Referência do Coletor de Dados - Serviços

Data Infrastructure Insights

NetApp
October 16, 2025

Índice

Referência do Coletor de Dados - Serviços

Coleta de dados do nó

O Data Infrastructure Insights coleta métricas do nó no qual você instala um agente.

Instalação

1. Em **Observabilidade > Coletores**, escolha um sistema operacional/plataforma. Observe que a instalação de qualquer coletor de dados de integração (Kubernetes, Docker, Apache, etc.) também configurará a coleta de dados do nó.
2. Siga as instruções para configurar o agente. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados como métricas do nó:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Sistema de arquivos Node	Tipo de caminho do dispositivo UUID do nó	IP do nó Nome do nó Modo do sistema operacional do nó	Inodes livres Inodes livres Total de inodes usados Total usado Total usado
Disco de nó	Disco UUID do nó	IP do nó Nome do nó SO do nó	Tempo de E/S Total de IOPS em andamento Bytes de leitura (por segundo) Tempo de leitura Total de leituras (por segundo) Tempo de E/S ponderado Total de bytes de gravação (por segundo) Tempo de gravação Total de gravações (por segundo) Comprimento da fila de disco atual Tempo de gravação Tempo de leitura Tempo de E/S
CPU do nó	UUID da CPU do nó	IP do nó Nome do nó SO do nó	Uso da CPU do sistema Uso da CPU do usuário Uso da CPU ociosa Uso da CPU do processador Uso da CPU de interrupção Uso da CPU do DPC

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Nó	UUID do nó	IP do nó Nome do nó SO do nó	Tempo de inicialização do kernel Trocas de contexto do kernel (por segundo) Entropia do kernel disponível Interrupções do kernel (por segundo) Processos do kernel bifurcados (por segundo) Memória Memória ativa disponível Memória total disponível Memória em buffer Memória em cache Limite de confirmação Memória confirmada como memória Memória suja Memória livre Memória livre alta Memória livre alta Memória total Tamanho de página enorme Memória Páginas enormes Memória livre Páginas enormes Total de memória Memória baixa Memória livre baixa Memória total Memória mapeada Tabelas de páginas Memória Memória compartilhada Memória slab Troca Memória em cache Troca Memória livre Troca Memória total Memória total usada Memória total usada Memória Vmalloc Fragmento de memória Vmalloc Memória total usada por Vmalloc Writeback de memória total Writeback de memória Tmp Falhas de cache de memória Demanda de memória Falhas zero Falhas de página de memória Páginas de memória Memória não paginada Memória paginada Cache de memória principal Cache de espera Memória normal Cache de espera Memória de reserva Falhas de transição Processos Processos bloqueados Processos

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Rede de nós	UUID do nó da interface de rede	Nome do nó IP do nó SO do nó	Bytes recebidos Bytes enviados Pacotes enviados Pacotes descartados Erros de saída Pacotes recebidos Pacotes descartados Erros recebidos Pacotes recebidos Pacotes enviados

Configurar

Informações sobre configuração e solução de problemas podem ser encontradas no"Configurando um Agente" página.

Coletor de Dados ActiveMQ

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do ActiveMQ.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha ActiveMQ.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.

[Configuração do ActiveMQ]

Configurar

Informações podem ser encontradas em "Documentação do ActiveMQ"

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Fila ActiveMQ	Servidor de porta de fila de namespace	Nome do nó IP do nó UUID do nó	Contagem de consumidores Contagem de retirada da fila Contagem de enfileiramento Tamanho da fila
Assinante ActiveMQ	ID do cliente ID de conexão Porta Servidor Namespace	Nome do nó de destino ativo IP do nó UUID do nó Seletor de sistema operacional do nó Assinatura	Contagem de desenfileiramento Contagem despachada Tamanho da fila despachada Contagem de enfileiramento Tamanho da fila pendente
Tópico ActiveMQ	Espaço para nome do servidor de porta de tópico	Nome do nó IP do nó UUID do nó SO do nó	Contagem de consumidores Contagem de desenfileiramento Contagem de enfileiramento Tamanho

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de Dados Apache

Este coletor de dados permite a coleta de dados de servidores Apache em seu locatário.

Pré-requisitos

- Você deve ter seu servidor Apache HTTP configurado e funcionando corretamente
- Você deve ter permissões de sudo ou administrador no host/VM do seu agente
- Normalmente, o módulo *mod_status* do Apache é configurado para expor uma página no local '/server-status?auto' do servidor Apache. A opção *ExtendedStatus* deve ser habilitada para coletar todos os campos disponíveis. Para obter informações sobre como configurar seu servidor, consulte a documentação do módulo Apache: https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha Apache.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.

4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.

[Configuração do Apache]

Configurar

O plugin do Telegraf para o servidor HTTP do Apache depende do módulo 'mod_status' para ser habilitado. Quando isso estiver habilitado, o servidor HTTP do Apache exporá um ponto de extremidade HTML que pode ser visualizado no seu navegador ou extraído para extração do status de todas as configurações do servidor HTTP do Apache.

Compatibilidade:

A configuração foi desenvolvida no servidor HTTP versão 2.4.38 do Apache.

Habilitando mod_status:

Habilitar e expor os módulos 'mod_status' envolve duas etapas:

- Módulo de habilitação
- Expondo estatísticas do módulo

Módulo de habilitação:

O carregamento de módulos é controlado pelo arquivo de configuração em '/usr/local/apache/conf/httpd.conf'. Edite o arquivo de configuração e descomente as seguintes linhas:

```
LoadModule status_module modules/mod_status.so
Include conf/extra/httpd-info.conf
```

Expondo estatísticas do módulo:

A exposição de 'mod_status' é controlada pelo arquivo de configuração em '/usr/local/apache2/conf/extra/httpd-info.conf'. Certifique-se de ter o seguinte no arquivo de configuração (pelo menos, outras diretivas estarão lá):

```
# Allow server status reports generated by mod_status,
# with the URL of http://servername/server-status
<Location /server-status>
    SetHandler server-status
</Location>

#
# ExtendedStatus controls whether Apache will generate "full" status
# information (ExtendedStatus On) or just basic information
(ExtendedStatus
# Off) when the "server-status" handler is called. The default is Off.
#
ExtendedStatus On
```

Para obter instruções detalhadas sobre o módulo 'mod_status', consulte o"Documentação do Apache"

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Apache	Servidor de namespace	IP do nó Nome do nó Porta Configuração do servidor pai Geração Servidor pai Geração de MPM O tempo de atividade do servidor está parando	Trabalhadores Ocupados Bytes por Solicitação Bytes por Segundo Filhos da CPU Sistema Filhos da CPU Usuário Carga da CPU CPU Sistema Usuário Conexões Assíncronas Fechando Conexões Assíncronas Manter Ativo Conexões Assíncronas Escrevendo Conexões Duração Total por Solicitação Trabalhadores Ociosos Carga Média (últimos 1m) Carga Média (últimos 15m) Carga Média (últimos 5m) Processos Solicitações por Segundo Total de Acessos Duração Total Total de KBytes Placar Fechando Placar Pesquisas DNS Placar Finalizando Placar Limpeza Ociosa Placar Manter Ativo Placar Registro Placar Abrir Placar Lendo Placar Enviando Placar Iniciando Placar Aguardando

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de Dados do Cônsul

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Consul.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha Cônsul.

   Se você não configurou um Agente para coleta, você será solicitado a"instalar um agente" no seu inquilino.

   Se você já tiver um agente configurado, selecione o Sistema Operacional ou Plataforma apropriada e clique em **Continuar**.

2. Siga as instruções na tela Configuração do Cônsul para configurar o coletor de dados. As instruções

variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.

Configurar

Informações podem ser encontradas em"Documentação do Cônsul" .

Objetos e Contadores para cônsul

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Cônsul	Nó de serviço de verificação de ID de namespace	IP do nó SO do nó UUID do nó Nome do nó Nome do serviço Verificar nome ID do serviço Status	Aviso de ultrapassagem crítica

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de dados Couchbase

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Couchbase.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha Couchbase.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.

[Configuração do Couchbase]

Configurar

Informações podem ser encontradas em"Documentação do Couchbase" .

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Nó Couchbase	Nome do host do nó do cluster do namespace Couchbase	Nome do nó IP do nó	Memória Livre Total de Memória
Balde Couchbase	Cluster de bucket de namespace	Nome do nó IP do nó	Dados usados Buscas de dados Disco usado Contagem de itens Memória usada Operações por segundo Cota usada

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de dados CouchDB

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do CouchDB.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha CouchDB.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.

[Configuração do CouchDB]

Configurar

Informações podem ser encontradas em"Documentação do CouchDB" .

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
CouchDB	Servidor de namespace	Nome do nó IP do nó	Acertos do cache de autenticação Acertos do cache de autenticação Leituras do banco de dados Gravações do banco de dados Bancos de dados abertos Arquivos abertos do sistema operacional Tempo máximo de solicitação Tempo mínimo de solicitação Métodos de solicitação HTTP Copiar métodos de solicitação HTTP Excluir métodos de solicitação HTTP Obter métodos de solicitação HTTP Cabeçalho Métodos de solicitação HTTP Postar métodos de solicitação HTTP Colocar códigos de status 200 Códigos de status 201 Códigos de status 202 Códigos de status 301 Códigos de status 304 Códigos de status 400 Códigos de status 401 Códigos de status 403 Códigos de status 404 Códigos de status 405 Códigos de status 409 Códigos de status 412 Códigos de status 500

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de dados do Docker

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Docker.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha Docker.

   Se você não configurou um Agente para coleta, você será solicitado a"instalar um agente" no seu inquilino.

Se você já tiver um agente configurado, selecione o Sistema Operacional ou Plataforma apropriada e clique em **Continuar**.

2. Siga as instruções na tela Configuração do Docker para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.

[Configuração do Docker]

Configurar

O plugin de entrada Telegraf para Docker coleta métricas por meio de um soquete UNIX especificado ou de um ponto de extremidade TCP.

Compatibilidade

A configuração foi desenvolvida no Docker versão 1.12.6.

Configurando

Acessando o Docker por meio de um soquete UNIX

Se o agente Telegraf estiver em execução no baremetal, adicione o usuário Telegraf Unix ao grupo Docker Unix executando o seguinte:

```
 sudo usermod -aG docker telegraf
Se o agente Telegraf estiver sendo executado em um pod do Kubernetes,
exponha o soquete Docker Unix mapeando o soquete no pod como um volume e,
em seguida, montando esse volume em /var/run/docker.sock.  Por exemplo,
adicione o seguinte ao PodSpec:
```

```
volumes:
...
- name: docker-sock
hostPath:
path: /var/run/docker.sock
type: File
```

Em seguida, adicione o seguinte ao Container:

```
volumeMounts:
...
- name: docker-sock
mountPath: /var/run/docker.sock
```

Observe que o instalador do Data Infrastructure Insights fornecido para a plataforma Kubernetes cuida desse mapeamento automaticamente.

Acesse o Docker por meio de um ponto de extremidade TCP

Por padrão, o Docker usa a porta 2375 para acesso não criptografado e a porta 2376 para acesso criptografado.

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Motor Docker	Mecanismo Docker de namespace	Nome do nó IP do nó UUID do nó SO do nó Cluster Kubernetes Versão do Docker Unidade	Contêineres de memória Contêineres Contêineres em pausa Contêineres em execução CPUs paradas Rotinas Go Imagens Eventos de ouvinte usados Descritores de arquivo Dados disponíveis Dados totais de dados usados Metadados disponíveis Metadados totais de metadados usados Tamanho do bloco do pool

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Contêiner Docker	Nome do contêiner do namespace Docker Engine	Hash do contêiner do Kubernetes Portas do contêiner do Kubernetes Contagem de reinicialização do contêiner do Kubernetes Caminho da mensagem de término do contêiner do Kubernetes Política de mensagem de término do contêiner do Kubernetes Período de carência de término do pod do Kubernetes Imagem do contêiner Status do contêiner Versão do contêiner Nome do nó Caminho do log do contêiner do Kubernetes Nome do contêiner do Kubernetes Tipo de Docker do Kubernetes Nome do pod do Kubernetes Namespace do pod do Kubernetes UID do pod do Kubernetes ID do sandbox do Kubernetes IP do nó UUID do nó Versão do Docker Configuração de E/S do Kubernetes vista Origem da configuração de E/S do Kubernetes OpenShift IO SCC Descrição do Kubernetes Nome de exibição do OpenShift Tags do Kompose Service Pod Template Hash Controller Revisão Geração do modelo de pod do Hash Licença Data de construção do esquema Licença Nome do esquema URL do esquema URL do VCS do esquema Fornecedor do esquema Versão do esquema Esquema Mantenedor da versão do esquema Pod do cliente Kubernetes StatefulSet Nome do pod Tenant Arquitetura do console da Web URL de origem	Memória Ativa Memória Anônima Memória Ativa Arquivo Cache Memória Limite Hierárquico Memória Inativa Memória Anônima Arquivo Inativo Limite de Memória Arquivo Mapeado Uso Máximo de Memória Falha de Página de Memória Página de Memória Falha Grave Memória Paginada para Dentro Memória Paginada para Fora Tamanho do Conjunto Residente de Memória Tamanho do Conjunto Residente de Memória Memória Enorme Total de Memória Ativa Anônima Total de Memória de Arquivo Ativa Total de Memória Cache Total de Memória Anônima Inativa Total de Memória de Arquivo Inativo Total de Memória de Arquivo Mapeado Total de Memória de Falha de Página Total de Memória Falha Grave de Página Total Paginada para Dentro Memória Total de Memória Paginada para Fora Tamanho Total do Conjunto Residente de Memória Tamanho Total do Conjunto Residente de Memória Enorme Total de Memória Não Removível Uso de Memória Não Removível Porcentagem de Uso de Memória Código de Saída OOM Eliminado PID Iniciado em Sequência de Falhas

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Bloco de E/S do contêiner Docker	Namespace Nome do contêiner Dispositivo Docker Engine	Hash do contêiner do Kubernetes Portas do contêiner do Kubernetes Contagem de reinicialização do contêiner do Kubernetes Caminho da mensagem de término do contêiner do Kubernetes Política de mensagem de término do contêiner do Kubernetes Período de carência de término do pod do Kubernetes Imagem do contêiner Status do contêiner Versão do contêiner Nome do nó Caminho do log do contêiner do Kubernetes Nome do contêiner do Kubernetes Tipo de Docker do Kubernetes Nome do pod do Kubernetes Namespace do pod do Kubernetes UID do pod do Kubernetes ID do sandbox do Kubernetes IP do nó UUID do nó Versão do Docker Configuração do Kubernetes Vista Configuração do Kubernetes Origem OpenShift SCC Descrição do Kubernetes Nome de exibição do Kubernetes Tags do OpenShift Esquema Versão do esquema Hash do modelo do pod Revisão Hash do controlador Geração do modelo do pod do Kompose Serviço Data de compilação do esquema Licença do esquema Nome do esquema Fornecedor do esquema Pod do cliente Kubernetes StatefulSet Nome do pod Tenant Data de compilação do console da Web Licença Fornecedor Arquitetura URL da fonte autorizada Host de compilação do RH	Bytes de serviço de E/S Recursivo Assíncrono Bytes de serviço de E/S Recursivo Leitura Recursiva Bytes de serviço de E/S Recursivo Sincronização Recursiva Bytes de serviço de E/S Total de bytes de serviço de E/S Recursivo Gravação Recursiva E/S atendida Recursiva Assíncrona E/S atendida Recursiva Leitura Recursiva E/S atendida Recursiva Sincronização Recursiva E/S atendida Recursiva Total de E/S atendida Recursiva Gravação

