



Riferimento Data Collector - servizi

Data Infrastructure Insights

NetApp
January 17, 2025

Sommario

Riferimento Data Collector - servizi	1
Raccolta dati nodo	1
ActiveMQ Data Collector	3
Apache Data Collector	5
Consul Data Collector	8
Couchbase Data Collector	9
Data Collector di CouchDB	11
Docker Data Collector	13
Elasticsearch Data Collector	20
Flink Data Collector	22
Data Collector Hadoop	29
HAProxy Data Collector	34
Data Collector JVM	40
Data Collector Kafka	45
Kibana Data Collector	48
Installazione e configurazione dell'operatore di monitoraggio Kubernetes	50
Data Collector Memcached	69
MongoDB Data Collector	71
MySQL Data Collector	74
Netstat Data Collector	79
Data Collector nginx	80
PostgreSQL Data Collector	83
Puppet Agent Data Collector	85
Redis Data Collector	87

Riferimento Data Collector - servizi

Raccolta dati nodo

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

Installazione

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

Oggetti e contatori

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

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

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

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

Setup (Configurazione)

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

ActiveMQ Data Collector

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

Installazione

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

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



ActiveMQ Configuration

Gathers ActiveMQ metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-activemq.conf file.

```
[[inputs.activemq]]
  ## Required ActiveMQ Endpoint, port
  ## USER-ACTION: Provide address of ActiveMQ, HTTP port for ActiveMQ
  server = "<INSERT_ACTIVEMQ_ADDRESS>"
  port = <INSERT_ACTIVEMQ_PORT>
```

- 2 Replace <INSERT_ACTIVEMQ_ADDRESS> with the applicable ActiveMQ server address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT_ACTIVEMQ_PORT> with the applicable ActiveMQ server HTTP port.
- 4 Replace <INSERT_ACTIVEMQ_USERNAME> and <INSERT_ACTIVEMQ_PASSWORD> with the applicable ActiveMQ credentials.
- 5 Modify 'webadmin' if needed (if ActiveMQ server changes web admin root path).
- 6 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 7 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Setup (Configurazione)

Le informazioni sono disponibili in ["Documentazione ActiveMQ"](#)

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

Apache Data Collector

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

Prerequisiti

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

Installazione

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

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

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



Apache Configuration

Gathers Apache metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Ensure that the Apache HTTP Server system you're going to gather metrics on has the 'mod_status' module enabled and exposed. For details refer to the following document.
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-apache.conf file.

```
[[inputs.apache]]
  ## An array of URLs to gather from, must be directed at the machine
  ## readable version of the mod_status page including the auto query string.
  ## USER-ACTION: Provide address of apache server, port for apache server, confirm path for
  server-status.
  ## Please specify actual machine IP address and provide full path to localhost address if -
```

- 3 Replace <INSERT_APACHE_ADDRESS> with the applicable Apache server address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_APACHE_PORT> with the applicable Apache server port.
- 5 Modify the '/server-status' path in accordance to the Apache server configuration.
- 6 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup (Configurazione)

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

Compatibilità:

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

Abilitazione mod_status:

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

- Modulo di abilitazione
- Esposizione delle statistiche dal modulo

Modulo di abilitazione:

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

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

Esposizione delle statistiche dal modulo:

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

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

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

Per istruzioni dettagliate sul modulo 'mod_status', vedere la ["Documentazione di Apache"](#)

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

Consul Data Collector

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

Installazione

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

Se non è stato configurato un agente per il ritiro, viene richiesto di selezionare ["installare un agente"](#) il locatario.

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

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

raccolta dei dati.

Setup (Configurazione)

Le informazioni sono disponibili nella "[Documentazione di Consul](#)".

Oggetti e contatori per console

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "[Supporto](#)" pagina .

Couchbase Data Collector

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

Installazione

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

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



Couchbase Configuration

Gathers Couchbase metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-couchbase.conf file.

```
## Read metrics from one or many couchbase clusters
[[inputs.couchbase]]
  ## specify servers via a url matching:
  ## [protocol://][:password]@address[:port]
  ## e.g.
  ## http://username:password@127.0.0.1:8090
```

- 2 Replace <INSERT_USERNAME> and <INSERT_PASSWORD> with couchbase server account credentials.
- 3 Replace <INSERT_COUCHBASE_ADDRESS> with the applicable Couchbase address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_COUCHBASE_PORT> with the applicable Couchbase port.
- 5 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Setup (Configurazione)

Le informazioni sono disponibili nella "[Documentazione di Couchbase](#)".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

Data Collector di CouchDB

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

Installazione

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

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



CouchDB Configuration

Gathers CouchDB metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-couchdb.conf file.

```
## Read CouchDB Stats from one or more servers
[[inputs.couchdb]]
  ## Works with CouchDB stats endpoints out of the box
  ## Multiple Hosts from which to read CouchDB stats:
  ## USER-ACTION: Provide comma-separated list of couchdb IP(s) and port(s).
  ## USER-ACTION: Multiple Hosts from which to read CouchDB stats:
  ## USER-ACTION: Provide comma-separated list of couchdb IP(s) and port(s).
```

- 2 Replace <INSERT_COUCHDB_ADDRESS> with the applicable CouchDB address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT_COUCHDB_PORT> with the applicable CouchDB port.
- 4 Modify the URL if CouchDB monitoring is exposed at different path
- 5 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup (Configurazione)

Le informazioni sono disponibili nella ["Documentazione di CouchDB"](#).

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

Docker Data Collector

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

Installazione

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

Se non è stato configurato un agente per il ritiro, viene richiesto di selezionare ["installare un agente"](#) il locatario.

