



Referencia de recopilador de datos - Servicios

Data Infrastructure Insights

NetApp
December 19, 2024

Tabla de contenidos

- Referencia de recopilador de datos - Servicios 1
 - Recopilación de datos de nodo 1
 - Recopilador de datos ActiveMQ 3
 - Recopilador de datos Apache 5
 - Cónsul colector de datos 8
 - Recopilador de datos de Couchbase 9
 - CouchDB Collector datos 11
 - Recopilador de datos de Docker 13
 - Recopilador de datos de Elasticsearch 21
 - Colector de datos Flink 23
 - Recopilador de datos de Hadoop 30
 - Recopilador de datos de HAProxy 35
 - Recopilador de datos JVM 41
 - Recopilador de datos Kafka 46
 - Recopilador de datos de Kibana 49
 - Instalación y configuración del operador de supervisión de Kubernetes 51
 - Recopilador de datos en caché 69
 - Recopilador de datos MongoDB 73
 - Recopilador de datos de MySQL 75
 - Recopilador de datos de netstat 80
 - Recopilador de datos nginx 81
 - Recopilador de datos PostgreSQL 84
 - Recopilador de datos de Puppet Agent 86
 - Recopilador de datos Redis 88

Referencia de recopilador de datos - Servicios

Recopilación de datos de nodo

Data Infrastructure Insights recopila métricas del nodo en el que se instala un agente.

Instalación

1. En **Observabilidad > Colectores**, elige un sistema operativo/plataforma. Tenga en cuenta que instalar cualquier recopilador de datos de integración (Kubernetes, Docker, Apache, etc.) también configurará la recogida de datos de nodos.
2. Siga las instrucciones para configurar el agente. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.

Objetos y contadores

Los objetos siguientes y sus contadores se recopilan como métricas Node:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Sistema de archivos de nodos	Tipo de ruta de dispositivo de UUID de nodo	Nodo IP nodo Nombre nodo modo de sistema operativo nodo	Inodos libres inodos total inodos usados total usado total usado
Disco de nodo	Disco UUID de nodo	Nodo IP nodo Nombre nodo SO nodo	Tiempo de I/o IOPS total en curso bytes de lectura (por segundo) tiempo de lectura total de lecturas (por segundo) tiempo de I/o ponderado total de bytes de escritura (por segundo) tiempo de escritura total de escrituras (por segundo) tiempo de I/o de lectura actual duración de la cola de disco tiempo de escritura tiempo de I/O.
CPU de nodo	CPU UUID de nodo	Nodo IP nodo Nombre nodo SO nodo	Uso de CPU del sistema uso de CPU de usuario uso de CPU inactivo procesador uso de CPU interrupción uso de CPU uso de DPC uso de CPU

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Nodo	UUID de nodo	Nodo IP nodo Nombre nodo SO nodo	Switches de contexto de kernel de tiempo de arranque del kernel (por segundo) interrupciones de kernel disponibles (por segundo) procesos de kernel Forked (por segundo) Memoria activa memoria total disponible memoria en búfer memoria memoria caché memoria caché memoria caché límite de confirmación memoria comprometida como memoria sucia memoria libre memoria alta memoria total alta memoria enorme tamaño de página memoria enorme memoria libre Páginas enormes memoria total memoria baja memoria total memoria baja memoria asignada total memoria tablas de páginas de memoria asignada total baja memoria Memoria compartida Slab Memory Swap memoria caché intercambio memoria en caché memoria libre intercambio memoria total memoria total utilizada memoria total memoria utilizada memoria utilizada memoria Vmalloc memoria Vmalloc memoria usada memoria cableada Writeback memoria total Writeback tmp fallos memoria caché tmp memoria demanda cero fallos memoria memoria memoria páginas memoria Memoria no paginada caché de memoria caché de núcleo memoria caché de espera memoria normal memoria en espera Reserva de memoria errores de transición de memoria

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Red de nodos	UUID de nodo de interfaz de red	Nombre del nodo IP nodo SO del nodo	Bytes recibidos bytes enviados paquetes Outboud descartados paquetes Outboud errores recibidos paquetes descartados errores recibidos paquetes recibidos paquetes enviados

Configuración

La información de configuración y solución de problemas se puede encontrar en "[Configuración de un agente](#)" la página.

Recopilador de datos ActiveMQ

Data Infrastructure Insights usa este recopilador de datos para recopilar métricas de ActiveMQ.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Seleccione ActiveMQ.
 Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.
2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las "[Instalación del agente](#)" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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
```

Configuración

Puede encontrar información en la "[Documentación de ActiveMQ](#)"

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Cola ActiveMQ	Servidor de puertos de cola de espacio de nombres	UUID de nodo IP nodo de nombre	Recuento de consumidor Dequeue recuento de colas Tamaño de cola de cola
Suscriptor de ActiveMQ	ID de cliente Identificador de conexión espacio de nombres de servidor de puerto	Es Active Destination Node Name IP Node UUID de nodo OS Selector de SO de nodo	Recuento de colas recuento de colas enviado Tamaño de cola enviado recuento de colas pendientes Tamaño de cola pendiente
Tema ActiveMQ	Espacio de nombres de servidor de puerto de tema	Nombre de nodo IP nodo UUID de nodo operativo	Recuento de consumidor Tamaño de recuento de colas de entrada

Resolución de problemas

Puede encontrar información adicional en la "[Soporte técnico](#)" página.

Recopilador de datos Apache

Este recopilador de datos permite la recopilación de datos de los servidores Apache en su inquilino.

Requisitos previos

- Debe tener su servidor Apache HTTP configurado y funcionando correctamente
- Debe tener permisos sudo o de administrador en el host/máquina virtual del agente
- Normalmente, el módulo Apache *mod_status* se configura para exponer una página en la ubicación `/Server-status?auto` del servidor Apache. La opción *ExtendedStatus* debe estar habilitada para poder recopilar todos los campos disponibles. Para obtener información sobre cómo configurar el servidor, consulte la documentación del módulo Apache: https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Elija Apache.

Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las "[Instalación del agente](#)" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores

de datos, por ejemplo, por sistema operativo/plataforma.

4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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 refrain from using a loopback address. If a
```
- 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
```

Configuración

El complemento de Telegraf para el servidor HTTP de Apache se basa en el módulo 'mod_status' para activarlo. Cuando esto está habilitado, el servidor HTTP de Apache expondrá un punto final HTML que se

puede ver en el explorador o se puede raspar para extraer el estado de toda la configuración del servidor HTTP de Apache.

Compatibilidad:

La configuración se desarrolló contra Apache HTTP Server versión 2.4.38.

Habilitar mod_status:

La activación y exposición de los módulos 'mod_status' implica dos pasos:

- Módulo de activación
- Exposición de las estadísticas del módulo

Módulo de activación:

La carga de módulos se controla mediante el archivo de configuración en '/usr/local/apache/conf/httpd.conf'. Edite el archivo de configuración y anule el comentario de las siguientes líneas:

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

Exposición de las estadísticas del módulo:

La exposición de 'mod_status' está controlada por el archivo de configuración bajo '/usr/local/apache2/conf/extra/httpd-info.conf'. Asegúrese de que dispone de lo siguiente en ese archivo de configuración (al menos, habrá otras directivas):

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

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

Para obtener instrucciones detalladas sobre el módulo 'od_status', consulte la ["Documentación de Apache"](#)

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Apache	Servidor de espacio de nombres	Nodo IP Nombre de nodo Puerto Padre servidor principal generación de configuración servidor principal MPM generación tiempo de actividad del servidor principal se está deteniendo	Bytes de trabajadores ocupados por bytes de solicitud por segunda CPU Children System CPU Children User CPU Load System CPU System CPU User Asynchronous Connections Closing Asynchronous Connections Writing Connections duración total per Request Idle Workers Load Average (último 1 m) Load Average (último 15 m) Load Average (últimos 5 m) Procesos solicitudes por segundo acceso total duración total total KBytes cuadro de indicadores Cerrar cuadro de indicadores DNS consultas de indicadores acabado cuadro de indicadores Limpieza en vacío cuadro de indicadores mantener activo Registro cuadro de indicadores Abrir cuadro de indicadores lectura cuadro de indicadores Enviar cuadro de indicadores iniciando cuadro de indicadores esperando

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

Cónsul colector de datos

Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Consul.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Seleccione Cónsul.

Si no ha configurado un agente para la recopilación, se le pedirá que lo haga ["instale un agente"](#) en su

inquilino.

Si ya ha configurado un agente, seleccione el sistema operativo o la plataforma adecuados y haga clic en **continuar**.

2. Siga las instrucciones de la pantalla Configuración del Cónsul para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.

Configuración

La información se puede encontrar en el "[Documentación del Cónsul](#)".

Objetos y contadores para consul

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Cónsul	Nodo del servicio de identificación de comprobación de espacio de nombres	Nodo IP nodo OS nodo UUID Nombre de nodo Nombre de servicio comprobar nombre ID de servicio Estado	Advertencia de paso crítico

Resolución de problemas

Puede encontrar información adicional en la "[Soporte técnico](#)" página.

Recopilador de datos de Couchbase

Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Couchbase.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Elija Couchbase.

Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.
2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las "[Instalación del agente](#)" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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
```

Configuración

La información se puede encontrar en el ["Documentación de Couchbase"](#).

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Nodo Couchbase	Nombre de host del nodo Couchbase del clúster de espacios de nombres	Dirección IP del nodo de nombre	Memoria libre total
Bloque de Couchbase	Cluster de bloque de espacio de nombres	Dirección IP del nodo de nombre	Datos usados datos utilizados Conteo de elementos usados memoria usada Operaciones usadas por segundo cupos usados

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

CouchDB Collector datos

Data Infrastructure Insights usa este recopilador de datos para recopilar métricas de CouchDB.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Elija CouchDB.

Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las ["Instalación del agente"](#) instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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
```

Configuración

La información se puede encontrar en el "[Documentación de CouchDB](#)".

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
CouchDB	Servidor de espacio de nombres	Dirección IP del nodo de nombre	Autenticación Cache Hits Authentication Cache Miss Database Lecturas Database Databases Open OS Files Max Request Time Min Request metodos Copy httpd Request metodos Delete httpd Request metodos Get httpd Request metodos Head httpd Request metodos Post httpd Request metodos put httpd códigos de estado 200 códigos de estado 201 códigos de estado 202 códigos de estado 301 códigos de estado 304 códigos de estado 400 códigos de estado 401 códigos de estado 403 códigos de estado 404 códigos de estado 405 códigos de estado 409 códigos de estado 412 códigos de estado 500

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

Recopilador de datos de Docker

Data Infrastructure Insights usa este recopilador de datos para recopilar métricas de Docker.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Elija Docker.

Si no ha configurado un agente para la recopilación, se le pedirá que lo haga ["instale un agente"](#) en su inquilino.

Si ya ha configurado un agente, seleccione el sistema operativo o la plataforma adecuados y haga clic en **continuar**.

2. Siga las instrucciones de la pantalla de configuración de Docker para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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
```

Configuración

El complemento de entrada de Telegraf para Docker recopila métricas a través de un socket UNIX o un extremo TCP especificado.

Compatibilidad

La configuración se desarrolló en comparación con Docker, versión 1.12.6.

Configuración

Acceso a Docker a través de un socket de UNIX

Si el agente de Telegraf se está ejecutando en baremetal, agregue el usuario de Unix telegraf al grupo Unix docker ejecutando lo siguiente:

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

Si el agente de Telegraf se ejecuta en un pod de Kubernetes, exponga el socket Unix Docker asignando el socket al pod como un volumen y, a continuación, monte dicho volumen a /var/run/docker.sock. Por ejemplo, agregue lo siguiente a PodSpec:

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

A continuación, añada lo siguiente al contenedor:

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

Tenga en cuenta que el instalador de Data Infrastructure Insights proporcionado para la plataforma Kubernetes se encarga de esta asignación de forma automática.

Acceda a Docker a través de un extremo de TCP

De forma predeterminada, Docker utiliza el puerto 2375 para el acceso no cifrado y el puerto 2376 para el acceso cifrado.

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Motor Docker	Namespace Docker Engine	Nombre de nodo IP nodo UUID nodo OS Kubernetes Cluster Unidad de versión de Docker	Contenedores de memoria Contenedores en pausa Contenedores en ejecución Contenedores CPUs detenidas Ir rutinas Ir Imágenes Listener Eventos usados Descriptores de archivos datos disponibles datos totales datos usados metadatos disponibles total de metadatos usados Tamaño de bloque usado de Pool

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Contenedor Docker	Nombre de contenedor de espacio de nombres Docker Engine	Contenedor Kubernetes Hash puertos de contenedor Kubernetes Container Restart Count Kubernetes Container Termination Message Path Kubernetes Container Termination Message Policy Kubernetes Pod Termination Message Container Termination período Grace Container Status Container Version Nombre de nodo Nombre de contenedor Kubernetes Container Log Nombre de contenedor Kubernetes Nombre de contenedor Docker Nombre de Kubernetes Pod Nombre de espacio de nombres Kubernetes Pod Pod UID Kubernetes Sandbox ID nodo IP UUID nodo Versión Docker Configuración de Kubernetes IO visto Kubernetes IO Config Source OpenShift IO SCC Kubernetes Descripción Kubernetes Display Name OpenShift Etiquetas Kompose Service Pod Template Hash Controller revisión plantilla Hash Pod Generation License Schema creación Fecha Esquema de licencia Nombre de esquema de licencia URL Esquema de URL de SCHEMA Esquema de proveedor Versión de esquema Versión de esquema Maintainer Customer Pod Kubernetes Statilusionados Nombre de Pod arrendatario Arquitectura de consola web autoritativa URL de origen Fecha de creación de host RH alcance de distribución de componentes instalar	Memoria Active Anonymous Memory caché de archivos activos memoria de límite jerárquico memoria inactiva memoria de archivos inactivos límite de memoria de archivos asignados memoria de uso máximo memoria de página fallo memoria de página principal memoria paginada en memoria salida residente memoria Tamaño de conjunto residente Tamaño de memoria Resident Tamaño enorme memoria total activa Memoria anónima memoria total Active File Memory memoria total Anonymous Inactive memoria total Inactive File memoria total asignada total Page memoria total Página falla memoria Principal error memoria total paginado en memoria total paginado agotado memoria total Resident Set Size memoria total Resident Set Size enorme memoria total Memoria de Unevictable uso de memoria de Unevictable uso de memoria porcentaje de uso de código de salida OOM asesinado PID iniciado en fallo de Streak

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Docker Container Block IO	Nombre de contenedor de espacio de nombres dispositivo Docker Engine	Contenedor Kubernetes Hash puertos de contenedor Kubernetes Container Restart Count Kubernetes Container Termination Message Path Kubernetes Container Termination Message Policy Kubernetes Pod Termination Message Container Termination período Grace Container Status Container Version Nombre de nodo Nombre de contenedor Kubernetes Container Log Nombre de contenedor Kubernetes Nombre de contenedor Docker Nombre de Kubernetes Pod Nombre de espacio de nombres Kubernetes Pod Pod UID Kubernetes Sandbox ID nodo IP UUID de nodo Versión Docker Configuración de Kubernetes vista Código de configuración de Kubernetes OpenShift SCC Kubernetes Descripción de Kubernetes Nombre de visualización OpenShift Etiquetas Esquema Versión de esquema plantilla Pod Revisión de controlador de hash generación de plantilla de Pod de esquema de servicio creación de esquema de fecha de creación de esquema de licencia Nombre de esquema de esquema de cliente de proveedor Pod Kubernetes StatefulSet Pod Name Intenant WebConsole Fecha de creación Arquitectura de proveedor Dirección URL de origen autoritativa RH Build Host RH Component Distribution Scope Install Maintainer Release Run	Bytes de servicio IO asíncrono recursivo bytes de servicio IO de lectura recursiva bytes de servicio IO de sincronización recursiva bytes de servicio IO total de servicio E/S bytes de servicio E/S de escritura recursiva E/S de escritura recursiva E/S asincrónica Serviced Recursive Read IO Serviced Recursive Sync IO Serviced Recursive total IO total IO Serviced Recursive Write

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Red de contenedores Docker	Namespace Container Name Network Docker Engine	Contenedor Image Container Status Container Status Container Version Nombre de nodo IP nodo UUID de nodo SO K8s Cluster Docker Version Container ID	RX bytes borrados RX errores RX paquetes RX bytes TX bytes TX errores TX paquetes TX

Objeto:	Identificadores:	Atributos:	Puntos de datos:
CPU de contenedor Docker	Namespace Container Name CPU Docker Engine	Kubernetes Container Hash Kubernetes Container Ports Kubernetes Container Restart Count Kubernetes Container Termination Message Path Kubernetes Container Termination Message Policy Kubernetes Pod Termination Message período Grace Kubernetes Config visto Kubernetes Config OpenShift SCC Container Image Container Status Container Version Nombre de nodo Nombre de contenedor Kubernetes Container Log Nombre de contenedor Kubernetes Docker Escriba Kubernetes Pod Name Kubernetes Pod Namespace Kubernetes Pod UID Kubernetes Sandbox ID nodo IP UUID nodo SO nodo Kubernetes Cluster Docker Versión Kubernetes Descripción Kubernetes Mostrar nombre OpenShift Etiquetas Esquema Versión plantilla Pod Revisión controladora Hash plantilla generación Hash Pod Nombre de esquema de servicio creación de esquema de fecha de creación de esquema de licencia Nombre de esquema de licencia Esquema Proveedor de cliente ilusionados Kubernetes StatSet Pod Nombre de Pod arrendatario WebConsole Fecha de creación Licencia Arquitectura de proveedor Dirección de origen autoritativa RH construir Host RH ámbito de distribución de	Los períodos de aceleración aceleran los períodos de regulación acelerando el uso de tiempo en modo Kernel en uso de modo Usuario Porcentaje de uso de sistema total

Resolución de problemas

Problema:	Pruebe lo siguiente:
No veo mis métricas de Docker en Data Infrastructure Insights después de seguir las instrucciones en la página de configuración.	Compruebe si el agente de Telegraf registra el siguiente error: E! Error en el plugin [inputs.docker]: Se le ha denegado el permiso al intentar conectarse a la toma del demonio Docker. Si lo hace, siga los pasos necesarios para proporcionar al agente Telegraf acceso al socket Unix Docker según se ha especificado anteriormente.

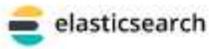
Puede encontrar información adicional en la ["Soporte técnico"](#) página.

Recopilador de datos de Elasticsearch

Data Infrastructure Insights usa este recopilador de datos para recopilar métricas de Elasticsearch.

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Seleccione Elasticsearch.

Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.
2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las ["Instalación del agente"](#) instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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
```

Configuración

La información se puede encontrar en el "[Documentación de Elasticsearch](#)".

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:
Clúster de Elasticsearch	Cluster de espacio de nombres	Nodo IP Node Name Cluster Status
Nodo de Elasticsearch	Namespace Cluster es Node ID es Node IP es Node	ID de zona

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

Colector de datos Flink

Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Flink.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Seleccione Flink.

 Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.
2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las ["Instalación del agente"](#) instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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
```

Configuración

Un despliegue completo de Flink implica los siguientes componentes:

JobManager: El sistema primario Flink. Coordina una serie de TaskManagers. En una configuración de alta disponibilidad, el sistema tendrá más de un JobManager. **TaskManager:** Aquí es donde se ejecutan los operadores Flink. El plugin de tinta se basa en el complemento Jolokia de telegraf. Como un requisito para recopilar información de todos los componentes de Flink, JMX debe configurarse y exponerse a través de Jolokia en todos los componentes.