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Rede de contêineres Docker	Namespace Nome do contêiner Rede Docker Engine	Imagem do contêiner Status do contêiner Versão do contêiner Nome do nó IP do nó UUID do nó SO do nó Cluster K8s Versão do Docker ID do contêiner	RX Bytes RX Perdidos Erros RX Pacotes RX TX Bytes TX Perdidos Erros TX Pacotes TX

Objeto:	Identificadores:	Atributos:	Pontos de dados:
CPU de contêiner Docker	Nome do contêiner do namespace CPU Docker Engine	Hash do contêiner do Kubernetes Portas do contêiner do Kubernetes Contagem de reinicialização do contêiner do Kubernetes Caminho da mensagem de término do contêiner do Kubernetes Política de mensagem de término do contêiner do Kubernetes Período de carência de término do pod do Kubernetes Configuração do Kubernetes vista Origem da configuração do Kubernetes OpenShift Imagem do contêiner SCC Status do contêiner Versão do contêiner Nome do nó Caminho do log do contêiner do Kubernetes Nome do contêiner do Kubernetes Tipo de Docker do Kubernetes Nome do pod do Kubernetes Namespace do pod do Kubernetes UID do pod do Kubernetes ID do sandbox do Kubernetes IP do nó UUID do nó SO do nó Cluster do Kubernetes Versão do Docker Descrição do Kubernetes Nome de exibição do Kubernetes Tags do OpenShift Versão do esquema Hash do modelo do pod Revisão do controlador Hash Geração do modelo do pod do serviço Kompose Data de compilação do esquema Licença do esquema Nome do esquema Fornecedor do esquema Pod do cliente do Kubernetes StatefulSet Nome do pod do Tenant Data de compilação do console da Web Licença Fornecedor Arquitetura URL de origem autorizada Host de compilação do	Períodos de limitação Períodos de limitação Tempo de limitação Uso no modo kernel Uso no modo usuário Porcentagem de uso Uso do sistema Total

Solução de problemas

Problema:	Experimente isto:
Não vejo minhas métricas do Docker no Data Infrastructure Insights depois de seguir as instruções na página de configuração.	Verifique os logs do agente Telegraf para ver se ele relata o seguinte erro: E! Erro no plugin [inputs.docker]: Permissão negada ao tentar conectar ao soquete do daemon do Docker. Se isso acontecer, tome as medidas necessárias para fornecer ao agente Telegraf acesso ao soquete Docker Unix, conforme especificado acima.

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de dados Elasticsearch

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Elasticsearch.

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha Elasticsearch.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.

[Configuração do Elasticsearch]

Configurar

Informações podem ser encontradas em"Documentação do Elasticsearch" .

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:
Cluster do Elasticsearch	Cluster de namespace	IP do nó Nome do nó Status do cluster
Nó Elasticsearch	Cluster de namespace ID do nó ES IP do nó ES	ID da zona

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de Dados Flink

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Flink.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha Flink.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.

[Configuração do Flink]

Configurar

Uma implantação completa do Flink envolve os seguintes componentes:

JobManager: O sistema primário do Flink. Coordena uma série de TaskManagers. Em uma configuração de alta disponibilidade, o sistema terá mais de um JobManager. Gerenciador de Tarefas: É aqui que os operadores do Flink são executados. O plugin Flink é baseado no plugin Jolokia do Telegraf. Como requisito para coletar informações de todos os componentes do Flink, o JMX precisa ser configurado e exposto via Jolokia em todos os componentes.

Compatibilidade

A configuração foi desenvolvida no Flink versão 1.7.0.

Configurando

Agente Jolokia Jar

Para todos os componentes individuais, uma versão do arquivo jar do agente Jolokia deve ser baixada. A versão testada foi"Agente Jolokia 1.6.0" .

As instruções abaixo pressupõem que o arquivo jar baixado (jolokia-jvm-1.6.0-agent.jar) esteja localizado no local '/opt/flink/lib/'.

Gerenciador de Tarefas

Para configurar o JobManager para expor a API do Jolokia, você pode configurar a seguinte variável de ambiente em seus nós e reiniciar o JobManager:

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
Você pode escolher um porto diferente para Jolokia (8778).  Se você tiver
um IP interno para bloquear o Jolokia, você pode substituir o "catch all"
0.0.0.0 pelo seu próprio IP.  Observe que este IP precisa ser acessível
pelo plugin Telegraf.
```

Gerenciador de Tarefas

Para configurar o(s) TaskManager(s) para expor a API Jolokia, você pode configurar a seguinte variável de ambiente em seus nós e reiniciar o TaskManager:

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
Você pode escolher um porto diferente para Jolokia (8778).  Se você tiver
um IP interno para bloquear o Jolokia, você pode substituir o "catch all"
0.0.0.0 pelo seu próprio IP.  Observe que este IP precisa ser acessível
pelo plugin Telegraf.
```

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Gerenciador de Tarefas Flink	Servidor de namespace de cluster	Nome do nó ID do gerenciador de tarefas IP do nó	Segmentos de memória disponíveis na rede Segmentos totais de memória da rede Contagem de MarkSweep do PS de coleta de lixo Tempo de MarkSweep do PS de coleta de lixo Contagem de limpeza do PS de coleta de lixo Tempo de limpeza do PS de coleta de lixo Memória heap confirmada Inicialização da memória heap Memória heap Máxima de memória heap usada Contagem de threads Contagem de threads do daemon Contagem de pico de threads Contagem total de threads iniciada
Trabalho Flink	ID da tarefa do servidor de namespace do cluster	Nome do nó Nome do trabalho IP do nó Último ponto de verificação Caminho externo Hora de reinicialização	Tempo de inatividade Reinicializações completas Último alinhamento de ponto de verificação Buffered Duração do último ponto de verificação Tamanho do último ponto de verificação Número de pontos de verificação concluídos Número de pontos de verificação com falha Número de pontos de verificação em andamento Número de pontos de verificação Tempo de atividade

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Gerenciador de Tarefas Flink	Servidor de namespace de cluster	Nome do nó IP do nó	Contagem de MarkSweep do PS de coleta de lixo Tempo de MarkSweep do PS de coleta de lixo Contagem de coleta de lixo do PS de coleta de lixo Tempo de coleta de lixo do PS de coleta de lixo Memória heap comprometida Inicialização da memória heap Memória heap máxima usada Número de gerenciadores de tarefas registrados Número de trabalhos em execução Slots de tarefa disponíveis Contagem total de threads Contagem de threads do daemon Contagem de pico de threads Contagem total de threads iniciada

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Tarefa Flink	ID da tarefa do namespace do cluster ID da tarefa	Nome do nó do servidor Nome do trabalho Índice de subtarefas ID da tentativa da tarefa Número da tentativa da tarefa Nome da tarefa ID do gerenciador de tarefas IP do nó Entrada atual Marca d'água	Buffers no uso do pool Buffers no comprimento da fila Buffers fora do uso do pool Buffers fora do comprimento da fila Número de buffers no local Número de buffers no local Contagem por segundo Número de buffers na taxa local por segundo Número de buffers no remoto Número de buffers no remoto Contagem por segundo Número de buffers no remoto Taxa por segundo Número de buffers fora Número de buffers fora por segundo Contagem Número de buffers fora por segundo Taxa de segundo Número de bytes no local Número de bytes no local Contagem por segundo Número de bytes no local Contagem por segundo Número de bytes no remoto Contagem por segundo Número de bytes no remoto Taxa por segundo Número de bytes fora Número de bytes fora por segundo Contagem Número de bytes fora por segundo Taxa Número de registros em Número de registros em Contagem por segundo Número de registros em Taxa por segundo Número de registros fora por segundo Contagem Número de registros fora por segundo Taxa

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Operador de Tarefas Flink	ID do trabalho do namespace do cluster ID do operador ID da tarefa	Nome do nó do servidor Nome do trabalho Nome do operador Índice de subtarefas ID da tentativa da tarefa Número da tentativa da tarefa Nome da tarefa ID do gerenciador de tarefas IP do nó	Marca d'água de entrada atual Marca d'água de saída atual Número de registros em Número de registros em por segundo Contagem Número de registros em por segundo Taxa Número de registros fora Número de registros fora por segundo Contagem Número de registros fora por segundo Taxa Número de registros atrasados descartados Partições atribuídas Bytes consumidos Taxa de confirmação Latência média de confirmação Latência máxima de confirmação Taxa de confirmação Commits com falha Commits bem-sucedidos Taxa de fechamento de conexão Contagem de conexão Taxa de criação de conexão Contagem Latência de busca Média Latência de busca Máxima Taxa de busca Tamanho médio Tamanho máximo de busca Tempo de aceleração de busca Tempo médio de aceleração de busca Máximo Taxa de pulsação Taxa de bytes de entrada Taxa de E/S Tempo de E/S Média (ns) Taxa de espera de E/S Tempo de espera de E/S Média (ns) Taxa de junção Tempo de junção Média Última pulsação atrás Taxa de E/S de rede Taxa de bytes de saída Registros consumidos Taxa de atraso de registros Máximo de registros por solicitação Média Taxa de solicitação Tamanho médio da solicitação Máximo Taxa de resposta Taxa de seleção Taxa de sincronização Tempo de

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de Dados Hadoop

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Hadoop.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha Hadoop.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.

[Configuração do Hadoop] [Configuração do Hadoop]

Configurar

Uma implantação completa do Hadoop envolve os seguintes componentes:

- NameNode: O sistema primário do Hadoop Distributed File System (HDFS). Coordena uma série de DataNodes.
- NameNode secundário: um failover quente para o NameNode principal. No Hadoop, a promoção para NameNode não ocorre automaticamente. O NameNode secundário coleta informações do NameNode para estar pronto para ser promovido quando necessário.
- DataNode: proprietário real dos dados.
- ResourceManager: O sistema primário de computação (Yarn). Coordena uma série de NodeManagers.
- NodeManager: O recurso para computação. Localização real para execução de aplicativos.
- JobHistoryServer: Responsável por atender a todas as solicitações relacionadas ao histórico de empregos.

O plugin Hadoop é baseado no plugin Jolokia do Telegraf. Como requisito para coletar informações de todos os componentes do Hadoop, o JMX precisa ser configurado e exposto via Jolokia em todos os componentes.

Compatibilidade

A configuração foi desenvolvida no Hadoop versão 2.9.2.

Configurando

Agente Jolokia Jar

Para todos os componentes individuais, uma versão do arquivo jar do agente Jolokia deve ser baixada. A versão testada foi"Agente Jolokia 1.6.0" .

As instruções abaixo pressupõem que o arquivo jar baixado (jolokia-jvm-1.6.0-agent.jar) esteja localizado no local '/opt/hadoop/lib/'.

NomeNode

Para configurar o NameNode para expor a API Jolokia, você pode configurar o seguinte em <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_NAMENODE_OPTS="$HADOOP_NAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7800,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8000
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8000 above) and Jolokia (7800).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Nome secundárioNode

Para configurar o Secondary NameNode para expor a API Jolokia, você pode configurar o seguinte em <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_SECONDARYNAMENODE_OPTS="$HADOOP_SECONDARYNAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7802,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8002
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8002 above) and Jolokia (7802).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Nó de dados

Para configurar os DataNodes para expor a API Jolokia, você pode configurar o seguinte em <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_DATANODE_OPTS="$HADOOP_DATANODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7801,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8001
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8001 above) and Jolokia (7801).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Gerenciador de Recursos

Para configurar o ResourceManager para expor a API Jolokia, você pode configurar o seguinte em <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export YARN_RESOURCEMANAGER_OPTS="$YARN_RESOURCEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7803,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8003
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8003 above) and Jolokia (7803).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Gerenciador de nós

Para configurar os NodeManagers para expor a API Jolokia, você pode configurar o seguinte em <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export YARN_NODEMANAGER_OPTS="$YARN_NODEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7804,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8004
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8004 above) and Jolokia (7804).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Servidor de histórico de empregos

Para configurar o JobHistoryServer para expor a API Jolokia, você pode configurar o seguinte em <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_JOB_HISTORYSERVER_OPTS="$HADOOP_JOB_HISTORYSERVER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7805,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8005
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8005 above) and Jolokia (7805).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:
Nome secundário do nó do Hadoop	Servidor de namespace de cluster	Nome do nó IP do nó Informações de compilação Versão
Gerenciador de Nós do Hadoop	Servidor de namespace de cluster	Nome do nó IP do nó
Gerenciador de Recursos do Hadoop	Servidor de namespace de cluster	Nome do nó IP do nó
Nó de dados do Hadoop	Servidor de namespace de cluster	Nome do nó IP do nó ID do cluster Versão

Objeto:	Identificadores:	Atributos:
Nome do nó do Hadoop	Servidor de namespace de cluster	Nome do nó IP do nó ID da transação Última gravação Hora desde as últimas edições carregadas Estado do HA Estado do sistema de arquivos ID do pool de blocos ID do cluster Informações de compilação Contagem de versão distinta Versão
Servidor de histórico de tarefas do Hadoop	Servidor de namespace de cluster	Nome do nó IP do nó

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de dados HAProxy

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do HAProxy.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha HAProxy.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.

[Configuração do HAProxy]

Configurar

O plugin do Telegraf para HAProxy depende da ativação do HAProxy Stats. Esta é uma configuração incorporada ao HAProxy, mas não vem habilitada de fábrica. Quando ativado, o HAProxy exporá um ponto de extremidade HTML que pode ser visualizado no seu navegador ou extraído para extração do status de todas as configurações do HAProxy.

Compatibilidade:

A configuração foi desenvolvida na versão 1.9.4 do HAProxy.

Configuração:

Para habilitar estatísticas, edite seu arquivo de configuração do haproxy e adicione as seguintes linhas após a seção 'defaults', usando seu próprio usuário/senha e/ou URL do haproxy:

```
stats enable
stats auth myuser:mypassword
stats uri  /haproxy?stats
```

A seguir está um exemplo simplificado de arquivo de configuração com estatísticas habilitadas:

```
global
  daemon
  maxconn 256

defaults
  mode http
  stats enable
  stats uri /haproxy?stats
  stats auth myuser:mypassword
  timeout connect 5000ms
  timeout client 50000ms
  timeout server 50000ms

frontend http-in
  bind *:80
  default_backend servers

frontend http-in9080
  bind *:9080
  default_backend servers_2

backend servers
  server server1 10.128.0.55:8080 check ssl verify none
  server server2 10.128.0.56:8080 check ssl verify none

backend servers_2
  server server3 10.128.0.57:8080 check ssl verify none
  server server4 10.128.0.58:8080 check ssl verify none
```

Para obter instruções completas e atualizadas, consulte o"Documentação do HAProxy" .