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

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



Docker Configuration

Gathers Docker metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new `.conf` file under the `/etc/telegraf/telegraf.d/` directory. For example, copy the contents to the `/etc/telegraf/telegraf.d/cloudinsights-docker.conf` file.

```
[[inputs.docker]]
  ## Docker Endpoint
  ## To use TCP, set endpoint = "tcp://[ip]:[port]". By default, Docker uses port 2375 for
  unencrypted and 2376 for encrypted
  ## To use environment variables (ie, docker-machine), set endpoint = "ENV"
```

- 2 Replace `<INSERT_DOCKER_ENDPOINT>` with the applicable Docker endpoint.
- 3 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 4 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup (Configurazione)

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

Compatibilità

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

Configurazione

Accesso a Docker tramite un socket UNIX

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

```
sudo usermod -aG docker telegraf
```

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

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

Quindi, aggiungere quanto segue al contenitore:

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

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

Accedere a Docker tramite un endpoint TCP

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

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

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

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

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

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

Risoluzione dei problemi

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

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

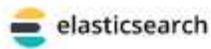
Elasticsearch Data Collector

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

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

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

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



Elasticsearch Configuration

Gathers Elasticsearch metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-elasticsearch.conf file.

```
[[inputs.elasticsearch]]
  ## USER-ACTION: Provide comma-separated list of Elasticsearch servers.
  ## Note that for scenarios in which metrics from multiple Elasticsearch clusters are being
  ## sent to Cloud Insights, the Elasticsearch cluster names must be unique.
  ## Please specify actual machine IP address, and refrain from using a loopback address
```

- 2 Replace <INSERT_ELASTICSEARCH_ADDRESS> with the applicable Elasticsearch address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT_ELASTICSEARCH_PORT> with the applicable Elasticsearch port.
- 4 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup (Configurazione)

Le informazioni sono disponibili nella "[Documentazione Elasticsearch](#)".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Oggetto:	Identificatori:	Attributi:
Nodo Elasticsearch	Namespace Cluster ES Node ID ES Node IP ES Node	ID zona

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

Flink Data Collector

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

Installazione

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

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

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



Flink Configuration

Gathers Flink metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Install Jolokia on your Flink JobManager(s) and Flink Task Manager(s). For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-flink.conf file.

```
## *****  
## JobManager  
## *****  
[[inputs.jolokia2_agent]]  
  ## USER-ACTION: Provide address(es) of flink Job Manager(s), port for jolokia, add one URL  
  ## USER-ACTION: Provide address(es) of flink Task Manager(s), port for jolokia, add one URL
```

- 3 Replace <INSERT_FLINK_JOBMANAGER_ADDRESS> with the applicable Flink Job Manager address(es). Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_FLINK_TASKMANAGER_ADDRESS> with the applicable Flink Task Manager address(es). Please specify a real machine address, and refrain from using a loopback address.
- 5 Replace <INSERT_JOLOKIA_PORT> with the applicable jolokia port.
- 6 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 7 Modify 'Cluster' if needed for Flink cluster designation.
- 8 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Setup (Configurazione)

Un'implementazione Flink completa comprende i seguenti componenti:

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

Compatibilità

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

Configurazione

Jolokia Agent Jar

Per tutti i singoli componenti, è necessario scaricare una versione del file Jar dell'agente di Jolokia. La versione testata era ["Agente di Jookia 1.6.0"](#).

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

JobManager

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

```
export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-agent.jar=port=8778,host=0.0.0.0"
```

È possibile scegliere una porta diversa per Jolokia (8778). Se si dispone di un IP interno su cui bloccare Jolokia, è possibile sostituire il "catch all" 0.0.0.0 con il proprio IP. Si noti che questo IP deve essere accessibile dal plugin telegraf.

Taskmanager

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

```
export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-agent.jar=port=8778,host=0.0.0.0"
```

È possibile scegliere una porta diversa per Jolokia (8778). Se si dispone di un IP interno su cui bloccare Jolokia, è possibile sostituire il "catch all" 0.0.0.0 con il proprio IP. Si noti che questo IP deve essere accessibile dal plugin telegraf.

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

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

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

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

Data Collector Hadoop

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

Installazione

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

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

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



Hadoop Configuration

Gathers Hadoop metrics.

What Operating System or Platform Are You Using? [Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

Need Help?

- 1 Install Jolokia on your Hadoop NameNode, Secondary NameNode, DataNode(s), ResourceManager, NodeManager(s) and JobHistoryServer. For details refer to the following [document](#).
- 2 Copy the contents below into a new `.conf` file under the `/etc/telegraf/telegraf.d/` directory. For example, copy the contents to the `/etc/telegraf/telegraf.d/cloudinsights-hadoop.conf` file.

```
#####  
# NAMENODE #  
#####  
[[inputs.jolokia2_agent]]  
  ## USER-ACTION: Provide address(es) of Hadoop NameNode, port for jolokia  
  ## Please specify real machine address(es) and refrain from using a loopback address
```

- 3 Replace `<INSERT_HADOOP_NAMENODE_ADDRESS>` with the applicable Hadoop NameNode address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding `<INSERT_JOLOKIA_PORT>` with the NameNode's assigned Jolokia port.
- 4 Replace `<INSERT_HADOOP_SECONDARYNAMENODE_ADDRESS>` with the applicable Hadoop Secondary NameNode address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding `<INSERT_JOLOKIA_PORT>` with the Secondary NameNode's assigned Jolokia port.
- 5 Replace `<INSERT_HADOOP_DATANODE_ADDRESS>` with the applicable Hadoop DataNode address(es). Please specify a real machine address, and refrain from using a loopback address. Replace corresponding `<INSERT_JOLOKIA_PORT>` with the DataNode's assigned Jolokia port.
- 6 Replace `<INSERT_HADOOP_RESOURCEMANAGER_ADDRESS>` with the applicable Hadoop ResourceManager address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding `<INSERT_JOLOKIA_PORT>` with the ResourceManager's assigned Jolokia port.
- 7 Replace `<INSERT_HADOOP_NODEMANAGER_ADDRESS>` with the applicable Hadoop NodeManager address(es). Please specify a real machine address, and refrain from using a loopback address. Replace corresponding `<INSERT_JOLOKIA_PORT>` with the NodeManager's assigned Jolokia port.
- 8 Replace `<INSERT_HADOOP_JOBHISTORYSERVER_ADDRESS>` with the applicable Hadoop Job History Server address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding `<INSERT_JOLOKIA_PORT>` with the Job History Server's assigned Jolokia port.
- 9 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 10 Modify 'Cluster' if needed for Hadoop cluster designation.
- 11 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup (Configurazione)

Un'implementazione Hadoop completa comprende i seguenti componenti:

- NameNode: Il sistema primario HDFS (Distributed file System) di Hadoop. Coordina una serie di DataNode.