Compatibilidad

La configuración se desarrolló contra Flink versión 1.7.0.

Configuración

Agente Jolokia Jar

Para todos los componentes individuales, se debe descargar una versión del archivo JAR del agente JAR Jolokia. La versión probada con respecto a fue "[Agente Jolokia 1.6.0](#)".

Las instrucciones siguientes asumen que el archivo JAR descargado (jolokia-jvm-1.6.0-agent.jar) se coloca en la ubicación '/opt/flink/lib/'.

JobManager

Para configurar JobManager para exponer la API de Jolokia, puede configurar la siguiente variable de entorno en los nodos y, a continuación, reiniciar JobManager:

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

Puede elegir un puerto diferente para Jolokia (8778). Si usted tiene un IP interno para bloquear Jolokia en usted puede reemplazar el "Catch all" 0.0.0.0 por su propio IP. Tenga en cuenta que este IP debe ser accesible desde el plugin de telegraf.

Administrador de tareas

Para configurar TaskManager para exponer la API de Jolokia, puede configurar la siguiente variable de entorno en los nodos y, a continuación, reiniciar TaskManager:

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

Puede elegir un puerto diferente para Jolokia (8778). Si usted tiene un IP interno para bloquear Jolokia en usted puede reemplazar el "Catch all" 0.0.0.0 por su propio IP. Tenga en cuenta que este IP debe ser accesible desde el plugin de telegraf.

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Gestor de tareas de tinta	Servidor de espacio de nombres del cluster	Nombre del nodo Task Manager ID IP del nodo	Segmentos de memoria disponibles en red segmentos de memoria totales recolección de basura PS MarkSweep Count recolección de basura PS MarkSweep Time recolección de elementos basura PS Scavenge Count recolección de elementos de basura PS Scavenge Time Heap Memory Demised Heap Memory Init Heap Max Heap Memory memoria memoria de pila usada recuento de subprocesos recuento de pico recuento de subprocesos Total iniciado
Trabajo de tinta	Identificador de trabajo del servidor de espacio de nombres del clúster	Nombre del nodo Nombre del trabajo IP del nodo último punto de comprobación Ruta de acceso externa hora de reinicio	Tiempo de inactividad completo reinicia último punto de comprobación alineación búfer duración último punto de comprobación Tamaño último punto de comprobación número de puntos de comprobación completados número de puntos de comprobación fallidos número de puntos de comprobación en curso número de puntos de comprobación de tiempo de actividad

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Gestor de trabajos de tinta	Servidor de espacio de nombres del cluster	Dirección IP del nodo de nombre	Recolección de elementos no utilizados PS MarkSweep Count Garbage Collection PS MarkSweep Time Garbage Collection PS Scvenge Count Garbage Collection PS Scavenge Time Heap Memory Asked Heap Memory Init memoria memoria heap Max Heap número usado gestores de tareas número ejecutando trabajos ranuras de tareas disponibles Tragamonedas de tareas total de subprocesos Demon Count Recuento de subprocesos máximos recuento de subprocesos total iniciado

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Tarea de tinta	ID de tarea de ID de trabajo de espacio de nombres del clúster	Nombre de nodo de servidor Nombre de trabajo Subíndice de tarea Id. De intento de tarea número de intento de tarea Nombre de tarea Id. De nodo IP Marca de agua de entrada actual	Búferes en búferes de uso de pool en búferes de longitud de cola fuera búferes de uso de pool fuera búferes de longitud de cola en buffers de número local por segundo búferes de número de cuenta en búferes de número local por segundo en búferes de número de frecuencia remotos en búferes de número de cuenta remotos por segundo en remoto por Segundo número de tasa de búferes de salida número de búferes de salida por segundo número de búferes de salida por segundo número de tasa en bytes de número local por segundo número de bytes en bytes de número de tasa local por segundo en bytes de número de bytes remotos en bytes de número de cuenta remotos por segundo en remoto Por segundo número de tasa bytes de salida número de bytes por segundo número de recuento bytes por segundo número de tasa registros en número de registros por segundo número de recuento registros por segundo número de tasa registros número de salida registros por segundo número de registros salida registros por segundo número de cuenta registros por segunda tasa

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Operador de tareas de tinta	ID de trabajo ID de espacio de nombres de clúster ID de tarea de operador	Nombre del nodo del servidor Nombre del trabajo Nombre del operador Subíndice de tarea número de tarea número de intento de tarea Nombre de tarea ID del administrador de tareas IP del nodo	Registros de número de Marca de agua de entrada actual número de Marca de agua de salida actual registros en número de registros por segundo número de cuenta registros por segundo número de tarifa registros de salida número de registros por segundo número de salida registros por segundo número de tasa registros atrasados particiones asignadas bytes consumidos tasa Commit latencia media Tasa de confirmación máx. De confirmaciones fallidas conexión correcta Convalidación de frecuencia de cierre recuento de conexiones recuento de frecuencia de creación tasa de obtención latencia media de obtención tasa de obtención tasa de obtención Tamaño medio de obtención Tamaño de sesión Máx. Tiempo de aceleración de obtención Promedio tiempo de aceleración velocidad máxima de latido tasa de latidos entrantes tasa de E/S tiempo medio (ns) E/S Ratio de espera tiempo de espera de E/S Avg (ns) tiempo de unión media tiempo de unión Fecha de la última hora de latido de red tasa de E/S de salida registros tasa de frecuencia consumido registros de retraso máx. Registros por solicitud promedio Tamaño de solicitud promedio Tamaño de solicitud tiempo de respuesta máximo Seleccione frecuencia de sincronización de la velocidad tiempo de latido

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

Recopilador de datos de Hadoop

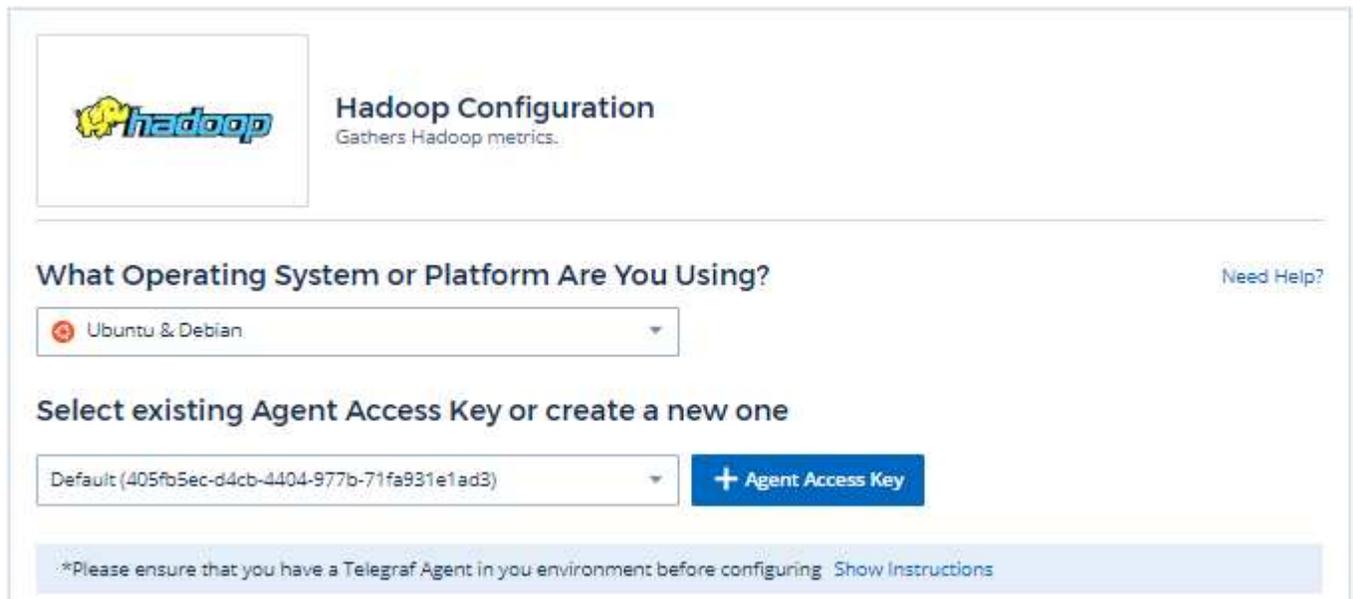
Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Hadoop.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Elija Hadoop.

Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las ["Instalación del agente"](#) instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



