Riferimento Data Collector - servizi

Data Infrastructure Insights

NetApp
August 19, 2025

Sommario

Riferimento Data Collector - servizi

Raccolta dati nodo

Data Infrastructure Insights raccoglie le metriche dal nodo in cui si installa un agente.

Installazione

1. Da **osservabilità > Collector**, scegliere un sistema operativo/piattaforma. Si noti che l'installazione di qualsiasi data collector di integrazione (Kubernetes, Docker, Apache, ecc.) configurerà anche la raccolta di dati dei nodi.
2. Seguire le istruzioni per configurare l'agente. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.

Oggetti e contatori

I seguenti oggetti e i relativi contatori vengono raccolti come metriche del nodo:

Oggetto:	Identificatori:	Attributi:	Punti dati:
File system del nodo	Nodo UUID Device Path Type (tipo percorso dispositivo UUID nodo)	Nodo IP Node Name Node OS Mode	Nodi liberi nodi liberi nodi totali utilizzati totale utilizzato totale utilizzato
Disco del nodo	Disco UUID nodo	Nodo IP Node Name Node OS	Tempo di io totale IOPS in corso byte di lettura (per sec) tempo di lettura totale letture (per sec) tempo di io ponderato totale byte di scrittura (per sec) tempo di scrittura totale scritture (per sec) lunghezza corrente della coda del disco tempo di scrittura tempo di lettura tempo di io
CPU nodo	CPU UUID nodo	Nodo IP Node Name Node OS	Utilizzo della CPU utilizzo della CPU utente utilizzo della CPU inattivo utilizzo della CPU utilizzo della CPU interruzione utilizzo della CPU utilizzo della CPU DPC utilizzo della CPU

Oggetto:	Identificatori:	Attributi:	Punti dati:
Nodo	UUID nodo	Nodo IP Node Name Node OS	Tempo di avvio del kernel kernel Opzioni di contesto del kernel (per sec) intropia del kernel disponibile interrupt del kernel (per sec) processi del kernel forcati (per sec) Memoria attiva memoria disponibile memoria totale disponibile memoria con buffer memoria cache limite di impegno memoria allocata come memoria memoria sporca memoria libera memoria libera elevata memoria totale elevata memoria enorme dimensione pagina memoria pagine enormi memoria libera pagine enormi memoria totale bassa memoria libera memoria totale bassa memoria mappata memoria tabelle pagine Memoria Shared Memory Slab Memory Swap cache Memory Swap Free Memory Swap Total Memory memoria totale utilizzata memoria totale utilizzata memoria utilizzata memoria Vmalloc Chunk Memory Vmalloc Total Memory Vmalloc Used Memory Wired Memory Writeback Total Memory Writeback TMP Memory cache FLAUTS Memory Demand Zero FLAUTS Memory Page FLAUTS Memory Memory Memory Memory Memoria NONPAGED memoria paging cache Core memoria Standby cache memoria normale Standby cache riserva memoria errori di transizione processi bloccati processi inattivi processi inattivi processi di paging processi in esecuzione processi in sospensione processi

Oggetto:	Identificatori:	Attributi:	Punti dati:
Rete di nodi	UUID nodo interfaccia di rete	Nome nodo nodo nodo IP nodo SO	Byte ricevuti byte inviati pacchetti Outboud scartati pacchetti Outboud errori pacchetti ricevuti pacchetti scartati ricevuti errori ricevuti pacchetti ricevuti pacchetti inviati

Setup (Configurazione)

Le informazioni relative all'installazione e alla risoluzione di problemi si trovano in "Configurazione di un agente"questa pagina.

ActiveMQ Data Collector

Data Infrastructure Insights utilizza questo data collector per raccogliere metriche da ActiveMQ.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere ActiveMQ.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.

[Configurazione ActiveMQ]

Setup (Configurazione)

Le informazioni sono disponibili in "Documentazione ActiveMQ"

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Coda ActiveMQ	Namespace Queue Port Server	Node Name Node IP Node UID	Consumer Count Dequeue Count Enqueue Count dimensione coda

Oggetto:	Identificatori:	Attributi:	Punti dati:
Abbonato ActiveMQ	ID client ID Connection ID Port Server namespace	È attivo Node di destinazione Node Node IP Node UID Node OS Selector Subscription	Numero di dequeue numero di invii dimensione coda spedita Conteggio coda in attesa dimensione coda
Argomento ActiveMQ	Argomento namespace Port Server	Node Name Node IP Node UID Node OS	Dimensioni Conteggio incoditi Conteggio incoditi Conte clienti

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

Apache Data Collector

Questo data collector consente la raccolta di dati dai server Apache sul tenant.

Prerequisiti

- Il server HTTP Apache deve essere configurato e correttamente in esecuzione
- È necessario disporre delle autorizzazioni di sudo o amministratore per l'host/VM dell'agente
- In genere, il modulo Apache *mod_status* è configurato per esporre una pagina nella posizione '/server-status?auto' del server Apache. L'opzione *ExtendedStatus* deve essere attivata per raccogliere tutti i campi disponibili. Per informazioni su come configurare il server, consultare la documentazione del modulo Apache: https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegli Apache.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.

[Configurazione di Apache]

Setup (Configurazione)

Il plug-in di Telegraf per HTTP Server di Apache si basa sul modulo 'mod_status' per essere attivato. Quando questa opzione è attivata, il server HTTP di Apache espone un endpoint HTML che può essere visualizzato sul browser o scartato per l'estrazione dello stato di tutte le configurazioni HTTP Server di Apache.

Compatibilità:

La configurazione è stata sviluppata rispetto al server HTTP Apache versione 2.4.38.

Abilitazione mod_status:

L'attivazione e l'esposizione dei moduli "mod_status" richiede due passaggi:

- Modulo di abilitazione
- Esposizione delle statistiche dal modulo

Modulo di abilitazione:

Il caricamento dei moduli è controllato dal file di configurazione sotto '/usr/local/apache/conf/httpd.conf'. Modificare il file di configurazione e rimuovere il commento dalle seguenti righe:

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

Esposizione delle statistiche dal modulo:

L'esposizione di 'mod_status' è controllata dal file di configurazione in '/usr/local/apache2/conf/extra/httpd-info.conf'. Assicurarsi di avere quanto segue nel file di configurazione (almeno altre direttive saranno presenti):

```
# 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
```

Per istruzioni dettagliate sul modulo 'mod_status', vedere la "Documentazione di Apache"

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Apache	Server namespace	Nodo IP Node Name Port Parent Server Config Generation Parent Server MPM Generation Server uptime is stopping	Occupati byte per richiesta byte per secondo CPU bambini CPU sistema bambini CPU utente carico CPU sistema CPU utente connessioni asincrone chiusura connessioni asincrone mantenimento connessioni asincrone scrittura connessioni totale durata per richiesta lavoratori inattivi carico medio (ultimi 1 m) carico medio (ultimi 15 m) carico medio (ultimi 5 m) Elabora le richieste al secondo accessi totali durata totale KByte Scoreboard chiusura Scoreboard Lookups DNS Scoreboard finitura Scoreboard Idle Cleanup Scoreboard Keep Alive Scoreboard Logging Scoreboard Open Scoreboard Reading Scoreboard Sending Scoreboard Starting Scoreboard Waiting

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

Consul Data Collector

Data Infrastructure Insights utilizza questo data collector per raccogliere le metriche da Consul.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Console.

   Se non è stato configurato un agente per il ritiro, viene richiesto di selezionare "installare un agente" il locatario.

   Se si dispone di un agente già configurato, selezionare il sistema operativo o la piattaforma appropriati e fare clic su **continua**.

2. Seguire le istruzioni nella schermata Consul Configuration (Configurazione console) per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la

raccolta dei dati.

Setup (Configurazione)

Le informazioni sono disponibili nella "Documentazione di Consul".

Oggetti e contatori per console

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Console	Namespace Check ID Service Node	Nodo IP nodo SO nodo UUID nodo Nome nodo Nome servizio Nome controllo ID servizio Stato	Avviso di passaggio critico

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

Couchbase Data Collector

Data Infrastructure Insights utilizza questo data collector per raccogliere le metriche da Couchbase.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Couchbase.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.

[Configurazione di Couchbase]

Setup (Configurazione)

Le informazioni sono disponibili nella "Documentazione di Couchbase".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Nodo Couchbase	Namespace Cluster Couchbase Node Hostname	Nome nodo IP nodo	Memoria libera totale
Bucket Couchbase	Cluster bucket namespace	Nome nodo IP nodo	Data used Data Fetches Disk used Item Count Memory used Operations per second quota utilizzata

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

Data Collector di CouchDB

Data Infrastructure Insights utilizza questo data collector per raccogliere le metriche da CouchDB.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere CouchDB.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.

[Configurazione di CouchDB]

Setup (Configurazione)

Le informazioni sono disponibili nella "Documentazione di CouchDB".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Database dei CouchDB	Server namespace	Nome nodo IP nodo	Authentication cache Hits Authentication cache Miss Database Reads Database Scritture Database Open Open OS Files Max Request Time min Request Time httpd Request Methods Copy httpd Request Methods Delete httpd Request Methods Get httpd Request Methods Head httpd Request Methods Put Status Codes 200 Status Codes 201 codici di stato 202 codici di stato 301 codici di stato 304 codici di stato 400 codici di stato 401 codici di stato 403 codici di stato 404 codici di stato 405 codici di stato 409 codici di stato 412 codici di stato 500

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

Docker Data Collector

Data Infrastructure Insights utilizza questo data collector per raccogliere le metriche da Docker.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegli Docker.

   Se non è stato configurato un agente per il ritiro, viene richiesto di selezionare "installare un agente" il locatario.

   Se si dispone di un agente già configurato, selezionare il sistema operativo o la piattaforma appropriati e fare clic su **continua**.

2. Seguire le istruzioni nella schermata Configurazione Docker per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.

[Configurazione di Docker]

Setup (Configurazione)

Il plug-in di input Telegraf per Docker raccoglie le metriche attraverso un socket UNIX specificato o un endpoint TCP.

Compatibilità

La configurazione è stata sviluppata rispetto alla versione 1.12.6 di Docker.

Configurazione

Accesso a Docker tramite un socket UNIX

Se l'agente Telegraf è in esecuzione su baretal, aggiungere l'utente telegraf Unix al gruppo docker Unix eseguendo quanto segue:

```
 sudo usermod -aG docker telegraf
Se l'agente Telegraf viene eseguito all'interno di un pod Kubernetes,
esporre il socket Unix di Docker mappando il socket nel pod come volume e
montandolo su /var/run/docker.sock. Ad esempio, aggiungere quanto segue al
PodSpec:
```

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

Quindi, aggiungere quanto segue al contenitore:

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

Si noti che il programma di installazione di Data Infrastructure Insights fornito per la piattaforma Kubernetes si occupa automaticamente di questa mappatura.

Accedere a Docker tramite un endpoint TCP

Per impostazione predefinita, Docker utilizza la porta 2375 per l'accesso non crittografato e la porta 2376 per l'accesso crittografato.

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Motore Docker	Namespace Docker Engine	Node Name Node IP Node UID Node OS Kubernetes Cluster Docker Version Unit	Container di memoria Container in pausa Container in esecuzione Container CPU interrotte Vai routine immagini listener Eventi utilizzati descrittori di file dati disponibili dati totali utilizzati metadati disponibili metadati totali utilizzati dimensione blocco pool

Oggetto:	Identificatori:	Attributi:	Punti dati:
Container Docker	Namespace Container Name 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 Version Node Name Kubernetes Container Log Path Kubernetes Container Name Kubernetes Docker Type Kubernetes Pod Name Pod UID Kubernetes Sandbox ID Node IP Node UUID Docker Version Kubernetes io Config visto Kubernetes io Config Source OpenShift io SCC Kubernetes Descrizione Kubernetes Display Name OpenShift Tags Kompose Service Pod Template Hash Controller Revisione Hash Pod Pod generazione Template License Schema build Date Schema License Schema Name Schema URL Schema URL VCS Schema fornitore Schema versione Schema versione Maintainer Customer Pod Kubernetes StatefulSet Pod Name Tenant Webconsole Architecture Authoritative Source URL Data di build RH host RH Component Distribution Scope Install Release Run Summary Uninstall VCS Ref VCS Type VCS Version Vendor Version Health Status Container ID	Memoria attiva Anonymous Memory Active file Memory cache Memory Hierarchical Limit Memory Inactive Anonymous Memory Inactive file Memory Limit Memory Mapped file Memory Max Usage Memory Page Fault Memory Memory Pageed out Memory Resident Set Size Memory Resident Set Size memoria enorme memoria totale attiva Memoria anonima totale memoria file attiva totale memoria cache totale memoria non attiva memoria anonima totale memoria file inattiva memoria totale file mappato memoria totale memoria errori pagine totali memoria principale errori pagine totali memoria totale pagine in uscita memoria totale dimensioni set residenti memoria totale set residenti dimensioni memoria enorme memoria totale Memoria unevictable utilizzo della memoria utilizzo della memoria percentuale di utilizzo Codice di uscita OOM Killed PID Started at Finding Streak

Oggetto:	Identificatori:	Attributi:	Punti dati:
Io blocco container Docker	Namespace Container Name Device 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 Version Node Name Kubernetes Container Log Path Kubernetes Container Name Kubernetes Docker Type Kubernetes Pod Name Pod UID Kubernetes Sandbox ID Node IP Node UUID Docker Version Kubernetes Config visto Kubernetes Config Source OpenShift SCC Kubernetes Descrizione Kubernetes Display Name OpenShift Tags Schema versione modello modello Pod Hash Controller Revisione modello Hash Pod generazione modello Kompose Service Schema Data build Schema licenza Schema Nome Schema fornitore cliente Pod Kubernetes StatefulSet Pod Name Tenant Webconsole Data di build licenza Vendor Architecture Authoritative Source URL RH build host RH Component Distribution Scope Install Maintainer Release Run Summary Uninstall VCS Ref VCS Type Version Schema URL Schema VCS URL Schema versione Container ID	Io Service Bytes Recursive Async io Service Bytes Recursive Read io Service Bytes Recursive Sync io Service Bytes Recursive io Recursive Serviced Async io Serviced Recursive Read io Serviced Recursive io Serviced Recursive Total io Serviced Recursive Recursive Write

Oggetto:	Identificatori:	Attributi:	Punti dati:
Docker Container Network	Namespace Container Name Network Docker Engine	Container Image Container Status Container Version Node Name Node IP Node UUID Node OS K8s Cluster Docker Version Container ID	RX dromed RX bytes RX errors RX packets TX dromed TX bytes TX errors TX packets

Oggetto:	Identificatori:	Attributi:	Punti dati:
CPU Docker Container	Namespace Container Name CPU Docker Engine	Contenitore Kubernetes Hash Kubernetes Container Ports Kubernetes Container Restart Count Kubernetes Container Termination message Path Kubernetes Container Termination message Policy Kubernetes Pod Termination Grace Period Kubernetes Config Sawed Kubernetes Config Source OpenShift SCC Container Image Container Status Container Version Node Name Kubernetes Container Log Path Kubernetes Container Digitare Kubernetes Pod Name Kubernetes Pod namespace Kubernetes Pod UID Kubernetes Sandbox ID Node IP Node UUID Node OS Kubernetes Cluster Docker Version Kubernetes Descrizione Kubernetes Display Name OpenShift Tags Schema versione modello Pod modello Hash Controller Revisione modello Hash Pod generazione Servizio Kompose Schema Data di costruzione Schema Schema Schema licenza Schema Nome Schema Vendor Customer Pod Kubernetes StatefulSet Pod Name Tenant Webconsole Data di build License Vendor Architecture Authitative Source URL RH build host RH Component Distribution Scope Install Maintainer Release Run Summary Uninstall VCS Ref VCS Type Version Schema URL Schema VCS URL Schema Version Container ID	Periodi di rallentamento periodi di rallentamento periodi di rallentamento riduzione tempi di rallentamento utilizzo in modalità kernel utilizzo in modalità utente percentuale utilizzo sistema totale

Risoluzione dei problemi

Problema:	Prova:
Non riesco a trovare le metriche Docker in Data Infrastructure Insights dopo aver seguito le istruzioni sulla pagina di configurazione.	Controllare i registri degli agenti di Telegraf per verificare se riporta il seguente errore: E! Errore nel plug-in [inputs.docker]: Permesso ottenuto negato durante il tentativo di connessione al socket del daemon Docker. In caso contrario, eseguire i passaggi necessari per fornire all'agente Telegrafo l'accesso al socket Docker Unix come specificato sopra.

