Referência do coletor de dados - Serviços

Data Infrastructure Insights

NetApp
January 10, 2025

Índice

Referência do coletor de dados - Serviços

Coleta de dados de nó

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

Instalação

1. A partir de **Observability > Collectors**, 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 de nós.
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 Node:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Sistema de ficheiros do nó	Tipo caminho dispositivo UUUID nó	Nome do nó IP do nó modo de SO do nó	Livres inodes livres inodes totais usados Total usado Total usado usado
Disco do nó	Disco UUUID nó	Nome do nó IP do nó os do nó	Tempo de e/S Total IOPS em andamento ler bytes (por seg) tempo de leitura Total leituras (por seg) tempo de e/S ponderado Total de bytes de gravação (por seg) tempo de gravação Total de gravações (por seg) tempo de gravação tempo de leitura tempo de e/S
CPU de nó	CPU UUUID nó	Nome do nó IP do nó os do nó	Uso da CPU do usuário uso da CPU ocioso uso da CPU processador CPU interrupção uso da CPU uso da CPU DPC CPU uso

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Nó	UUID de nó	Nome do nó IP do nó os do nó	Kernel tempo de inicialização Kernel Context switches (por seg) Kernel Entropy available Kernel interrupts (por seg) Kernel processes forked (por seg) memória ativa disponível memória Total memória disponível memória Buffered
Rede de nós	UUID do nó de interface de rede	Nó Nome nó IP nó os	Bytes recebidos bytes recebidos Pacotes enviados Outboud Pacotes descartados erros Outboud Pacotes recebidos Pacotes descartados Pacotes recebidos erros recebidos Pacotes recebidos pacotes recebidos pacotes enviados

Configuração

As informações de configuração e resolução de problemas podem ser encontradas "Configurando um Agente"na página.

ActiveMQ Data Collector

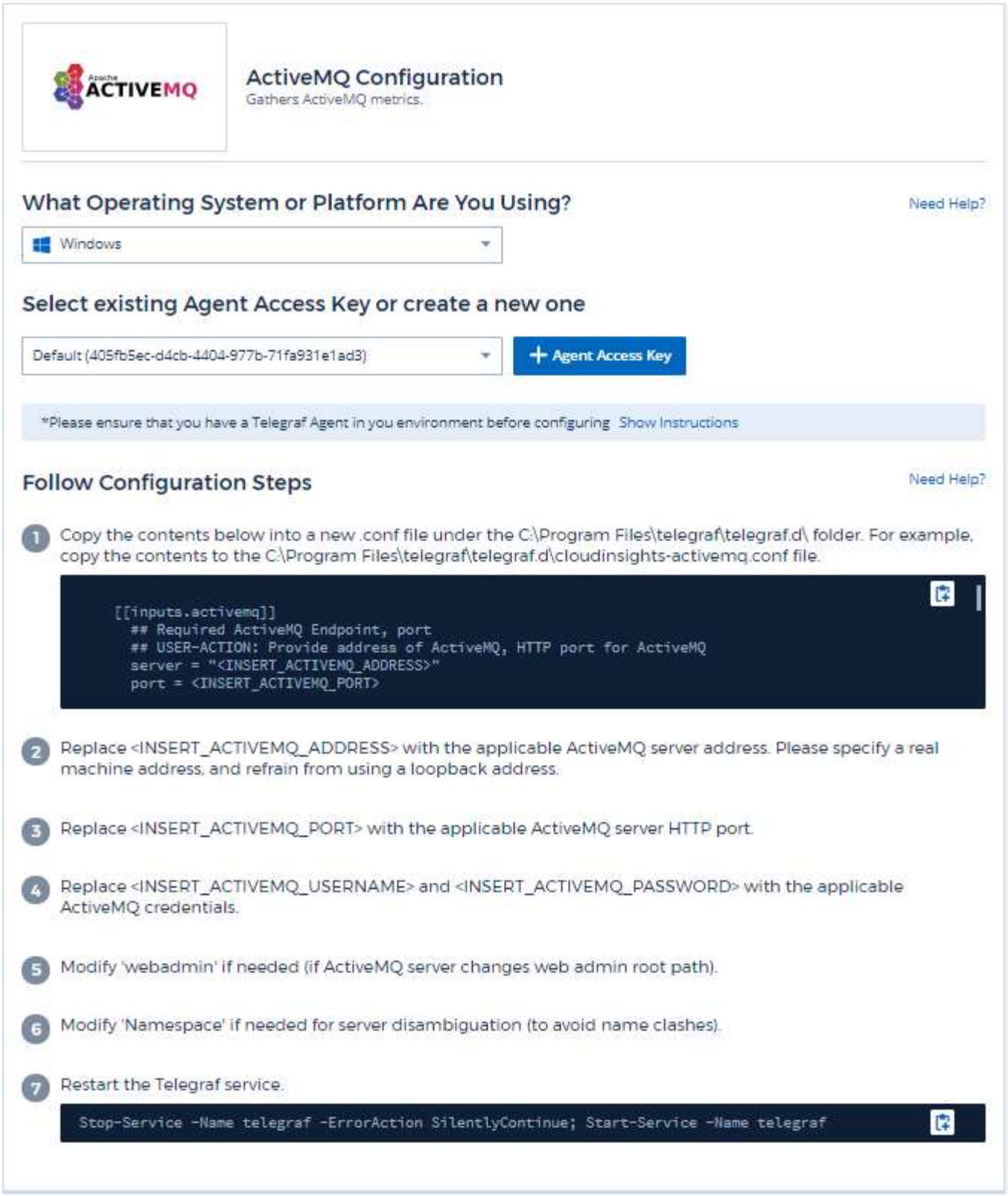
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do ActiveMQ.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha ActiveMQ.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

As informações podem ser encontradas no "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	UUUID do nó IP do nó de nome do nó	Tamanho da fila de contagem de filas de contagem de filas de contagem de filas de contagem de filas de contagem de filas
Assinante ActiveMQ	ID de conexão ID de cliente Port Server namespace	É subscrição do Seletor de SO do nó de nome do nó de destino ativo nó UUUID do nó de destino ativo	Contagem de desfila despachada contagem despachado tamanho da fila contagem de espera pendente contagem Enqueue tamanho da fila
Tópico ActiveMQ	Tópico servidor de porta namespace	Nó Nome nó nó IP nó UUUID nó os	Tamanho da contagem Enqueue contagem contagem contagem Dequeue consumidores

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

Apache Data Collector

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

Pré-requisitos

- Você deve ter seu servidor HTTP Apache configurado e funcionando corretamente
- Você deve ter permissões de sudo ou administrador no host/VM do agente
- Normalmente, o módulo Apache *mod_status* está configurado para expor uma página na localização '/Server-status?auto' do servidor Apache. A opção *ExtendedStatus* deve estar ativada 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

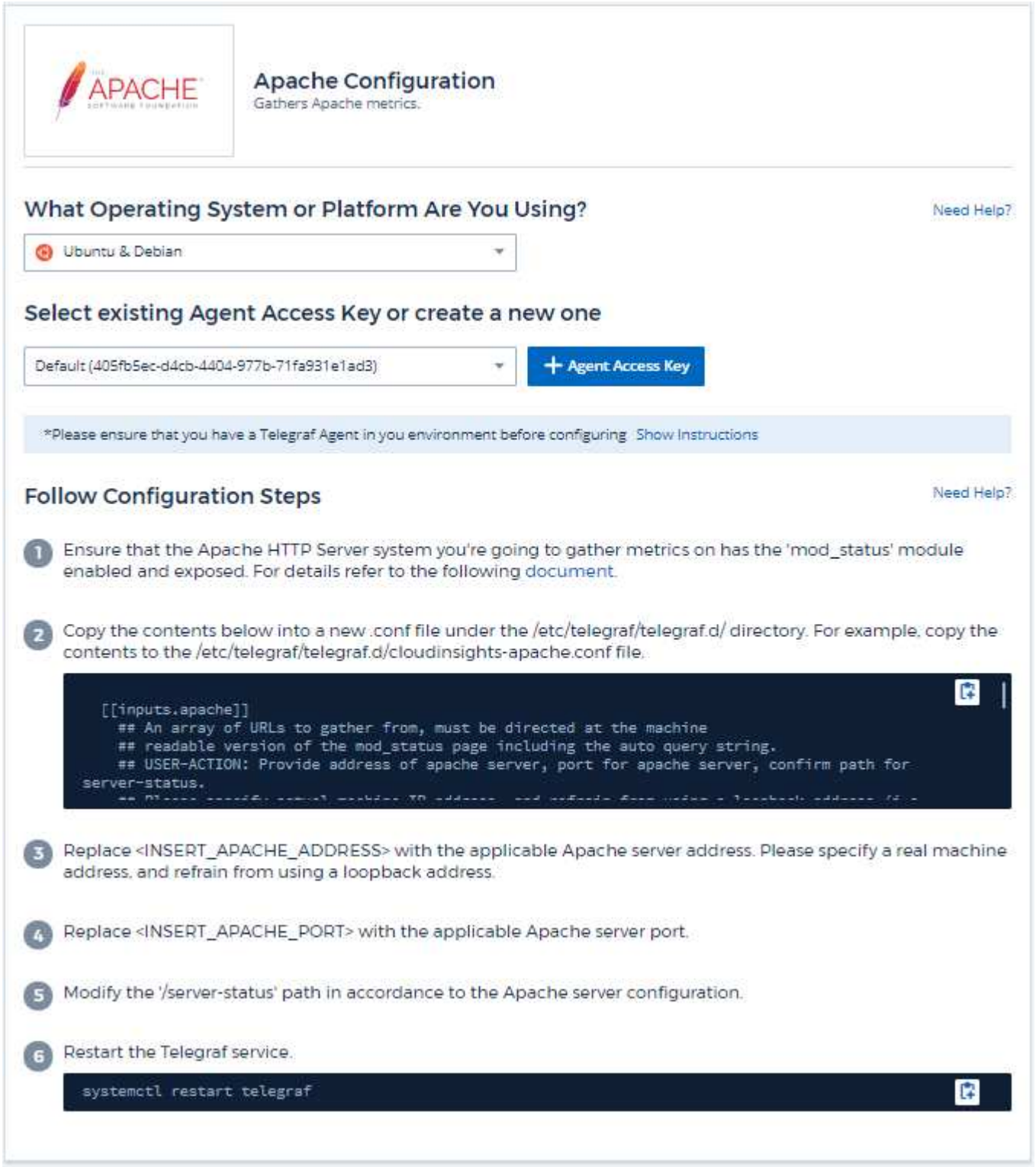
1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Apache.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

O plugin do Telegraf para o servidor HTTP do Apache depende do módulo 'od_status' para ser ativado. Quando isso estiver ativado, o servidor HTTP do Apache irá expor um endpoint HTML que pode ser visualizado no seu navegador ou raspado para extração do status de todas as configurações do servidor HTTP do Apache.

Compatibilidade:

A configuração foi desenvolvida em relação ao servidor HTTP do Apache versão 2,4.38.

Ativar mod_status:

Ativar e expor os módulos 'od_status' envolve duas etapas:

- Módulo de ativação
- Expondo estatísticas do módulo

Módulo de ativação:

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 do 'mod_status' é controlada pelo arquivo de configuração sob '/usr/local/apache2/conf/extra/httpd-info.conf'. Certifique-se de que você tem o seguinte 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 'od_status', consulte "Documentação do Apache"

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Apache	Servidor de namespace	O tempo de atividade do servidor principal da geração do servidor principal do servidor de geração MPM do nó IP está a parar	Workers ocupados bytes por solicitação bytes por segundo CPU Crianças sistema CPU Crianças Usuário CPU carga CPU sistema CPU usuários conexões assíncronas fechando conexões assíncronas manter Alive 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

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

Consul Data Collector

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

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Cônsul.

   Se você não tiver configurado um Agente para coleta, será solicitado "instale um agente"ao locatário.

   Se você já tiver um agente configurado, selecione o sistema operacional ou a Plataforma apropriada e clique em **continuar**.

2. Siga as instruções na tela Consul Configuration (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.

Configuração

As informações podem ser encontradas no "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 ID de verificação de namespace	Nó IP nó os nó UUUID Nome do nó Serviço Nome verificar Nome ID do serviço Status	Aviso de aprovação crítica

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

Coletor de dados Couchbase

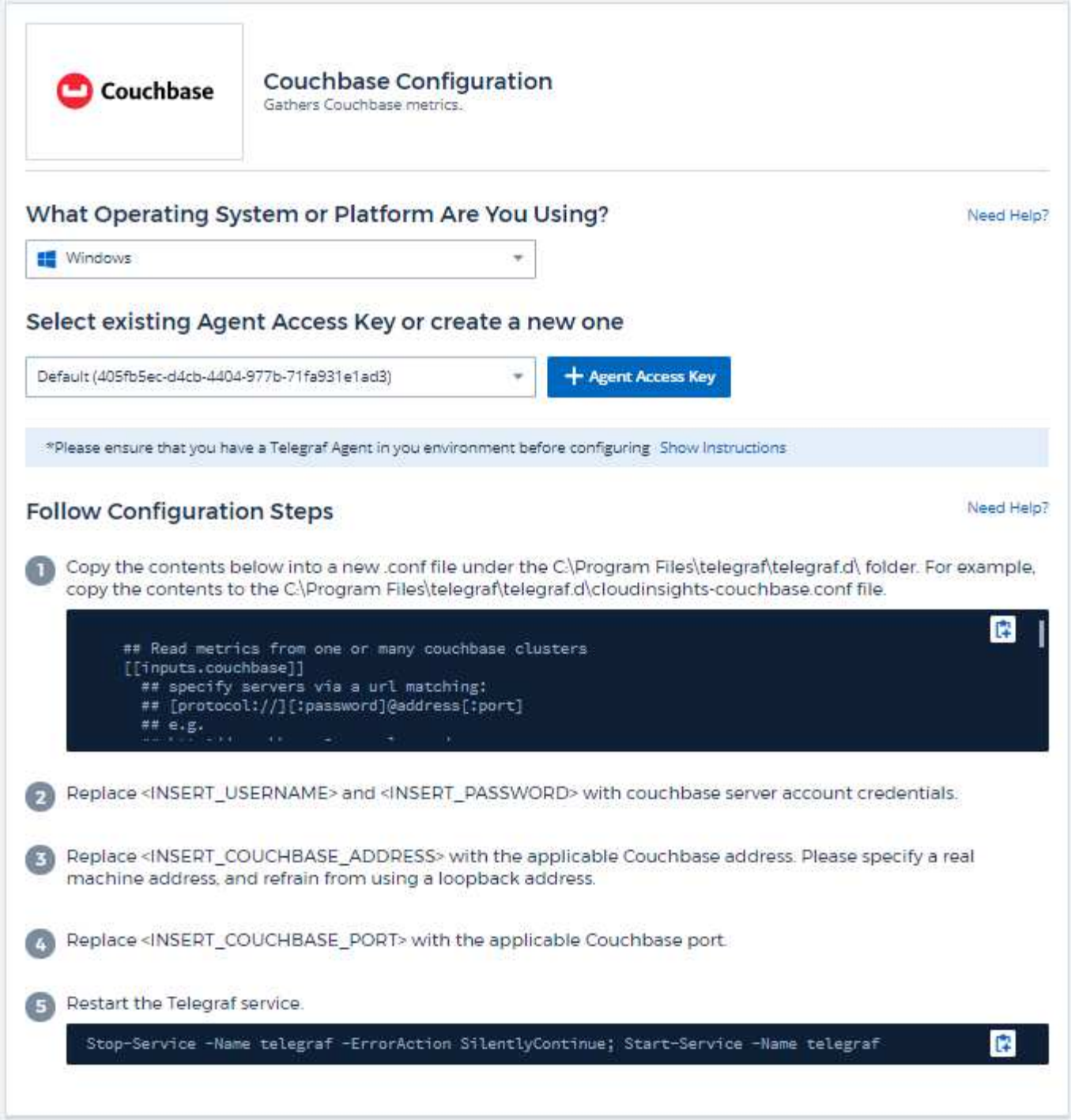
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Couchbase.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Couchbase.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

As informações podem ser encontradas no "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 Couchbase do namespace Cluster	IP do nó de nome do nó	Memória livre Total de memória
Balde Couchbase	Cluster de bucket do namespace	IP do nó de nome do nó	Dados usados dados Registros disco usado contagem de itens memória operações usadas por segundo cota usada