The screenshot shows the 'Hadoop Configuration' page. At the top left is the Hadoop logo. To its right, the text reads 'Hadoop Configuration' and 'Gathers Hadoop metrics.' Below this is a section titled 'What Operating System or Platform Are You Using?' with a 'Need Help?' link. A dropdown menu is set to 'Ubuntu & Debian'. Below that is another section titled 'Select existing Agent Access Key or create a new one'. A dropdown menu shows 'Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)' and a blue button labeled '+ Agent Access Key'. At the bottom, a light blue banner contains the text: '*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 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
```

Configuración

Una puesta en marcha completa de Hadoop incluye los siguientes componentes:

- NameNode: El sistema primario de archivos distribuidos de Hadoop (HDFS). Coordina una serie de DataNodes.

- **NombreNodo secundario:** Una conmutación por error en caliente para el NameNode principal. En Hadoop, la promoción a NameNode no se realiza automáticamente. El NombreNodo secundario recopila información de NameNode para que esté listo para ser promovido cuando sea necesario.
- **DataNode:** Propietario real de los datos.
- **ResourceManager:** El sistema primario de computación (Yarn). Coordina una serie de NodeManagers.
- **NodeManager:** El recurso para la computación. Ubicación real para ejecutar aplicaciones.
- **JobHistoryServer:** Responsable del servicio de todas las solicitudes relacionadas con el historial de trabajos.

El complemento Hadoop se basa en el complemento Jolokia de telegraf. Como un requisito para recopilar información de todos los componentes de Hadoop, JMX debe configurarse y exponerse a través de Jolokia en todos los componentes.

Compatibilidad

La configuración se desarrolló con Hadoop versión 2.9.2.

Configuración

Agente Jolokia Jar

Para todos los componentes individuales, se debe descargar una versión del archivo JAR del agente JAR Jolokia. La versión probada con respecto a fue "[Agente Jolokia 1.6.0](#)".

Las instrucciones siguientes asumen que el archivo JAR descargado (jolokia-jvm-1.6.0-agent.jar) se coloca en la ubicación '/opt/hadoop/lib/'.

NombreNodo

Para configurar NameNode para exponer la API de Jolokia, puede configurar lo siguiente en <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.

NombreNodo secundario

Para configurar el nodo secundario NameNode para exponer la API de Jolokia, puede configurar lo siguiente en `<HADOOP_HOME>/etc/hadoop/hadoop-env.sh`:

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

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

Nodo de datos

Para configurar DataNodes para exponer la API de Jolokia, puede configurar lo siguiente en `<HADOOP_HOME>/etc/hadoop/hadoop-env.sh`:

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

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

ResourceManager

Para configurar ResourceManager para exponer la API de Jolokia, puede configurar lo siguiente en `<HADOOP_HOME>/etc/hadoop/hadoop-env.sh`:

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

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

NodeManager

Para configurar NodeManagers para exponer la API de Jolokia, puede configurar lo siguiente en <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

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

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

JobHistoryServer

Para configurar JobHistoryServer para exponer la API de Jolokia, puede configurar lo siguiente en <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

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

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

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:
Nombre secundario de Hadoop	Servidor de espacio de nombres del cluster	Nombre del nodo IP Compile Info Version
NodeManager de Hadoop	Servidor de espacio de nombres del cluster	Dirección IP del nodo de nombre
Administrador de recursos de Hadoop	Servidor de espacio de nombres del cluster	Dirección IP del nodo de nombre
Nodo de datos de Hadoop	Servidor de espacio de nombres del cluster	Node Name IP Node Cluster ID Version
NombreHadoop	Servidor de espacio de nombres del cluster	Nombre del nodo ID de transacción IP del nodo última vez que se cargó Edits ha Estado del sistema Estado del sistema bloque ID de grupo ID de clúster compilación Info Versión de recuento de versiones distinta
Hadoop JobHistoryServer	Servidor de espacio de nombres del cluster	Dirección IP del nodo de nombre

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

Recopilador de datos de HAProxy

Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de HAProxy.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Seleccione HAProxy.

Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las "[Instalación del agente](#)" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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
  ## eg localhost:1936/stats; 10.10.3.33:1936/xxxxx?xxxxx
```

- 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
```

Configuración

El complemento de Telegraf para HAProxy se basa en la habilitación de HAProxy Stats. Se trata de una configuración integrada en HAProxy pero no está activada de forma inmediata. Cuando se habilita, HAProxy

expondrá un punto final HTML que se puede ver en el explorador o se puede raspar para extraer el estado de todas las configuraciones de HAProxy.

Compatibilidad:

La configuración se desarrolló contra HAProxy versión 1.9.4.

Configuración:

Para habilitar las estadísticas, edite el archivo de configuración de haproxy y agregue las siguientes líneas después de la sección 'valores predeterminados', utilizando su propia contraseña/usuario y/o URL de haproxy:

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

A continuación se muestra un ejemplo de archivo de configuración simplificado con estadísticas habilitadas:

```
global
  daemon
  maxconn 256

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

frontend http-in
  bind *:80
  default_backend servers

frontend http-in9080
  bind *:9080
  default_backend servers_2

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

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

Para obtener instrucciones completas y actualizadas, consulte la ["Documentación de HAProxy"](#).

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Interfaz HAProxy	Proxy de direcciones de espacio de nombres	Nodo IP Nombre de nodo ID de proxy modo Id. De proceso sesiones límite de número de sesiones id de servidor Estado de límite	Bytes in bytes OUT Cache Hits Cache LOOKUP bytes de compresión bytes de compresión omitidos en bytes de compresión respuestas de compresión tasa de conexión Max Connections solicitudes totales denegadas por solicitudes de regla de conexión denegadas por respuestas de seguridad denegadas por solicitudes de problemas de seguridad denegadas por solicitudes de regla de sesión respuesta de errores 1xx Respuestas 2xx respuestas 3xx respuestas 4xx respuestas 5xx respuestas otras solicitudes interceptadas sesiones tasa máx. Solicitudes tasa máx. Solicitudes tasa máx. Solicitudes máx. Sesiones sesiones máx. Sesiones sesiones número máx. De solicitudes reescrituras

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Servidor HAProxy	Servidor proxy de direcciones del espacio de nombres	Nombre de nodo IP Comprobación tiempo de finalización Comprobación Configuración de caída comprobar valor de estado comprobar configuración de elevación comprobar estado ID de proxy última hora última hora última sesión modo de proceso id. De servidor Peso	Servidores activos copia de seguridad servidores bytes en bytes sin comprobar las dus Comprobación de errores cliente falla aborta conexiones Conexión tiempo medio inactividad total respuestas denegadas errores de conexión respuestas 1xx respuestas 2xx respuestas 3xx respuestas 4xx respuestas 5xx otro servidor seleccionado Cola total actual Máx. Cola sesiones de tiempo medio por Segunda sesiones por segundo tiempo máximo de respuesta de reutilización sesiones promedio sesiones transferencia máxima de servidor aborta sesiones total sesiones solicitudes promedio de tiempo total Redistribuye solicitudes de reescrituras de reintentos

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Backend de HAProxy	Proxy de direcciones de espacio de nombres	Nodo IP Nombre de nodo ID de proxy última hora de cambio última sesión modo de proceso id. De servidor sesiones límite Peso	Servidores activos copia de seguridad de servidores bytes en bytes caché aciertos en caché consultas en caché Comprobación de clientes de Downs aborta bytes de compresión bytes de compresión omitidos en bytes de compresión respuestas de compresión conexiones tiempo medio de inactividad de conexión solicitudes totales denegadas por problemas de seguridad respuestas denegadas por errores de conexión respuesta errores de respuesta 1xx respuestas 2xx respuestas 3xx respuestas 4xx respuestas 5xx respuestas otro servidor seleccionado Cola total Cola actual Máx. Cola sesiones de tiempo medio por segundo sesiones por segundo número máximo de solicitudes total tiempo de respuesta de reutilización sesiones promedio sesiones Máx. Transferencia de servidores aborta sesiones total sesiones número de sesiones solicitudes promedio de tiempo total Redistribuye solicitudes de reintentos Reescrituras

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

Recopilador de datos JVM

Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de JVM.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Seleccione JVM.

Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las "[Instalación del agente](#)" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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 you 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
```

Configuración

La información se puede encontrar en "[Documentación de JVM](#)".

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
JVM	JVM de espacio de nombres	Arquitectura del sistema operativo Nombre del sistema operativo Versión tiempo de ejecución especificación de tiempo de ejecución de proveedor Versión de tiempo de ejecución tiempo de ejecución VM Nombre de tiempo de ejecución VM tiempo de ejecución de proveedor VM Versión de nodo Nombre IP de nodo	Clase cargada clase total cargada memoria descargada memoria recargada memoria heap memoria asignada Heap memoria Init Heap memoria máxima utilizada memoria no asignada memoria no heap Init no heap memoria máxima memoria no heap memoria no utilizada objetos de memoria pendientes finalización pendiente procesadores de sistema operativo disponibles SO memoria virtual confirmada SO libre Tamaño de memoria física OS espacio libre intercambio Tamaño de espacio SO máximo número de descriptores de archivos de sistema operativo número de descriptores de archivos de código de sistema procesador de SO carga de CPU tiempo de CPU sistema de sistema de sistema carga media del sistema OS Tamaño total de memoria física SO total intercambio espacio Tamaño total Demonio recuento de subprocesos recuento de subprocesos Recuento de subprocesos total iniciado recuento de basura Coleccionista de copias Colección recuento de basura Coleccionista de basura tiempo recolección de elementos de basura Coleccionista de elementos de basura Coleccionista de marcas-barrido Coleccionista de tiempo de recolección de elementos de la generación antigua G1 Coleccionista de elementos de recolección de elementos de basura Coleccionista de

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

Recopilador de datos Kafka

Data Infrastructure Insights usa este recopilador de datos para recopilar métricas de Kafka.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Elige Kafka.

Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las ["Instalación del agente"](#) instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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
```

Configuración

El complemento Kafka se basa en el complemento Jolokia de telegraf. Como un requisito para recopilar información de todos los corredores Kafka, JMX debe configurarse y exponerse a través de Jolokia en todos los componentes.

Compatibilidad

La configuración se desarrolló contra Kafka versión 0.11.0.2.

Configuración

Todas las instrucciones a continuación suponen que su ubicación de instalación para kafka es '/opt/kafka'. Puede adaptar las instrucciones siguientes para reflejar la ubicación de la instalación.

Agente Jolokia Jar

Una versión El archivo jar del agente Jolokia debe ser "[descargado](#)". La versión probada en contra fue el agente Jolokia 1.6.0.

Las instrucciones siguientes asumen que el archivo JAR descargado (jolokia-jvm-1.6.0-agent.jar) se coloca bajo la ubicación '/opt/kafka/libs/'.

Kafka Brokers

Para configurar Kafka Brokers para exponer la API de Jolokia, puede agregar lo siguiente en <KAFKA_HOME>/bin/kafka-Server-start.sh, justo antes de la llamada '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"
```

Tenga en cuenta que el ejemplo anterior utiliza 'hostname -i' para configurar la variable de entorno 'RMI_HOSTNAME'. En múltiples equipos IP, esto tendrá que ser ajustado para reunir la IP que usted cuida para las conexiones RMI.

Puede elegir un puerto diferente para JMX (9999 arriba) y Jolokia (8778). Si usted tiene un IP interno para bloquear Jolokia en usted puede reemplazar el "Catch all" 0.0.0.0 por su propio IP. Tenga en cuenta que este IP debe ser accesible desde el plugin de telegraf. Puede utilizar la opción '-Dcom.sun.management.jmxremote.authenticate=false' si no desea autenticar. Uso bajo su propio riesgo.

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:
Kafka Broker	Agente de espacio de nombres del clúster	Dirección IP del nodo de nombre

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

Recopilador de datos de Kibana

Data Infrastructure Insights usa este recopilador de datos para recopilar métricas de Kibana.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Elige Kibana.

Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las ["Instalación del agente"](#) instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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 `'password'` 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
```

Configuración

La información se puede encontrar en el "[Documentación de Kibana](#)".

