Mapear Eventos
9	Ignorar Eventos

(Tabela 309 na página 1507) lista as severidades suportadas pelo Agent Builder.

Tabela 309. Gravidades suportadas pelo SNMP Provedor de Dados	
Gravidade	**Representação textual**
0	Limpar
1	Indeterminado
2	Aviso
3	Erro Menor
4	Crítico
5	Erro Mais Grave

Status Suportados

(Tabela 310 na página 1507) mostra os status definidos no arquivo de configuração do Agent Builder.

Tabela 310. Status suportados pelo SNMP Provedor de Dados	
Estado	**Representação textual**
0	Inalterado
1	Desconhec.
2	Para cima
3	Marginal
4	Inativo
5	Não gerenciado
6	Confirmar
7	Usuário1
8	Usuário2

IDs de Origem Suportados

(Tabela 311 na página 1508) lista os IDs de origem suportados por `trapcnfg`.

Tabela 311. IDs de origem suportados pelo SNMP Provedor de Dados

ID de origem	Descrição
a	Aplicativo
A	Agente
C	Xnmcollect
d	Demo
D	Data Collector
E	Nvevents
I	Ipmap
L	LoadMIB
m	Shpmon
M	Topologia de IP
n	netmon relacionado
N	Traps gerados por netmon
O	OSI SA
E	Traps não IP
r	Tralertd
s	Spappld
S	Agente de Segurança
t	Xnmtrap
e	Trapd
V	Fornecedor relacionado
?	Desconhec.

Referência dos Comandos Executar Ação

Uma visão geral dos comandos Executar Ação, referências sobre os comando Executar Ação e descrições dos comandos especiais Executar Ação.

Sobre Comandos Executar Ação

Os comandos Executar Ação podem ser incluídos em um agente de monitoramento do Agent Builder. Os comandos Executar Ação podem ser executados a partir de um cliente de portal ou incluídos em uma situação ou uma política. Quando incluído em uma situação, o comando é executado quando a situação se torna verdadeira. Um comando Executar Ação em uma situação também é conhecida como automação de reflexo. Quando você ativa um comando executar ação em uma situação, automatiza uma resposta para condições do sistema. Por exemplo, você pode usar um comando Executar Ação para enviar um comando para reiniciar um processo no sistema gerenciado. Também é possível usar um comando Executar Ação para enviar uma mensagem de texto para um telefone celular.

A automação avançada usa políticas para executar ações, planejar trabalho e automatizar tarefas manuais. Uma política compreende uma série etapas automatizadas chamadas atividades que estão conectadas para criar um fluxo de trabalho. Após a conclusão de uma atividade, o Tivoli Enterprise Portal recebe feedback do código de retorno e a lógica de automação avançada responde com atividades subsequentes prescritas pelo feedback.

O comando básico Executar Ação exibe o código de retorno da operação em uma caixa de mensagem ou arquivo de log que é exibido após a conclusão da ação. Depois de fechar esse janela, nenhuma informação nova é disponível para essa ação.

Mais informações sobre Comandos Executar Ação

Para obter informações adicionais sobre como trabalhar com comandos Executar Ação, consulte *Tivoli Enterprise Portal: Guia do Usuário*.

Para obter uma lista e descrição dos comandos Executar Ação para este agente de monitoramento, consulte ("Comandos Executar Ação Especiais" na página 1509). Consulte também as informações nessa seção para cada comando individual.

Comandos Executar Ação Especiais

Um agente de monitoramento do Agent Builder pode reconhecer e executar processamento especial para um conjunto de comandos Executar Ação:

- SSHEXEC

Para obter mais informações sobre a criação desses comandos e incluí-los em um projeto de agente de monitoramento do Agent Builder, consulte ("Criando Espaços de Trabalho, Comandos Executar Ação e Situações" na página 1371).

Ação SSHEXEC

Antes de Iniciar

Para obter informações adicionais sobre os comandos Executar Ação, consulte ("Referência dos Comandos Executar Ação" na página 1508).