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

CouchDB Data Collector

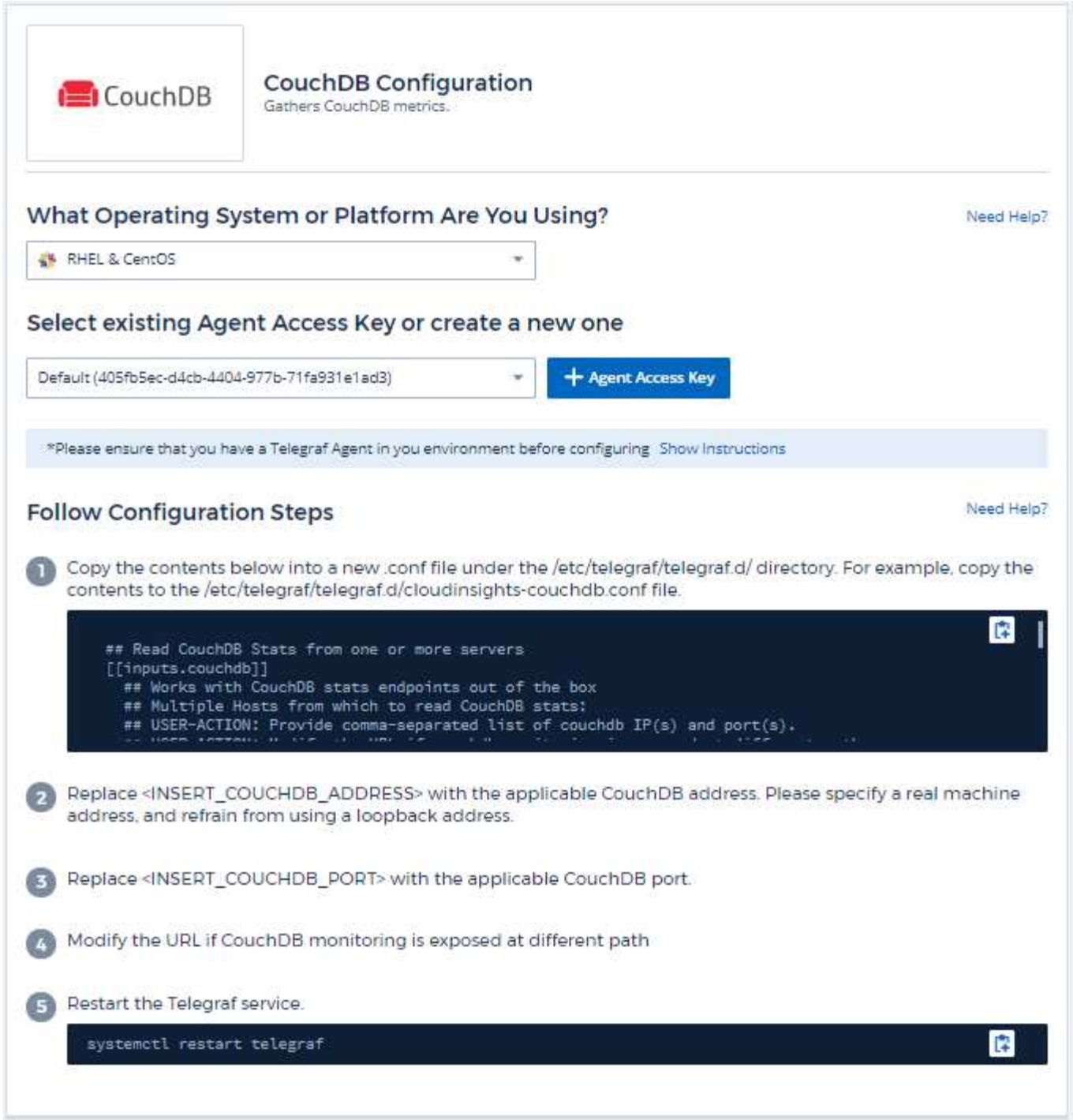
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do CouchDB.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha CouchDB.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

As informações podem ser encontradas no "Documentação do CouchDB".

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
CouchDB	Servidor de namespace	IP do nó de nome do nó	Autenticação Cache Hits Autenticação Cache Miss Banco de dados lê Banco de dados escreve bancos de dados abrir arquivos do sistema operacional tempo máximo pedido min tempo de solicitação httpd métodos Copiar httpd Request métodos Excluir httpd Request métodos obter httpd Request métodos Head httpd Request métodos Post httpd Request métodos put Status Codes 200 405 500 Status Codes 304 403 409 Status Codes 400 404 412 Status Codes 401 Status 202 Status Codes 301 Status 201 Status Codes

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

Docker Data Collector

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

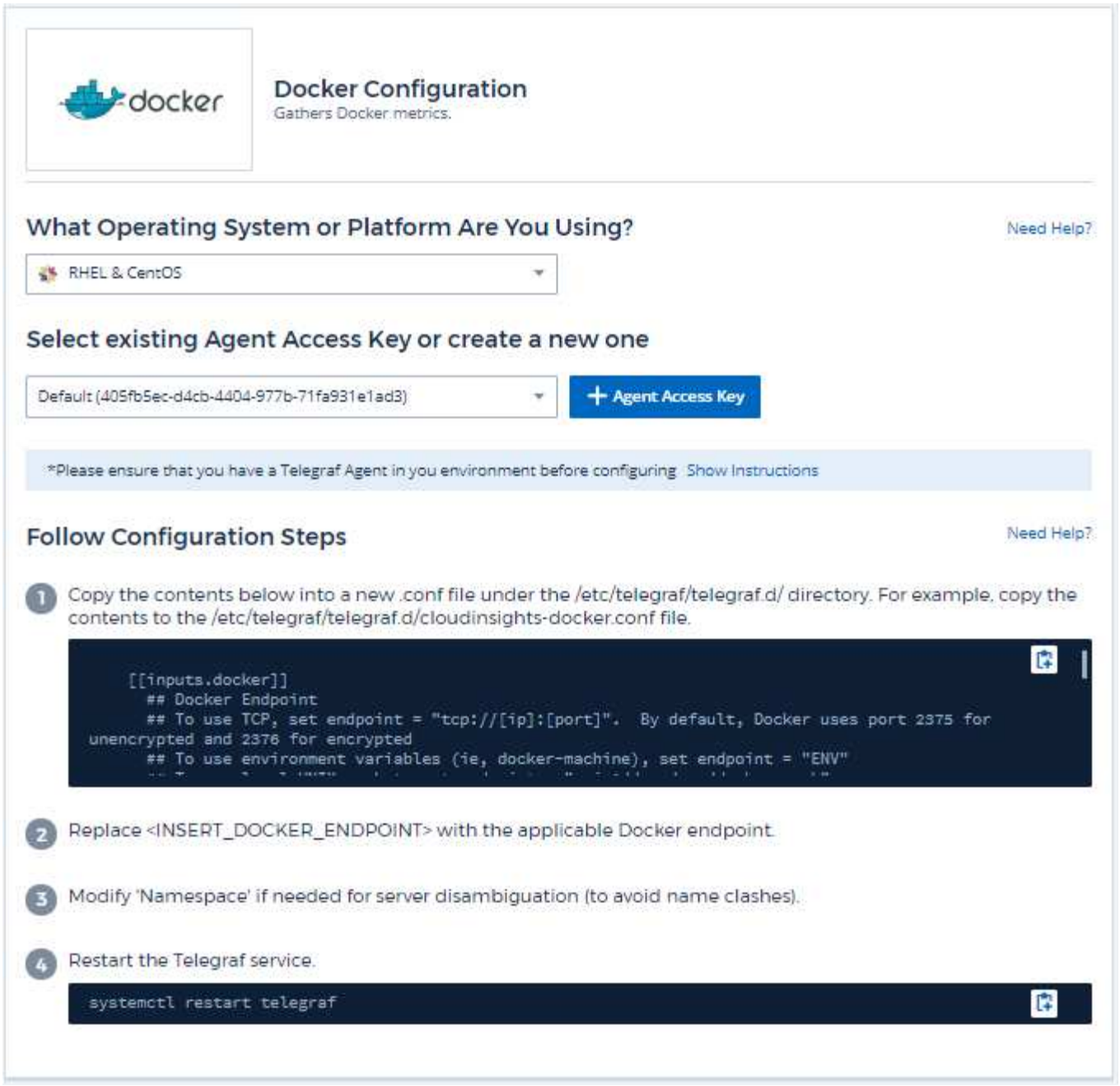
Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Docker.

   Se você não tiver configurado um Agente para coleta, será solicitado "instale um agente"ao locatário.

   Se você já tiver um agente configurado, selecione o sistema operacional ou a 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

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

Compatibilidade

A configuração foi desenvolvida em relação ao Docker versão 1.12.6.

Configuração

Acessando o Docker através de um soquete UNIX

Se o agente Telegraf estiver sendo executado no baremetal, adicione o usuário Unix telegraf ao grupo Unix docker executando o seguinte:

```
 sudo usermod -aG docker telegraf
Se o agente Telegraf estiver sendo executado em um pod Kubernetes, exponha o soquete Unix do Docker 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 recipiente:

```
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 endpoint 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:
Docker Engine	Motor Docker de namespace	Nó Nome nó nó IP UUUID Node os Kubernetes Cluster Docker Version Unit	Contentores de memória Containers usados Containers em execução Containers parados CPUs Go Routines imagens Listener Eventos usado descritores de Arquivo dados disponíveis dados totais dados usados metadados disponíveis metadados Total metadados metadados metadados Total metadados usado Pool blocksize
Contêiner do Docker	Nome do contêiner do namespace Docker Engine	Kubernetes Container Hash Kubernetes Container Ports Kubernetes Container Restart Count Kubernetes Container Termination Message Path Kubernetes Container Termination Message Policy Kubernetes Pod Termination Quote Container Image Container Status Container Status Container Version Node Name Kubernetes Container Log Path	Memória ativa memória anônima memória ativa memória Cache memória limite hierárquico memória inativa memória inativa Arquivo inativo memória memória memória mapeada memória máxima utilização memória Página Falha memória memória Principal memória pagada memória pagada na memória memória
Docker Container Block io	Nome do contentor Nome do dispositivo Docker Engine	Kubernetes Container Hash Kubernetes Container Ports Kubernetes Container Restart Count Kubernetes Container Termination Message Path Kubernetes Container Termination Message Policy Kubernetes Pod Termination Grace Period Container Image Container Status Container Status Container Version Node Name Kubernetes Container Log Path	Io Service bytes recursive Async io Service bytes recursive Read io Service bytes recursive Sync io Service bytes recursive Total io Service bytes recursive Write io recursive IO Serviced recursive Read IO Serviced Sync io recursive resposta recursiva IO de resposta recursiva Total io Write recursive

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Docker Container Network	Nome do contentor do namespace Network Docker Engine	Container Image Container Status Container Version Node Name Node IP Node UUUID Node os K8s Cluster Docker Version Container ID	RX dropped RX bytes RX erros RX pacotes RX TX dropped TX bytes TX erros TX pacotes TX
CPU de contêiner do Docker	Nome do contêiner do namespace CPU Docker Engine	Kubernetes Container Hash Kubernetes Container Ports Kubernetes Container Restart Count Kubernetes Container Termination Message Path Kubernetes Container Termination Message Policy Kubernetes Pod Termination Quote Form Grace Period Kubernetes Config seen Kubernetes Config	Estrangulamento períodos estrangulados estrangulados períodos estrangulados utilização do tempo estrangulado no modo Kernel utilização no modo Utilizador percentagem utilização do sistema Total de utilização

Solução de problemas

Problema:	Tente 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 do Telegraf para ver se ele relata o seguinte erro: E! Erro no plugin [inputs.Docker]: Obteve permissão negada ao tentar se conetar ao socket do daemon do Docker, se isso acontecer, siga as etapas necessárias para fornecer ao agente Telegraf acesso ao socket Unix do Docker, conforme especificado acima.

Informações adicionais podem ser encontradas na "Suporte"página.

Elasticsearch Data Collector

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

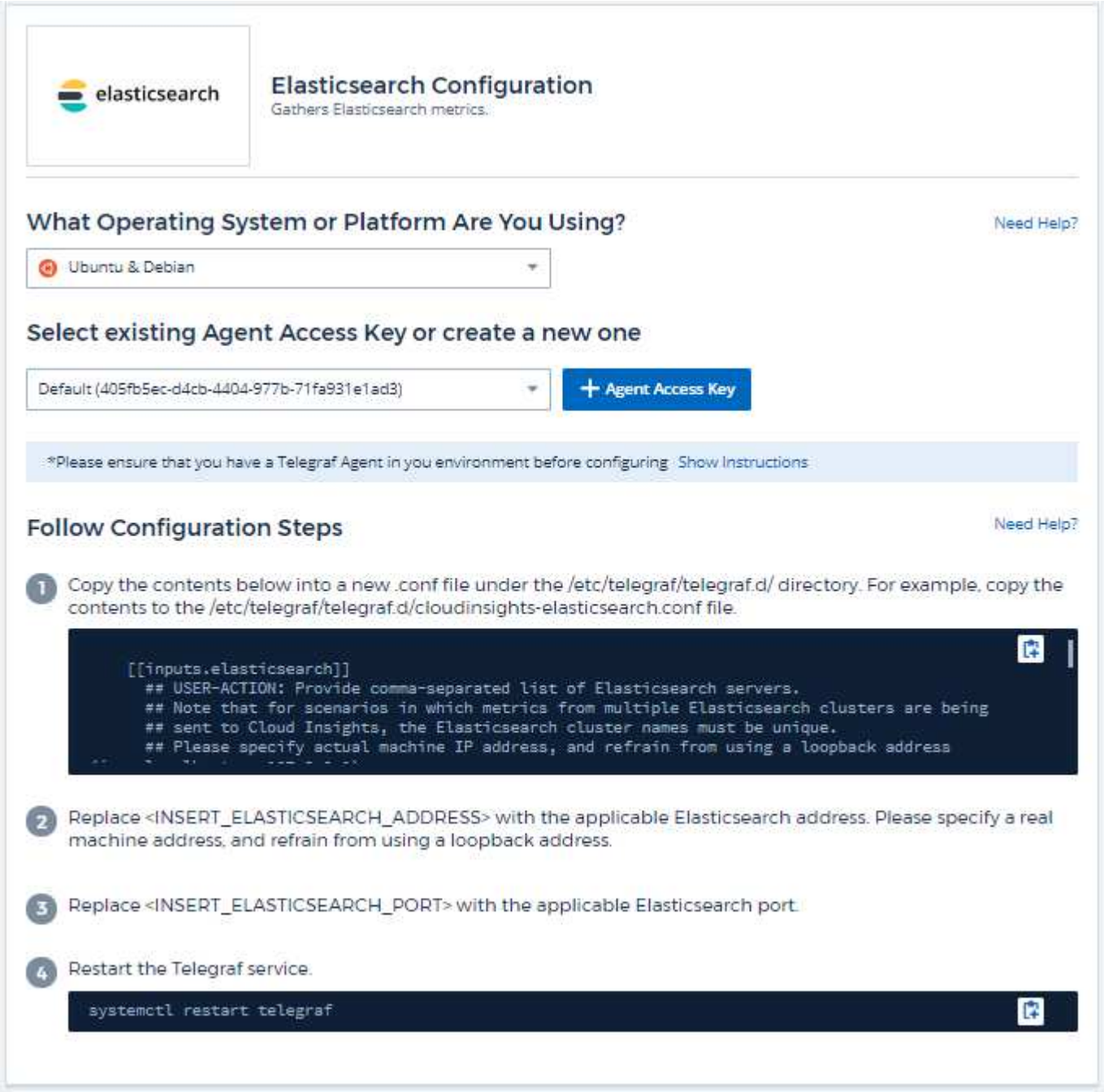
1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Elasticsearch.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada:

Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

As informações podem ser encontradas no "Documentação do Elasticsearch".