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Interface HAProxy	Proxy de endereço de namespace	IP do nó Nome do nó ID do proxy Modo ID do processo Limite de taxa de sessões ID do servidor Limite de sessões Status	Bytes de entrada Bytes de saída Acertos no cache Pesquisas no cache Compressão Bytes ignorados Compressão Bytes de entrada Compressão Bytes de saída Compressão Respostas Taxa de conexão Taxa de conexão Máximo de conexões Total de solicitações negadas pela regra de conexão Solicitações negadas por problemas de segurança Respostas negadas por problemas de segurança Solicitações negadas pela regra de sessão Erros de solicitações Respostas 1xx Respostas 2xx Respostas 3xx Respostas 4xx Respostas 5xx Respostas Outras solicitações Taxa de sessões interceptadas Taxa de sessões Taxa de solicitações Máximo de solicitações Taxa de solicitações Máximo de solicitações Total de sessões Sessões Máximo de sessões Total de solicitações Reescritas

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Servidor HAProxy	Servidor proxy de endereço de namespace	IP do nó Nome do nó Verificar tempo para terminar Verificar configuração de queda Verificar valor de integridade Verificar configuração de ascensão Verificar status ID do proxy Última hora de alteração Última hora da sessão Modo ID do processo ID do servidor Status Peso	Servidores ativos Servidores de backup Bytes de entrada Bytes de saída Verificações de baixa Verificações Falhas de cliente Aborta conexões Tempo médio de conexão Tempo de inatividade Total de respostas negadas Erros de conexão Erros de resposta Respostas 1xx Respostas 2xx Respostas 3xx Respostas 4xx Respostas 5xx Respostas Outro servidor selecionado Fila total Fila atual Tempo médio máximo da fila Sessões por segundo Sessões por segundo Tempo máximo de resposta de reutilização de conexão Média de sessões Sessões Máximas de transferências do servidor Aborta sessões Total de sessões Tempo total Média de solicitações Reenvios Solicitações Tentativas Solicitações Reescritas

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Backend HAProxy	Proxy de endereço de namespace	IP do nó Nome do nó ID do proxy Última hora de alteração Última hora da sessão Modo ID do processo ID do servidor Limite de sessões Status Peso	Servidores ativos Servidores de backup Bytes de entrada Bytes de saída Acertos no cache Pesquisas no cache Verificações de baixa do cliente Abortos de compactação Bytes ignorados Bytes de compactação em compressão Bytes de saída Respostas de compactação Conexões Tempo médio de inatividade Total de solicitações negadas por problemas de segurança Respostas negadas por problemas de segurança Erros de conexão Erros de resposta Respostas 1xx Respostas 2xx Respostas 3xx Respostas 4xx Respostas 5xx Respostas Outro servidor selecionado Fila total Fila atual Tempo médio máximo da fila Sessões por segundo Sessões por segundo Máximo de solicitações Tempo total de resposta de reutilização de conexão Média de sessões Sessões Máximo de abortos de transferência do servidor Sessões Total de sessões Tempo total de solicitações Média de solicitações Reenvios Solicitações Tentativas Solicitações Reescritas

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de dados de JVM

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas da JVM.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha JVM.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.

[Configuração JVM]

Configurar

Informações podem ser encontradas em"Documentação do JVM" .

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
JVM	Espaço para nome JVM	Arquitetura do SO Nome do SO Versão do SO Especificação de tempo de execução Especificação de tempo de execução Fornecedor Especificação de tempo de execução Versão Tempo de atividade Nome da VM de tempo de execução Fornecedor da VM de tempo de execução Versão da VM de tempo de execução Nome do nó IP do nó	Classe carregada Classe carregada Total de classe descarregada Heap de memória comprometido Heap de memória inicial Heap de memória usado Máximo de memória Heap usado Memória não comprometida Memória não iniciada Não heap Memória máxima Não heap usada Objetos de memória Finalização pendente Processadores do SO disponíveis Tamanho da memória virtual comprometida do SO Tamanho da memória física livre do SO Tamanho do espaço de swap livre do SO Contagem máxima de descritores de arquivo do SO Contagem de descritores de arquivo abertos do SO Carga da CPU do processador do SO Tempo de CPU do processador do SO Carga da CPU do sistema SO Carga média do sistema SO Tamanho total da memória física do SO Tamanho total do espaço de swap do SO Contagem do daemon do thread Contagem de pico do thread Contagem de threads Contagem total de threads iniciadas Contagem da coleta de cópias do coletor de lixo Tempo de coleta de cópias do coletor de lixo Contagem da coleta de marcação e varredura do coletor de lixo Tempo de coleta de marcação e varredura do coletor de lixo Contagem da coleta de geração antiga do coletor de lixo G1 Tempo de coleta da geração antiga do coletor de lixo G1 Contagem da coleta

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de Dados Kafka

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Kafka.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha Kafka.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.

[Configuração do Kafka]

Configurar

O plugin Kafka é baseado no plugin Jolokia do Telegraf. Como requisito para coletar informações de todos os corretores do Kafka, o JMX precisa ser configurado e exposto via Jolokia em todos os componentes.

Compatibilidade

A configuração foi desenvolvida no Kafka versão 0.11.0.2.

Configurando

Todas as instruções abaixo pressupõem que o local de instalação do kafka seja '/opt/kafka'. Você pode adaptar as instruções abaixo para refletir seu local de instalação.

Agente Jolokia Jar

Uma versão do arquivo jar do agente Jolokia deve ser"baixado" . A versão testada foi o agente Jolokia 1.6.0.

As instruções abaixo pressupõem que o arquivo jar baixado (jolokia-jvm-1.6.0-agent.jar) esteja no local '/opt/kafka/libs/'.

Corretores Kafka

Para configurar o Kafka Brokers para expor a API Jolokia, você pode adicionar o seguinte em <KAFKA_HOME>/bin/kafka-server-start.sh, logo antes da chamada 'kafka-run-class.sh':

```
export JMX_PORT=9999
export RMI_HOSTNAME=`hostname -I`
export KAFKA_JMX_OPTS="-javaagent:/opt/kafka/libs/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0
-Dcom.sun.management.jmxremote.password.file=/opt/kafka/config/jmxremote.p
assword -Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname=$RMI_HOSTNAME
-Dcom.sun.management.jmxremote.rmi.port=$JMX_PORT"
```

Observe que o exemplo acima está usando 'hostname -I' para configurar a variável de ambiente 'RMI_HOSTNAME'. Em máquinas com vários IPs, isso precisará ser ajustado para coletar o IP desejado para conexões RMI.

Você pode escolher uma porta diferente para JMX (9999 acima) e Jolokia (8778). Se você tiver um IP interno para bloquear o Jolokia, você pode substituir o "catch all" 0.0.0.0 pelo seu próprio IP. Observe que este IP precisa ser acessível pelo plugin Telegraf. Você pode usar a opção '-Dcom.sun.management.jmxremote.authenticate=false' se não quiser autenticar. Use por sua conta e risco.

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:
Corretor Kafka	Agente de namespace de cluster	Nome do nó IP do nó

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de Dados Kibana

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Kibana.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha Kibana.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.

4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.

[Configuração do Kibana]

Configurar

Informações podem ser encontradas em"Documentação do Kibana" .

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Kibana	Endereço do namespace	IP do nó Nome do nó Versão Status	Conexões simultâneas Heap Heap máximo usado Solicitações por segundo Tempo de resposta Tempo médio de resposta Tempo máximo de atividade

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

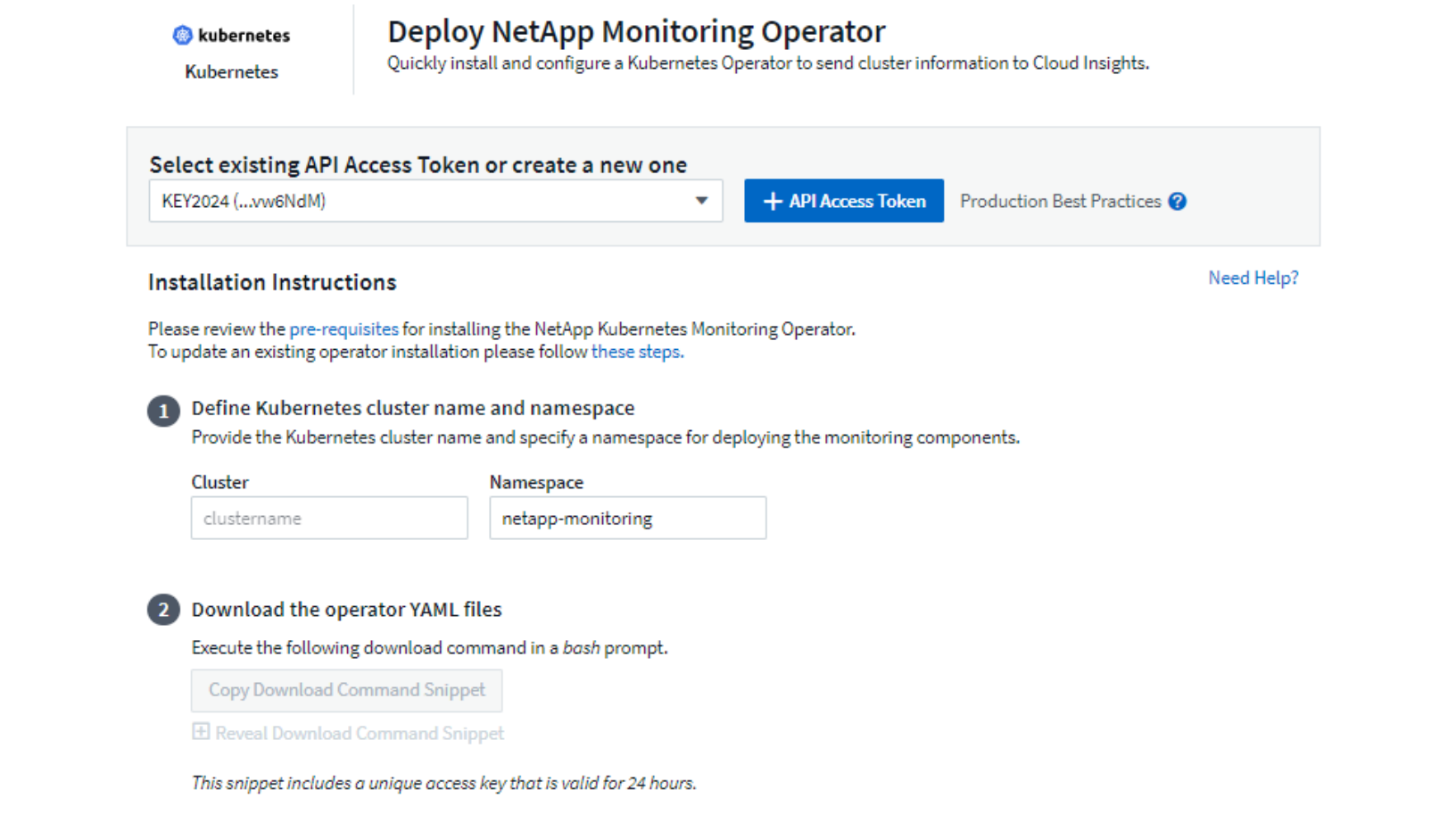
Instalação e configuração do operador de monitoramento do Kubernetes

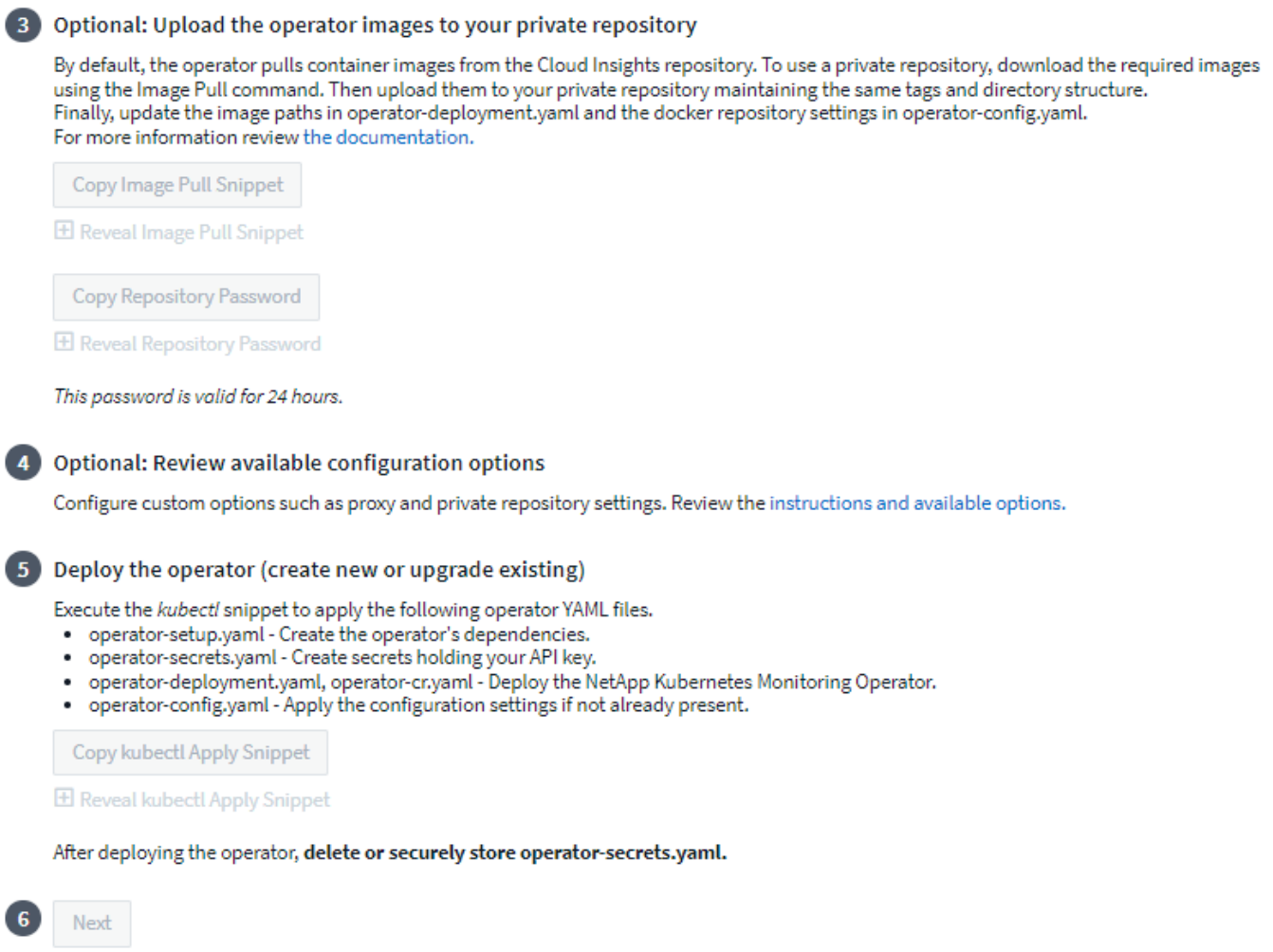
O Data Infrastructure Insights oferece o **Kubernetes Monitoring Operator** para a coleção Kubernetes. Navegue até **Kubernetes > Coletores > +Kubernetes Collector** para implantar um novo operador.

Antes de instalar o Kubernetes Monitoring Operator

Veja o"Pré-requisitos" documentação antes de instalar ou atualizar o Kubernetes Monitoring Operator.