Sobre Esta Tarefa

A ação SSHEXEC é reconhecida por um aplicativo monitorado que possui pelo menos um grupo de atributos de script SSH. Isso indica que o comando que segue o teclado SSHEXEC é iniciado remotamente no sistema de destino SSH. O comando é iniciado com as credenciais e privilégios do usuário configurados para monitorar o sistema de destino SSH. O comando é executado no sistema remoto que está representado pelo Nome do Sistema Gerenciado.

Procedimento

Para incluir o comando executar ação em uma situação ou política de fluxo de trabalho, utilize a seguinte sintaxe do comando do sistema:

```
SSHEXEC [Command]
```

Exemplo:

```
SSHEXEC [ls &path]
```

Nota: É possível customizar o comando ou as partes do comando durante a chamada de Executar Ação usando a opção de argumentos de Executar Ação com o *Comando*.

Nota: Se o *Comando* incluir vários argumentos, então considere incluir colchetes para ativar a chamada do comando Executar Ação com a interface da linha de comandos **tacmd**.

Recursos de Acessibilidade

Os recursos de acessibilidade ajudam os usuários que possuem uma deficiência, como mobilidade restrita ou visão limitada, a usar o conteúdo de tecnologia da informação com êxito.

Recursos de Acessibilidade

A interface baseada na web do IBM Cloud Application Performance Management é o Console do Cloud APM. O console inclui os seguintes recursos principais de acessibilidade:

- Permite que usuários usem tecnologias assistivas, como o software de leitor de tela e o sintetizador de voz digital, para ouvir o que é exibido na tela. Consulte a documentação do produto da tecnologia assistida para obter detalhes sobre como utilizar essas tecnologias juntamente com o produto.
- Permite que usuários operem recursos específicos ou equivalentes usando apenas o teclado.
- Comunica todas as informações independentemente de cor. As páginas [1]

O Console do Cloud APM usa o W3C Standard mais recente, WAI-ARIA 1.0 (http://www.w3.org/TR/wai-aria/), para garantir conformidade com US Section 508 (http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) e Web Content Accessibility Guidelines (WCAG) 2.0 . Para aproveitar os recursos de acessibilidade, use a liberação mais recente do seu leitor de tela junto com o navegador da web mais recente suportado por este produto.

A documentação on-line do produto Console do Cloud APM no IBM Knowledge Center é ativada para acessibilidade. Os recursos de acessibilidade do IBM Knowledge Center são descritos nas notas sobre a liberação do IBM Knowledge Center .

Navegação por Teclado

Este produto usa as chaves de navegação padrão.

Informações da Interface

A interface com o usuário da web do Console do Cloud APM não depende das folhas de estilo em cascata para renderizar o conteúdo corretamente e fornecem uma experiência utilizável. No entanto, a documentação do produto depende de folhas de estilo em cascata. O IBM Knowledge Center fornece uma maneira equivalente para usuários com deficiência visual usarem suas configurações de exibição customizadas, incluindo o modo de alto contraste. É possível controlar o tamanho da fonte usando o dispositivo ou as configurações do navegador.

A interface com o usuário da web Console do Cloud APM inclui referências de navegação WAI-ARIA que você pode usar para navegar rapidamente para áreas funcionais no aplicativo.

A interface com o usuário do Console do Cloud APM não possui conteúdo que pisca de 2 a 55 vezes por segundo.

Informações de acessibilidade relacionadas

Além do IBM help desk padrão e dos websites de suporte, a IBM estabeleceu um serviço telefônico TTY para que os clientes surdos ou com deficiência auditiva acessem os serviços de vendas e suporte:

Serviço de TTY
800-IBM-3383 (800-426-3383) (na América do Norte)

[1] Exceções incluem alguma **Configuração do agente** do console do Performance Management.

IBM e Acessibilidade

Para obter mais informações sobre o compromisso que a IBM tem com a acessibilidade, consulte IBM Accessibility (www.ibm.com/able).