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

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

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

Flink Data Collector

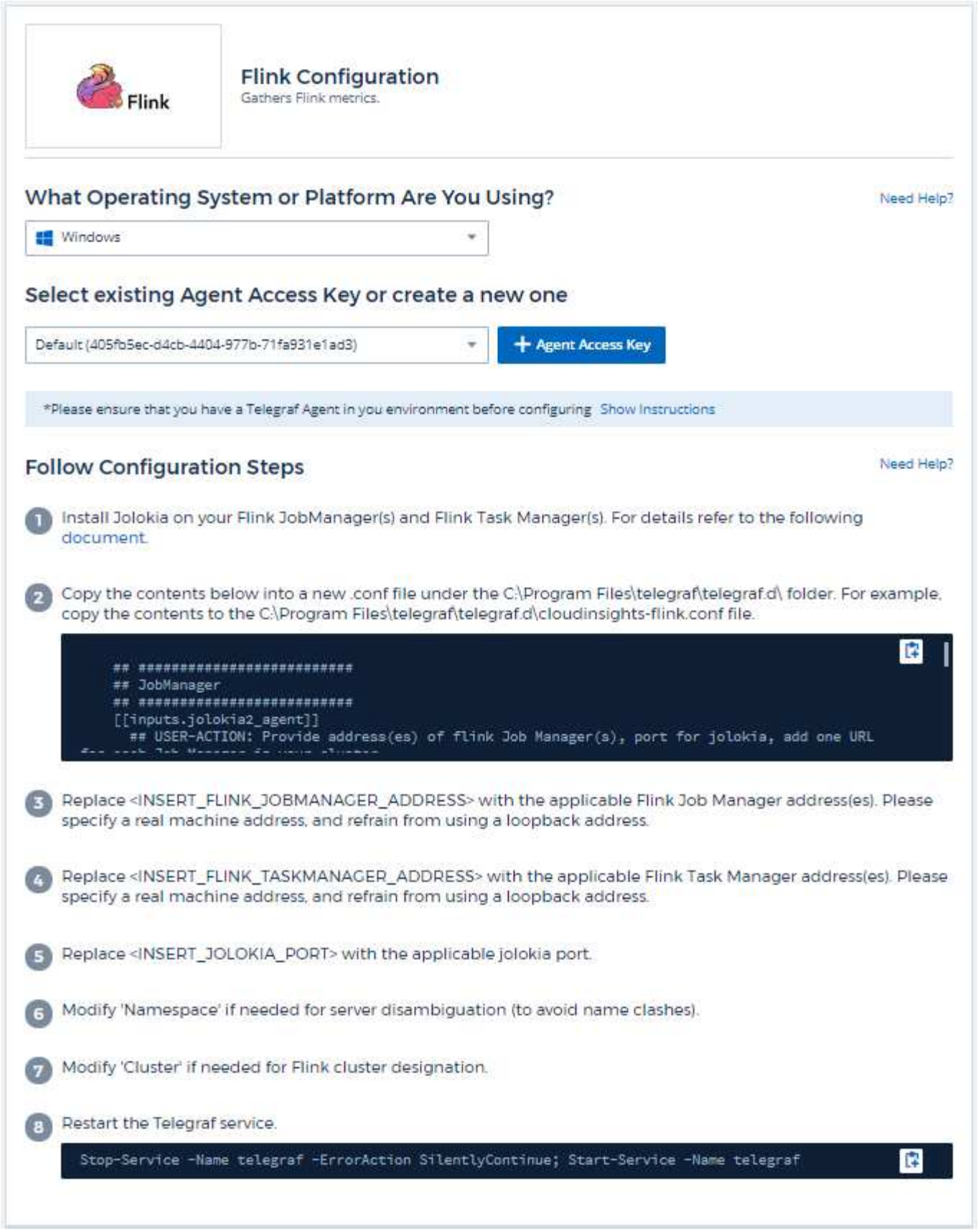
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Flink.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Flink.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

Uma implantação completa do Flink envolve os seguintes componentes:

JobManager: O sistema primário Flink. Coordena uma série de TaskManagers. Em uma configuração de alta disponibilidade, o sistema terá mais de um JobManager. TaskManager: É aqui que os operadores Flink são executados. O plugin Flink é baseado no plugin Jolokia da telegraf. Como um requisito para reunir 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 em relação ao Flink versão 1,7.0.

Configuração

Jolokia Agent JAR

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

As instruções abaixo supõem que o arquivo jar baixado (jolokia-jvm-1,6.0-Agent.jar) é colocado sob a localização '/opt/flink/lib/'.

JobManager

Para configurar o JobManager para expor a API 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 tem um
IP interno para bloquear Jolokia, você pode substituir o "Catch All"
0.0.0.0 pelo seu próprio IP. Observe que esse IP precisa ser acessível a
partir do plugin telegraf.
```

TaskManager

Para configurar o(s) TaskManager(s) para expor a API Jolokia, você pode configurar a seguinte variável de ambiente nos 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 tem um
IP interno para bloquear Jolokia, você pode substituir o "Catch All"
0.0.0.0 pelo seu próprio IP. Observe que esse IP precisa ser acessível a
partir do plugin telegraf.
```

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Flink Task Manager	Servidor de namespace de cluster	Nome do nó IP do nó de ID do Gestor de tarefas	Rede disponível segmentos de memória rede Total segmentos de memória coleção de lixo PS MarkSweep contagem de lixo PS MarkSweep tempo coleta de lixo contagem de scavenge contagem de lixo contagem de lixo PS scavenge tempo Heap memória comprometida memória de Heap memória de Heap máximo memória de heap usada contagem de threads Daemon contagem de threads contagem de threads contagem de threads Total de threads iniciado
Trabalho Flink	ID do trabalho do servidor de namespace do cluster	Nome do nó Nome do trabalho Nome do nó IP último Checkpoint caminho Externo tempo de reinício	Tempo de inatividade reinicializações completas último alinhamento do Checkpoint Buffered Last Checkpoint duração último tamanho do Checkpoint número de Checkpoints concluídos número de Checkpoints falhados número de Checkpoints em curso número de Checkpoints uptime
Flink Job Manager	Servidor de namespace de cluster	IP do nó de nome do nó	Coleção de lixo PS MarkSweep contagem de lixo PS MarkSweep tempo coleta de lixo contagem de scavenge contagem de lixo PS scavenge tempo Heap memória comprometida memória de heap memória de Heap máximo memória de heap usada número registrado Gerenciadores de tarefas em execução Slots de tarefa disponíveis contagem de

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Tarefa Flink	ID da tarefa do ID da tarefa do namespace do cluster	Nome do nó do servidor Nome do trabalho Sub-tarefa Indice tentativa da tarefa número da tentativa da tarefa Nome da tarefa Gestor de tarefas ID nó IP atual marca de água da entrada	Buffers em uso do pool Buffers em comprimento da fila Buffers out uso do pool Buffers out comprimento da fila número Buffers em número local Buffers em número local por segundo número número Buffers em número local por segundo número de taxa Buffers em número remoto por segundo número de contagem de Registros por segundo número local por segundo número de Registros por segundo número remoto por segundo número de Registros por segundo número
Operador tarefa Flink	ID da tarefa ID do operador do namespace do cluster	Nome do nó do servidor Nome do trabalho Nome do Operador Sub-tarefa ID tentativa da tarefa número tentativa da tarefa Nome da tarefa Nome da tarefa Gestor de tarefas ID Node IP	Entrada atual marca de água saída atual número de marca de água Registos em número Registos em por segundo número de contagem Registos em por segundo número de registo para fora número de contagem número de registos para fora por segundo número de taxa de registo

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

Coletor de dados Hadoop

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

Instalação

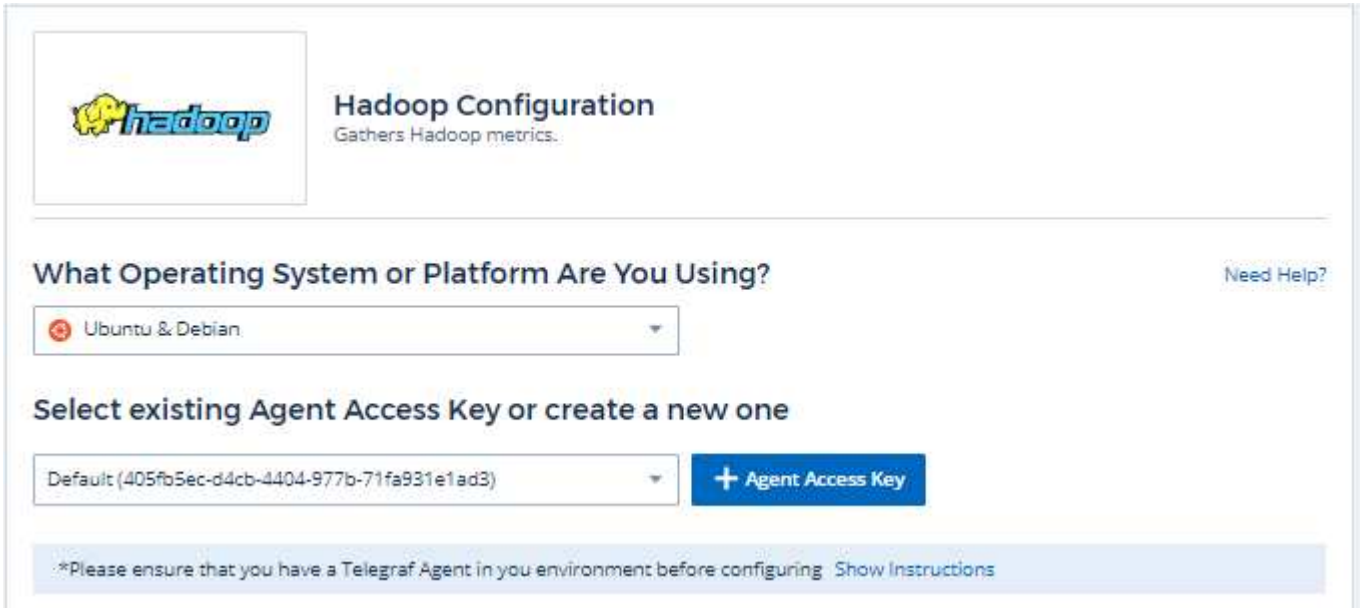
1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Hadoop.

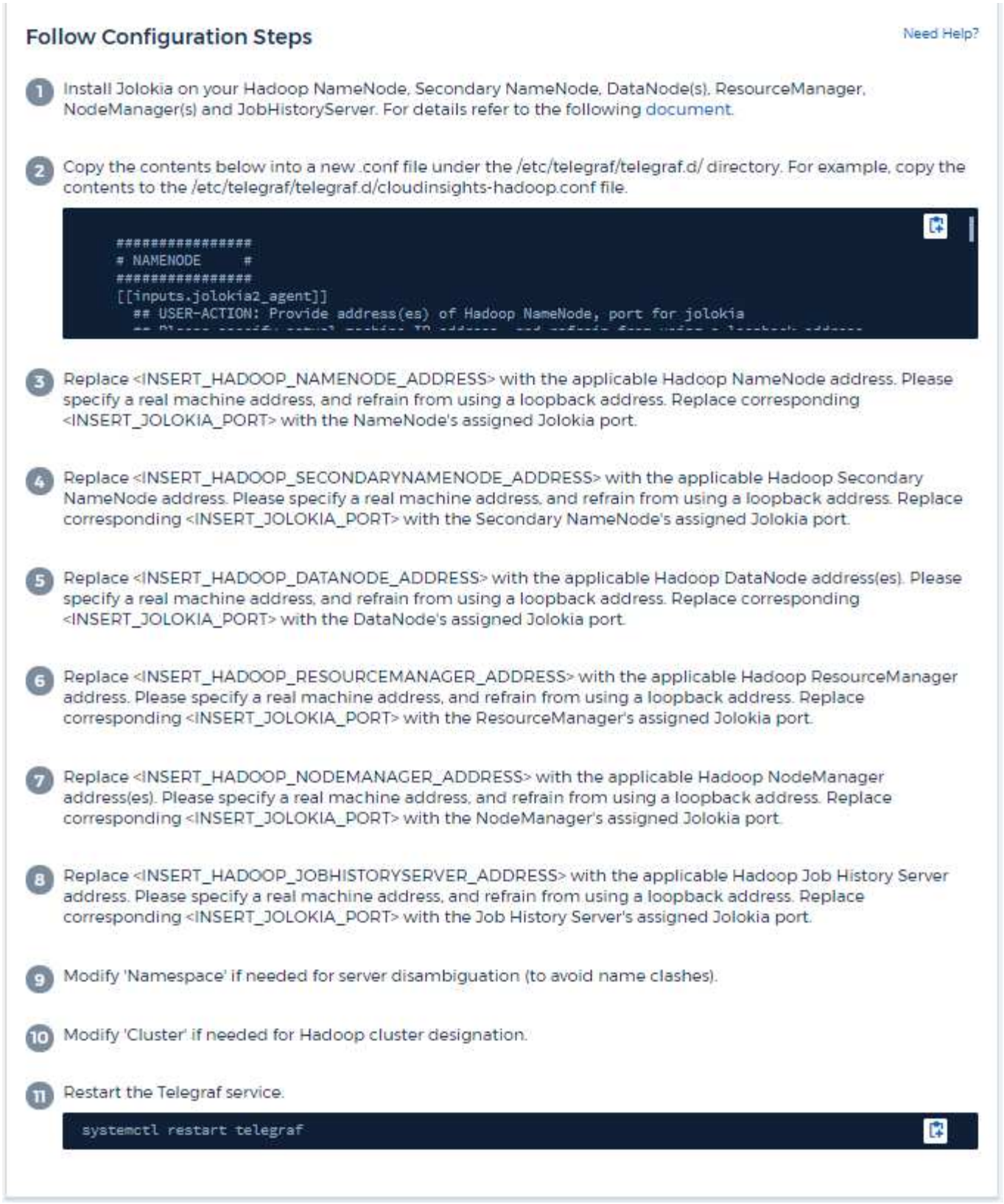
   Selecione o sistema operacional ou a plataforma na qual o agente Telegraf está instalado.

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema

operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

Uma implantação completa do Hadoop envolve os seguintes componentes:

- NameNode: O sistema principal do Hadoop Distributed File System (HDFS). Coordena uma série de DataNodes.

- NameNode secundário: Um failover morno para o NameNode principal. No Hadoop, a promoção para NameNode não ocorre automaticamente. NameNode secundário reúne 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. Local real para execução de aplicativos.
- JobHistoryServer: Responsável por atender todas as solicitações relacionadas ao histórico de tarefas.

O plugin Hadoop é baseado no plugin Jolokia da telegraf. Como um requisito para reunir 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 em relação ao Hadoop versão 2,9.2.

Configuração

Jolokia Agent JAR

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

As instruções abaixo supõem que o arquivo jar baixado (jolokia-jvm-1,6.0-Agent.jar) é colocado sob o local '/opt/hadoop/lib/'.

NameNode

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.
```

NameNode secundário

Para configurar o NameNode secundário 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.
```

DataNode

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.
```

ResourceManager

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.
```

NodeManager

Para configurar o 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.
```

JobHistoryServer

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:
NameNode secundário Hadoop	Servidor de namespace de cluster	Node Name Node IP Compile Info versão
Hadoop NodeManager	Servidor de namespace de cluster	IP do nó de nome do nó
Hadoop ResourceManager	Servidor de namespace de cluster	IP do nó de nome do nó
DataNode do Hadoop	Servidor de namespace de cluster	Versão do ID do cluster IP do nó de nome do nó
NameNode Hadoop	Servidor de namespace de cluster	ID da transação IP do nó Nome do nó último tempo escrito desde a última versão carregada Edits HA State File System State Block Pool ID Cluster Info compilação versão contagem de versão distinta
Hadoop JobHistoryServer	Servidor de namespace de cluster	IP do nó de nome do nó

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

Coletor de dados HAProxy

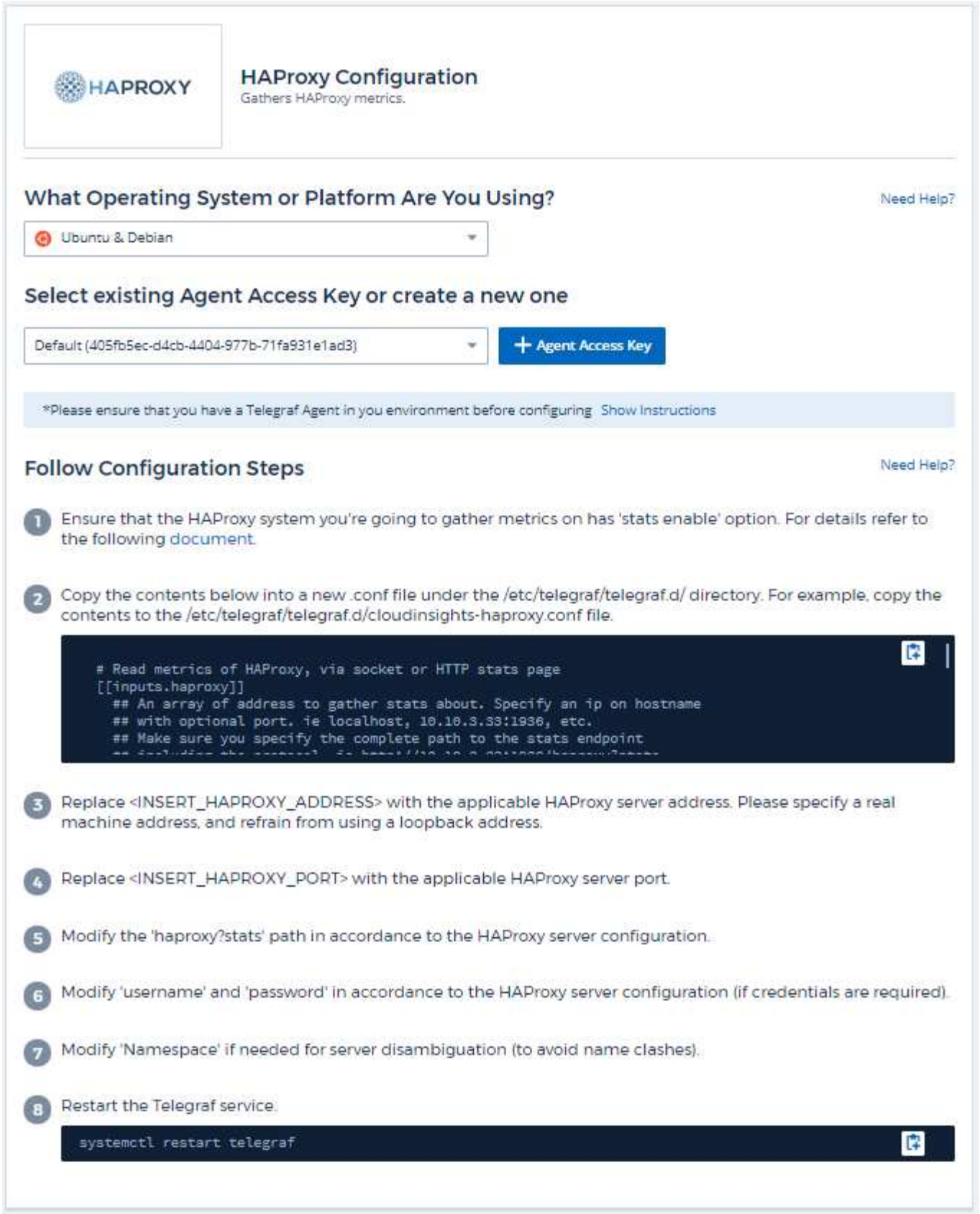
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do HAProxy.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha HAProxy.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

O plugin da Telegraf para HAProxy depende da habilitação do HAProxy Stats. Esta é uma configuração incorporada no HAProxy, mas não está ativada fora da caixa. Quando ativado, o HAProxy irá expor um

endpoint HTML que pode ser visualizado no seu navegador ou eliminado para extração do estado de todas as configurações do HAProxy.

Compatibilidade:

A configuração foi desenvolvida contra o HAProxy versão 1,9.4.

Configuração:

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

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

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