Instalando o Operador de Monitoramento do Kubernetes


kubernetes
Kubernetes
Deploy NetApp Monitoring Operator
Quickly install and configure a Kubernetes Operator to send cluster information to Cloud Insights.
Select existing API Access Token or create a new one
KEY2024 (...vw6NdM)
+ API Access Token
Production Best Practices
Installation Instructions
Need Help?
Please review the pre-requisites for installing the NetApp Kubernetes Monitoring Operator.
To update an existing operator installation please follow these steps.
1 Define Kubernetes cluster name and namespace
Provide the Kubernetes cluster name and specify a namespace for deploying the monitoring components.
Cluster
clustername
Namespace
netapp-monitoring
2 Download the operator YAML files
Execute the following download command in a bash prompt.
Copy Download Command Snippet
Reveal Download Command Snippet
This snippet includes a unique access key that is valid for 24 hours.



Etapas para instalar o agente do Operador de Monitoramento do Kubernetes no Kubernetes:

1. Insira um nome de cluster e um namespace exclusivos. Se você éatualizando de um operador Kubernetes anterior, use o mesmo nome de cluster e namespace.
2. Depois de inseri-los, você pode copiar o trecho do Comando de Download para a área de transferência.
3. Cole o snippet em uma janela *bash* e execute-o. Os arquivos de instalação do Operador serão baixados. Observe que o snippet tem uma chave única e é válido por 24 horas.
4. Se você tiver um repositório personalizado ou privado, copie o snippet opcional Image Pull, cole-o em um shell *bash* e execute-o. Depois que as imagens forem extraídas, copie-as para seu repositório privado. Certifique-se de manter as mesmas tags e estrutura de pastas. Atualize os caminhos em *operator-deployment.yaml*, bem como as configurações do repositório do Docker em *operator-config.yaml*.
5. Se desejar, revise as opções de configuração disponíveis, como configurações de proxy ou repositório privado. Você pode ler mais sobre"opções de configuração" .
6. Quando estiver pronto, implante o Operador copiando o snippet kubectl Apply, baixando-o e executando-o.
7. A instalação prossegue automaticamente. Quando estiver concluído, clique no botão *Avançar*.
8. Quando a instalação estiver concluída, clique no botão *Avançar*. Certifique-se também de excluir ou armazenar com segurança o arquivo *operator-secrets.yaml*.

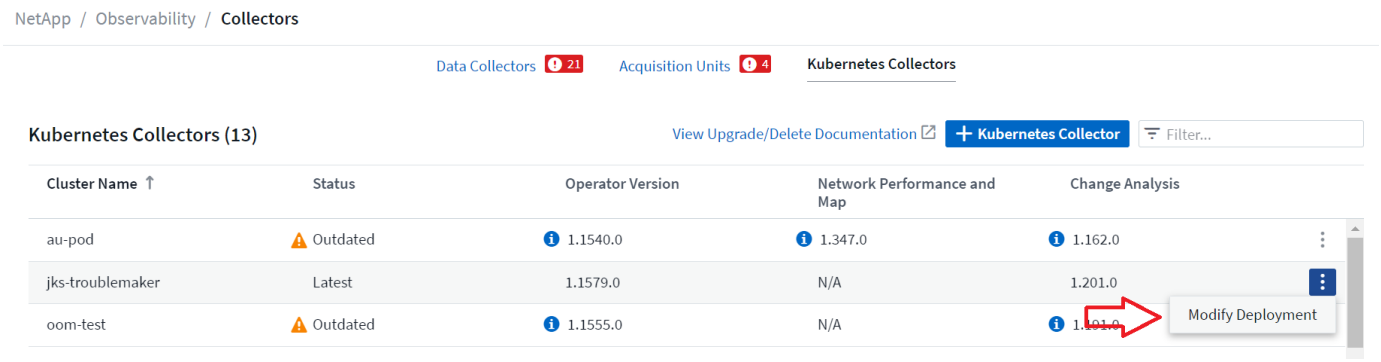
Se você tiver um repositório personalizado, leia sobreusando um repositório docker personalizado/privado .

Componentes de monitoramento do Kubernetes

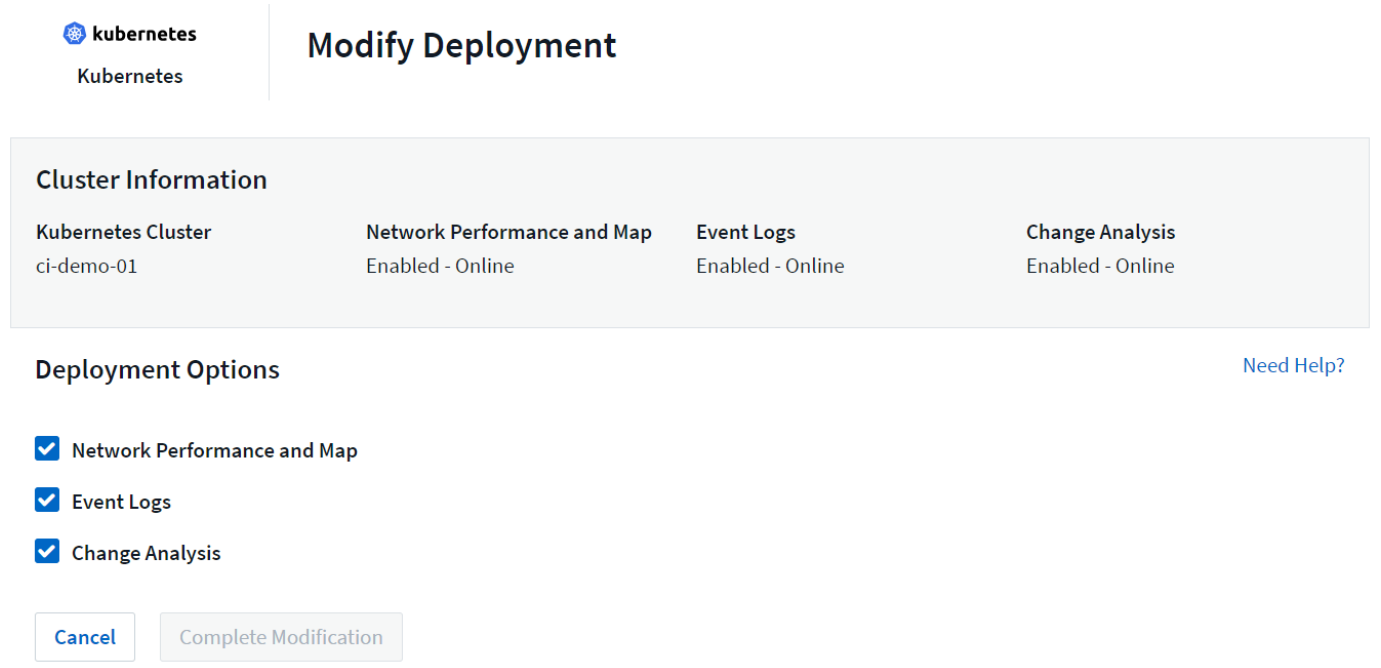
O Data Infrastructure Insights Kubernetes Monitoring é composto por quatro componentes de monitoramento:

- Métricas de Cluster
- Desempenho e mapa de rede (opcional)
- Registros de eventos (opcional)
- Análise de Mudanças (opcional)

Os componentes opcionais acima são habilitados por padrão para cada coletor do Kubernetes; se você decidir que não precisa de um componente para um coletor específico, poderá desabilitá-lo navegando até **Kubernetes > Coletores** e selecionando *Modificar implantação* no menu de "três pontos" do coletor, à direita da tela.



A tela mostra o estado atual de cada componente e permite que você desabilite ou habilite componentes para aquele coletor, conforme necessário.



Atualizando para o mais recente Kubernetes Monitoring Operator

Atualizações de botão DII

Você pode atualizar o Kubernetes Monitoring Operator por meio da página DII Kubernetes Collectors. Clique no menu ao lado do cluster que você gostaria de atualizar e selecione *Atualizar*. O operador verificará as assinaturas de imagem, fará um snapshot da sua instalação atual e realizará a atualização. Em poucos minutos, você verá o progresso do status do operador, passando de Atualização em andamento para a mais recente. Se você encontrar um erro, pode selecionar o status Erro para obter mais detalhes e consultar a tabela de solução de problemas de atualizações por botão abaixo.

Atualizações por botão com repositórios privados

Se o seu operador estiver configurado para usar um repositório privado, certifique-se de que todas as imagens necessárias para executar o operador e suas assinaturas estejam disponíveis no seu repositório. Se você encontrar um erro durante o processo de atualização de imagens ausentes, basta adicioná-las ao seu repositório e tentar atualizar novamente. Para carregar as assinaturas de imagem no seu repositório, use a ferramenta cosign da seguinte forma, certificando-se de carregar as assinaturas de todas as imagens especificadas em 3 Opcional: Carregue as imagens do operador no seu repositório privado > Image Pull Snippet

```
cosign copy example.com/src:v1 example.com/dest:v1
#Example
cosign copy <DII container registry>/netapp-monitoring:<image version>
<private repository>/netapp-monitoring:<image version>
```

Revertendo para uma versão anterior

Se você atualizou usando o recurso de atualizações por botão e encontrar alguma dificuldade com a versão atual do operador dentro de sete dias após a atualização, você pode fazer o downgrade para a versão anterior usando o snapshot criado durante o processo de atualização. Clique no menu ao lado do cluster que você gostaria de reverter e selecione *Reverter*.

Atualizações manuais

Determine se existe um AgentConfiguration com o Operador existente (se o seu namespace não for o *netapp-monitoring* padrão, substitua pelo namespace apropriado):

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
Se existir uma AgentConfiguration:
```

- Instalaro operador mais recente sobre o operador existente.
  - Certifique-se de que você estápuxando as últimas imagens de contêiner se você estiver usando um repositório personalizado.

Se o AgentConfiguration não existir:

- Anote o nome do seu cluster conforme reconhecido pelo Data Infrastructure Insights (se o seu namespace não for o netapp-monitoring padrão, substitua pelo namespace apropriado):

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Crie um backup do Operador existente (se o seu namespace não for o
netapp-monitoring padrão, substitua pelo namespace apropriado):
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-operator,Desinstalar>>o Operador
existente.
* <<installing-the-kubernetes-monitoring-operator,Instalar>>o mais
recente Operador.
```

- Use o mesmo nome de cluster.
- Depois de baixar os arquivos YAML mais recentes do Operator, transfira todas as personalizações encontradas em agent_backup.yaml para o operator-config.yaml baixado antes de implantar.
- Certifique-se de que você estápuxando as últimas imagens de contêiner se você estiver usando um repositório personalizado.

Parando e iniciando o operador de monitoramento do Kubernetes

Para interromper o Operador de Monitoramento do Kubernetes:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
Para iniciar o Operador de Monitoramento do Kubernetes:
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Desinstalando

Para remover o Operador de Monitoramento do Kubernetes

Observe que o namespace padrão para o Kubernetes Monitoring Operator é "netapp-monitoring". Se você tiver definido seu próprio namespace, substitua-o nestes e em todos os comandos e arquivos subsequentes.

Versões mais recentes do operador de monitoramento podem ser desinstaladas com os seguintes comandos:

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

Se o operador de monitoramento foi implantado em seu próprio namespace dedicado, exclua o namespace:

```
 kubectl delete ns <NAMESPACE>
Observação: se o primeiro comando retornar "Nenhum recurso encontrado",
use as instruções a seguir para desinstalar versões mais antigas do
operador de monitoramento.
```

Execute cada um dos seguintes comandos em ordem. Dependendo da sua instalação atual, alguns desses comandos podem retornar mensagens de "objeto não encontrado". Essas mensagens podem ser ignoradas com segurança.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

Se uma Restrição de Contexto de Segurança foi criada anteriormente:

```
kubectl delete scc telegraf-hostaccess
```

Sobre Kube-state-metrics

O NetApp Kubernetes Monitoring Operator instala suas próprias métricas de estado do kube para evitar conflitos com outras instâncias.

Para obter informações sobre Kube-State-Metrics, consulte"esta página" .

Configurando/Personalizando o Operador

Estas seções contêm informações sobre como personalizar a configuração do seu operador, trabalhar com proxy, usar um repositório Docker personalizado ou privado ou trabalhar com o OpenShift.

Opções de configuração

As configurações mais comumente modificadas podem ser configuradas no recurso personalizado *AgentConfiguration*. Você pode editar este recurso antes de implantar o operador editando o arquivo *operator-config.yaml*. Este arquivo inclui exemplos comentados de configurações. Veja a lista de"configurações disponíveis" para a versão mais recente do operador.

Você também pode editar esse recurso depois que o operador for implantado usando o seguinte comando:

```
 kubectl -n netapp-monitoring edit AgentConfiguration
Para determinar se a versão implantada do operador oferece suporte ao
AgentConfiguration, execute o seguinte comando:
```

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Se você vir uma mensagem “Erro do servidor (Não encontrado)”, seu operador
deverá ser atualizado antes que você possa usar o AgentConfiguration.
```

Configurando o suporte a proxy

Há dois lugares onde você pode usar um proxy no seu locatário para instalar o Kubernetes Monitoring Operator. Esses podem ser os mesmos sistemas proxy ou sistemas separados:

- Proxy necessário durante a execução do snippet de código de instalação (usando "curl") para conectar o sistema onde o snippet é executado ao seu ambiente do Data Infrastructure Insights
- Proxy necessário para o cluster Kubernetes de destino se comunicar com seu ambiente do Data Infrastructure Insights

Se você usar um proxy para um ou ambos, para instalar o Kubernetes Operating Monitor, primeiro você deve garantir que seu proxy esteja configurado para permitir uma boa comunicação com seu ambiente do Data Infrastructure Insights . Se você tiver um proxy e puder acessar o Data Infrastructure Insights do servidor/VM do qual deseja instalar o Operator, é provável que seu proxy esteja configurado corretamente.

Para o proxy usado para instalar o Kubernetes Operating Monitor, antes de instalar o Operator, defina as variáveis de ambiente *http_proxy/https_proxy*. Para alguns ambientes de proxy, talvez você também precise definir a variável de ambiente *no_proxy*.

Para definir a(s) variável(is), execute as seguintes etapas no seu sistema **antes** de instalar o Kubernetes Monitoring Operator:

1. Defina as variáveis de ambiente *https_proxy* e/ou *http_proxy* para o usuário atual:
   a. Se o proxy que está sendo configurado não tiver autenticação (nome de usuário/senha), execute o seguinte comando:

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Se o proxy que está sendo configurado tiver autenticação (nome de
usuário/senha), execute este comando:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Para que o proxy usado no seu cluster Kubernetes se comunique com seu ambiente do Data Infrastructure Insights , instale o Kubernetes Monitoring Operator depois de ler todas estas instruções.

Configure a seção proxy do AgentConfiguration em operator-config.yaml antes de implantar o Kubernetes Monitoring Operator.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Usando um repositório docker personalizado ou privado

Por padrão, o Kubernetes Monitoring Operator extrairá imagens de contêiner do repositório do Data Infrastructure Insights . Se você tiver um cluster Kubernetes usado como destino para monitoramento e esse cluster estiver configurado para extrair apenas imagens de contêiner de um repositório Docker personalizado ou privado ou de um registro de contêiner, você deverá configurar o acesso aos contêineres necessários para o Kubernetes Monitoring Operator.

Execute o “Image Pull Snippet” do bloco de instalação do NetApp Monitoring Operator. Este comando fará login no repositório do Data Infrastructure Insights , extrairá todas as dependências de imagem do operador e sairá do repositório do Data Infrastructure Insights . Quando solicitado, digite a senha temporária do repositório fornecida. Este comando baixa todas as imagens usadas pelo operador, inclusive para recursos opcionais. Veja abaixo para quais recursos essas imagens são usadas.

Funcionalidade do Operador Principal e Monitoramento do Kubernetes

- monitoramento netapp
- ci-kube-rbac-proxy
- ci-ksm
- ci-telegraf
- distroless-usuário-root

Registro de eventos

- ci-fluent-bit
- ci-kubernetes-event-exporter

Desempenho e Mapa da Rede

- observador ci-net

Envie a imagem do Docker do operador para seu repositório Docker privado/local/empresarial de acordo com suas políticas corporativas. Certifique-se de que as tags de imagem e os caminhos de diretório para essas imagens no seu repositório sejam consistentes com aqueles no repositório do Data Infrastructure Insights .

Edite a implantação do operador de monitoramento em operator-deployment.yaml e modifique todas as referências de imagem para usar seu repositório privado do Docker.

