Riferimento al Data Collector - Servizi

Data Infrastructure Insights

NetApp
February 11, 2026

Sommario

Riferimento al Data Collector - Servizi

Raccolta dati nodo

Data Infrastructure Insights raccoglie le metriche dal nodo su cui installi un agente.

Installazione

1. Da **Observability > Collectors**, seleziona un sistema operativo/piattaforma. Si noti che l'installazione di qualsiasi raccoglitore di dati di integrazione (Kubernetes, Docker, Apache, ecc.) configurerà anche la raccolta di dati del nodo.
2. Seguire le istruzioni per configurare l'agente. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.

Oggetti e contatori

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

Oggetto:	Identificatori:	Attributi:	Punti dati:
File system del nodo	Tipo di percorso del dispositivo UUID del nodo	IP del nodo Nome del nodo Modalità del sistema operativo del nodo	Inode liberi Inode liberi Totale inode utilizzati Totale utilizzato Totale utilizzato
Nodo Disco	Disco UUID del nodo	IP del nodo Nome del nodo Sistema operativo del nodo	Tempo di I/O Totale IOPS in corso Byte letti (al sec) Tempo di lettura Letture totali (al sec) Tempo di I/O ponderato Byte scritti totali (al sec) Tempo di scrittura Scritture totali (al sec) Lunghezza coda disco corrente Tempo di scrittura Tempo di lettura Tempo di I/O
Nodo CPU	CPU UUID del nodo	IP del nodo Nome del nodo Sistema operativo del nodo	Utilizzo CPU di sistema Utilizzo CPU utente Utilizzo CPU inattiva Utilizzo CPU processore Utilizzo CPU interrupt Utilizzo CPU DPC

Oggetto:	Identificatori:	Attributi:	Punti dati:
Nodo	Nodo UUID	IP del nodo Nome del nodo Sistema operativo del nodo	Tempo di avvio del kernel Commutazioni di contesto del kernel (al secondo) Entropia del kernel disponibile Interrupt del kernel (al secondo) Processi del kernel forkati (al secondo) Memoria attiva Memoria disponibile Memoria totale disponibile Memoria bufferizzata Memoria memorizzata nella cache Limite di commit Memoria memorizzata come memoria Memoria sporca Memoria libera alta Memoria libera alta Memoria totale Memoria di dimensioni di pagina enormi Pagine enormi Memoria libera Pagine enormi Memoria totale bassa Memoria libera bassa Memoria totale Memoria mappata Tabelle delle pagine Memoria Memoria condivisa Memoria slab Swap di memoria nella cache Swap di memoria libera Swap di memoria totale Memoria totale utilizzata Memoria totale utilizzata Memoria Vmalloc Chunk Memory Vmalloc Memoria totale Vmalloc utilizzata Memoria cablata Writeback di memoria Writeback di memoria totale Memoria temporanea Errori della cache di memoria Richiesta di memoria Zero errori Errori di pagina di memoria Pagine di memoria Memoria non di paging Memoria di paging Memoria core della cache Cache di standby Memoria normale Cache di standby di riserva Errori di transizione di memoria Processi Processi bloccati Processi morti Processi

Oggetto:	Identificatori:	Attributi:	Punti dati:
Rete di nodi	UUID del nodo dell'interfaccia di rete	Nome nodo IP nodo Sistema operativo nodo	Byte ricevuti Byte inviati Pacchetti in uscita Pacchetti scartati Pacchetti in uscita Errori Pacchetti ricevuti Pacchetti scartati Pacchetti ricevuti Errori Pacchetti ricevuti Pacchetti inviati

Impostare

Le informazioni sulla configurazione e sulla risoluzione dei problemi sono disponibili su"Configurazione di un agente" pagina.

Raccoglitore dati ActiveMQ

Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da ActiveMQ.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli ActiveMQ.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.

[Configurazione ActiveMQ]

Impostare

Le informazioni possono essere trovate nel "Documentazione ActiveMQ"

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Coda ActiveMQ	Server porta coda spazio dei nomi	Nome nodo IP nodo UUID nodo	Conteggio consumatori Conteggio de-accodamento Conteggio accodamento Dimensione coda
Abbonato ActiveMQ	ID client ID connessione Porta Spazio dei nomi del server	È attivo Nome nodo di destinazione IP nodo UUID nodo Selettore sistema operativo nodo Sottoscrizione	Conteggio dei dequeue Conteggio dei dispatched Dimensione coda inviata Conteggio dei enqueue Dimensione coda in sospeso
Argomento ActiveMQ	Spazio dei nomi del server della porta dell'argomento	Nome nodo IP nodo UUID nodo Sistema operativo nodo	Conteggio consumatori Conteggio de-accodamento Conteggio accodamento Dimensione

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Apache Data Collector

Questo raccoglitore di dati consente la raccolta di dati dai server Apache sul tuo tenant.

Prerequisiti

- Devi avere il tuo server Apache HTTP configurato e funzionante correttamente
- Devi avere i permessi sudo o amministratore sul tuo host agente/VM
- In genere, il modulo Apache *mod_status* è configurato per esporre una pagina nella posizione '/server-status?auto' del server Apache. Per raccogliere tutti i campi disponibili, è necessario abilitare l'opzione *ExtendedStatus*. 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 > Collettori**, fare clic su **+Collettore dati**. Scegli Apache.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.

[Configurazione di Apache]

Impostare

Il plugin di Telegraf per il server HTTP di Apache si basa sull'abilitazione del modulo 'mod_status'. Se questa opzione è abilitata, il server HTTP di Apache esporrà un endpoint HTML che può essere visualizzato sul browser o recuperato per l'estrazione dello stato di tutta la configurazione del server HTTP di Apache.

Compatibilità:

La configurazione è stata sviluppata per la versione 2.4.38 del server HTTP di Apache.

Abilitazione di mod_status:

L'abilitazione e l'esposizione dei moduli 'mod_status' comporta due passaggi:

- Modulo di abilitazione
- Esposizione delle statistiche dal modulo

Modulo di abilitazione:

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

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

Visualizzazione delle statistiche dal modulo:

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

```
# 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"Documentazione di Apache"

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Apache	Server dello spazio dei nomi	IP del nodo Nome del nodo Porta Generazione della configurazione del server padre Generazione MPM del server padre Il tempo di attività del server si sta interrompendo	Lavoratori occupati Byte per richiesta Byte al secondo CPU CPU di sistema figli CPU utente figli Carico CPU di sistema CPU utente Connessioni asincrone Chiusura Connessioni asincrone Keep Alive Connessioni asincrone Scrittura Connessioni Durata totale per richiesta Lavoratori inattivi Carico medio (ultimo minuto) Carico medio (ultimi 15 minuti) Carico medio (ultimi 5 minuti) Processi Richieste al secondo Accessi totali Durata totale Kbyte totali Tabellone segnapunti Chiusura tabellone segnapunti Ricerche DNS Tabellone segnapunti Completamento tabellone segnapunti Pulizia inattiva tabellone segnapunti Keep Alive Registrazione tabellone segnapunti Apertura tabellone segnapunti Lettura tabellone segnapunti Invio tabellone segnapunti Avvio tabellone segnapunti In attesa

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Consul Data Collector

Data Infrastructure Insights utilizza questo strumento di raccolta dati per raccogliere metriche da Consul.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Console.

   Se non hai configurato un agente per la raccolta, ti verrà richiesto di"installare un agente" sul tuo inquilino.

   Se hai già configurato un agente, seleziona il sistema operativo o la piattaforma appropriati e fai clic su **Continua**.

2. Seguire le istruzioni nella schermata Configurazione del Consul per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.

Impostare

Le informazioni possono essere trovate nel"Documentazione del console" .

Oggetti e contatori per console

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Console	Nodo del servizio ID di controllo dello spazio dei nomi	IP del nodo Sistema operativo del nodo UUID del nodo Nome del nodo Nome del servizio Controlla nome ID del servizio Stato	Avviso di sorpasso critico

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Couchbase Data Collector

Data Infrastructure Insights utilizza questo strumento di raccolta dati per raccogliere metriche da Couchbase.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Couchbase.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.

4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.

[Configurazione Couchbase]

Impostare

Le informazioni possono essere trovate nel"Documentazione di Couchbase" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Nodo Couchbase	Nome host del nodo Couchbase del cluster dello spazio dei nomi	Nome nodo IP nodo	Memoria libera Memoria totale
Secchio Couchbase	Cluster di bucket dello spazio dei nomi	Nome nodo IP nodo	Dati utilizzati Recuperi dati Disco utilizzato Numero di elementi Memoria utilizzata Operazioni al secondo Quota utilizzata

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

CouchDB Data Collector

Data Infrastructure Insights utilizza questo strumento di raccolta dati per raccogliere metriche da CouchDB.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli CouchDB.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.

[Configurazione di CouchDB]

Impostare

Le informazioni possono essere trovate nel"Documentazione di CouchDB" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
CouchDB	Server dello spazio dei nomi	Nome nodo IP nodo	Hit della cache di autenticazione Miss della cache di autenticazione Letture del database Scritture del database Database aperti File del sistema operativo aperti Tempo massimo di richiesta Tempo minimo di richiesta Metodi di richiesta HTTPD Copia Metodi di richiesta HTTPD Elimina Metodi di richiesta HTTPD Ottieni Metodi di richiesta HTTPD Intestazione Metodi di richiesta HTTPD Post Metodi di richiesta HTTPD Inserisci Codici di stato 200 Codici di stato 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 possono essere trovate presso"Supporto" pagina.

Docker Data Collector

Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da Docker.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Docker.

Se non hai configurato un agente per la raccolta, ti verrà richiesto di"installare un agente" sul tuo inquilino.

Se hai già configurato un agente, seleziona il sistema operativo o la piattaforma appropriati e fai clic su **Continua**.

2. Seguire le istruzioni nella schermata Configurazione Docker per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.

[Configurazione Docker]

Impostare

Il plugin di input Telegraf per Docker raccoglie le metriche tramite un socket UNIX specificato o un endpoint TCP.

Compatibilità

La configurazione è stata sviluppata per Docker versione 1.12.6.

Impostazione

Accesso a Docker tramite un socket UNIX

Se l'agente Telegraf è in esecuzione su baremetal, aggiungere l'utente Unix Telegraf al gruppo Unix Docker eseguendo quanto segue:

```
 sudo usermod -aG docker telegraf
Se l'agente Telegraf è in esecuzione all'interno di un pod Kubernetes,
esporre il socket Docker Unix mappando il socket nel pod come volume e
quindi montando tale volume su /var/run/docker.sock.  Ad esempio, aggiungi
quanto segue al PodSpec:
```

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

Quindi, aggiungi quanto segue al contenitore:

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

Si noti che il programma di installazione Data Infrastructure Insights fornito per la piattaforma Kubernetes si

occupa automaticamente di questa mappatura.

Accedi 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	Motore Docker dello spazio dei nomi	Nome nodo IP nodo UUID nodo Sistema operativo nodo Cluster Kubernetes Versione Docker Unità	Contenitori di memoria Contenitori Contenitori in pausa Contenitori in esecuzione CPU arrestate Routine di avvio Immagini Eventi di ascolto Descrittori di file utilizzati Dati Dati disponibili Dati totali utilizzati Metadati Metadati disponibili Metadati totali utilizzati Dimensione blocco pool

Oggetto:	Identificatori:	Attributi:	Punti dati:
Contenitore Docker	Nome del contenitore dello spazio dei nomi Docker Engine	Hash del contenitore Kubernetes Porte del contenitore Kubernetes Conteggio riavvii del contenitore Kubernetes Percorso del messaggio di terminazione del contenitore Kubernetes Criterio del messaggio di terminazione del contenitore Kubernetes Periodo di grazia per la terminazione del pod Kubernetes Immagine del contenitore Stato del contenitore Versione del contenitore Nome del nodo Percorso del registro del contenitore Kubernetes Nome del contenitore Kubernetes Tipo di Docker Kubernetes Nome del pod Kubernetes Spazio dei nomi del pod Kubernetes UID del pod Kubernetes ID sandbox Kubernetes IP del nodo UUID del nodo Versione Docker Configurazione IO Kubernetes visualizzata Sorgente della configurazione IO Kubernetes SCC IO OpenShift Descrizione Kubernetes Nome visualizzato Kubernetes Tag OpenShift Kompose Service Pod Template Hash Controller Revisione Hash Generazione del modello del pod Licenza Schema Data di build Schema Licenza Nome schema URL schema URL VCS schema Fornitore schema Versione schema Schema Versione schema Manutentore Pod cliente Kubernetes StatefulSet Nome pod Tenant Webconsole Architettura URL origine autorevole Data di build Host build RH Componente RH	Memoria attiva Memoria anonima Memoria attiva Memoria file cache Limite gerarchico della memoria Memoria inattiva Memoria anonima Memoria inattiva Limite di memoria file Memoria file mappata Utilizzo massimo della memoria Errore di pagina della memoria Errore di pagina maggiore della memoria Memoria paginata in memoria paginata in memoria paginata in memoria Dimensione del set residente della memoria Dimensione del set residente della memoria Enorme Memoria totale attiva Memoria anonima Memoria file attiva Memoria cache totale Memoria anonima Memoria file inattiva Memoria file mappata Memoria totale Errore di pagina maggiore della memoria Totale Memoria paginata in memoria totale Paginata in memoria totale Paginata in memoria totale Dimensione del set residente della memoria Totale Dimensione del set residente della memoria Enorme Memoria totale non rimuovibile Utilizzo della memoria non rimuovibile Percentuale di utilizzo della memoria Codice di uscita OOM PID eliminato Avviato con sequenza di errori

Oggetto:	Identificatori:	Attributi:	Punti dati:
Docker Container Block IO	Namespace Contenitore Nome Dispositivo Motore Docker	Hash del contenitore Kubernetes Porte del contenitore Kubernetes Conteggio riavvii del contenitore Kubernetes Percorso del messaggio di terminazione del contenitore Kubernetes Criterio del messaggio di terminazione del contenitore Kubernetes Periodo di grazia per la terminazione del pod Kubernetes Immagine del contenitore Stato del contenitore Versione del contenitore Nome del nodo Percorso del registro del contenitore Kubernetes Nome del contenitore Kubernetes Tipo di Docker Kubernetes Nome del pod Kubernetes Spazio dei nomi del pod Kubernetes UID del pod Kubernetes ID sandbox Kubernetes IP del nodo UUID del nodo Versione Docker Configurazione Kubernetes visualizzata Sorgente della configurazione Kubernetes OpenShift SCC Descrizione di Kubernetes Nome visualizzato di Kubernetes Tag di OpenShift Schema Versione dello schema Hash del modello del pod Hash di revisione del controller Generazione del modello del pod Servizio Kompose Data di build dello schema Licenza dello schema Nome dello schema Fornitore dello schema Pod del cliente Nome del pod StatefulSet di Kubernetes Tenant Webconsole Data di build Fornitore della licenza Architettura URL sorgente autorevole Host di build RH Componente RH Ambito di distribuzione	Byte del servizio IO ricorsivi asincroni Byte del servizio IO ricorsivi in lettura Byte del servizio IO ricorsivi in sincronizzazione Byte del servizio IO ricorsivi totali Byte del servizio IO ricorsivi in scrittura Byte del servizio IO ricorsivi in asincroni serviti in lettura ricorsiva Byte del servizio IO ricorsivi in sincronizzazione serviti in lettura ricorsiva Byte del servizio IO ricorsivi totali serviti in scrittura ricorsiva

Oggetto:	Identificatori:	Attributi:	Punti dati:
Rete di contenitori Docker	Namespace Container Nome Rete Docker Engine	Immagine del contenitore Stato del contenitore Versione del contenitore Nome del nodo IP del nodo UUID del nodo Sistema operativo del nodo Cluster K8s Versione Docker ID del contenitore	RX eliminati Byte RX Errori RX Pacchetti RX TX eliminati Byte TX Errori TX Pacchetti TX

Oggetto:	Identificatori:	Attributi:	Punti dati:
CPU del contenitore Docker	Nome del contenitore dello spazio dei nomi CPU Motore Docker	Hash del contenitore Kubernetes Porte del contenitore Kubernetes Conteggio riavvii del contenitore Kubernetes Percorso del messaggio di terminazione del contenitore Kubernetes Criterio del messaggio di terminazione del contenitore Kubernetes Periodo di grazia per la terminazione del pod Kubernetes Configurazione Kubernetes visualizzata Origine della configurazione Kubernetes Immagine del contenitore OpenShift SCC Stato del contenitore Versione del contenitore Nome del nodo Percorso del registro del contenitore Kubernetes Nome del contenitore Kubernetes Tipo di Docker Kubernetes Nome del pod Kubernetes Spazio dei nomi del pod Kubernetes UID del pod Kubernetes ID sandbox Kubernetes IP del nodo UUID del nodo Sistema operativo del nodo Versione Docker del cluster Kubernetes Descrizione di Kubernetes Nome visualizzato di Kubernetes Tag OpenShift Versione dello schema Hash del modello del pod Hash di revisione del controller Generazione del modello del pod Servizio Kompose Data di build dello schema Licenza dello schema Nome dello schema Fornitore dello schema Pod del cliente Nome del pod StatefulSet Kubernetes Tenant Webconsole Data di build Fornitore della licenza Architettura URL sorgente autorevole Host di build	Periodi di limitazione Periodi di limitazione della limitazione Tempo di limitazione della limitazione Utilizzo in modalità kernel Utilizzo in modalità utente Percentuale di utilizzo Utilizzo del sistema Utilizzo totale

Risoluzione dei problemi

Problema:	Prova questo:
Dopo aver seguito le istruzioni nella pagina di configurazione, non vedo le mie metriche Docker in Data Infrastructure Insights .	Controllare i registri dell'agente Telegraf per vedere se segnala il seguente errore: E! Errore nel plugin [inputs.docker]: Autorizzazione negata durante il tentativo di connessione al socket del demone Docker. In tal caso, adottare le misure necessarie per consentire all'agente Telegraf di accedere al socket Unix Docker come specificato sopra.

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore dati Elasticsearch

Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da Elasticsearch.

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Elasticsearch.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.

[Configurazione Elasticsearch]

Impostare

Le informazioni possono essere trovate nel"Documentazione di Elasticsearch" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:
Cluster Elasticsearch	Cluster di spazi dei nomi	IP del nodo Nome del nodo Stato del cluster
Nodo Elasticsearch	Cluster dello spazio dei nomi ID nodo ES IP nodo ES Nodo ES	ID zona

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Flink Data Collector

Data Infrastructure Insights utilizza questo strumento di raccolta dati per raccogliere metriche da Flink.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Flink.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.

[Configurazione Flink]

Impostare

Una distribuzione completa di Flink prevede 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: è qui che vengono eseguiti gli operatori Flink. Il plugin Flink è basato sul plugin Jolokia di Telegraf. Poiché è un requisito per raccogliere informazioni da tutti i componenti Flink, JMX deve essere configurato ed esposto tramite Jolokia su tutti i componenti.

Compatibilità

La configurazione è stata sviluppata per la versione 1.7.0 di Flink.

Impostazione

Barattolo dell'agente Jolokia

Per tutti i singoli componenti è necessario scaricare una versione del file jar dell'agente Jolokia. La versione testata era"Agente Jolokia 1.6.0" .

Le istruzioni riportate di seguito presuppongono che il file jar scaricato (jolokia-jvm-1.6.0-agent.jar) sia posizionato nel percorso '/opt/flink/lib/'.

Gestore di lavori

Per configurare JobManager in modo che esponga l'API Jolokia, puoi impostare la seguente variabile di ambiente sui tuoi nodi, quindi 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"
Puoi scegliere una porta diversa per Jolokia (8778).  Se hai un IP interno
su cui bloccare Jolokia, puoi sostituire "catch all" 0.0.0.0 con il tuo
IP.  Si noti che questo IP deve essere accessibile dal plugin Telegraf.
```

Task Manager

Per configurare TaskManager in modo che esponga l'API Jolokia, puoi impostare la seguente variabile di ambiente sui tuoi nodi, quindi 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"
Puoi scegliere una porta diversa per Jolokia (8778).  Se hai un IP interno
su cui bloccare Jolokia, puoi sostituire "catch all" 0.0.0.0 con il tuo
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:
Gestore attività Flink	Server dello spazio dei nomi del cluster	Nome nodo ID Task Manager IP nodo	Segmenti di memoria disponibili in rete Segmenti di memoria totali in rete Garbage Collection PS MarkSweep Count Tempo di Garbage Collection PS MarkSweep Count Scavenge PS Garbage Collection PS Scavenge Count Tempo di Scavenge PS Garbage Collection Heap Memory Memoria Heap impegnata Heap di inizializzazione Heap Memory massima utilizzata Thread Count Thread Daemon Count Thread di picco Thread Count Totale avviato

Oggetto:	Identificatori:	Attributi:	Punti dati:
Lavoro Flink	ID processo del server dello spazio dei nomi del cluster	Nome nodo Nome lavoro IP nodo Ultimo checkpoint Percorso esterno Ora di riavvio	Tempo di inattività Riavvii completi Allineamento ultimo checkpoint Durata ultimo checkpoint in buffer Dimensione ultimo checkpoint Numero di checkpoint completati Numero di checkpoint non riusciti Numero di checkpoint in corso Numero di checkpoint Tempo di attività
Gestore di lavori Flink	Server dello spazio dei nomi del cluster	Nome nodo IP nodo	Conteggio PS MarkSweep di Garbage Collection Tempo PS MarkSweep di Garbage Collection Conteggio PS Scavenge di Garbage Collection Tempo PS Scavenge di Garbage Collection Memoria heap Memoria heap impegnata Memoria heap di inizializzazione Memoria heap massima utilizzata Numero di task manager registrati Numero di processi in esecuzione Slot attività Slot attività disponibili Conteggio thread totale Conteggio thread daemon Conteggio thread di picco Conteggio thread totale avviato

Oggetto:	Identificatori:	Attributi:	Punti dati:
Compito Flink	ID lavoro spazio dei nomi cluster ID attività	Nome nodo server Nome lavoro Indice sottoattività ID tentativo attività Numero tentativo attività Nome attività ID gestore attività IP nodo Input corrente Filigrana	Utilizzo del pool di buffer Lunghezza della coda di buffer Utilizzo del pool di buffer Lunghezza della coda di buffer Numero buffer in locale Numero buffer in locale al secondo Conteggio Numero buffer in locale al secondo Numero buffer in remoto Numero buffer in remoto al secondo Conteggio Numero buffer in remoto al secondo Numero buffer in uscita Numero buffer in uscita al secondo Conteggio Numero buffer in uscita al secondo Numero byte in locale Numero byte in locale al secondo Conteggio Numero byte in locale al secondo Numero byte in remoto Numero byte in remoto al secondo Conteggio Numero byte in remoto al secondo Numero byte in uscita Numero byte in uscita al secondo Conteggio Numero byte in uscita al secondo Numero record in ingresso Numero record in ingresso al secondo Numero record in ingresso al secondo Numero record in uscita Numero record in uscita al secondo Numero record in uscita al secondo

Oggetto:	Identificatori:	Attributi:	Punti dati:
Operatore di attività Flink	ID lavoro spazio dei nomi cluster ID operatore ID attività	Nome nodo server Nome lavoro Nome operatore Indice sottoattività ID tentativo attività Numero tentativo attività Nome attività ID gestore attività IP nodo	Filigrana di input corrente Filigrana di output corrente Numero record in ingresso Numero record in ingresso al secondo Conteggio Numero record in ingresso al secondo Numero record in uscita Numero record in uscita al secondo Conteggio Numero record in uscita al secondo Numero record in ritardo eliminati Partizioni assegnate Byte consumati Tasso Latenza commit Latenza commit media Tasso massimo commit Commit non riusciti Commit riusciti Tasso di chiusura connessione Conteggio connessioni Tasso di creazione connessione Conteggio Latenza fetch media Latenza fetch massima Tasso fetch Dimensione fetch Dimensione fetch media Tempo massimo di limitazione fetch Tempo medio di limitazione fetch Frequenza heartbeat massima Frequenza byte in ingresso Rapporto IO Tempo IO medio (ns) Rapporto di attesa IO Tempo di attesa IO medio (ns) Frequenza di unione Tempo di unione Ultimo heartbeat medio fa Frequenza IO di rete Tasso byte in uscita Record consumati Tasso Ritardo record Record massimi per richiesta Tasso medio di richiesta Dimensione richiesta Dimensione media richiesta Frequenza di risposta massima Seleziona frequenza Frequenza di sincronizzazione Tempo di sincronizzazione Tempo medio di risposta heartbeat Tempo di

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore dati Hadoop

Data Infrastructure Insights utilizza questo strumento di raccolta dati per raccogliere metriche da Hadoop.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Hadoop.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.

[Configurazione di Hadoop] [Configurazione di Hadoop]

Impostare

Una distribuzione completa di Hadoop prevede i seguenti componenti:

- NameNode: il sistema primario del file system distribuito Hadoop (HDFS). Coordina una serie di DataNode.
- NameNode secondario: un failover a caldo per il NameNode principale. In Hadoop la promozione a NameNode non avviene automaticamente. Il NameNode secondario raccoglie informazioni dal NameNode per essere pronto a essere promosso quando necessario.
- DataNode: Proprietario effettivo dei dati.
- ResourceManager: il sistema di elaborazione primario (Yarn). Coordina una serie di NodeManager.
- NodeManager: la risorsa per il calcolo. Posizione effettiva per l'esecuzione delle applicazioni.
- JobHistoryServer: responsabile della gestione di tutte le richieste relative alla cronologia dei lavori.

Il plugin Hadoop è basato sul plugin Jolokia di Telegraf. Poiché è un 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 per Hadoop versione 2.9.2.

Impostazione

Barattolo dell'agente Jolokia

Per tutti i singoli componenti è necessario scaricare una versione del file jar dell'agente Jolokia. La versione testata era"Agente Jolokia 1.6.0" .

Le istruzioni riportate di seguito presuppongono che il file jar scaricato (jolokia-jvm-1.6.0-agent.jar) sia posizionato nel percorso '/opt/hadoop/lib/'.

NomeNodo

Per configurare NameNode in modo che esponga l'API Jolokia, puoi impostare 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.
```

Nome secondarioNodo

Per configurare il Secondary NameNode in modo che esponga l'API Jolokia, puoi impostare 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.
```

Nodo dati

Per configurare i DataNode in modo che espongano l'API Jolokia, puoi impostare 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 che esponga l'API Jolokia, puoi impostare 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.
```

Gestore dei nodi

Per configurare i NodeManager in modo che espongano l'API Jolokia, puoi impostare 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.
```

JobHistoryServer

Per configurare JobHistoryServer in modo che esponga l'API Jolokia, è possibile impostare 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:
Nome secondario HadoopNode	Server dello spazio dei nomi del cluster	Nome nodo IP nodo Informazioni di compilazione Versione
Hadoop NodeManager	Server dello spazio dei nomi del cluster	Nome nodo IP nodo
Hadoop Resource Manager	Server dello spazio dei nomi del cluster	Nome nodo IP nodo

Oggetto:	Identificatori:	Attributi:
Hadoop DataNode	Server dello spazio dei nomi del cluster	Nome nodo IP nodo ID cluster Versione
Nome nodo Hadoop	Server dello spazio dei nomi del cluster	Nome nodo IP nodo ID transazione Ultima scrittura Ora dall'ultimo caricamento Modifiche Stato HA Stato del file system ID del pool di blocchi ID del cluster Informazioni sulla compilazione Conteggio distinta delle versioni Versione
Hadoop JobHistoryServer	Server dello spazio dei nomi del cluster	Nome nodo IP nodo

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore dati HAProxy

Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da HAProxy.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli HAProxy.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.

[Configurazione HAProxy]

Impostare

Il plugin di Telegraf per HAProxy si basa sull'abilitazione di HAProxy Stats. Questa è una configurazione integrata in HAProxy, ma non è abilitata di default. Se abilitato, HAProxy esporrà un endpoint HTML che può essere visualizzato sul browser o recuperato per l'estrazione dello stato di tutte le configurazioni HAProxy.

Compatibilità:

La configurazione è stata sviluppata per HAProxy versione 1.9.4.