```
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:
HAProxy Frontend	Proxy de endereço de namespace	Nome do nó IP do nó Proxy ID Mode Process id Sessions Rate Limit Server id Sessions Limit Status	Bytes in bytes out Cache Hits Cache Lookups Compression bytes Bypass Compression bytes out Compression bytes out Compression respostas taxa de conexão Max conexões Total de solicitações negadas pela regra de conexão solicitações negadas por preocupações de segurança solicitações negadas por solicitações de regras de sessão erros respostas 1xx 4xx respostas 2xx 5xx respostas 3xx respostas outras solicitações sessões intercetadas sessões Rate Requests Rate Requests Rate Max Total de sessões sessões reescreve

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Servidor HAProxy	Servidor Proxy de Endereço de namespace	Node IP Name Check Time to Finish Check Fall Configuration Check Health Value Check Rise Configuration Check Status ID Proxy ID Last Change Time Last Session Time Process id Server id Status Weight	Servidores ativos servidores de backup bytes em bytes out check Downs Check Fails Cliente aborta conexões tempo médio tempo de inatividade Total respostas negadas erros de conexão respostas 1xx respostas 2xx respostas 3xx respostas 4xx respostas 5xx respostas outro servidor selecionado Total fila atual fila máxima tempo média sessões por segundo sessões por segundo tempo máximo reutilização de conexão tempo média sessões sessões sessões sessões Max transferência de servidor aborta sessões Total de sessões Redespachos pedidos Redespachos pedidos RRecrutamento de solicitações
Backend HAProxy	Proxy de endereço de namespace	Nome do nó IP ID do proxy último tempo alteração tempo último modo sessão ID do processo ID do servidor sessões limite peso do estado	Servidores ativos servidores de backup bytes em bytes out Cache Hits Cache Lookups Check Downs Cliente aborta compactação bytes Bypass compactação bytes em compressão bytes out Compression respostas conexões tempo médio tempo de inatividade Total solicitações negadas por preocupações de Segurança respostas negadas por preocupações de Segurança erros de conexão erros de resposta respostas 1xx 4xx respostas 2xx 5xx respostas 3xx respostas

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

Coletor de dados JVM

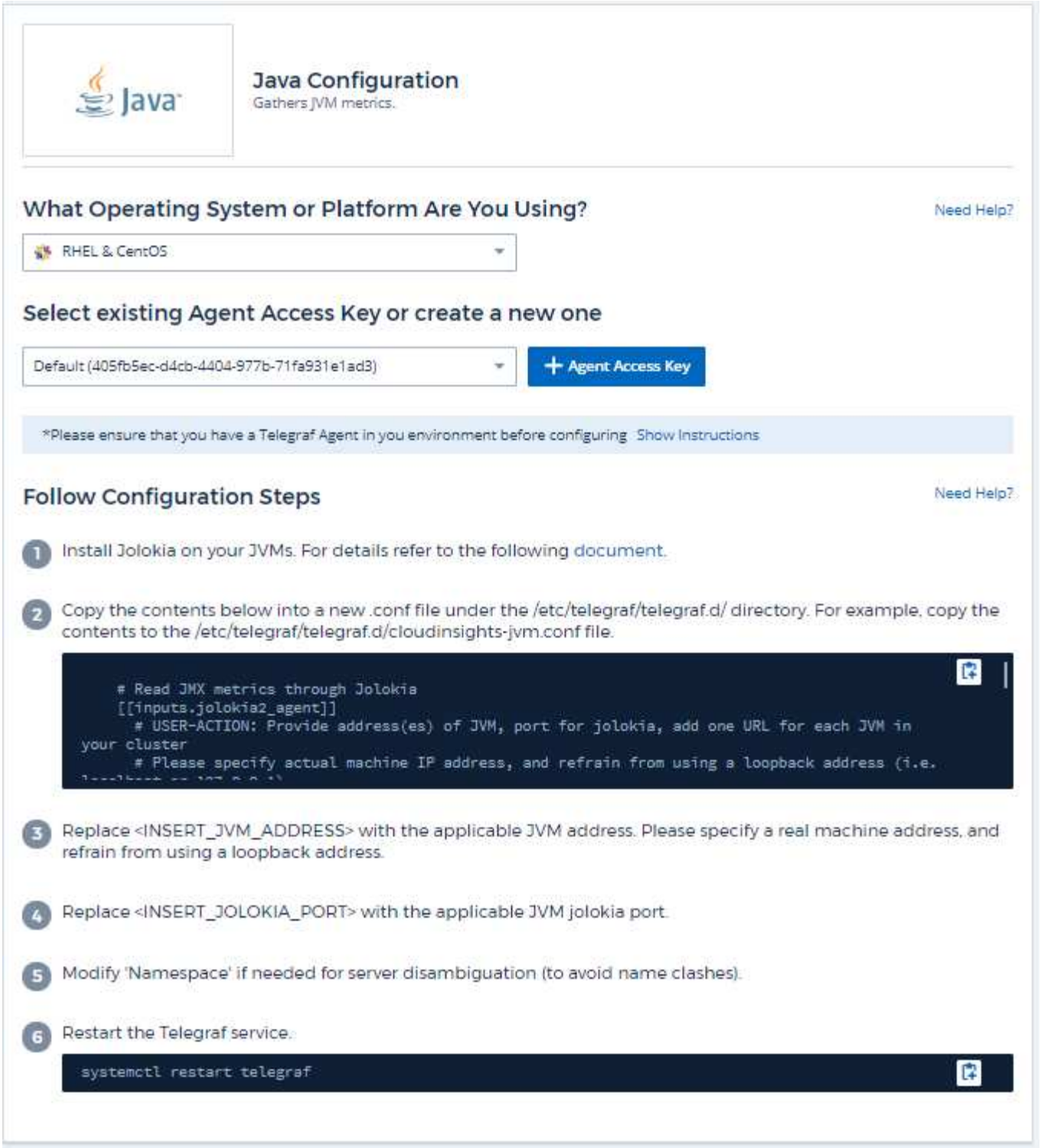
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas da JVM.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha JVM.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

As 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	JVM do namespace	Arquitetura OS Nome do SO versão Runtime especificação Runtime especificação Runtime do fornecedor Runtime especificação versão tempo de execução VM Nome tempo de execução VM Nome tempo de execução VM Vendor Runtime versão VM Nome nó IP	Classe carregada Classe carregada Total Class Unloaded Memory Heap Consolidated Memory Heap Init Memory Heap used Max Memory Heap used Memory Non Heap Consolidated Memory Non Heap Init Memory Non Heap Max Memory Non Heap used Memory Objects Pending G1 Sequence os Processors Available G1 G1 G1

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

Kafka Data Collector

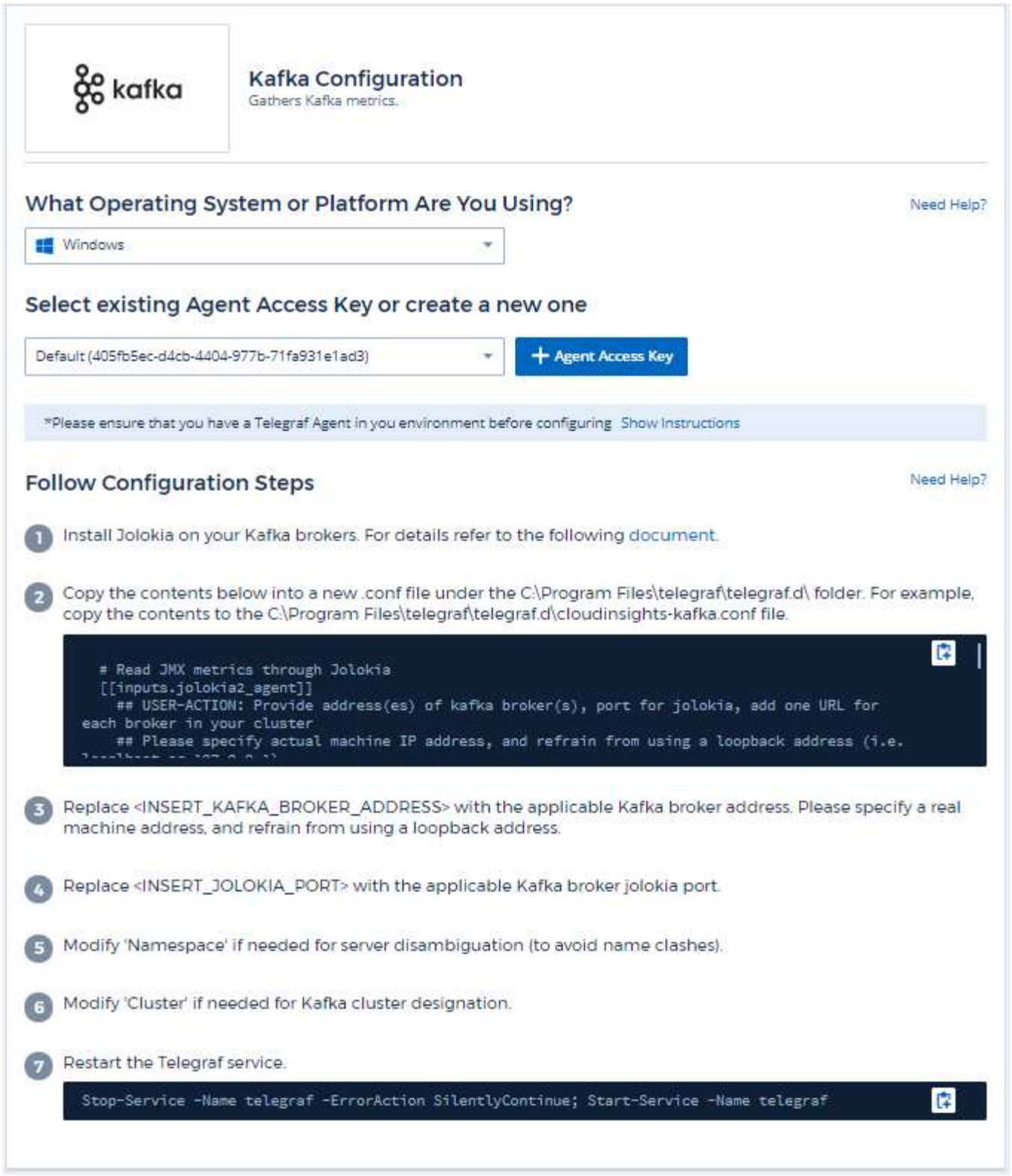
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Kafka.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Kafka.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

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

Compatibilidade

A configuração foi desenvolvida em relação ao Kafka versão 0.11.0.2.

Configuração

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

Jolokia Agent JAR

Uma versão o arquivo jar do agente Jolokia deve ser "transferido". A versão testada foi o agente Jolokia 1,6.0.

As instruções abaixo supõem que o arquivo jar baixado (jolokia-jvm-1,6.0-Agent.jar) é colocado sob o local '/opt/kafka/libs/'.

Kafka Brokers

Para configurar o Kafka Brokers para expor a API Jolokia, você pode adicionar o seguinte em <KAFKA_HOME>/bin/kafka-server-start.sh, imediatamente 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 várias máquinas IP, isso precisará ser ajustado para reunir o IP que você se importa para conexões RMI.

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

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:
Kafka Broker	Agente de namespace de cluster	IP do nó de nome do nó

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

Kibana Data Collector

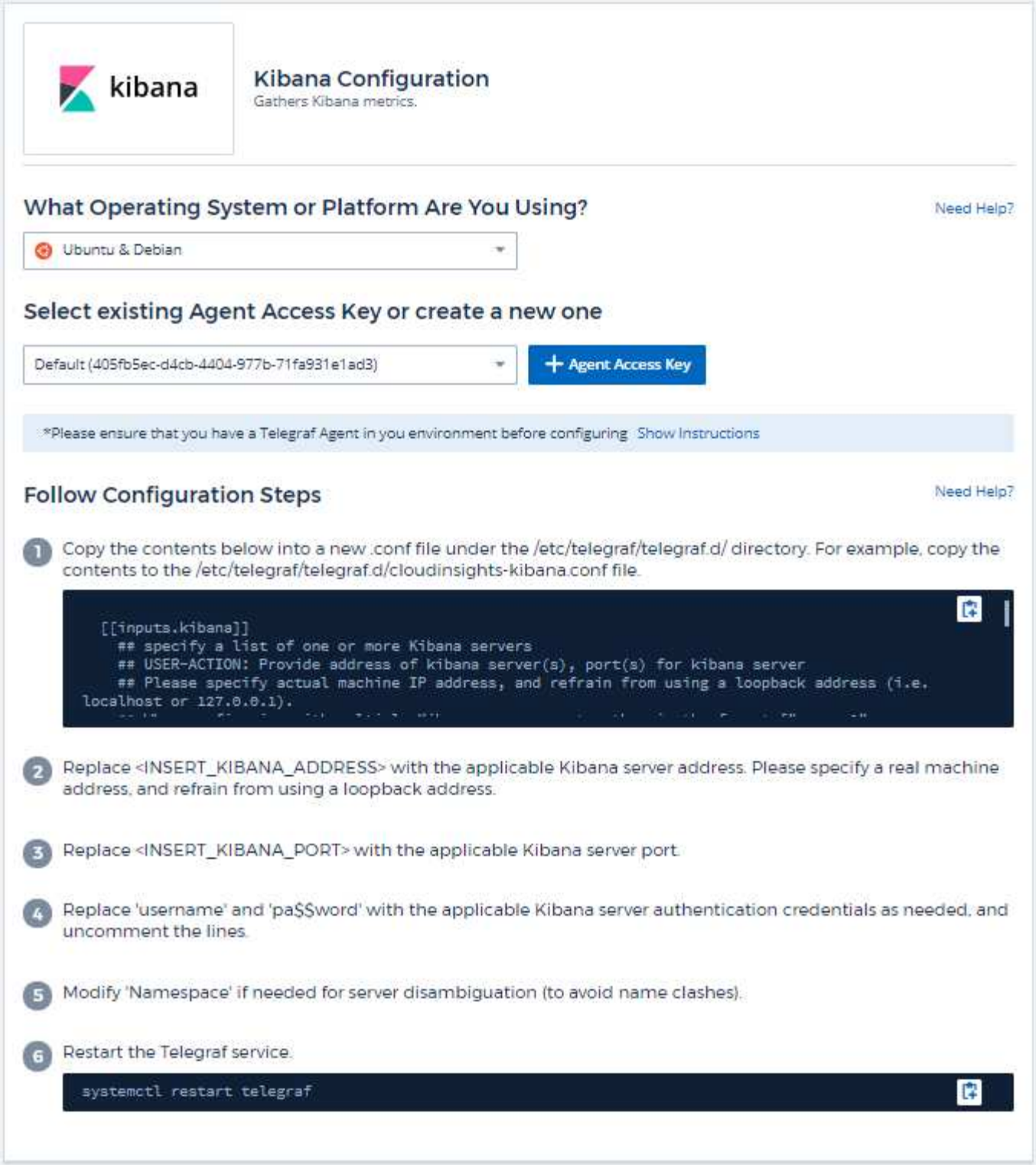
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas da Kibana.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Kibana.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

As informações podem ser encontradas no "Documentação do Kibana".