```
image: <docker repo of the enterprise/corp docker repo>/ci-kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Edite o AgentConfiguration em operator-config.yaml para refletir o novo local do repositório do Docker. Crie um novo imagePullSecret para seu repositório privado. Para mais detalhes, consulte *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation link here:
xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

Instruções do OpenShift

Se você estiver executando o OpenShift 4.6 ou superior, deverá editar o AgentConfiguration em *operator-config.yaml* para habilitar a configuração *runPrivileged*:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

O Openshift pode implementar um nível adicional de segurança que pode bloquear o acesso a alguns componentes do Kubernetes.

Tolerâncias e Manchas

Os DaemonSets *netapp-ci-telegraf-ds*, *netapp-ci-fluent-bit-ds* e *netapp-ci-net-observer-l4-ds* devem agendar um pod em cada nó do cluster para coletar dados corretamente em todos os nós. O operador foi configurado para tolerar algumas **manchas** bem conhecidas. Se você configurou alguma contaminação personalizada em seus nós, impedindo assim que os pods sejam executados em todos os nós, você pode criar uma **tolerância** para essas contaminações"na *Configuração do Agente*" . Se você tiver aplicado taints personalizados a todos os nós do cluster, também deverá adicionar as tolerâncias necessárias à implantação do operador para permitir que o pod do operador seja agendado e executado.

Saiba mais sobre o Kubernetes"Manchas e Tolerâncias" .

Voltar para o"* Página de instalação do operador de monitoramento do NetApp Kubernetes*"

Uma nota sobre segredos

Para remover a permissão do Kubernetes Monitoring Operator para visualizar segredos em todo o cluster, exclua os seguintes recursos do arquivo *operator-setup.yaml* antes da instalação:

```
 ClusterRole/netapp-ci<namespace>-agent-secret
 ClusterRoleBinding/netapp-ci<namespace>-agent-secret
```

Se for uma atualização, exclua também os recursos do seu cluster:

```
 kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

Se a Análise de Mudanças estiver habilitada, modifique *AgentConfiguration* ou *operator-config.yaml* para descomentar a seção de gerenciamento de mudanças e incluir *kindsToIgnoreFromWatch: '"secrets"'* na seção de gerenciamento de mudanças. Observe a presença e a posição das aspas simples e duplas nesta linha.

```
change-management:
  ...
  # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
  # # Each kind will have to be prefixed by its apigroup
  # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
  kindsToIgnoreFromWatch: '"secrets"'
  ...
```

Verificando assinaturas de imagem do operador de monitoramento do Kubernetes

A imagem do operador e todas as imagens relacionadas que ele implementa são assinadas pela NetApp. Você pode verificar manualmente as imagens antes da instalação usando a ferramenta cosign ou configurar um controlador de admissão do Kubernetes. Para mais detalhes, consulte o"Documentação do Kubernetes" .

A chave pública usada para verificar as assinaturas de imagem está disponível no bloco de instalação do Operador de Monitoramento em *Opcional: Carregar as imagens do operador para seu repositório privado > Chave Pública de Assinatura de Imagem*

Para verificar manualmente uma assinatura de imagem, execute as seguintes etapas:

1. Copie e execute o Image Pull Snippet
2. Copie e insira a senha do repositório quando solicitado
3. Armazene a chave pública da assinatura da imagem (dii-image-signing.pub no exemplo)
4. Verifique as imagens usando cosign. Consulte o seguinte exemplo de uso de cosigno