Impostazione:

Per abilitare le statistiche, modifica il file di configurazione haproxy e aggiungi le seguenti righe dopo la sezione 'defaults', utilizzando il tuo nome utente/password e/o l'URL haproxy:

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

Di seguito è riportato un esempio semplificato di file di configurazione con statistiche abilitate:

```
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, consultare il"Documentazione HAProxy" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Frontend HAProxy	Proxy indirizzo spazio dei nomi	IP nodo Nome nodo ID proxy Modalità ID processo Sessioni Limite velocità ID server Limite sessioni Stato	Byte in entrata Byte in uscita Cache Hits Cache Lookups Compressione Byte bypassati Compressione Byte in entrata Compressione Byte in uscita Compressione Risposte Velocità di connessione Velocità di connessione Connessioni massime Totale richieste rifiutate dalla regola di connessione Richieste rifiutate per problemi di sicurezza Risposte rifiutate per problemi di sicurezza Richieste rifiutate dalla regola di sessione Richieste Errori Risposte Risposte 1xx Risposte 2xx Risposte 3xx Risposte 4xx Risposte 5xx Altre richieste Sessioni intercettate Velocità sessioni Velocità richieste massime Velocità richieste Velocità richieste massime Totale sessioni Sessioni Sessioni massime Totale richieste Riscritture

Oggetto:	Identificatori:	Attributi:	Punti dati:
Server HAProxy	Server proxy indirizzo spazio dei nomi	IP del nodo Nome del nodo Controlla ora di fine Controlla configurazione caduta Controlla valore integrità Controlla configurazione salita Controlla stato ID proxy Ora ultima modifica Ora ultima sessione Modalità ID processo ID server Stato Peso	Server attivi Server di backup Byte in entrata Byte in uscita Controlli inattivi Controlli non riusciti Client interrompe Connessioni Tempo medio di connessione Tempo di inattività Totale risposte negate Errori di connessione Errori di risposta Risposte 1xx Risposte 2xx Risposte 3xx Risposte 4xx Risposte 5xx Altro server selezionato Coda totale Coda corrente Tempo medio massimo della coda Sessioni al secondo Sessioni al secondo Tempo massimo di riutilizzo della connessione Tempo di risposta Media sessioni Sessioni Massimo trasferimento server Interruzioni sessioni Totale sessioni Tempo medio totale Richieste Ridistribuzioni Richieste Nuovi tentativi Richieste Riscritture

Oggetto:	Identificatori:	Attributi:	Punti dati:
Backend HAProxy	Proxy indirizzo spazio dei nomi	IP nodo Nome nodo ID proxy Ora ultima modifica Ora ultima sessione Modalità ID processo ID server Limite sessioni Stato Peso	Server attivi Server di backup Byte in entrata Byte in uscita Cache Hit Cache Lookup Check Down Client Abort Compressione Byte bypassati Compressione Byte in entrata Compressione Byte in uscita Compressione Risposte Connessioni Tempo medio di connessione Tempo di inattività Richieste totali negate per problemi di sicurezza Risposte negate per problemi di sicurezza Errori di connessione Errori di risposta Risposte 1xx Risposte 2xx Risposte 3xx Risposte 4xx Risposte 5xx Altro server selezionato Coda totale Coda corrente Coda massima Tempo medio Sessioni al secondo Sessioni al secondo Richieste massime Riutilizzo della connessione Tempo di risposta Media sessioni Sessioni Massima server Trasferimento Abort Sessioni Sessioni totali Tempo totale Richieste medie Ridistribuzioni Richieste Nuovi tentativi Richieste Riscritture

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore dati JVM

Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da JVM.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli JVM.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.

[Configurazione JVM]

Impostare

Le informazioni possono essere trovate in"Documentazione JVM" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
JVM	JVM dello spazio dei nomi	Architettura del sistema operativo Nome del sistema operativo Versione del sistema operativo Specifiche di runtime Fornitore delle specifiche di runtime Versione delle specifiche di runtime Tempo di attività Nome della VM di runtime Fornitore della VM di runtime Versione della VM di runtime Nome del nodo IP del nodo	Classe caricata Classe caricata Totale Classe scaricata Heap di memoria impegnato Heap di memoria inizializzato Heap di memoria utilizzato Heap di memoria massimo utilizzato Memoria non heap impegnata Memoria non heap inizializzato Memoria non heap massima Memoria non heap utilizzata Oggetti di memoria in attesa di finalizzazione Processori del sistema operativo disponibili Dimensione della memoria virtuale impegnata del sistema operativo Dimensione della memoria fisica libera del sistema operativo Dimensione dello spazio di swap libero del sistema operativo Conteggio massimo dei descrittori di file del sistema operativo Conteggio dei descrittori di file aperti del sistema operativo Carico CPU del processore del sistema operativo Tempo CPU del processore del sistema operativo Carico CPU del sistema del sistema operativo Carico medio del sistema operativo Dimensione totale della memoria fisica del sistema operativo Dimensione totale dello spazio di swap del sistema operativo Conteggio dei daemon dei thread Conteggio dei picchi dei thread Conteggio dei thread Conteggio totale dei thread avviati Conteggio della raccolta copie del Garbage Collector Tempo di raccolta copie del Garbage Collector Conteggio della raccolta Mark-sweep del Garbage

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore di dati Kafka

Data Infrastructure Insights utilizza questo strumento di raccolta dati per raccogliere metriche da Kafka.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Kafka.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.

[Configurazione di Kafka]

Impostare

Il plugin Kafka è basato sul plugin Jolokia di Telegraf. Poiché è un 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 per la versione 0.11.0.2 di Kafka.

Impostazione

Tutte le istruzioni riportate di seguito presuppongono che il percorso di installazione di Kafka sia '/opt/kafka'. Puoi adattare le istruzioni riportate di seguito in base alla tua posizione di installazione.

Barattolo dell'agente Jolokia

Una versione del file jar dell'agente Jolokia deve essere"scaricato" . La versione testata era Jolokia Agent 1.6.0.

Le istruzioni riportate di seguito presuppongono che il file jar scaricato (jolokia-jvm-1.6.0-agent.jar) si trovi nel percorso '/opt/kafka/libs/'.

Kafka Brokers

Per configurare Kafka Brokers in modo che esponga l'API Jolokia, puoi aggiungere quanto segue in

<KAFKA_HOME>/bin/kafka-server-start.sh, subito 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 nell'esempio precedente si utilizza 'hostname -I' per impostare la variabile di ambiente 'RMI_HOSTNAME'. Nelle macchine con più IP, sarà necessario apportare modifiche per raccogliere l'IP di interesse per le connessioni RMI.

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

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Kibana Data Collector

Data Infrastructure Insights utilizza questo strumento di raccolta dati per raccogliere metriche da Kibana.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Kibana.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera

raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.

4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.

[Configurazione Kibana]

Impostare

Le informazioni possono essere trovate nel"Documentazione Kibana" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Kibana	Indirizzo dello spazio dei nomi	IP del nodo Nome del nodo Versione Stato	Heap di connessioni simultanee Heap massimo utilizzato Richieste al secondo Tempo di risposta Tempo di risposta medio Tempo di attività massimo

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

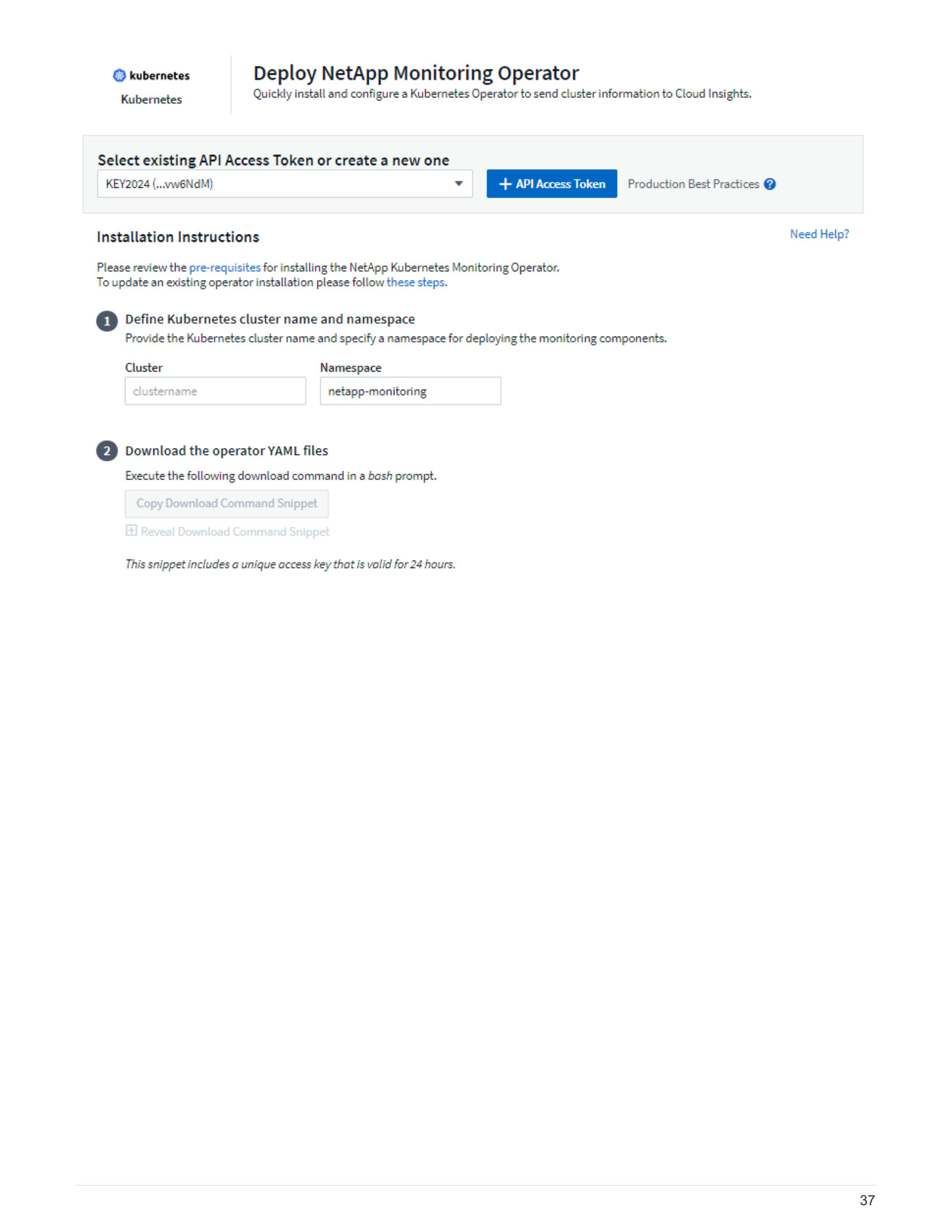
Installazione e configurazione dell'operatore di monitoraggio Kubernetes

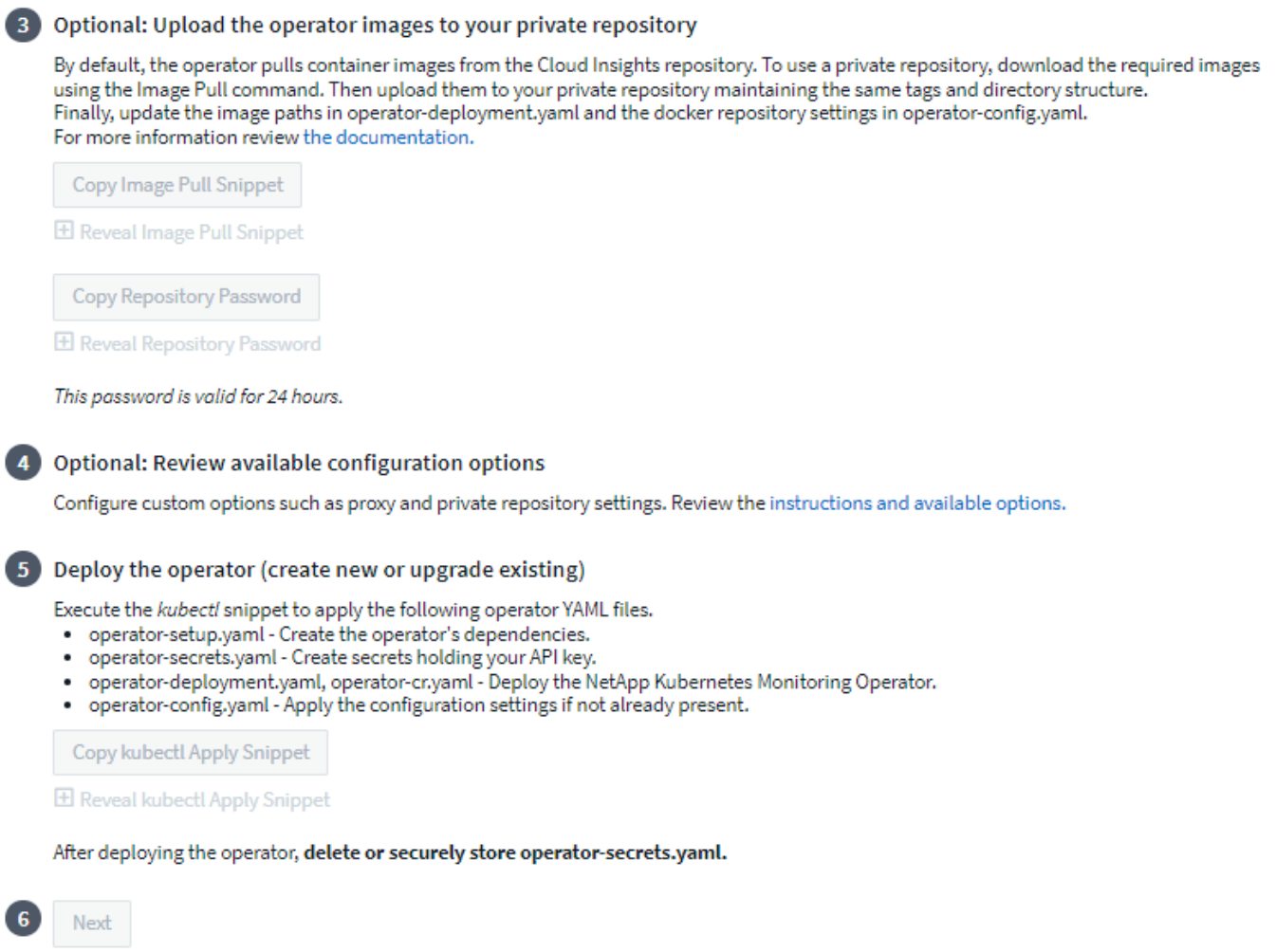
Data Infrastructure Insights offre l'**operatore di monitoraggio Kubernetes** per la raccolta Kubernetes. Passare a **Kubernetes > Collectors > +Kubernetes Collector** per distribuire un nuovo operatore.

Prima di installare Kubernetes Monitoring Operator

Vedi il"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 seiaggiornamento da un precedente operatore Kubernetes, utilizzare lo stesso nome del cluster e lo stesso spazio dei nomi.
2. Una volta inseriti questi dati, è possibile copiare il frammento del comando Download negli appunti.
3. Incolla lo snippet in una finestra *bash* ed eseguilo. Verranno scaricati i file di installazione dell'operatore. Si noti che lo snippet ha una chiave univoca ed è valido per 24 ore.
4. Se hai un repository personalizzato o privato, copia il frammento di codice Image Pull facoltativo, incollalo in una shell *bash* ed eseguilo. Una volta estratte le immagini, copiale nel tuo repository privato. Assicuratevi di mantenere gli stessi tag e la stessa struttura delle cartelle. Aggiornare i percorsi in *operator-deployment.yaml* e le impostazioni del repository Docker in *operator-config.yaml*.
5. Se lo si desidera, rivedere le opzioni di configurazione disponibili, come le impostazioni del proxy o del repository privato. Puoi leggere di più su"opzioni di configurazione" .
6. Quando sei pronto, distribuisci l'operatore copiando lo snippet Apply di kubectl, scaricandolo ed eseguendolo.
7. L'installazione procede automaticamente. Una volta completato, fare clic sul pulsante *Avanti*.
8. Al termine dell'installazione, fare clic sul pulsante *Avanti*. Assicurati di eliminare o archiviare in modo sicuro anche il file *operator-secrets.yaml*.

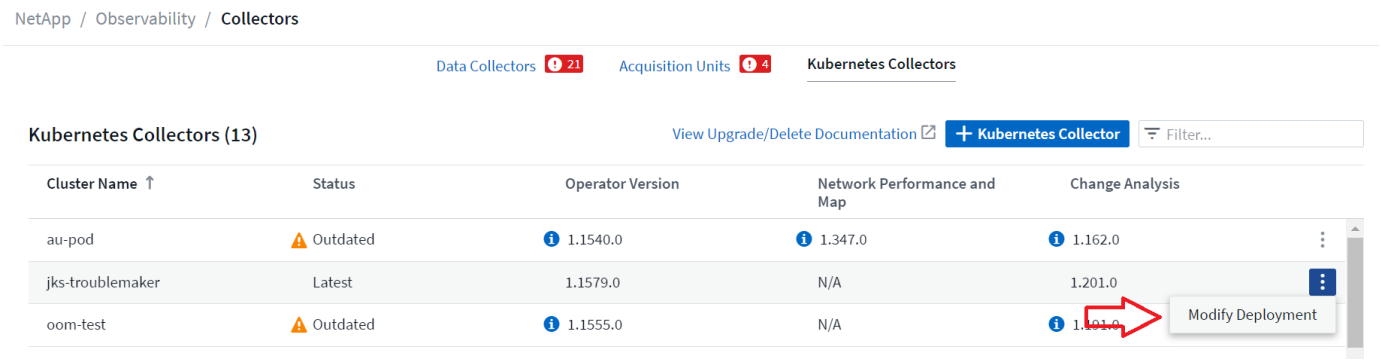
Se hai un repository personalizzato, leggi a riguardoutilizzando un repository Docker personalizzato/privato .

Componenti di monitoraggio di Kubernetes

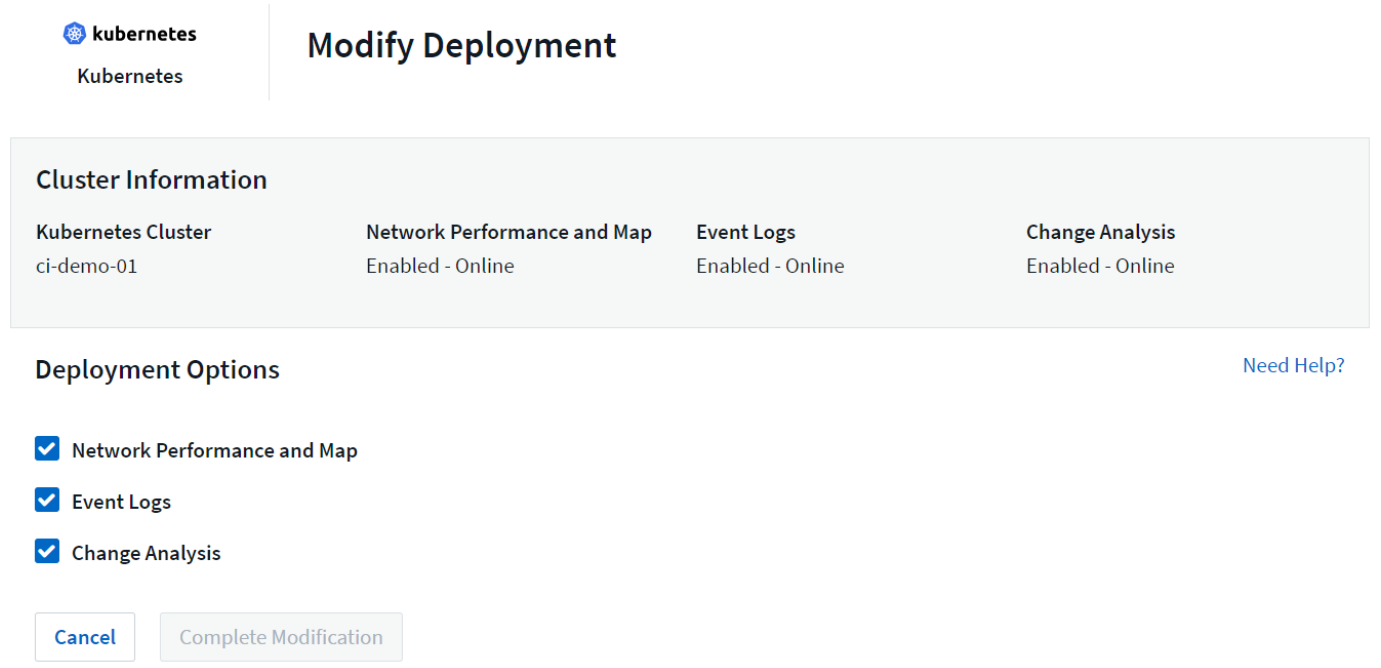
Data Infrastructure Insights Kubernetes Monitoring è composto da quattro componenti di monitoraggio:

- Metriche del cluster
- Prestazioni di rete e mappa (facoltativo)
- Registri eventi (facoltativo)
- Analisi del cambiamento (facoltativo)

I componenti facoltativi sopra indicati sono abilitati per impostazione predefinita per ciascun collector Kubernetes; se decidi che non hai bisogno di un componente per un collector specifico, puoi disabilitarlo andando su **Kubernetes > Collectors** e selezionando *Modifica distribuzione* dal menu "tre punti" del collector sulla destra dello schermo.



La schermata mostra lo stato attuale di ciascun componente e consente di disabilitare o abilitare i componenti per quel raccoglitore, a seconda delle necessità.



Aggiornamento all'ultima versione di Kubernetes Monitoring Operator

Aggiornamenti dei pulsanti DII

È possibile aggiornare Kubernetes Monitoring Operator tramite la pagina DII Kubernetes Collectors. Fare clic sul menu accanto al cluster che si desidera aggiornare e selezionare *Aggiorna*. L'operatore verificherà le firme delle immagini, eseguirà uno snapshot dell'installazione corrente ed eseguirà l'aggiornamento. Entro pochi minuti dovresti vedere l'avanzamento dello Stato dell'operatore da Aggiornamento in corso a Ultimo. Se si verifica un errore, è possibile selezionare lo stato Errore per maggiori dettagli e fare riferimento alla tabella di risoluzione dei problemi degli aggiornamenti tramite pulsante riportata di seguito.

Aggiornamenti rapidi con repository privati

Se il tuo operatore è configurato per utilizzare un repository privato, assicurati che tutte le immagini necessarie per eseguire l'operatore e le relative firme siano disponibili nel tuo repository. Se durante il processo di aggiornamento si verifica un errore per immagini mancanti, è sufficiente aggiungerle al repository e riprovare l'aggiornamento. Per caricare le firme delle immagini nel tuo repository, utilizza lo strumento di co-firma come segue, assicurandoti di caricare le firme per tutte le immagini specificate in 3 Facoltativo: carica le immagini dell'operatore nel tuo repository privato > Frammento di estrazione dell'immagine