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Kibana	Endereço do namespace	Estado da versão do nome do nó IP do nó	Conexões simultâneas Heap Max Heap usou solicitações por segundo tempo de resposta tempo de resposta tempo de resposta tempo de resposta tempo de resposta máximo de tempo de atividade

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

Instalação e configuração do operador de monitoramento Kubernetes

O Data Infrastructure Insights oferece a coleção **Operador de Monitoramento do Kubernetes** para Kubernetes. Navegue até **Kubernetes > Collectors > Kubernetes Collector** para implantar um novo operador.

Antes de instalar o operador de monitoramento do Kubernetes

Consulte "Pré-requisitos"a documentação antes de instalar ou atualizar o Operador de Monitoramento do Kubernetes.

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	Namespace
clustername	netapp-monitoring

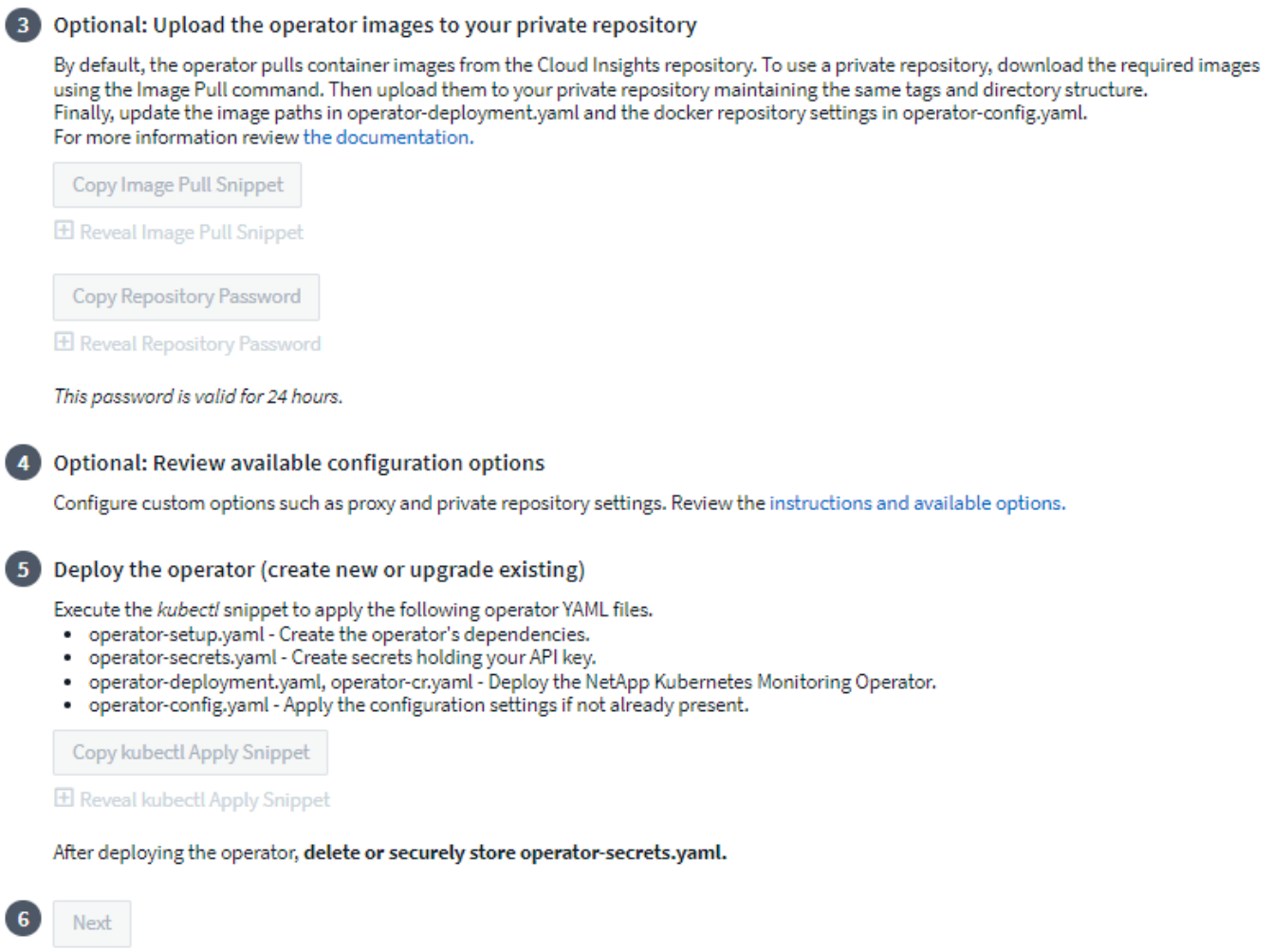
2 Download the operator YAML files

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 a atualizar é de um operador Kubernetes anterior, use o mesmo nome de cluster e namespace.
2. Uma vez que eles são inseridos, você pode copiar o snippet de comando de download para a área de transferência.
3. Cole o snippet em uma janela *bash* e execute-o. Os ficheiros de instalação do Operador serão transferidos. Observe que o snippet tem uma chave exclusiva e é válido por 24 horas.
4. Se você tiver um repositório personalizado ou privado, copie o trecho opcional Image Pull, cole-o em um shell *bash* e execute-o. Depois que as imagens tiverem sido puxadas, copie-as para o 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 docker em *operator-config.yaml*.
5. Se desejar, revise as opções de configuração disponíveis, como proxy ou configurações de repositório privado. Você pode ler mais sobre "opções de configuração".
6. Quando estiver pronto, implante o Operador copiando o snippet de aplicação kubectl, baixando-o e executando-o.
7. A instalação prossegue automaticamente. Quando estiver concluído, clique no botão *Next*.
8. Quando a instalação estiver concluída, clique no botão *Next*. Certifique-se também de excluir ou armazenar com segurança o arquivo *operator-secrets.yaml*.

Se estiver usando um proxy, leia sobre configurando proxy.

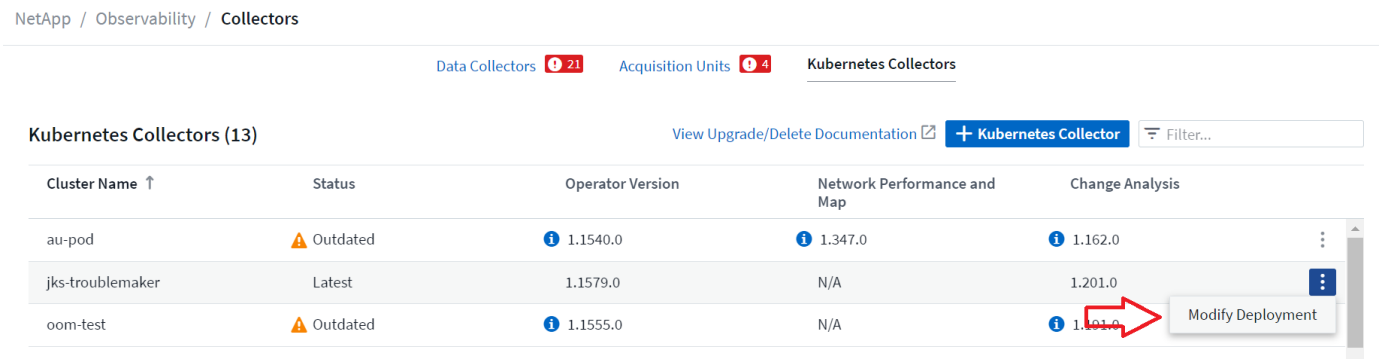
Se você tiver um repositório personalizado, leia sobre usando um repositório docker personalizado/privado.

Componentes de monitoramento do Kubernetes

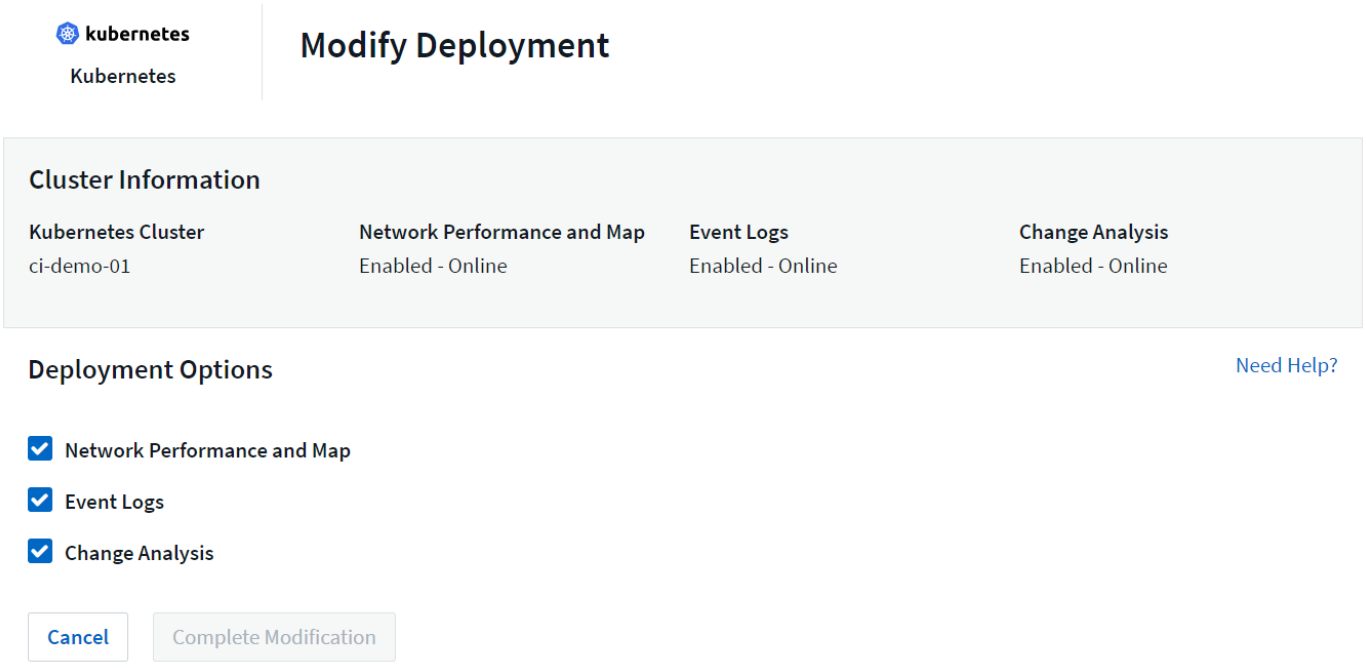
O monitoramento do Kubernetes do Data Infrastructure Insights é composto por quatro componentes de monitoramento:

- Métricas do cluster
- Desempenho de rede e mapa (opcional)
- Registos de eventos (opcional)
- Análise de mudança (opcional)

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



O ecrã mostra o estado atual de cada componente e permite desativar ou ativar componentes para esse coletor, conforme necessário.



Atualização para o operador de monitoramento mais recente do Kubernetes

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

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

- Instale O operador mais recente sobre o operador existente.
  - Certifique-se de que está puxando as imagens mais recentes do recipiente se estiver a utilizar um repositório personalizado.

Se o AgentConfiguration não existir:

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

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Crie uma cópia de segurança do Operador existente (se o seu namespace
não for o NetApp-monitoring predefinido, substitua o 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,Instale>> O operador
mais recente.
```

  - Use o mesmo nome de cluster.
  - Depois de baixar os arquivos YAML do Operador mais recentes, coloque as personalizações encontradas no Agent_backup.yaml para o operador-config.yaml baixado antes de implantar.
  - Certifique-se de que está puxando as imagens mais recentes do recipiente se estiver a utilizar um repositório personalizado.

Parando e iniciando o Operador de Monitoramento do Kubernetes

Para parar 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
```

Desinstalação

Para remover o operador de monitoramento do Kubernetes

Observe que o namespace padrão para o Operador de Monitoramento do Kubernetes é "NetApp-monitoring". Se você tiver definido seu próprio namespace, substitua esse namespace nesses e todos os comandos e arquivos subsequentes.

As 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>
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 "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 o Kube-State-metrics

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

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

Configurar/personalizar o Operador

Essas seções contêm informações sobre como personalizar a configuração do 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 esse recurso antes de implantar o operador editando o arquivo *operator-config.yaml*. Este arquivo inclui exemplos comentados de configurações. Consulte a lista de "definições disponíveis" para obter a versão mais recente do operador.

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

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

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Se você vir uma mensagem "erro do servidor (NotFound)", seu operador deve
ser atualizado antes de poder usar o AgentConfiguration.
```

Configurando o suporte Proxy

Há dois lugares onde você pode usar um proxy em seu locatário para instalar o Operador de Monitoramento do Kubernetes. Estes podem ser os mesmos ou sistemas proxy separados:

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

Se você usar um proxy para um ou ambos, para instalar o Monitor operacional Kubernetes, primeiro você deve garantir que o proxy esteja configurado para permitir uma boa comunicação com o ambiente Insights da infraestrutura de dados. Se você tiver um proxy e puder acessar o Data Infrastructure Insights do servidor/VM a partir do qual deseja instalar o Operador, o proxy provavelmente estará configurado corretamente.

Para o proxy usado para instalar o Monitor operacional Kubernetes, antes de instalar o Operador, defina as variáveis de ambiente *http_proxy/https_proxy*. Para alguns ambientes proxy, você também pode precisar definir a variável *no_proxy environment*.

Para definir a(s) variável(s), execute as seguintes etapas em seu sistema **antes** de instalar o Operador de Monitoramento do Kubernetes:

1. Defina a(s) variável(s) 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 para que o cluster do Kubernetes se comunique com o ambiente Data Infrastructure Insights, instale o Operador de Monitoramento do Kubernetes depois de ler todas essas instruções.

Configure a seção proxy do AgentConfiguration no operator-config.yaml antes de implantar o Operador de Monitoramento do Kubernetes.

```
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 operador de monitoramento do Kubernetes coletará imagens de contentor do repositório Data Infrastructure Insights. Se você tiver um cluster do Kubernetes usado como destino para monitoramento e esse cluster estiver configurado para extrair apenas imagens de contentor de um repositório ou Registro de contentor personalizado ou privado do Docker, configure o acesso aos contentores necessários pelo Operador de Monitoramento do Kubernetes.

Execute o "trecho de recebimento de imagem" do bloco de instalação do Operador de Monitoramento do NetApp. Esse comando fará login no repositório Data Infrastructure Insights, extrairá todas as dependências de imagem do operador e fará logout do repositório Data Infrastructure Insights. Quando solicitado, insira a senha temporária do repositório fornecida. Este comando transfere todas as imagens utilizadas pelo operador, incluindo as funcionalidades opcionais. Veja abaixo quais recursos essas imagens são usadas.

Funcionalidade do operador principal e monitoramento do Kubernetes

- monitoramento de NetApp
- ci-kube-rbac-proxy
- ci-ksm
- ci-telegraf
- distroless-root-user

Registo de eventos

- ci-fluente-bit
- ci-kurein-event-exporter

Desempenho de rede e mapa

- ci-net-observador

Envie a imagem do docker do operador para o 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 em seu repositório sejam consistentes com os do repositório Data Infrastructure Insights.