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

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

Compatibilità

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

Configurazione

Jolokia Agent Jar

Per tutti i singoli componenti, è necessario scaricare una versione del file Jar dell'agente di Jolokia. La versione testata era "[Agente di Jookia 1.6.0](#)".

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

NameNode

Per configurare NameNode in modo da esporre l'API di Jookia, è possibile configurare quanto segue in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

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

Node secondario

Per configurare il nodo del nome secondario in modo che esponga l'API di Jookia, è possibile configurare quanto segue in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_SECONDARYNAMENODE_OPTS="$HADOOP_SECONDARYNAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7802,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8002
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
```

You can choose a different port for JMX (8002 above) and Jolokia (7802). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

DataNode

Per configurare i DataNode in modo che esponano l'API di Jolokia, è possibile configurare quanto segue in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_DATANODE_OPTS="$HADOOP_DATANODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7801,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8001
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
```

You can choose a different port for JMX (8001 above) and Jolokia (7801). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

ResourceManager

Per configurare ResourceManager in modo da esporre l'API di Jolokia, è possibile configurare quanto segue in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export YARN_RESOURCEMANAGER_OPTS="$YARN_RESOURCEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7803,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8003
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
```

You can choose a different port for JMX (8003 above) and Jolokia (7803). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

NodeManager

Per configurare i NodeManager in modo che esponano l'API di Jookia, è possibile configurare quanto segue in `<HADOOP_HOME>/etc/hadoop/hadoop-env.sh`:

```
export YARN_NODEMANAGER_OPTS="$YARN_NODEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7804,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8004
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
```

You can choose a different port for JMX (8004 above) and Jolokia (7804). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

Server JobHistory

Per configurare il server di StoriaLavoro in modo che esponga l'API di Jookia, è possibile configurare quanto segue in `<HADOOP_HOME>/etc/hadoop/hadoop-env.sh`:

```
export HADOOP_JOB_HISTORYSERVER_OPTS="$HADOOP_JOB_HISTORYSERVER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7805,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8005
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
```

You can choose a different port for JMX (8005 above) and Jolokia (7805). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

HAProxy Data Collector

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

Installazione

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

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

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



HAProxy Configuration

Gathers HAProxy metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Ensure that the HAProxy system you're going to gather metrics on has 'stats enable' option. For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-haproxy.conf file.

```
# Read metrics of HAProxy, via socket or HTTP stats page
[[inputs.haproxy]]
  ## An array of address to gather stats about. Specify an ip on hostname
  ## with optional port. ie localhost, 10.10.3.33:1936, etc.
  ## Make sure you specify the complete path to the stats endpoint
  ## <url> for the endpoint? ie http://10.10.3.33:1936/haproxy?stats
```

- 3 Replace <INSERT_HAPROXY_ADDRESS> with the applicable HAProxy server address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_HAPROXY_PORT> with the applicable HAProxy server port.
- 5 Modify the 'haproxy?stats' path in accordance to the HAProxy server configuration.
- 6 Modify 'username' and 'password' in accordance to the HAProxy server configuration (if credentials are required).
- 7 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 8 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup (Configurazione)

Il plug-in di Telegraf per HAProxy si basa sull'abilitazione delle statistiche HAProxy. Si tratta di una configurazione integrata in HAProxy, ma non è attivata subito. Se attivato, HAProxy espone un endpoint HTML

che può essere visualizzato sul browser o scartato per l'estrazione dello stato di tutte le configurazioni HAProxy.

Compatibilità:

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

Configurazione:

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

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

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

```
global
  daemon
  maxconn 256

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

frontend http-in
  bind *:80
  default_backend servers

frontend http-in9080
  bind *:9080
  default_backend servers_2

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

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

Per istruzioni complete e aggiornate, vedere la "[Documentazione HAProxy](#)".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

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

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

Data Collector JVM

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

Installazione

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

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

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

dell'agente" istruzioni.

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



Java Configuration
Gathers JVM metrics.

What Operating System or Platform Are You Using? [Need Help?](#)

RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in your environment before configuring. [Show Instructions](#)

Follow Configuration Steps [Need Help?](#)

- 1 Install Jolokia on your JVMs. For details refer to the following [document](#).
- 2 Copy the contents below into a new `.conf` file under the `/etc/telegraf/telegraf.d/` directory. For example, copy the contents to the `/etc/telegraf/telegraf.d/cloudinsights-jvm.conf` file.

```
# Read JMX metrics through Jolokia
[[inputs.jolokia2_agent]]
  # USER-ACTION: Provide address(es) of JVM, port for jolokia, add one URL for each JVM in
  your cluster
  # Please specify actual machine IP address, and refrain from using a loopback address (i.e.
  10.1.1.1 or 127.0.0.1)
```
- 3 Replace `<INSERT_JVM_ADDRESS>` with the applicable JVM address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace `<INSERT_JOLOKIA_PORT>` with the applicable JVM jolokia port.
- 5 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 6 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup (Configurazione)

Le informazioni sono disponibili in ["Documentazione JVM"](#).

