Data Collector Reference - Services

Data Infrastructure Insights

NetApp
January 17, 2025

Sommaire

Data Collector Reference - Services

Collecte des données de nœud

Data Infrastructure Insights collecte les metrics à partir du nœud sur lequel vous installez un agent.

Installation

1. Dans **observabilité > Collectors**, choisissez un système d'exploitation/une plate-forme. Notez que l'installation d'un collecteur de données d'intégration (Kubernetes, Docker, Apache, etc.) configure également la collecte des données du nœud.
2. Suivez les instructions pour configurer l'agent. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés sous forme de metrics de nœud :

Objet :	Identifiants :	Attributs :	Points de données :
Système de fichiers de nœuds	Type de chemin d'accès de périphérique UUID de nœud	Nœud IP nœud Nom nœud mode OS	Inodes libres inodes libres nombre total d'inodes utilisé Total utilisé
Disque de nœud	Disque UUID de nœud	Nom de nœud IP de nœud OS	Temps d'E/S nombre total d'IOPS en cours lecture octets (par seconde) temps de lecture durée totale des lectures (par seconde) temps d'E/S pondéré durée totale des écritures (par seconde) temps d'écriture total des écritures (par seconde) durée actuelle de la file d'attente des disques temps d'écriture temps d'E/S de lecture
Processeur des nœuds	CPU UUID de nœud	Nom de nœud IP de nœud OS	Utilisation du CPU système utilisation du CPU utilisateur utilisation du CPU inactif utilisation du processeur interruption utilisation du CPU DPC utilisation du CPU

Objet :	Identifiants :	Attributs :	Points de données :
Nœud	UUID du nœud	Nom de nœud IP de nœud OS	Temps d'amorçage du noyau commutateurs de contexte du noyau (par seconde) interruption du noyau interruptions du noyau disponibles (par seconde) processus du noyau forgés (par seconde) Mémoire mémoire active mémoire active disponible mémoire totale mémoire disponible mémoire tampon mémoire cache limite mémoire cache mémoire vive comme mémoire non volatile mémoire libre mémoire haute mémoire libre mémoire haute capacité mémoire énorme taille de page mémoire énorme pages mémoire libre pages nombreuses pages mémoire libre mémoire totale mémoire faible mémoire disponible Table de pages mémoire mappée totale Mémoire partagée mémoire Bloc mémoire Bloc mémoire vive mémoire cache échange mémoire libre échange mémoire totale mémoire totale utilisée mémoire totale mémoire utilisée mémoire totale mémoire utilisée Vmalloc Bloc mémoire Vmalloc mémoire totale Vmalloc mémoire utilisée mémoire saturée mémoire filaire Retour mémoire totale mémoire mémoire Writeback mémoire mémoire tmp mémoire cache mémoire demande zéro pannes mémoire page mémoire pages mémoire Mémoire non paginée mémoire à l'origine mémoire à l'état principal mémoire à l'état de repos mémoire à la réserve mémoire à l'état normal processus à l'état

Objet :	Identifiants :	Attributs :	Points de données :
Réseau de nœuds	UUID de nœud d'interface réseau	OS de nœud Nom du nœud IP	Octets reçus octets envoyés paquets envoyés Outboud paquets rejetés erreurs Outboud paquets reçus paquets rejetés erreurs reçues paquets reçus erreurs paquets reçus paquets envoyés

Configuration

Des informations sur la configuration et le dépannage sont disponibles sur la "Configuration d'un agent" page.

Data Collector ActiveMQ

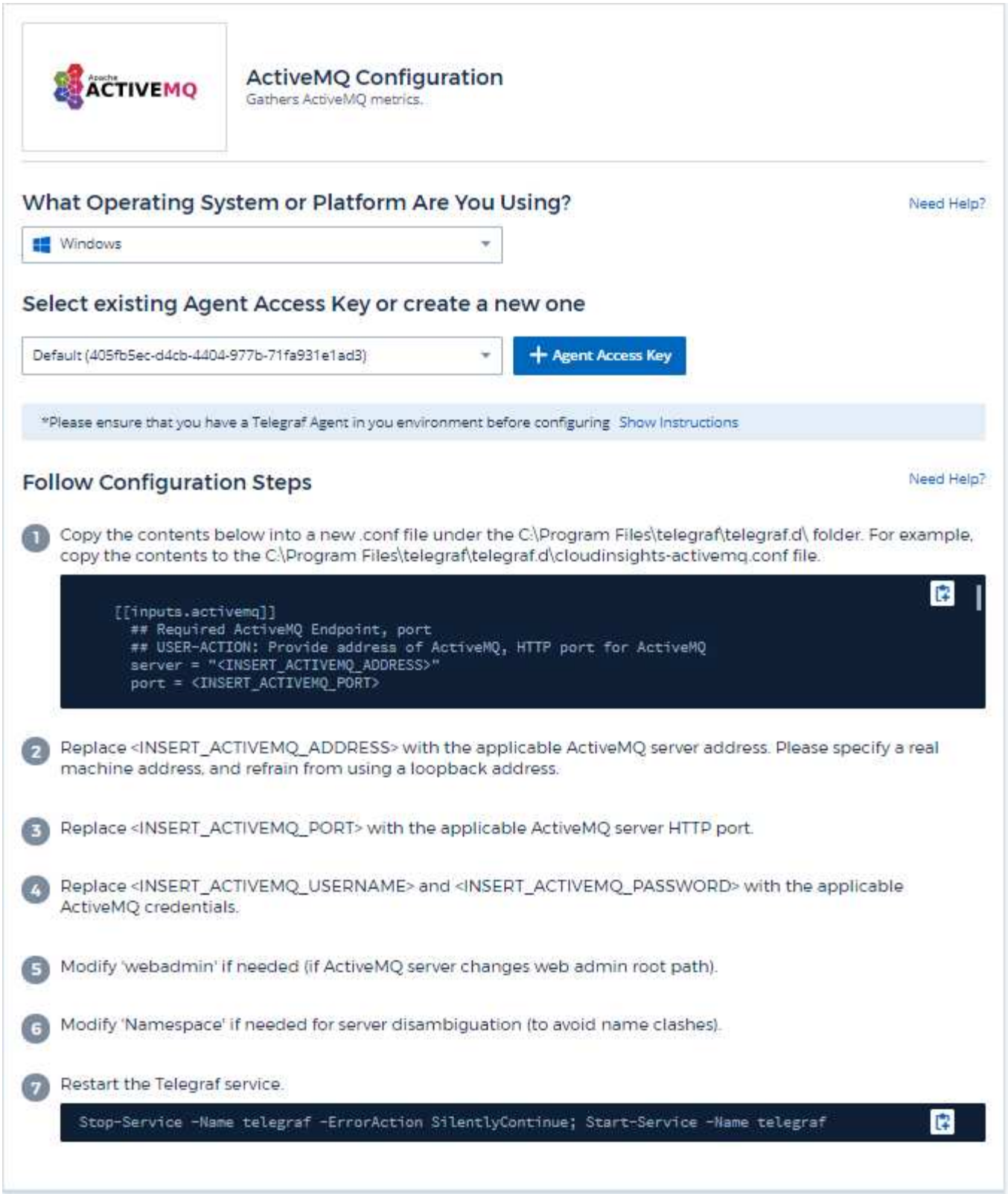
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir d'ActiveMQ.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez ActiveMQ.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Documentation ActiveMQ"

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
ActiveMQ Queue	Serveur de port de file d'attente d'espace de noms	UUID de nœud Nom du nœud IP	Nombre de consommateurs - nombre de files d'attente - nombre de files d'attente - taille de la file d'attente
Abonné ActiveMQ	ID client ID de connexion Port espace de noms du serveur	Est actif Nom du nœud de destination nœud IP nœud UUID Sélecteur de nœud d'exploitation	Nombre de files d'attente nombre de files d'attente expédiées taille de file d'attente nombre de files d'attente en attente taille de file d'attente
Thème ActiveMQ	Rubrique espace de noms du serveur de port	Nom de nœud nœud nœud IP nœud UUID de nœud OS	Nombre de consommateurs - nombre de files d'attente - taille du nombre de files d'attente

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Apache

Ce collecteur de données permet la collecte de données à partir des serveurs Apache de votre locataire.

Conditions préalables

- Votre serveur HTTP Apache doit être configuré et en cours d'exécution
- Vous devez disposer d'autorisations sudo ou administrateur sur votre hôte agent/machine virtuelle
- En général, le module Apache *mod_status* est configuré pour exposer une page à l'emplacement '/Server-status?auto' du serveur Apache. L'option *ExtendedStatus* doit être activée pour collecter tous les champs disponibles. Pour plus d'informations sur la configuration de votre serveur, reportez-vous à la documentation du module Apache : https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

Installation

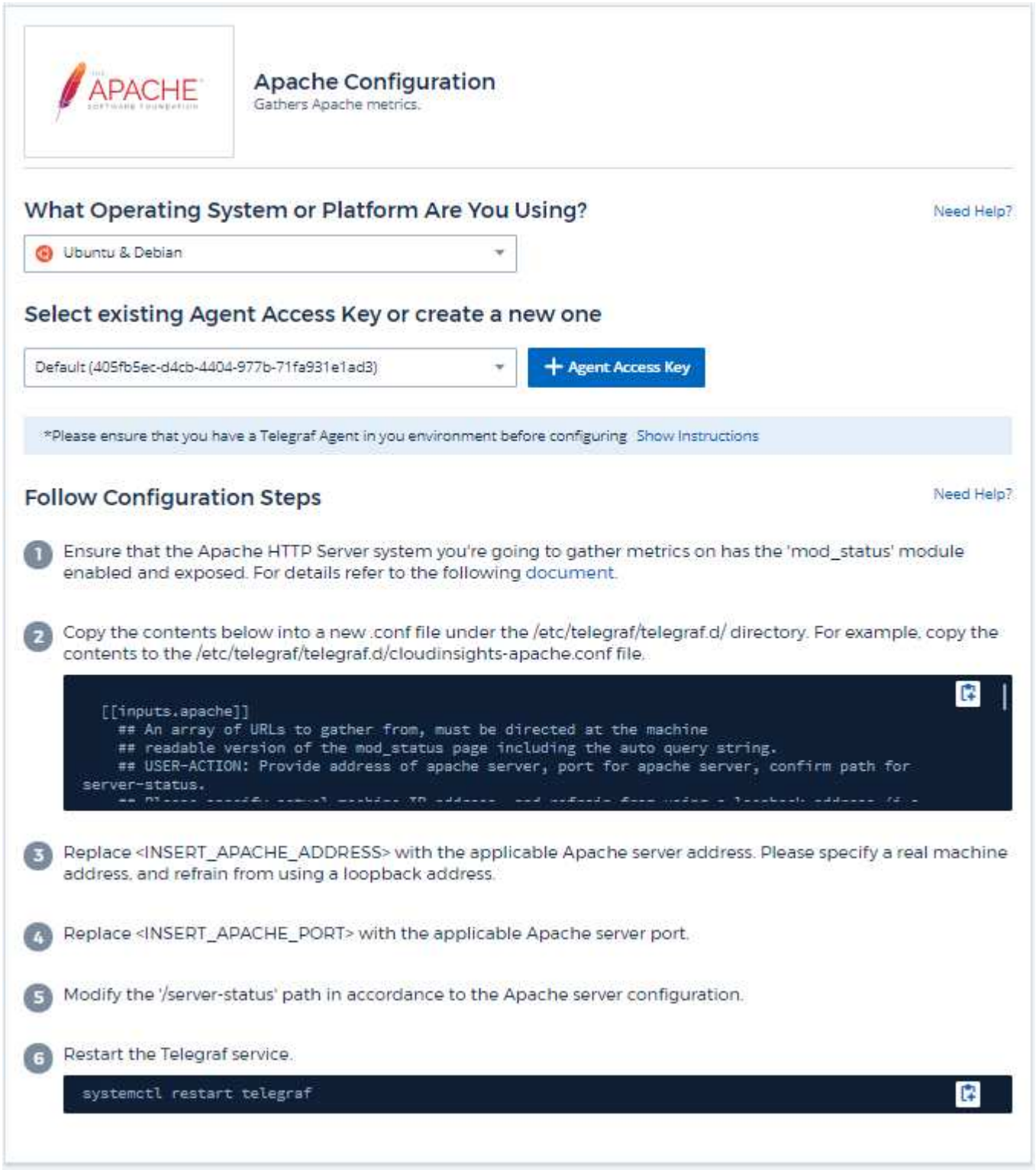
1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Apache.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique :

utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.

4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Le plug-in Telegraf pour le serveur HTTP Apache dépend du module 'mod_status' pour être activé. Lorsque

cette option est activée, le serveur HTTP d'Apache expose un noeud final HTML qui peut être affiché sur votre navigateur ou gratté pour l'extraction de l'état de toute la configuration du serveur HTTP d'Apache.

Compatibilité :

La configuration a été développée par le serveur HTTP Apache version 2.4.38.

Activation de mod_status :

L'activation et l'exposition des modules « od_status » implique deux étapes :

- Activation du module
- Exposition des stats à partir du module

Module d'activation :

Le chargement des modules est contrôlé par le fichier de configuration sous '/usr/local/apache/conf/httpd.conf'. Modifiez le fichier de configuration et annulez le commentaire des lignes suivantes :

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

Exposition des statistiques à partir du module :

L'exposition de 'mod_status' est contrôlée par le fichier de configuration sous '/usr/local/apache2/conf/extra/httpd-info.conf'. Assurez-vous que vous disposez des éléments suivants dans ce fichier de configuration (au moins, d'autres directives seront disponibles) :

```
# 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
```

Pour obtenir des instructions détaillées sur le module 'mod_status', reportez-vous au "Documentation Apache"

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Apache	Serveur d'espace de noms	Nœud Nom de nœud IP Port de configuration du serveur parent génération du serveur parent la continuité du serveur de génération MPM est en cours d'arrêt	Nombre de travailleurs occupés octets par requête par seconde UC enfants système processeur enfants charge UC utilisateur CPU système CPU utilisateurs connexions asynchrones fermeture connexions asynchrones connexion asynchrones maintien actif connexions asynchrones écriture connexions durée totale par demande travailleurs inactifs moyenne de charge (1 m dernier) moyenne de charge (15 m dernier) moyenne de charge (5 m dernier) Traitement des demandes par seconde Total des accès durée totale des Ko Tableau de bord fermeture Tableau de bord des recherches DNS Tableau de bord finition Tableau de bord nettoyage automatique Tableau de bord Tableau de bord garder actif Tableau de bord Tableau de bord Ouvrir Tableau de bord lecture Tableau de bord envoi Tableau de bord démarrage Tableau de bord en attente

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données consul

Data Infrastructure Insights utilise ce collecteur de données pour recueillir des mesures auprès de Consul.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Consul.

Si vous n'avez pas configuré un agent pour la collecte, vous êtes invité à "installez un agent"le faire sur votre locataire.

Si un agent est déjà configuré, sélectionnez le système d'exploitation ou la plate-forme approprié et cliquez sur **Continuer**.

2. Suivez les instructions de l'écran Configuration consul pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.

Configuration

Vous trouverez des informations dans le "Documentation consul".

Objets et compteurs pour consul

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Consul	Numéro de contrôle d'espace de noms nœud de service	Nœud IP nœud OS UUID Nom du nœud Nom du service Vérification Nom ID de service État	Avertissement de réussite critique

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Couchbase

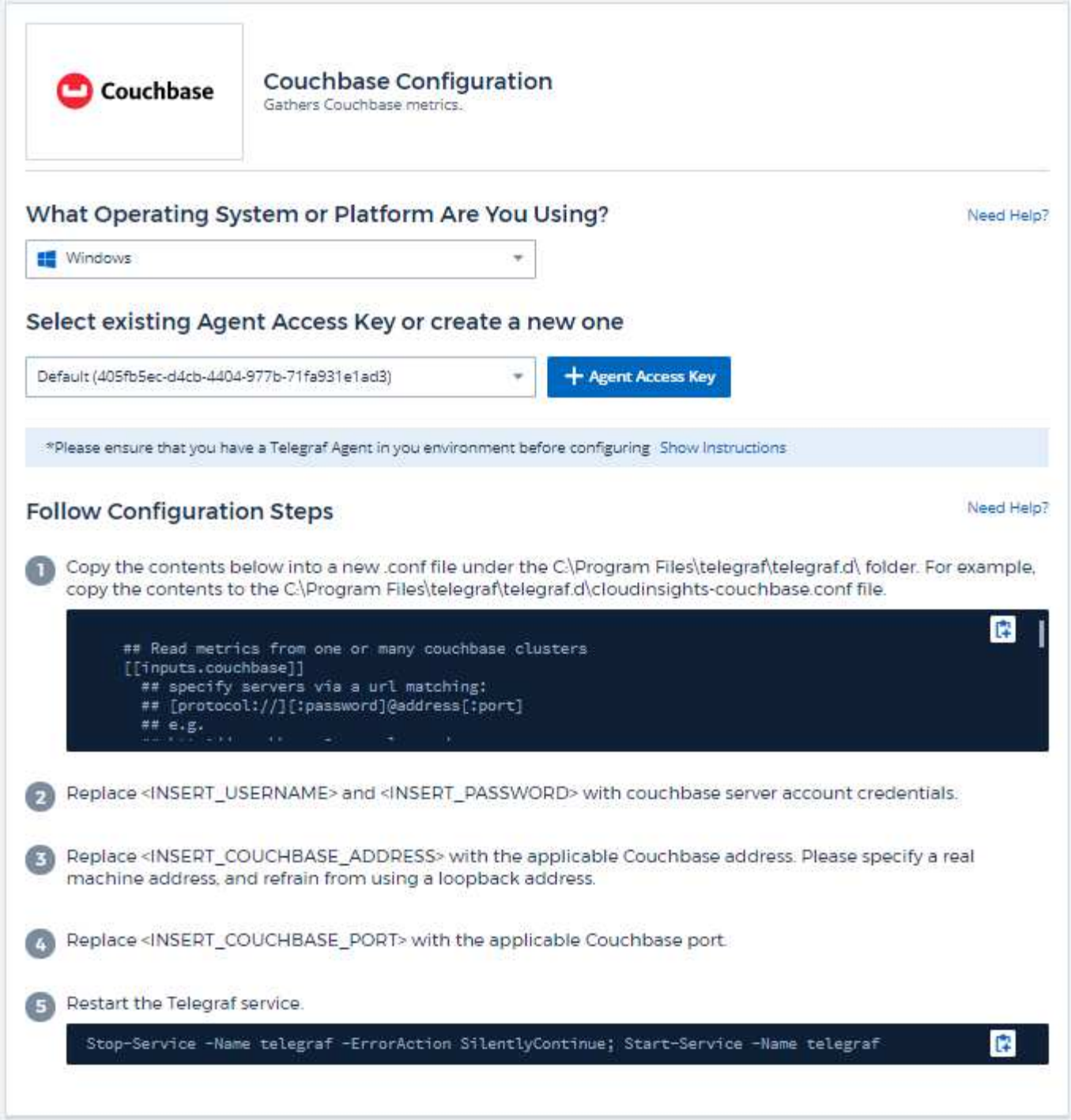
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de Couchbase.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Couchbase.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Documentation Couchbase".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Couchbase Node	Nom d'hôte du nœud Couchbase du cluster namespace	IP du nœud de nom de nœud	Mémoire mémoire mémoire disponible totale
Compartiment Couchbase	Cluster des compartiments d'espace de noms	IP du nœud de nom de nœud	Données utilisées Fetches Disk Used Item Count Memory Used opérations par seconde quota utilisé