Edite a implantação do operador de monitoramento no operator-deployment.yaml e modifique todas as referências de imagem para usar seu repositório Docker privado.

```
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 no operator-config.yaml para refletir o novo local de repo do docker. Crie uma nova imagePullSecret para o seu repositório privado, para obter 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 no OpenShift 4,6 ou superior, você deve editar o AgentConfiguration em *operator-config.yaml* para ativar 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.

Tolerações e taints

O *NetApp-ci-telegraf-ds*, o *NetApp-CI-Fluent-bit-ds* e o *NetApp-CI-NET-Observer-L4-DS* DaemonSets devem agendar um pod em cada nó do cluster para coletar corretamente os dados em todos os nós. O operador foi

configurado para tolerar alguns **taints** conhecidos. Se você tiver configurado quaisquer taints personalizados em seus nós, impedindo assim que os pods sejam executados em cada nó, você poderá criar uma **tolerância** para essas taints ."Em *AgentConfiguration*" Se você tiver aplicado taints personalizados a todos os nós do cluster, também será necessário adicionar as tolerâncias necessárias à implantação do operador para permitir que o pod do operador seja agendado e executado.

Saiba mais sobre o Kubernetes "Taints e Tolerations".

Volte ao **"Página de Instalação do Operador de Monitoramento do Kubernetes do NetApp"**

Uma Nota sobre Segredos

Para remover a permissão do Operador de Monitoramento do Kubernetes para exibir segredos em todo o cluster, exclua os seguintes recursos do arquivo *operator-setup.yaml* antes de instalar:

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

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

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

Se a análise de mudança estiver ativada, modifique o *AgentConfiguration* ou *operator-config.yaml* para descomentar a seção de gerenciamento de alterações e inclua *kindsToIgnoreFromWatch: '"segredos"'* na seção Gerenciamento de alterações. Observe a presença e a posição de 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 para o operador e todas as imagens relacionadas que ele implanta são assinadas pelo NetApp. Você pode verificar manualmente as imagens antes da instalação usando a ferramenta de cografia ou configurar um controlador de admissão do Kubernetes. Para obter mais detalhes, consulte "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: Carregue as imagens do operador para o 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 snippet de recebimento de imagem
2. Copie e insira a senha do repositório quando solicitado
3. Armazenar a chave Pública de assinatura de imagem (dii-image-signing.pub no exemplo)
4. Verifique as imagens usando o cosign. Consulte o exemplo a seguir de uso de cosign

```
$ 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 para tentar se você encontrar problemas para configurar o operador de monitoramento do Kubernetes:

Problema:	Tente isto:
Não vejo um hiperlink/conexão entre o meu volume persistente do Kubernetes e o dispositivo de armazenamento de back-end correspondente. Meu volume persistente do Kubernetes é configurado usando o nome de host do servidor de armazenamento.	Siga as etapas para desinstalar o agente Telegraf existente e reinstalar o agente Telegraf mais recente. Você precisa estar usando o Telegraf versão 2,0 ou posterior, e o storage de cluster do Kubernetes precisa ser monitorado ativamente pelo Data Infrastructure Insights.
Estou vendo mensagens nos logs que se assemelham ao seguinte: E0901 15 352:21 v1:39,962145 1 k8s 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:k8s:43,168161 1 reflector.go:178] 21.io/kube-State-State-lease	Essas mensagens podem ocorrer se você estiver executando o kube-State-metrics versão 2.0.0 ou superior com versões do Kubernetes abaixo de 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 leases'* para evitar que essas mensagens aconteçam, os usuários podem modificar sua implantação do kube-State-metrics para desativar os seguintes: *Mutatinghookhookhooks*

Problema:	Tente isto:
Vejo mensagens de erro do Telegraf semelhantes às seguintes, mas o Telegraf inicia e executa: Oct 11 14:23:41 ip-172-31-39-47 systemd[1]: Iniciou o agente de servidor orientado a plug-in para relatar métricas no InfluxDB. Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827]: Tempo 2021-10-11T14:23:41Z" não foi possível criar o diretório de cache. /Etc/telegraf/.cache/floco de neve, err: Mkdir /etc/telegraf/.CA che: Permissão negada. Ignorado. Func"gostonflake.(*defaultLogger).Errorf" file "log.go:120" Oct:10 ip-23-41Z-39-47 telegraf[1827]: 2021" 31"erro de 11 14:23:41:172". Abra /etc/telegraf/.cache/floco de neve/ocsp_response_cache.json: nenhum arquivo ou diretório desse tipo de arquivo ou diretório.(*defaultLogger).Errorf" arquivo "log.go:120 23" Oct 2021 41Z:10 ip-172-31-39-47 telegraf[1827]: 11 14-23:41 A iniciar o Telegraf 1.19.3	Este é um problema conhecido. "Este artigo do GitHub"Consulte para obter mais detalhes. Enquanto o Telegraf estiver ativo e em execução, os usuários podem ignorar essas mensagens de erro.
No Kubernetes, meu(s) pod(s) Telegraf está relatando o seguinte erro: "Erro no processamento de informações de mountstats: Failed to open mountstats file: /Hostfs/proc/1/mountstats, error: Open /hostfs/proc/1/mountstats: Permission denied"	Se o SELinux estiver habilitado e aplicando, provavelmente impedirá que o(s) pod(s) Telegraf acesse o arquivo /proc/1/mountstats no nó Kubernetes. Para superar essa restrição, edite a configuração do agentConfiguration e ative a configuração RUNGED Privileged. Para obter mais detalhes, consulte "Instruções do OpenShift"a .
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/kupere/pki/etcd/Server.crt:/etc/kuGES/pki/etcd/Server.key: Open /etc/kuurge/pki/etcd/Server.crt: nenhum arquivo ou diretório	O pod Telegraf ReplicaSet destina-se a ser executado em um nó designado como mestre ou para o etcd. Se o pod ReplicaSet não estiver sendo executado em um desses nós, você receberá esses erros. Verifique se seus nós master/etcd têm manchetes neles. Se o fizerem, adicione as tolerâncias necessárias ao Telegraf ReplicaSet, telegraf-rs. Por exemplo, edite o ReplicaSet… kubectl edite 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 do Pod (PSP) ou a admissão de Segurança do Pod (PSA), você deverá fazer o upgrade para o Operador de Monitoramento do Kubernetes mais recente. Siga estes passos para atualizar para o Operador atual com suporte para PSP/PSA: 1. Desinstalar o operador de monitoramento anterior: kubectl delete 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-rolebinding cluster-rolebinding.-rolebinding 2. Instale a versão mais recente do operador de monitorização.

Problema:	Tente isto:
Deparei-me com problemas ao tentar implementar o Operador e tenho PSP/PSA em utilização.	1. Edite o agente usando o seguinte comando: Kubectl -n <name-space> edit Agent 2. Marque "Segurança-política-ativada" como "falsa". Isso desativará as políticas de Segurança do Pod e a admissão de Segurança do Pod e permitirá que o Operador implante. Confirme usando os seguintes comandos: Kubectl Get PSP (deve mostrar a Política de Segurança Pod removida) kubectl get all -n <namespace>
grep -i psp (deve mostrar que nada é encontrado)	Erros "ImagePullBackoff" vistos
Esses erros podem ser vistos se você tiver um repositório docker personalizado ou privado e ainda não tiver configurado o Operador de Monitoramento do Kubernetes para reconhecê-lo adequadamente. Leia mais sobre a 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 comandos a seguir 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 (Workload Map) no namespace Operator estão em CrashLoopBackOff

Esses pods correspondem ao coletor de dados do mapa de workload para observabilidade de rede. Tente estes: • 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","ambiente":"prod","nível":"erro","msg":"falhou na validação. Razão: A versão 3.10.0 do kernel é menor que a versão mínima do kernel de 4.18.0","Time":"2022-11-09T08:23:08Z" ---- • os pods do Net-Observer requerem que a versão do kernel do Linux seja pelo menos 4.18.0. Verifique a versão do kernel usando o comando "uname -r" e certifique-se de que eles são > 4.18.0	Os pods estão em execução no namespace do operador (padrão: Monitoramento NetApp), mas nenhum dado é exibido na IU para mapa de workload ou métricas do Kubernetes em consultas

Problema:	Tente isto:
Verifique a configuração de hora nos nós do cluster K8S. Para uma auditoria precisa e relatórios de dados, 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 net-observer no namespace Operador estão no estado pendente
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 para CPU ou memória. Certifique-se de que a memória e a CPU necessárias estão disponíveis no nó.	Estou vendo o seguinte em meus logs imediatamente após instalar o Operador de Monitoramento do Kubernetes: [inputs.prometheus] erro no plugin: Erro ao fazer solicitação HTTP para http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Get http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Dial tcp: Lookup kube-State-metrics.<namespace>.svc.cluster.local: nenhum host
Normalmente, essa mensagem só é vista quando um novo operador é instalado e o pod *telegraf-rs* está ativo antes do pod *ksm* estar ativo. 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 a versão do Kubernetes (isto é `kubectl version`,). Se for v1,20.x ou inferior, esta é uma limitação esperada. A versão kube-State-metrics implantada com o Operador de Monitoramento do Kubernetes suporta apenas v1.CronJob. Com o Kubernetes 1,20.x e abaixo, o recurso CronJob está em v1beta.CronJob. Como resultado, as métricas de estado do kube não conseguem encontrar o recurso CronJob.	Depois de instalar o operador, os pods telegraf-ds entram em CrashLoopBackOff e os logs do pod indicam "su: Authentication failure".
Edite a seção telegraf em *AgentConfiguration* e defina *dockerMetricCollectionEnabled* como false. Para obter mais detalhes, consulte o "opções de configuração". … spec: … telegraf: … - Name: docker run-mode : - DaemonSet substituições: - Chave: DOCKER_UNIX_SOCK_PLACEHOLDER valor: unix:////run/docker.Sock … …	Vejo mensagens de erro repetitivas 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 enquanto aguarda cabeçalhos)
Edite a seção telegraf em *AgentConfiguration* e aumente *outputTimeout* para 10s. Para obter mais detalhes, consulte o "opções de configuração".	Estou faltando dados *involvedobject* para alguns Registros de eventos.
Certifique-se de que seguiu os passos indicados na "Permissões" secção 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>?

Problema:	Tente isto:
A partir de 12 de outubro de 2023, o Data Infrastructure Insights refatorou a operadora para melhor atender nossos usuários; para que essas alterações sejam totalmente adotadas, você retire o operador antigo deve e instale o novo.	Os eventos do meu kualves pararam inesperadamente de reportar ao Data Infrastructure Insights.
Recuperar o nome do pod de 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 de exportador de eventos apropriado encontrado na etapa anterior. Mais especificamente, LOG_FILE deve ser definido como "/var/log/containers/NetApp-CI-event-exporters.log" ou "/var/log/containers/event-exporters*.log" …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. Alternativamente, pode-se desinstalartambém e reinstale o agente.
Estou vendo POD(s) implantado(s) pelo Operador de Monitoramento do Kubernetes travarem devido a recursos insuficientes.	Consulte o Operador de Monitoramento do Kubernetes "opções de configuração"para aumentar os limites de CPU e/ou memória conforme necessário.
Uma imagem ausente ou uma configuração inválida fez com que os pods de métricas de estado do NetApp-ci-kube falhassem na inicialização ou se preparassem. Agora o StatefulSet está preso 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, salte os pods NetApp-CI-kube-State-metrics.
Os pods de métricas de estado do NetApp-ci-kube falham ao iniciar depois de executar uma atualização do Operador do Kubernetes, lançando o ErrImagePull (falha ao puxar a imagem).	Tente redefinir os pods manualmente.

Problema:	Tente isto:
"Evento descartado como sendo mais antigo do que maxEventAgeSeconds" mensagens estão sendo observadas para o meu cluster Kubernetes em Log Analysis.	Modifique o Operador *agentConfiguration* e aumente o *event-exporter-maxEventAgeds* (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 a "opções de configuração" página.
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 *desprotegido* como *true*. Isto instruirá o Telegraf a não tentar reservar páginas de memória bloqueadas. Embora isso possa representar um risco de segurança, pois segredos descriptografados podem ser trocados para o disco, ele permite a execução em ambientes onde não é possível reservar memória bloqueada. Para obter mais detalhes sobre as opções de configuração *desprotegidas*, consulte a "opções de configuração"página.
Vejo mensagens de aviso do Telegraf que se assemelham às seguintes: *W! [Inputs.diskio] não é possível reunir o nome do disco para "vdc": Erro ao ler /dev/vdc: nenhum arquivo ou diretório*	Para o Operador de Monitoramento do Kubernetes, essa mensagem de aviso é benigna e pode ser ignorada com segurança. Alternativamente, edite a seção telegraf em AgentConfiguration e defina *runDsPrivileged* como true. Para obter mais detalhes, consulte "opções de configuração do operador"a .

Problema:	Tente isto:

Meu pod fluente-bit está falhando com os seguintes erros: [2024 10/16 14/10/16 14 16:16 2024 23:23] [error] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno.24] muitos arquivos abertos [2024/10/16 14:16:23] [error] falha na inicialização tail,0 [Engine] [input]	Tente alterar suas configurações *fsnotify* no 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 entre as reinicializações do nó, 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>`

Informações adicionais podem ser encontradas na "Suporte" página ou no "Matriz de suporte do Data Collector".

Memcached Data Collector

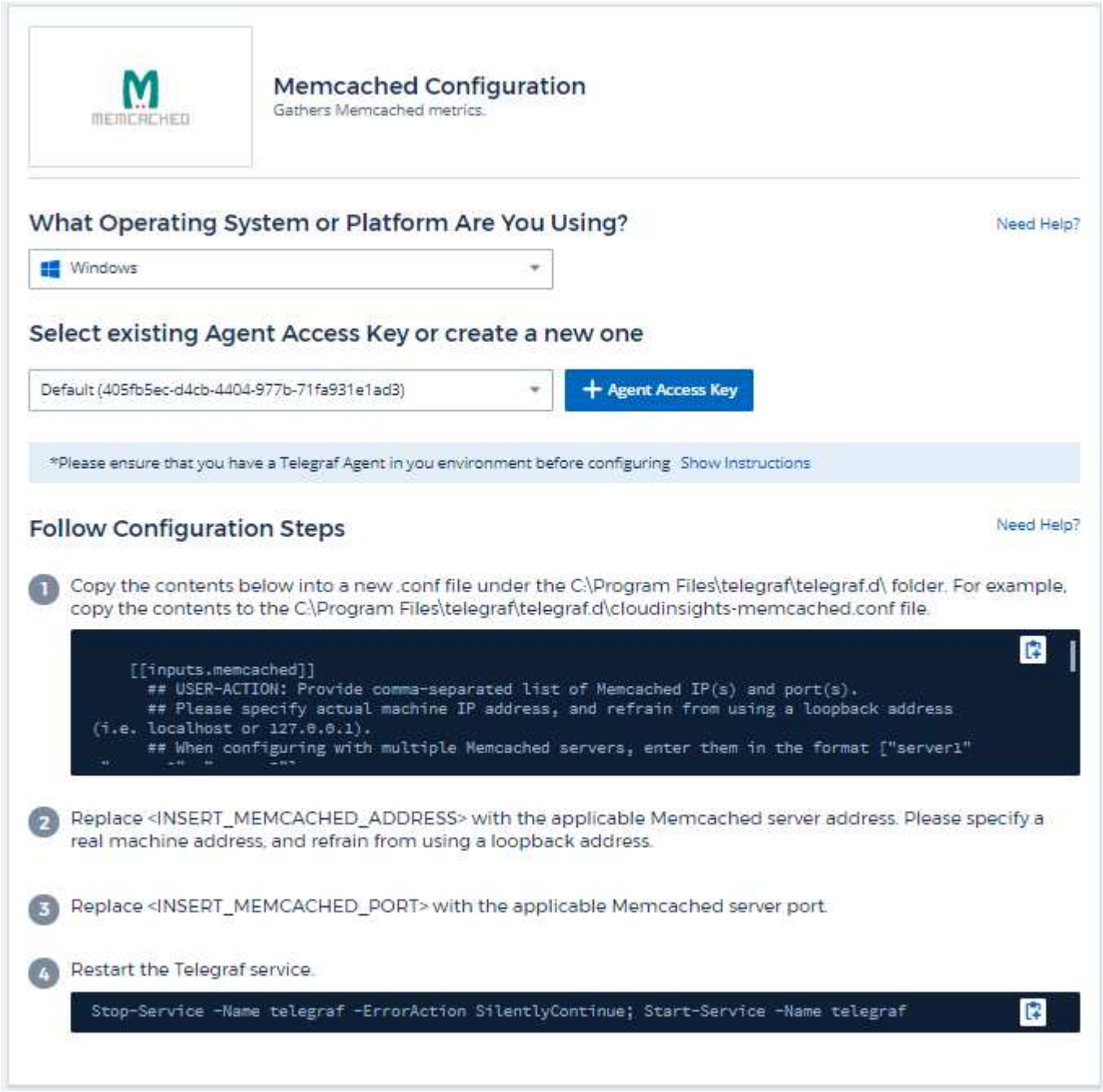
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do memcached.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha memcached.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

As informações podem ser encontradas no "Memcached wiki".