```
$ cosign verify --key dii-image-signing.pub --insecure-ignore-sct
--insecure-ignore-tlog <repository>/<image>:<tag>
Verification for <repository>/<image>:<tag> --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - The signatures were verified against the specified public key
[{"critical":{"identity":{"docker-
reference":"<repository>/<image>"},"image":{"docker-manifest-
digest":"sha256:<hash>"},"type":"cosign container image
signature"},"optional":null}]
```

Solução de problemas

Algumas coisas que você pode tentar se tiver problemas ao configurar o Kubernetes Monitoring Operator:

Problema:	**Experimente isto:**
Não vejo um hiperlink/conexão entre meu Volume Persistente do Kubernetes e o dispositivo de armazenamento de back-end correspondente. Meu volume persistente do Kubernetes é configurado usando o nome do host do servidor de armazenamento.	Siga as etapas para desinstalar o agente Telegraf existente e reinstale o agente Telegraf mais recente. Você deve estar usando o Telegraf versão 2.0 ou posterior, e seu armazenamento de cluster Kubernetes deve ser monitorado ativamente pelo Data Infrastructure Insights.

Problema:	Experimente isto:
Estou vendo mensagens nos logs semelhantes às seguintes: E0901 15:21:39.962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Falha ao listar *v1.MutatingWebhookConfiguration: o servidor não conseguiu encontrar o recurso solicitado E0901 15:21:43.168161 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Falha ao listar *v1.Lease: o servidor não conseguiu encontrar o recurso solicitado (obter leases.coordination.k8s.io) etc.	Essas mensagens podem ocorrer se você estiver executando o kube-state-metrics versão 2.0.0 ou superior com versões do Kubernetes inferiores à 1.20. Para obter a versão do Kubernetes: *kubectl version* Para obter a versão do kube-state-metrics: *kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* Para evitar que essas mensagens aconteçam, os usuários podem modificar sua implantação do kube-state-metrics para desabilitar os seguintes Leases: *mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources* Mais especificamente, eles podem usar o seguinte argumento da CLI: resources=certificatesigningrequests,configmaps,cronjobs,daemonsets, deployments,endpoints,horizontalpodautoscalers,ingresses,jobs,limitranges, namespaces,networkpolicies,nodes,persistentvolumeclaims,persistentvolumes, poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas, segredos, serviços, conjuntos de estado, classes de armazenamento A lista de recursos padrão é: "certificatesigningrequests, configmaps, cronjobs, daemonsets, implantações, endpoints, horizontalpodautoscalers, ingresses, jobs, leases, limitranges, mutatingwebhookconfigurations, namespaces, networkpolicies, nodes, persistentvolumeclaims, persistentvolumes, poddisruptionbudgets, pods, replicasets, replicationcontrollers, resourcequotas, secrets, services, statefulsets, storageclasses, validatingwebhookconfigurations, volumeattachments"
Vejo mensagens de erro do Telegraf semelhantes às seguintes, mas o Telegraf inicia e executa: 11 de outubro 14:23:41 ip-172-31-39-47 systemd[1]: Iniciado O agente do servidor controlado por plugin para relatar métricas no InfluxDB. 11 de out. 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="falha ao criar diretório de cache. /etc/telegraf/.cache/snowflake, err: mkdir /etc/telegraf/.ca che: permissão negada. ignorada\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11 de out. 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="falha ao abrir. Ignorado. abra /etc/telegraf/.cache/snowflake/ocsp_response_cache.json: arquivo ou diretório inexistente\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11 de out. 14:23:41 ip-172-31-39-47 telegraf[1827]: 2021-10-11T14:23:41Z Eu! Iniciando o Telegraf 1.19.3	Este é um problema conhecido. Consulte"Este artigo do GitHub" para mais detalhes. Enquanto o Telegraf estiver funcionando, os usuários podem ignorar essas mensagens de erro.

Problema:	Experimente isto:
No Kubernetes, meus pods Telegraf estão relatando o seguinte erro: "Erro no processamento de informações de mountstats: falha ao abrir o arquivo mountstats: /hostfs/proc/1/mountstats, erro: abrir /hostfs/proc/1/mountstats: permissão negada"	Se o SELinux estiver habilitado e em execução, é provável que ele esteja impedindo que o(s) pod(s) Telegraf acessem o arquivo /proc/1/mountstats no nó do Kubernetes. Para superar essa restrição, edite a configuração do agente e ative a configuração runPrivileged. Para mais detalhes, consulte as instruções do OpenShift.
No Kubernetes, meu pod Telegraf ReplicaSet está relatando o seguinte erro: [inputs.prometheus] Erro no plugin: não foi possível carregar o par de chaves /etc/kubernetes/pki/etcd/server.crt:/etc/kubernetes/pki/etcd/server.key: aberto /etc/kubernetes/pki/etcd/server.crt: nenhum arquivo ou diretório desse tipo	O pod Telegraf ReplicaSet foi projetado para ser executado em um nó designado como mestre ou para etcd. Se o pod ReplicaSet não estiver em execução em um desses nós, você receberá esses erros. Verifique se seus nós mestre/etcd têm contaminações. Se isso acontecer, adicione as tolerâncias necessárias ao Telegraf ReplicaSet, telegraf-rs. Por exemplo, edite o ReplicaSet… kubectl edit rs telegraf-rs …e adicione as tolerâncias apropriadas à especificação. Em seguida, reinicie o pod ReplicaSet.
Tenho um ambiente PSP/PSA. Isso afeta meu operador de monitoramento?	Se o seu cluster Kubernetes estiver em execução com a Política de Segurança de Pod (PSP) ou a Admissão de Segurança de Pod (PSA) em vigor, você deverá atualizar para a versão mais recente do Operador de Monitoramento do Kubernetes. Siga estas etapas para atualizar para a Operadora atual com suporte para PSP/PSA: 1. Desinstalar o operador de monitoramento anterior: kubectl delete agent agent-monitoring-netapp -n netapp-monitoring kubectl delete ns netapp-monitoring kubectl delete crd agents.monitoring.netapp.com kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding 2. Instalar a versão mais recente do operador de monitoramento.
Tive problemas ao tentar implantar o Operador e tenho o PSP/PSA em uso.	1. Edite o agente usando o seguinte comando: kubectl -n <name-space> edit agent 2. Marque 'security-policy-enabled' como 'false'. Isso desabilitará as Políticas de Segurança do Pod e a Admissão de Segurança do Pod e permitirá que o Operador faça a implantação. Confirme usando os seguintes comandos: kubectl get psp (deve mostrar que a Política de Segurança do Pod foi removida) kubectl get all -n <namespace>
grep -i psp (deve mostrar que nada foi encontrado)	Erros "ImagePullBackoff" vistos

Problema:	Experimente isto:
Esses erros podem ser vistos se você tiver um repositório docker personalizado ou privado e ainda não tiver configurado o Kubernetes Monitoring Operator para reconhecê-lo corretamente. Ler mais sobre configuração para repositório personalizado/privado.	Estou tendo um problema com a implantação do meu operador de monitoramento e a documentação atual não me ajuda a resolvê-lo.

Capture ou anote a saída dos seguintes comandos e entre em contato com a equipe de Suporte Técnico.
`kubectl -n netapp-monitoring get all`
`kubectl -n netapp-monitoring describe all`
`kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all-containers=true`
`kubectl -n netapp-monitoring logs <telegraf-pod> --all-containers=true`
	Os pods net-observer (Mapa de Carga de Trabalho) no namespace Operator estão em CrashLoopBackOff

Esses pods correspondem ao coletor de dados do Workload Map para Network Observability. Tente isto: • Verifique os logs de um dos pods para confirmar a versão mínima do kernel. Por exemplo: ---- {"ci-tenant-id":"your-tenant-id","collector-cluster":"your-k8s-cluster-name","environment":"prod","level":"error","msg":"falha na validação. Motivo: a versão do kernel 3.10.0 é inferior à versão mínima do kernel 4.18.0","time":"2022-11-09T08:23:08Z"} ---- • Os pods do Net-observer exigem que a versão do kernel Linux seja pelo menos 4.18.0. Verifique a versão do kernel usando o comando “uname -r” e certifique-se de que seja >= 4.18.0	Os pods estão sendo executados no namespace do Operador (padrão: netapp-monitoring), mas nenhum dado é mostrado na IU para o mapa de carga de trabalho ou métricas do Kubernetes em Consultas
Verifique a configuração de tempo nos nós do cluster K8S. Para auditoria e relatórios de dados precisos, é altamente recomendável sincronizar a hora na máquina do agente usando o Network Time Protocol (NTP) ou o Simple Network Time Protocol (SNTP).	Alguns dos pods do net-observer no namespace do operador estão no estado Pendente