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

Elasticsearch Data Collector

Data Infrastructure Insights utilizza questo data collector per raccogliere le metriche da Elasticsearch.

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Elasticsearch.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.

[Configurazione di Elasticsearch]

Setup (Configurazione)

Le informazioni sono disponibili nella "Documentazione Elasticsearch".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:
Cluster Elasticsearch	Cluster di namespace	Nodo IP Node Name Cluster Status (Nome nodo IP Stato cluster)
Nodo Elasticsearch	Namespace Cluster ES Node ID ES Node IP ES Node	ID zona

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

Flink Data Collector

Data Infrastructure Insights utilizza questo data collector per raccogliere le metriche da Flink.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Flink.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.

[Configurazione Flink]

Setup (Configurazione)

Un'implementazione Flink completa comprende i seguenti componenti:

JobManager: Il sistema primario Flink. Coordina una serie di TaskManager. In una configurazione ad alta disponibilità, il sistema avrà più di un JobManager. Taskmanager: Qui vengono eseguiti gli operatori Flink. Il plugin Flink si basa sul plugin di telegraf, Jolokia. Come requisito per la raccolta di informazioni da tutti i componenti Flink, JMX deve essere configurato ed esposto tramite Jolokia su tutti i componenti.

Compatibilità

La configurazione è stata sviluppata rispetto alla versione 1.7 di Flink.

Configurazione

Jolokia Agent Jar

Per tutti i singoli componenti, è necessario scaricare una versione del file Jar dell'agente di Jlokia. La versione testata era "Agente di Jookia 1.6.0".

Le istruzioni riportate di seguito presuppongono che il file jar scaricato (jookia-jvm-1.6.0-Agent.jar) sia posizionato nella posizione '/opt/flink/lib/'.

JobManager

Per configurare JobManager in modo da esporre l'API di Jookia, è possibile impostare la seguente variabile di ambiente sui nodi e riavviare JobManager:

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
È possibile scegliere una porta diversa per Jlokia (8778). Se si dispone
di un IP interno su cui bloccare Jolokia, è possibile sostituire il "catch
all" 0.0.0.0 con il proprio IP. Si noti che questo IP deve essere
accessibile dal plugin telegraf.
```

Taskmanager

Per configurare TaskManager in modo che esponga l'API di Jookia, è possibile impostare la seguente variabile di ambiente sui nodi e riavviare TaskManager:

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
È possibile scegliere una porta diversa per Jlokia (8778). Se si dispone
di un IP interno su cui bloccare Jolokia, è possibile sostituire il "catch
all" 0.0.0.0 con il proprio IP. Si noti che questo IP deve essere
accessibile dal plugin telegraf.
```

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Task Manager Flink	Server dello spazio dei nomi del cluster	Nome nodo Task Manager ID nodo IP	Rete disponibile segmenti di memoria rete totale segmenti di memoria Garbage Collection PS MarkSweep Count Garbage Collection PS MarkSweep Time Garbage Collection PS Scavenge Count Garbage Collection PS Scavenge Time Heap Memory memoria allocata memoria heap Init memoria heap Max memoria utilizzata Conteggio thread Demon Conteggio thread massimo Conteggio thread Conteggio thread Conteggio thread Conteggio thread Totale iniziato
Flink Job (collega lavoro)	ID lavoro del server dello spazio dei nomi del cluster	Nome nodo Nome processo IP nodo ultimo punto di controllo percorso esterno tempo di riavvio	Downtime riavvio completo ultimo allineamento checkpoint buffer durata ultimo checkpoint dimensione checkpoint numero di checkpoint completati numero di checkpoint non riusciti numero di checkpoint in corso numero di checkpoint in corso tempo di attività

Oggetto:	Identificatori:	Attributi:	Punti dati:
Flink Job Manager	Server dello spazio dei nomi del cluster	Nome nodo IP nodo	Garbage Collection PS MarkSweep Count Garbage Collection PS MarkSweep Time Garbage Collection PS Scavenge Count Garbage Collection PS Scavenge Time Heap Memory memoria memoria heap impegnata memoria heap Init memoria heap massima memoria heap utilizzata numero di gestori di attività registrati numero di processi in esecuzione slot di attività disponibili numero totale di thread Demon thread Count Numero massimo di thread Conteggio totale dei thread iniziato

Oggetto:	Identificatori:	Attributi:	Punti dati:
Attività Flink	ID attività ID lavoro spazio dei nomi cluster	Server Node Name Job Name Sub Task Index Task ID tentativo attività numero tentativo attività Nome attività ID Task Manager ID nodo IP Current Input Watermark	Buffer in buffer di utilizzo del pool in buffer di lunghezza della coda buffer di utilizzo del pool out buffer di lunghezza della coda buffer di numero in buffer di numero locale in buffer di numero locale al secondo buffer di numero locale al secondo buffer di numero remoto in buffer di numero remoto al secondo buffer di numero in remoto per Numero di seconda velocità buffer di numero in uscita buffer di numero in uscita al secondo numero di numero di velocità buffer in uscita al secondo numero di velocità byte in numero locale byte in numero di secondo numero di velocità byte in numero remoto byte in numero di secondo numero di numero di byte in remoto Numero di tasso al secondo byte in uscita numero byte in uscita al secondo numero di byte in uscita al secondo numero di tasso Record in numero record in per secondo numero di conteggio Record in per secondo numero di tasso Record in uscita numero record in uscita al secondo numero di conteggio Record in uscita al secondo tasso

Oggetto:	Identificatori:	Attributi:	Punti dati:
Operatore attività Flink	Namespace del cluster ID del job ID dell'operatore ID del task	Server Nome nodo Nome lavoro Nome operatore attività secondaria Indice attività ID tentativo attività numero tentativo attività Nome attività ID gestore attività IP nodo	Input corrente filigrana Output corrente numero filigrana Record in numero Record in per secondo numero numero Record in per secondo numero tasso Record out numero Records out per secondo numero numero Records out per secondo numero Rate out per secondo numero Records ultimi Records abbandonati partizioni assegnate byte consumati Rate Commit latenza Avg Commit latenza Max commit Rate commits Failed Commits successed Connection Close Rate Connection Count Connection Creation Rate Conteggio Fetch Latency Avg Fetch Latency Max Fetch Rate Fetch Size Avg Fetch Size Max Fetch Throttle Time Avg Fetch Throttle Time Max Heartbeat Rate Incoming Byte Rate io Ratio Ratio Time Avg (ns) io Rapporto di attesa io tempo di attesa medio (ns) tasso di adesione tempo di adesione tempo medio ultimo battito cardiaco fa rete io tasso di uscita byte tasso record di tasso consumato record di tasso massimo di ritardo record per richiesta media velocità richiesta dimensione media richiesta dimensione massima risposta velocità di selezione velocità di sincronizzazione tempo di sincronizzazione tempo di risposta medio battito cardiaco Tempo max. Di Unione tempo max. Di sincronizzazione

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

Data Collector Hadoop

Data Infrastructure Insights utilizza questo data collector per raccogliere le metriche da Hadoop.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegli Hadoop.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.

[Configurazione di Hadoop] [Configurazione di Hadoop]

Setup (Configurazione)

Un'implementazione Hadoop completa comprende i seguenti componenti:

- NameNode: Il sistema primario HDFS (Distributed file System) di Hadoop. Coordina una serie di DataNode.
- Secondary NameNode (nodo secondario): Un failover a caldo per il nodo principale di NameNode. In Hadoop la promozione a NameNode non avviene automaticamente. Secondary NameNode raccoglie le informazioni da NameNode per essere pronto per essere promosso quando necessario.
- DataNode: Proprietario effettivo dei dati.
- ResourceManager: Il sistema primario di calcolo (yarn). Coordina una serie di NodeManager.
- NodeManager: La risorsa per il calcolo. Posizione effettiva per l'esecuzione delle applicazioni.
- JobHistoryServer: Responsabile della manutenzione di tutte le richieste relative alla cronologia del lavoro.

Il plugin Hadoop si basa sul plugin di telegraf, Jolokia. Come requisito per raccogliere informazioni da tutti i componenti Hadoop, JMX deve essere configurato ed esposto tramite Jolokia su tutti i componenti.

Compatibilità

La configurazione è stata sviluppata rispetto alla versione 2.9 di Hadoop.

Configurazione

Jolokia Agent Jar

Per tutti i singoli componenti, è necessario scaricare una versione del file Jar dell'agente di Jlokia. La versione testata era "Agente di Jookia 1.6.0".

Le istruzioni riportate di seguito presuppongono che il file jar scaricato (jookia-jvm-1.6.0-Agent.jar) sia posizionato nella posizione '/opt/hadoop/lib/'.

NameNode

Per configurare NameNode in modo da esporre l'API di Jookia, è possibile configurare quanto segue in <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.
```

Node secondario

Per configurare il nodo del nome secondario in modo che esponga l'API di Jookia, è possibile configurare quanto segue in <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

Per configurare i DataNode in modo che espongano l'API di Jookia, è possibile configurare quanto segue in <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

Per configurare ResourceManager in modo da esporre l'API di Jlokia, è possibile configurare quanto segue in <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

Per configurare i NodeManager in modo che espongano l'API di Jookia, è possibile configurare quanto segue in <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.
```

Server JobHistory

Per configurare il server di StoriaLavoro in modo che esponga l'API di Jookia, è possibile configurare quanto segue in <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.
```

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:
Node secondario Hadoop	Server dello spazio dei nomi del cluster	Nome nodo nodo IP Compile Info versione
Hadoop NodeManager	Server dello spazio dei nomi del cluster	Nome nodo IP nodo
ResourceManager di Hadoop	Server dello spazio dei nomi del cluster	Nome nodo IP nodo

Oggetto:	Identificatori:	Attributi:
DataNode Hadoop	Server dello spazio dei nomi del cluster	Nome nodo IP nodo ID cluster versione
Node di Hadoop	Server dello spazio dei nomi del cluster	Nome nodo IP nodo ID transazione ultimo tempo di scrittura dall'ultimo caricamento modifiche ha Stato file sistema Stato blocco ID pool ID cluster informazioni di compilazione versione distinta Conteggio versione
Hadoop JobHistoryServer	Server dello spazio dei nomi del cluster	Nome nodo IP nodo

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

HAProxy Data Collector

Data Infrastructure Insights utilizza questo data collector per raccogliere le metriche da HAProxy.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere HAProxy.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.

[Configurazione HAProxy]

Setup (Configurazione)

Il plug-in di Telegraf per HAProxy si basa sull'abilitazione delle statistiche HAProxy. Si tratta di una configurazione integrata in HAProxy, ma non è attivata subito. Se attivato, HAProxy espone un endpoint HTML che può essere visualizzato sul browser o scartato per l'estrazione dello stato di tutte le configurazioni HAProxy.

Compatibilità:

La configurazione è stata sviluppata con la versione 1.9 di HAProxy.

Configurazione:

Per abilitare le statistiche, modificare il file di configurazione hadproxy e aggiungere le seguenti righe dopo la sezione 'default', utilizzando il proprio utente/password e/o URL hadproxy:

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

Di seguito viene riportato un esempio semplificato di file di configurazione con le statistiche attivate:

```
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
```

Per istruzioni complete e aggiornate, vedere la "Documentazione HAProxy".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
HAProxy Frontend	Proxy degli indirizzi dello spazio dei nomi	Nodo IP Node Name Proxy ID Mode Process id Sessions Rate Limit Server id Sessions Limit Status	Byte in byte in uscita cache riscontri cache ricerche cache byte di compressione bypassati byte di compressione in byte di compressione in uscita risposte di compressione velocità di connessione velocità di connessione connessioni max Richieste totali negate da richieste di regole di connessione negate da problemi di sicurezza risposte negate da problemi di sicurezza Richieste negate da richieste di regole di sessione errori risposte 1xx Risposte 2xx risposte 3xx risposte 4xx risposte 5xx risposte altre richieste intercettate sessioni Rate numero massimo di richieste Rate numero massimo di richieste Rate numero massimo di richieste sessioni totali sessioni numero massimo di sessioni totale di richieste riscritte

Oggetto:	Identificatori:	Attributi:	Punti dati:
Server HAProxy	Server proxy degli indirizzi dello spazio dei nomi	Nodo IP Node Name Check Time to Finish Check Fall Configuration Check Health Value Check Rise Configuration Check Status Proxy ID Last Change Time Last Session Time Mode Process id Server id Status Weight	Server attivi Server di backup byte in byte out Check Downs Check fails il client interrompe le connessioni tempo medio downtime totale Denied Responses errori di connessione Responses 1xx Responses 2xx Responses 3xx Responses 4xx Responses 5xx Responses Other Server Selected Total Queue Current Queue Max Time Sessions Average per Seconda sessione al secondo Max Connection Reuse Response Time Sessions Average Sessions Max Server Transfer Aborts Sessions Total Time Average Requests Repatches Requests Requests Requests Requests Rewrite

Oggetto:	Identificatori:	Attributi:	Punti dati:
HAProxy back-end	Proxy degli indirizzi dello spazio dei nomi	Nodo IP Node Name ID proxy Last Change Time Last Session Time Mode Process id Server id Sessions Limit Status Weight	Server attivi Server di backup byte in byte out cache Hits Lookup cache Check Downs il client interrompe la compressione byte bypassati byte di compressione in byte di compressione out risposte di compressione connessioni tempo medio downtime totale richieste negate da problemi di sicurezza risposte negate da problemi di sicurezza errori di connessione errori di risposta risposte 1xx risposte 2xx risposte 3xx risposte 4xx risposte 5xx risposte Altro server selezionato coda totale coda corrente coda massima durata media sessioni al secondo Richieste max connessione tempo di risposta tempo di risposta sessioni max Server Transfer interrompe le sessioni totale sessioni tempo totale media richieste di reinvio Richieste tentativi Riscrive

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

Data Collector JVM

Data Infrastructure Insights utilizza questo data collector per raccogliere le metriche da JVM.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere JVM.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione

dell'agente" istruzioni.

3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.

[Configurazione JVM]

Setup (Configurazione)

Le informazioni sono disponibili in "Documentazione JVM".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
JVM	JVM spazio dei nomi	Architettura del sistema operativo Nome del sistema operativo versione Runtime specifica del runtime fornitore specifica del runtime versione tempo di attività Runtime Nome della macchina virtuale Runtime fornitore versione della macchina virtuale Nome del nodo IP	Classe caricata Classe totale caricata Classe scaricata memoria heap memoria impegnata heap Init memoria heap utilizzata memoria massima heap utilizzata memoria non heap memoria impegnata memoria non heap memoria init memoria non heap memoria massima non heap oggetti memoria utilizzati in attesa di finalizzazione OS processori disponibili OS memoria virtuale impegnata dimensione OS libero Memoria fisica dimensione OS spazio libero di swap dimensione OS massimo file descrittore Conteggio OS Open file Descriptors Conteggio OS processore CPU carico OS processore tempo SO sistema operativo carico sistema operativo carico sistema operativo medio totale memoria fisica dimensione OS spazio totale di swap dimensione thread Conteggio dei demon thread Conteggio dei picchi di thread Conteggio thread totale iniziato Conteggio Garbage Collector Copy Collection Conteggio Garbage Collector tempo di raccolta Garbage Collector Mark-sweep Collector Conteggio Garbage Collector tempo di raccolta Garbage Collector G1 tempo di raccolta Old Generation Garbage Collector G1 Conteggio raccolta Young Generation Garbage Collector G1 Tempo di raccolta di giovani generazioni Garbage Collector tempo di

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

Data Collector Kafka

Data Infrastructure Insights utilizza questo data collector per raccogliere metriche da Kafka.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegli Kafka.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.

[Configurazione di Kafka]

Setup (Configurazione)

Il plugin Kafka si basa sul plugin di telegraf, Jolokia. Come requisito per raccogliere informazioni da tutti i broker Kafka, JMX deve essere configurato ed esposto tramite Jolokia su tutti i componenti.

Compatibilità

La configurazione è stata sviluppata rispetto alla versione 0.11.0 di Kafka.

Configurazione

Tutte le istruzioni riportate di seguito presuppongono che la posizione di installazione di kafka sia "/opt/kafka". È possibile adattare le istruzioni riportate di seguito in base alla posizione di installazione.

Jolokia Agent Jar

Una versione il file Jolokia Agent jar deve essere "scaricato". La versione testata era l'agente di Jookia 1.6.0.

Le istruzioni riportate di seguito presuppongono che il file jar scaricato (jookia-jvm-1.6.0-Agent.jar) si trovi nella posizione '/opt/kafka/libs/'.

Kafka Brokers

Per configurare i broker Kafka in modo che espongano l'API di Jokia, è possibile aggiungere quanto segue in <KAFKA_HOME>/bin/kafka-server-start.sh, appena prima della chiamata '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"
```

Si noti che l'esempio precedente utilizza 'hostname -i' per impostare la variabile di ambiente 'RMI_HOSTNAME'. In più computer IP, questo dovrà essere modificato per raccogliere l'IP che si occupa delle connessioni RMI.

È possibile scegliere una porta diversa per JMX (9999 sopra) e Jlokia (8778). Se si dispone di un IP interno su cui bloccare Jolokia, è possibile sostituire il "catch all" 0.0.0.0 con il proprio IP. Si noti che questo IP deve essere accessibile dal plugin telegraf. Se non si desidera autenticare, è possibile utilizzare l'opzione '-Dcom.sun.management.jmxremote.authenticate=false'. Utilizzare a proprio rischio.

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:
Broker Kafka	Cluster namespace Broker	Nome nodo IP nodo

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

Kibana Data Collector

Data Infrastructure Insights utilizza questo data collector per raccogliere metriche da Kibana.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegli Kibana.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.

4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.

[Configurazione di Kibana]

Setup (Configurazione)

Le informazioni sono disponibili nella "Documentazione di Kibana".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Kibana	Indirizzo dello spazio dei nomi	Nodo IP Node Name Version Status (Stato versione nome nodo IP)	Connessioni simultanee heap massimo heap richieste utilizzate al secondo tempo di risposta medio tempo di risposta tempo di attività massimo

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

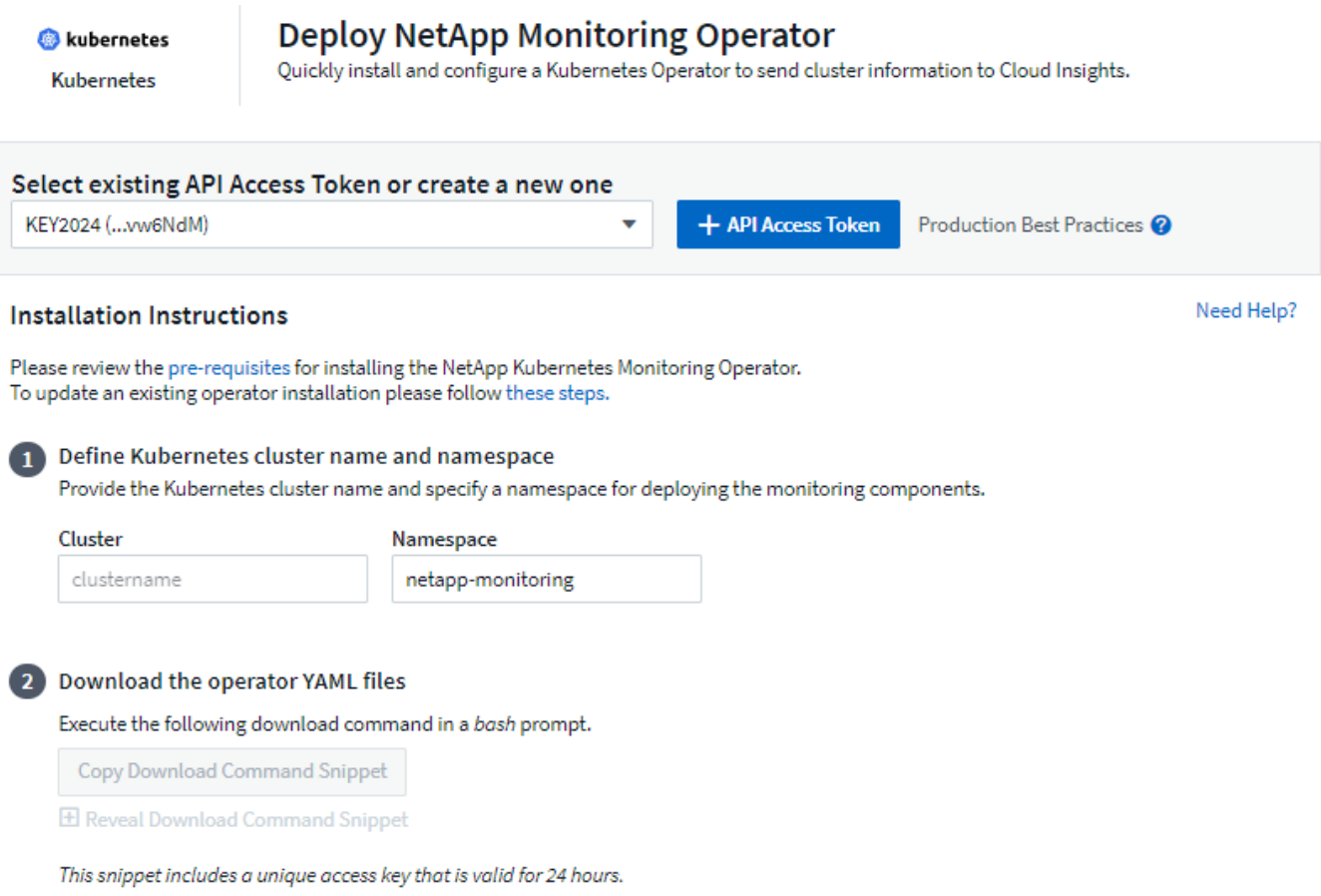
Installazione e configurazione dell'operatore di monitoraggio Kubernetes

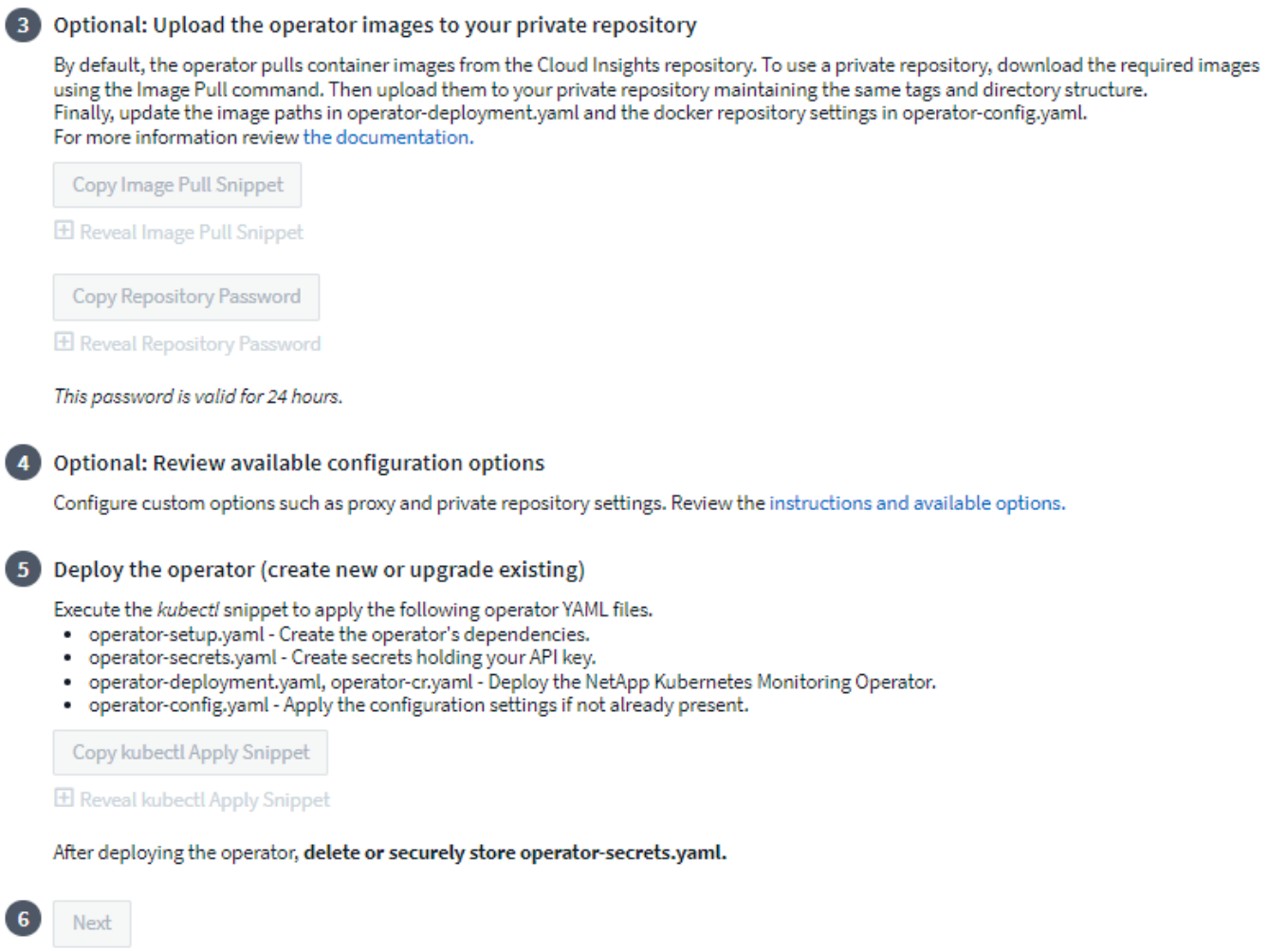
Data Infrastructure Insights offre la raccolta **Kubernetes Monitoring Operator** for Kubernetes. Navigare a **Kubernetes > Collector > +Kubernetes Collector** per implementare un nuovo operatore.

Prima di installare l'operatore di monitoraggio Kubernetes

Consultare la "Prerequisiti" documentazione prima di installare o aggiornare Kubernetes Monitoring Operator.

Installazione dell'operatore di monitoraggio Kubernetes


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



Passaggi per installare l'agente Kubernetes Monitoring Operator su Kubernetes:

1. Immettere un nome cluster e uno spazio dei nomi univoci. Se si aggiornamento in corsoproviene da un operatore Kubernetes precedente, utilizzare lo stesso nome cluster e lo stesso namespace.
2. Una volta immessi, è possibile copiare il frammento Download Command negli Appunti.
3. Incollare il frammento in una finestra *bash* ed eseguirlo. I file di installazione dell'operatore verranno scaricati. Tenere presente che il frammento ha una chiave univoca ed è valido per 24 ore.
4. Se si dispone di un repository personalizzato o privato, copiare il frammento Image Pull opzionale, incollarlo in una shell *bash* ed eseguirlo. Una volta estratte le immagini, copiarle nel repository privato. Assicurarsi di mantenere gli stessi tag e la stessa struttura di cartelle. Aggiornare i percorsi in *operator-deployment.yaml* e le impostazioni del repository di docker in *operator-config.yaml*.
5. Se lo si desidera, esaminare le opzioni di configurazione disponibili, ad esempio le impostazioni del proxy o del repository privato. È possibile leggere ulteriori informazioni su "opzioni di configurazione".
6. Quando sei pronto, implementa l'operatore copiando il frammento kubectl apply, scaricandolo ed eseguendolo.
7. L'installazione procede automaticamente. Una volta completata l'operazione, fare clic sul pulsante *Avanti*.
8. Al termine dell'installazione, fare clic sul pulsante *Next*. Assicurarsi inoltre di eliminare o memorizzare in modo sicuro il file *operator-secrets.yaml*.