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données CouchDB

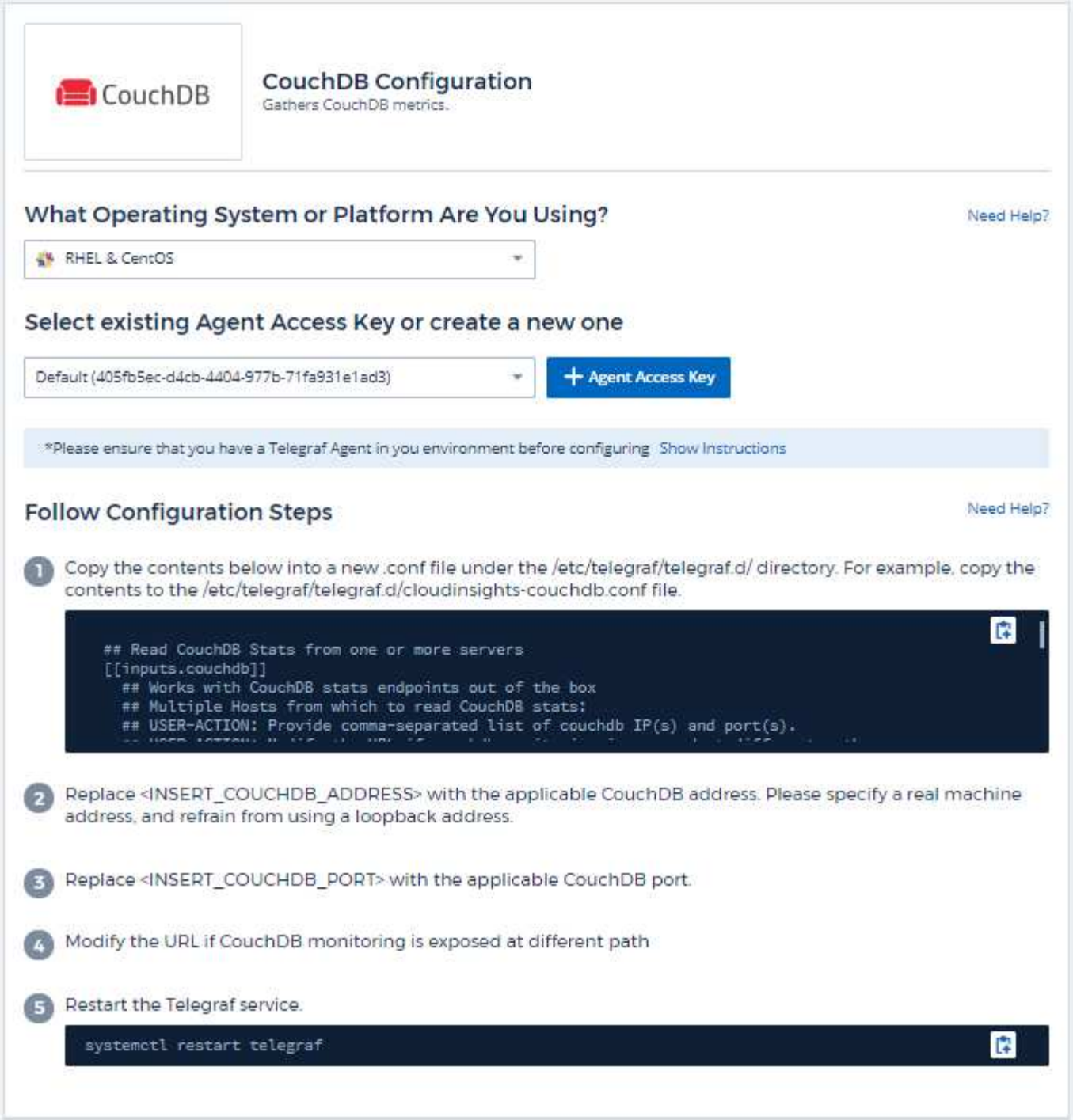
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de CouchDB.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez CouchDB.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Documentation CouchDB".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
CouchDB	Serveur d'espace de noms	IP du nœud de nom de nœud	Cache d'authentification Hits cache d'authentification Miss base de données lit base de données écrit bases Open fichiers système d'exploitation Max temps de demande min temps de demande httpd méthodes de demande httpd Copier méthodes de demande httpd suivre méthodes de demande httpd méthodes de requête post méthodes de requête httpd mettre les codes d'état 200 codes d'état 201 codes d'état 202 codes d'état 301 codes d'état 304 codes d'état 400 codes d'état 401 codes d'état 403 codes d'état 404 codes d'état 405 codes d'état 409 codes d'état 412 codes d'état 500

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Docker

Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de Docker.

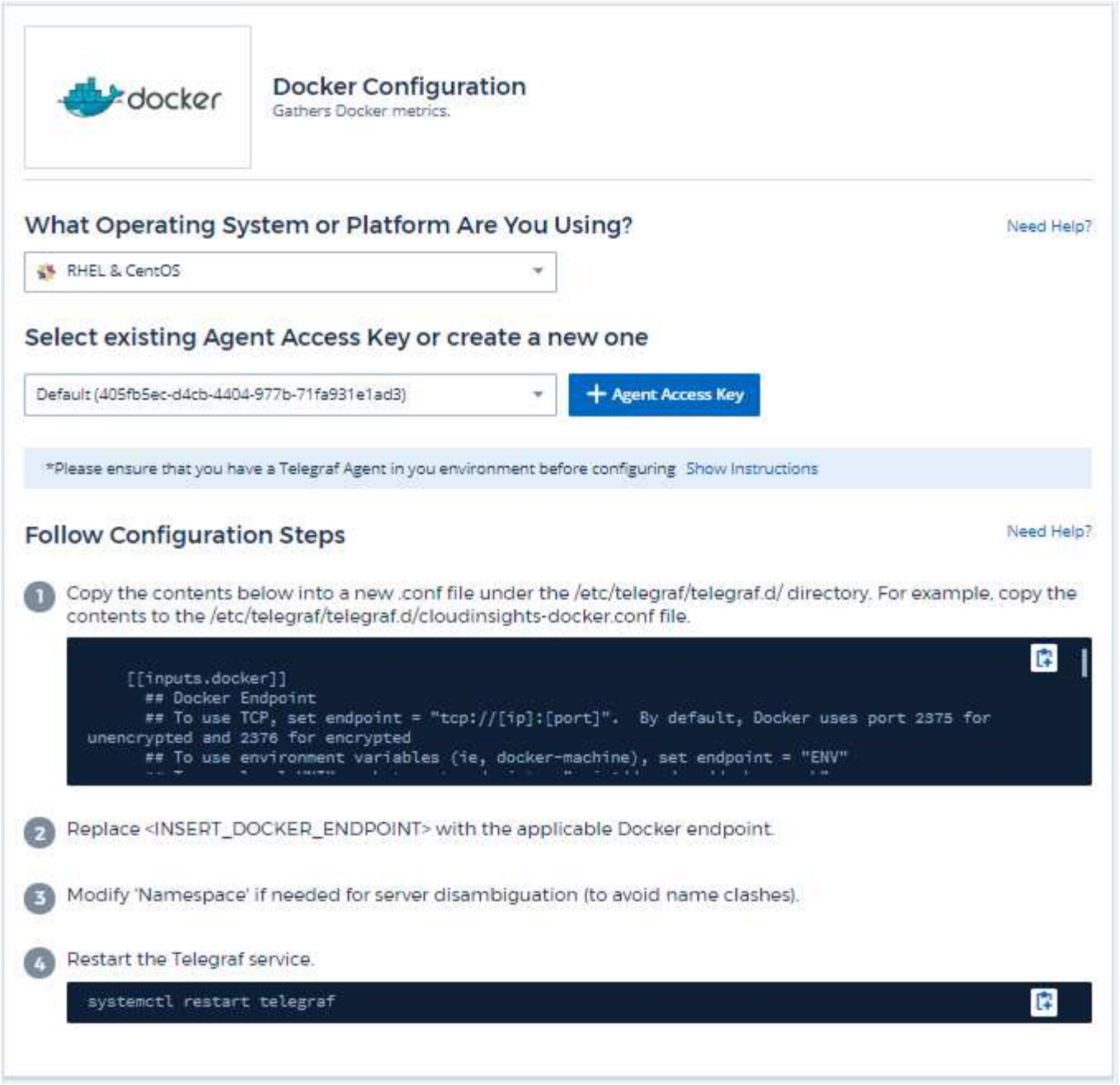
Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Docker.

   Si vous n'avez pas configuré un agent pour la collecte, vous êtes invité à "installez un agent"le faire sur votre locataire.

   Si un agent est déjà configuré, sélectionnez le système d'exploitation ou la plate-forme approprié et cliquez sur **Continuer**.

2. Suivez les instructions de l'écran de configuration de Docker pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Le plug-in d'entrée Telegraf pour Docker collecte des mesures via une socket UNIX ou un noeud final TCP spécifié.

Compatibilité

La configuration a été développée à partir de la version 1.12.6 de Docker.

Configuration

Accès à Docker via un socket UNIX

Si l'agent Telegraf s'exécute sur une base sans système d'exploitation, ajoutez l'utilisateur telegraf Unix au groupe docker Unix en exécutant ce qui suit :

```
 sudo usermod -aG docker telegraf
Si l'agent Telegraf s'exécute dans un pod Kubernetes, exposez le socket
Docker Unix en effectuant le mappage du socket dans le pod en tant que
volume, puis en le montant dans /var/run/docker.Sock. Par exemple, ajoutez
ce qui suit à PodSpec :
```

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

Ajoutez ensuite les éléments suivants au conteneur :

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

Notez que le programme d'installation Data Infrastructure Insights fourni pour la plateforme Kubernetes prend automatiquement en charge ce mappage.

Accès à Docker via un terminal TCP

Par défaut, Docker utilise le port 2375 pour un accès non chiffré et le port 2376 pour un accès crypté.

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Moteur Docker	Namespace Docker Engine	Noeud Nom noeud IP noeud UUID noeud OS Kubernetes Cluster version unité Docker	Conteneurs de mémoire conteneurs conteneurs utilisés conteneurs exécution de conteneurs CPU arrêtés routines Images Listener événements descripteurs de fichiers utilisés données disponibles Total des données utilisées métadonnées disponibles métadonnées totales utilisées nombre de métadonnées utilisées nombre total de blocs de données utilisés

Objet :	Identifiants :	Attributs :	Points de données :
Conteneur Docker	Nom du conteneur de l’espace de noms moteur Docker	Hachage en conteneurs Kubernetes ports de conteneur Kubernetes nombre de redémarrage du conteneur Kubernetes résiliation du message chemin de terminaison du conteneur Kubernetes politique de message de résiliation du conteneur Kubernetes Pod délai de grâce image conteneur Statut du conteneur version Nom du nœud Kubernetes Container chemin du journal Kubernetes Docker Type Kubernetes Pod Nom du pod Kubernetes espace de noms Kubernetes UID pod UID Kubernetes Sandbox ID nœud IP UUID Docker version Kubernetes IO Config vu Kubernetes IO Source OpenShift IO SCC Kubernetes Description Kubernetes Nom d’affichage balises OpenShift Kompose modèle de pod de service modèle Hash Controller révision modèle de pod modèle de hachage création de schéma de licence schéma de création de la date de création de schéma de licence URL de schéma de schéma de licence de schéma de schéma de schéma de nom de schéma Schéma URL du schéma du fournisseur version du schéma du schéma du fournisseur version Maintainer client Pod Kubernetes StatefulSet Nom du pod tenant webconsole Architecture autorité URL source Date de création RH hôte RH distribution étendue installation Résumé de l’exécution	Mémoire active mémoire anonyme active mémoire cache de fichiers active mémoire cache limite hiérarchique mémoire inactive mémoire inactive mémoire morte mémoire mappée fichier mémoire usage maximal mémoire page défaut mémoire principale panne mémoire paginée dans la mémoire mise en mémoire mémoire affectation de mémoire mémoire taille de l’ensemble mémoire interne taille de l’ensemble de mémoire énorme mémoire active totale Mémoire anonyme mémoire totale des fichiers actifs mémoire totale mémoire cache totale inactive mémoire totale des fichiers inactifs mémoire totale des fichiers mappés mémoire totale des pages défaut mémoire totale des pages mémoire principale des pannes mémoire totale des erreurs Total des pages en mémoire Total de la mémoire paginée taille totale des ensembles résidents taille totale des ensembles résidents taille totale des ensembles de mémoire énorme Total des données des résidents Mémoire inévitable mémoire inévitable mémoire usage mémoire pourcentage Code de sortie OOM Code de sortie PID tué démarré à Streak défaillant

Objet :	Identifiants :	Attributs :	Points de données :
Les E/S de bloc de conteneur Docker	Espace de noms Container Name Device Docker Engine	Hachage en conteneurs Kubernetes ports de conteneur Kubernetes nombre de redémarrage du conteneur Kubernetes résiliation du message chemin de terminaison du conteneur Kubernetes politique de message de résiliation du conteneur Kubernetes Pod délai de grâce image conteneur Statut du conteneur version Nom du nœud Kubernetes Container chemin du journal Kubernetes Docker Type Kubernetes Pod Nom du pod Kubernetes espace de noms Kubernetes UID de pod ID de test Kubernetes nœud IP UUID de nœud UUID de conteneur Docker version Kubernetes Config vu Kubernetes Config Source OpenShift SCC Description Kubernetes Nom d'affichage balises OpenShift Schema version modèle de pod modèle de hachage de révision de contrôleur génération de modèle de hachage Kompose de schéma de service Date de création de schéma de licence Nom de schéma de licence client du fournisseur Pod Kubernetes StatefulSet Nom du pod tenant webconsole Date de création Licence Architecture du fournisseur URL source faisant autorité RH build hôte RH composant distribution Scope installation Maintainer version Résumé Désinstaller VCS Type version schéma URL Schéma URL VCS version conteneur ID	Octets de service d'E/S recursive Async octets de service d'E/S en lecture récursive Sync octets de service d'E/S récursives octets de service d'E/S en écriture récursive Write Serviced E/S récursives Recursive Read ursive Read IO Serviced Recursive Write Serviced

Objet :	Identifiants :	Attributs :	Points de données :
Réseau de conteneurs Docker	Nom du conteneur de l’espace de noms moteur Docker réseau	Image conteneur conteneur conteneur version conteneur Nom de nœud nœud IP nœud UUID nœud OS K8s Cluster version ID de conteneur	RX a déposé RX octets RX erreurs RX paquets RX paquets TX a abandonné TX octets TX erreurs TX paquets TX

Objet :	Identifiants :	Attributs :	Points de données :
Processeur du conteneur Docker	Namespace Container Name CPU Docker Engine	Hachage en conteneurs Kubernetes ports de conteneur Kubernetes nombre de redémarrage du conteneur Kubernetes nombre de messages de terminaison du conteneur Kubernetes politique de message de terminaison du conteneur Kubernetes délai de grâce période de suppression de la configuration Kubernetes Config. Vue de l'état du conteneur OpenShift SCC image conteneur conteneur version Nom du nœud Kubernetes Container Log Path Kubernetes Container name Kubernetes Docker Type Kubernetes Pod Name Kubernetes Pod espace de noms Kubernetes Pod UID Kubernetes Sandbox ID noeud IP nœud UUID nœud OS Kubernetes Cluster version Kubernetes Description Kubernetes Nom d'affichage OpenShift Tags Schema version Pod modèle Hash Controller Revision modèle Hash Pod génération Kompose Service Schema Date de création Nom de schéma de licence Schéma Vendor Customer Pod Kubernetes StatefulSet Pod Name tenant webconsole Date de création Licence Vendor Architecture autorité Source URL RH build Host RH composant distribution Scope installation Maintainer version Résumé Désinstaller VCS Ref Type version schéma URL schéma URL VCS version conteneur ID	Périodes de restriction périodes de restriction périodes de restriction durée de restriction utilisation en mode noyau utilisation en mode utilisateur pourcentage utilisation du système Total

Dépannage

Problème :	Essayer :
Après avoir suivi les instructions de la page de configuration, je ne vois pas mes metrics Docker dans Data Infrastructure Insights.	Vérifiez les journaux de l'agent Telegraf pour voir s'il signale l'erreur suivante : E! Erreur dans le plug-in [inputs.docker] : obtention de l'autorisation refusée lors de la tentative de connexion à la socket du démon Docker si c'est le cas, suivez les étapes nécessaires pour fournir l'accès de l'agent Telegraf au socket Docker Unix, comme indiqué ci-dessus.

Vous trouverez des informations supplémentaires sur la "Assistance" page.