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
Memcached	Servidor de namespace	Nome do nó IP	Aceitar conexões manipuladas solicitações de autenticação autenticações falhadas bytes usados bytes leitura (por seg) bytes escritos (por seg) CAS Badaval acessos CAS falhas de descarga Reqs (por seg) obter Reqs (por seg) Definir Reqs (por seg) toque Reqs (por seg) falhas de Acesso Total de acessos por seg. Falhas de acessos por seg. Solicitações de Segurança falhas de Segurança Total de acessos por seg. Falhas de acessos por seg. Falhas de acessos por seg

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

MongoDB Data Collector

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

Instalação

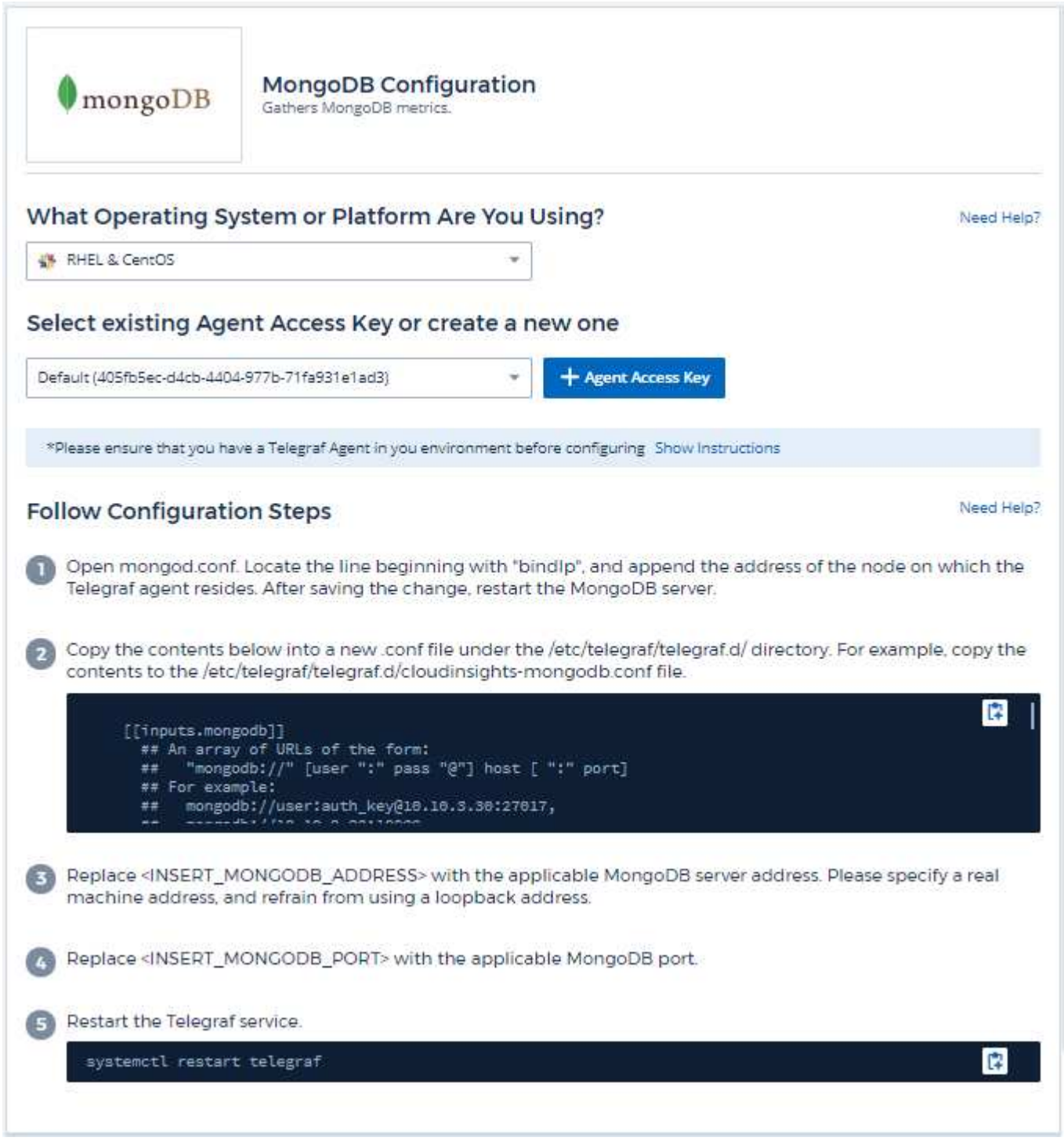
1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha MongoDB.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

As informações podem ser encontradas no "Documentação do MongoDB".

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

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

Solução de problemas

Informações podem ser encontradas na "Suporte"página.

MySQL Data Collector

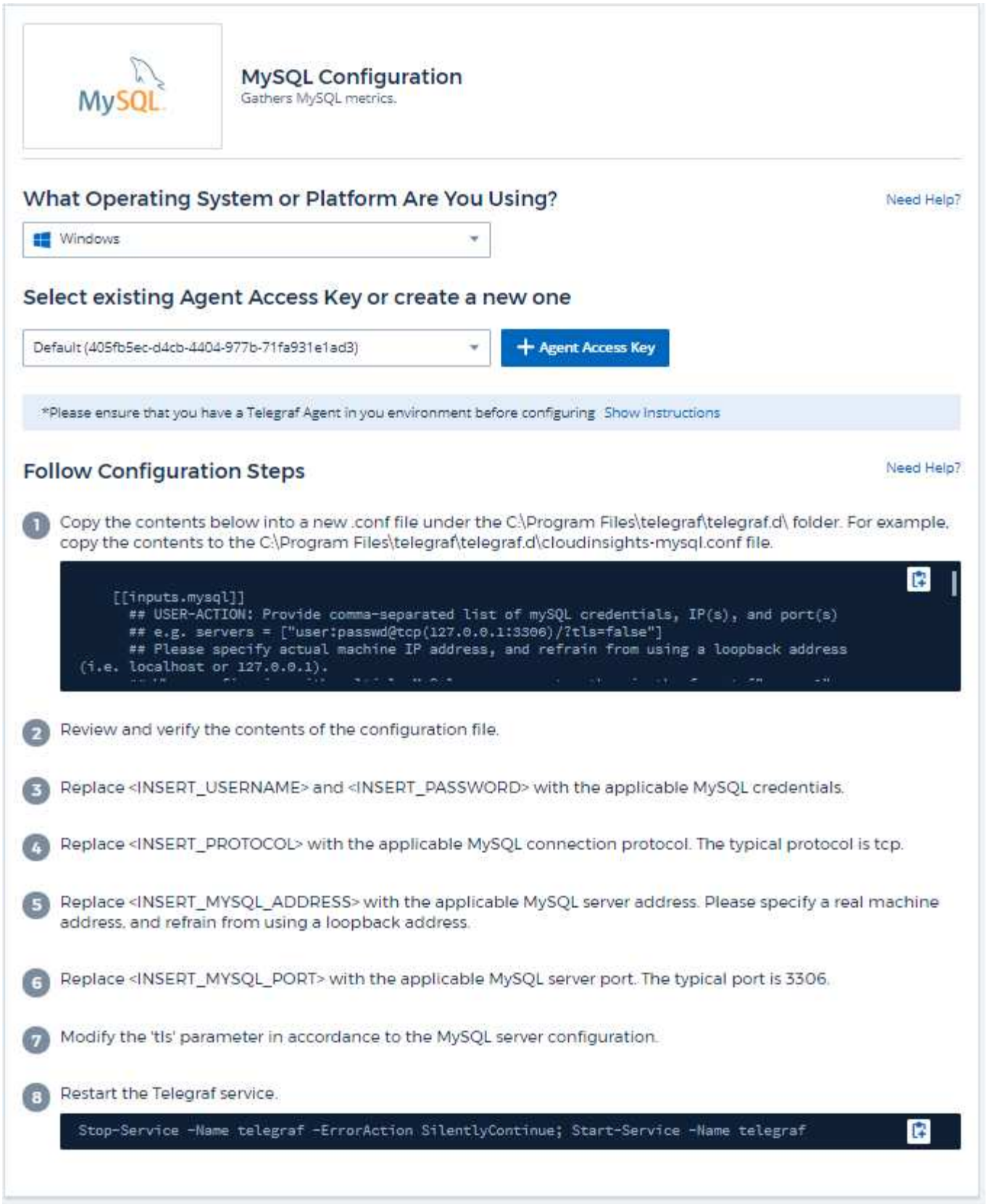
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do MySQL.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha MySQL.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

As informações podem ser encontradas no "Documentação do MySQL".

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:
MySQL	Servidor de namespace MySQL	Nome do nó IP	Clientes abortados (por seg) conexões abortadas (por seg) bytes RX (por seg) bytes TX (por seg) comandos Admin (por seg) comandos Alter comandos de evento Alter comandos de função Alter comandos de instância Alter comandos de procedimento Alter

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

Netstat Data Collector

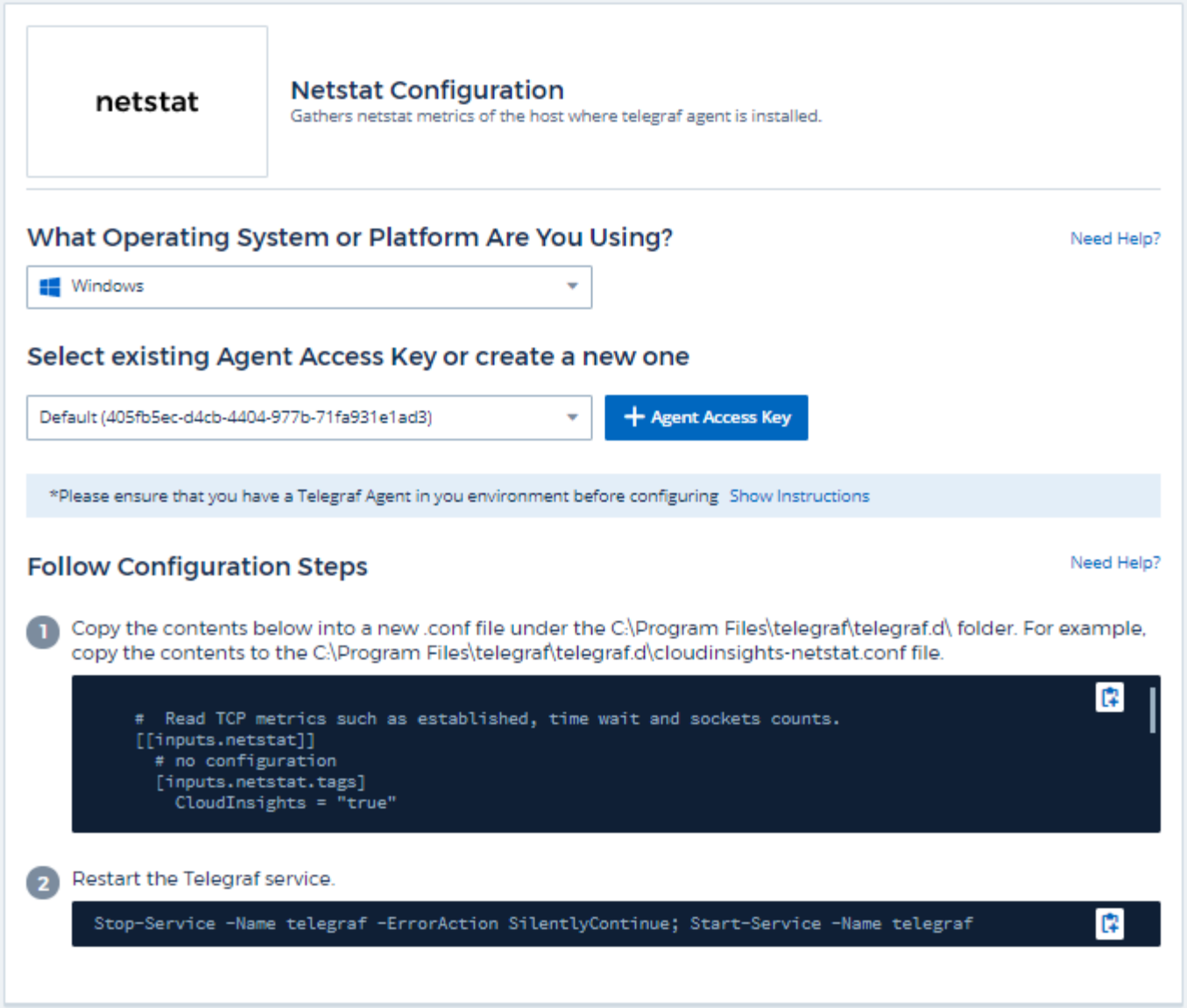
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Netstat.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Netstat.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

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

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

Nginx Data Collector

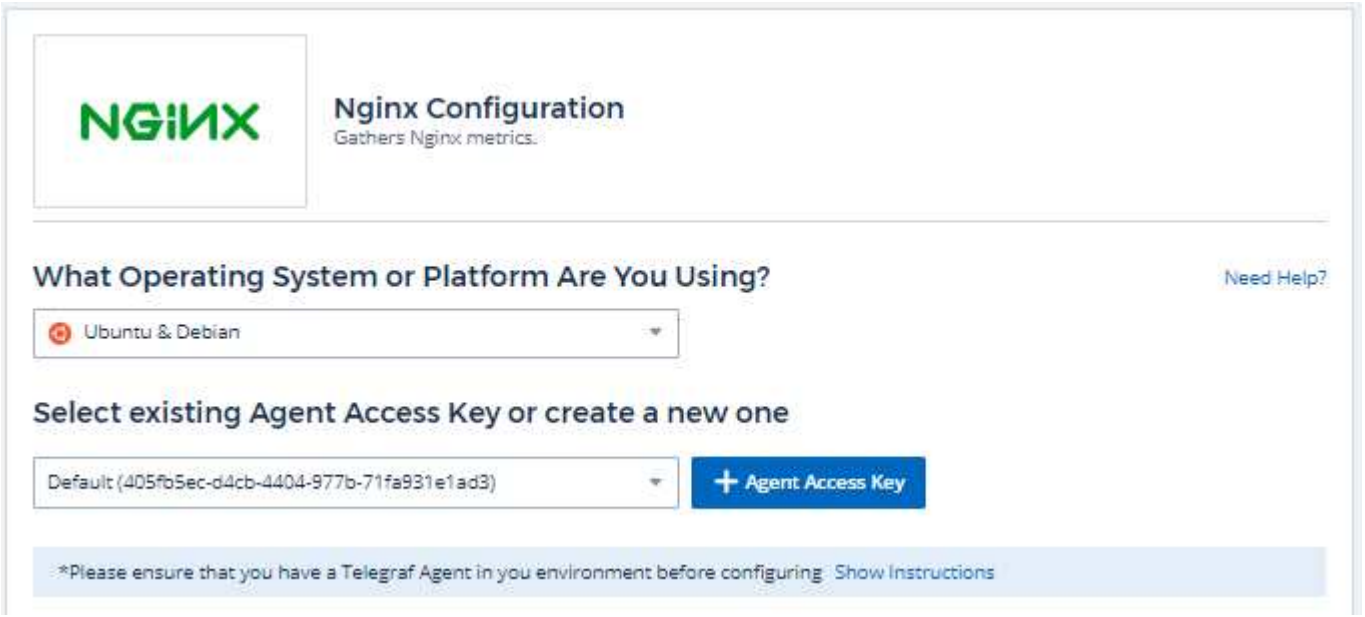
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do nginx.