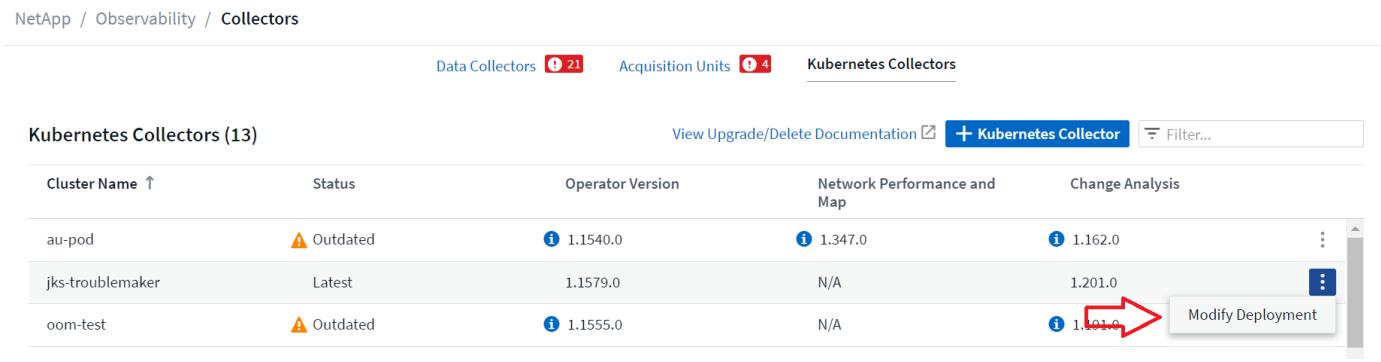
Se si dispone di un repository personalizzato, consultare informazioni su utilizzando un repository di docker personalizzato/privato.

Componenti di monitoring Kubernetes

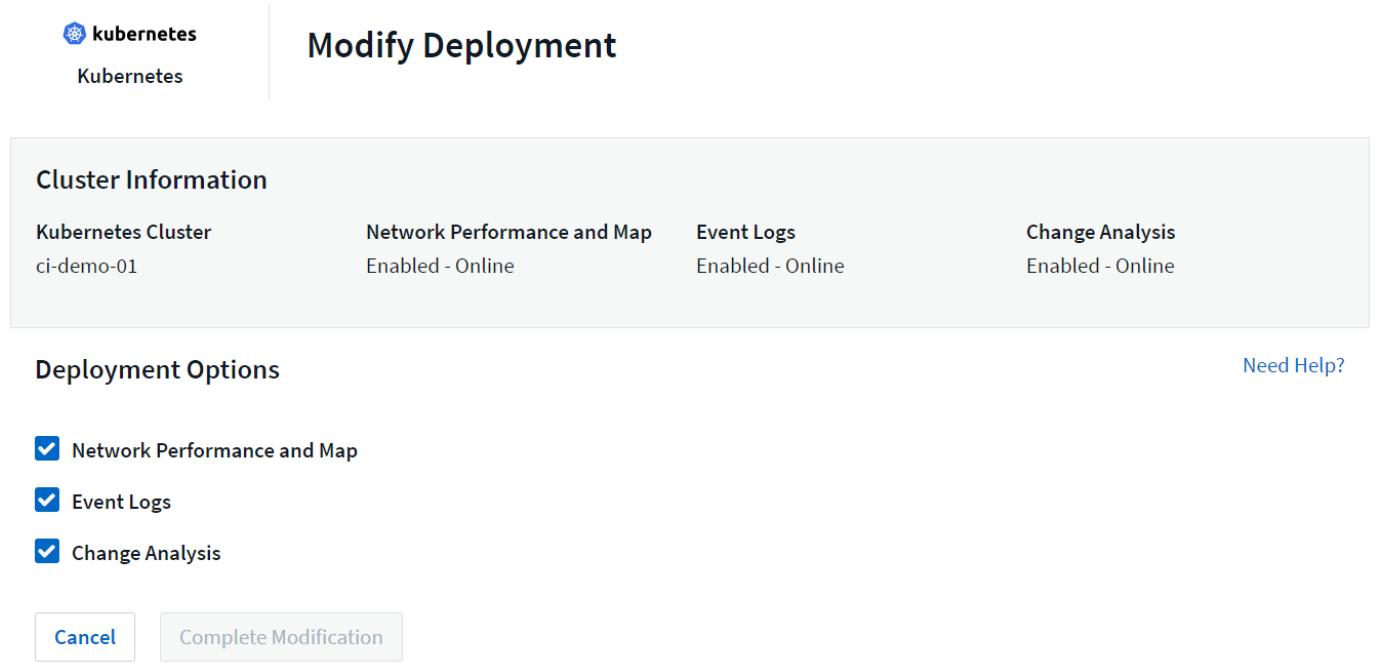
Data Infrastructure Insights Kubernetes Monitoring comprende quattro componenti di monitoring:

- Metriche cluster
- Mappa e prestazioni della rete (opzionale)
- Registri eventi (opzionali)
- Analisi delle modifiche (opzionale)

I componenti opzionali elencati in precedenza sono abilitati per impostazione predefinita per ogni collettore di Kubernetes; se si decide di non avere bisogno di un componente per un determinato collettore, è possibile disattivarlo accedendo a **Kubernetes > Collectors** e selezionando *Modify Deployment* dal menu "Three Dots" del collettore sulla destra dello schermo.



La schermata mostra lo stato corrente di ciascun componente e consente di disattivare o attivare i componenti per tale collettore, se necessario.



Aggiornamento alla versione più recente di Kubernetes Monitoring Operator

Aggiornamenti a pulsante DII

Puoi aggiornare Kubernetes Monitoring Operator attraverso la pagina DII Kubernetes Collectors. Fai clic sul menu accanto al cluster che desideri aggiornare e seleziona *Upgrade*. L'operatore verificherà le firme delle immagini, eseguirà un'istantanea dell'installazione corrente ed eseguirà l'aggiornamento. Entro pochi minuti dovrebbe essere visualizzato l'avanzamento dello stato dell'operatore attraverso l'aggiornamento in corso al più recente. Se si verifica un errore, è possibile selezionare lo stato Error (errore) per ulteriori dettagli e fare riferimento alla tabella di risoluzione dei problemi degli aggiornamenti a pulsante riportata di seguito.

Aggiornamenti a pulsante con repository privati

Se l'operatore è configurato per utilizzare un archivio privato, assicurarsi che tutte le immagini richieste per l'esecuzione dell'operatore e le relative firme siano disponibili nel repository. Se si verifica un errore durante il processo di aggiornamento per le immagini mancanti, è sufficiente aggiungerle al repository e riprovare l'aggiornamento. Per caricare le firme delle immagini nel vostro repository, usate lo strumento di cogenerazione come segue, assicurandovi di caricare le firme per tutte le immagini specificate in 3 opzionale: Caricate le immagini dell'operatore nel vostro repository privato > immagine pull Snippet

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

Ripristino di una versione precedente

Se l'aggiornamento è stato eseguito utilizzando la funzione di aggiornamento tramite pulsante e si verificano problemi con la versione corrente dell'operatore entro sette giorni dall'aggiornamento, è possibile eseguire il downgrade alla versione precedente utilizzando lo snapshot creato durante il processo di aggiornamento. Fai clic sul menu accanto al cluster che desideri ripristinare e seleziona *Roll back*.

Aggiornamenti manuali

Determinare se esiste una configurazione Agentcon l'operatore esistente (se lo spazio dei nomi non è il *monitoraggio netapp* predefinito, sostituire lo spazio dei nomi appropriato):

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
Se esiste una configurazione AgentConfiguration:
```

- Installare L'operatore più recente rispetto all'operatore esistente.
  - Assicurarsi di estrarre le immagini container più recentiutilizzare un repository personalizzato.

Se AgentConfiguration non esiste:

- Prendere nota del nome del cluster come riconosciuto da Data Infrastructure Insights (se il namespace non è quello predefinito di NetApp-monitoring, sostituire il namespace appropriato):

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Creare un backup dell'operatore esistente (se lo spazio dei nomi non è
il monitoraggio netapp predefinito, sostituire lo spazio dei nomi
appropriato):
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-operator,Disinstallare>>
L'operatore esistente.
* <<installing-the-kubernetes-monitoring-operator,Installare>>
L'operatore più recente.
```

- Utilizzare lo stesso nome del cluster.
- Dopo aver scaricato i file YAML dell'operatore più recenti, portare le personalizzazioni trovate in Agent_backup.yaml nell'operator-config.yaml scaricato prima di eseguire la distribuzione.
- Assicurarsi di estrarre le immagini container più recentiutilizzare un repository personalizzato.

Arresto e avvio dell'operatore di monitoraggio Kubernetes

Per arrestare l'operatore di monitoraggio Kubernetes:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
Per avviare l'operatore di monitoraggio Kubernetes:
```

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

Disinstallazione in corso

Per rimuovere l'operatore di monitoraggio Kubernetes

Si noti che il namespace predefinito per Kubernetes Monitoring Operator è "netapp-monitoring". Se è stato impostato uno spazio dei nomi personalizzato, sostituire tale spazio dei nomi in questi e in tutti i comandi e file successivi.

Le versioni più recenti dell'operatore di monitoraggio possono essere disinstallate con i seguenti comandi:

```
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 l'operatore di monitoraggio è stato distribuito nel proprio spazio dei nomi dedicato, eliminare lo spazio dei nomi:

```
 kubectl delete ns <NAMESPACE>
Nota: Se il primo comando restituisce "Nessuna risorsa trovata", seguire
le istruzioni riportate di seguito per disinstallare le versioni
precedenti dell'operatore di monitoraggio.
```

Eseguire ciascuno dei seguenti comandi nell'ordine indicato. A seconda dell'installazione corrente, alcuni di questi comandi potrebbero restituire messaggi "Object Not Found" (oggetto non trovato). Questi messaggi possono essere ignorati in modo sicuro.

```
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 in precedenza è stato creato un vincolo del contesto di protezione:

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

A proposito di Kube-state-metrics

NetApp Kubernetes Monitoring Operator installa le proprie metriche di stato kube per evitare conflitti con altre istanze.

Per informazioni su Kube-state-Metrics, vedere "questa pagina".

Configurazione/personalizzazione dell'operatore

Queste sezioni contengono informazioni sulla personalizzazione della configurazione dell'operatore, sull'utilizzo di proxy, sull'utilizzo di un repository di docker personalizzato o privato o sull'utilizzo di OpenShift.

Opzioni di configurazione

Le impostazioni più comunemente modificate possono essere configurate nella risorsa personalizzata *AgentConfiguration*. È possibile modificare questa risorsa prima di implementare l'operatore modificando il file *operator-config.yaml*. Questo file include esempi di impostazioni commentate. Vedere l'elenco di "impostazioni

disponibili" per la versione più recente dell'operatore.

È anche possibile modificare questa risorsa dopo che l'operatore è stato distribuito utilizzando il seguente comando:

```
 kubectl -n netapp-monitoring edit AgentConfiguration
Per determinare se la versione implementata dell'operatore supporta
AgentConfiguration, eseguire il seguente comando:
```

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Se viene visualizzato il messaggio "Error from server (notfound)" (errore
dal server (non trovato)), l'operatore deve essere aggiornato prima di
poter utilizzare AgentConfiguration.
```

Configurazione del supporto proxy

Esistono due posizioni in cui è possibile utilizzare un proxy sul tenant per installare l'operatore di monitoraggio Kubernetes. Questi possono essere sistemi proxy identici o separati:

- Proxy necessario durante l'esecuzione del frammento di codice di installazione (utilizzando "curl") per connettere il sistema in cui il frammento viene eseguito all'ambiente Data Infrastructure Insights
- Proxy necessario dal cluster Kubernetes di destinazione per comunicare con l'ambiente Data Infrastructure Insights

Se si utilizza un proxy per uno o per entrambi, per installare il monitor operativo Kubernetes è necessario innanzitutto assicurarsi che il proxy sia configurato in modo da consentire una buona comunicazione con l'ambiente Data Infrastructure Insights. Se si dispone di un proxy e si può accedere a Data Infrastructure Insights dal server/VM da cui si desidera installare l'operatore, è probabile che il proxy sia configurato correttamente.

Per il proxy utilizzato per installare il monitor operativo Kubernetes, prima di installare l'operatore, impostare le variabili di ambiente *http_proxy/https_proxy*. Per alcuni ambienti proxy, potrebbe essere necessario impostare la variabile *no_proxy environment*.

Per impostare le variabili, eseguire i seguenti passaggi sul sistema **prima** di installare l'operatore di monitoraggio Kubernetes:

1. Impostare le variabili di ambiente *https_proxy* e/o *http_proxy* per l'utente corrente:
   a. Se il proxy da configurare non dispone dell'autenticazione (nome utente/password), eseguire il seguente comando:

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Se il proxy da configurare dispone dell'autenticazione (nome
utente/password), eseguire questo comando:
```

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

Per il proxy utilizzato per il cluster Kubernetes e per comunicare con l'ambiente Data Infrastructure Insights, installare Kubernetes Monitoring Operator dopo aver letto tutte queste istruzioni.

Configurare la sezione proxy di AgentConfiguration in operator-config.yaml prima di distribuire l'operatore di monitoraggio 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
  ...
...
```

Utilizzando un repository di docker personalizzato o privato

Per impostazione predefinita, l'operatore di monitoring Kubernetes estrarrà le immagini dei container dal repository di Data Infrastructure Insights. Se hai un cluster Kubernetes utilizzato come destinazione per il monitoring e tale cluster è configurato in modo da estrarre solo le immagini dei container da un repository Docker o da un registro dei container personalizzato o privato, devi configurare l'accesso ai container necessari da Kubernetes Monitoring Operator.

Eseguire il frammento Image Pull dalla sezione di installazione di NetApp Monitoring Operator. Questo comando consente di accedere al repository Data Infrastructure Insights, di estrarre tutte le dipendenze dell'immagine per l'operatore e di disconnettersi dal repository Data Infrastructure Insights. Quando richiesto, inserire la password temporanea del repository fornita. Questo comando scarica tutte le immagini utilizzate dall'operatore, incluse le funzioni opzionali. Vedere di seguito per quali funzioni vengono utilizzate queste immagini.

Funzionalità principale dell'operatore e monitoraggio Kubernetes

- monitoraggio netapp
- ci-kube-rbac-proxy
- ci-ksm
- ci-telegraf
- distroless-root-user

Registro eventi

- ci-fluent-bit
- ci-kukasub-esportatore-di-eventi

Mappa e performance di rete

- ci-net-osservatore

Trasferire l'immagine del gestore nel repository del supporto privato/locale/aziendale in base alle policy aziendali. Verificare che i tag delle immagini e i percorsi delle directory per queste immagini nel repository siano coerenti con quelli nel repository Data Infrastructure Insights.