```
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 precedentemente in esecuzione

Se hai effettuato l'aggiornamento utilizzando la funzionalità di aggiornamento tramite pulsante e riscontri difficoltà con la versione corrente dell'operatore entro sette giorni dall'aggiornamento, puoi effettuare il downgrade alla versione in esecuzione in precedenza utilizzando lo snapshot creato durante il processo di aggiornamento. Fare clic sul menu accanto al cluster di cui si desidera eseguire il rollback e selezionare *Roll back*.

Aggiornamenti manuali

Determinare se esiste un *AgentConfiguration* con l'operatore esistente (se il namespace non è il *netapp-monitoring* predefinito, sostituire il namespace appropriato):

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
Se esiste un _AgentConfiguration_:
```

- Installarel'ultimo Operatore rispetto all'Operatore esistente.
  - Assicurati di essereestrazione delle ultime immagini del contenitore se si utilizza un repository personalizzato.

Se *AgentConfiguration* non esiste:

- Prendi nota del nome del tuo cluster riconosciuto da Data Infrastructure Insights (se il tuo namespace non è quello predefinito netapp-monitoring, sostituiscilo con il namespace appropriato):

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Crea un backup dell'operatore esistente (se il tuo namespace non è il
netapp-monitoring predefinito, sostituiscilo con il namespace
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'ultimo
Operatore.
```

- Utilizzare lo stesso nome del cluster.
- Dopo aver scaricato gli ultimi file YAML dell'Operator, trasferisci tutte le personalizzazioni trovate in *agent_backup.yaml* nel *operator-config.yaml* scaricato prima della distribuzione.
- Assicurati di essereestrazione delle ultime immagini del contenitore se si utilizza un repository personalizzato.

Arresto e avvio dell'operatore di monitoraggio Kubernetes

Per arrestare Kubernetes Monitoring Operator:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
Per avviare Kubernetes Monitoring Operator:
```

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

Disinstallazione

Per rimuovere l'operatore di monitoraggio Kubernetes

Si noti che lo spazio dei nomi predefinito per l'operatore di monitoraggio Kubernetes è "netapp-monitoring". Se hai impostato un tuo namespace, sostituiscilo 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 namespace dedicato, eliminare il namespace:

```
 kubectl delete ns <NAMESPACE>
Nota: se il primo comando restituisce "Nessuna risorsa trovata",
utilizzare le seguenti istruzioni 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 di tipo "oggetto non trovato". Questi messaggi possono essere tranquillamente ignorati.

```
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 di contesto di sicurezza:

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

Informazioni su Kube-state-metrics

NetApp Kubernetes Monitoring Operator installa le proprie metriche kube-state 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 del proxy, sull'utilizzo di un repository Docker personalizzato o privato o sull'utilizzo di OpenShift.

Opzioni di configurazione

Le impostazioni modificate più comunemente possono essere configurate nella risorsa personalizzata *AgentConfiguration*. È possibile modificare questa risorsa prima di distribuire l'operatore modificando il file *operator-config.yaml*. Questo file include esempi di impostazioni commentati. Vedi l'elenco di"impostazioni disponibili" per la versione più recente dell'operatore.

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

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

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Se viene visualizzato il messaggio "Errore dal server (NotFound)", è
necessario aggiornare l'operatore prima di poter utilizzare
AgentConfiguration.
```

Configurazione del supporto proxy

Esistono due posti in cui è possibile utilizzare un proxy sul tenant per installare Kubernetes Monitoring Operator. Possono essere gli stessi sistemi proxy o sistemi proxy separati:

- Proxy necessario durante l'esecuzione dello snippet di codice di installazione (utilizzando "curl") per connettere il sistema in cui viene eseguito lo snippet al tuo ambiente Data Infrastructure Insights
- Proxy necessario al cluster Kubernetes di destinazione per comunicare con l'ambiente Data Infrastructure Insights

Se si utilizza un proxy per uno o entrambi questi elementi, per installare Kubernetes Operating Monitor è necessario innanzitutto assicurarsi che il proxy sia configurato per consentire una buona comunicazione con l'ambiente Data Infrastructure Insights . Se disponi di un proxy e puoi accedere a Data Infrastructure Insights dal server/VM da cui desideri installare l'operatore, è probabile che il tuo proxy sia configurato correttamente.

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

Per impostare le variabili, esegui i seguenti passaggi sul tuo sistema **prima** di installare Kubernetes Monitoring Operator:

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

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

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

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

Configura la sezione proxy di *AgentConfiguration* in *operator-config.yaml* prima di distribuire Kubernetes Monitoring Operator.

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

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

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

Utilizzo di un repository Docker personalizzato o privato

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

Eseguire "Image Pull Snippet" dal riquadro di installazione di NetApp Monitoring Operator. Questo comando effettuerà l'accesso al repository Data Infrastructure Insights , estrarrà tutte le dipendenze delle immagini per l'operatore e uscirà dal repository Data Infrastructure Insights . Quando richiesto, immettere la password temporanea del repository fornita. Questo comando scarica tutte le immagini utilizzate dall'operatore, comprese quelle per le funzionalità opzionali. Di seguito sono riportate le funzioni per cui vengono utilizzate queste immagini.

Funzionalità dell'operatore principale e monitoraggio di Kubernetes

- monitoraggio netapp
- ci-kube-rbac-proxy
- ci-ksm
- ci-telegraf

- utente root senza distribuzione

Registro eventi

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

Prestazioni e mappa della rete

- ci-net-observer

Invia l'immagine Docker dell'operatore al tuo repository Docker privato/locale/aziendale in base alle policy aziendali. Assicurati che i tag delle immagini e i percorsi delle directory di queste immagini nel tuo repository siano coerenti con quelli nel repository Data Infrastructure Insights .

Modifica la distribuzione monitoring-operator in operator-deployment.yaml e modifica tutti i riferimenti alle immagini per utilizzare il tuo 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>
```

Modifica *AgentConfiguration* in *operator-config.yaml* per riflettere la nuova posizione del docker repo. 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
```

Token di accesso API per password a lungo termine

Alcuni ambienti (ad esempio repository proxy) richiedono password a lungo termine per il Data Infrastructure Insights docker repository. La password fornita nell'interfaccia utente al momento dell'installazione è valida solo per 24 ore. Invece di utilizzare quella, si può usare un API Access Token come password del docker repository. Questa password sarà valida finché l'API Access Token sarà valido. Si può generare un nuovo API Access Token per questo scopo specifico o utilizzarne uno esistente.

"Leggi qui" per istruzioni su come creare un nuovo token di accesso API.