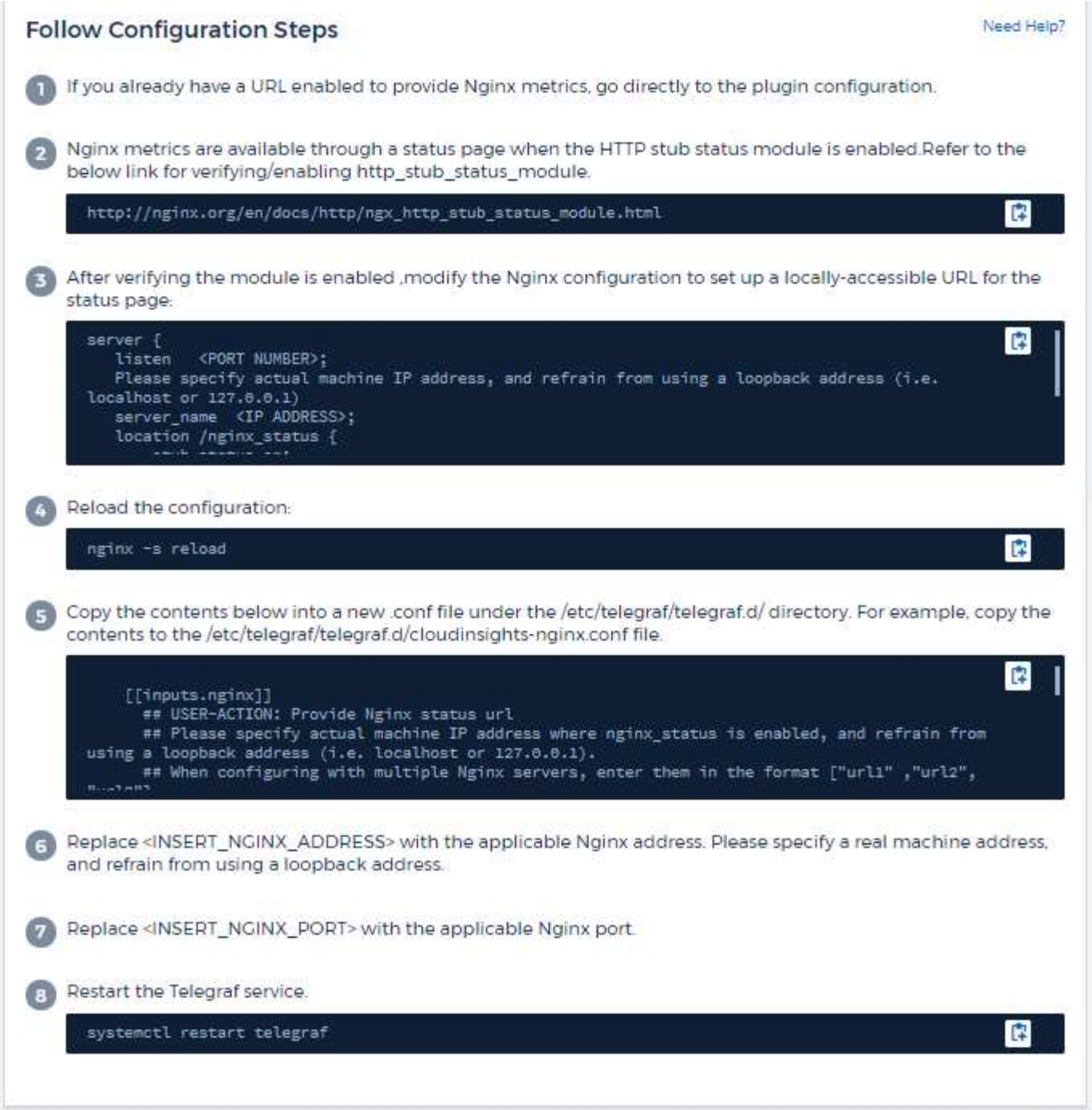
Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha nginx.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

A coleção de métricas nginx requer que o nginx "http_stub_status_module" seja ativado.

Informações adicionais podem ser encontradas no "Documentação do nginx".

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

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

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

PostgreSQL Data Collector

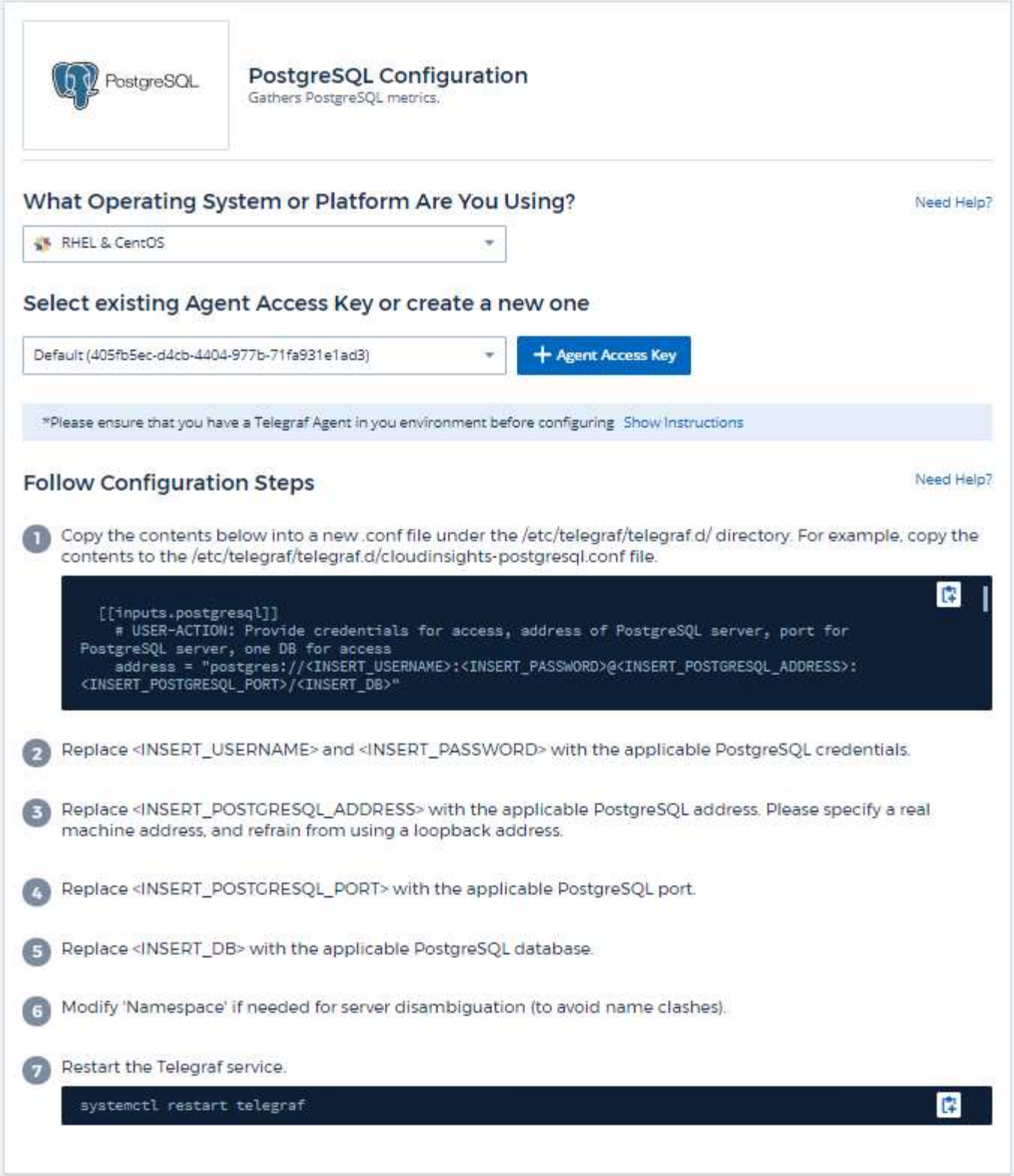
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do PostgreSQL.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha PostgreSQL.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

As informações podem ser encontradas no "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	IP do nó de nome do nó	Buffers alocados Buffers backend Buffers backend File Sync Buffers Checkpoints Limpar Checkpoints Sync Time Checkpoints Write Time Checkpoints Checkpoints Requests Checkpoints Checkpoints Timed Max written clean
Banco de dados PostgreSQL	Servidor de Banco de dados de namespace	IP nó Nome nó OID base dados	Blocos de tempo de leitura blocos de tempo de gravação blocos de tempo hits blocos lê conflitos deadlocks número do cliente arquivos temporários bytes arquivos de temperatura número linhas excluídas linhas recuperadas linhas inseridas linhas retornadas transações atualizadas transações confirmadas Rollbacked

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

Puppet Agent Data Collector

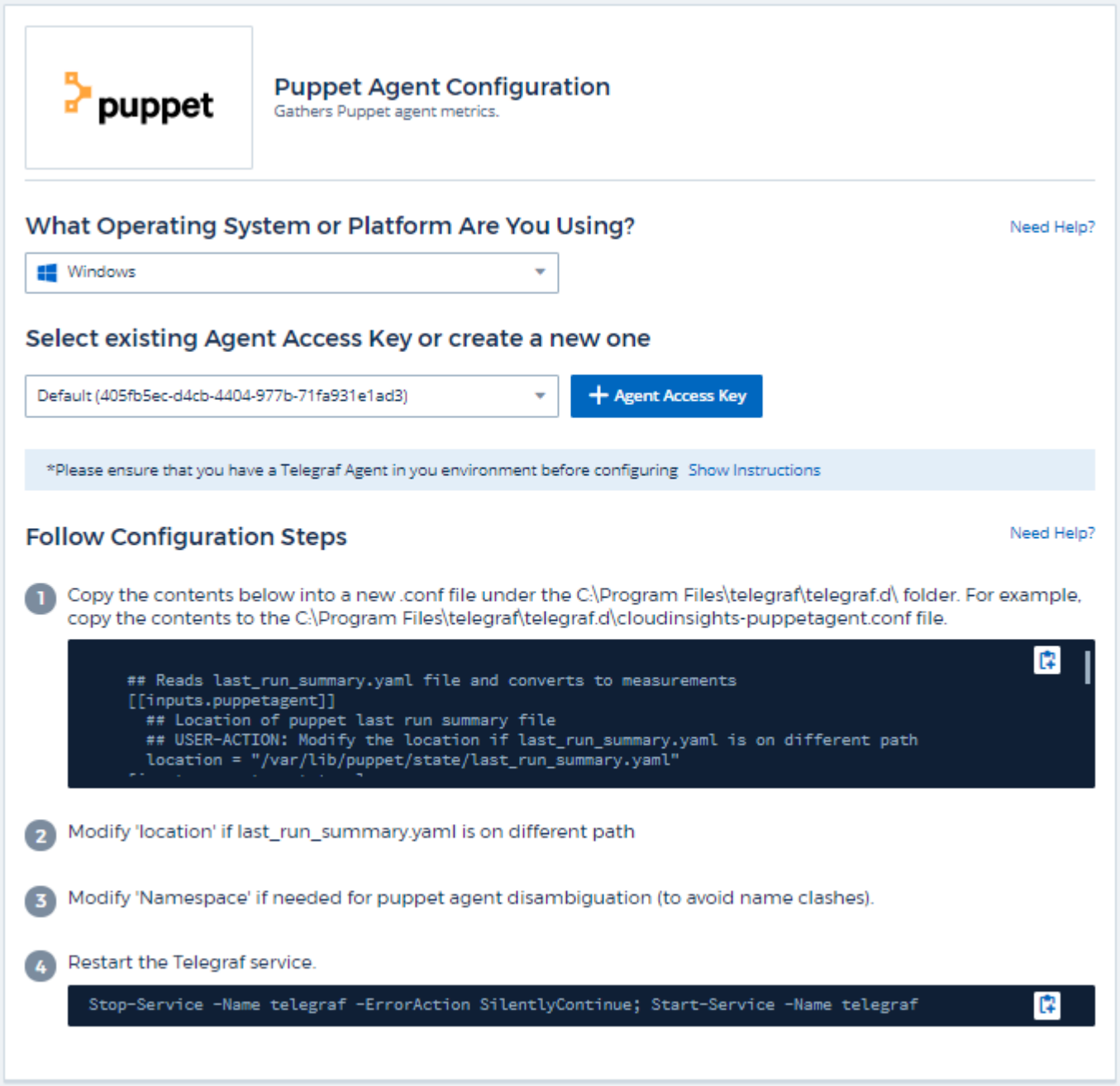
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Puppet Agent.

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Puppet.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

As informações podem ser encontradas no "Documentação da marionete"

Objetos e contadores

Os seguintes objetos e seus contadores são coletados:

Objeto:	Identificadores:	Atributos:	Pontos de dados:

Agente de fantoche	UUUID nó namespace	Nome do nó localização nó versão IP Configstring versão Puppet	Alterações Total Eventos falhas Eventos sucesso Eventos recursos totais recursos alterados recursos Falha recursos Falha ao reiniciar recursos recursos Outofsync recursos reiniciados recursos programados recursos ignorados tempo total tempo de ancoragem tempo de recuperação da configuração tempo tempo tempo do cron tempo Exec tempo do arquivo tempo do arquivo tempo do pacote tempo horário do pacote horário do serviço tempo do Sshaughhorizedkey tempo Total do Usuário

Solução de problemas

Informações adicionais podem ser encontradas na "Suporte"página.

Redis Data Collector

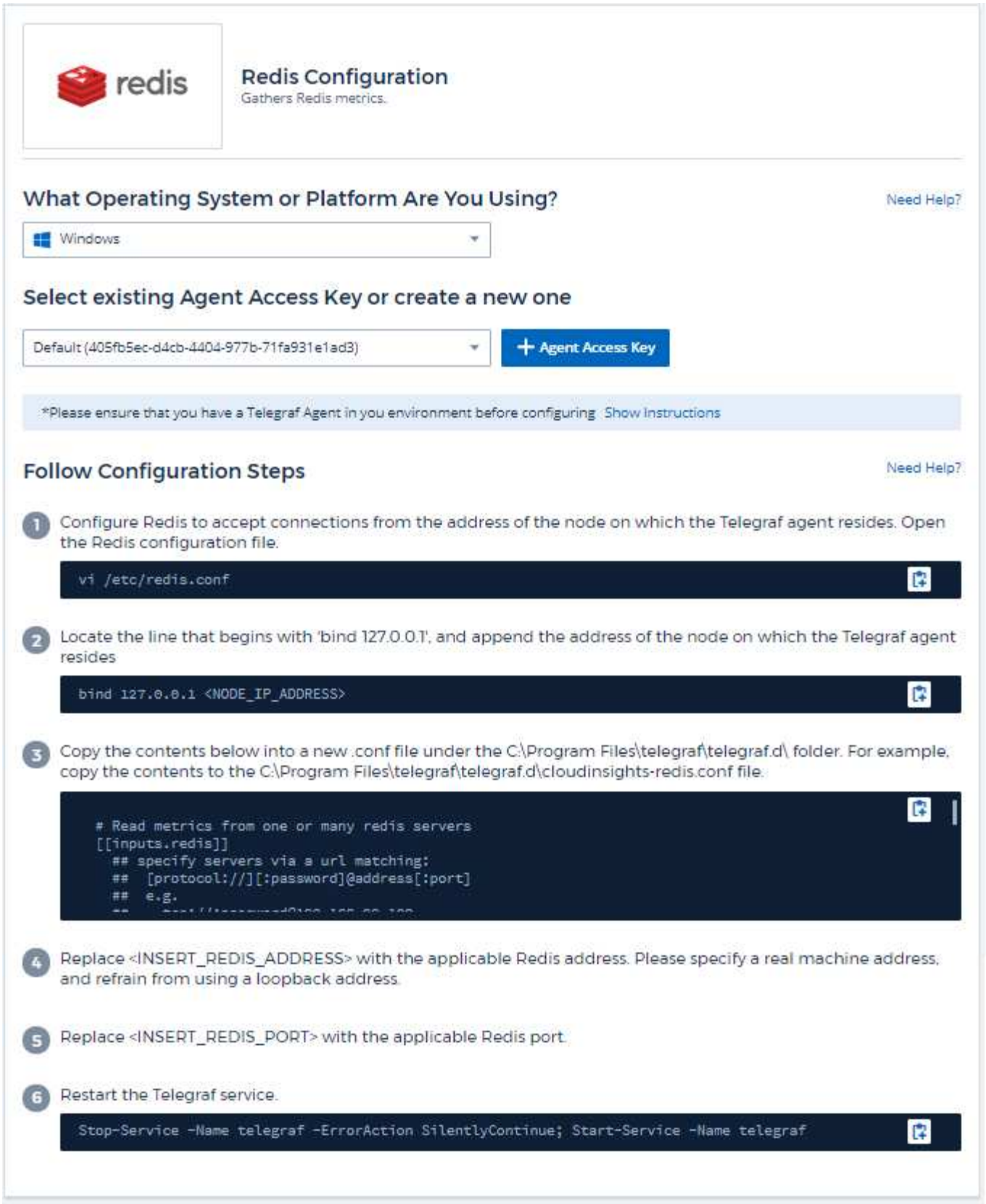
O Data Infrastructure Insights usa esse coletor de dados para coletar métricas do Redis. Redis é um armazenamento de estrutura de dados em memória de código aberto usado como um banco de dados, cache e corretor de mensagens, suportando as seguintes estruturas de dados: Strings, hashes, listas, conjuntos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

Instalação

1. A partir de **Observability > Collectors**, clique em * Data Collector*. Escolha Redis.

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

2. Se você ainda não instalou um Agente para coleção ou deseja instalar um Agente para um sistema operacional ou plataforma diferente, clique em *Mostrar instruções* para expandir as "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 ao agente clicando no botão * chave de acesso ao agente*. Prática recomendada: Use uma chave de acesso de agente diferente somente quando você quiser agrupar coletores de dados, por exemplo, por SO/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

As informações podem ser encontradas no "Documentação 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 na "Suporte"página.

Informações sobre direitos autorais

Informações sobre marcas comerciais