Modificare l'implementazione dell'operatore di monitoraggio in operator-deployment.yaml e modificare tutti i riferimenti alle immagini per utilizzare il repository Docker privato.

```
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>
```

Modificare la configurazione dell'agente in operator-config.yaml in modo che rifletta la nuova posizione del responsabile del docker. Crea un nuovo imagePullSecret per il tuo repository privato, per maggiori dettagli vedi *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
```

Istruzioni per OpenShift

Se si utilizza OpenShift 4.6 o versione successiva, è necessario modificare la configurazione dell'agente in *operator-config.yaml* per attivare l'impostazione *runPrivileged*:

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

OpenShift potrebbe implementare un ulteriore livello di sicurezza che potrebbe bloccare l'accesso ad alcuni componenti di Kubernetes.

Tolerazioni e contamini

I DaemonSet *netapp-ci-telegraf-ds*, *netapp-ci-fluent-bit-ds* e *netapp-ci-net-observer-L4-ds* devono pianificare un pod su ogni nodo del cluster per raccogliere correttamente i dati su tutti i nodi. L'operatore è stato configurato in modo da tollerare alcuni **segni** noti. Se sono stati configurati dei tag personalizzati sui nodi, impedendo così l'esecuzione dei pod su ogni nodo, è possibile creare una **tolleranza** per tali tag "In *AgentConfiguration*". Se sono stati applicati dei tipi di manutenzione personalizzati a tutti i nodi del cluster, è necessario aggiungere anche le tolleranze necessarie all'implementazione dell'operatore per consentire la pianificazione e l'esecuzione del pod operatore.

Scopri di più su Kubernetes "Contamini e pedaggi".

Tornare al **"Pagina Installazione dell'operatore di monitoraggio NetApp Kubernetes"**

Una nota sui segreti

Per rimuovere l'autorizzazione per l'operatore di monitoraggio Kubernetes a visualizzare segreti a livello del cluster, eliminare le seguenti risorse dal file *operatore-setup.yaml* prima di eseguire l'installazione:

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

Se si tratta di un aggiornamento, eliminare anche le risorse dal cluster:

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

Se l'analisi delle modifiche è attivata, modificare *AgentConfiguration* o *operator-config.yaml* per annullare il commento alla sezione di gestione delle modifiche e includere *kindsToIgnoreFromWatch: "'secrets"'* nella sezione di gestione delle modifiche. Notare la presenza e la posizione di virgolette singole e doppie in questa riga.

```
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"'
  ...
```

Verifica delle firme dell'immagine dell'operatore di monitoraggio Kubernetes

L'immagine per l'operatore e tutte le immagini correlate che implementa sono firmate da NetApp. Puoi verificare manualmente le immagini prima dell'installazione usando lo strumento csign, o configurare un controller di ammissione Kubernetes. Per ulteriori informazioni, vedere "Documentazione Kubernetes".

La chiave pubblica utilizzata per verificare le firme delle immagini è disponibile nel riquadro di installazione dell'operatore di monitoraggio in *Optional: Upload the operator images to your private repository > Image Signature Public Key*

Per verificare manualmente la firma di un'immagine, attenersi alla seguente procedura:

1. Copiare ed eseguire il frammento di estrazione dell'immagine
2. Quando richiesto, copiare e immettere la password dell'archivio
3. Memorizzare la chiave pubblica di firma dell'immagine (dii-image-signing.pub nell'esempio)
4. Verificare le immagini utilizzando il copiglia. Fare riferimento al seguente esempio di utilizzo dei cognomi