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos EUA. Este material pode estar disponível na IBM em outros idiomas. Entretanto, pode ser necessário que possua uma cópia do produto ou versão de produto nesse idioma a fim de acessá-lo.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou aplicativos de patentes pendentes relativas aos assuntos tratados nesta publicação. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Consultas sobre licenças devem ser enviadas, por escrito, para:

Gerência
de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo,
Rio de Janeiro, RJ
CEP 22290-240

Para pedidos de licença relacionados a informações de DBCS (Conjuntos de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA" SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO LIMITADO ÀS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Estas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a websites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses websites. Os materiais nesses websites não fazem parte dos materiais para esse produto IBM e o uso desses websites é de inteira responsabilidade do Cliente.

A IBM pode usar ou distribuir qualquer informação que você fornecer de qualquer forma que julgar apropriada sem incorrer em qualquer obrigação para com você.

Os licenciados deste programa que desejarem obter informações sobre este assunto com o propósito de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) o uso mútuo das informações trocadas, deverão entrar em contato com:

Gerência
de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo,
Rio de Janeiro, RJ
CEP 22290-240

Tais informações podem estar disponíveis, sujeitas aos termos e condições apropriados, incluindo em alguns casos, o pagamento de uma taxa.

O programa licenciado descrito neste documento e todo o material licenciado disponível para ele são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato de Licença de Programa Internacional IBM ou de qualquer outro contrato equivalente entre as partes.

Os dados de desempenho discutidos aqui são apresentados como derivados sob as condições operacionais específicas. Os resultados reais podem variar.

As informações referentes a produtos não IBM foram obtidas dos fornecedores desses produtos, seus anúncios publicados ou outras fontes disponíveis publicamente. A IBM não testou esses produtos e não pode confirmar a precisão dos desempenhos, compatibilidade ou quaisquer outras reivindicações relacionadas a produtos não IBM. Dúvidas sobre os recursos de produtos não IBM devem ser encaminhadas aos fornecedores desses produtos.

As declarações relacionadas a direção ou intenção futuros da IBM estão sujeitas a alteração ou retirada sem aviso prévio e representam metas e objetivos apenas.

Essas informações são apenas para planejamento. As informações aqui contidas estão sujeitas a mudanças antes que os produtos descritos estejam disponíveis.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos têm os nomes de pessoas, empresas, marcas e produtos. Todos esses nomes são fictícios e qualquer semelhança com pessoas reais ou empresas é mera coincidência.

LICENÇA DE COPYRIGHT:

Estas informações contêm exemplo de programas aplicativos na linguagem fonte, que ilustram técnicas de programação em várias plataformas operacionais. O Cliente pode copiar, modificar e distribuir essas amostras em qualquer formato sem a necessidade de pagamento à IBM, com objetivos de desenvolvimento, utilização, marketing ou distribuição de programas aplicativos em conformidade com a interface de programação de aplicativo da plataforma operacional para a qual os programas de amostra são gravados. Esses exemplos não foram testados completamente em todas as condições. Portanto, a IBM não pode garantir ou implicar a confiabilidade, capacidade de manutenção ou função destes programas. Os programas de amostra são fornecidos "NO ESTADO EM QUE SE ENCONTRAM", sem garantia de qualquer tipo. A IBM não poderá ser responsabilizada por quaisquer danos decorrentes ao uso dos programas de amostra.

Cada cópia ou qualquer parte desses programas de amostra ou qualquer trabalho derivado deve incluir um aviso de copyright
como
a seguir:
© (nome da sua empresa) (ano).
Portions of this code are derived from
IBM Corp. Sample Programs.
© Copyright IBM Corp. 2014, 2015.

Marcas comerciais

IBM, o logotipo IBM e ibm.com são marcas ou marcas registradas da International Business Machines Corp., registradas em vários países no mundo todo. Outros nomes de produtos e serviços podem ser

marcas registradas da IBM ou de outras empresas. Uma lista atual de marcas comerciais da IBM está disponível na web em "Copyright and trademark information" em www.ibm.com/legal/copytrade.shtml.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e/ou em outros países.