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Kibana	Dirección del espacio de nombres	Estado de la versión del nombre del nodo IP	Conexiones simultáneas Heap Max Heap solicitudes usadas por segundo tiempo de respuesta promedio tiempo de respuesta máximo tiempo de actividad

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

Instalación y configuración del operador de supervisión de Kubernetes

Data Infrastructure Insights ofrece el **Operador de Monitoreo de Kubernetes** para la colección de Kubernetes. Vaya a **Kubernetes > Colectores > +Kubernetes Collector** para implementar un nuevo operador.

Antes de instalar el operador de supervisión de Kubernetes

Consulte ["Requisitos previos"](#) la documentación antes de instalar o actualizar el operador de supervisión de Kubernetes.

Instalación del operador de supervisión de 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

Pasos para instalar el agente del operador de supervisión de Kubernetes en Kubernetes:

1. Introduzca un nombre de clúster y un espacio de nombres únicos. Si es [actualizando](#) de un operador de Kubernetes anterior, utilice el mismo nombre de clúster y espacio de nombres.
2. Una vez introducidos, puede copiar el fragmento del comando de descarga en el portapapeles.
3. Pegue el fragmento en una ventana `bash` y ejecútelo. Se descargarán los archivos de instalación del operador. Tenga en cuenta que el fragmento tiene una clave única y es válido durante 24 horas.
4. Si tiene un repositorio personalizado o privado, copie el fragmento opcional Image pull, péguelo en un shell `bash` y ejecútelo. Una vez extraídas las imágenes, cópielas en tu repositorio privado. Asegúrese de mantener las mismas etiquetas y la misma estructura de carpetas. Actualice las rutas de acceso en `operator-deployment.yaml`, así como la configuración del repositorio de Docker en `operator-config.yaml`.
5. Si lo desea, revise las opciones de configuración disponibles, como la configuración de repositorio privado o proxy. Puedes leer más sobre ["opciones de configuración"](#).
6. Cuando esté listo, despliegue el Operador copiando el fragmento de aplicación `kubectl`, descargándolo y ejecutándolo.
7. La instalación se realiza automáticamente. Cuando haya terminado, haga clic en el botón `Next`.
8. Una vez finalizada la instalación, haga clic en el botón `Next`. Asegúrese también de eliminar o almacenar de forma segura el archivo `operator-secrets.yaml`.

Si está utilizando un proxy, lea acerca de [configurando proxy](#).

Si tiene un repositorio personalizado, lea acerca de [utilizando un repositorio de docker personalizado/privado](#).

Componentes de supervisión de Kubernetes

Información de la infraestructura de datos La supervisión de Kubernetes se compone de cuatro componentes de supervisión:

- Métricas de cluster
- Rendimiento de red y mapa (opcional)
- Registros de eventos (opcional)
- Análisis de cambios (opcional)

Los componentes opcionales anteriores están habilitados de forma predeterminada para cada recopilador de Kubernetes; si decide que no necesita un componente para un recopilador en particular, puede deshabilitarlo navegando a **Kubernetes > Colectores** y seleccionando *Modify Deployment* en el menú de tres puntos del recopilador a la derecha de la pantalla.

NetApp / Observability / Collectors

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

Kubernetes Collectors (13)

[View Upgrade/Delete Documentation](#)

[+ Kubernetes Collector](#)

Filter...

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 pantalla muestra el estado actual de cada componente y le permite desactivar o activar componentes para ese recopilador según sea necesario.

 **kubernetes**
Kubernetes

Modify Deployment

Cluster Information

Kubernetes Cluster
ci-demo-01

Network Performance and Map
Enabled - Online

Event Logs
Enabled - Online

Change Analysis
Enabled - Online

Deployment Options

[Need Help?](#)

- Network Performance and Map
- Event Logs
- Change Analysis

Cancel

Complete Modification

Actualiza al operador de supervisión de Kubernetes más reciente

Determine si existe una AgentConfiguration con el operador existente (si el espacio de nombres no es el valor predeterminado `netapp-monitoring`, sustituya el espacio de nombres adecuado):

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

Si existe una configuración de agente:

- **Instale** El último operador sobre el operador existente.
 - Asegúrese de que está [extracción de las imágenes de contenedor más recientes](#) utilizando un repositorio personalizado.

Si la configuración de agente no existe:

- Anote el nombre de su clúster como reconocido por Data Infrastructure Insights (si su espacio de nombres no es la supervisión NetApp predeterminada, sustituya el espacio de nombres adecuado):

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

* Cree una copia de seguridad del Operador existente (si su espacio de nombres no es el control de netapp predeterminado, sustituya el espacio de nombres adecuado):

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

* <<to-remove-the-kubernetes-monitoring-operator,Desinstalar>> El operador existente.

* <<installing-the-kubernetes-monitoring-operator,Instale>> El último operador.

- Utilice el mismo nombre de clúster.
- Después de descargar los últimos archivos YAML del operador, transfiera cualquier personalización encontrada en `agent_backup.yaml` al `operator-config.yaml` descargado antes de implementar.
- Asegúrese de que está [extracción de las imágenes de contenedor más recientes](#) utilizando un repositorio personalizado.

Detener e iniciar el operador de supervisión de Kubernetes

Para detener el operador de supervisión de Kubernetes:

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

Para iniciar el operador de supervisión de Kubernetes:

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

Desinstalando

Para eliminar el operador de supervisión de Kubernetes

Tenga en cuenta que el espacio de nombres predeterminado para el operador de supervisión de Kubernetes es la «supervisión de netapp». Si ha definido su propio espacio de nombres, sustituya este espacio de nombres en estos y todos los comandos y archivos subsiguientes.

Las versiones más recientes del operador de supervisión se pueden desinstalar con los siguientes comandos:

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

Si el operador de supervisión se ha desplegado en su propio espacio de nombres dedicado, suprima el espacio de nombres:

```
kubectl delete ns <NAMESPACE>
```

Si el primer comando devuelve “no se han encontrado recursos”, utilice las siguientes instrucciones para desinstalar versiones anteriores del operador de supervisión.

Ejecute cada uno de los comandos siguientes en orden. Dependiendo de su instalación actual, algunos de estos comandos pueden devolver mensajes de ‘no se ha encontrado el objeto’. Estos mensajes pueden ignorarse con seguridad.

```
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>
```

Si se ha creado previamente una restricción de contexto de seguridad:

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

Acerca de las métricas de estado de Kube

El operador de supervisión de Kubernetes de NetApp instala sus propias métricas de estado kube para evitar conflictos con otras instancias.

Para obtener más información sobre Kube-State-Metrics, consulte ["esta página"](#).

Configuración/Personalización del Operador

Estas secciones contienen información sobre cómo personalizar la configuración del operador, cómo trabajar con proxy, cómo usar un repositorio de Docker personalizado o privado o cómo trabajar con OpenShift.

Opciones de configuración

La configuración más comúnmente modificada se puede configurar en el recurso personalizado *AgentConfiguration*. Puede editar este recurso antes de desplegar el operador editando el archivo *operator-config.yaml*. Este archivo incluye ejemplos de configuración comentados. Consulte la lista de ["ajustes disponibles"](#) para obtener la versión más reciente del operador.

También puede editar este recurso después de desplegar el operador mediante el siguiente comando:

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

Para determinar si la versión implementada del operador admite *AgentConfiguration*, ejecute el siguiente comando:

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

Si ve un mensaje "Error from server (NotFound)", su operador debe actualizarse antes de poder usar *AgentConfiguration*.

Configurar el soporte del proxy

Hay dos lugares en los que puede usar un proxy en su inquilino para instalar el operador de monitoreo de Kubernetes. Pueden ser los mismos sistemas proxy o independientes:

- Proxy necesario durante la ejecución del fragmento de código de instalación (mediante «curl») para conectar el sistema donde se ejecuta el fragmento a su entorno de Data Infrastructure Insights
- Proxy que necesita el clúster de Kubernetes de destino para comunicarse con su entorno de Data Infrastructure Insights

Si usas un proxy para una o ambas de ellas, para instalar el Monitor Operativo de Kubernetes, primero debes asegurarte de que tu proxy esté configurado para permitir una buena comunicación con tu entorno de Información de Infraestructura de Datos. Si tiene un proxy y puede acceder a Data Infrastructure Insights desde el servidor/VM desde el que desea instalar el Operador, es probable que su proxy esté configurado correctamente.

Para el proxy utilizado para instalar el monitor operativo de Kubernetes, antes de instalar el operador, defina las variables de entorno `http_proxy/https_proxy`. En algunos entornos proxy, también es posible que tenga que establecer la variable `no_proxy Environment`.

Para configurar las variables, realice los siguientes pasos en su sistema **antes** de instalar el Operador de monitoreo de Kubernetes:

1. Establezca las variables de entorno `https_proxy` y/o `http_proxy` para el usuario actual:
 - a. Si el proxy que se está estableciendo no tiene autenticación (nombre de usuario/contraseña), ejecute el siguiente comando:

```
export https_proxy=<proxy_server>:<proxy_port>
.. Si el proxy que se está estableciendo tiene autenticación (nombre de usuario/contraseña), ejecute este comando:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_port>
```

Para que el proxy utilizado para su clúster de Kubernetes se comunique con su entorno de Información de infraestructura de datos, instale el operador de supervisión de Kubernetes después de leer todas estas instrucciones.