```
$ 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}]
```

Risoluzione dei problemi

Alcuni elementi da provare in caso di problemi durante la configurazione dell'operatore di monitoring Kubernetes:

Problema:	Prova:
Non viene visualizzato un collegamento ipertestuale/connessione tra il volume persistente Kubernetes e il dispositivo di storage back-end corrispondente. Il volume persistente Kubernetes viene configurato utilizzando il nome host del server di storage.	Seguire la procedura per disinstallare l'agente Telegraf esistente, quindi reinstallare l'agente Telegraf più recente. Devi utilizzare Telegraf versione 2,0 o successiva e lo storage del cluster Kubernetes deve essere monitorato attivamente da Data Infrastructure Insights.
Sto vedendo messaggi nei log che assomigliano a quanto segue: E0901 15:21 178 v1:39,962145 1 k8s k8s Reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Impossibile elencare *352.MutatingWebhookConfigurazione: Il server non ha trovato la risorsa richiesta E0901 15:21:43,168161 1:v1 Reflector.go.me.get coordinazione del server.go.oblies	Questi messaggi possono verificarsi se si utilizza kube-state-metrics versione 2.0.0 o superiore con versioni di Kubernetes inferiori alla 1.20. Per ottenere la versione di Kubernetes: *Kubectl version* per ottenere la versione di kube-state-metrics: *Kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* per evitare che questi messaggi si verifichino, gli utenti possono modificare la loro implementazione di kube-state-metrics per disabilitare le seguenti Leases: _Mutatingwebcooki_argomenti_conservil possono usare le configurazioni_convalide_costruzione_web: Resources=certificatesigningrequests,configmaps,crontowjobs,demonset,implementazioni,endpoint,horizontalpodautoscaler,ingassets,proxims, validatingwebhookconfigurations,volumeattachments"
Vedo messaggi di errore da Telegraf che assomigliano ai seguenti, ma Telegraf si avvia ed esegue: Oct 11 14:23:41:00 ip-172-31-39-47 systemd[1]: Avviato l'agente server plugin-driven per la generazione di rapporti in InfluxDB. Ottobre 11 14:23:41 ip-172-31-39-47 telegraf[1827]: Time="2021-10-11T14:23:41Z" level=error msg="Impossibile creare la directory della cache. /Etc/telegraf/.cache/snowflake, err: Mkdir /etc/telegraf/.ca che: Permesso negato. Ignorato\n" func="gosnowflake.(*defaultLogger).errorf" file="log.go:172 1827 23" ott 2021 41Z:39-47 10 ip-31-23:41 telegraf[120]:-11 14"="errore di apertura. Ignorato. Open /etc/telegraf/.cache/snowflake/ocsp_Response_cache.json: No such file o directory\n" func="gosnowflake.(*defaultLogger).errorf" file="log.go:23" Oct 2021 41Z:10 ip-1827-31:39-47 traf[172]: 11 14-23:41:120! Avvio di Telegraf 1.19.3	Si tratta di un problema noto. Per "Questo articolo di GitHub"ulteriori dettagli, fare riferimento a. Finché Telegraf è in funzione, gli utenti possono ignorare questi messaggi di errore.

Problema:	Prova:
Su Kubernetes, i miei pod Telegraf riportano il seguente errore: "Errore nell'elaborazione delle informazioni sui mountstats: Impossibile aprire il file mountstats: /Hostfs/proc/1/mountstats, errore: Open /hostfs/proc/1/mountstats: Permesso negato"	Se SELinux è abilitato e abilitato, probabilmente impedisce ai pod Telegraf di accedere al file /proc/1/mountstats sul nodo Kubernetes. Per superare questa restrizione, modificare la configurazione dell'agente e attivare l'impostazione runPrivileged. Per maggiori dettagli, fare riferimento alle istruzioni di OpenShift.
Su Kubernetes, il mio pod ReplicaSet Telegraf riporta il seguente errore: [inputs.prometheus] errore nel plugin: Impossibile caricare la coppia di chiavi /etc/kubernetes/pki/etcd/server.crt:/etc/kubernetes/pki/etcd/server.key: Aprire /etc/kubernetes/pki/etcd/server.no	Il pod ReplicaSet di Telegraf è destinato all'esecuzione su un nodo designato come master o etcd. Se il pod ReplicaSet non è in esecuzione su uno di questi nodi, si otterranno questi errori. Verificare se i nodi master/etcd presentano delle contaminazioni. In tal caso, aggiungere le tolleranze necessarie a Telegraf ReplicaSet, telegraf-rs. Ad esempio, modificare il Replica Set… kubectl edita rs telegraf-rs …e aggiunga le tolleranze appropriate alla specifica. Quindi, riavviare il pod ReplicaSet.
Ho un ambiente PSP/PSA. Questo influisce sul mio operatore di monitoraggio?	Se il cluster Kubernetes è in esecuzione con Pod Security Policy (PSP) o Pod Security Admission (PSA), è necessario eseguire l'aggiornamento all'ultima versione di Kubernetes Monitoring Operator. Per eseguire l'aggiornamento all'operatore corrente con il supporto per PSP/PSA, procedere come segue: 1. Disinstallare l'operatore di monitoraggio precedente: 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-ruolo-proxy agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-rolebinding-proxy-ading-cluster-2. Installare la versione più recente dell'operatore di monitoraggio.
Ho riscontrato dei problemi durante la distribuzione dell'operatore e ho utilizzato PSP/PSA.	1. Modificare l'agente usando il seguente comando: Kubectl -n <name-space> edit Agent 2. Contrassegna "Security-policy-enabled" come "false". In questo modo si disattivano i criteri di protezione del pod e l'ammissione alla protezione del pod e si consente all'operatore di eseguire la distribuzione. Confermare con i seguenti comandi: Kubectl Get psp (dovrebbe mostrare la politica di sicurezza Pod rimossa) kubectl Get all -n <namespace>
grep -i psp (dovrebbe mostrare che non viene trovato nulla)	Errori "ImagePullBackoff" rilevati

Problema:	Prova:
Questi errori possono essere rilevati se si dispone di un repository di docker personalizzato o privato e non è ancora stato configurato l'operatore di monitoraggio Kubernetes in modo da riconoscerlo correttamente. Scopri di più informazioni sulla configurazione per repo personalizzato/privato.	Si verifica un problema con l'implementazione dell'operatore di monitoraggio e la documentazione corrente non mi aiuta a risolverlo.

Acquisire o annotare in altro modo l'output dei seguenti comandi e contattare il team di supporto tecnico.
`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`
	I pod Net-observer (mappa del carico di lavoro) nello spazio dei nomi Operator si trovano in CrashLoopBackOff

Questi pod corrispondono al data collector Workload Map per l'osservabilità della rete. Prova: • Verifica i log di uno dei pod per confermare la versione minima del kernel. Ad esempio: ---- {"ci-tenant-id":"your-tenant-id","collector-cluster":"your-k8s-cluster-name","ambiente":"prod","level":"error","msg":"failed in validation. Motivo: La versione del kernel 3.10.0 è inferiore alla versione minima del kernel di 4.18.0","Time":"2022-11-09T08:23:08Z"} --- • i pod Net-Observer richiedono che la versione del kernel Linux sia almeno 4.18.0. Controllare la versione del kernel usando il comando "uname -r" e assicurarsi che siano >= 4.18.0	I pod vengono eseguiti in Operator namespace (predefinito: Monitoring netapp), ma non vengono visualizzati dati nell'interfaccia utente per la mappa dei carichi di lavoro o le metriche Kubernetes nelle query
Controllare l'impostazione dell'ora sui nodi del cluster K8S. Per un controllo accurato e la creazione di report dei dati, si consiglia di sincronizzare l'ora sul computer dell'agente utilizzando il protocollo NTP (Network Time Protocol) o SNTP (Simple Network Time Protocol).	Alcuni dei pod net-observer nello spazio dei nomi Operator sono in stato Pending

Problema:	Prova:
NET-osservatore è un DemonSet che esegue un pod in ogni nodo del cluster k8s. • Prendere nota del pod in stato Pending (in sospeso) e verificare se si verifica un problema di risorse per la CPU o la memoria. Assicurarsi che la memoria e la CPU richieste siano disponibili nel nodo.	Nei miei registri, subito dopo l'installazione dell'operatore di monitoraggio di Kubernetes, viene visualizzato quanto segue: [inputs.prometheus] errore nel plugin: Errore durante la richiesta HTTP a 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: No such host