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

Data Collector Kafka

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

Installazione

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

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

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



Kafka Configuration

Gathers Kafka metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Install Jolokia on your Kafka brokers. For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-kafka.conf file.

```
# Read JMX metrics through Jolokia
[[inputs.jolokia2_agent]]
  ## USER-ACTION: Provide address(es) of kafka broker(s), port for jolokia, add one URL for
  ## each broker in your cluster
  ## Please specify actual machine IP address, and refrain from using a loopback address (i.e.
  ## 192.168.1.1 or 127.0.0.1)
```

- 3 Replace <INSERT_KAFKA_BROKER_ADDRESS> with the applicable Kafka broker address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_JOLOKIA_PORT> with the applicable Kafka broker jolokia port.
- 5 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 6 Modify 'Cluster' if needed for Kafka cluster designation.
- 7 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Setup (Configurazione)

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

Compatibilità

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

Configurazione

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

Jolokia Agent Jar

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

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

Kafka Brokers

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

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

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

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

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella "[Supporto](#)" pagina .

Kibana Data Collector

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

Installazione

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

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

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



Kibana Configuration

Gathers Kibana metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new `.conf` file under the `/etc/telegraf/telegraf.d/` directory. For example, copy the contents to the `/etc/telegraf/telegraf.d/cloudinsights-kibana.conf` file.

```
[[inputs.kibana]]
  ## specify a list of one or more Kibana servers
  ## USER-ACTION: Provide address of kibana server(s), port(s) for kibana server
  ## Please specify actual machine IP address, and refrain from using a loopback address (i.e.
  localhost or 127.0.0.1).
```

- 2 Replace `<INSERT_KIBANA_ADDRESS>` with the applicable Kibana server address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace `<INSERT_KIBANA_PORT>` with the applicable Kibana server port.
- 4 Replace `'username'` and `'pa$$word'` with the applicable Kibana server authentication credentials as needed, and uncomment the lines.
- 5 Modify `'Namespace'` if needed for server disambiguation (to avoid name clashes).
- 6 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup (Configurazione)

Le informazioni sono disponibili nella ["Documentazione di Kibana"](#).

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

Installazione e configurazione dell'operatore di monitoraggio Kubernetes

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

Prima di installare l'operatore di monitoraggio Kubernetes

Consultare la ["Prerequisiti"](#) documentazione prima di installare o aggiornare Kubernetes Monitoring Operator.

Installazione dell'operatore di monitoraggio Kubernetes

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.

3 Optional: Upload the operator images to your private repository

By default, the operator pulls container images from the Cloud Insights repository. To use a private repository, download the required images using the Image Pull command. Then upload them to your private repository maintaining the same tags and directory structure. Finally, update the image paths in `operator-deployment.yaml` and the docker repository settings in `operator-config.yaml`. For more information review [the documentation](#).

Copy Image Pull Snippet

Reveal Image Pull Snippet

Copy Repository Password

Reveal Repository Password

This password is valid for 24 hours.

4 Optional: Review available configuration options

Configure custom options such as proxy and private repository settings. Review the [instructions and available options](#).

5 Deploy the operator (create new or upgrade existing)

Execute the `kubectl` snippet to apply the following operator YAML files.

- `operator-setup.yaml` - Create the operator's dependencies.
- `operator-secrets.yaml` - Create secrets holding your API key.
- `operator-deployment.yaml`, `operator-cr.yaml` - Deploy the NetApp Kubernetes Monitoring Operator.
- `operator-config.yaml` - Apply the configuration settings if not already present.

Copy kubectl Apply Snippet

Reveal kubectl Apply Snippet

After deploying the operator, **delete or securely store `operator-secrets.yaml`**.

6 Next

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

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

Se si utilizza un proxy, consultare informazioni su [configurazione del proxy](#).

Se si dispone di un repository personalizzato, consultare informazioni su [utilizzando un repository di docker personalizzato/privato](#).

Componenti di monitoring Kubernetes

Data Infrastructure Insights Kubernetes Monitoring comprende quattro componenti di monitoring:

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

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

NetApp / Observability / Collectors

Data Collectors 21 Acquisition Units 4 **Kubernetes Collectors**

Kubernetes Collectors (13) [View Upgrade/Delete Documentation](#) [+ Kubernetes Collector](#)

Cluster Name ↑	Status	Operator Version	Network Performance and Map	Change Analysis	
au-pod	Outdated	1.1540.0	1.347.0	1.162.0	⋮
jks-troublemaker	Latest	1.1579.0	N/A	1.201.0	⋮
oom-test	Outdated	1.1555.0	N/A	1.161.0	⋮ Modify Deployment

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

kubernetes
Kubernetes

Modify Deployment

Cluster Information

Kubernetes Cluster	Network Performance and Map	Event Logs	Change Analysis
ci-demo-01	Enabled - Online	Enabled - Online	Enabled - Online

Deployment Options

[Need Help?](#)

- Network Performance and Map
- Event Logs
- Change Analysis

Aggiornamento alla versione più recente di Kubernetes Monitoring Operator

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

```
kubectl -n netapp-monitoring get agentconfiguration netapp-monitoring-configuration
```

Se esiste una configurazione AgentConfiguration:

- **Installare** L'operatore più recente rispetto all'operatore esistente.
 - Assicurarsi di [estrarre le immagini container più recenti](#) utilizzare un repository personalizzato.

Se AgentConfiguration non esiste:

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

```
kubectl -n netapp-monitoring get agent -o jsonpath='{.items[0].spec.cluster-name}'
```

* Creare un backup dell'operatore esistente (se lo spazio dei nomi non è il monitoraggio netapp predefinito, sostituire lo spazio dei nomi appropriato):

```
kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
```

* <<to-remove-the-kubernetes-monitoring-operator,Disinstallare>>
L'operatore esistente.