Configure la sección proxy de AgentConfiguration en `operator-config.yaml` antes de implementar el operador de supervisión de 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
  ...
  ...

```

Uso de un repositorio de Docker personalizado o privado

De forma predeterminada, el operador de supervisión de Kubernetes extraerá imágenes de contenedor del repositorio de información de infraestructura de datos. Si tiene un clúster de Kubernetes utilizado como destino para la supervisión, y ese clúster está configurado para extraer solo imágenes de contenedor de un repositorio Docker privado o personalizado o un registro de contenedores, debe configurar el acceso a los contenedores que necesita el operador de supervisión de Kubernetes.

Ejecute «Image pull Snippet» desde el icono de instalación del operador de supervisión de NetApp. Este comando iniciará sesión en el repositorio de Data Infrastructure Insights, extraerá todas las dependencias de imágenes del operador y cerrará la sesión en el repositorio de Data Infrastructure Insights. Cuando se le solicite, introduzca la contraseña temporal del repositorio proporcionada. Este comando descarga todas las imágenes utilizadas por el operador, incluidas las funciones opcionales. Consulte a continuación las funciones para las que se utilizan estas imágenes.

Funcionalidad del operador principal y supervisión de Kubernetes

- supervisión de netapp
- ci-kube-rbac-proxy
- ci-ksm
- ci-telegraf
- usuario raíz sin interrupciones

Registro de eventos

- bits ci-fluido

- ci-kubernetes-event-exporter

Rendimiento de red y mapa

- ci-net-observador

Introduzca la imagen del operador docker en el repositorio de su proveedor de servicios de empresa/local/privado de acuerdo con las políticas de su empresa. Asegúrese de que las etiquetas de imagen y las rutas de directorio a estas imágenes del repositorio sean coherentes con las del repositorio de Data Infrastructure Insights.

Edite el despliegue de operador de supervisión en `operator-deployment.yaml` y modifique todas las referencias de imagen para utilizar su repositorio Docker privado.

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

Edite `AgentConfiguration` en `operator-config.yaml` para reflejar la nueva ubicación de repositorio de Docker. Cree una nueva `imagePullSecret` para su repositorio privado, para más detalles consulte <https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/>

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

Instrucciones de OpenShift

Si se ejecuta en OpenShift 4,6 o superior, debe editar la configuración de `AgentConfiguration` en `operator-config.yaml` para activar la configuración `runPrivileged`:

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

OpenShift puede implementar un nivel de seguridad añadido que puede bloquear el acceso a algunos componentes de Kubernetes.

Toleraciones y daños

Los *netapp-ci-telegraf-ds*, *netapp-ci-fluent-bit-ds* y *netapp-ci-net-observer-L4-ds* DaemonSets deben programar un pod en cada nodo del clúster para recopilar correctamente los datos en todos los nodos. El operador ha sido configurado para tolerar algunos **taints** bien conocidos. Si ha configurado algún daño personalizado en sus nodos, evitando así que los pods se ejecuten en cada nodo, puede crear una **tolerancia** para esos daños "En el campo *AgentConfiguration*". Si ha aplicado daños personalizados a todos los nodos del cluster, también debe agregar las toleraciones necesarias al despliegue del operador para permitir que el pod del operador se programe y ejecute.

Más información sobre Kubernetes "Tolerancias y taints".

Vuelva a la "[NetApp Kubernetes Monitoreo de la página de instalación del operador](#)"

Una nota sobre los secretos

Para eliminar el permiso del operador de supervisión de Kubernetes para ver los secretos en todo el clúster, elimine los siguientes recursos del archivo *operator-setup.yaml* antes de instalar:

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

Si se trata de una actualización, suprima también los recursos del clúster:

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

Si el análisis de cambios está activado, modifique *AgentConfiguration* o *operator-config.yaml* para anular el comentario de la sección de gestión de cambios e incluya *kindsToIgnoreFromWatch: "secrets"* en la sección de gestión de cambios. Observe la presencia y posición de comillas simples y dobles en esta línea.

```
# 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"'
...
```

Verificación de las firmas de imagen del operador de supervisión de Kubernetes

La imagen del operador y todas las imágenes relacionadas que despliega están firmadas por NetApp. Puede verificar manualmente las imágenes antes de la instalación usando la herramienta de cosign, o configurar un controlador de admisión de Kubernetes. Para obtener más detalles, consulte el "[Documentación de](#)

Kubernetes".

La clave pública utilizada para verificar las firmas de imagen está disponible en el mosaico de instalación del operador de supervisión en *Opcional: Cargue las imágenes del operador en su repositorio privado > Clave pública de firma de imagen*

Para verificar manualmente una firma de imagen, realice los siguientes pasos:

1. Copie y ejecute el fragmento de extracción de imagen
2. Copie e introduzca la contraseña del repositorio cuando se le solicite
3. Almacenar la clave pública de firma de imagen (dii-image-signing.pub en el ejemplo)
4. Verifique las imágenes usando el signo cosign. Consulte el siguiente ejemplo de uso de signo conjunto