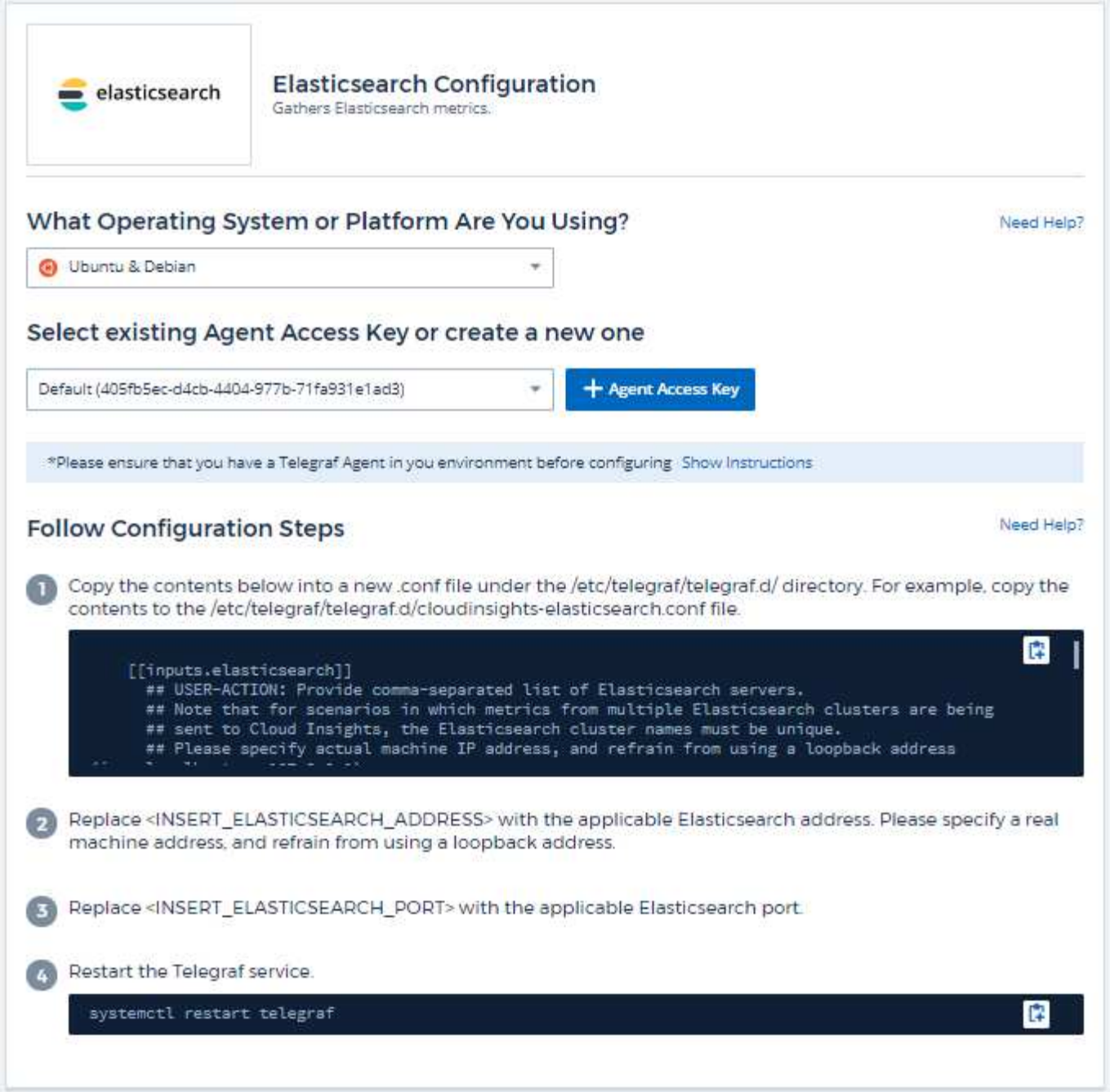
Collecteur de données Elasticsearch

Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de Elasticsearch.

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Elasticsearch.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Documentation relative à Elasticsearch".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :
Cluster Elasticsearch	Cluster de namespace	Nom de nœud IP du nœud État du cluster

Objet :	Identifiants :	Attributs :
Nœud Elasticsearch	Nom du nœud ES du cluster d'espace de noms noeud ES noeud IP noeud ES	ID de zone

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Flink

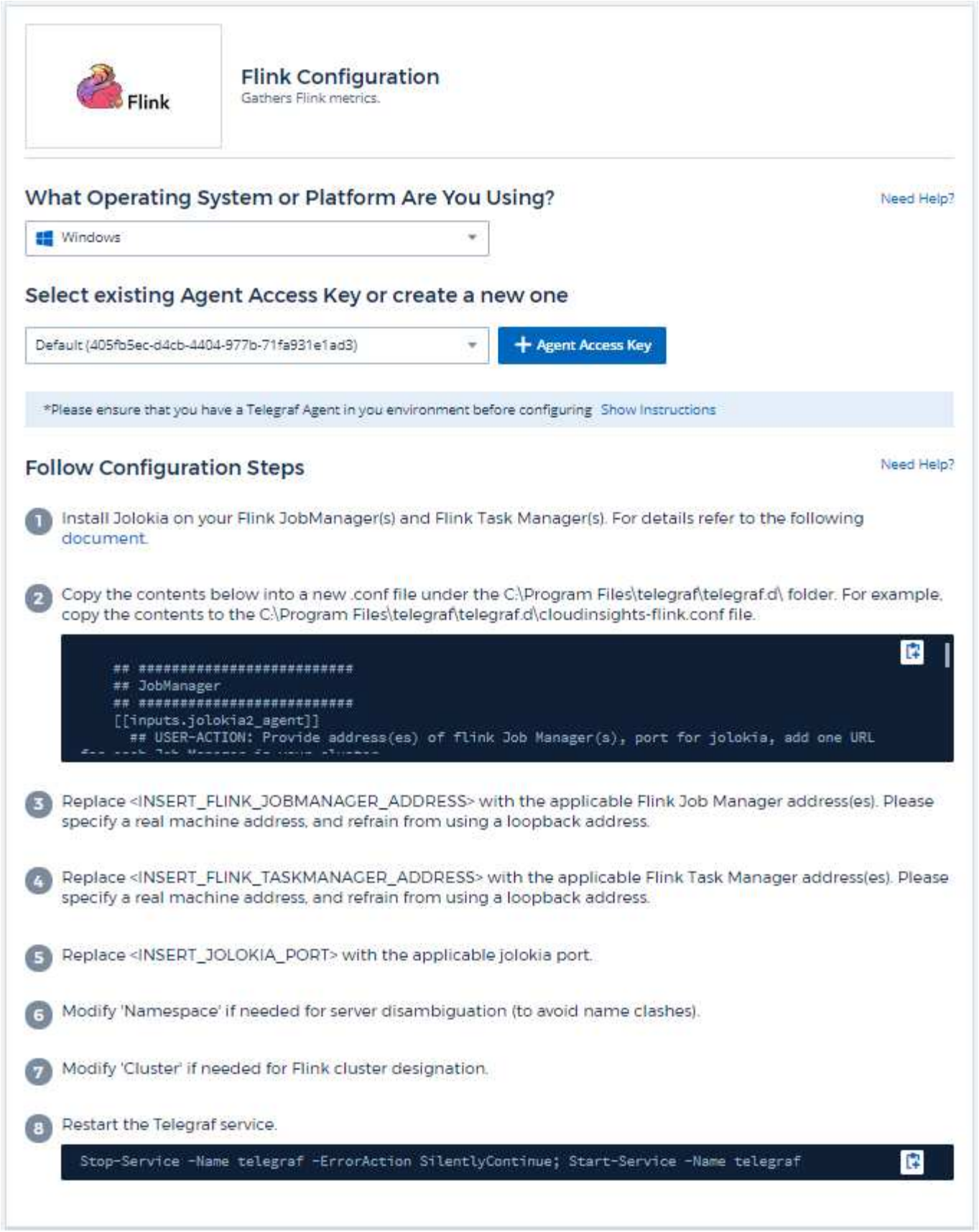
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de Flink.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Flink.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Un déploiement de Flink complet implique les composants suivants :

JobManager : système principal de Flink. Coordonne une série de gestionnaires de tâches. Dans une configuration haute disponibilité, le système aura plusieurs JobManager. TaskManager : c'est là que les opérateurs Flink sont exécutés. Le plug-in Flink est basé sur le plug-in Jolokia de telegraf. Par exemple, pour collecter des informations de tous les composants de Flink, JMX doit être configuré et exposé via Jolokia sur tous les composants.

Compatibilité

La configuration a été développée par rapport à la version 1.7.0 de Flink.

Configuration

Bol d'agent Jolokia

Pour tous les composants individuels, une version du fichier JAR de l'agent Jolokia doit être téléchargée. La version testée était "Agent de Jolokia 1.6.0".

Les instructions ci-dessous supposent que le fichier jar téléchargé (jolokia-jvm-1.6.0-agent.jar) est placé sous l'emplacement '/opt/flink/lib/'.

JobManager

Pour configurer JobManager de manière à exposer l'API Jolokia, vous pouvez configurer la variable d'environnement suivante sur vos nœuds, puis redémarrer JobManager :

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
Vous pouvez choisir un autre port pour Jolokia (8778). Si vous avez un IP
interne pour verrouiller Jolokia sur vous pouvez remplacer le 0.0.0.0
"tout capturer" par votre propre IP. Notez que cette adresse IP doit être
accessible à partir du plug-in telegraf.
```

Gestionnaire des tâches

Pour configurer TaskManager(s) pour exposer l'API Jolokia, vous pouvez configurer la variable d'environnement suivante sur vos nœuds, puis redémarrer TaskManager :

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
Vous pouvez choisir un autre port pour Jolokia (8778). Si vous avez un IP
interne pour verrouiller Jolokia sur vous pouvez remplacer le 0.0.0.0
"tout capturer" par votre propre IP. Notez que cette adresse IP doit être
accessible à partir du plug-in telegraf.
```

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Gestionnaire de tâches Flink	Serveur d’espace de noms de cluster	Nom du nœud ID du gestionnaire de tâches IP du nœud	Segments de mémoire disponibles réseau Total des segments de mémoire Garbage Collection PS MarkSweep nombre de déchets collecte PS MarkSweep temps Garbage Collection PS Svenge Combage Collection PS Scravenge temps démon de récupération mémoire vive mémoire vive mémoire vive mémoire vive mémoire vive mémoire vive mémoire vive maximale nombre de threads utilisés nombre de threads maximum nombre de threads Total démarré
Travail de cartouche	ID du travail du serveur d’espace de noms de cluster	Nom du nœud Nom du travail noeud IP dernier point de contrôle chemin externe heure de redémarrage	Temps d’arrêt redémarrage complet dernière alignement du point de contrôle durée du dernier point de contrôle Date du dernier point de contrôle taille nombre de points de contrôle terminés nombre de points de contrôle en cours nombre de points de contrôle en cours nombre de points de contrôle disponibilité

Objet :	Identifiants :	Attributs :	Points de données :
Gestionnaire des travaux de Flink	Serveur d’espace de noms de cluster	IP du nœud de nom de nœud	Garbage Collection PS MarkSweep nombre Garbage Collection PS MarkSweep temps Garbage Collection PS Scravenge nombre Garbage Collection PS Scravenge temps mémoire Heap mémoire vive mémoire vive mémoire vive mémoire vive saturée nombre maximum de mémoire utilisée nombre de tâches enregistrées gestionnaires nombre de tâches exécution tâches nombre de tâches nombre de threads disponibles emplacements de tâches du démon total Nombre maximum de threads nombre total de threads démarré

Objet :	Identifiants :	Attributs :	Points de données :
Tâche de Flink	ID de tâche d'espace de noms de cluster	Nom du nœud du serveur Nom du travail sous-index des tâches ID de la tâche tentative Numéro Nom de la tâche ID du gestionnaire des tâches noeud IP filigrane actuel	Tampons dans utilisation de pool tampons dans longueur de file tampons utilisation de pool tampons utilisation de pool tampons sortie longueur de file d'attente tampons dans nombre local Buffers dans local nombre par seconde nombre de tampons dans local par seconde nombre de taux nombre de tampons dans nombre distant tampons dans nombre distant par seconde nombre de tampons dans Remote par distant Second Rate Number tampons Out Number tampons Out Number Buffers Out par seconde Count Number Buffers Out par seconde Rate Number Bytes in local Number Bytes in local par seconde Count Number Bytes in local par seconde Rate Number Bytes in Remote Number Bytes in Remote Number Bytes in Remote per second Count Number Bytes in Remote Par seconde Numéro de taux octets hors nombre octets hors par seconde nombre nombre octets hors par seconde Numéro de taux enregistrements nombre enregistrements en nombre en nombre par seconde nombre enregistrements en nombre de taux en nombre de seconde nombre de taux enregistrements hors nombre par seconde nombre de nombres enregistrements hors nombre par seconde nombre de nombres enregistrements hors taux par seconde

Objet :	Identifiants :	Attributs :	Points de données :
Opérateur de tâche Flink	Nom du cluster ID de tâche ID d'opérateur ID de tâche	Nom du noeud du serveur Nom du travail Nom de l'opérateur sous-index des tâches ID de la tâche tentative Numéro Nom de la tâche ID du gestionnaire des tâches IP du noeud	Watermark Current Input Current Output Watermark Number enregistrements en nombre enregistrements en nombre enregistrements par seconde nombre nombre enregistrements en par seconde nombre de débits en dehors nombre enregistrements en dehors par seconde nombre d'enregistrements en dehors par seconde nombre de débits en retard enregistrements en chute partitions attribuées octets en retard latence de validation de taux en moyenne Le taux maximal de validation a échoué les validations de connexion a réussi le nombre de connexions de fermeture nombre de connexions nombre de taux de création de connexion durée de récupération moyenne de latence de récupération débit maximal taille de récupération taille de récupération moyenne de l'accélérateur temps de récupération moyenne de l'accélérateur vitesse de transfert max. Taux de pulsation nombre d'octets entrants taux d'E/S moy Rapport d'attente temps d'attente d'E/S moy (ns) temps d'assemblage temps d'attente moy. Dernier Heartbeat ago débit d'E/S débit d'octets sortant enregistrements taux de consommation décalage max enregistrements par demande débit moyen taille de demande moyenne vitesse de réponse max. Sélection temps de synchronisation de taux moyenne réponse

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Hadoop

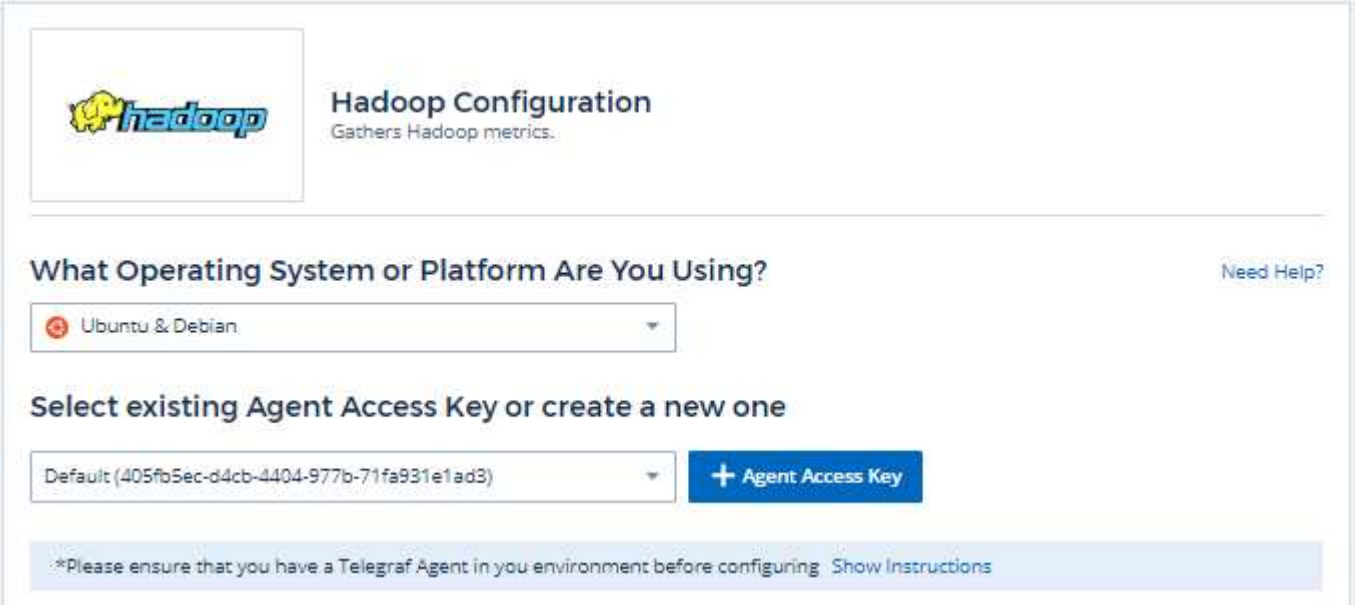
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de Hadoop.