* <<installing-the-kubernetes-monitoring-operator,Installare>>
L'operatore più recente.

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

Arresto e avvio dell'operatore di monitoraggio Kubernetes

Per arrestare l'operatore di monitoraggio Kubernetes:

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=0
```

Per avviare l'operatore di monitoraggio Kubernetes:

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

Disinstallazione in corso

Per rimuovere l'operatore di monitoraggio Kubernetes

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

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

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

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

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

Eeguire ciascuno dei seguenti comandi nell'ordine indicato. A seconda dell'installazione corrente, alcuni di questi comandi potrebbero restituire i messaggi 'oggetto non trovato'. Questi messaggi possono essere ignorati in modo sicuro.

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

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

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

A proposito di Kube-state-metrics

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

Per informazioni su Kube-state-Metrics, vedere ["questa pagina"](#).

Configurazione/personalizzazione dell'operatore

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

Opzioni di configurazione

Le impostazioni più comunemente modificate possono essere configurate nella risorsa personalizzata *AgentConfiguration*. È possibile modificare questa risorsa prima di implementare l'operatore modificando il file *operator-config.yaml*. Questo file include esempi di impostazioni commentate. Vedere l'elenco di ["impostazioni disponibili"](#) per la versione più recente dell'operatore.

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

```
kubectl -n netapp-monitoring edit AgentConfiguration
```

Per determinare se la versione implementata dell'operatore supporta *AgentConfiguration*, eseguire il seguente comando:

```
kubectl get crd agentconfigurations.monitoring.netapp.com
```

Se viene visualizzato il messaggio "Error from server (notfound)" (errore dal server (non trovato)), l'operatore deve essere aggiornato prima di poter utilizzare *AgentConfiguration*.

Configurazione del supporto proxy

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

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

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

correttamente.

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

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

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

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

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

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

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