Per estrarre un API Access Token esistente da un file *operator-secrets.yaml* scaricato, gli utenti possono eseguire quanto segue:

```
grep '\.dockerconfigjson' operator-secrets.yaml |sed 's/.*\.dockerconfigjson:
//g' |base64 -d |jq
```

Per estrarre un API Access Token esistente da un'installazione dell'operatore in esecuzione, gli utenti possono eseguire quanto segue:

```
kubectl -n netapp-monitoring get secret netapp-ci-docker -o
jsonpath='{.data.\.dockerconfigjson}' |base64 -d |jq
```

Istruzioni OpenShift

Se si utilizza OpenShift 4.6 o versioni successive, è necessario modificare *AgentConfiguration* in *operator-config.yaml* per abilitare l'impostazione *runPrivileged*:

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

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

Tolleranze e difetti

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 per tollerare alcune **imperfezioni** ben note. Se hai configurato delle taint personalizzate sui tuoi nodi, impedendo così ai pod di essere eseguiti su ogni nodo, puoi creare una **tolleranza** per quelle taint"nella *AgentConfiguration*" . Se hai applicato taint personalizzati a tutti i nodi del tuo cluster, devi anche aggiungere le tolleranze necessarie alla distribuzione dell'operatore per consentire la pianificazione e l'esecuzione del pod dell'operatore.

Scopri di più su Kubernetes"Contaminazioni e tolleranze" .

Ritorno al"* Pagina di installazione dell'operatore di monitoraggio NetApp Kubernetes*"

Una nota sui segreti

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

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

Se si tratta di un aggiornamento, elimina anche le risorse dal tuo 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 abilitata, modificare *AgentConfiguration* o *operator-config.yaml* per rimuovere il commento dalla sezione change-management e includere *kindsToIgnoreFromWatch: '"secrets"'* nella sezione change-management. Notare la presenza e la posizione delle 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 delle immagini degli operatori di monitoraggio di Kubernetes

L'immagine per l'operatore e tutte le immagini correlate che distribuisce sono firmate da NetApp. È possibile verificare manualmente le immagini prima dell'installazione utilizzando lo strumento di co-firma oppure configurare un controller di ammissione Kubernetes. Per maggiori dettagli si prega di consultare il"Documentazione di Kubernetes" .

La chiave pubblica utilizzata per verificare le firme delle immagini è disponibile nel riquadro di installazione dell'operatore di monitoraggio in *Facoltativo: carica le immagini dell'operatore nel tuo repository privato > Chiave pubblica della firma dell'immagine*

Per verificare manualmente una firma immagine, procedere come segue:

1. Copia ed esegui l'Image Pull Snippet
2. Copia e inserisci la password del repository quando richiesto
3. Memorizza la chiave pubblica della firma dell'immagine (dii-image-signing.pub nell'esempio)
4. Verificare le immagini tramite co-firma. Fare riferimento al seguente esempio di utilizzo del cosign

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

Risoluzione dei problemi

Ecco alcune cose da provare se riscontri problemi durante la configurazione dell'operatore di monitoraggio Kubernetes:

Problema:	Prova questo:
Non vedo alcun collegamento ipertestuale/connessione tra il mio volume persistente Kubernetes e il dispositivo di archiviazione back-end corrispondente. Il mio volume persistente Kubernetes è configurato utilizzando il nome host del server di archiviazione.	Seguire i passaggi per disinstallare l'agente Telegraf esistente, quindi reinstallare l'agente Telegraf più recente. È necessario utilizzare Telegraf versione 2.0 o successiva e l'archiviazione del cluster Kubernetes deve essere monitorata attivamente da Data Infrastructure Insights.

Problema:	Prova questo:
Nei log vedo messaggi simili ai seguenti: E0901 15:21:39.962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Impossibile elencare *v1.MutatingWebhookConfiguration: il server non è riuscito a trovare la risorsa richiesta E0901 15:21:43.168161 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Impossibile elencare *v1.Lease: il server non è riuscito a trovare la risorsa richiesta (ottenere leases.coordination.k8s.io) ecc.	Questi messaggi possono essere visualizzati se si esegue kube-state-metrics versione 2.0.0 o successiva con versioni di Kubernetes precedenti 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 distribuzione di kube-state-metrics per disabilitare i seguenti lease: *mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources* Più specificamente, possono utilizzare il seguente argomento CLI: resources=certificatesigningrequests,configmaps,cronjobs,daemonsets, deployments,endpoints,horizontalpodautoscalers,ingresses,jobs,limitranges, namespaces,networkpolicies,nodes,persistentvolumeclaims,persistentvolumes, poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas, secrets,services,statefulsets,storageclasses L’elenco di risorse predefinito è: "certificatesigningrequests,configmaps,cronjobs,daemonsets,deployments, endpoints,horizontalpodautoscalers,ingresses,jobs,leases,limitranges, mutatingwebhookconfigurations,namespaces,networkpolicies,nodes, persistentvolumeclaims,persistentvolumes,poddisruptionbudgets,pods,replicasets, replicationcontrollers,resourcequotas,secrets,services, statefulsets,storageclasses, validatingwebhookconfigurations,volumeattachments"

Problema:	Prova questo:
Vedo messaggi di errore da Telegraf simili ai seguenti, ma Telegraf si avvia ed è in esecuzione: 11 ott 14:23:41 ip-172-31-39-47 systemd[1]: Avviato L'agente server basato su plugin per la segnalazione delle metriche in InfluxDB. 11 ott 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:120" 11 ott 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="apertura non riuscita. Ignorato. Apri /etc/telegraf/.cache/snowflake/ocsp_response_cache.json: nessun file o directory\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11 ott 14:23:41 ip-172-31-39-47 telegraf[1827]: 2021-10-11T14:23:41Z I! Avvio di Telegraf 1.19.3	Questo è un problema noto. Fare riferimento a"Questo articolo di GitHub" per maggiori dettagli. Finché Telegraf è attivo e funzionante, gli utenti possono ignorare questi messaggi di errore.
Su Kubernetes, i miei pod Telegraf segnalano il seguente errore: "Errore nell'elaborazione delle informazioni mountstats: impossibile aprire il file mountstats: /hostfs/proc/1/mountstats, errore: apertura /hostfs/proc/1/mountstats: autorizzazione negata"	Se SELinux è abilitato e applicato, è probabile che impedisca ai pod Telegraf di accedere al file /proc/1/mountstats sul nodo Kubernetes. Per superare questa restrizione, modificare agentconfiguration e abilitare l'impostazione runPrivileged. Per maggiori dettagli, fare riferimento alle istruzioni di OpenShift.
Su Kubernetes, il mio pod Telegraf ReplicaSet segnala 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.crt: nessun file o directory del genere	Il pod Telegraf ReplicaSet è progettato per essere eseguito su un nodo designato come master o per etcd. Se il pod ReplicaSet non è in esecuzione su uno di questi nodi, verranno visualizzati questi errori. Controlla se i tuoi nodi master/etcd presentano delle anomalie. In tal caso, aggiungere le tolleranze necessarie al Telegraf ReplicaSet, telegraf-rs. Ad esempio, modifica ReplicaSet… kubectl edit rs telegraf-rs …e aggiungi le tolleranze appropriate alla specifica. Quindi, riavviare il pod ReplicaSet.

Problema:	Prova questo:
Ho un ambiente PSP/PSA. Ciò ha ripercussioni 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 alla versione più recente di Kubernetes Monitoring Operator. Per effettuare l'aggiornamento all'operatore corrente con supporto per PSP/PSA, seguire questi passaggi: 1. Disinstallare l'operatore di monitoraggio precedente: kubectl delete agent agent-monitoring-netapp -n netapp-monitoring kubectl delete ns netapp-monitoring kubectl delete crd agents.monitoring.netapp.com kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding 2. Installare l'ultima versione dell'operatore di monitoraggio.
Ho riscontrato problemi nel tentativo di distribuire l'Operatore e sto utilizzando PSP/PSA.	1. Modificare l'agente utilizzando il seguente comando: kubectl -n <name-space> edit agent 2. Contrassegna 'security-policy-enabled' come 'false'. In questo modo verranno disattivati i criteri di sicurezza del Pod e l'ammissione di sicurezza del Pod e sarà consentito all'operatore di effettuare la distribuzione. Confermare utilizzando i seguenti comandi: kubectl get psp (dovrebbe mostrare che la politica di sicurezza del pod è stata rimossa) kubectl get all -n <namespace>
grep -i psp (dovrebbe mostrare che non è stato trovato nulla)	Errori "ImagePullBackoff" rilevati
Questi errori potrebbero verificarsi se si dispone di un repository Docker personalizzato o privato e non è ancora stato configurato Kubernetes Monitoring Operator per riconoscerlo correttamente. Per saperne di più sulla configurazione per repository personalizzati/privati.	Ho un problema con la distribuzione del mio operatore di monitoraggio e la documentazione attuale non mi aiuta a risolverlo.

Problema:	Prova questo:

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 (Workload Map) nello spazio dei nomi Operator sono in CrashLoopBackOff

Questi pod corrispondono al raccoglitore di dati Workload Map per Network Observability. Prova questi: • Controlla 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","environment":"prod","level":"error","msg":"fallimento nella convalida. Motivo: la versione del kernel 3.10.0 è inferiore alla versione minima del kernel 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 utilizzando il comando "uname -r" e assicurarsi che sia >= 4.18.0	I pod sono in esecuzione nello spazio dei nomi Operatore (predefinito: netapp-monitoring), ma nell'interfaccia utente non vengono visualizzati dati per la mappa del carico di lavoro o metriche Kubernetes nelle query
Controllare l'impostazione dell'ora sui nodi del cluster K8S. Per un audit e una segnalazione dei dati accurati, si consiglia vivamente di sincronizzare l'ora sulla macchina dell'agente utilizzando il protocollo NTP (Network Time Protocol) o il protocollo SNTP (Simple Network Time Protocol).	Alcuni dei pod net-observer nello spazio dei nomi Operator sono nello stato In sospeso
Net-observer è un DaemonSet ed esegue un pod in ogni nodo del cluster k8s. • Prendi nota del pod che si trova nello stato In sospeso e controlla se sta riscontrando un problema di risorse per la CPU o la memoria. Assicurarsi che nel nodo siano disponibili la memoria e la CPU richieste.	Subito dopo aver installato Kubernetes Monitoring Operator, vedo quanto segue nei miei log: [inputs.prometheus] Errore nel plugin: errore durante la richiesta HTTP a http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Ottieni http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: dial tcp: cerca kube-state-metrics.<namespace>.svc.cluster.local: nessun host del genere

Problema:	Prova questo:
In genere questo messaggio viene visualizzato solo quando viene installato un nuovo operatore e il pod *telegraf-rs* è attivo prima del pod *ksm*. Questi messaggi dovrebbero cessare una volta che tutti i pod saranno in esecuzione.	Non vedo alcuna metrica raccolta per i CronJob di Kubernetes presenti nel mio cluster.
Verifica la tua versione di Kubernetes (ad esempio `kubectl version`). Se la versione è v1.20.x o precedente, si tratta di una limitazione prevista. La versione kube-state-metrics distribuita con Kubernetes Monitoring Operator supporta solo v1.CronJob. Con Kubernetes 1.20.x e versioni precedenti, la risorsa CronJob si trova in v1beta.CronJob. Di conseguenza, kube-state-metrics non riesce a trovare la risorsa CronJob.	Dopo aver installato l'operatore, i pod telegraf-ds entrano in CrashLoopBackOff e i log dei pod indicano "su: Authentication failure".
Modifica la sezione telegraf in *AgentConfiguration* e imposta *dockerMetricCollectionEnabled* su false. Per maggiori dettagli, fai riferimento a "opzioni di configurazione" dell'operatore. … spec: … telegraf: … - name: docker run-mode: - DaemonSet substitutions: - key: DOCKER_UNIX_SOCK_PLACEHOLDER value: unix:///run/docker.sock … …	Nei miei registri di Telegraf vedo messaggi di errore ricorrenti simili ai seguenti: E! [agente] Errore durante la scrittura su output.http: Post "https://<tenant_url>/rest/v1/lake/ingest/influxdb": scadenza del contesto superata (Client.Timeout superato durante l'attesa delle intestazioni)
Modificare la sezione telegraf in *AgentConfiguration* e aumentare *outputTimeout* a 10 s. Per maggiori dettagli fare riferimento al manuale dell'operatore"opzioni di configurazione" .	Mancano i dati *involvedobject* per alcuni registri eventi.
Assicurati di aver seguito i passaggi indicati in"Permessi" sezione sopra.	Perché vedo due pod di operatori di monitoraggio 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 riorganizzato l'operatore per servire meglio i nostri utenti; affinché tali modifiche vengano adottate completamente, è necessariorimuovere il vecchio operatore Einstallare quello nuovo .	I miei eventi Kubernetes hanno smesso inaspettatamente di segnalare a Data Infrastructure Insights.
Recupera il nome del pod event-exporter: `` `kubectl -n netapp-monitoring get pods ``	grep event-exporter

Problema:	Prova questo:
awk '{print $1}'	sed 's/event-exporter./event-exporter/` Dovrebbe essere "netapp-ci-event-exporter" o "event-exporter". Successivamente, modifica l'agente di monitoraggio `kubectl -n netapp-monitoring edit agent` e impostare il valore per LOG_FILE in modo che rifletta il nome appropriato del pod di esportazione eventi trovato nel passaggio precedente. Più specificatamente, LOG_FILE dovrebbe essere impostato su "/var/log/containers/netapp-ci-event-exporter.log" o "/var/log/containers/event-exporter*.log" …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. In alternativa, si può anchedisinstallare Ereinstallare l'agente.
Vedo che i pod distribuiti dal Kubernetes Monitoring Operator si bloccano a causa di risorse insufficienti.	Fare riferimento all'operatore di monitoraggio Kubernetes"opzioni di configurazione" per aumentare i limiti della CPU e/o della memoria secondo necessità.
Un'immagine mancante o una configurazione non valida hanno impedito l'avvio o la disponibilità dei pod netapp-ci-kube-state-metrics. Ora StatefulSet è bloccato e le modifiche alla configurazione non vengono applicate ai pod netapp-ci-kube-state-metrics.	Lo StatefulSet è in un"rotto" stato. Dopo aver risolto eventuali problemi di configurazione, riavviare i pod netapp-ci-kube-state-metrics.
I pod netapp-ci-kube-state-metrics non riescono ad avviarsi dopo aver eseguito un aggiornamento dell'operatore Kubernetes, generando l'errore ErrImagePull (impossibilità di estrarre l'immagine).	Prova a reimpostare manualmente i pod.
Durante l'analisi dei log, vengono visualizzati i messaggi "Evento scartato perché più vecchio di maxEventAgeSeconds" per il mio cluster Kubernetes.	Modificare l'operatore *agentconfiguration* e aumentare *event-exporter-maxEventAgeSeconds* (ad esempio a 60 s), *event-exporter-kubeQPS* (ad esempio a 100) e *event-exporter-kubeBurst* (ad esempio a 500). Per maggiori dettagli su queste opzioni di configurazione, vedere"opzioni di configurazione" pagina.