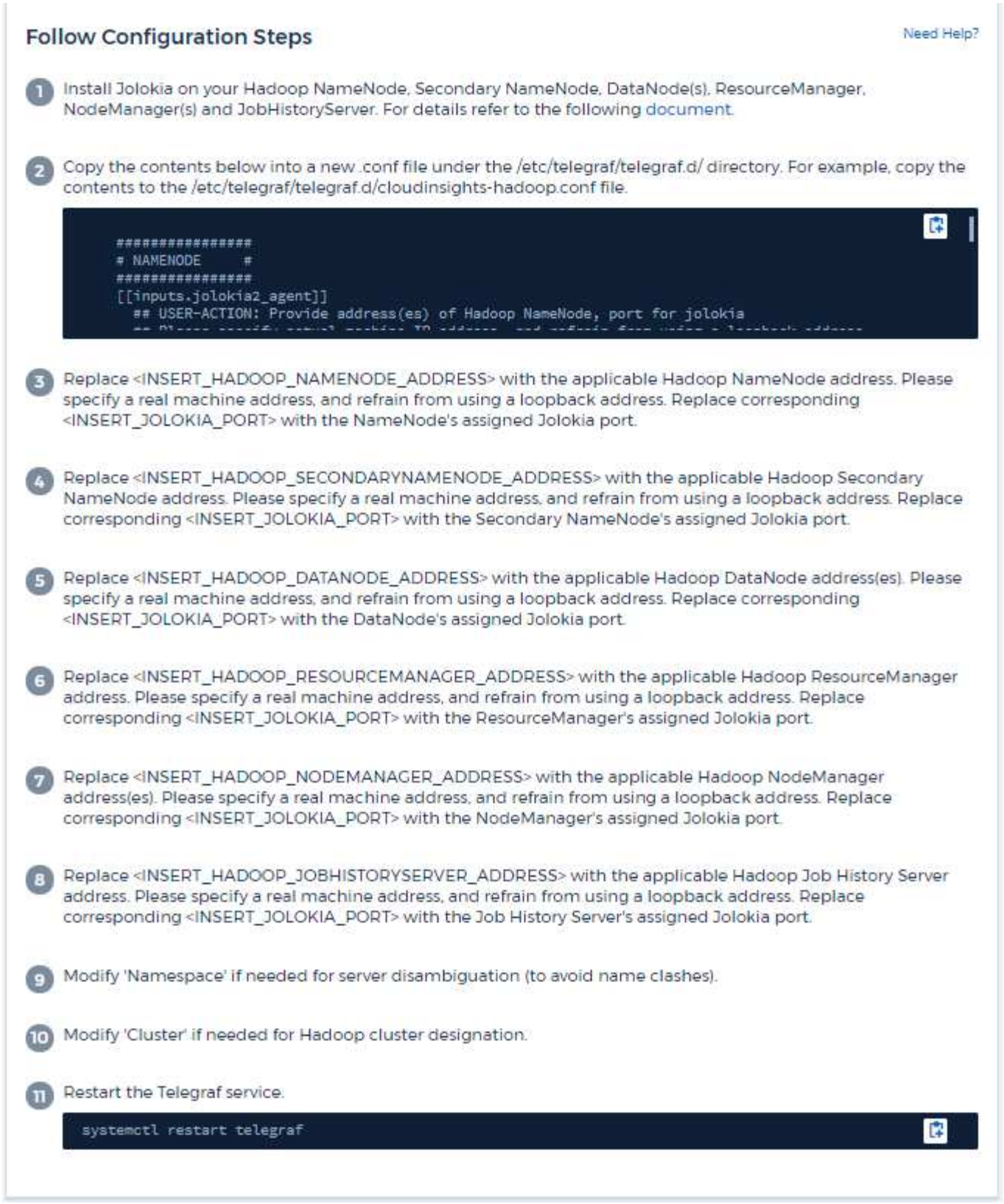
Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Avec Hadoop

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.





Configuration

Un déploiement Hadoop complet nécessite les composants suivants :

- NameNode : système principal Hadoop Distributed File System (HDFS). Coordonne une série de DataNodes.

- Second NameNode : basculement à chaud pour le NameNode principal. Dans Hadoop, la promotion vers NameNode n'a pas lieu automatiquement. Second NameNode collecte les informations du NameNode pour être prêt à être promu au besoin.
- DataNode : propriétaire réel des données.
- ResourceManager : le système principal de calcul (Yarn). Coordonne une série de gestionnaires de nœud.
- NodeManager : la ressource pour le calcul. Emplacement réel pour l'exécution des applications.
- JobHistoriyServer : responsable du traitement de toutes les requêtes liées à l'historique des travaux.

Le plug-in Hadoop est basé sur le plug-in Jolokia de telegraf. Par exemple, pour collecter des informations à partir de tous les composants Hadoop, JMX doit être configuré et exposé via Jolokia sur tous les composants.

Compatibilité

La configuration a été développée à partir de la version Hadoop 2.9.2.

Configuration

Bol d'agent Jolokia

Pour tous les composants individuels, une version du fichier JAR de l'agent Jolokia doit être téléchargée. La version testée était "Agent de Jolokia 1.6.0".

Les instructions ci-dessous supposent que le fichier jar téléchargé (jolokia-jvm-1.6.0-agent.jar) est placé sous l'emplacement '/opt/hadoop/lib/'.

Nom de nœud

Pour configurer NameNode afin d'exposer l'API Jolokia, vous pouvez configurer les éléments suivants dans <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.
```

Nom de nœud secondaire

Pour configurer le NameNode secondaire pour exposer l'API Jolokia, vous pouvez configurer les éléments suivants dans <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.
```

Nœud de données

Pour configurer les DataNodes pour exposer l'API Jolokia, vous pouvez configurer les éléments suivants dans <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

Pour configurer ResourceManager pour exposer l'API Jolokia, vous pouvez configurer les éléments suivants dans <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.
```

Gestionnaire de nœud

Pour configurer les gestionnaires de nœud afin d'exposer l'API Jolokia, vous pouvez configurer les éléments suivants dans <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.
```

JobHistoriyServer

Pour configurer JobHistoriyServer afin d'exposer l'API Jolokia, vous pouvez configurer les éléments suivants dans <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.
```

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :
Nom de nœud secondaire Hadoop	Serveur d'espace de noms de cluster	Noeud Nom noeud IP Compile Info version
Hadoop NodeManager	Serveur d'espace de noms de cluster	IP du nœud de nom de nœud
Gestionnaire de ressources Hadoop	Serveur d'espace de noms de cluster	IP du nœud de nom de nœud
Nœud de données Hadoop	Serveur d'espace de noms de cluster	Version de l'ID de cluster IP du nœud de nom de nœud
Nom de nœud Hadoop	Serveur d'espace de noms de cluster	Nom du nœud Nom de la transaction IP ID de transaction dernière heure écrite depuis la dernière édition de l'état HA fichier Etat du système Etat du système ID de bloc ID de groupe Infos de cluster version distincte nombre de versions
Hadoop JobHistoriyServer	Serveur d'espace de noms de cluster	IP du nœud de nom de nœud

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données HAProxy

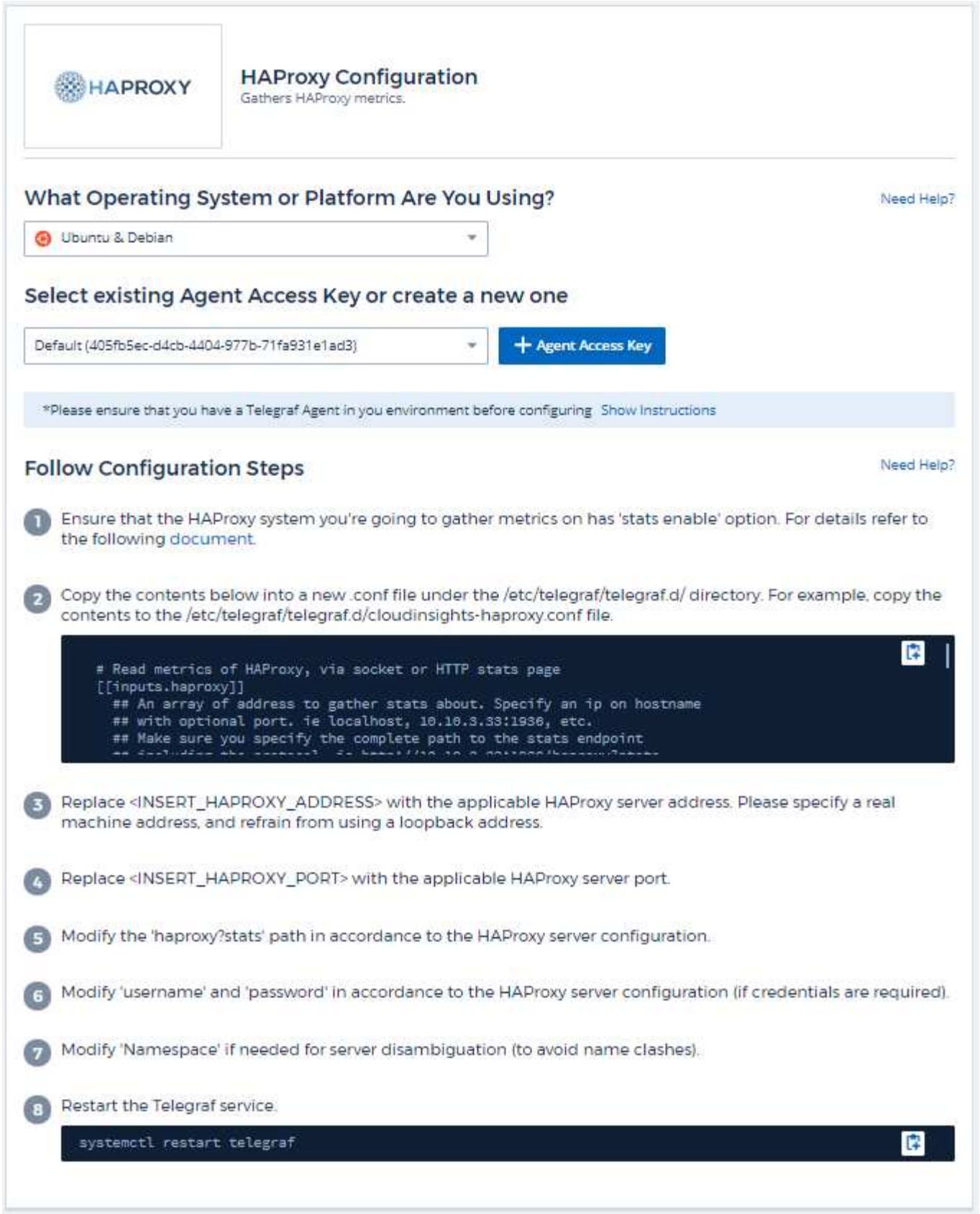
Data Infrastructure Insights utilise ce collecteur de données pour collecter des mesures à partir de HASProxy.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez HASProxy.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Le plug-in de Telegraf pour HAProxy repose sur l'activation des statistiques HAProxy. Il s'agit d'une configuration intégrée dans HAProxy, mais elle n'est pas prête à l'emploi. Lorsqu'il est activé, HAProxy expose

un noeud final HTML qui peut être affiché sur votre navigateur ou gratté pour extraction de l'état de toutes les configurations HAProxy.

Compatibilité :

La configuration a été développée par HAProxy version 1.9.4.

Configuration :

Pour activer les statistiques, modifiez votre fichier de configuration hproxy et ajoutez les lignes suivantes après la section « attaques », en utilisant votre propre utilisateur/mot de passe et/ou URL de proxy :

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

Voici un exemple de fichier de configuration simplifié avec des statistiques activées :

```
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
```

Pour obtenir des instructions complètes et à jour, reportez-vous au "Documentation HABProxy".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
HAVANCHAproxy frontal	Proxy d'adresse d'espace de noms	Noeud IP Nom de noeud ID proxy mode ID de processus sessions limite de taux sessions ID de serveur Etat limite de limite de nombre de sessions	Octets en octets hors cache Hits cache recherches cache octets de compression Bytes de compression Bytes de compression réponses de compression taux de connexion nombre maximal de demandes refusées par règle de connexion demandes refusées par des problèmes de sécurité réponses refusées par des demandes de sécurité refusées par la règle de session demandes d'erreurs réponses 1xx Réponses 2xx réponses 3xx réponses 4xx réponses 5xx autres demandes interceptées sessions Rate sessions demandes Rate Max demandes Rate demandes Rate nombre max sessions nombre max sessions nombre total sessions nombre total de requêtes nombre de réécritures

Objet :	Identifiants :	Attributs :	Points de données :
Serveur HAProxy	Serveur proxy d'adresse d'espace de noms	Nœud Nom du nœud IP heure de vérification de la vérification de la configuration de chute Vérification de la valeur de l'état Vérification de l'état de l'état ID du proxy dernière modification de la dernière session mode de l'heure de la dernière session ID du processus ID du serveur poids de l'état	Serveurs actifs serveurs de sauvegarde octets en octets hors octets Vérification Downs échec client liaisons connexion temps moyen d'arrêt Total réponses refusées erreurs de connexion réponses 1xx réponses 2xx réponses 3xx réponses 4xx réponses 5xx autres réponses serveur sélectionné File d'attente totale de la file d'attente actuelle durée moyenne des sessions par Seconde sessions par seconde Max Connection Reuse temps de réponse sessions moyennes sessions Max Server Transfer interrompt sessions Total sessions Total Time moyenne demandes rerépartit les demandes nouvelles tentatives réécritures

Objet :	Identifiants :	Attributs :	Points de données :
Système back-end HANProxy	Proxy d'adresse d'espace de noms	Noeud IP Nom de noeud ID proxy dernière modification heure dernière session mode temps processus ID de serveur sessions limite poids d'état	Serveurs actifs serveurs de sauvegarde octets en octets en octets en octets en cache Hits cache recherches cache Check Downs client abandonne les octets de compression ignorés octets de compression réponses de compression connexions temps moyen de connexion nombre de demandes refusées par des problèmes de sécurité réponses refusées par des problèmes de sécurité erreurs de connexion réponses aux erreurs de réponse 1xx réponses 2xx réponses 3xx réponses 4xx réponses 5xx autres réponses serveur sélectionné File d'attente totale file d'attente actuelle maximale file d'attente moyenne sessions par seconde nombre max demandes durée moyenne de la connexion réutilisation nombre total de sessions nombre moyen de sessions transfert serveur nombre total de sessions nombre total de sessions nombre total de sessions nombre total de fois nombre de requêtes redistribue les demandes de nouvelles Réécrit

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données JVM

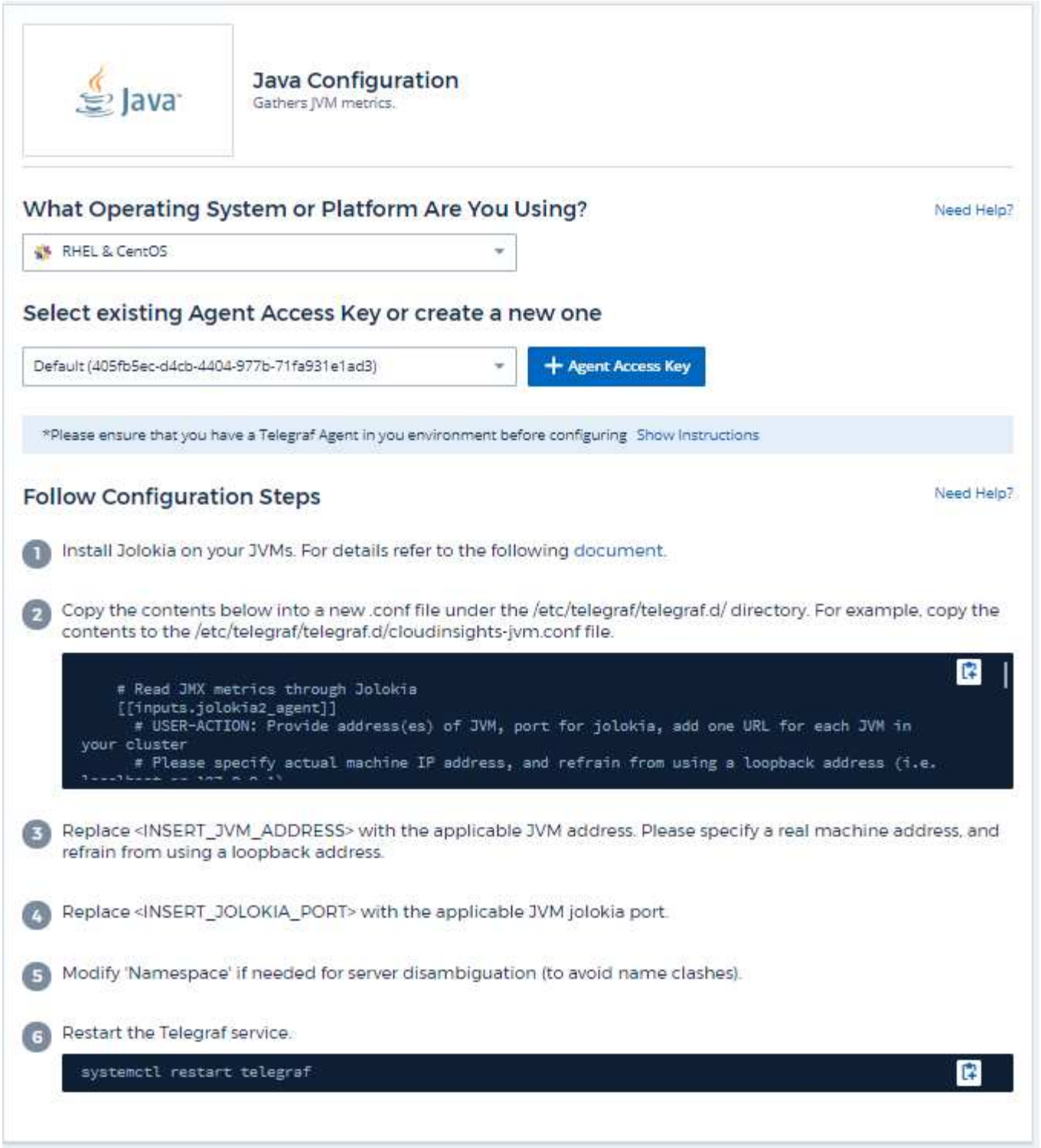
Data Infrastructure Insights utilise ce collecteur de données pour collecter des mesures à partir de JVM.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez JVM.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans "Documentation de l'JVM".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
JVM	JVM d’espace de noms	Architecture OS Nom OS version OS spécification d’exécution spécification d’exécution version spécification d’exécution Vendor version Uptime Runtime Nom VM Runtime VM Runtime version vendeur Nom du nœud IP	Classe chargée Total de la mémoire non chargée de la classe chargée mémoire vive mémoire vive mémoire vive mémoire vive mémoire vive utilisée mémoire maximale mémoire vive mémoire vive mémoire non mémoire non résolue mémoire non Heap mémoire non mémoire non mémoire vive objets de mémoire non utilisée en attente Finalisation processeurs OS disponibles taille de mémoire virtuelle OS non résolue Taille de la mémoire physique espace libre du système d’exploitation taille de l’espace libre du système d’exploitation nombre de descripteurs de fichier ouverts du système d’exploitation nombre de descripteurs de fichier du processeur du système d’exploitation charge du système d’exploitation CPU du système d’exploitation charge système d’exploitation taille moyenne de la mémoire physique totale du système d’exploitation nombre total de threads nombre de pics de threads Thread Count Thread Total Started Count Garbage Collector Copy Count Garbage Collector Copy collecte Time Garbage Collector Mark-balayage Collection Count Garbage Collector Mark-balayage collecte temps collecteur d’ordures G1 Old Generation Collection temps collecteur d’ordures ancien génération G1 Young Generation Collection Count Garbage

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Kafka

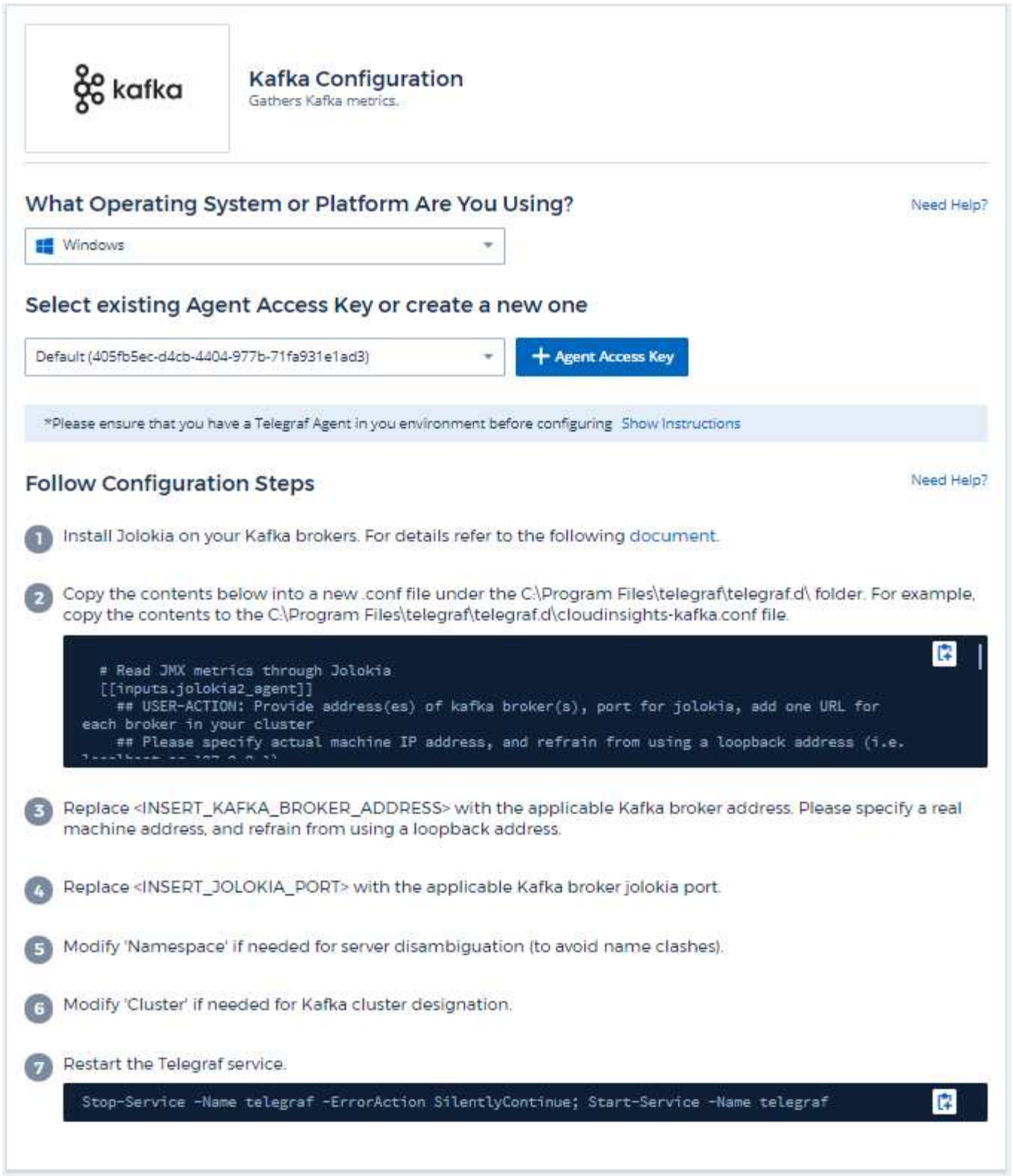
Data Infrastructure Insights utilise ce collecteur de données pour collecter les metrics de Kafka.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Kafka.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Le plug-in Kafka est basé sur le plug-in Jolokia de telegraf. Par exemple, pour recueillir des informations auprès de tous les courtiers Kafka, JMX doit être configuré et exposé via Jolokia sur tous les composants.

Compatibilité

La configuration a été développée par rapport à Kafka version 0.11.0.2.

Configuration

Toutes les instructions ci-dessous supposent que votre emplacement d'installation pour kafka est '/opt/kafka'. Vous pouvez adapter les instructions ci-dessous en fonction de votre emplacement d'installation.

Bol d'agent Jolokia

Une version le fichier JAR de l'agent Jolokia doit être "téléchargé". La version testée était l'agent Jolokia 1.6.0.

Les instructions ci-dessous supposent que le fichier jar téléchargé (jolokia-jvm-1.6.0-agent.jar) est placé sous l'emplacement '/opt/kafka/libs/'.

Kafka Brokers

Pour configurer Kafka Brokers afin d'exposer l'API Jolokia, vous pouvez ajouter ce qui suit dans <KAFKA_HOME>/bin/kafka-Server-start.sh, juste avant l'appel 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"
```