Microsoft, Windows, Windows NT e o logotipo Windows são marcas comerciais da Microsoft Corporation nos Estados Unidos e/ou em outros países.

UNIX é uma marca registrada do The Open Group nos Estados Unidos e em outros países.

Java e todas as marcas registradas e logotipos baseados em Java são marcas ou marcas registradas da Oracle e/ou de suas afiliadas.

Termos e condições para documentação do produto

Permissões para o uso destas publicações são concedidas sujeitas aos seguintes termos e condições.

Aplicabilidade

Esses termos e condições estão em adição a quaisquer termos de uso do website da IBM.

Uso pessoal

O Cliente pode reproduzir essas publicações para seu uso pessoal, não comercial, desde que todos os avisos do proprietário sejam preservados. Você não pode distribuir, exibir ou fazer trabalho derivado dessas publicações, ou qualquer parte delas, sem o consentimento expresso da IBM.

Uso comercial

O Cliente pode reproduzir, distribuir e exibir essas publicações unicamente dentro de sua empresa desde que todos os avisos do proprietário sejam preservados. O Cliente não pode criar trabalhos derivados dessas publicações ou reproduzir, distribuir ou exibir essas publicações ou qualquer parte delas fora de sua empresa, sem o consentimento expresso da IBM.

Direitos

Exceto conforme expressamente concedido nesta permissão, nenhuma outra permissão, licença ou direito são concedidos, seja expressa ou implícita, para as publicações ou quaisquer informações, dados, software ou outra propriedade intelectual neles contidos.

A IBM se reserva o direito de retirar as permissões aqui concedidas sempre que, a seu critério, o uso das publicações for prejudicial ao seu interesse ou, conforme determinado pela IBM, as instruções acima não estão sendo seguidas adequadamente.

O Cliente não pode fazer download, exportar ou reexportar estas informações, exceto em conformidade total com todas as leis e regulamentações aplicáveis, incluindo todas as leis e regulamentos da exportação dos Estados Unidos.

A IBM NÃO OFERECE GARANTIA SOBRE O CONTEÚDO DESTAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO FORNECIDAS "NO ESTADO EM QUE SE ENCONTRAM" E SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO, NÃO INFRAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO.

Declaração de privacidade on-line da IBM

Os produtos de software IBM, incluindo soluções de software como serviço, ("Ofertas de Software") podem usar cookies ou outras tecnologias para coletar informações de uso do produto, para ajudar a melhorar a experiência do usuário final, para customizar as interações com o usuário final ou para outros propósitos. Em muitos casos, nenhuma informação pessoalmente identificável é coletada pelas Ofertas de Software. Algumas de nossas Ofertas de Software podem ajudar a permitir a coleta de informações identificáveis pessoalmente. Se essa Oferta de Software usar cookies para coletar informações pessoalmente identificáveis, informações específicas sobre o uso dessa oferta de cookies serão apresentadas nos parágrafos a seguir.

Dependendo das configurações implementadas, essa Oferta de Software pode usar cookies de sessão que coletam cada nome de usuário do usuário para propósitos de gerenciamento de sessão, autenticação e configuração de conexão única. Esses cookies podem ser desativados, mas desativá-los provavelmente também eliminará a funcionalidade que eles ativam.

Se as configurações implementadas nesta Oferta de Software fornecerem a você como cliente a capacidade de coletar informações identificáveis pessoalmente dos usuários finais por meio de cookies e outras tecnologias, você deverá consultar seu próprio conselho jurídico sobre as leis aplicáveis a tal coleta de dados, incluindo os requisitos para aviso e consentimento.

Para obter mais informações sobre o uso de várias tecnologias, incluindo cookies, para esses propósitos, consulte a Política de privacidade da IBM em http://www.ibm.com/privacy e a Declaração de privacidade on-line da IBM na seção http://www.ibm.com/privacy/details titulada "Cookies, Web Beacons and Other Technologies" e "IBM Software Products and Software-as-a-Service Privacy Statement" em http://www.ibm.com/software/info/product-privacy.