```

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

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

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

```

Utilizzando un repository di docker personalizzato o privato

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

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

Funzionalità principale dell'operatore e monitoraggio Kubernetes

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

Registro eventi

- ci-fluent-bit

- ci-kukasub-esportatore-di-eventi

Mappa e performance di rete

- ci-net-osservatore

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

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

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

Modificare la configurazione dell'agente in `operator-config.yaml` in modo che rifletta la nuova posizione del responsabile del docker. Crea un nuovo `imagePullSecret` per il tuo repository privato, per maggiori dettagli vedi <https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/>

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

Istruzioni per OpenShift

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

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

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

Tollerazioni e contami

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

Scopri di più su Kubernetes "[Contami e pedaggi](#)".

Tornare al "[Pagina Installazione dell'operatore di monitoraggio NetApp Kubernetes](#)"

Una nota sui segreti

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

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

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

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

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

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

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

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

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

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

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

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

Risoluzione dei problemi

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

Problema:	Prova:
Non viene visualizzato un collegamento ipertestuale/connessione tra il volume persistente Kubernetes e il dispositivo di storage back-end corrispondente. Il volume persistente Kubernetes viene configurato utilizzando il nome host del server di storage.	Seguire la procedura per disinstallare l'agente Telegraf esistente, quindi reinstallare l'agente Telegraf più recente. Devi utilizzare Telegraf versione 2,0 o successiva e lo storage del cluster Kubernetes deve essere monitorato attivamente da Data Infrastructure Insights.

Problema:	Prova:
<p>Su Kubernetes, il mio pod ReplicaSet Telegraf riporta il seguente errore: [inputs.prometheus] errore nel plugin: Impossibile caricare la coppia di chiavi /etc/kubernetes/pki/etcd/server.crt:/etc/kubernetes/pki/etcd/server.key: Aprire /etc/kubernetes/pki/etcd/server.no</p>	<p>Il pod ReplicaSet di Telegraf è destinato all'esecuzione su un nodo designato come master o etcd. Se il pod ReplicaSet non è in esecuzione su uno di questi nodi, si otterranno questi errori. Verificare se i nodi master/etcd presentano delle contaminazioni. In tal caso, aggiungere le tolleranze necessarie a Telegraf ReplicaSet, telegraf-rs. Ad esempio, modificare il Replica Set... kubectl edit rs telegraf-rs ...e aggiunga le tolleranze appropriate alla specifica. Quindi, riavviare il pod ReplicaSet.</p>
<p>Ho un ambiente PSP/PSA. Questo influisce sul mio operatore di monitoraggio?</p>	<p>Se il cluster Kubernetes è in esecuzione con Pod Security Policy (PSP) o Pod Security Admission (PSA), è necessario eseguire l'aggiornamento all'ultima versione di Kubernetes Monitoring Operator. Per eseguire l'aggiornamento all'operatore corrente con il supporto per PSP/PSA, procedere come segue: 1. Disinstallare l'operatore di monitoraggio precedente: kubectl delete agent-monitoring-NetApp -n NetApp-monitoring kubectl delete ns NetApp-monitoring kubectl delete crd agents.monitoring.NetApp.com kubectl delete clusterrole agent-manager-ruolo-proxy agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-rolebinding-proxy-ading-cluster-2. Installare la versione più recente dell'operatore di monitoraggio.</p>
<p>Ho riscontrato dei problemi durante la distribuzione dell'operatore e ho utilizzato PSP/PSA.</p>	<p>1. Modificare l'agente usando il seguente comando: Kubectl -n <name-space> edit Agent 2. Contrassegna "Security-policy-enabled" come "false". In questo modo si disattivano i criteri di protezione del pod e l'ammissione alla protezione del pod e si consente all'operatore di eseguire la distribuzione. Confermare con i seguenti comandi: Kubectl Get psp (dovrebbe mostrare la politica di sicurezza Pod rimossa) kubectl Get all -n <namespace></p>
<p>grep -i psp (dovrebbe mostrare che non viene trovato nulla)</p>	<p>Errori "ImagePullBackoff" rilevati</p>
<p>Questi errori possono essere rilevati se si dispone di un repository di docker personalizzato o privato e non è ancora stato configurato l'operatore di monitoraggio Kubernetes in modo da riconoscerlo correttamente. Scopri di più informazioni sulla configurazione per repo personalizzato/privato.</p>	<p>Si verifica un problema con l'implementazione dell'operatore di monitoraggio e la documentazione corrente non mi aiuta a risolverlo.</p>

Problema:	Prova:
<p>Acquisire o annotare in altro modo l'output dei seguenti comandi e contattare il team di supporto tecnico.</p> <pre data-bbox="131 296 808 751"> kubect1 -n netapp-monitoring get all kubect1 -n netapp-monitoring describe all kubect1 -n netapp-monitoring logs <monitoring-operator-pod> --all -containers=true kubect1 -n netapp-monitoring logs <telegraf-pod> --all -containers=true </pre>	<p>I pod Net-observer (mappa del carico di lavoro) nello spazio dei nomi Operator si trovano in CrashLoopBackOff</p>
<p>Questi pod corrispondono al data collector Workload Map per l'osservabilità della rete. Prova: • Verifica i log di uno dei pod per confermare la versione minima del kernel. Ad esempio: --- {"ci-tenant-id":"your-tenant-id","collector-cluster":"your-k8s-cluster-name","ambiente":"prod","level":"error","msg":"failed in validation. Motivo: La versione del kernel 3.10.0 è inferiore alla versione minima del kernel di 4.18.0","Time":"2022-11-09T08:23:08Z"} --- • i pod Net-Observer richiedono che la versione del kernel Linux sia almeno 4.18.0. Controllare la versione del kernel usando il comando "uname -r" e assicurarsi che siano >= 4.18.0</p>	<p>I pod vengono eseguiti in Operator namespace (predefinito: Monitoring netapp), ma non vengono visualizzati dati nell'interfaccia utente per la mappa dei carichi di lavoro o le metriche Kubernetes nelle query</p>
<p>Controllare l'impostazione dell'ora sui nodi del cluster K8S. Per un controllo accurato e la creazione di report dei dati, si consiglia di sincronizzare l'ora sul computer dell'agente utilizzando il protocollo NTP (Network Time Protocol) o SNTP (Simple Network Time Protocol).</p>	<p>Alcuni dei pod net-observer nello spazio dei nomi Operator sono in stato Pending</p>
<p>NET-osservatore è un DemonSet che esegue un pod in ogni nodo del cluster k8s. • Prendere nota del pod in stato Pending (in sospeso) e verificare se si verifica un problema di risorse per la CPU o la memoria. Assicurarsi che la memoria e la CPU richieste siano disponibili nel nodo.</p>	<p>Nei miei registri, subito dopo l'installazione dell'operatore di monitoraggio di Kubernetes, viene visualizzato quanto segue: [inputs.prometheus] errore nel plugin: Errore durante la richiesta HTTP a http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Get http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Dial tcp: Lookup kube-state-metrics.<namespace>.svc.cluster.local: No such host</p>

Problema:	Prova:
<p>Questo messaggio viene visualizzato in genere solo quando viene installato un nuovo operatore e il pod <i>telegraf-rs</i> è attivo prima che il pod <i>ksm</i> sia attivo. Questi messaggi dovrebbero interrompersi una volta che tutti i pod sono in esecuzione.</p>	<p>Non vedo alcuna metrica raccolta per Kubernetes Cronjobs che esiste nel mio cluster.</p>
<p>Verificare la versione di Kubernetes (ad es. <code>kubectl version</code>). Se è v1.20.x o inferiore, si tratta di un limite previsto. La release kube-state-metrics implementata con Kubernetes Monitoring Operator supporta solo v1.cronjob. Con Kubernetes 1.20.x e versioni precedenti, la risorsa cronjob è v1beta.cronjob. Di conseguenza, le metriche dello stato del kube non riescono a trovare la risorsa di crono-job.</p>	<p>Dopo aver installato l'operatore, i pod telegraf-ds entrano in CrashLoopBackOff e i registri del pod indicano "su: Authentication failure" (su: Errore di autenticazione).</p>
<p>Modificare la sezione telegraf in <i>AgentConfiguration</i> e impostare <i>dockerMetricCollectionEnabled</i> su false. Per ulteriori dettagli, fare riferimento alla "opzioni di configurazione". telegraf: ... - Name: docker run-mode: - DaemonSet sostituzioni: - Chiave: DOCKER_UNIX_SOCKET_PLACEHOLDER valore: unix://run/docker.sock</p>	<p>Vedo messaggi di errore ricorrenti simili ai seguenti nei miei registri Telegraf: E! [Agent] errore di scrittura in outputs.http: Post "https://<tenant_url>/REST/v1/Lake/ingerment/influenzxdb": Scadenza contesto superata (client. Timeout durante l'attesa delle intestazioni)</p>
<p>Modificare la sezione telegraf in <i>AgentConfiguration</i> e aumentare <i>outputTimeout</i> a 10s. Per ulteriori dettagli, fare riferimento alla "opzioni di configurazione".</p>	<p>Mancano i dati <i>involvedobject</i> per alcuni registri eventi.</p>
<p>Assicurarsi di aver seguito i passaggi descritti nella "Permessi" sezione precedente.</p>	<p>Perché vedo due pod operatore di monitoring in esecuzione, uno denominato netapp-ci-monitoring-operator-<pod> e l'altro denominato monitoring-operator-<pod>?</p>
<p>A partire dal 12 ottobre 2023, Data Infrastructure Insights ha ridefinito l'operatore per servire meglio i nostri utenti; affinché tali modifiche vengano completamente adottate, è necessario rimuovere il vecchio operatore e installare il nuovo.</p>	<p>I miei eventi kuowdi hanno interrotto inaspettatamente la segnalazione a Data Infrastructure Insights.</p>
<p>Recuperare il nome del pod dell'esportatore di eventi:</p> <pre> `kubectl -n netapp-monitoring get pods </pre>	<p>grep event-exporter</p>

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

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

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina o nella ["Matrice di supporto Data Collector"](#).

Data Collector Memcached

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

Installazione

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

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

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



Memcached Configuration

Gathers Memcached metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-memcached.conf file.