Notez que l'exemple ci-dessus utilise 'hostname -i' pour configurer la variable d'environnement 'RMI_HOSTNAME'. Dans plusieurs machines IP, vous devez modifier cette configuration pour recueillir l'IP sur laquelle vous vous prenez en charge pour les connexions RMI.

Vous pouvez choisir un autre port pour JMX (9999 ci-dessus) et Jolokia (8778). Si vous avez un IP interne pour verrouiller Jolokia sur vous pouvez remplacer le 0.0.0.0 "tout capturer" par votre propre IP. Notez que cette adresse IP doit être accessible à partir du plug-in telegraf. Vous pouvez utiliser l'option -Dcom.sun.management.jmxremote.authenticate=false' si vous ne souhaitez pas vous authentifier. Utilisation à vos propres risques.

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :
Courtier Kafka	Courtier d'espace de noms de cluster	IP du nœud de nom de nœud

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Kibana

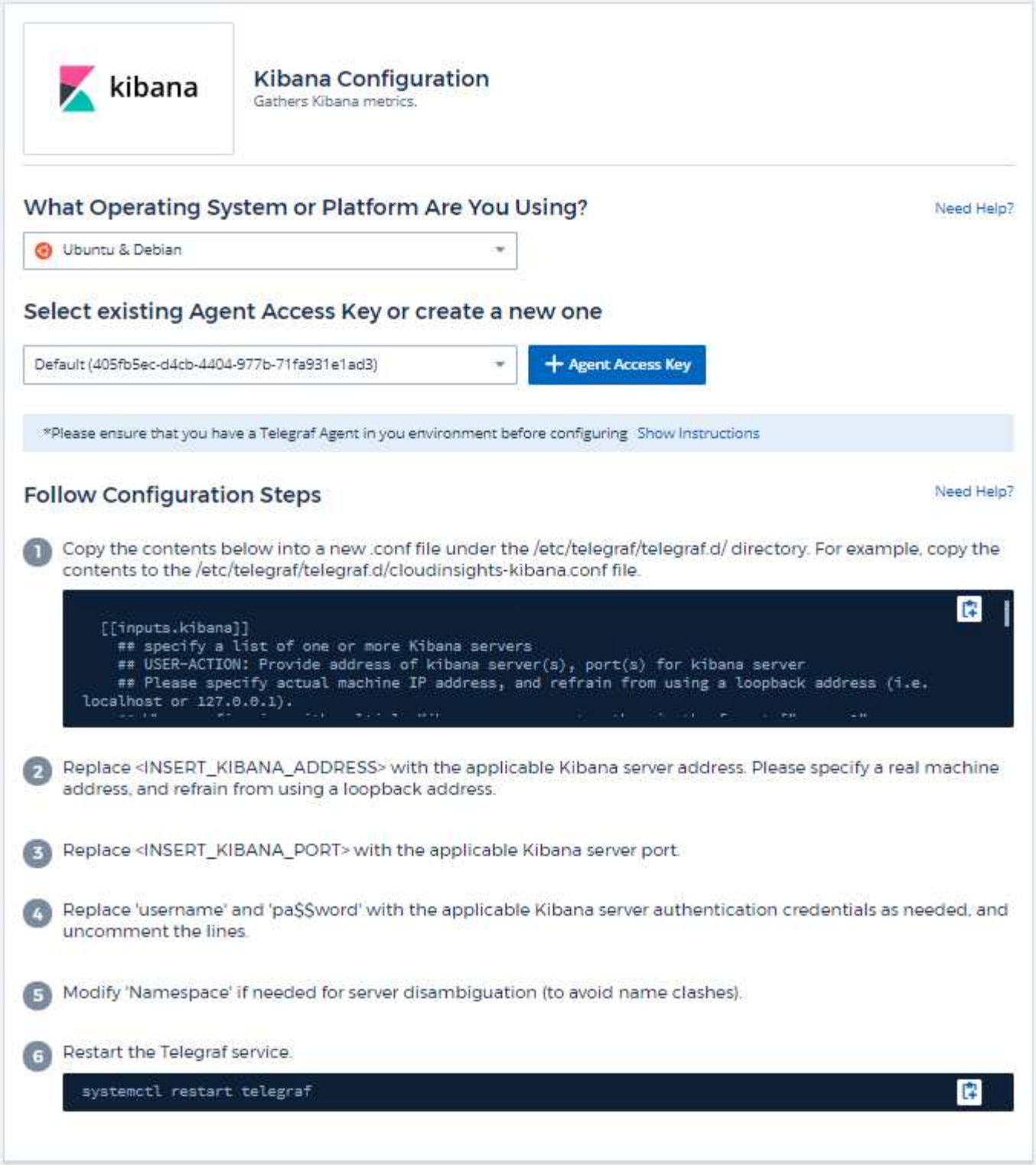
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de Kibana.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Kibana.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Documentation Kibana".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Kibana	Adresse de l'espace de noms	État de la version du nom de nœud IP du nœud	Connexions simultanées Heap Max Heap utilisait des requêtes par seconde temps de réponse moyen temps de réponse maximum disponibilité

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

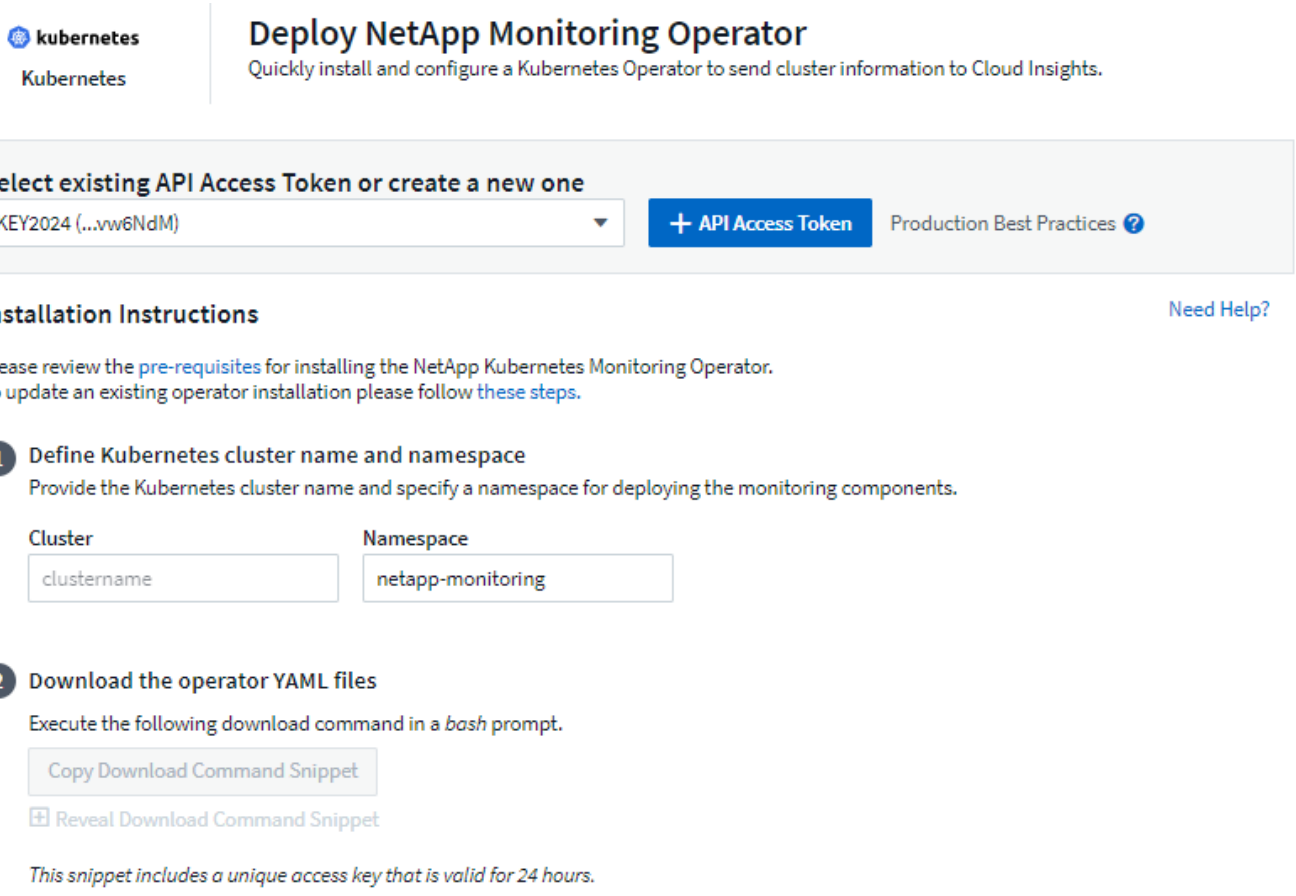
Installation et configuration de l'opérateur de contrôle Kubernetes

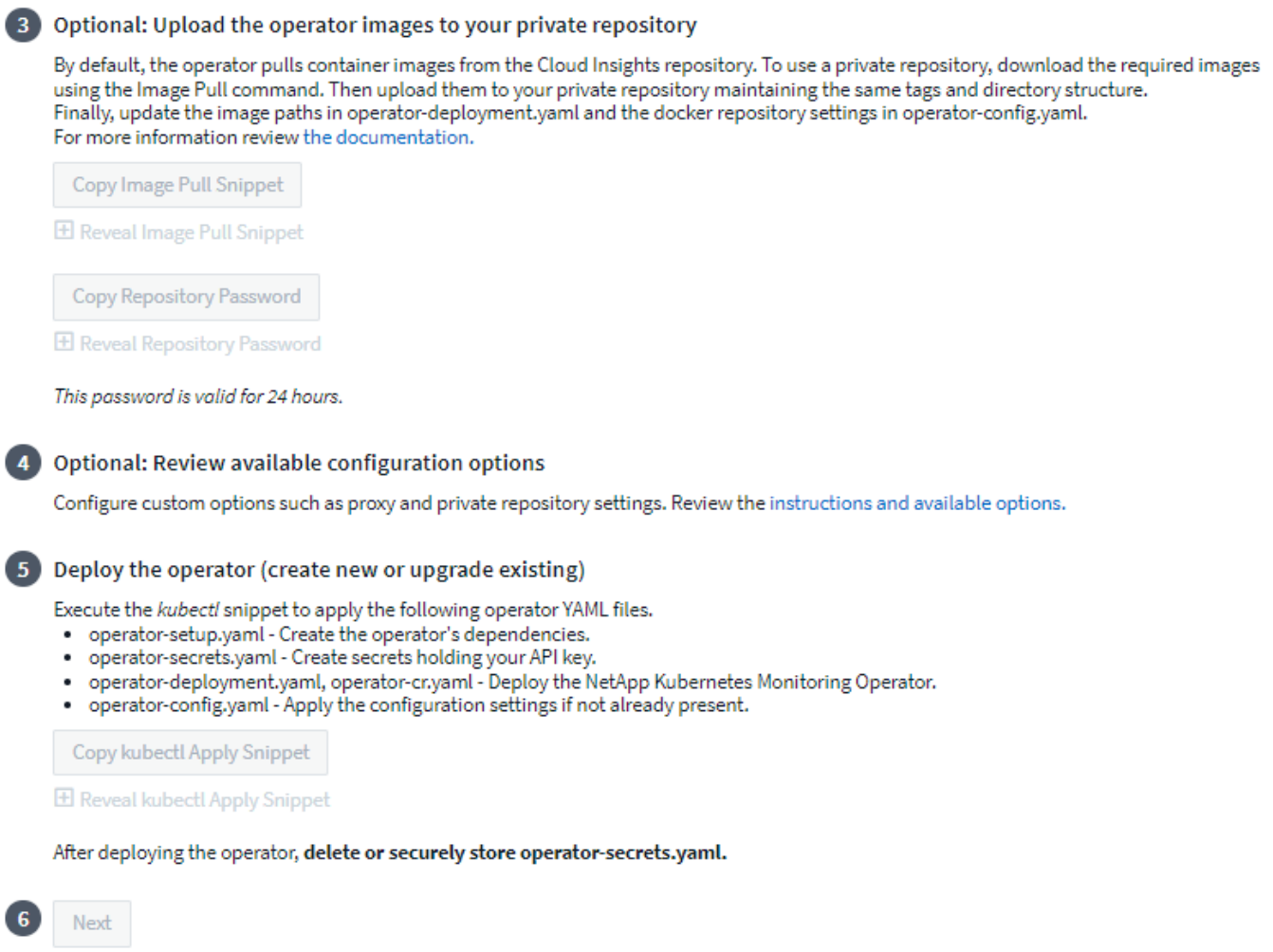
Data Infrastructure Insights propose l'opérateur **Kubernetes Monitoring Operator** pour la collecte Kubernetes. Accédez à **Kubernetes > Collectors > +Kubernetes Collector** pour déployer un nouvel opérateur.

Avant d'installer l'opérateur de surveillance Kubernetes

Consultez "Conditions préalables"la documentation avant d'installer ou de mettre à niveau l'opérateur de surveillance Kubernetes.