Problema:	Experimente isto:
Net-observer é um DaemonSet e executa um pod em cada nó do cluster k8s. • Observe o pod que está no estado Pendente e verifique se ele está enfrentando um problema de recurso de CPU ou memória. Certifique-se de que a memória e a CPU necessárias estejam disponíveis no nó.	Estou vendo o seguinte em meus logs imediatamente após instalar o Kubernetes Monitoring Operator: [inputs.prometheus] Erro no plugin: erro ao fazer solicitação HTTP para http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Obter http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: discar tcp: procurar kube-state-metrics.<namespace>.svc.cluster.local: nenhum host
Essa mensagem normalmente só é vista quando um novo operador é instalado e o pod *telegraf-rs* é ativado antes do pod *ksm*. Essas mensagens devem parar quando todos os pods estiverem em execução.	Não vejo nenhuma métrica sendo coletada para os CronJobs do Kubernetes que existem no meu cluster.
Verifique sua versão do Kubernetes (ou seja, `kubectl version`). Se for v1.20.x ou anterior, esta é uma limitação esperada. A versão kube-state-metrics implantada com o Kubernetes Monitoring Operator suporta apenas a v1.CronJob. Com o Kubernetes 1.20.x e versões anteriores, o recurso CronJob está em v1beta.CronJob. Como resultado, o kube-state-metrics não consegue encontrar o recurso CronJob.	Após instalar o operador, os pods telegraf-ds entram em CrashLoopBackOff e os logs dos pods indicam "su: Falha de autenticação".
Edite a seção telegraf em *AgentConfiguration* e defina *dockerMetricCollectionEnabled* como false. Para mais detalhes, consulte o manual do operador"opções de configuração" . … especificação: … telégrafo: … - nome: docker run-mode: - Substituições do DaemonSet: - chave: DOCKER_UNIX_SOCK_PLACEHOLDER valor: unix:///run/docker.sock … …	Vejo mensagens de erro repetidas semelhantes às seguintes nos meus logs do Telegraf: E! [agent] Erro ao gravar em outputs.http: Post "https://<tenant_url>/rest/v1/lake/ingest/influxdb": prazo de contexto excedido (Client.Timeout excedido ao aguardar cabeçalhos)
Edite a seção telegraf em *AgentConfiguration* e aumente *outputTimeout* para 10s. Para mais detalhes, consulte o manual do operador"opções de configuração" .	Estou sem dados *involvedobject* para alguns Logs de Eventos.
Certifique-se de ter seguido os passos no"Permissões" seção acima.	Por que estou vendo dois pods de operador de monitoramento em execução, um chamado netapp-ci-monitoring-operator-<pod> e o outro chamado monitoring-operator-<pod>?
A partir de 12 de outubro de 2023, o Data Infrastructure Insights refatorou o operador para melhor atender nossos usuários; para que essas mudanças sejam totalmente adotadas, você deveremover o operador antigo einstalar o novo .	Meus eventos do Kubernetes pararam inesperadamente de reportar ao Data Infrastructure Insights.

Problema:	Experimente isto:
Recupere o nome do pod do exportador de eventos: `` `kubectl -n netapp-monitoring get pods ``	grep event-exporter
awk '{print $1}'	sed 's/event-exporter./event-exporter/` Deve ser "netapp-ci-event-exporter" ou "event-exporter". Em seguida, edite o agente de monitoramento `kubectl -n netapp-monitoring edit agent` e defina o valor para LOG_FILE para refletir o nome do pod do exportador de eventos apropriado encontrado na etapa anterior. Mais especificamente, LOG_FILE deve ser definido como "/var/log/containers/netapp-ci-event-exporter.log" ou "/var/log/containers/event-exporter*.log" …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. Alternativamente, também se podedesinstalar ereinstalar o agente.
Estou vendo pod(s) implantado(s) pelo Kubernetes Monitoring Operator travando devido a recursos insuficientes.	Consulte o Operador de Monitoramento do Kubernetes"opções de configuração" para aumentar os limites da CPU e/ou memória conforme necessário.
Uma imagem ausente ou configuração inválida fez com que os pods netapp-ci-kube-state-metrics falhassem na inicialização ou ficassem prontos. Agora o StatefulSet está travado e as alterações de configuração não estão sendo aplicadas aos pods netapp-ci-kube-state-metrics.	O StatefulSet está em um"quebrado" estado. Depois de corrigir quaisquer problemas de configuração, faça o retorno dos pods netapp-ci-kube-state-metrics.
Os pods netapp-ci-kube-state-metrics falham ao iniciar após executar uma atualização do Kubernetes Operator, gerando ErrImagePull (falha ao extrair a imagem).	Tente redefinir os pods manualmente.

Problema:	Experimente isto:
Mensagens "Evento descartado por ser mais antigo que maxEventAgeSeconds" estão sendo observadas no meu cluster Kubernetes na Análise de Log.	Modifique o operador *agentconfiguration* e aumente *event-exporter-maxEventAgeSeconds* (ou seja, para 60s), *event-exporter-kubeQPS* (ou seja, para 100) e *event-exporter-kubeBurst* (ou seja, para 500). Para obter mais detalhes sobre essas opções de configuração, consulte o"opções de configuração" página.
O Telegraf avisa ou trava por causa de memória bloqueável insuficiente.	Tente aumentar o limite de memória bloqueável para o Telegraf no sistema operacional/nó subjacente. Se aumentar o limite não for uma opção, modifique a configuração do agente NKMO e defina *unprotected* como *true*. Isso instruirá o Telegraf a não tentar reservar páginas de memória bloqueadas. Embora isso possa representar um risco à segurança, pois segredos descriptografados podem ser transferidos para o disco, isso permite a execução em ambientes onde não é possível reservar memória bloqueada. Para mais detalhes sobre as opções de configuração *desprotegidas*, consulte o"opções de configuração" página.
Vejo mensagens de aviso do Telegraf parecidas com as seguintes: *W! [inputs.diskio] Não foi possível coletar o nome do disco para "vdc": erro ao ler /dev/vdc: arquivo ou diretório inexistente*	Para o Operador de Monitoramento do Kubernetes, essas mensagens de aviso são inofensivas e podem ser ignoradas com segurança. Como alternativa, edite a seção telegraf em AgentConfiguration e defina *runDsPrivileged* como true. Para mais detalhes, consulte o"opções de configuração do operador" .

Problema:	Experimente isto:

Meu pod fluent-bit está falhando com os seguintes erros: [2024/10/16 14:16:23] [erro] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno=24] Muitos arquivos abertos [2024/10/16 14:16:23] [erro] falha ao inicializar a entrada tail.0 [2024/10/16 14:16:23] [erro] falha na inicialização da entrada [engine]	Tente alterar as configurações do *fsnotify* no seu cluster:
	
	`sudo sysctl fs.inotify.max_user_instances (take note of setting)`
	
	`sudo sysctl fs.inotify.max_user_instances=<something larger than current setting>`
	
	`sudo sysctl fs.inotify.max_user_watches (take note of setting)`
	
	`sudo sysctl fs.inotify.max_user_watches=<something larger than current setting>`
	
	Reinicie o Fluent-bit.
	
	Observação: para tornar essas configurações persistentes nas reinicializações dos nós, você precisa colocar as seguintes linhas em */etc/sysctl.conf*
	
	`fs.inotify.max_user_instances=<something larger than current setting>`
	`fs.inotify.max_user_watches=<something larger than current setting>`

Problema:	Experimente isto:
Os pods do Telegraf DS estão relatando erros referentes ao plug-in de entrada do Kubernetes que não consegue fazer solicitações HTTP devido à incapacidade de validar o certificado TLS. Por exemplo: E! [inputs.kubernetes] Erro no plugin: erro ao fazer solicitação HTTP para"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": Pegar"<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": tls: falha ao verificar o certificado: x509: não é possível validar o certificado para <kubelet_IP> porque ele não contém nenhum SAN IP	Isso ocorrerá se o kubelet estiver usando certificados autoassinados e/ou o certificado especificado não incluir o <kubelet_IP> na lista *Nome alternativo do assunto* dos certificados. Para resolver isso, o usuário pode modificar o"configuração do agente" , e defina *telegraf:insecureK8sSkipVerify* como *true*. Isso configurará o plugin de entrada do Telegraf para pular a verificação. Alternativamente, o usuário pode configurar o kubelet para"servidorTLSBootstrap" , que acionará uma solicitação de certificado da API 'certificates.k8s.io'.

Informações adicionais podem ser encontradas em"Apoiar" página ou no"Matriz de Suporte ao Coletor de Dados" .

Coletor de Dados Memcached

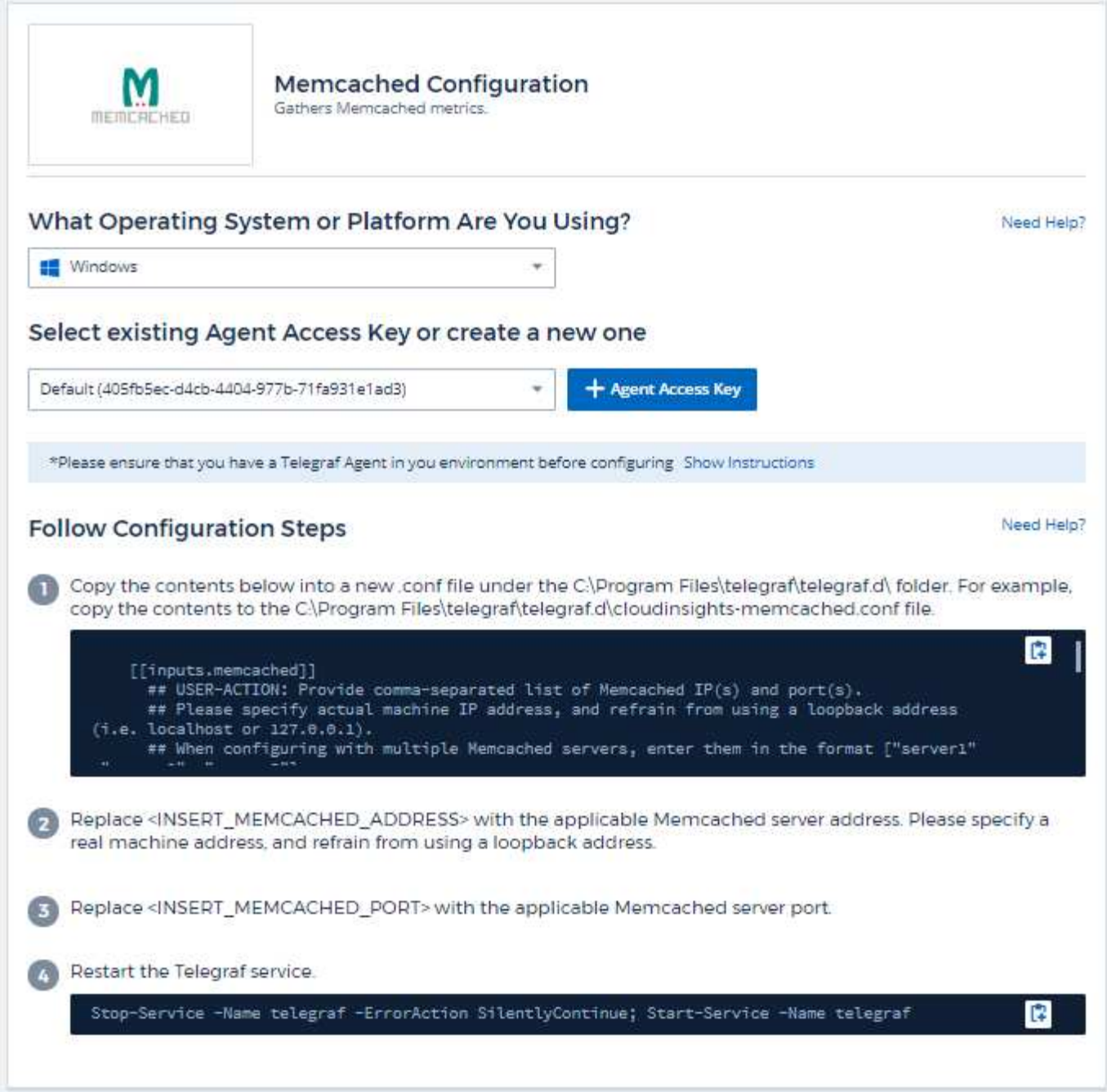
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Memcached.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha Memcached.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.