Problema:	Prova questo:
Telegraf avvisa o si blocca a causa di una memoria bloccabile insufficiente.	Prova ad aumentare il limite di memoria bloccabile per Telegraf nel sistema operativo/nodo sottostante. Se aumentare il limite non è un'opzione, modificare la configurazione dell'agente NKMO e impostare *unprotected* su *true*. Ciò indicherà a Telegraf di non tentare di riservare pagine di memoria bloccate. Sebbene ciò possa rappresentare un rischio per la sicurezza, in quanto i segreti decrittati potrebbero essere trasferiti su disco, consente l'esecuzione in ambienti in cui non è possibile riservare memoria bloccata. Per maggiori dettagli sulle opzioni di configurazione *non protette*, fare riferimento a"opzioni di configurazione" pagina.
Vedo messaggi di avviso da Telegraf simili ai seguenti: *W! [inputs.diskio] Impossibile raccogliere il nome del disco per "vdc": errore durante la lettura di /dev/vdc: nessun file o directory del genere*	Per il Kubernetes Monitoring Operator, questi messaggi di avviso sono benigni e possono essere ignorati senza problemi. In alternativa, modifica la sezione telegraf in AgentConfiguration e imposta *runDsPrivileged* su true. Per maggiori dettagli, consulta il "opzioni di configurazione dell'operatore".

Problema:	Prova questo:

Il mio pod fluent-bit non funziona con i seguenti errori: [2024/10/16 14:16:23] [errore] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno=24] Troppi file aperti [2024/10/16 14:16:23] [errore] inizializzazione input tail.0 non riuscita [2024/10/16 14:16:23] [errore] [motore] inizializzazione input non riuscita	Prova a modificare le impostazioni *fsnotify* nel tuo 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>`
	Riavvia Fluent-bit.
	Nota: per rendere queste impostazioni persistenti tra i riavvii del nodo, 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>`

Problema:	Prova questo:
I pod DS di Telegraf segnalano errori relativi al plugin di input Kubernetes che non riesce a effettuare richieste HTTP a causa dell’impossibilità di convalidare il certificato TLS. Ad esempio: E! [inputs.kubernetes] Errore nel plugin: errore durante la richiesta HTTP a"<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 alcun IP SAN	Ciò si verifica se il kubelet utilizza certificati autofirmati e/o il certificato specificato non include <kubelet_IP> nell'elenco *Subject Alternative Name* dei certificati. Per risolvere questo problema, l'utente può modificare il"configurazione dell'agente" e impostare *telegraf:insecureK8sSkipVerify* su *true*. In questo modo il plugin di input Telegraf verrà configurato 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'.
Ricevo il seguente errore nei pod Fluent-bit e il pod non può essere avviato: 026/01/12 20:20:32] [error] [sqldb] error=unable to open database file [2026/01/12 20:20:32] [error] [input:tail:tail.0] db: could not create 'in_tail_files' table [2026/01/12 20:20:32] [error] [input:tail:tail.0] could not open/create database [2026/01/12 20:20:32] [error] failed initialize input tail.0 [2026/01/12 20:20:32] [error] [engine] input initialization failed	Assicurarsi che la directory host in cui risiede il file DB disponga dei permessi di lettura/scrittura appropriati. Più specificamente, la directory host dovrebbe concedere permessi di lettura/scrittura agli utenti non root. Il percorso predefinito del file DB è /var/log/ a meno che non venga sovrascritto dall'opzione fluent-bit-dbFile *agentconfiguration*. Se SELinux è abilitato, provare a impostare l'opzione fluent-bit-seLinuxOptionsType agentconfiguration su 'spc_t'

Ulteriori informazioni possono essere trovate presso"Supporto" pagina o nella"Matrice di supporto del raccoglitore dati" .

Memcached Data Collector

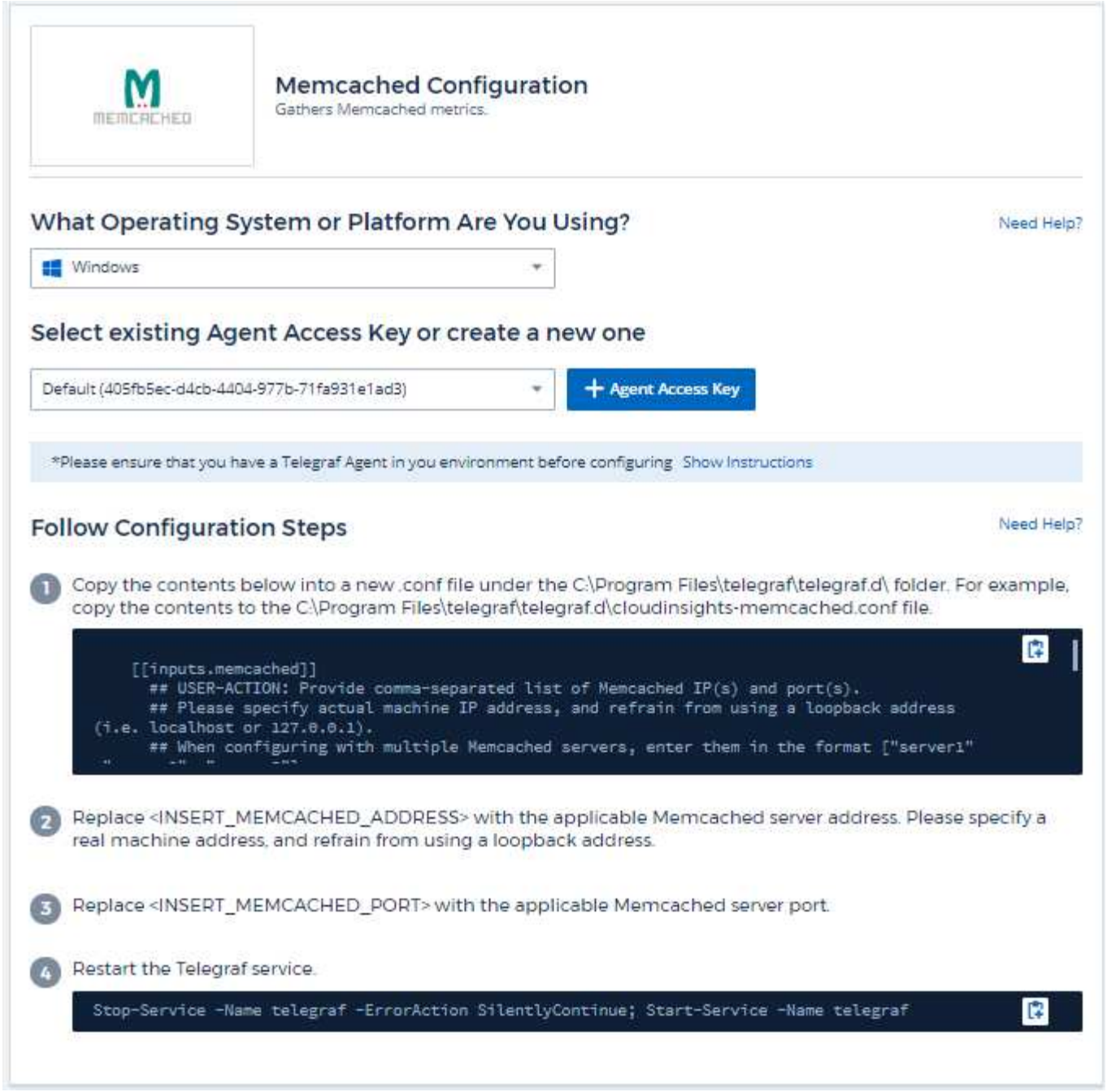
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da Memcached.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Memcached.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel"Wiki di Memcached" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Memcached	Server dello spazio dei nomi	IP del nodo Nome del nodo	Accettazione di connessioni Gestite Richieste di autenticazione Autenticazioni non riuscite Byte utilizzati Byte letti (al sec) Byte scritti (al sec) CAS Badval CAS Hit CAS Misses Richieste di svuotamento (al sec) Richieste di ottenimento (al sec) Richieste di impostazione (al sec) Richieste di tocco (al sec) Rendimenti di connessione (al sec) Strutture di connessione Connessioni aperte Elementi archiviati correnti Richieste di decr Hit (al sec) Richieste di decr Misses (al sec) Richieste di eliminazione Hit (al sec) Richieste di eliminazione Misses (al sec) Elementi espulsi Espulsioni valide Elementi scaduti Hit di ottenimento (al sec) Misses di ottenimento (al sec) Byte hash utilizzati L'hash è in espansione Livello di potenza hash Richieste di incremento Hit (al sec) Richieste di incremento Misses (al sec) Byte massimi del server Ascolto disabilitato Numero thread worker recuperati Conteggio Totale connessioni aperte Totale elementi archiviati Hit di tocco Misses di tocco Tempo di attività del server

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore dati MongoDB

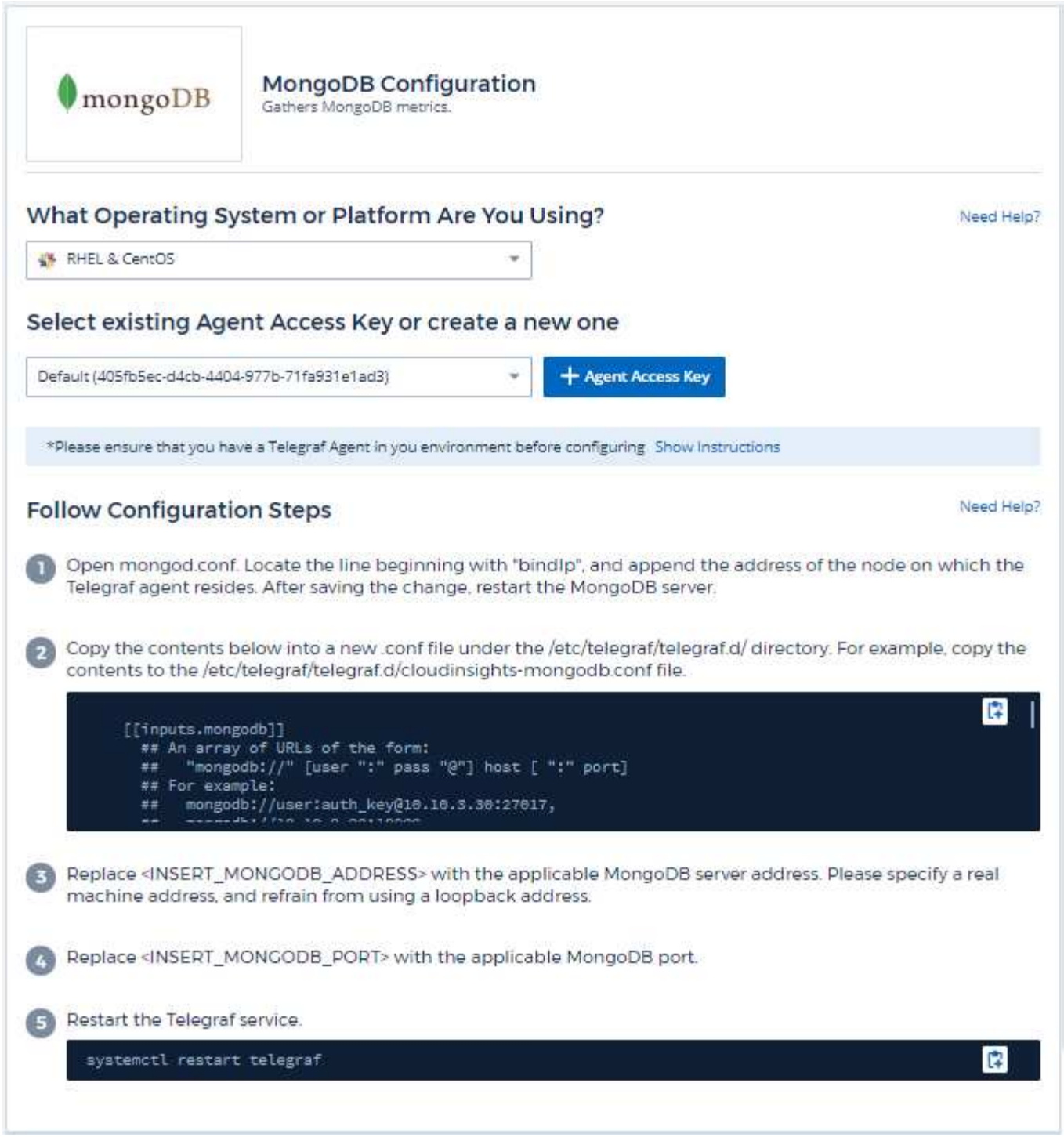
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da MongoDB.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli MongoDB.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel"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 del database		

Risoluzione dei problemi

Le informazioni possono essere trovate da"Supporto" pagina.