Installation de l'opérateur de surveillance Kubernetes


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



Étapes d'installation de l'agent opérateur de surveillance Kubernetes sur Kubernetes :

1. Entrez un nom de cluster et un espace de noms uniques. Si vous mise à niveauutilisez un opérateur Kubernetes précédent, utilisez le même nom de cluster et le même espace de noms.
2. Une fois ces données saisies, vous pouvez copier le fragment de commande de téléchargement dans le presse-papiers.
3. Collez le fragment dans une fenêtre *bash* et exécutez-le. Les fichiers d'installation de l'opérateur seront téléchargés. Notez que l'extrait de code possède une clé unique et est valide pendant 24 heures.
4. Si vous disposez d'un référentiel personnalisé ou privé, copiez le fragment facultatif image Pull, collez-le dans un shell *bash* et exécutez-le. Une fois les images extraites, copiez-les dans votre référentiel privé. Assurez-vous de conserver les mêmes balises et la même structure de dossiers. Mettez à jour les chemins dans *operator-deployment.yaml* ainsi que les paramètres du référentiel docker dans *operator-config.yaml*.
5. Si vous le souhaitez, passez en revue les options de configuration disponibles, telles que les paramètres de proxy ou de référentiel privé. Vous pouvez en savoir plus sur "options de configuration".
6. Lorsque vous êtes prêt, déployez l'opérateur en copiant le fragment kubectl Apply, en le téléchargeant et en l'exécutant.
7. L'installation se poursuit automatiquement. Une fois terminé, cliquez sur le bouton *Suivant*.
8. Une fois l'installation terminée, cliquez sur le bouton *Suivant*. Assurez-vous également de supprimer ou de stocker en toute sécurité le fichier *operator-secrets.yaml*.

Si vous utilisez un proxy, lisez à propos de configuration du proxy.

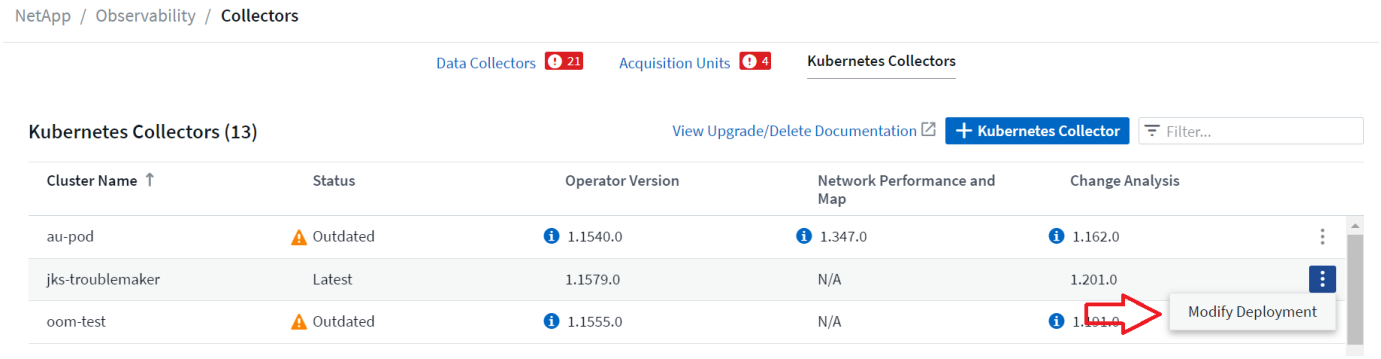
Si vous disposez d'un référentiel personnalisé, lisez à propos de à l'aide d'un référentiel docker personnalisé/privé.

Composants de surveillance Kubernetes

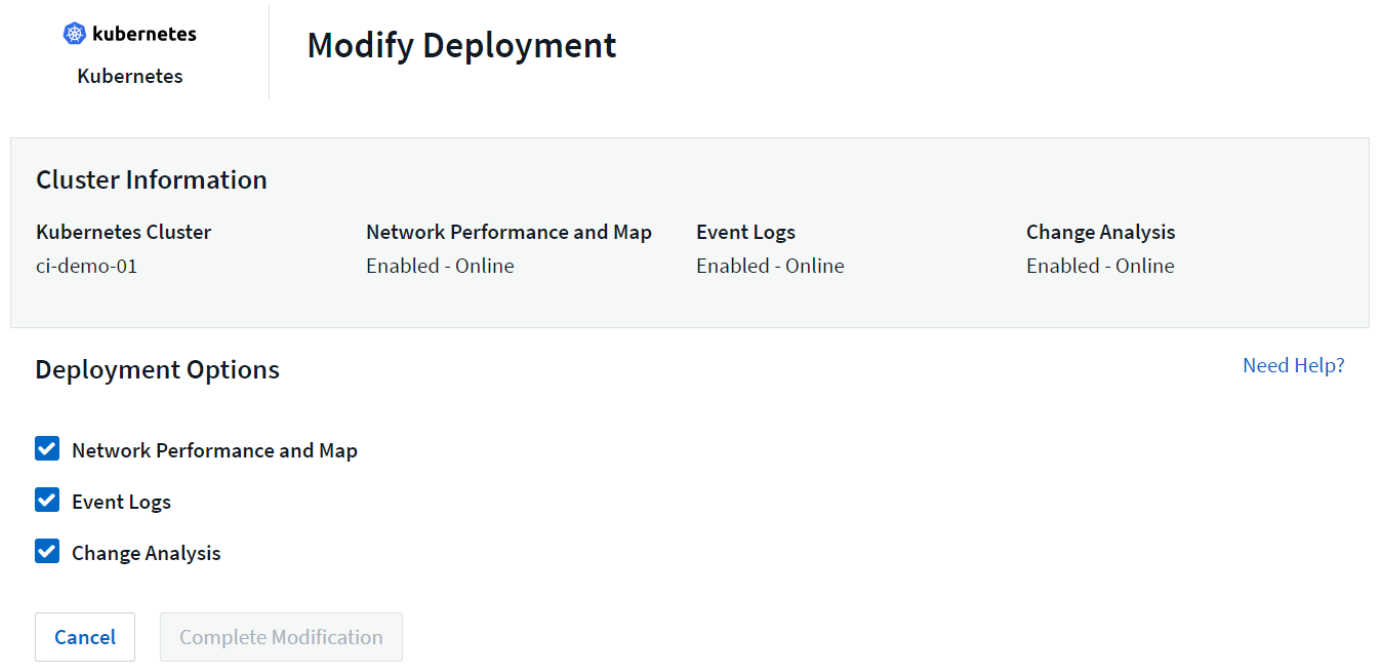
La surveillance Kubernetes de Data Infrastructure Insights comprend quatre composants de surveillance :

- Metrics du cluster
- Carte et performances réseau (en option)
- Journaux d'événements (facultatif)
- Analyse des modifications (facultatif)

Les composants facultatifs ci-dessus sont activés par défaut pour chaque collecteur Kubernetes. Si vous décidez que vous n'avez pas besoin d'un composant pour un collecteur particulier, vous pouvez le désactiver en accédant à **Kubernetes > Collectors** et en sélectionnant *Modify Deployment* dans le menu « trois points » du collecteur à droite de l'écran.



L'écran affiche l'état actuel de chaque composant et vous permet de désactiver ou d'activer les composants pour ce collecteur selon vos besoins.



Mise à niveau vers le dernier opérateur de surveillance Kubernetes

Déterminez si une configuration d'agentConfiguration existe avec l'opérateur existant (si votre espace de noms n'est pas le *netapp-monitoring* par défaut, remplacez l'espace de noms approprié) :

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-monitoring-
configuration
Si une configuration d'agentConfiguration existe :
```

- Installez Dernier opérateur par rapport à l'opérateur existant.
  - Assurez-vous que vous extraction des dernières images du conteneurutilisez un référentiel personnalisé.

Si AgentConfiguration n'existe pas :

- Notez le nom de votre cluster tel qu'il a été reconnu par les informations d'infrastructure de données (si votre namespace n'est pas le contrôle NetApp par défaut, remplacez l'espace de noms approprié) :

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Créer une sauvegarde de l'opérateur existant (si votre namespace n'est
pas la surveillance netapp par défaut, remplacez le namespace approprié)
:
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-operator,Désinstaller>>
L'opérateur existant.
* <<installing-the-kubernetes-monitoring-operator,Installez>> Le dernier
opérateur.
```

  - Utilisez le même nom de cluster.
  - Après avoir téléchargé les derniers fichiers Operator YAML, porter toutes les personnalisations trouvées dans agent_backup.yaml à l'opérateur-config.yaml téléchargé avant le déploiement.
  - Assurez-vous que vous extraction des dernières images du conteneurutilisez un référentiel personnalisé.

Arrêt et démarrage de l'opérateur de surveillance Kubernetes

Pour arrêter l'opérateur de surveillance Kubernetes :

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
Pour démarrer l'opérateur de surveillance Kubernetes :
```

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

Désinstallation

Pour supprimer l'opérateur de surveillance Kubernetes

Notez que l'espace de noms par défaut de l'opérateur de surveillance Kubernetes est « netapp-monitoring ». Si vous avez défini votre propre espace de noms, remplacez-le dans ces commandes et tous les fichiers suivants.

Les nouvelles versions de l'opérateur de surveillance peuvent être désinstallées à l'aide des commandes suivantes :

```
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 l'opérateur de surveillance a été déployé dans son propre espace de noms dédié, supprimer l'espace de noms :

```
 kubectl delete ns <NAMESPACE>
Si la première commande renvoie "aucune ressource trouvée", suivez les
instructions ci-dessous pour désinstaller les anciennes versions de
l'opérateur de surveillance.
```

Exécutez chacune des commandes suivantes dans l'ordre indiqué. Selon votre installation actuelle, certaines de ces commandes peuvent renvoyer des messages "objet non trouvé". Ces messages peuvent être ignorés en toute sécurité.

```
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 une contrainte de contexte de sécurité a été créée précédemment :

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

À propos des indicateurs Kube-State

L'opérateur de surveillance NetApp Kubernetes installe ses propres metrics kube-State pour éviter les conflits avec d'autres instances.

Pour plus d'informations sur Kube-State-Metrics, reportez-vous à "cette page"la section .

Configuration/personnalisation de l'opérateur

Ces sections contiennent des informations sur la personnalisation de la configuration de votre opérateur, l'utilisation du proxy, l'utilisation d'un référentiel docker personnalisé ou privé ou l'utilisation d'OpenShift.

Options de configuration

Les paramètres les plus fréquemment modifiés peuvent être configurés dans la ressource personnalisée *AgentConfiguration*. Vous pouvez modifier cette ressource avant de déployer l'opérateur en modifiant le fichier *Operator-config.yaml*. Ce fichier contient des exemples de paramètres commentés. Voir la liste des pour la version la plus récente de "paramètres disponibles"l'opérateur.

Vous pouvez également modifier cette ressource après le déploiement de l'opérateur à l'aide de la commande suivante :

```
 kubectl -n netapp-monitoring edit AgentConfiguration
Pour déterminer si votre version déployée de l'opérateur prend en charge
AgentConfiguration, exécutez la commande suivante :
```

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Si vous voyez un message "erreur du serveur (NotFound)", votre opérateur
doit être mis à niveau avant de pouvoir utiliser AgentConfiguration.
```

Configuration du support de proxy

Vous pouvez utiliser un proxy sur votre locataire à deux endroits pour installer l'opérateur Kubernetes Monitoring. Il peut s'agir de systèmes proxy identiques ou distincts :

- Proxy nécessaire lors de l'exécution de l'extrait de code d'installation (à l'aide de « curl ») pour connecter le système sur lequel l'extrait de code est exécuté à votre environnement Data Infrastructure Insights
- Proxy requis par le cluster Kubernetes cible pour communiquer avec votre environnement Data Infrastructure Insights

Si vous utilisez un proxy pour l'une ou l'autre de ces opérations, ou pour les deux, vous devez d'abord vous assurer que votre proxy est configuré pour permettre une bonne communication avec votre environnement Data Infrastructure Insights. Si vous disposez d'un proxy et que vous pouvez accéder à Data Infrastructure Insights à partir du serveur/de la machine virtuelle à partir duquel vous souhaitez installer l'opérateur, votre proxy est probablement configuré correctement.

Pour le proxy utilisé pour installer le moniteur d'exploitation Kubernetes, avant d'installer l'opérateur, définissez les variables d'environnement *http_proxy/https_proxy*. Pour certains environnements proxy, il peut être nécessaire de définir la variable *no_proxy Environment*.

Pour définir la ou les variable(s), effectuez les opérations suivantes sur votre système **avant** installation de l'opérateur de surveillance Kubernetes :

1. Définissez les variables d'environnement *https_proxy* et/ou *http_proxy* pour l'utilisateur actuel :
   a. Si le proxy en cours de configuration n'a pas d'authentification (nom d'utilisateur/mot de passe), exécutez la commande suivante :

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Si le proxy en cours de configuration dispose d'une
authentification (nom d'utilisateur/mot de passe), exécutez la
commande suivante :
```

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

Pour que le proxy utilisé pour votre cluster Kubernetes communique avec votre environnement Data Infrastructure Insights, installez l'opérateur de surveillance Kubernetes après avoir lu toutes ces instructions.

Configurez la section proxy d'AgentConfiguration dans Operator-config.yaml avant de déployer l'opérateur de surveillance 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
  ...
...
```

À l'aide d'un référentiel docker personnalisé ou privé

Par défaut, l'opérateur de surveillance Kubernetes extrait les images de conteneur du référentiel Data Infrastructure Insights. Si vous utilisez un cluster Kubernetes comme cible pour la surveillance et que ce cluster est configuré pour extraire uniquement les images de conteneur à partir d'un référentiel Docker personnalisé ou privé ou d'un registre de conteneurs, vous devez configurer l'accès aux conteneurs requis par l'opérateur de surveillance Kubernetes.

Exécutez l'extrait de code image dans la mosaïque d'installation de NetApp Monitoring Operator. Cette commande permet de se connecter au référentiel Data Infrastructure Insights, d'extraire toutes les dépendances d'image pour l'opérateur et de se déconnecter du référentiel Data Infrastructure Insights. Lorsque vous y êtes invité, saisissez le mot de passe temporaire du référentiel fourni. Cette commande permet de télécharger toutes les images utilisées par l'opérateur, y compris pour les fonctions facultatives. Voir ci-dessous pour connaître les caractéristiques auxquelles ces images sont utilisées.

Fonctionnalités centrales de l'opérateur et surveillance Kubernetes

- surveillance netapp
- proxy ci-kube-rbac
- ci-ksm
- ci-telegraf
- utilisateur-root-distroless

Journal des événements

- bit fluide ci

- ci-kubernetes-exportateur-événements

Performances et carte réseau

- ci-net-observateur

Envoyez l'image de docker de l'opérateur à votre référentiel docker privé, local ou d'entreprise, conformément aux règles de votre entreprise. Assurez-vous que les balises d'image et les chemins de répertoire vers ces images dans votre référentiel sont cohérents avec ceux du référentiel Data Infrastructure Insights.

Modifiez le déploiement de l'opérateur de surveillance dans Operator-deployment.yaml, et modifiez toutes les références d'image pour utiliser votre référentiel Docker privé.

```
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>
```

Modifiez la configuration d'agentConfiguration dans Operator-config.yaml pour refléter le nouvel emplacement docker repo. Créez une nouvelle imagePullSecret pour votre référentiel privé. Pour plus de détails, voir *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
```

Instructions OpenShift

Si vous exécutez sur OpenShift 4.6 ou une version ultérieure, vous devez modifier la configuration d'agentConfiguration dans *operator-config.yaml* pour activer le paramètre *runPrivileged* :

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

OpenShift peut implémenter un niveau de sécurité supplémentaire qui peut bloquer l'accès à certains composants Kubernetes.

Tolérances et tainations

Les *netapp-ci-telegraf-ds*, *netapp-ci-Fluent-bit-ds* et *netapp-ci-net-observateur-l4-ds* Demonsets doivent planifier un pod sur chaque nœud de votre cluster afin de collecter correctement les données sur tous les nœuds. L'opérateur a été configuré pour tolérer certains **taints** bien connus. Si vous avez configuré des fichiers d'accès personnalisés sur vos nœuds, empêchant ainsi les modules de s'exécuter sur chaque nœud, vous pouvez créer une **tolérance** pour ces fichiers d'accès "Dans *AgentConfiguration*". Si vous avez appliqué des rejets personnalisés à tous les nœuds de votre cluster, vous devez également ajouter les tolérances nécessaires au déploiement de l'opérateur pour permettre la planification et l'exécution du pod opérateur.

En savoir plus sur Kubernetes "Teintes et tolérances".

Revenir au **"Page installation de l'opérateur de surveillance NetApp Kubernetes"**

Remarque sur les secrets

Pour supprimer l'autorisation pour l'opérateur de surveillance Kubernetes d'afficher les secrets à l'échelle du cluster, supprimez les ressources suivantes du fichier *Operator-setup.yaml* avant d'installer :

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

S'il s'agit d'une mise à niveau, supprimez également les ressources de votre cluster :

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

Si l'option analyse des modifications est activée, modifiez *AgentConfiguration* ou *Operator-config.yaml* pour annuler le commentaire de la section de gestion des modifications et incluez *kindsToIgnoreFromWatch: '"secrets"'* dans la section de gestion des modifications. Notez la présence et la position des guillemets simples et doubles dans cette ligne.

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

Vérification des signatures d'images de l'opérateur de surveillance Kubernetes

L'image de l'opérateur et toutes les images associées qu'il déploie sont signées par NetApp. Vous pouvez vérifier manuellement les images avant l'installation à l'aide de l'outil de co-signer ou configurer un contrôleur d'admission Kubernetes. Pour plus de détails, veuillez consulter le "Documentation Kubernetes".

La clé publique utilisée pour vérifier les signatures d'image est disponible dans la mosaïque d'installation de l'opérateur de surveillance sous *Facultatif : télécharger les images de l'opérateur dans votre référentiel privé > clé publique de signature d'image*

Pour vérifier manuellement une signature d'image, effectuez les opérations suivantes :

1. Copiez et exécutez l'extrait d'image
2. Copiez et saisissez le mot de passe du référentiel lorsque vous y êtes invité
3. Stocker la clé publique de signature d'image (dii-image-Signing.pub dans l'exemple)
4. Vérifiez les images à l'aide du cosigne. Reportez-vous à l'exemple suivant d'utilisation des coenseignes