Questo messaggio viene visualizzato in genere solo quando viene installato un nuovo operatore e il pod *telegraf-rs* è attivo prima che il pod *ksm* sia attivo. Questi messaggi dovrebbero interrompersi una volta che tutti i pod sono in esecuzione.	Non vedo alcuna metrica raccolta per Kubernetes Cronjobs che esiste nel mio cluster.
Verificare la versione di Kubernetes (ad es. `kubectl version`). Se è v1.20.x o inferiore, si tratta di un limite previsto. La release kube-state-metrics implementata con Kubernetes Monitoring Operator supporta solo v1.cronjob. Con Kubernetes 1.20.x e versioni precedenti, la risorsa cronjob è v1beta.cronjob. Di conseguenza, le metriche dello stato del kube non riescono a trovare la risorsa di crono-job.	Dopo aver installato l'operatore, i pod telegraf-ds entrano in CrashLoopBackOff e i registri del pod indicano "su: Authentication failure" (su: Errore di autenticazione).
Modificare la sezione telegraf in *AgentConfiguration* e impostare *dockerMetricCollectionEnabled* su false. Per ulteriori dettagli, fare riferimento alla "opzioni di configurazione". telegraf: … - Name: docker run-mode: - DaemonSet sostituzioni: - Chiave: DOCKER_UNIX_SOCK_PLACEHOLDER valore: unix://run/docker.sock … …	Vedo messaggi di errore ricorrenti simili ai seguenti nei miei registri Telegraf: E! [Agent] errore di scrittura in outputs.http: Post "https://<tenant_url>/REST/v1/Lake/ingerment/influenzxdb": Scadenza contesto superata (client. Timeout durante l'attesa delle intestazioni)
Modificare la sezione telegraf in *AgentConfiguration* e aumentare *outputTimeout* a 10s. Per ulteriori dettagli, fare riferimento alla "opzioni di configurazione".	Mancano i dati *involvedobject* per alcuni registri eventi.
Assicurarsi di aver seguito i passaggi descritti nella "Permessi"sezione precedente.	Perché vedo due pod operatore di monitoring in esecuzione, uno denominato netapp-ci-monitoring-operator-<pod> e l'altro denominato monitoring-operator-<pod>?
A partire dal 12 ottobre 2023, Data Infrastructure Insights ha ridefinito l'operatore per servire meglio i nostri utenti; affinché tali modifiche vengano completamente adottate, è necessario rimuovere il vecchio operatore e installare il nuovo.	I miei eventi kuowdi hanno interrotto inaspettatamente la segnalazione a Data Infrastructure Insights.

Problema:	Prova:
Recuperare il nome del pod dell'esportatore di eventi: `kubectl -n netapp-monitoring get pods`	grep event-exporter
awk '{print $1}'	sed 's/event-exporter./event-exporter/` Deve essere "netapp-ci-event-exportant" o "event-exportant". Quindi, modificare l'agente di monitoraggio `kubectl -n netapp-monitoring edit agent` e impostare il valore per LOG_FILE in modo che rifletta il nome del pod dell'esportatore di eventi appropriato trovato nel passaggio precedente. In particolare, LOG_FILE deve essere impostato su "/var/log/containers/netapp-ci-event-exportant.log" o "/var/log/containers/event-exportant*.log" …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. In alternativa, si può anche disinstallazione e reinstallare l'agente.
Sto vedendo i pod implementati dal crash dell'operatore di monitoring Kubernetes a causa di risorse insufficienti.	Fare riferimento a Kubernetes Monitoring Operator "opzioni di configurazione" per aumentare i limiti di CPU e/o memoria secondo necessità.
Un'immagine mancante o una configurazione non valida ha causato il mancato avvio o la mancata preparazione dei pod di metriche a stato di netapp-ci-kube. Ora StatefulSet è bloccato e le modifiche della configurazione non vengono applicate ai pod di metriche stato netapp-ci-kube.	StatefulSet è in uno "rotto" stato. Dopo aver risolto eventuali problemi di configurazione, bounce i pod di metrica stato netapp-ci-kube.
I pod con metriche a stato di netapp-ci-kube non si avviano dopo l'aggiornamento di un operatore Kubernetes, lanciando ErrImagePull (non riuscendo a estrarre l'immagine).	Provare a reimpostare i pod manualmente.
I messaggi "evento scartato come vecchio allora maxEventAgeSeconds" vengono osservati per il mio cluster Kubernetes in Log Analysis.	Modificare l'operatore *agentconfiguration* e aumentare il *event-exportant-maxEventAgeSeconds* (cioè a 60s), il *event-exportant-kubeQPS* (cioè a 100) e il *event-exportant-kubeBurst* (cioè a 500). Per ulteriori informazioni su queste opzioni di configurazione, consultare la "opzioni di configurazione" pagina.

Problema:	Prova:
Telegraf avverte di, o si blocca a causa di, memoria bloccabile insufficiente.	Provare ad aumentare il limite di memoria bloccabile per Telegraf nel sistema operativo/nodo sottostante. Se l'aumento del limite non è un'opzione, modificare la configurazione dell'agente NKMO e impostare *non protetto* su *true*. In questo modo, Telegraf non tenterà di riservare pagine di memoria bloccate. Sebbene ciò possa rappresentare un rischio per la sicurezza poiché i segreti decrittografati potrebbero essere scambiati sul disco, consente l'esecuzione in ambienti in cui non è possibile riservare la memoria bloccata. Per ulteriori informazioni sulle opzioni di configurazione *non protetto*, fare riferimento alla "opzioni di configurazione"pagina.
Vedo messaggi di avviso da Telegraf simili a quanto segue: *W! [Inputs.diskio] Impossibile raccogliere il nome del disco per "vdc": Errore di lettura /dev/vdc: Nessun file o directory*	Per l'operatore di monitoring Kubernetes, questi messaggi di avviso sono benigni e possono essere ignorati in modo sicuro. In alternativa, modificare la sezione telegraf in AgentConfiguration e impostare *runDsPrivileged* su true. Per ulteriori informazioni, fare riferimento alla "opzioni di configurazione dell'operatore".

Problema:	Prova:

Il mio Fluent-bit pod non funziona con i seguenti errori: [2024/10/16 14 16:16 23:23] [errore] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:tail,0 errno=2024] troppi file aperti [10/16 14/10/16 14:16:23] [errore] Inizializzazione input non riuscita [24/2024:360] [errore] [motore] Inizializzazione non riuscita	Prova a modificare le impostazioni di *fsnotify* nel 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>`
	
	Riavviare Fluent-bit.
	
	Nota: Per rendere queste impostazioni persistenti durante i riavvii dei nodi, è necessario inserire le seguenti righe in */etc/sysctl.conf*
	
	`fs.inotify.max_user_instances=<something larger than current setting>`
	`fs.inotify.max_user_watches=<something larger than current setting>`

I pod DS di telegraf riportano errori relativi al mancato invio di richieste HTTP da parte del plugin di input kuPdi a causa dell’impossibilità di convalidare il certificato TLS. Ad esempio: E! [Inputs.kuPQ] errore nel plugin: Errore durante la richiesta HTTP di "<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary":ottenere "<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": tls: Impossibile verificare il certificato: X509: Impossibile convalidare il certificato per <kubelet_IP> perché non contiene alcuna SAN IP	Questo si verifica se il kubelet utilizza certificati autofirmati e/o il certificato specificato non include il <kubelet_IP> nell'elenco dei certificati *Subject alternative Name*. Per risolvere questo problema, l'utente può modificare il "configurazione dell'agente"e impostare *telegraf:insecureK8sSkipVerify* su *true*. Questo configurerà il plugin di input telegraf per saltare la verifica. In alternativa, l'utente può configurare il kubelet per "ServerTLSBootstrap", che attiverà una richiesta di certificato dall'API 'certificates.k8s.io'.

Ulteriori informazioni sono disponibili nella "Supporto"pagina o nella "Matrice di supporto Data Collector".

Data Collector Memcached

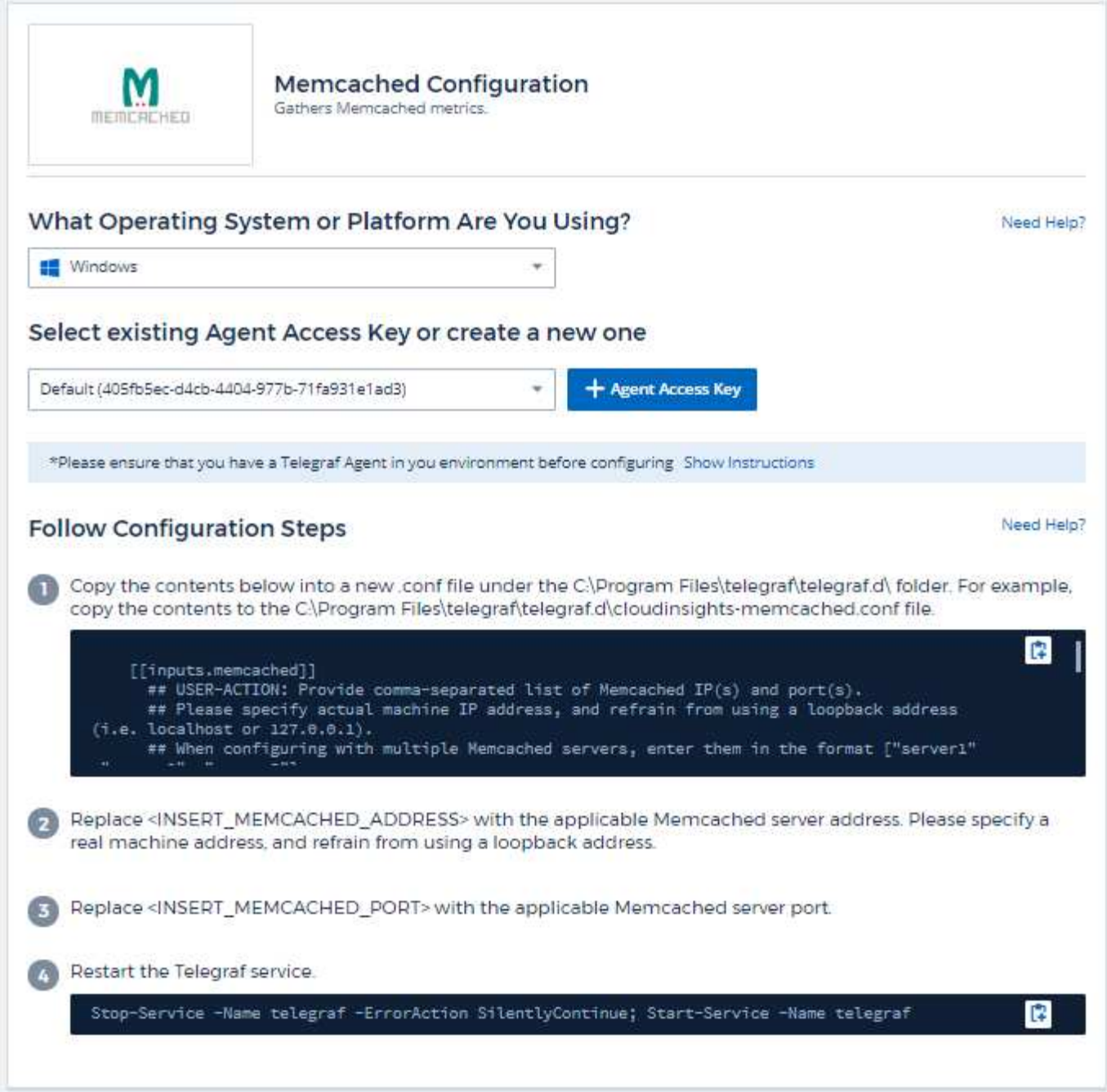