Raccoglitore dati MySQL

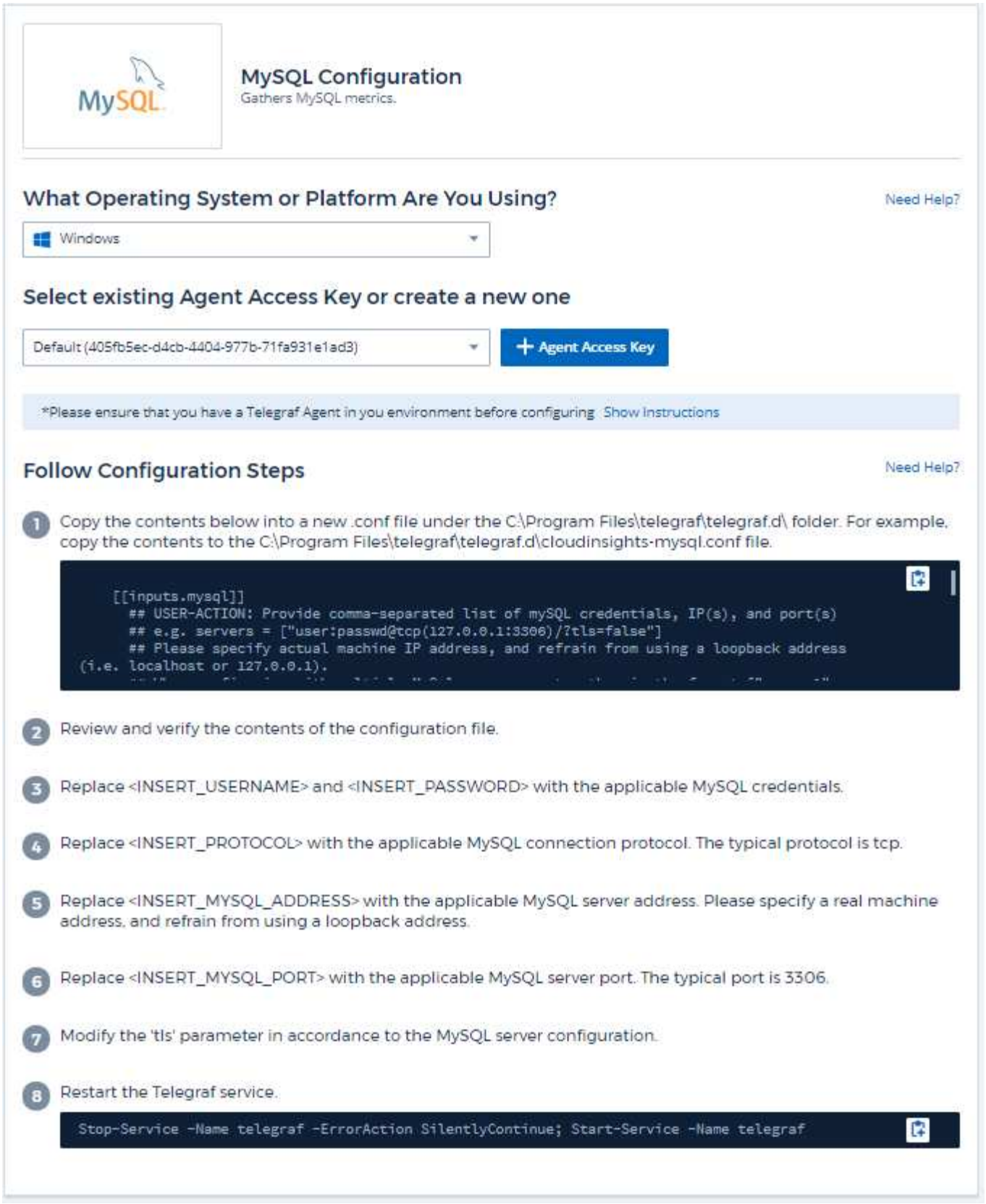
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da MySQL.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli MySQL.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel"Documentazione MySQL" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
MySQL	Spazio dei nomi MySQL Server	IP del nodo Nome del nodo	Client interrotti (al secondo) Connessioni interrotte (al secondo) Byte RX (al secondo) Byte TX (al secondo) Comandi Admin (al secondo) Comandi Comandi Alter Event Comandi Alter Function Comandi Alter Instance Comandi Alter Procedure Comandi Alter Server Comandi Alter Table Comandi Alter Tablespace Comandi Alter User Comandi Analyze Comandi Assign To Keycache Comandi Begin Comandi Binlog Comandi Call Procedure Comandi Change DB Comandi Change Master Comandi Change Repl Filter Comandi Check Comandi Checksum Comandi Commit Comandi Create DB Comandi Create Event Comandi Create Function Comandi Create Index Comandi Create Procedure Comandi Create Server Comandi Create Table Comandi Create Trigger Comandi Create UDF Comandi Create User Comandi Create View Errori di connessione SQL Dealloc Accetta tabelle disco Tmp create Errori ritardati Comandi Flush Gestore Commit Byte del buffer pool Innodb Blocchi chiave dati non svuotati Richieste di lettura chiave Richieste di scrittura chiave Scritture chiave Tempo massimo di esecuzione Superato il numero massimo di connessioni utilizzate File aperti Prestazioni Schema Account persi Conteggio stmt preparati Qcache Blocchi liberi Query Domande Seleziona

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore dati Netstat

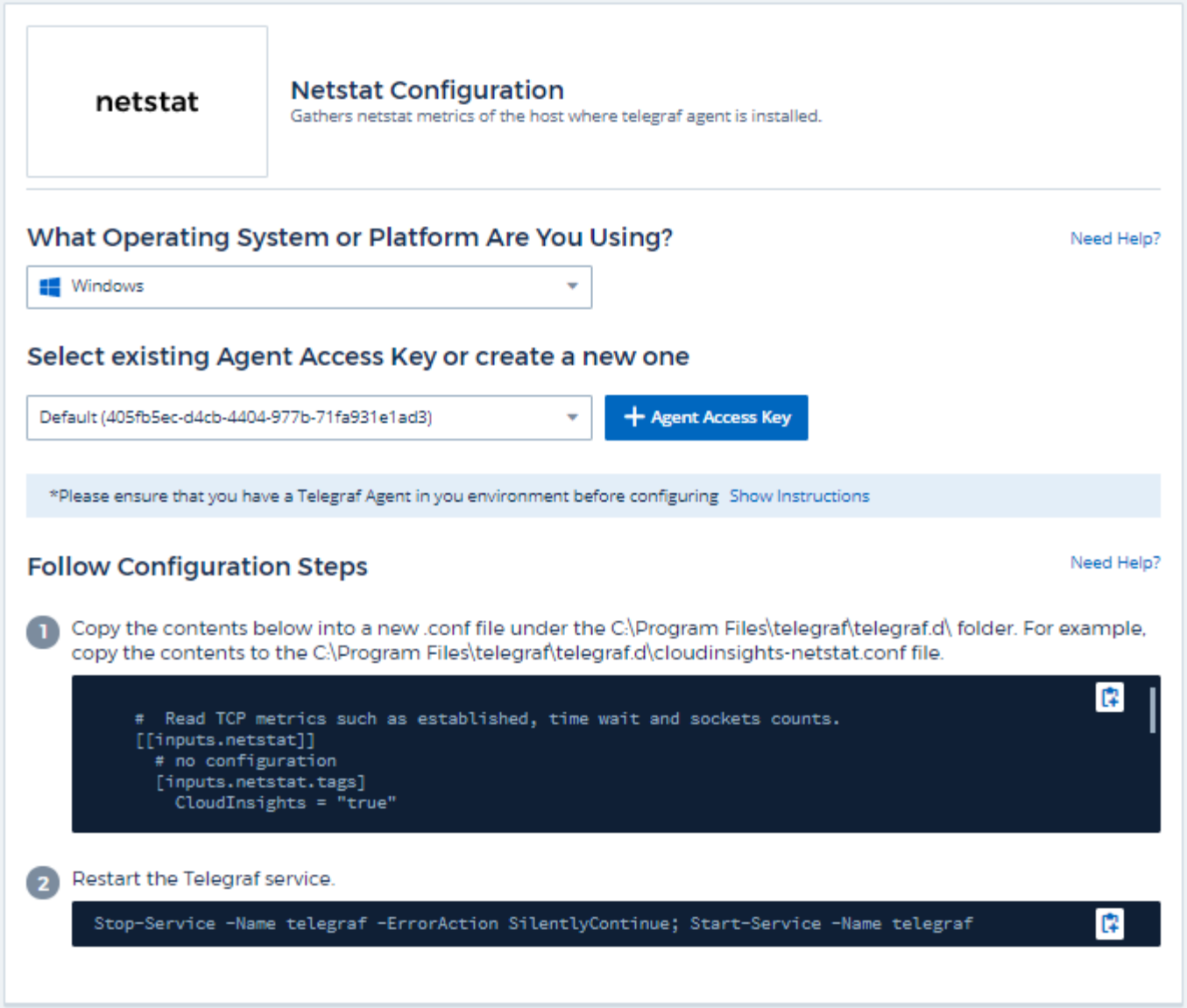
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere le metriche Netstat.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Selezionare Netstat.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore dati Nginx

Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da

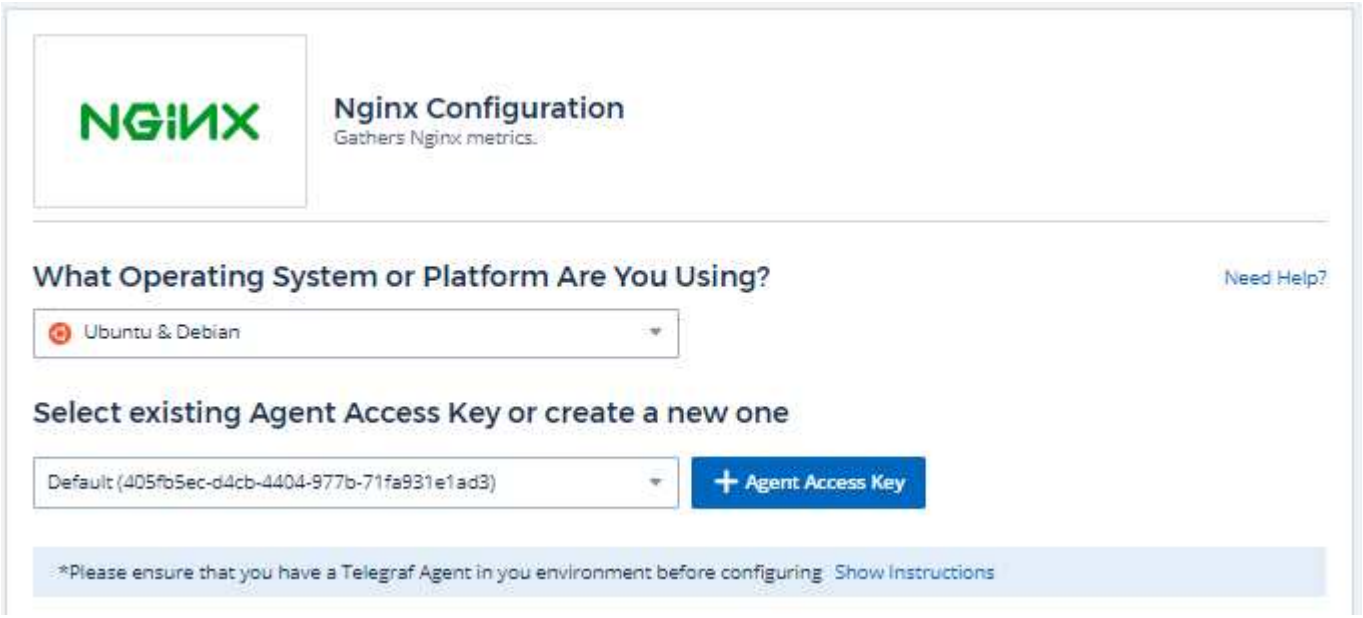
Nginx.

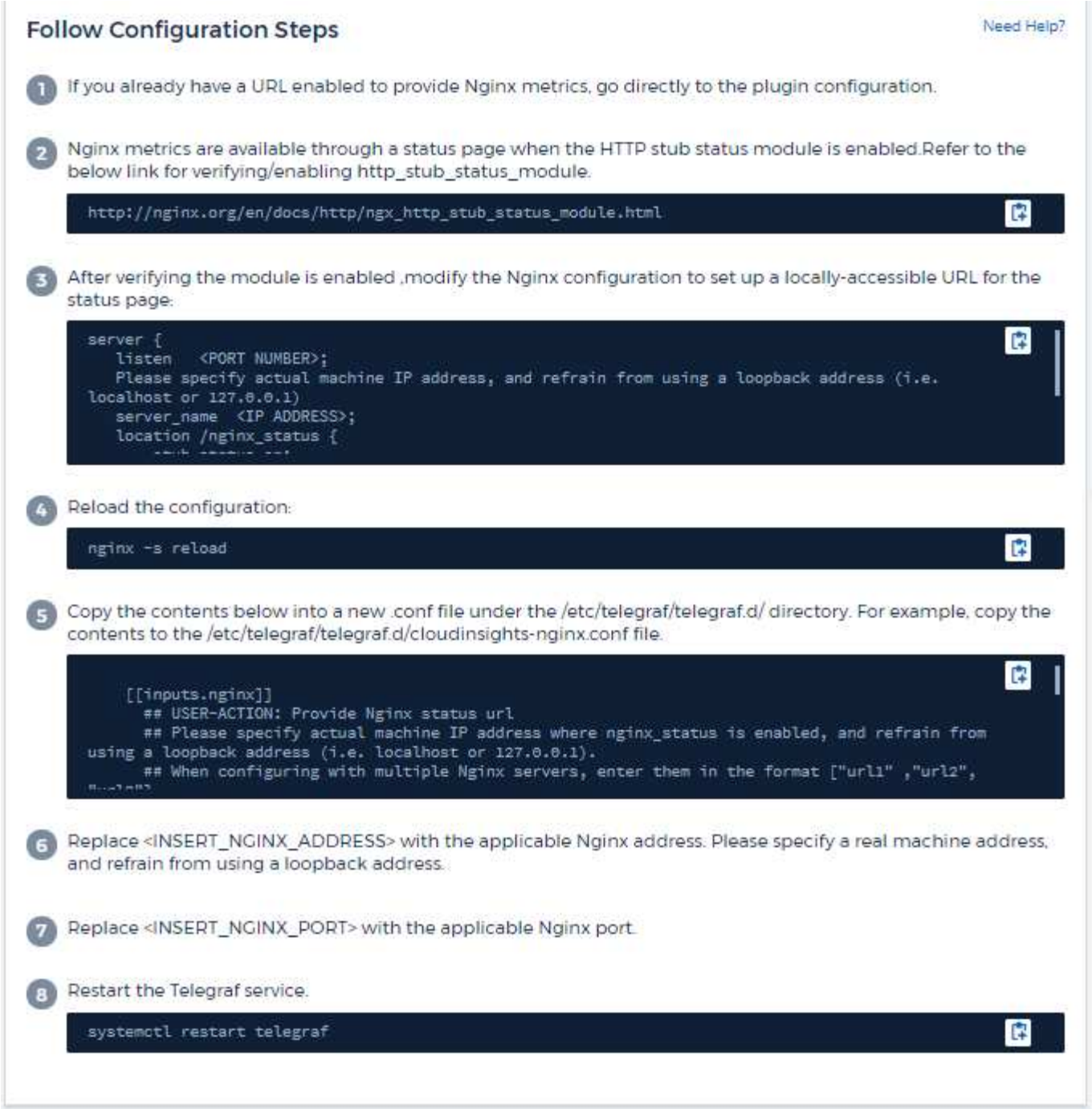
Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Nginx.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.





Impostare

La raccolta delle metriche Nginx richiede che Nginx"http_stub_status_module" essere abilitato.