Configurar

Informações podem ser encontradas em"Wiki do Memcached" .

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Memcached	Servidor de namespace	IP do nó Nome do nó	Conexões aceitas processadas Solicitações de autenticação Autenticações com falha Bytes usados Bytes lidos (por segundo) Bytes gravados (por segundo) CAS inválido Acertos de CAS Faltas de CAS Requisições de liberação (por segundo) Requisições de obtenção (por segundo) Requisições de definição (por segundo) Requisições de toque (por segundo) Rendimentos de conexão (por segundo) Estruturas de conexão Conexões abertas Itens armazenados atuais Acertos de solicitações de redução (por segundo) Acertos de solicitações de redução (por segundo) Acertos de solicitações de exclusão (por segundo) Acertos de solicitações de exclusão (por segundo) Itens removidos Remoções válidas Itens expirados Acertos de obtenção (por segundo) Acertos de obtenção (por segundo) Bytes de hash usados Hash está se expandindo Nível de poder de hash Acertos de solicitações de aumento (por segundo) Acertos de solicitações de aumento (por segundo) Máximo de bytes do servidor Número de threads de trabalho recuperados Contagem Total de conexões abertas Total de itens armazenados Acertos de toque Acertos de toque Tempo de atividade do servidor

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de Dados MongoDB

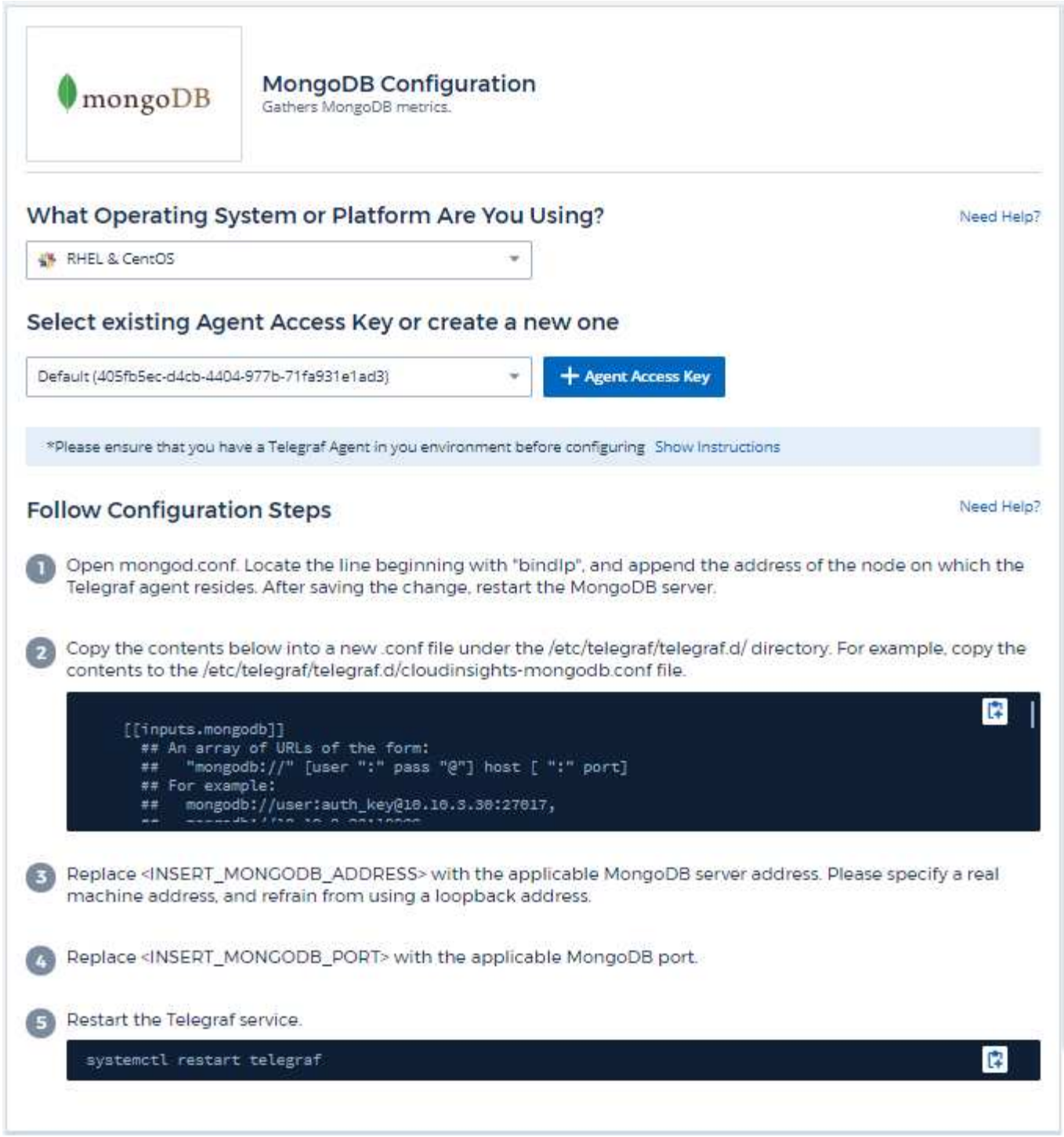
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do MongoDB.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha MongoDB.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.



Configurar

Informações podem ser encontradas em"Documentação do MongoDB" .

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
MongoDB	Nome do host do namespace		
Banco de dados MongoDB	Nome do host do namespace Nome do banco de dados		

Solução de problemas

Informações podem ser encontradas no"Apoiar" página.

Coletor de dados MySQL

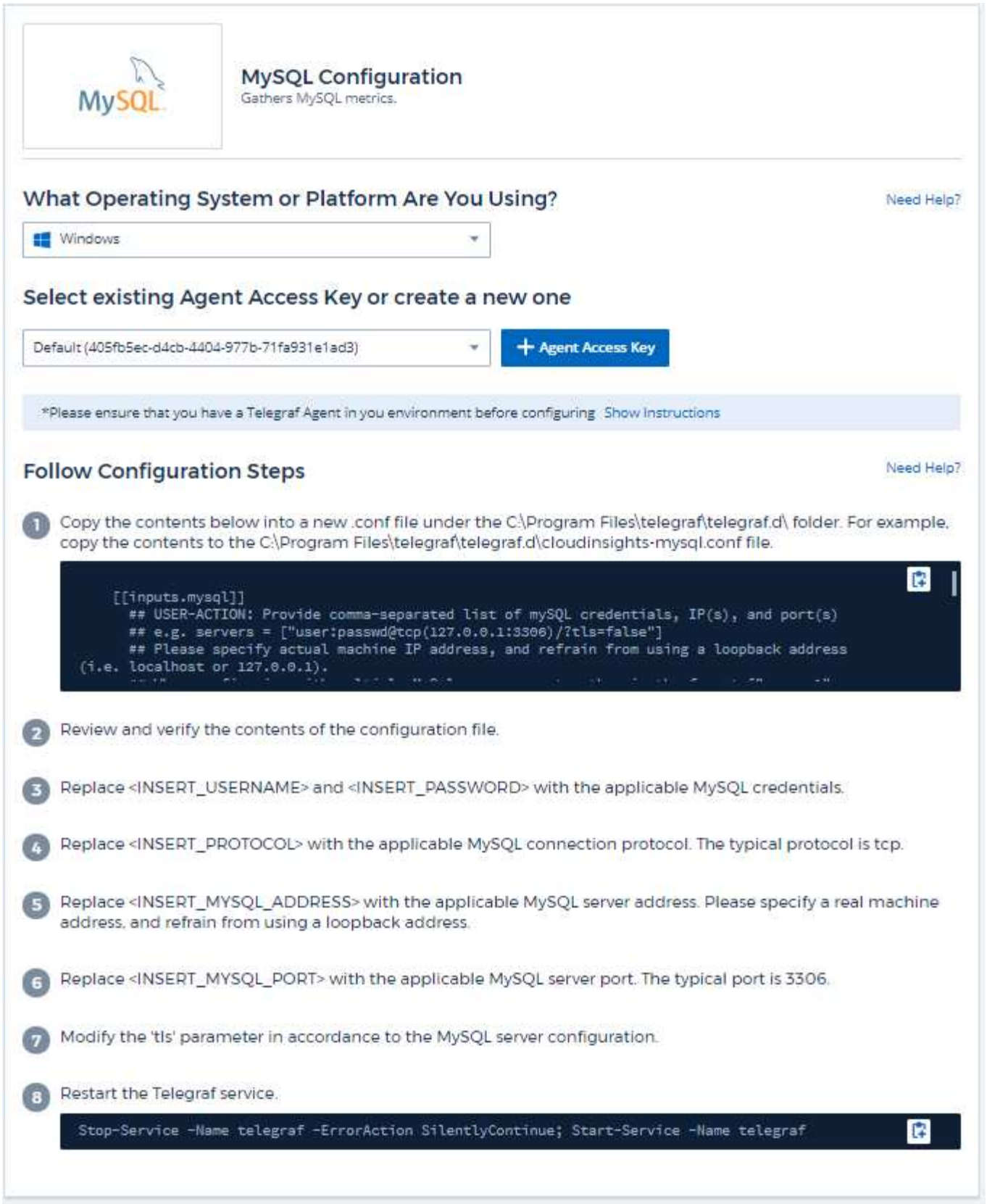
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do MySQL.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha MySQL.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.



Configurar

Informações podem ser encontradas em"Documentação do MySQL" .

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
MySQL	Servidor MySQL de namespace	IP do nó Nome do nó	Clientes Abortados (por segundo) Conexões Abortadas (por segundo) Bytes RX (por segundo) Bytes TX (por segundo) Comandos Admin (por segundo) Comandos Comandos Alterar Evento Comandos Alterar Função Comandos Alterar Instância Comandos Alterar Procedimento Comandos Alterar Servidor Comandos Alterar Tabela Comandos Alterar Espaço de Tabela Comandos Alterar Usuário Comandos Analisar Comandos Atribuir ao Keycache Comandos Iniciar Comandos Binlog Comandos de Procedimento de Chamada Comandos Alterar BD Comandos Alterar Mestre Comandos Alterar Filtro de Replicação Comandos Verificar Comandos de Soma de Verificação Comandos Confirmar Comandos Criar BD Comandos Criar Evento Comandos Criar Função Comandos Criar Índice Comandos Criar Procedimento Comandos Criar Servidor Comandos Criar Tabela Comandos Criar Comandos de Gatilho Criar Comandos UDF Criar Comandos Usuário Criar Comandos de Exibição Erros de Conexão SQL Desalocar Aceitar Tabelas de Disco Tmp Criadas Erros Atrasados Comandos de Liberação Comprometimento do Manipulador Bytes do Pool de Buffers Innodb Blocos de Chave de Dados Não Liberados Solicitações de Leitura de

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de dados Netstat

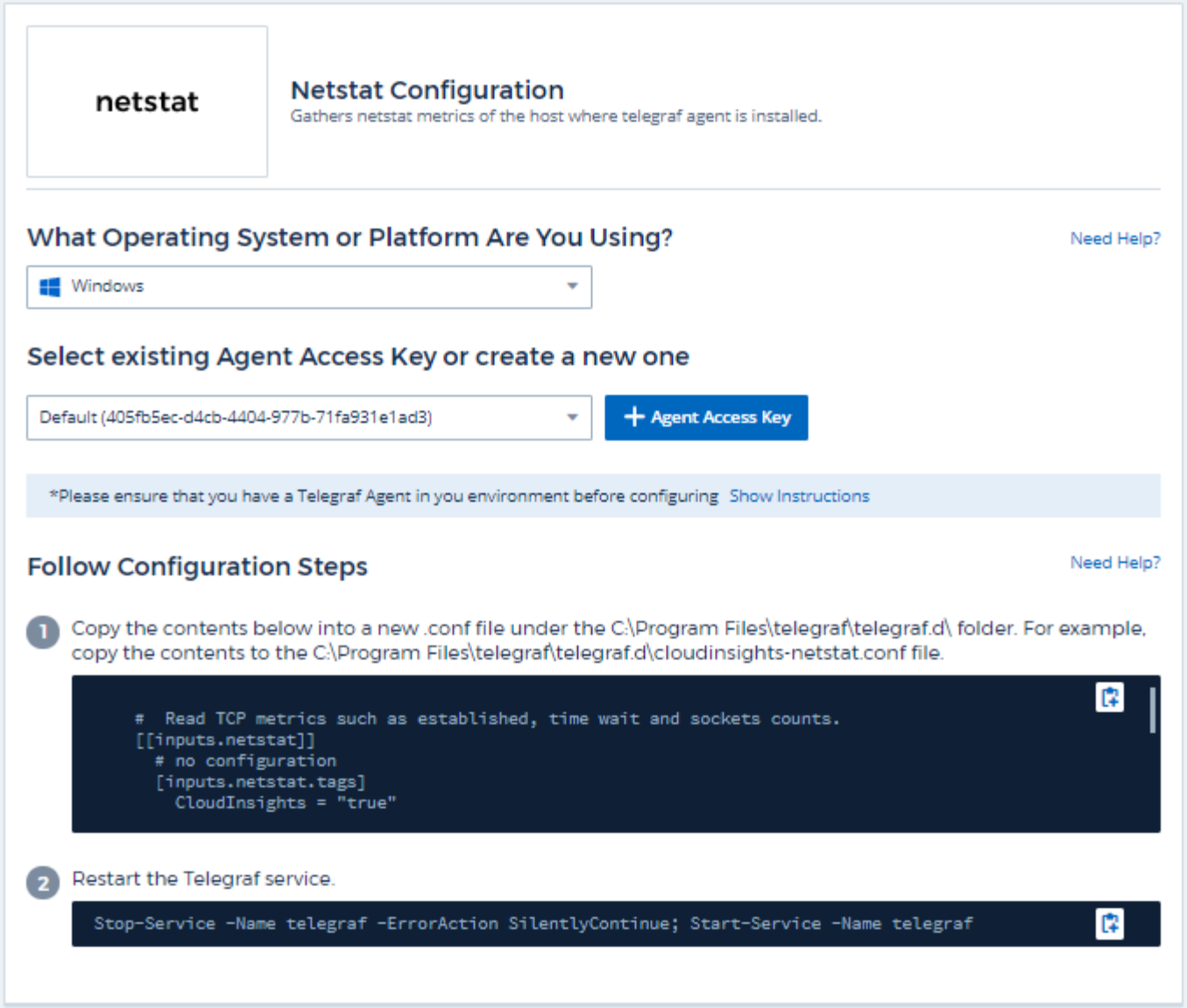
O Data Infrastructure Insights usa esse coletor de dados para reunir métricas do Netstat.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha Netstat.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.



Configurar

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Netstat	UUID do nó	IP do nó Nome do nó	

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de dados Nginx

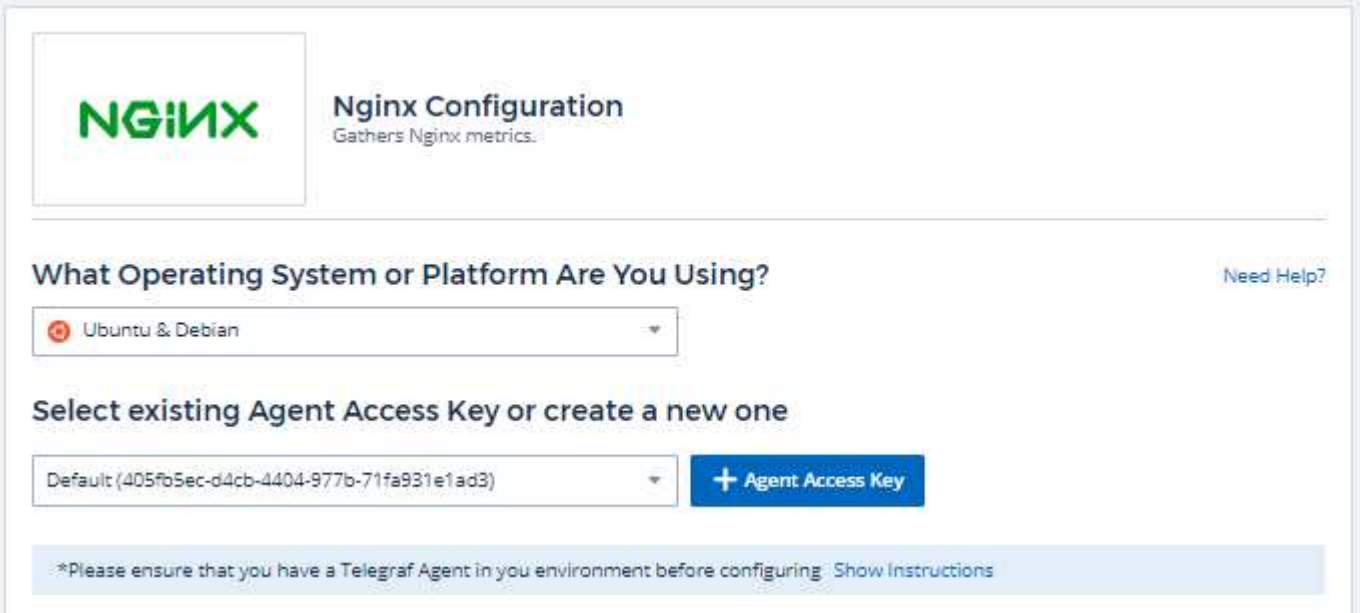
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Nginx.

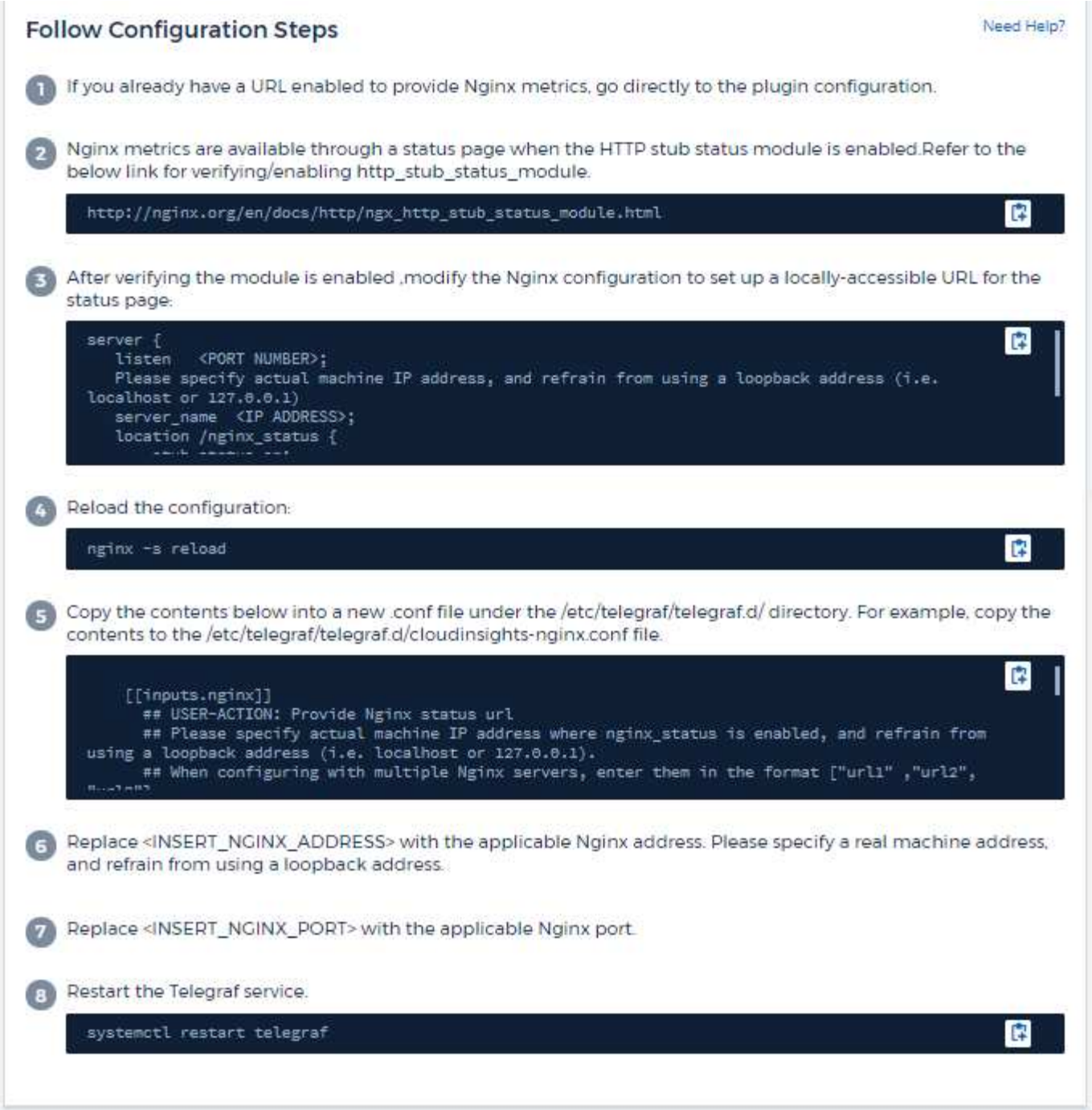
Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha Nginx.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.





Configurar

A coleta de métricas do Nginx requer que o Nginx"http_stub_status_module" ser habilitado.

Informações adicionais podem ser encontradas em"Documentação do Nginx" .

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Nginx	Servidor de namespace	IP do nó Nome do nó Porta	Aceita solicitações de leitura ativas aguardando escrita

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de Dados PostgreSQL

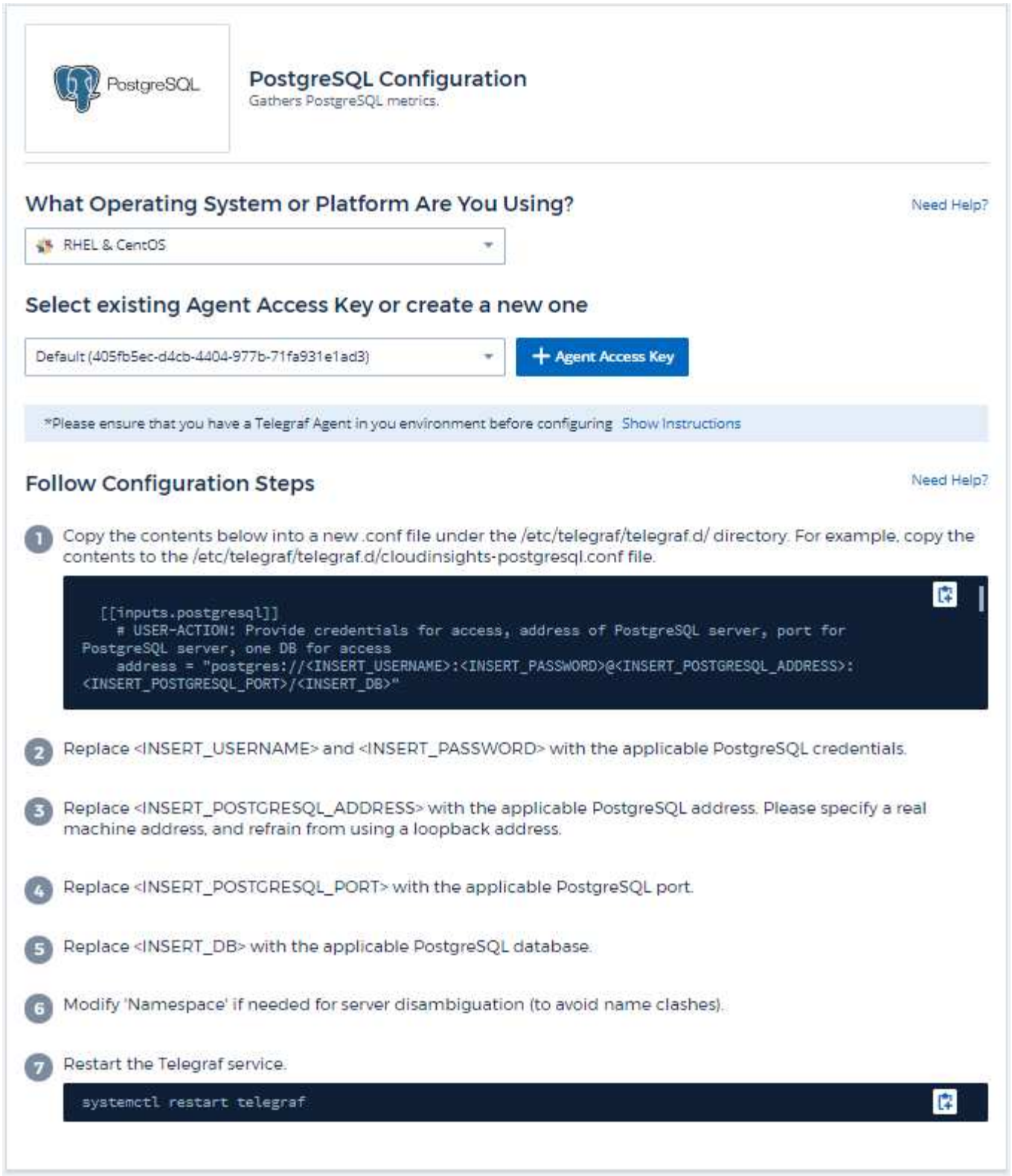
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do PostgreSQL.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha PostgreSQL.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.



Configurar

Informações podem ser encontradas em"Documentação do PostgreSQL" .

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Servidor PostgreSQL	Servidor de banco de dados de namespace	Nome do nó IP do nó	Buffers Buffers alocados Buffers de backend Buffers de sincronização de arquivo de backend Buffers de ponto de verificação Pontos de verificação limpos Tempo de sincronização Pontos de verificação Tempo de gravação Pontos de verificação Solicitações Pontos de verificação Tempo máximo de gravação Limpeza
Banco de dados PostgreSQL	Servidor de banco de dados de namespace	OID do banco de dados Nome do nó IP do nó	Blocos Tempo de leitura Blocos Tempo de gravação Blocos Acertos Blocos Leituras Conflitos Deadlocks Número de clientes Arquivos temporários Bytes Arquivos temporários Número Linhas Linhas excluídas Linhas recuperadas Linhas inseridas Linhas retornadas Transações atualizadas Transações confirmadas Revertidas

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de dados do agente fantoche

O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Puppet Agent.

Instalação

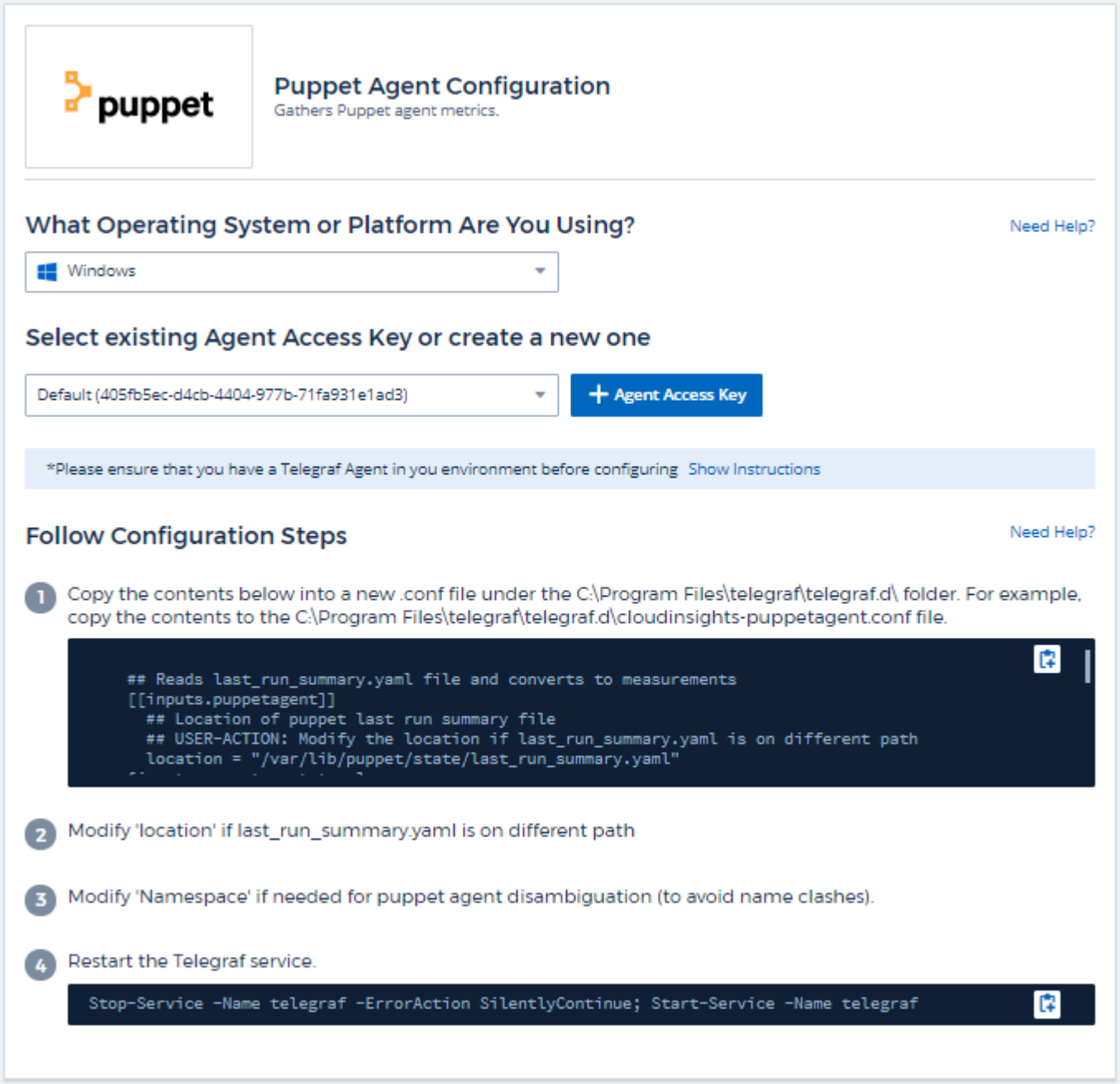
1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha Puppet.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática

recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.

4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.



Configurar

Informações podem ser encontradas em "Documentação do Puppet"

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:

Agente Fantoche	UUID do nó do namespace	Nome do nó Localização IP do nó Versão Configstring Versão Puppet	Alterações Total de Eventos Eventos de Falha Eventos de Sucesso Total de Recursos Recursos Alterados Recursos com Falha Recursos com Falha ao Reiniciar Recursos Recursos Fora de Sincronia Recursos Reiniciados Recursos Agendados Recursos Ignorados Tempo Total Tempo de Âncora Tempo de Recuperação de Configuração Tempo Cron Tempo de Execução Tempo de Arquivo Tempo de Filebucket Tempo de Última Execução Tempo de Pacote Tempo de Agendamento Tempo de Serviço Tempo de Sshauthorizedkey Tempo Total de Usuário

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Coletor de dados Redis

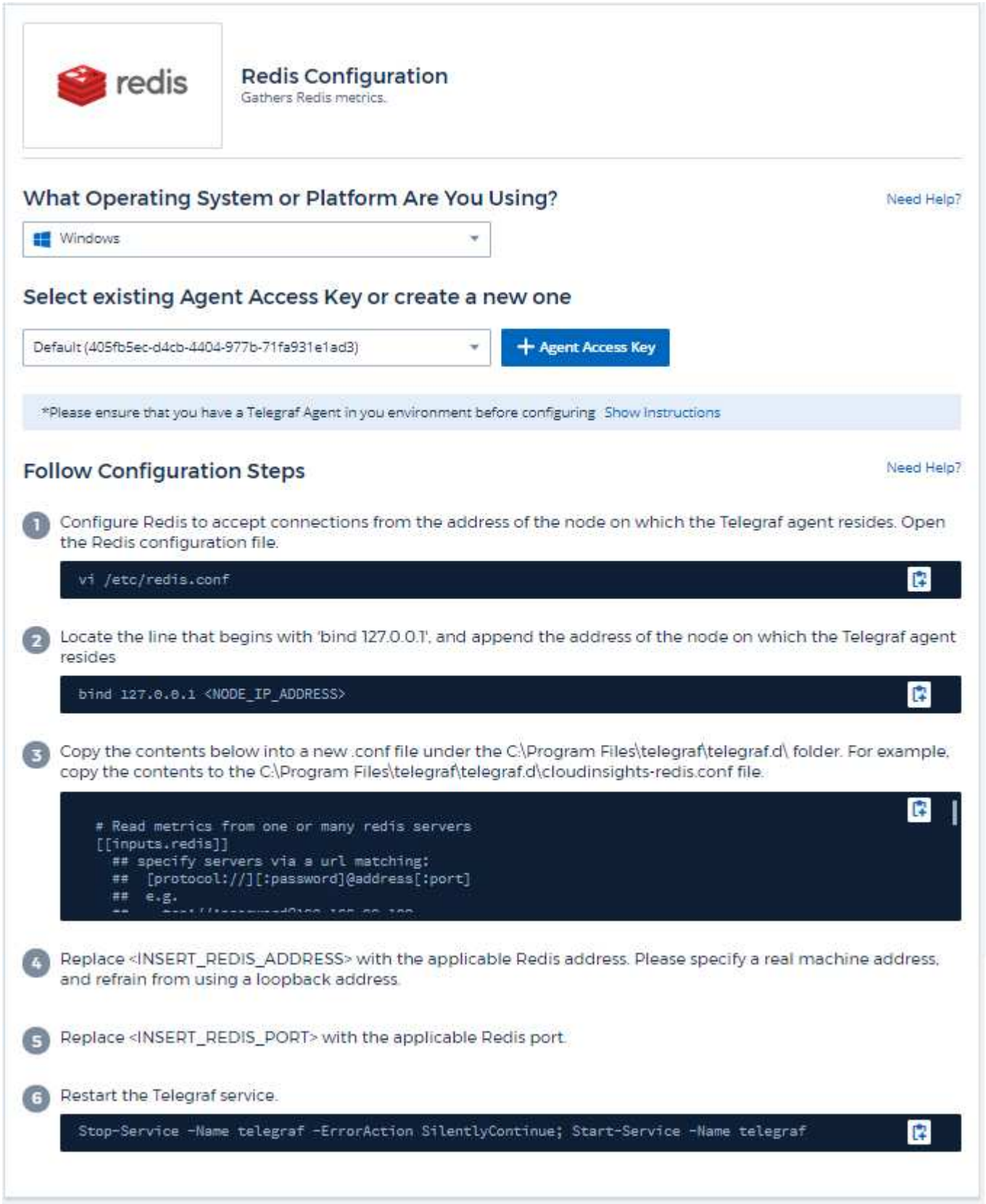
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Redis. Redis é um armazenamento de estrutura de dados de código aberto, na memória, usado como banco de dados, cache e corretor de mensagens, suportando as seguintes estruturas de dados: strings, hashes, listas, conjuntos e muito mais.

Instalação

1. Em **Observabilidade > Coletores**, clique em **+Coletor de Dados**. Escolha Redis.

   Selecione o sistema operacional ou plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleta ou deseja instalar um Agente para um Sistema Operacional ou Plataforma diferente, clique em *Mostrar Instruções* para expandir o"Instalação do agente" instruções.
3. Selecione a Chave de Acesso do Agente para uso com este coletor de dados. Você pode adicionar uma nova Chave de Acesso do Agente clicando no botão **+ Chave de Acesso do Agente**. Prática recomendada: use uma chave de acesso de agente diferente somente quando quiser agrupar coletores de dados, por exemplo, por sistema operacional/plataforma.
4. Siga as etapas de configuração para configurar o coletor de dados. As instruções variam dependendo do tipo de sistema operacional ou plataforma que você está usando para coletar dados.



Configurar

Informações podem ser encontradas em"Documentação do Redis" .

Objetos e Contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Redis	Servidor de namespace		

Solução de problemas

Informações adicionais podem ser encontradas em"Apoiar" página.

Informações sobre direitos autorais

Informações sobre marcas comerciais