Data Infrastructure Insights utilizza questo data collector per raccogliere metriche da Memcached.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Memcached.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili nella "Wiki Memcached".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Memcached	Server namespace	Nome nodo IP	Accettazione delle connessioni richieste di autenticazione gestite autenticazioni non riuscite byte utilizzati byte lettura (per sec) byte scritti (per sec) CAS Badval CAS accessi CAS errori requisiti di flusso (per sec) ottenere requisiti (per sec) requisiti impostati (per sec) requisiti di tocco (per sec) rese di connessione (per sec) Strutture di connessione connessioni aperte elementi memorizzati correnti Richieste di decr riscontri (per sec) Richieste di decr perse (per sec) Richieste di eliminazione riscontri (per sec) Richieste di eliminazione mancati (per sec) elementi sfratti validi elementi scaduti riscontri (per sec) Hash byte utilizzati Hash sta espandendo Hash Power Level Incr Requests Hits (per sec) Incr Requests miss (per sec) Server Max byte Listen Disabled Num Reclaimed Worker Threads Conteggio totale connessioni aperte totale elementi memorizzati Touch Hits Touch manca il tempo di attività del server

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

MongoDB Data Collector

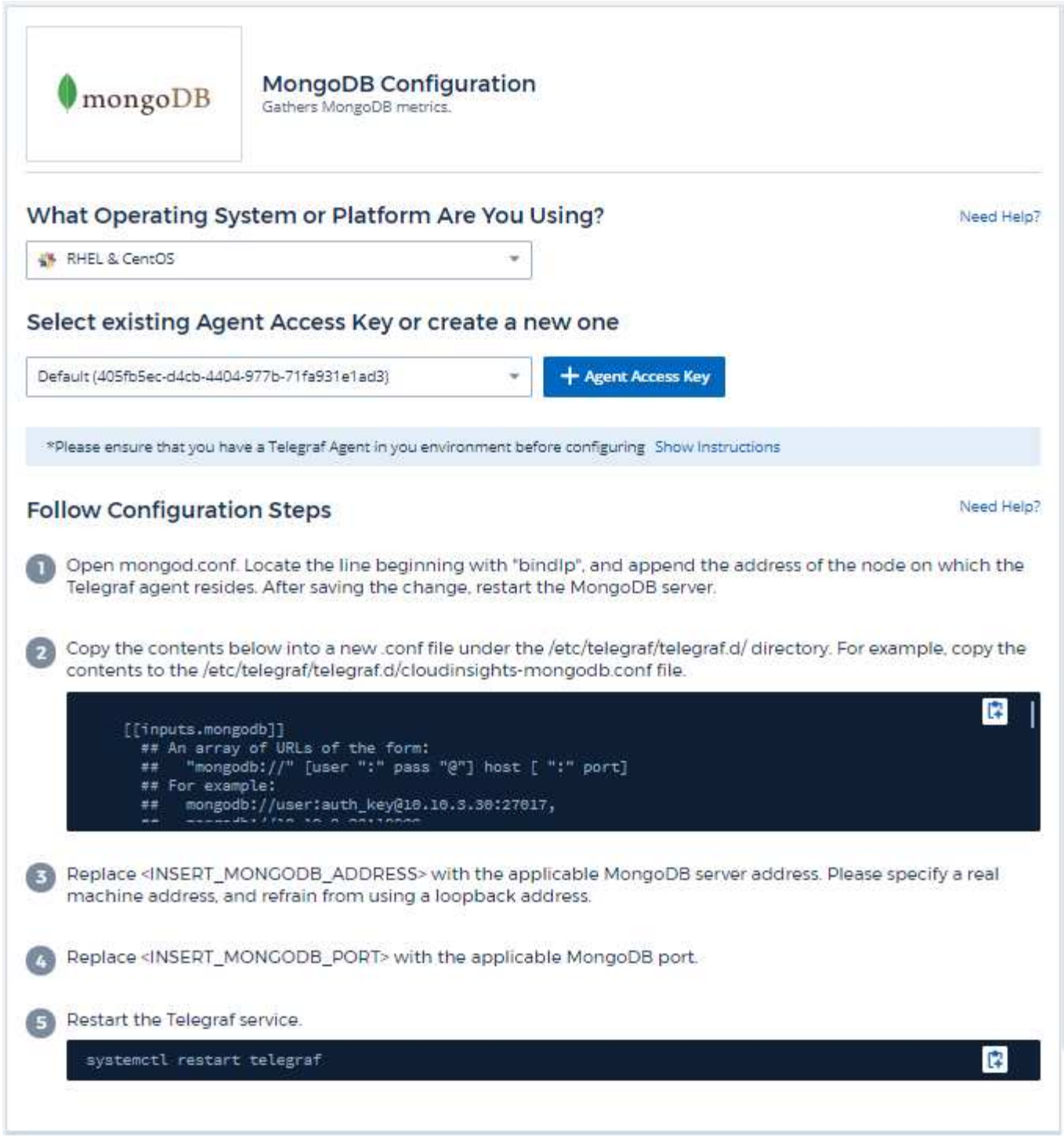
Data Infrastructure Insights utilizza questo data collector per raccogliere metriche da MongoDB.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegli MongoDB.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili nella "Documentazione MongoDB".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
MongoDB	Nome host dello spazio dei nomi		
Database MongoDB	Nome host dello spazio dei nomi Nome database		

Risoluzione dei problemi

Le informazioni sono disponibili nella "Supporto" pagina .

MySQL Data Collector

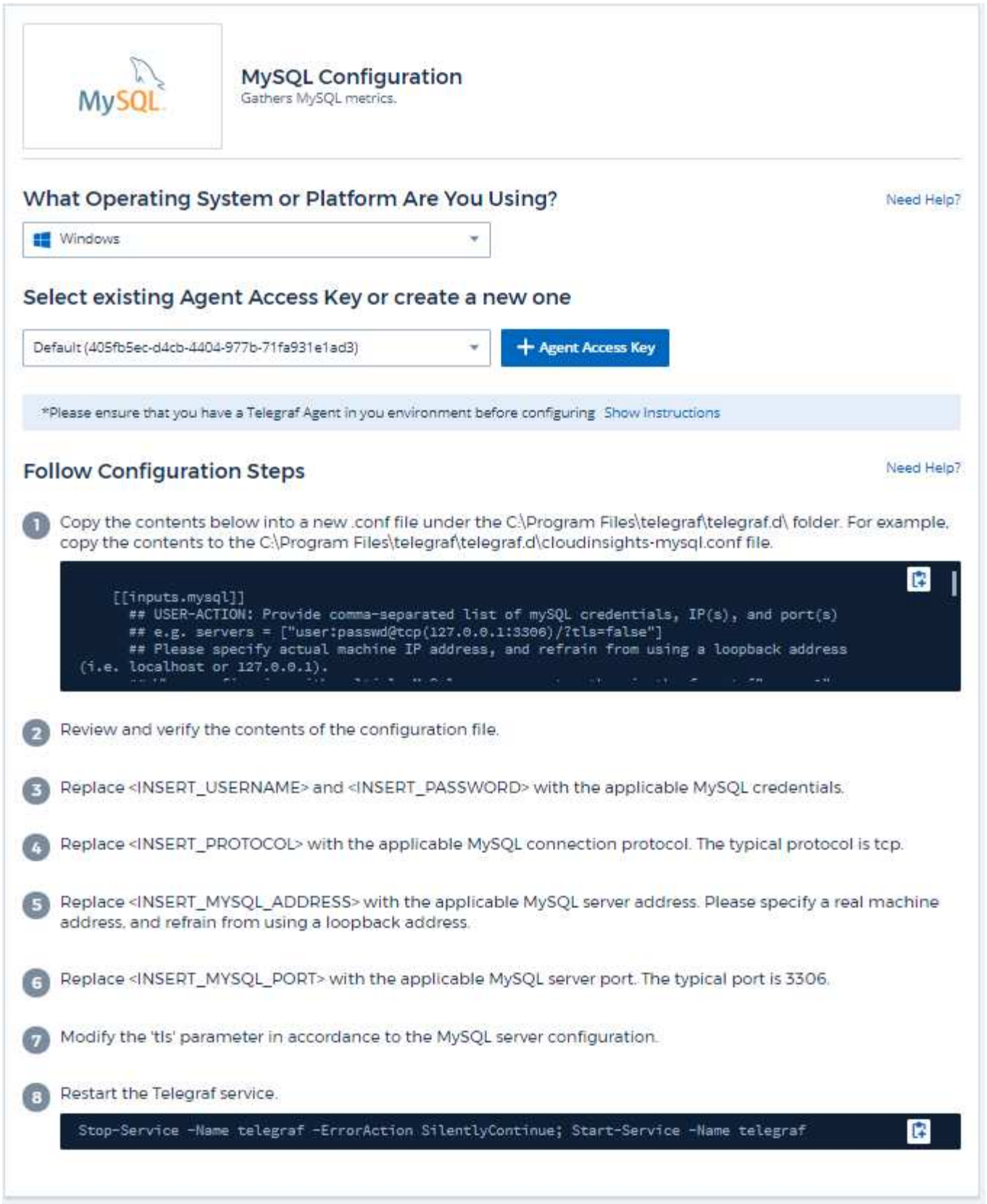
Data Infrastructure Insights utilizza questo data collector per raccogliere le metriche da MySQL.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegli MySQL.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili nella "Documentazione MySQL".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
MySQL	Namespace server MySQL	Nome nodo IP	Client interrotti (per sec) connessioni interrotte (per sec) byte RX (per sec) byte TX (per sec) comandi Admin (per sec) Comandi Alter comandi evento Alter comandi funzione Alter comandi istanza Alter comandi procedura Alter comandi server comandi Alter comandi tabella Alter comandi tablespace Alter comandi utente Analyze comandi Assegna a Keycache comandi Begin comandi Binlog comandi procedura di chiamata comandi Cambia comandi DB Cambia comandi master Cambia comandi filtro Repl comandi di controllo Comandi checksum comandi commit Crea comandi DB Crea comandi evento Crea comandi funzione Crea comandi indice Crea comandi procedura Crea comandi server Crea comandi tabella Crea comandi trigger Crea comandi UDF Crea comandi utente Crea comandi Visualizza Dealloc SQL errori di connessione Accetta tabelle dischi tmp creati errori ritardati comandi Flush Handler Commit InnoDB buffer Pool byte Data Key Blocks Not Flushed Key Requests Key Write Key Write Max Execution Time Exceeded Max Connections Open Files Performance Schema Accounts Lost Prepared stmt Count Qcache Free Blocks Questions Select Full Join Select Full Range Join Select Range Check Selezionare Scan Table Locks immediate (blocco immediato tavolo di

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

Netstat Data Collector

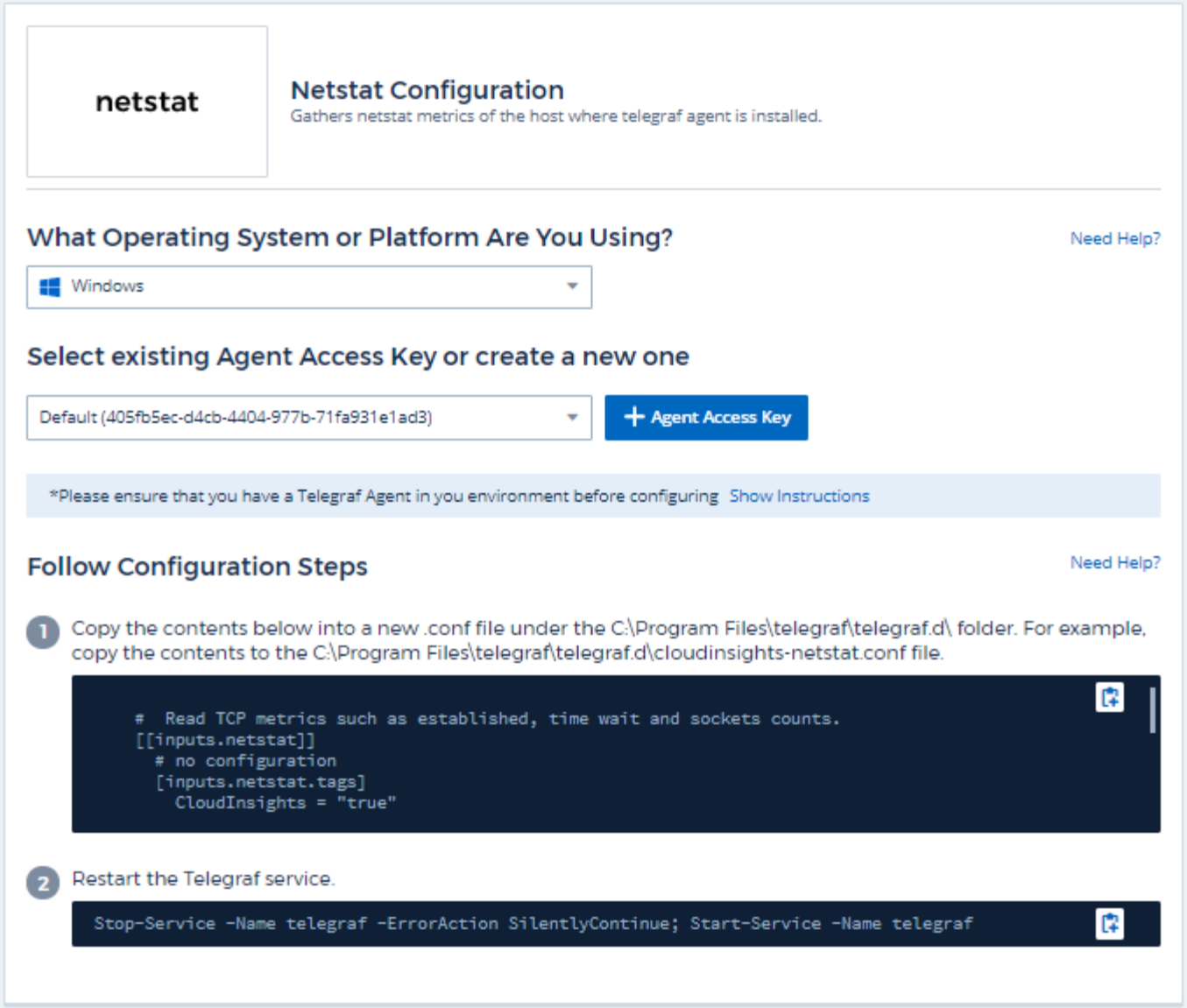
Data Infrastructure Insights utilizza questo data collector per raccogliere le metriche Netstat.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Netstat.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Netstat	UUID nodo	Nome nodo IP	

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

Data Collector nginx

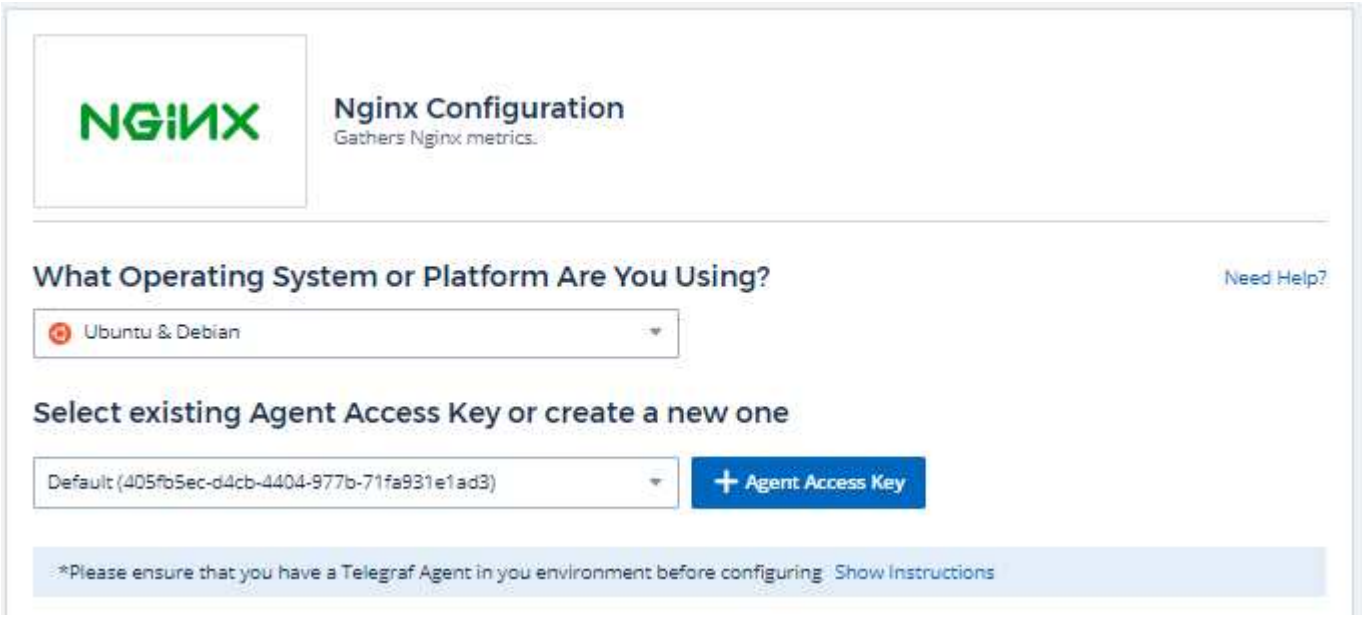
Data Infrastructure Insights utilizza questo data collector per raccogliere le metriche da Nginx.

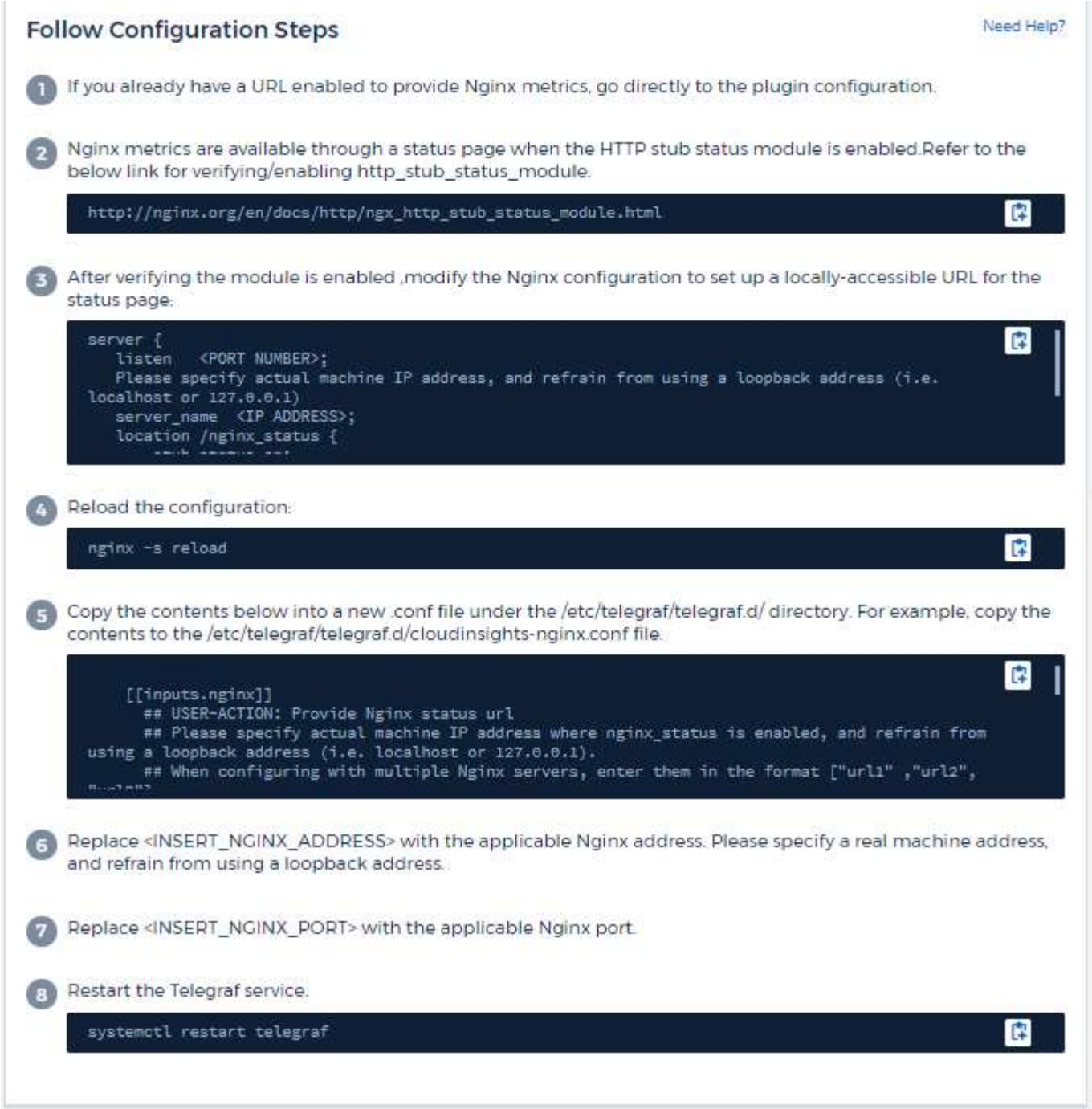
Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Nginx.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.





Setup (Configurazione)

L'insieme di metriche nginx richiede l'attivazione di Nginx"http_stub_status_module".

Ulteriori informazioni sono disponibili nella "Documentazione nginx".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Nginx	Server namespace	Nodo IP Node Name Port (porta nome nodo IP)	Accetta richieste di lettura gestite attive in attesa di scrittura

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

PostgreSQL Data Collector

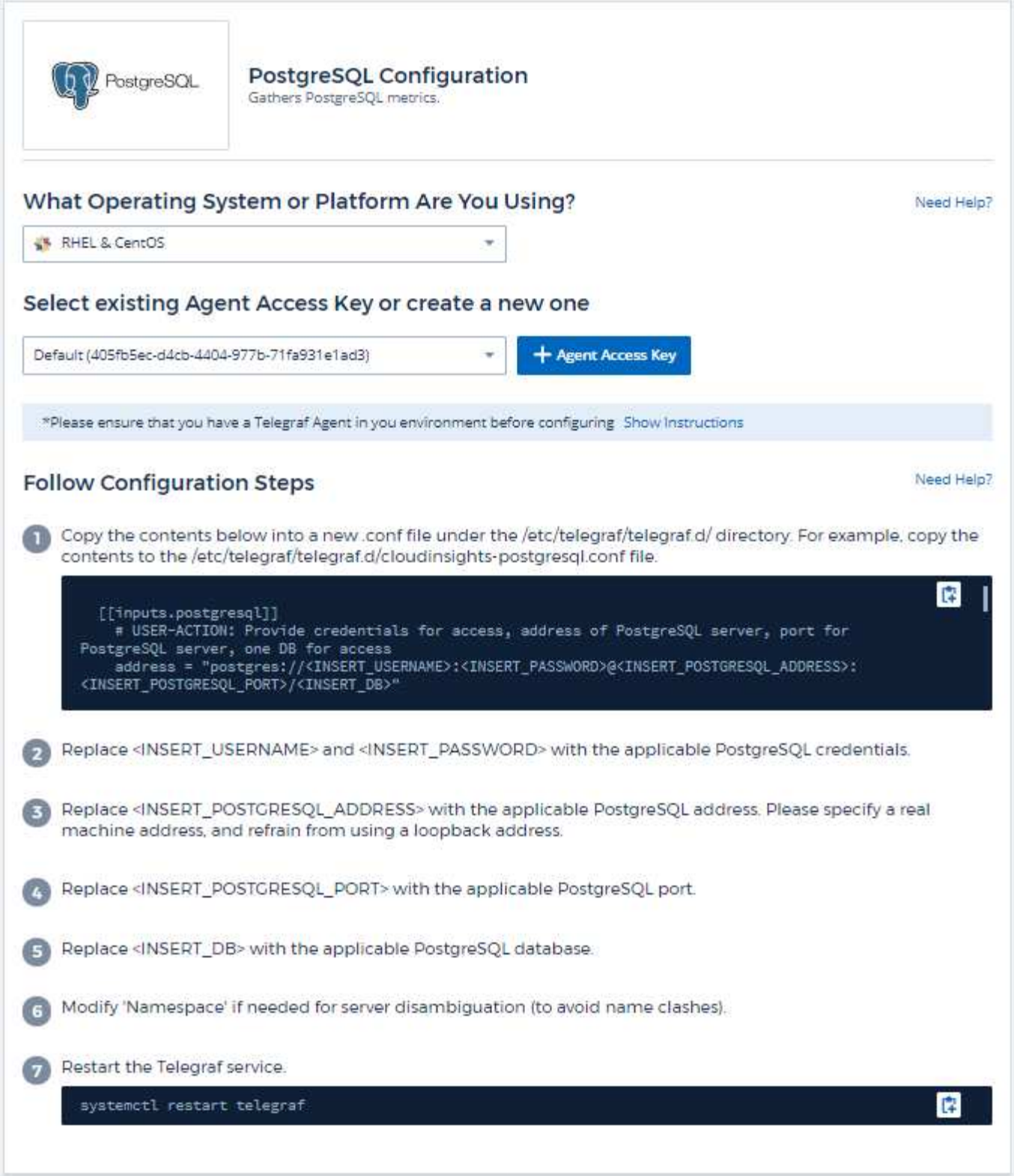
Data Infrastructure Insights utilizza questo data collector per raccogliere le metriche da PostgreSQL.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere PostgreSQL.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili nella "Documentazione PostgreSQL".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Server PostgreSQL	Server database namespace	Nome nodo IP nodo	Buffer allocati buffer backend buffer di sincronizzazione file backend buffer di controllo buffer di controllo punti di controllo puliti punti di controllo di sincronizzazione tempo di scrittura punti di controllo Richieste punti di controllo Timed Max scritto pulito
Database PostgreSQL	Server database namespace	Database OID Node Name Node IP	Blocchi di tempo di lettura blocchi di tempo di scrittura blocchi di accessi blocchi di lettura conflitti deadlock numero di client file di temperatura byte file di temperatura numero di righe cancellate righe recuperate righe inserite righe restituite transazioni aggiornate transazioni impegnate operazioni supportate dal rollback

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

Puppet Agent Data Collector

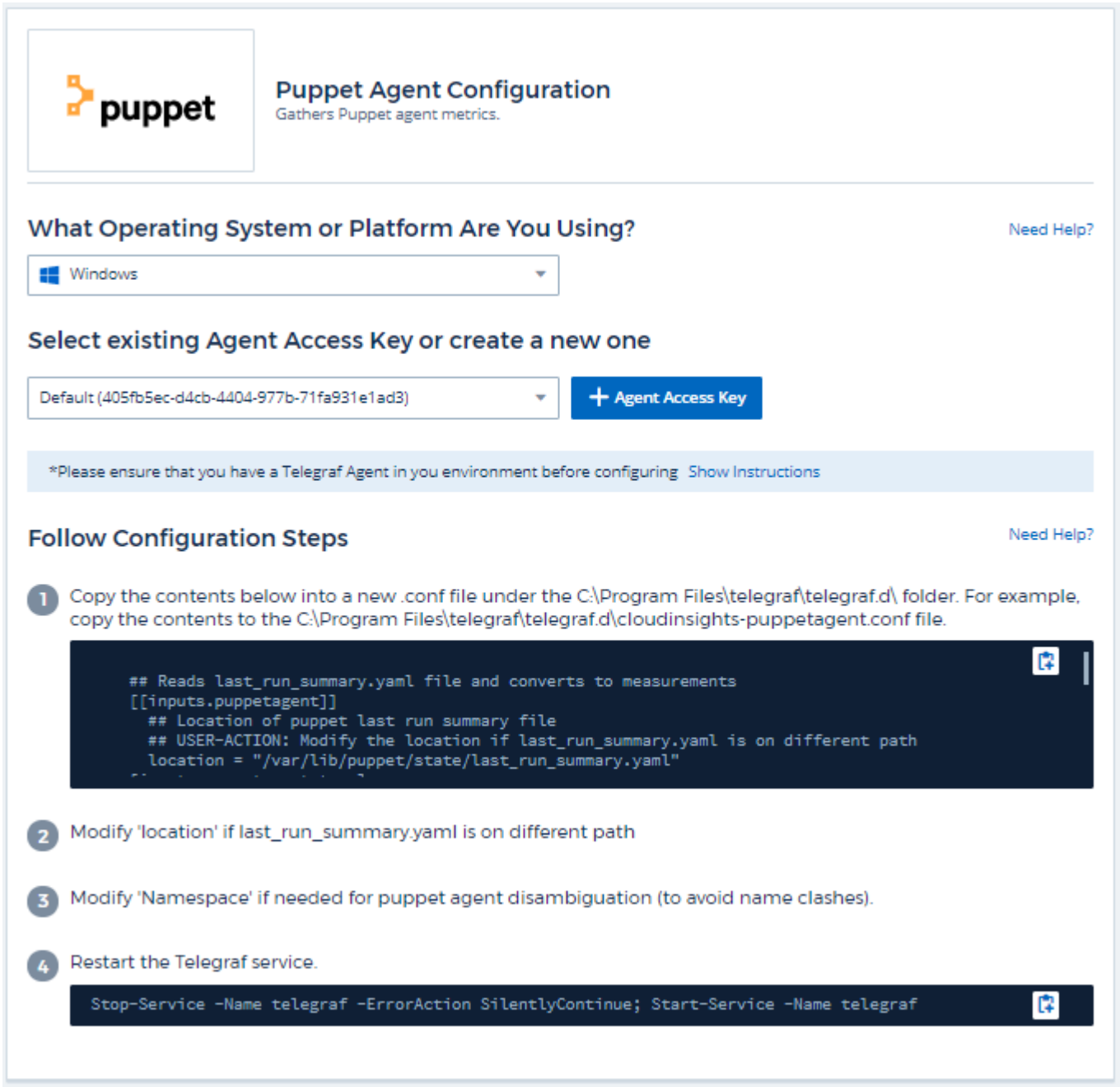
Data Infrastructure Insights utilizza questo data collector per raccogliere le metriche da Puppet Agent.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Puppet.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili in "Documentazione delle marionette"

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:

Agente di puppet	UUID nodo spazio dei nomi	Nome nodo posizione nodo versione IP stringa di configurazione versione Puppet	Modifiche eventi totali Eventi di errore Eventi di successo risorse totali risorse modificate risorse non riuscite riavvio risorse risorse Outofsync risorse riavviate risorse pianificate risorse ignorate tempo totale di ancoraggio tempo di recupero tempo di configurazione tempo di esecuzione tempo di esecuzione tempo di esecuzione file tempo di caricamento tempo di esecuzione tempo di esecuzione tempo tempo di esecuzione tempo tempo tempo di servizio tempo di gestione tempo totale Time User

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

Redis Data Collector

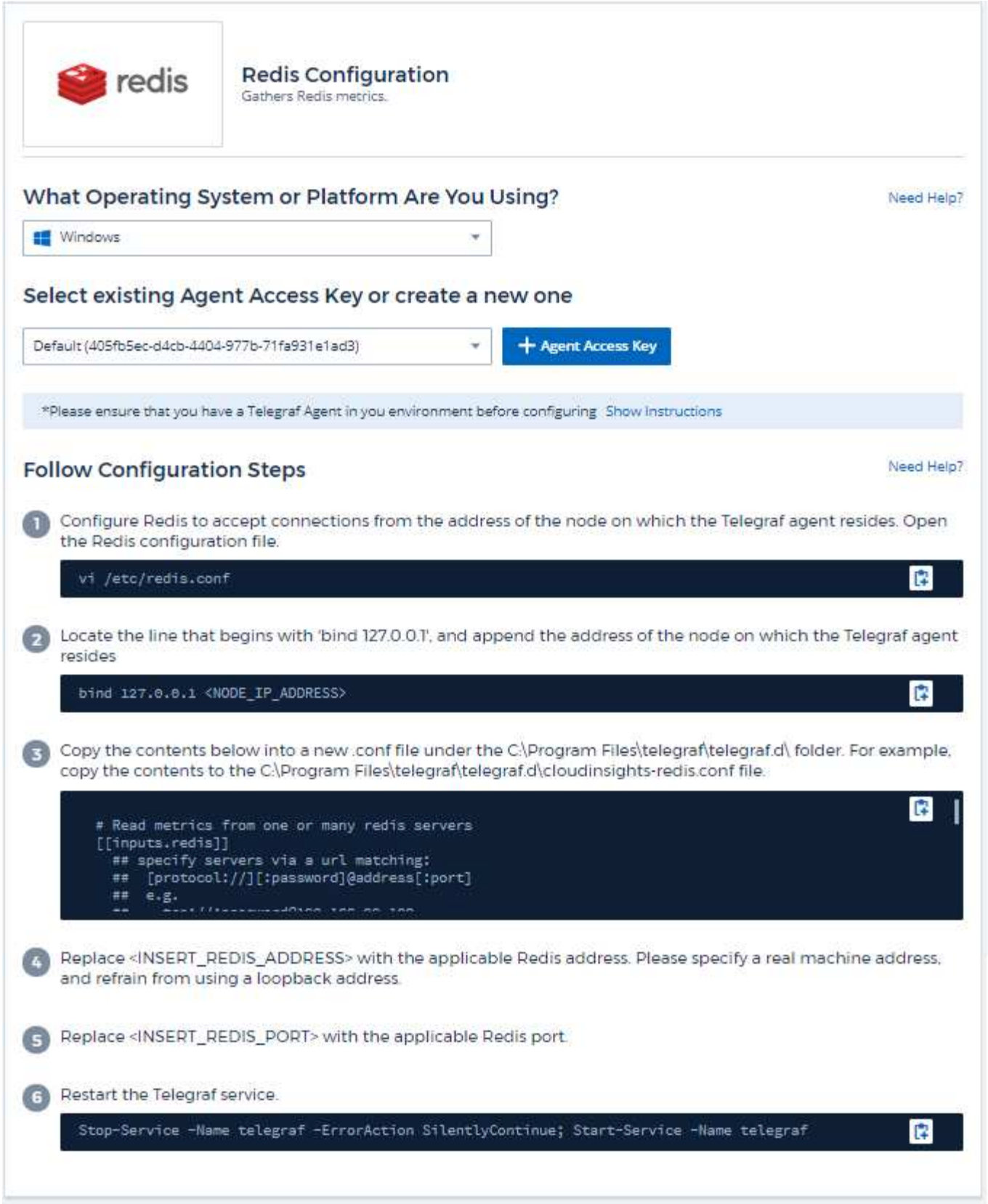
Data Infrastructure Insights utilizza questo data collector per raccogliere metriche da Redis. Redis è un archivio di strutture di dati in-memory open source utilizzato come database, cache e message broker, che supporta le seguenti strutture di dati: Stringhe, hash, elenchi, set e molto altro.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Redis.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per il ritiro o se si desidera installare un Agent per un sistema operativo o una piattaforma diversi, fare clic su *Mostra istruzioni* per espandere le "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili nella "Documentazione Redis".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Redis	Server namespace		

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "Supporto" pagina .

Informazioni sul copyright

Informazioni sul marchio commerciale