Ulteriori informazioni possono essere trovate nel"Documentazione Nginx" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Nginx	Server dello spazio dei nomi	IP del nodo Nome del nodo Porta	Accetta richieste di lettura gestite attive in attesa di scrittura

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore dati PostgreSQL

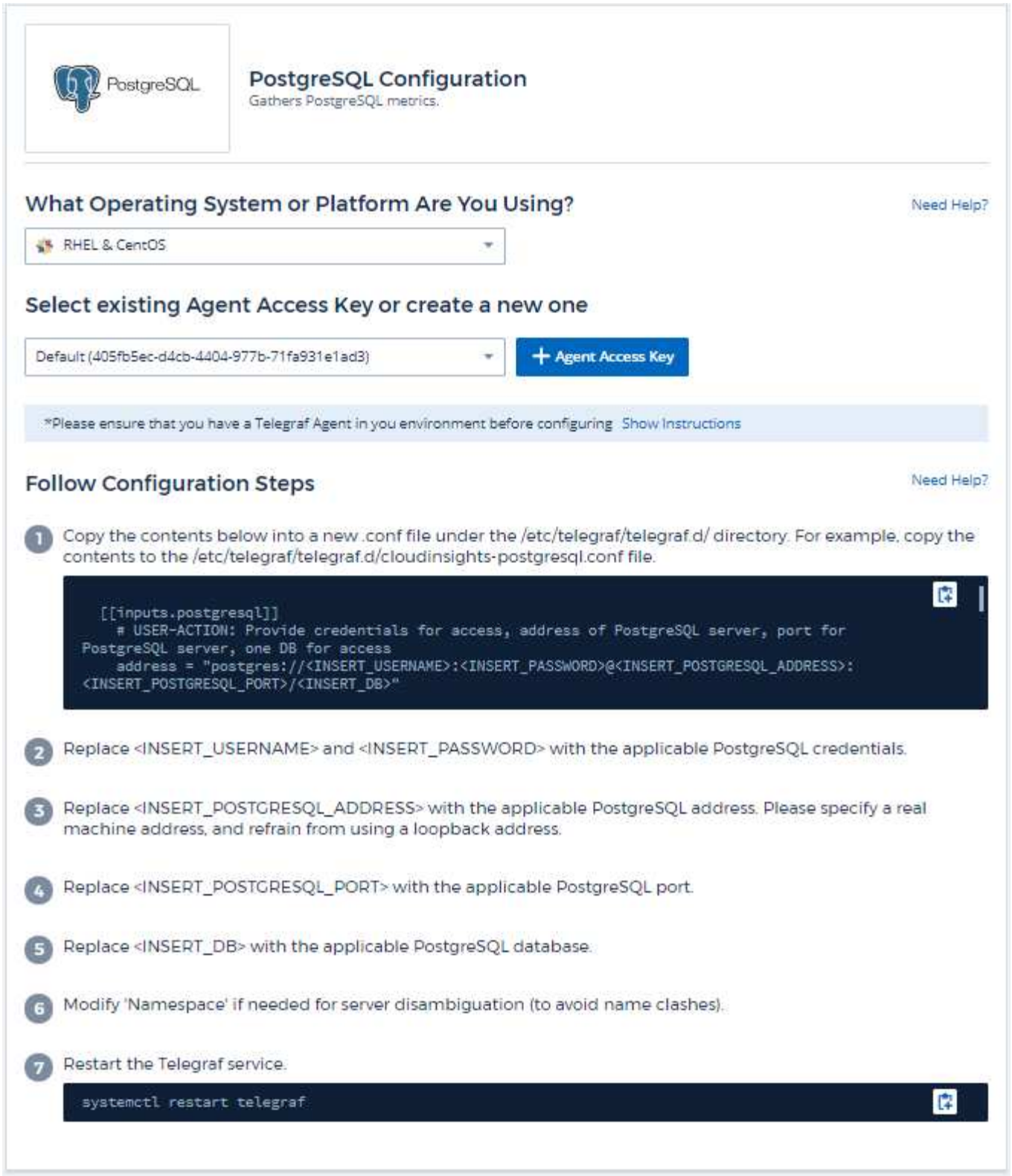
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da PostgreSQL.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli PostgreSQL.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel"Documentazione PostgreSQL" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Server PostgreSQL	Server di database dello spazio dei nomi	Nome nodo IP nodo	Buffer allocati Buffer backend Buffer di sincronizzazione file backend Buffer di checkpoint Checkpoint puliti Checkpoint di tempo di sincronizzazione Checkpoint di tempo di scrittura Richieste Checkpoint Tempo massimo di scrittura pulita
Database PostgreSQL	Server di database dello spazio dei nomi	OID del database Nome del nodo IP del nodo	Blocchi Tempo di lettura Blocchi Tempo di scrittura Blocchi Hit Blocchi Letture Conflitti Deadlock Numero client File temporanei Byte Numero file temporanei Righe Righe eliminate Righe recuperate Righe inserite Righe restituite Transazioni aggiornate Transazioni confermate Rollback

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Raccoglitore di dati dell'agente fantoccio

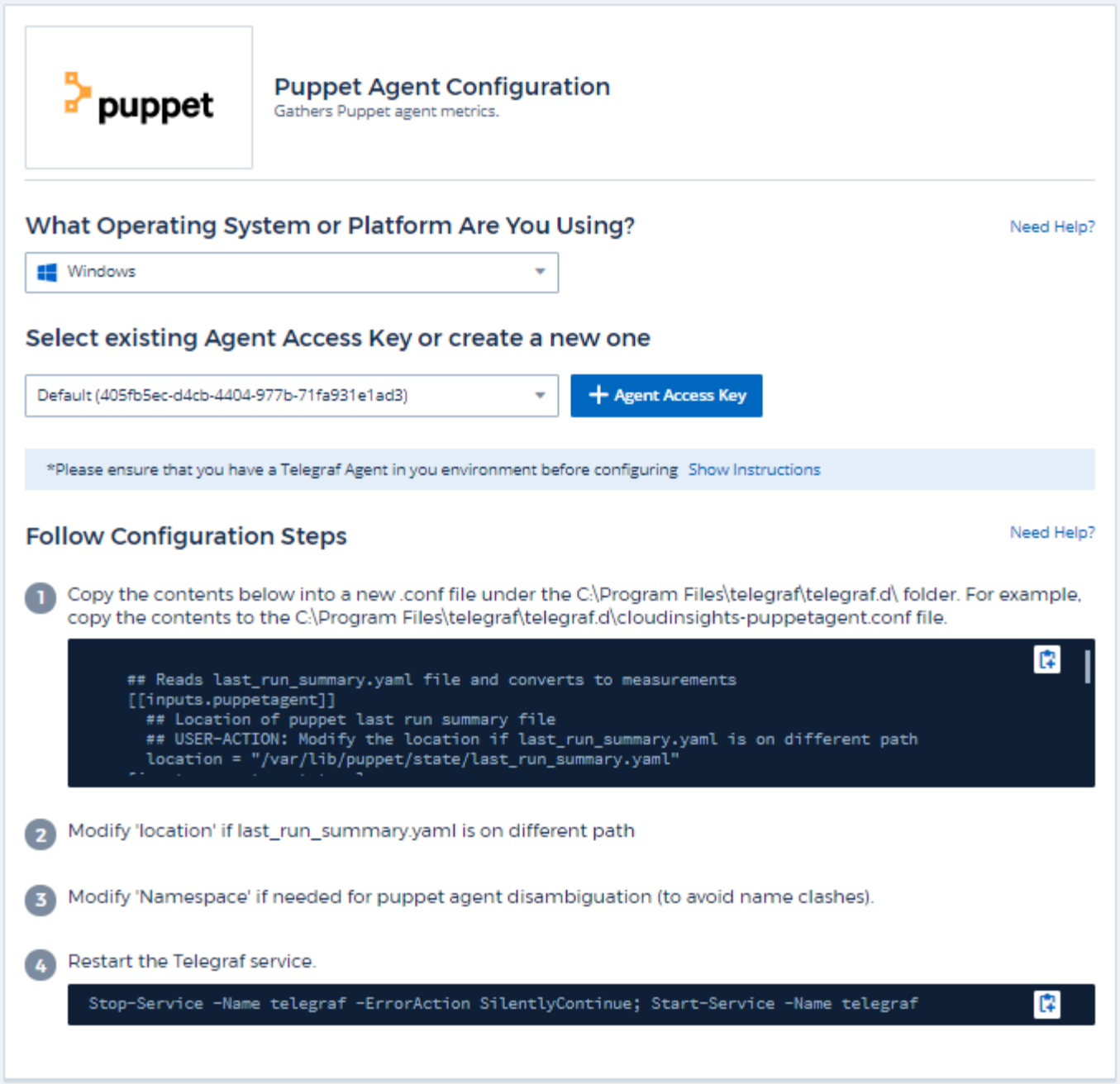
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da Puppet Agent.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Marionetta.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel "Documentazione dei burattini"

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:

Agente burattino	UUID del nodo dello spazio dei nomi	Nome nodo Posizione IP nodo Versione Configstring Versione Puppet	Modifiche Eventi totali Eventi di errore Eventi di successo Risorse totali Risorse modificate Risorse non riuscite Risorse non riavviate Risorse non sincronizzate Risorse riavviate Risorse pianificate Risorse ignorate Tempo totale Tempo di ancoraggio Tempo di configretrieval Tempo di cron Tempo di esecuzione Tempo di file Tempo di filebucket Tempo di ultima esecuzione Tempo del pacchetto Tempo di pianificazione Tempo di servizio Tempo di sshauthorizedkey Tempo totale utente

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Redis Data Collector

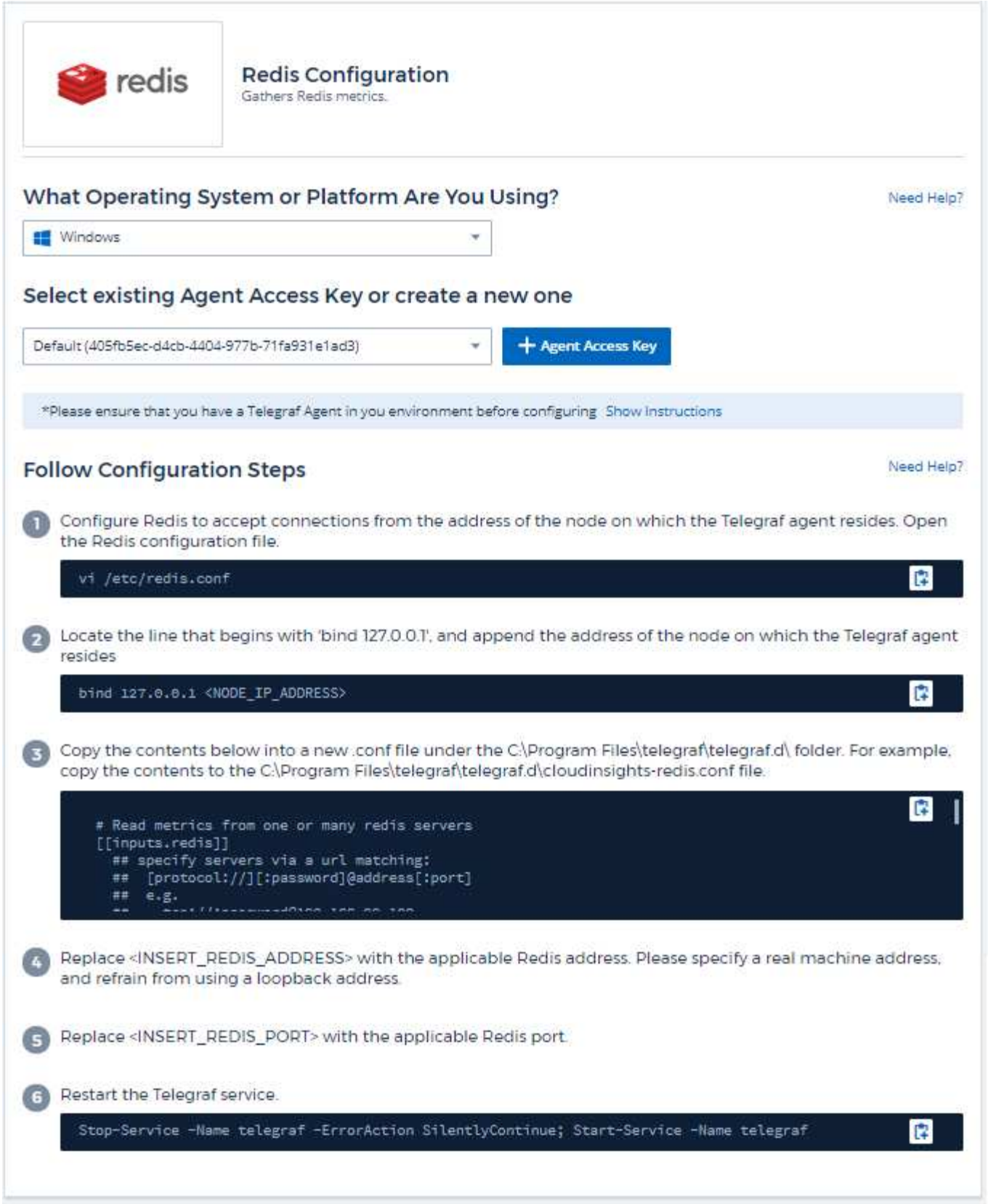
Data Infrastructure Insights utilizza questo raccoglitore di dati per raccogliere metriche da Redis. Redis è un archivio di strutture dati in memoria open source utilizzato come database, cache e broker di messaggi, che supporta le seguenti strutture dati: stringhe, hash, elenchi, set e altro ancora.

Installazione

1. Da **Osservabilità > Collettori**, fare clic su **+Collettore dati**. Scegli Redis.

   Selezionare il sistema operativo o la piattaforma su cui è installato l'agente Telegraf.

2. Se non hai ancora installato un agente per la raccolta o desideri installare un agente per un sistema operativo o una piattaforma diversi, fai clic su *Mostra istruzioni* per espandere la"Installazione dell'agente" istruzioni.
3. Selezionare la chiave di accesso dell'agente da utilizzare con questo raccoglitore dati. È possibile aggiungere una nuova chiave di accesso agente facendo clic sul pulsante **+ Chiave di accesso agente**. Procedura consigliata: utilizzare una chiave di accesso agente diversa solo quando si desidera raggruppare i raccoglitori di dati, ad esempio in base al sistema operativo/piattaforma.
4. Seguire i passaggi di configurazione per configurare il raccoglitore dati. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per raccogliere i dati.



Impostare

Le informazioni possono essere trovate nel"Documentazione Redis" .

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Redis	Server dello spazio dei nomi		

Risoluzione dei problemi

Ulteriori informazioni possono essere trovate presso"Supporto" pagina.

Informazioni sul copyright

Informazioni sul marchio commerciale