```
$ 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}]
```

Dépannage

Voici quelques points à essayer en cas de problème lors de la configuration de l'opérateur de surveillance Kubernetes :

Problème :	Essayer :
Je ne vois pas de lien hypertexte/connexion entre mon volume persistant Kubernetes et le périphérique de stockage back-end correspondant. Mon volume persistant Kubernetes est configuré en utilisant le nom d'hôte du serveur de stockage.	Procédez comme suit pour désinstaller l'agent Telegraf existant, puis réinstaller l'agent Telegraf le plus récent. Vous devez utiliser Telegraf version 2.0 ou ultérieure et le stockage de votre cluster Kubernetes doit être activement surveillé par Data Infrastructure Insights.

Problème :	Essayer :
Je vois des messages dans les journaux qui ressemblent à ce qui suit : E0901 15 352:21:39.962145 178 1 Reflector.Go:178] k8s.io/kube-state-metrics/Internal/store/Builder.Go:43.168161 : échec de la liste *v1.MutatingWebhookio Configuration : le serveur n'a pas pu trouver la ressource demandée E0901 15:21/352/Reflector.s.Go.so	Ces messages peuvent se produire si vous exécutez des metrics d'état kube version 2.0.0 ou supérieure avec les versions Kubernetes inférieures à 1.20. Pour obtenir la version Kubernetes : *kubectl version* pour obtenir la version kube-state-metrics : *kubectl get deployment/kube-state-metrics -o jsonpath='{..image}'* pour éviter que ces messages se produisent, les utilisateurs peuvent modifier leur déploiement de metrics kube-state-metrics pour désactiver les baux suivants : *hookingwebconfigurations*. Ressources=certificats,demandes persistantes,configmaps,cronjobs,demonets, déploiements,noeuds finaux,horizontalepodpodscalers,ingresources,details, resuts,undats,depositionsstatees,depositigmats,defiees,resottes,depositionssecuts,defiees,dees,depositionunedats,delimantees,delimantees,deficedats,dees,delimantees,delimantees,delimantees,deficedats,delimantees,deficedats,delimantees,deficedats,deficedats,dees,delimantees,delimantees,dees,delimantees,deficedats,dees,delimantees,delimantees,delimantees,delimantees,de vaillewebconfiguration,v'
Je vois des messages d'erreur de Telegraf ressemblant aux messages suivants, mais Telegraf démarre et s'exécute : oct 11 14:23:41 ip-172-31-39-47 systemd[1] : lancé l'agent serveur piloté par des plug-ins pour signaler des mesures dans InfluxDB. Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827] : heure="2021-10-11T14:23:41Z" level=erreur msg="Impossible de créer le répertoire de cache. /Etc/telegraf/.cache/flocon de neige, err : mkdir /etc/telegraf/.ca che : permission refusée. Ignored\n » func="nowgosflake.(*defaultLogger).Errorf" file="log.Go:10" Oct 1827 23:2021:39-47 ip-172-31-41 telegraf[11 14] : échec de l'ouverture:23:120. Ignoré. Ouvrir /etc/telegraf/.cache/flocon/ocsp_Response_cache.json : pas de fichier ou répertoire\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.Go:120 10" Oct 23:2021:39-47 ip-1827-31 telegraf[172]: 23-41-11 14:11Z! Démarrage de Telegraf 1.19.3	Il s'agit d'un problème connu. Voir "Article GitHub"pour plus de détails. Tant que Telegraf est opérationnel, les utilisateurs peuvent ignorer ces messages d'erreur.
Sur Kubernetes, mes coffee pad(s) Telegraf ont signalé l'erreur suivante : "erreur lors du traitement des informations de mountstats : échec de l'ouverture du fichier mountstats: /Hostfs/proc/1/mountstats, erreur: Ouvrir /hostfs/proc/1/mountstats: Permission refusée"	Si SELinux est activé et applique, il empêche probablement le ou les pod(s) Telegraf d'accéder au fichier /proc/1/mountstats sur le nœud Kubernetes. Pour contourner cette restriction, modifiez la configuration d'agentconfiguration et activez le paramètre runPrivileged. Pour plus de détails, reportez-vous au "Instructions OpenShift".

Problème :	Essayer :
Sur Kubernetes, mon pod Telegraf ReplicaSet signale l'erreur suivante : [inputs.prometheus] erreur dans le plug-in : impossible de charger keypair /etc/kubernetes/pki/ETcd/Server.crt:/etc/kubernetes/pki/ETcd/Server.key : ouvrir /etc/kubernetes/pki/ETcd/Server.crt : aucun fichier ni répertoire	Le pod Télégraf ReplicaSet est conçu pour s'exécuter sur un nœud désigné comme maître ou pour ETCD. Si le pod ReplicaSet n'est pas en cours d'exécution sur l'un de ces nœuds, vous obtenez ces erreurs. Vérifiez si vos nœuds maître/ETCD ont des astuces sur eux. S'ils le font, ajoutez les tolérances nécessaires à Telegraf ReplicaSet, telegraf-RS. Par exemple, modifiez le ReplicaSet… kubectl edit RS telegraf-RS …et ajoutez les tolérances appropriées à la spécification. Redémarrez ensuite le pod ReplicaSet.
J'ai un environnement PSP/PSA. Cela affecte-t-il mon opérateur de surveillance ?	Si votre cluster Kubernetes s'exécute avec la règle de sécurité Pod (PSP) ou l'admission de sécurité Pod (PSA) sur place, vous devez effectuer la mise à niveau vers l'opérateur de surveillance Kubernetes le plus récent. Procédez comme suit pour mettre à niveau vers l'opérateur actuel avec la prise en charge de PSP/PSA : 1. Désinstaller le précédent opérateur de surveillance : kubectl delete agent-monitoring-NetApp -n NetApp-monitoring kubectl delete ns NetApp-monitoring kubectl delete crd agents.monitoring.NetApp.com kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-cluster-agent-roleadmin-binding-cluster-2-agent-binding. Installez dernière version de l'opérateur de surveillance.
J'ai rencontré des problèmes lors de la tentative de déploiement de l'opérateur, et j'ai utilisé PSP/PSA.	1. Modifiez l'agent à l'aide de la commande suivante : kubectl -n <name-space> edit agent 2. Marquez « Security-policy-enabled » comme « false ». Ceci désactivera les stratégies de sécurité du Pod et l'admission de sécurité du Pod et permettra à l'opérateur de déployer. Confirmez en utilisant les commandes suivantes : kubectl get psp (devrait afficher Pod Security Policy supprimé) kubectl get all -n <namespace>
grep -i psp (doit montrer que rien n'a été trouvé)	Erreurs « ImagePullBackoff » détectées
Ces erreurs peuvent se produire si vous disposez d'un référentiel docker personnalisé ou privé et que vous n'avez pas encore configuré l'opérateur de surveillance Kubernetes pour qu'il le reconnaisse correctement. En savoir plus a propos de la configuration pour référentiel personnalisé/privé.	J'ai un problème avec mon déploiement d'opérateur de surveillance, et la documentation actuelle ne m'aide pas à le résoudre.

Problème :	Essayer :

Capturer ou noter le résultat des commandes suivantes et contacter l'équipe de support technique.
`kubectl -n netapp-monitoring get all`
`kubectl -n netapp-monitoring describe all`
`kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all-containers=true`
`kubectl -n netapp-monitoring logs <telegraf-pod> --all-containers=true`
	Les pods net-observateur (Workload Map) de l'espace de noms de l'opérateur se trouvent dans CrashLoopBackOff

Ces pods correspondent au collecteur de données Workload Map pour l'observabilité réseau. Essayez : • Vérifiez les journaux de l'un des modules pour confirmer la version minimale du noyau. Par exemple : --- {"ci-tenant-ID":"votre-tenant-ID","collectionneur-cluster":"votre-k8s-cluster-name","Environment":"prod","level":"error","msg":"échec de la validation. Raison : la version 3.10.0 du noyau est inférieure à la version minimale du noyau de 4.18.0","Time":"2022-11-09T08:23:08Z"} ---- • les pods Net-observateur requièrent que la version du noyau Linux soit au moins 4.18.0. Vérifiez la version du noyau à l'aide de la commande "uname -r" et assurez-vous qu'ils sont >= 4.18.0	Les pods s'exécutent dans l'espace de noms Operator (par défaut : surveillance netapp), mais aucune donnée n'est affichée dans l'interface pour la carte des workloads ou les metrics Kubernetes dans les requêtes
Vérifiez le réglage de l'heure sur les nœuds du cluster K8S. Pour un audit et un reporting précis des données, il est vivement recommandé de synchroniser l'heure sur l'ordinateur de l'agent à l'aide du protocole NTP (Network Time Protocol) ou SNTP (simple Network Time Protocol).	Certains des pods net-observateur dans l'espace de noms de l'opérateur sont à l'état en attente
Net-observateur est un DemonSet et exécute un pod dans chaque nœud du cluster k8s. • Notez le pod qui est à l'état en attente et vérifiez s'il rencontre un problème de ressource pour le processeur ou la mémoire. Assurez-vous que la mémoire et le processeur requis sont disponibles dans le nœud.	Je vois ce qui suit dans mes journaux immédiatement après l'installation de l'opérateur de surveillance Kubernetes : [inputs.prometheus] erreur dans le plug-in : erreur lors de la demande HTTP vers http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics : get http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics : Dial tcp: kube-state-metrics.<namespace>.svc.cluster.local : pas de recherche d'hôte

Problème :	Essayer :
Ce message n'apparaît généralement que lorsqu'un nouvel opérateur est installé et que le module *telegraf-RS* est en marche avant que le module *ksm* ne soit en marche. Ces messages doivent s'arrêter une fois que tous les modules sont en cours d'exécution.	Je ne vois aucun indicateur collecté pour les cronjobs Kubernetes qui existent dans mon cluster.
Vérifiez votre version de Kubernetes (c'est-à-dire `kubectl version`). S'il est v1.20.x ou inférieur, il s'agit d'une limitation attendue. La version de kube-state-metrics déployée avec l'opérateur de surveillance Kubernetes ne prend en charge que v1.cronjob. Avec Kubernetes 1.20.x et versions antérieures, la ressource cronjob est à v1beta.cronjob. Par conséquent, les indicateurs d'état kube ne peuvent pas trouver la ressource cronjob.	Après l'installation de l'opérateur, les modules telegraf-ds entrent dans CrashLoopBackOff et les journaux du pod indiquent « su: Authentication failure ».
Modifiez la section telegraf dans *AgentConfiguration* et définissez *dockerMetricCollectionEnabled* sur FALSE. Pour plus de détails, reportez-vous au "options de configuration"manuel de l'opérateur . … spec: … telegraf: … - Nom: docker run-mode : - DemonSet substitutions: - Key: DOCKER_UNIX_SOCK_PLACEHOLDER valeur: unix:///run/docker.sock … …	Je vois des messages d'erreur récurrents ressemblant à ce qui suit dans mes journaux Telegraf: E! [Agent] erreur d'écriture dans outputs.http: Post "https://<tenant_url>/REST/v1/Lake/iningt/influxdb": Délai de contexte dépassé (client. Dépassement du délai d'attente des en-têtes)
Modifiez la section telegraf dans *AgentConfiguration* et augmentez *outputTimeout* à 10 s. Pour plus de détails, reportez-vous au "options de configuration"manuel de l'opérateur .	Il me manque des données *involvedobject* pour certains journaux d'événements.