```
[[inputs.memcached]]
  ## USER-ACTION: Provide comma-separated list of Memcached IP(s) and port(s).
  ## Please specify actual machine IP address, and refrain from using a loopback address
  ## (i.e. localhost or 127.0.0.1).
  ## When configuring with multiple Memcached servers, enter them in the format ["server1"
```

- 2 Replace <INSERT_MEMCACHED_ADDRESS> with the applicable Memcached server address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT_MEMCACHED_PORT> with the applicable Memcached server port.
- 4 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Setup (Configurazione)

Le informazioni sono disponibili nella ["Wiki Memcached"](#).

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

MongoDB Data Collector

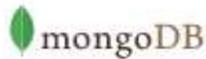
Data Infrastructure Insights utilizza questo data collector per raccogliere metriche da MongoDB.

Installazione

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

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

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



MongoDB Configuration

Gathers MongoDB metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Open mongod.conf. Locate the line beginning with "bindIp", and append the address of the node on which the Telegraf agent resides. After saving the change, restart the MongoDB server.
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-mongodb.conf file.

```
[[inputs.mongodb]]
  ## An array of URLs of the form:
  ## "mongodb://" [user ":" pass "@"] host [ ":" port]
  ## For example:
  ## mongodb://user:auth_key@10.10.3.30:27017,
  ## mongodb://10.10.0.0:27017
```

- 3 Replace <INSERT_MONGODB_ADDRESS> with the applicable MongoDB server address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_MONGODB_PORT> with the applicable MongoDB port.
- 5 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup (Configurazione)

Le informazioni sono disponibili nella ["Documentazione MongoDB"](#).

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Le informazioni sono disponibili nella ["Supporto"](#) pagina .

MySQL Data Collector

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

Installazione

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

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

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



MySQL Configuration

Gathers MySQL metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-mysql.conf file.

```
[[inputs.mysql]]
  ## USER-ACTION: Provide comma-separated list of MySQL credentials, IP(s), and port(s)
  ## e.g. servers = ["user:passwd@tcp(127.0.0.1:3306)?tls=false"]
  ## Please specify actual machine IP address, and refrain from using a loopback address
  (i.e. localhost or 127.0.0.1).
```

- 2 Review and verify the contents of the configuration file.
- 3 Replace <INSERT_USERNAME> and <INSERT_PASSWORD> with the applicable MySQL credentials.
- 4 Replace <INSERT_PROTOCOL> with the applicable MySQL connection protocol. The typical protocol is tcp.
- 5 Replace <INSERT_MYSQL_ADDRESS> with the applicable MySQL server address. Please specify a real machine address, and refrain from using a loopback address.
- 6 Replace <INSERT_MYSQL_PORT> with the applicable MySQL server port. The typical port is 3306.
- 7 Modify the 'tls' parameter in accordance to the MySQL server configuration.
- 8 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Setup (Configurazione)

Le informazioni sono disponibili nella ["Documentazione MySQL"](#).

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

Netstat Data Collector

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

Installazione

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

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

netstat

Netstat Configuration

Gathers netstat metrics of the host where telegraf agent is installed.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows
▼

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)
▼

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1

Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-netstat.conf file.

```
# Read TCP metrics such as established, time wait and sockets counts.
[[inputs.netstat]]
# no configuration
[inputs.netstat.tags]
  CloudInsights = "true"
```
- 2

Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Setup (Configurazione)

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

Data Collector nginx

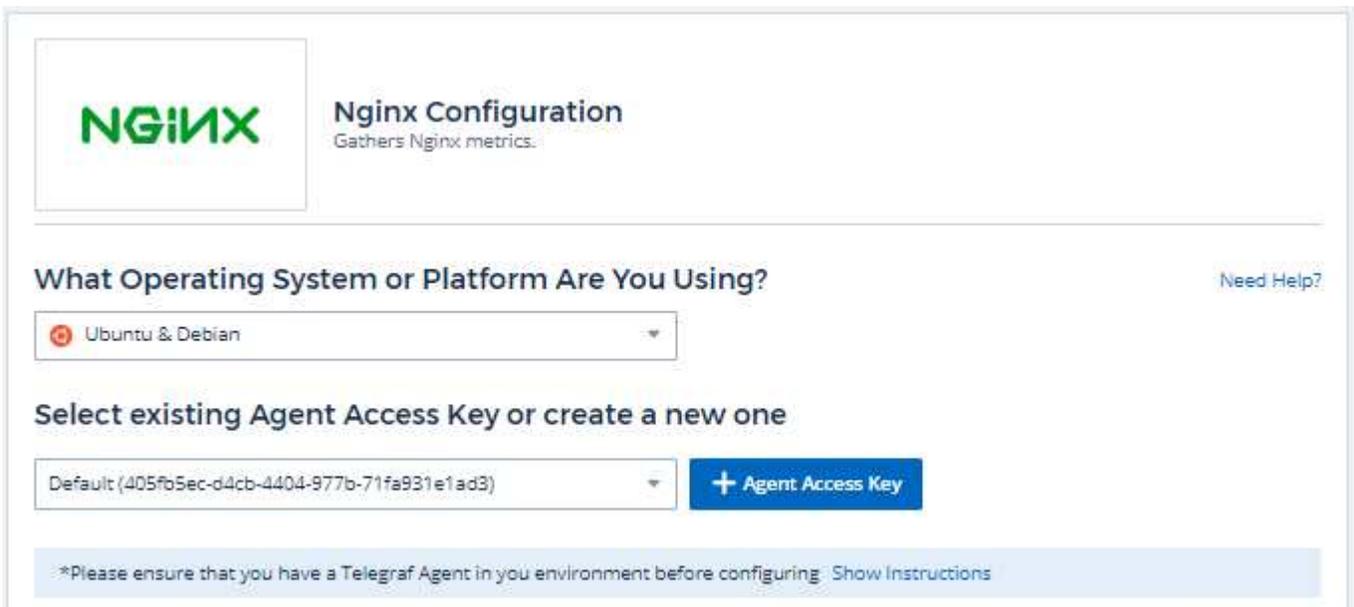
Data Infrastructure Insights utilizza questo data collector per raccogliere le metriche da Nginx.

Installazione

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

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

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



NGINX Nginx Configuration
Gathers Nginx metrics.

What Operating System or Platform Are You Using? [Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

1 If you already have a URL enabled to provide Nginx metrics, go directly to the plugin configuration.

2 Nginx metrics are available through a status page when the HTTP stub status module is enabled. Refer to the below link for verifying/enabling `http_stub_status_module`.