```
$ 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}]
```

Resolución de problemas

Algunas cosas que debe probar si encuentra problemas para configurar el operador de supervisión de Kubernetes:

Problema:	Pruebe lo siguiente:
No veo un hipervínculo/conexión entre mi volumen persistente Kubernetes y el dispositivo de almacenamiento back-end correspondiente. Mi volumen persistente de Kubernetes se configura usando el nombre de host del servidor de almacenamiento.	Siga los pasos para desinstalar el agente de Telegraf existente y, a continuación, vuelva a instalar el último agente de Telegraf. Debe utilizar Telegraf versión 2,0 o posterior, y Data Infrastructure Insights debe supervisar de forma activa su almacenamiento en clúster de Kubernetes.

Problema:	Pruebe lo siguiente:
<p>En Kubernetes, mi pod Telegraf ReplicaSet informa del siguiente error: [inputs.prometheus] error en el plugin: No se pudo cargar keypair /etc/kubernetes/pki/etcd/Server.crt:/etc/kubernetes/pki/etcd/Server.key: Open /etc/kubernetes/pki/etcd/Server.crt: No existe ese archivo o directorio</p>	<p>El Pod Telegraf ReplicaSet está diseñado para ejecutarse en un nodo designado como maestro o etcd. Si el Pod ReplicaSet no se está ejecutando en uno de estos nodos, obtendrá estos errores. Compruebe si los nodos maestro/etcd tienen sugerencias. Si lo hacen, añada las toleraciones necesarias al Telegraf ReplicaSet, telegraf-rs. Por ejemplo, edite ReplicaSet... <code>kubectl edit rs telegraf-rs...</code> y añada las toleraciones adecuadas a la especificación. A continuación, reinicie el Pod ReplicaSet.</p>
<p>Tengo un entorno PSP/PSA. ¿Afecta esto a mi operador de supervisión?</p>	<p>Si su clúster de Kubernetes se ejecuta con la política de seguridad de Pod (PSP) o la admisión de seguridad de Pod (PSA), debe actualizar al último operador de supervisión de Kubernetes. Siga estos pasos para actualizar al Operador actual con soporte para PSP/PSA: 1. Desinstalar el operador de supervisión anterior: <code>kubectl delete agent-monitoring-NetApp -n NetApp-monitoring</code> <code>kubectl delete ns NetApp-monitoring</code> <code>kubectl delete crd agents.monitoring.NetApp.com</code> <code>kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader</code> <code>kubectl delete clusterrolebinding agent-manager-rolebinding agent-cluster-rolebinding agent-2</code>. 2. Instale la última versión del operador de monitorización.</p>
<p>Me encontré con problemas tratando de implementar el Operador, y tengo PSP/PSA en uso.</p>	<p>1. Edite el agente con el siguiente comando: <code>Kubectl -n <name-space> edit agent</code> 2. Marque "Security-policy-enabled" como "false". Esto desactivará las políticas de seguridad de Pod y la admisión de seguridad de Pod y permitirá que el operador se despliegue. Confirme utilizando los siguientes comandos: <code>Kubectl Get psp</code> (debería mostrar la política de seguridad de Pod eliminada) <code>knotbtl get all -n <namespace></code></p>
<p><code>grep -i psp</code> (debería mostrar que no se encuentra nada)</p>	<p>Se han visto errores "ImagePullBackoff"</p>
<p>Estos errores pueden verse si tiene un repositorio de Docker personalizado o privado y aún no ha configurado el operador de supervisión de Kubernetes para reconocerlo correctamente. Leer más acerca de la configuración para repositorio personalizado/privado.</p>	<p>Tengo un problema con la implementación de mi operador de supervisión y la documentación actual no me ayuda a resolverla.</p>

Problema:	Pruebe lo siguiente:
<p>Capture o anote el resultado de los siguientes comandos y póngase en contacto con el equipo de soporte técnico.</p> <pre data-bbox="136 296 802 751"> 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>Los pods de Net-Observer (Workload Map) en el espacio de nombres del operador están en CrashLoopBackOff</p>
<p>Estos pods corresponden al recopilador de datos de asignación de cargas de trabajo para la observabilidad de red. Pruebe estos:</p> <ul style="list-style-type: none"> • Compruebe los registros de uno de los pods para confirmar la versión mínima del kernel. Por ejemplo: --- {«ci-tenant-id»: «Your-tenant-id», «collector-cluster»: «Your-k8s-cluster-name», «environment»: «Prod», «level»: «Error», «msg»: «Failed in validation. Razón: La versión del kernel 3.10.0 es menor que la versión mínima del kernel de 4.18.0», «tiempo»: “2022-11-09T08:23:08Z”} ---- • Los pods de Net-Observer requieren que la versión del kernel de Linux sea al menos 4.18.0. Compruebe la versión del núcleo con el comando “uname -r” y asegúrese de que son >= 4.18.0 	<p>Los pods se ejecutan en el espacio de nombres del operador (predeterminado: Supervisión de netapp), pero no se muestran datos en la interfaz de usuario para el mapa de cargas de trabajo o las métricas de Kubernetes en consultas</p>
<p>Compruebe la configuración de hora en los nodos del clúster K8S. Para obtener informes precisos de auditoría y datos, se recomienda encarecidamente sincronizar la hora en el equipo del agente mediante el Protocolo de hora de red (NTP) o el Protocolo de hora de red simple (SNTP).</p>	<p>Algunos de los pods del observador de red en el espacio de nombres del operador están en estado Pendiente</p>
<p>NET-observer es un DaemonSet y ejecuta un pod en cada nodo del cluster k8s.</p> <ul style="list-style-type: none"> • Observe el pod que está en estado Pendiente y compruebe si está experimentando un problema de recursos para la CPU o la memoria. Asegúrese de que la memoria y la CPU requeridas estén disponibles en el nodo. 	<p>Estoy viendo lo siguiente en mis registros inmediatamente después de instalar el operador de supervisión de Kubernetes: [inputs.prometheus] Error en el plugin: Error al hacer la solicitud 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.local: No hay tal host</p>

Problema:	Pruebe lo siguiente:
<p>Este mensaje normalmente solo aparece cuando se instala un nuevo operador y el pod <i>telegraf-rs</i> está activo antes de que el pod <i>ksm</i> esté activo. Estos mensajes deben detenerse una vez que todos los pods se estén ejecutando.</p>	<p>No veo que se esté recopilando ninguna métrica para los cronjobs de Kubernetes que existen en mi clúster.</p>
<p>Compruebe la versión de Kubernetes (es decir, <code>kubectl version</code>). Si es v1,20.x o inferior, esta es una limitación esperada. La versión de métricas de estado de kube implementada con el operador de supervisión de Kubernetes solo admite v1.cronjob. Con Kubernetes 1,20.x y más abajo, el recurso cronjob está en v1beta.cronjob. Como resultado, kube-state-metrics no puede encontrar el recurso cronjob.</p>	<p>Después de instalar el operador, los pods de telegraf-rs ingresan CrashLoopBackOff y los registros de pod indican "su: Error de autenticación".</p>
<p>Edite la sección telegraf en <i>AgentConfiguration</i> y establezca <i>dockerMetricCollectionEnabled</i> en false. Para obtener más información, consulte la sección del operador "opciones de configuración". ... spec: ... telegraf: ... - Nombre: docker run-mode :- DaemonSet substitutions :- Clave: DOCKER_unix_SOCKET_PLACEHOLDER valor: unix://run/docker.SOCK</p>	<p>Veo mensajes de error repetidos que se parecen a los siguientes en mis registros de Telegraf: E! [Agent] Error al escribir en outputs.http: Post «\https://<tenant_url>/rest/v1/lake/ingest/influxdb»: Fecha límite de contexto excedida (Cliente. Se ha excedido el tiempo de espera de cabeceras)</p>
<p>Edite la sección telegraf en <i>AgentConfiguration</i> y aumente <i>outputTimeout</i> a 10s. Para obtener más información, consulte la sección del operador "opciones de configuración".</p>	<p>Faltan datos <i>involved object</i> para algunos registros de eventos.</p>
<p>Asegúrese de haber seguido los pasos de la "Permisos" sección anterior.</p>	<p>¿Por qué veo que funcionan dos pods del operador de supervisión, uno llamado netapp-ci-monitoring-operator-<pod> y otro llamado monitoring-operator-<pod>?</p>
<p>A partir del 12 de octubre de 2023, Data Infrastructure Insights ha refactorizado el operador para prestar un mejor servicio a nuestros usuarios; para que esos cambios se adopten por completo, debe retire el operador antiguo y instale la nueva.</p>	<p>Los eventos de My kubernetes dejaron de generar informes inesperadamente para la información de Data Infrastructure.</p>
<p>Recupere el nombre del pod de evento-exportador:</p> <pre> `kubectl -n netapp-monitoring get pods </pre>	<p>grep event-exporter</p>

Problema:	Pruebe lo siguiente:
<pre>awk '{print \$1}'</pre>	<pre>sed 's/event-exporter./event-exporter/'</pre> <p>Debe ser «exportador-de-centro-eventos-netapp» o «exportador-de-eventos». A continuación, edite el agente de supervisión <code>kubectl -n netapp-monitoring edit agent</code> y defina el valor para <code>LOG_FILE</code> para reflejar el nombre de pod de evento-exportador adecuado encontrado en el paso anterior. Más concretamente, <code>EL ARCHIVO_REGISTRO</code> debe establecerse en «<code>/var/log/containers/netapp-ci-event-exporter.log</code>» o «<code>/var/log/containers/event-exporter*.log</code>»</p> <pre>.... fluent-bit: ... - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log</pre> <p>Alternativamente, uno también puede desinstalar y volver a instalar el agente.</p>
<p>Estoy viendo que los pods han sido puestos en marcha por el operador de supervisión de Kubernetes se han bloqueado debido a la falta de recursos.</p>	<p>Consulte el operador de supervisión de Kubernetes "opciones de configuración" para aumentar los límites de CPU y/o memoria según sea necesario.</p>
<p>La falta de una imagen o una configuración no válida provocó que los pods de métricas de estado de netapp-ci-kube no se iniciaran o estuvieran listos. Ahora, StatefulSet se bloquea y los cambios de configuración no se aplican a los pods de métricas de estado-ci-kube.</p>	<p>El StatefulSet está en un "roto" estado. Después de resolver cualquier problema de configuración, renueve los pods de métricas de estado-ci-kube-state.</p>
<p>Los pods de métricas de estado-ci-kube-state no se pueden iniciar tras ejecutar una actualización del operador de Kubernetes y lanzar ErrImagePull (no lograr extraer la imagen).</p>	<p>Intente restablecer los pods manualmente.</p>
<p>Los mensajes de «Event discarded as as older then maxEventAgeSeconds» se observan para mi clúster de Kubernetes en Log Analysis.</p>	<p>Modifique el Operador <i>agentconfiguration</i> y aumente el <i>event-exporter-maxEventAgeSeconds</i> (es decir, a 60s), <i>event-exporter-kubeQPS</i> (es decir, a 100) y <i>event-exporter-kubeBurst</i> (es decir, a 500). Para obtener más información sobre estas opciones de configuración, consulte la "opciones de configuración" página.</p>

Problema:	Pruebe lo siguiente:
<p>Telegraf advierte de, o se bloquea debido a, memoria bloqueable insuficiente.</p>	<p>Intente aumentar el límite de memoria bloqueable para Telegraf en el sistema operativo/nodo subyacente. Si aumentar el límite no es una opción, modifique la configuración de agentconfiguration NKMO y establezca <i>UNPROTECTED</i> en <i>TRUE</i>. Esto indicará a Telegraf que no intente reservar páginas de memoria bloqueadas. Aunque esto puede suponer un riesgo para la seguridad, ya que los secretos descifrados se pueden intercambiar en el disco, permite su ejecución en entornos en los que no es posible reservar la memoria bloqueada. Para obtener más información sobre las opciones de configuración <i>UNPROTECTED</i>, consulte la "opciones de configuración" página.</p>
<p>Veo mensajes de advertencia de Telegraf parecidos a los siguientes: <i>W! [Inputs.diskio] No se puede recopilar el nombre del disco para "vdc": Error al leer /dev/vdc: No tal archivo o directorio</i></p>	<p>Para el operador de supervisión de Kubernetes, estos mensajes de advertencia son benignos y se pueden ignorar con seguridad. Alternativamente, edite la sección telegraf en AgentConfiguration y establezca <i>runDsPrivileged</i> en true. Para obtener más información, consulte la "opciones de configuración del operador".</p>

Problema:	Pruebe lo siguiente:
<p>Mi pod de bits fluidos está fallando con los siguientes errores: [2024/10/16 14:16 23:23] [error] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno=24] Demasiados archivos abiertos [2024/16:2024:10/16 14] [error] fallo al inicializar la entrada tail,0 [16/23:10/16 14] [error] [error]</p>	<p>Intente cambiar la configuración de <i>fsnotify</i> en su clúster:</p> <pre data-bbox="820 258 1485 955">sudo sysctl fs.inotify.max_user_instances (take note of setting) sudo sysctl fs.inotify.max_user_instances=<something larger than current setting> sudo sysctl fs.inotify.max_user_watches (take note of setting) sudo sysctl fs.inotify.max_user_watches=<something larger than current setting></pre> <p>Reinicie el bit fluido.</p> <p>Nota: Para que estos ajustes sean persistentes en todos los reinicios de nodos, debe poner las siguientes líneas en <i>/etc/sysctl.conf</i></p> <pre data-bbox="820 1186 1485 1449">fs.inotify.max_user_instances=<something larger than current setting> fs.inotify.max_user_watches=<something larger than current setting></pre>

Puede encontrar información adicional en la ["Soporte técnico"](#) página o en el ["Matriz de compatibilidad de recopilador de datos"](#).

Recopilador de datos en caché

Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Memcached.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Seleccione Memcached.

Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las "Instalación del agente" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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
```

Configuración

La información se puede encontrar en el ["Wiki memcached"](#).

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Memcached	Servidor de espacio de nombres	Nombre del nodo IP	Aceptación de las solicitudes de autenticación gestionadas peticiones de autenticación fallidas bytes usados bytes leídos (por segundo) bytes escritos (por segundo) CAS Badval CAS Hits CAS Misses Flush Reqs (por segundo) Get Reqs (por segundo) Set Reqs (por segundo) resultados de conexión Touch Reqs (por segundo) (por segundo) Estructuras de conexión conexiones abiertas elementos almacenados actuales solicitudes de retirada aciertos (por segundo) solicitudes de retirada omisiones (por segundo) Eliminar solicitudes de eliminación Hits (por segundo) Eliminar solicitudes de falta (por segundo) elementos desalojados elementos válidos de expulsión Artículos caducados obtener Hits (por segundo) obtener omisiones (por segundo) Hash bytes usados hash Hash está ampliando el nivel de potencia Hash solicitudes incl. Aciertos (por segundo) Incr solicitudes de pérdidas (por segundo) Server Max bytes Listen Inescuchar Desactivado Num Reked Worker Threads total de conexiones abiertas total de elementos almacenados Touch Hits Touch Misses servidor tiempo activo

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

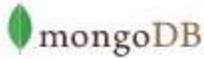
Recopilador de datos MongoDB

Data Infrastructure Insights usa este recopilador de datos para recopilar métricas de MongoDB.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Seleccione MongoDB.

Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.
2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las ["Instalación del agente"](#) instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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://10.10.0.0:27020
```

- 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
```

Configuración

La información se puede encontrar en el "[Documentación de MongoDB](#)".

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
MongoDB	Nombre de host del espacio de nombres		
Base de datos MongoDB	Nombre de base de datos del nombre de host del espacio		

Resolución de problemas

La información se puede encontrar en la ["Soporte técnico"](#) página.

Recopilador de datos de MySQL

Data Infrastructure Insights usa este recopilador de datos para recopilar métricas de MySQL.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Elija MySQL.

Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las ["Instalación del agente"](#) instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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
```

Configuración

La información se puede encontrar en el "[Documentación de MySQL](#)".

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
MySQL	Espacio de nombres MySQL Server	Nombre del nodo IP	Clientes cancelados (por segundo) conexiones canceladas (por segundo) bytes RX (por segundo) bytes TX (por segundo) comandos Admin (por segundo) Comandos Alter Event Commands Alter Function Alter Instance Commands Alter Procedure comandos Alter Server comandos Alter Table comandos Alter Tablespace comandos Alter comandos Alter comandos de usuario analizar comandos asignar a Keycache comandos Begin comandos Binlog comandos de procedimiento de llamada comandos Cambiar DB comandos Cambiar Master comandos Change Repl Filter comandos Check comandos Comandos de suma de comprobación comandos commit Crear comandos de base de datos Crear comandos de evento Crear comandos de índice Crear comandos de procedimiento Crear comandos de servidor Crear comandos de tabla Crear comandos de desencadenador Crear comandos UDF Crear comandos de usuario Crear comandos de vista errores de conexión SQL de bloque aceptar tablas de disco de tmp creados errores de retardo comandos Flush Handler commit InnoDB Buffer Pool bytes de datos bloques de claves no vaciados Key Read Requests de escritura de claves Escrituras de clave tiempo de ejecución

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

Recopilador de datos de netstat

Data Infrastructure Insights utiliza este recopilador de datos para recopilar métricas de Netstat.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Seleccione Netstat.

Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.
2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las ["Instalación del agente"](#) instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.

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
```

Configuración

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Netstat	UUID de nodo	Nombre del nodo IP	

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

Recopilador de datos nginx

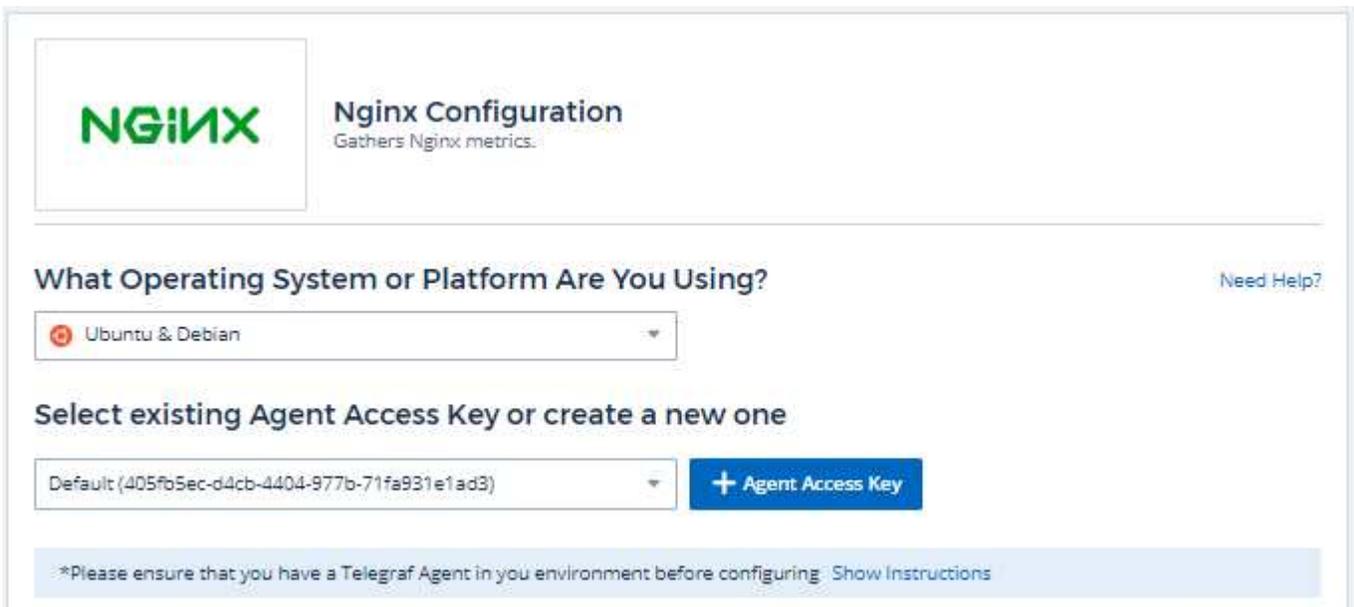
Data Infrastructure Insights usa este recopilador de datos para recopilar métricas de Nginx.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Elija Nginx.

Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las "[Instalación del agente](#)" instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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
```

Configuración

La recopilación de métricas nginx requiere que se active Nginx "`http_stub_status_module`".

Se puede encontrar información adicional en el "[Documentación de nginx](#)".

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Nginx	Servidor de espacio de nombres	Puerto de nombre de nodo IP	Acepta solicitudes de lectura gestionadas activas en espera de escritura

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

Recopilador de datos PostgreSQL

Data Infrastructure Insights usa este recopilador de datos para recopilar métricas de PostgreSQL.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Elija PostgreSQL.
 Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.
2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las ["Instalación del agente"](#) instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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
```

Configuración

La información se puede encontrar en el ["Documentación de PostgreSQL"](#).

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Servidor PostgreSQL	Servidor de bases de datos Namespace	Dirección IP del nodo de nombre	Búferes asignados búferes búferes búferes de backend búferes de sincronización de archivos de fondo búferes de punto de comprobación puntos de comprobación puntos de control de tiempo de sincronización puntos de control de tiempo de escritura solicitudes puntos de control Timed Max writed Clean
Base de datos PostgreSQL	Servidor de bases de datos Namespace	ID de nodo de nombre de nodo de base de datos IP	Bloques de tiempo de lectura bloques de tiempo de escritura bloques de aciertos bloques de lectura conflictos deinterlocks número de cliente Archivos temporales bytes Archivos temporales número de filas eliminadas filas devueltas filas insertadas filas devueltas transacciones confirmadas transacciones actualizadas Rollted

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

Recopilador de datos de Puppet Agent

Data Infrastructure Insights usa este recopilador de datos para recopilar métricas de Puppet Agent.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Elija Puppet.

Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.

2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las ["Instalación del agente"](#) instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica

recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.

4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.

Puppet Agent Configuration
Gathers Puppet agent metrics.

What Operating System or Platform Are You Using?

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

- 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
```

Configuración

Puede encontrar información en la "[Documentación de Puppet](#)"

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
---------	------------------	------------	------------------

Agente de Puppet	UUID de nodo de espacio de nombres	Nombre de nodo ubicación nodo IP Versión de Configstring Versión Puppet	Cambios total Eventos de fallo Eventos de éxito total Recursos cambiados Recursos fallidos Recursos no reinicializar Recursos Outofsync Recursos reiniciados Recursos programados Recursos omitidos Recursos tiempo total ancla tiempo de Configrecuperación tiempo de Crón tiempo de Exec tiempo de archivo tiempo de Filebucket tiempo de paquete Hora de programa tiempo de servicio tiempo de Sshauthorizedkey total Usuario de tiempo
------------------	------------------------------------	--	--

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

Recopilador de datos Redis

Data Infrastructure Insights usa este recopilador de datos para recopilar métricas de Redis. Redis es un almacén de estructura de datos en memoria de código abierto que se utiliza como base de datos, caché y agente de mensajes, y que admite las siguientes estructuras de datos: Cadenas, hashes, listas, conjuntos y mucho más.

Instalación

1. En **Observabilidad > Colectores**, haz clic en **+Recopilador de datos**. Seleccione Redis.

Seleccione el sistema operativo o la plataforma en la que está instalado el agente Telegraf.
2. Si aún no ha instalado un agente para la recopilación, o si desea instalar un agente para un sistema operativo o plataforma diferente, haga clic en *Mostrar instrucciones* para ampliar las ["Instalación del agente"](#) instrucciones.
3. Seleccione la clave de acceso del agente para utilizarla con este recopilador de datos. Puede agregar una nueva clave de acceso del agente haciendo clic en el botón **+ clave de acceso del agente**. Práctica recomendada: Utilice una clave de acceso de agente diferente sólo cuando desee agrupar recopiladores de datos, por ejemplo, por sistema operativo/plataforma.
4. Siga los pasos de configuración para configurar el recopilador de datos. Las instrucciones varían en función del tipo de sistema operativo o plataforma que utilice para recopilar datos.



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
```

Configuración

La información se puede encontrar en el "[Documentación de Reis](#)".

Objetos y contadores

Se recopilan los objetos siguientes y sus contadores:

Objeto:	Identificadores:	Atributos:	Puntos de datos:
Redis	Servidor de espacio de nombres		

Resolución de problemas

Puede encontrar información adicional en la ["Soporte técnico"](#) página.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.