```
http://nginx.org/en/docs/http/nginx_http_stub_status_module.html
```

3 After verifying the module is enabled, modify the Nginx configuration to set up a locally-accessible URL for the status page:

```
server {
    listen    <PORT NUMBER>;
    Please specify actual machine IP address, and refrain from using a loopback address (i.e.
    localhost or 127.0.0.1)
    server_name <IP ADDRESS>;
    location /nginx_status {
        stub_status on;
    }
}
```

4 Reload the configuration:

```
nginx -s reload
```

5 Copy the contents below into a new `.conf` file under the `/etc/telegraf/telegraf.d/` directory. For example, copy the contents to the `/etc/telegraf/telegraf.d/cloudinsights-nginx.conf` file.

```
[[inputs.nginx]]
  ## USER-ACTION: Provide Nginx status url
  ## Please specify actual machine IP address where nginx_status is enabled, and refrain from
  ## using a loopback address (i.e. localhost or 127.0.0.1).
  ## When configuring with multiple Nginx servers, enter them in the format ["url1", "url2",
  ## ...]
```

6 Replace `<INSERT_NGINX_ADDRESS>` with the applicable Nginx address. Please specify a real machine address, and refrain from using a loopback address.

7 Replace `<INSERT_NGINX_PORT>` with the applicable Nginx port.

8 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup (Configurazione)

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

Ulteriori informazioni sono disponibili nella "[Documentazione nginx](#)".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

PostgreSQL Data Collector

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

Installazione

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



PostgreSQL Configuration

Gathers PostgreSQL metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-postgresql.conf file.

```
[[inputs.postgresql]]
# USER-ACTION: Provide credentials for access, address of PostgreSQL server, port for
PostgreSQL server, one DB for access
address = "postgres://<INSERT_USERNAME>:<INSERT_PASSWORD>@<INSERT_POSTGRESQL_ADDRESS>:
<INSERT_POSTGRESQL_PORT>/<INSERT_DB>"
```

- 2 Replace <INSERT_USERNAME> and <INSERT_PASSWORD> with the applicable PostgreSQL credentials.
- 3 Replace <INSERT_POSTGRESQL_ADDRESS> with the applicable PostgreSQL address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT_POSTGRESQL_PORT> with the applicable PostgreSQL port.
- 5 Replace <INSERT_DB> with the applicable PostgreSQL database.
- 6 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 7 Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup (Configurazione)

Le informazioni sono disponibili nella "[Documentazione PostgreSQL](#)".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

Puppet Agent Data Collector

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

Installazione

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

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

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



Puppet Agent Configuration

Gathers Puppet agent metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-puppetagent.conf file.

```
## Reads last_run_summary.yaml file and converts to measurements
[[inputs.puppetagent]]
  ## Location of puppet last run summary file
  ## USER-ACTION: Modify the location if last_run_summary.yaml is on different path
  location = "/var/lib/puppet/state/last_run_summary.yaml"
```

- 2 Modify 'location' if last_run_summary.yaml is on different path
- 3 Modify 'Namespace' if needed for puppet agent disambiguation (to avoid name clashes).
- 4 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Setup (Configurazione)

Le informazioni sono disponibili in "[Documentazione delle marionette](#)"

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
----------	-----------------	------------	-------------

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

Redis Data Collector

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

Installazione

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

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

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



Redis Configuration

Gathers Redis metrics.

What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

Follow Configuration Steps

[Need Help?](#)

- 1 Configure Redis to accept connections from the address of the node on which the Telegraf agent resides. Open the Redis configuration file.

```
vi /etc/redis.conf
```

- 2 Locate the line that begins with 'bind 127.0.0.1', and append the address of the node on which the Telegraf agent resides

```
bind 127.0.0.1 <NODE_IP_ADDRESS>
```

- 3 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-redis.conf file.

```
# Read metrics from one or many redis servers
[[inputs.redis]]
  ## specify servers via a url matching:
  ## [protocol://][:password]@address[:port]
  ## e.g.
  ## http://127.0.0.1:6379
```

- 4 Replace <INSERT_REDIS_ADDRESS> with the applicable Redis address. Please specify a real machine address, and refrain from using a loopback address.

- 5 Replace <INSERT_REDIS_PORT> with the applicable Redis port.

- 6 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Setup (Configurazione)

Le informazioni sono disponibili nella "[Documentazione Redis](#)".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

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

Risoluzione dei problemi

Ulteriori informazioni sono disponibili nella ["Supporto"](#) pagina .

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.