Assurez-vous d'avoir suivi les étapes de la "Autorisations" section ci-dessus.	Pourquoi deux modules d'opérateurs de surveillance s'exécutent, l'un nommé netapp-ci-monitoring-Operator-<pod> et l'autre Monitoring-Operator-<pod> ?
Depuis le 12 octobre 2023, Data Infrastructure Insights a été décidé de réorganiser l'opérateur pour mieux répondre aux besoins de nos utilisateurs. Pour que ces changements soient entièrement adoptés, vous devez retirez l'ancien opérateur et installez le nouveau.	Mes événements kubernetes ont cessé de générer des rapports à Data Infrastructure Insights de manière inattendue.
Récupérer le nom du pod Event-exportateur : `` `kubectl -n netapp-monitoring get pods ``	grep event-exporter

Problème :	Essayer :
awk '{print $1}'	sed 's/event-exporter./event-exporter/'` Il doit être « netapp-ci-event-exportatrice » ou « event-exportatrice ». Ensuite, modifiez l'agent de surveillance `kubectl -n netapp-monitoring edit agent` et définissez la valeur de LOG_FILE pour qu'elle reflète le nom de pod d'exportation d'événements approprié trouvé à l'étape précédente. Plus précisément, LOG_FILE doit être défini sur «/var/log/containers/netapp-ci-event-exportatrice.log » ou «/var/log/containers/event-exportatrice*.log ». …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. Sinon, on peut aussi désinstaller et réinstallez l'agent.
J'constate que le ou les pods déployés par l'opérateur de surveillance Kubernetes sont en panne en raison de ressources insuffisantes.	Reportez-vous à l'opérateur de surveillance Kubernetes "options de configuration"pour augmenter les limites de processeur et/ou de mémoire selon les besoins.
Si une image manquante ou une configuration non valide a entraîné l'échec du démarrage ou de la préparation des pods de metrics d'état de netapp-ci-kube. L'état StatefulSet est bloqué et les modifications de configuration ne sont pas appliquées aux pods de metrics netapp-ci-kube-state.	StatefulSet est dans un "cassé" état. Après avoir résolu tout problème de configuration, utilisez les pods de metrics netapp-ci-kube-état.
les pods de metrics d'état-ci-kube-netapp ne parviennent pas à démarrer après l'exécution d'une mise à niveau d'opérateur Kubernetes, et lancent ErrImagePull (échec de l'extraction de l'image).	Essayez de réinitialiser les modules manuellement.
Des messages « événement ignoré comme étant plus ancien que maxEventAgeSeconds » sont observés pour mon cluster Kubernetes sous analyse du journal.	Modifiez l'opérateur *agentconfiguration* et augmentez les valeurs *event-exportatrice-maxEventAgeSeconds* (c.-à-d. à 60 s), *event-exportatrice-kubeQPS* (c.-à-d. à 100) et *event-exportatrice-kubeBurst* (c.-à-d. à 500). Pour plus de détails sur ces options de configuration, reportez-vous à la "options de configuration" page.

Problème :	Essayer :
Telegraf avertit ou se bloque en raison d'une mémoire verrouillable insuffisante.	Essayez d'augmenter la limite de mémoire verrouillable pour Telegraf dans le système d'exploitation/nœud sous-jacent. Si l'augmentation de la limite n'est pas une option, modifiez la configuration de l'agentNKMO et définissez *Unprotected* sur *true*. Cela indique à Telegraf de ne pas tenter de réserver des pages de mémoire verrouillées. Bien que cela puisse présenter un risque de sécurité car les secrets déchiffrés peuvent être échangés sur disque, il permet une exécution dans des environnements où il est impossible de réserver de la mémoire verrouillée. Pour plus de détails sur les options de configuration *Unprotected*, reportez-vous à la "options de configuration" page.
Je vois des messages d'avertissement de Telegraf ressemblant à ce qui suit: _W! [Inputs.diskio] Impossible de récupérer le nom du disque pour « vdc » : erreur lors de la lecture de /dev/vdc : pas de fichier ou de répertoire	Pour l'opérateur de surveillance Kubernetes, ces messages d'avertissement sont bénins et peuvent être ignorés en toute sécurité. Vous pouvez également modifier la section telegraf dans AgentConfiguration et définir *runDsPrivileged* sur TRUE. Pour plus de détails, reportez-vous au "options de configuration de l'opérateur".

Problème :	Essayer :

Mon pod Fluent-bit échoue avec les erreurs suivantes : [2024/10/16 14 23:16:23] [erreur] [/src/fluent-bit/plugins/In_tail/tail_fs_inotify.c:360 errno=10/16 14] trop de fichiers ouverts [2024/10/16 14:16:23] [erreur] échec de l'initialisation de l'entrée tail.0 [2024/24:16] [erreur d'initialisation du moteur]	Essayez de modifier vos paramètres *fsnotify* dans votre cluster :
	`sudo sysctl fs.inotify.max_user_instances (take note of setting)`
	`sudo sysctl fs.inotify.max_user_instances=<something larger than current setting>`
	`sudo sysctl fs.inotify.max_user_watches (take note of setting)`
	`sudo sysctl fs.inotify.max_user_watches=<something larger than current setting>`
	Redémarrez Fluent-bit.
	Remarque : pour que ces paramètres soient persistants lors des redémarrages de nœud, vous devez placer les lignes suivantes dans */etc/sysctl.conf*
	`fs.inotify.max_user_instances=<something larger than current setting>`
	`fs.inotify.max_user_watches=<something larger than current setting>`

Problème :	Essayer :
Les pods telegraf DS signalent des erreurs liées au plug-in d’entrée kubernetes qui ne parviennent pas à faire de requêtes HTTP en raison de l’incapacité à valider le certificat TLS. Par exemple : E! [Inputs.kubernetes] erreur dans le plug-in : erreur lors de la demande HTTP pour "<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": obtenir "<a href="https://<kubelet_IP>:10250/stats/summary": " class="bare">https://<kubelet_IP>:10250/stats/summary": tls : échec de la vérification du certificat : x509 : impossible de valider le certificat pour <kubelet_IP> car il ne contient pas de SAN IP	Cela se produit si le kubelet utilise des certificats auto-signés et/ou si le certificat spécifié n'inclut pas le <kubelet_IP> dans la liste des certificats *Subject alternative Name*. Pour résoudre ce problème, l'utilisateur peut modifier le "configuration de l'agent", et définir *telegraf:insecureK8sSkipVerify* sur *true*. Cela va configurer le plug-in d'entrée telegraf pour ignorer la vérification. Sinon, l'utilisateur peut configurer le kubelet pour "ServerTLSBootstrap", qui déclenchera une demande de certificat à partir de l'API 'certificates.k8s.io'.

Des informations supplémentaires sont disponibles sur la "Assistance" page ou dans le "Matrice de prise en charge du Data Collector".

Collecteur de données Memcached

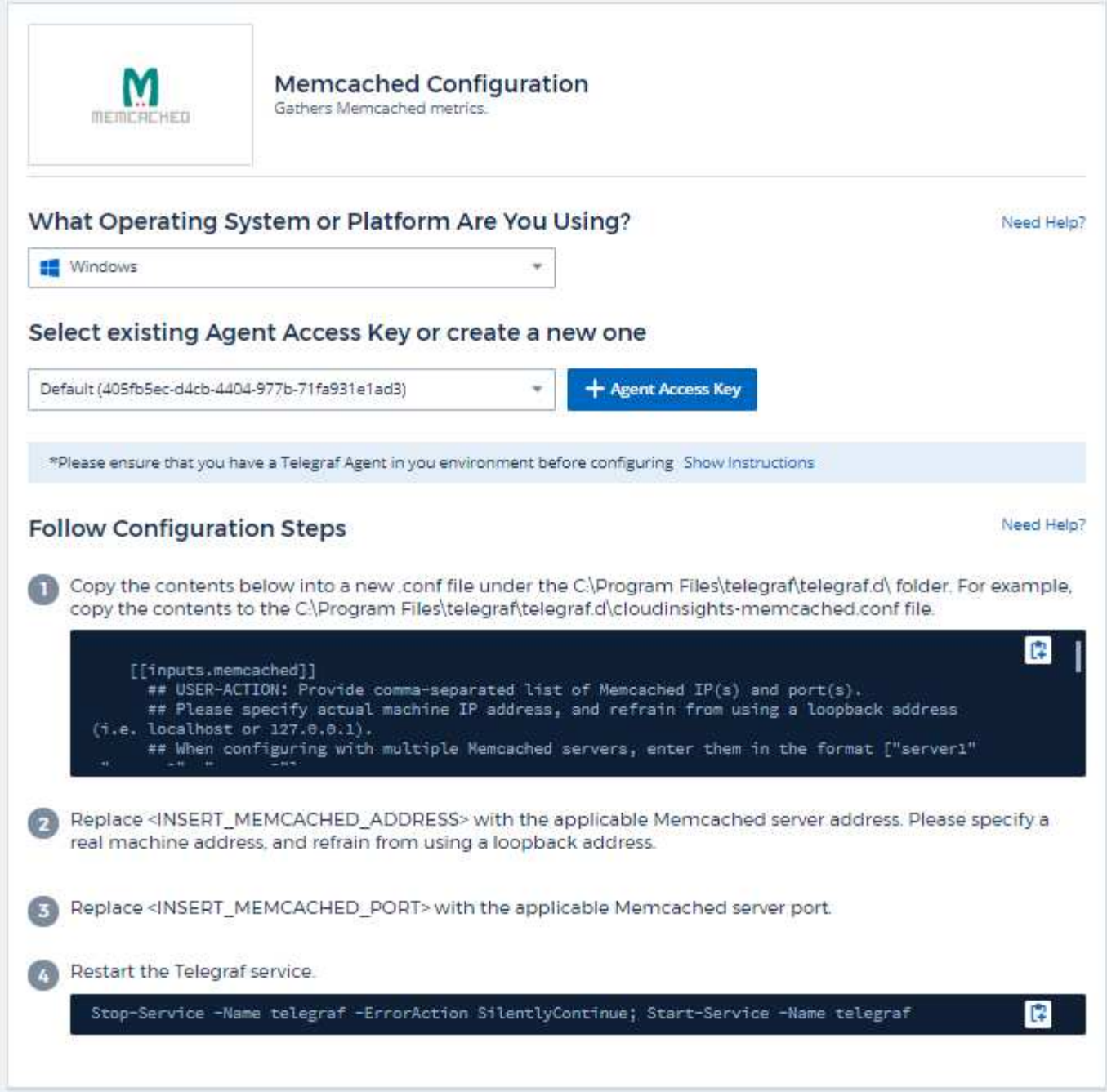
Data Infrastructure Insights utilise ce collecteur de données pour collecter des mesures à partir de Memcached.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Sélectionnez Memcached.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Wiki Memcached".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Mise en mémoire cache	Serveur d’espace de noms	Nom du nœud IP du nœud	Acceptation des connexions traitées demandes d’authentification échouées octets utilisés octets lus (par seconde) octets écrits (par seconde) cas Banval cas Hits cas échecs rinçage cas demandes (par seconde) get Reqs (par seconde) set Reqs (par seconde) Touch Reqs (par seconde) rendements de connexion (par seconde) Structures de connexion Open Connections éléments stockés actuels demandes décr Hits (par seconde) demandes décr Hits (par seconde) demandes de suppression Hits (par seconde) demandes de suppression d’échecs (par seconde) éléments expulsés nombre d’expulsions valides nombre d’éléments expirés obtenir Hits (par seconde) échecs (par seconde) Hachage en octets utilisés le hachage est en train d’étendre le Hash Power Level Incr Requests (par seconde) demandes d’incr Hits (par seconde) nombre max octets d’écoute du serveur nombre de threads de travail récupérés Num désactivé nombre total de connexions ouvertes nombre total d’éléments stockés Touch Hits Touch Touch échecs du serveur Uptime

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données MongoDB

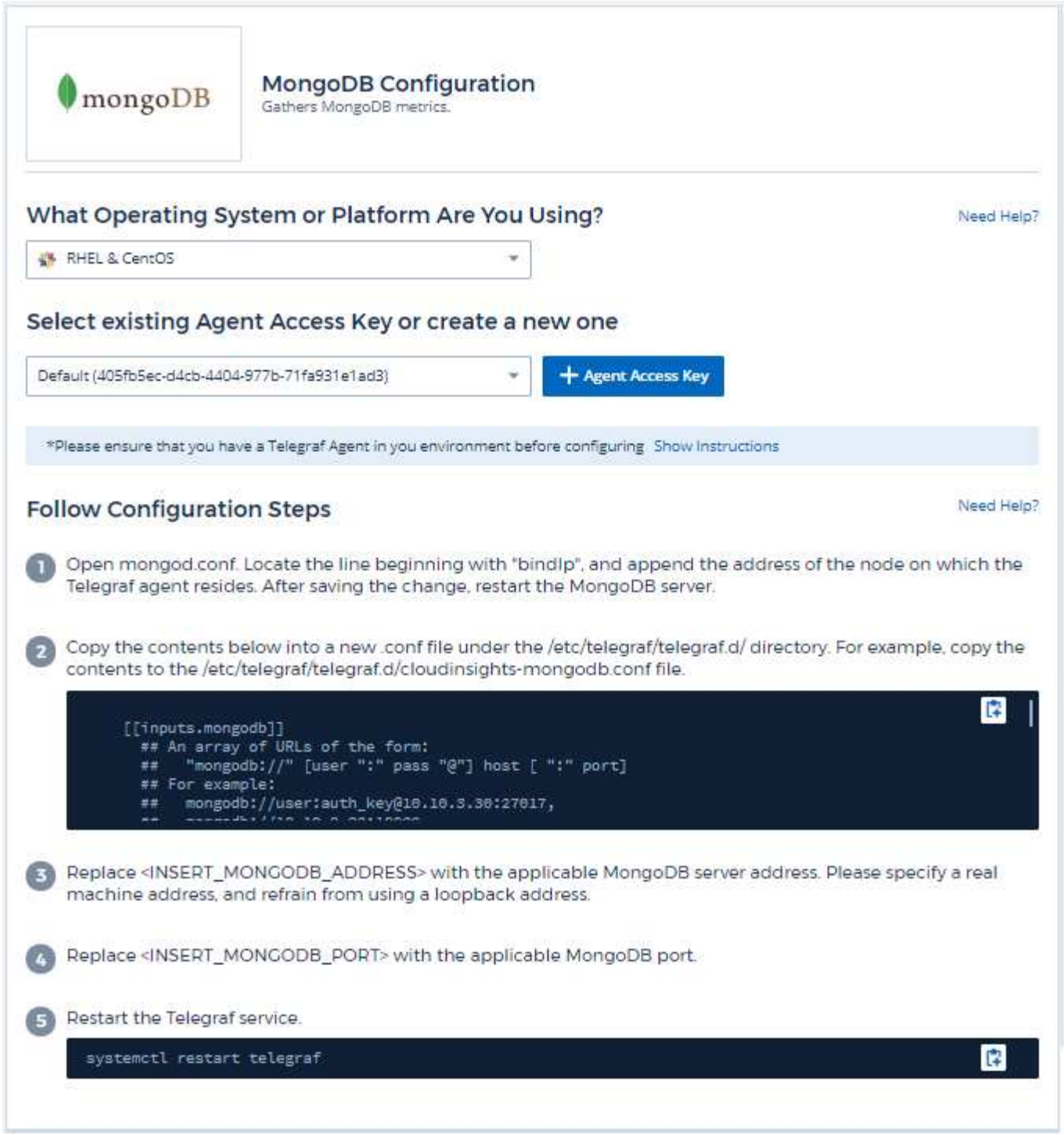
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de MongoDB.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez MongoDB.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Documentation MongoDB".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
MongoDB	Nom d'hôte du namespace		
Base de données MongoDB	Nom d'hôte de l'espace de noms Nom de la		

Dépannage

Vous trouverez des informations à partir de la "Assistance" page.

Collecteur de données MySQL

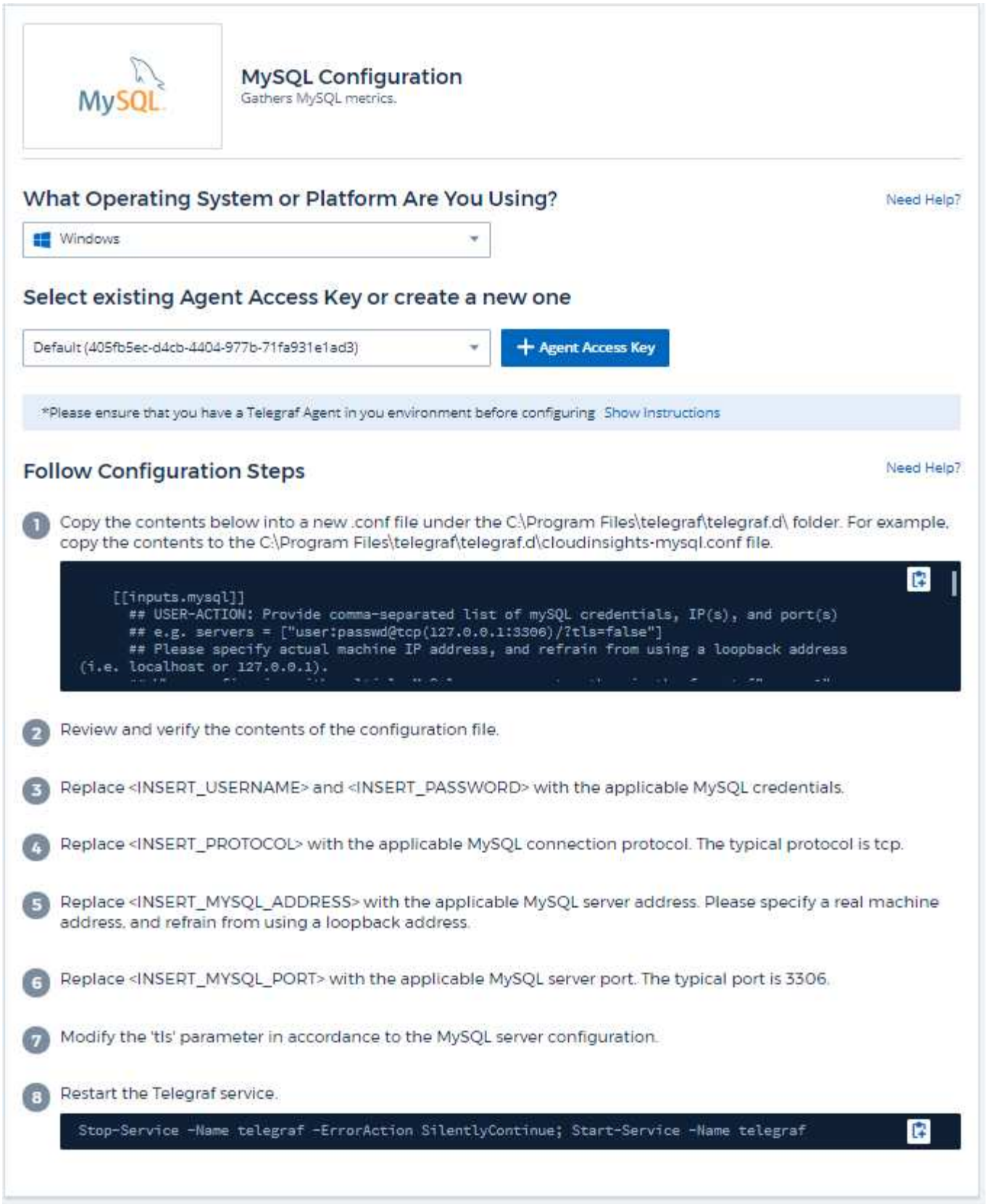
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics de MySQL.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez MySQL.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Documentation MySQL".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
MySQL	Espace de noms serveur MySQL	Nom du nœud IP du nœud	Clients abandonnés (par seconde) connexions abandonnées (par seconde) RX Bytes (par seconde) TX Bytes (par seconde) commandes Admin (par seconde) Commandes ALTER Event commandes ALTER fonction commandes ALTER instance commandes ALTER procédure commandes ALTER Server commandes ALTER Table commandes ALTER Tablespace commandes ALTER User commandes Analyze commandes Assign to Keycache commandes Begin log procédure commandes change DB commandes change DB commandes change Master change Repl Filter commandes Check commandes Commandes de la somme de contrôle commandes d'archivage commandes de création de bases de données commandes de création d'événements commandes de création d'index commandes de procédure création de commandes de création de tableaux commandes de déclenchement création de commandes UDF création de commandes d'affichage commandes de DEALLOC erreurs de connexion SQL acceptent les tables de disques tmp erreurs retardées commandes de rinçage Gestionnaire de validation InnoDB tampon octets de pool de données blocs de clés non vidés clés demandes de lecture clés demandes d'écriture clé durée d'exécution max. Dépassée

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données netstat

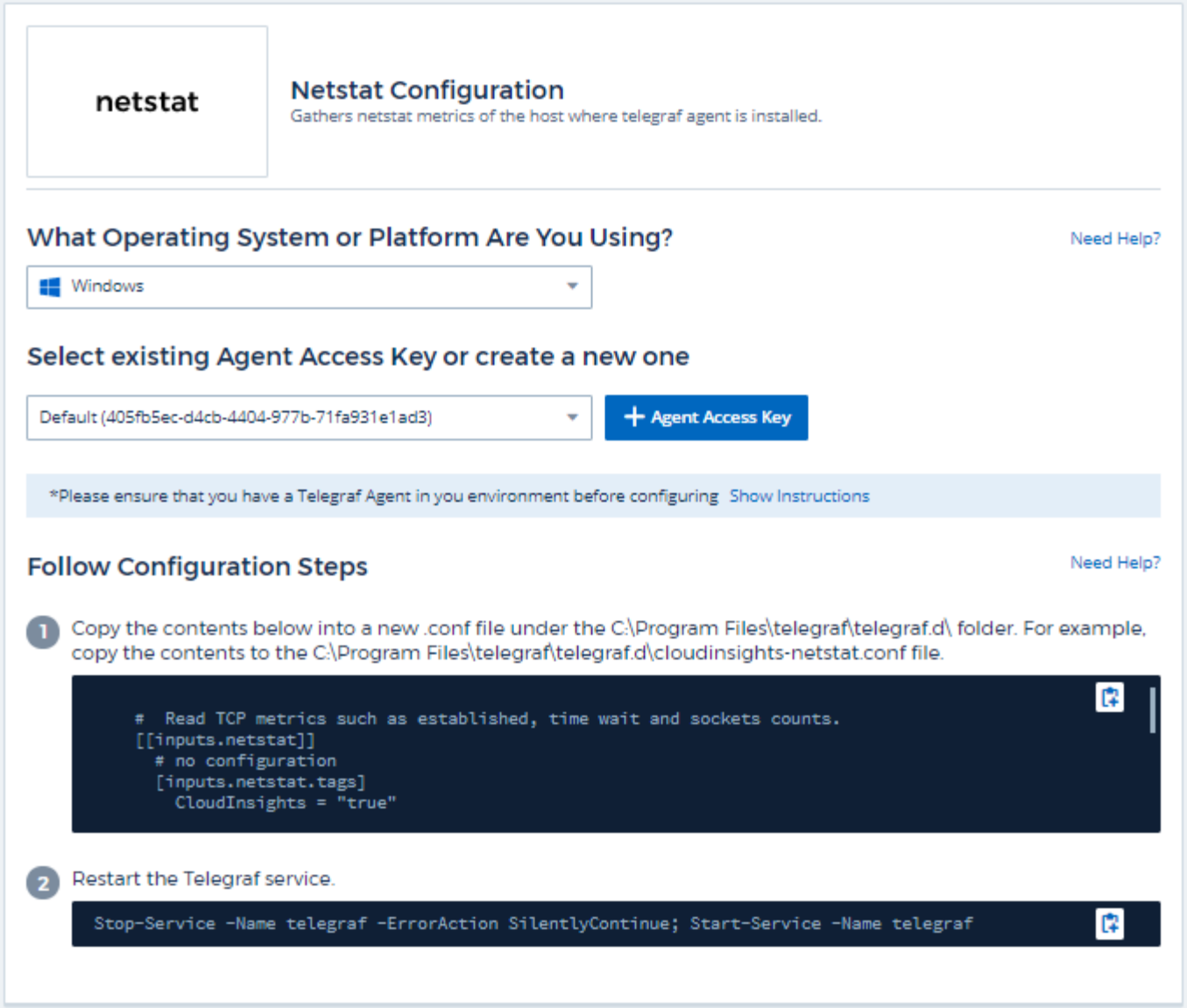
Data Infrastructure Insights utilise ce collecteur de données pour collecter les metrics Netstat.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Netstat.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Netstat	UUID du nœud	Nom du nœud IP du nœud	

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Nginx

Data Infrastructure Insights utilise ce collecteur de données pour collecter les metrics de

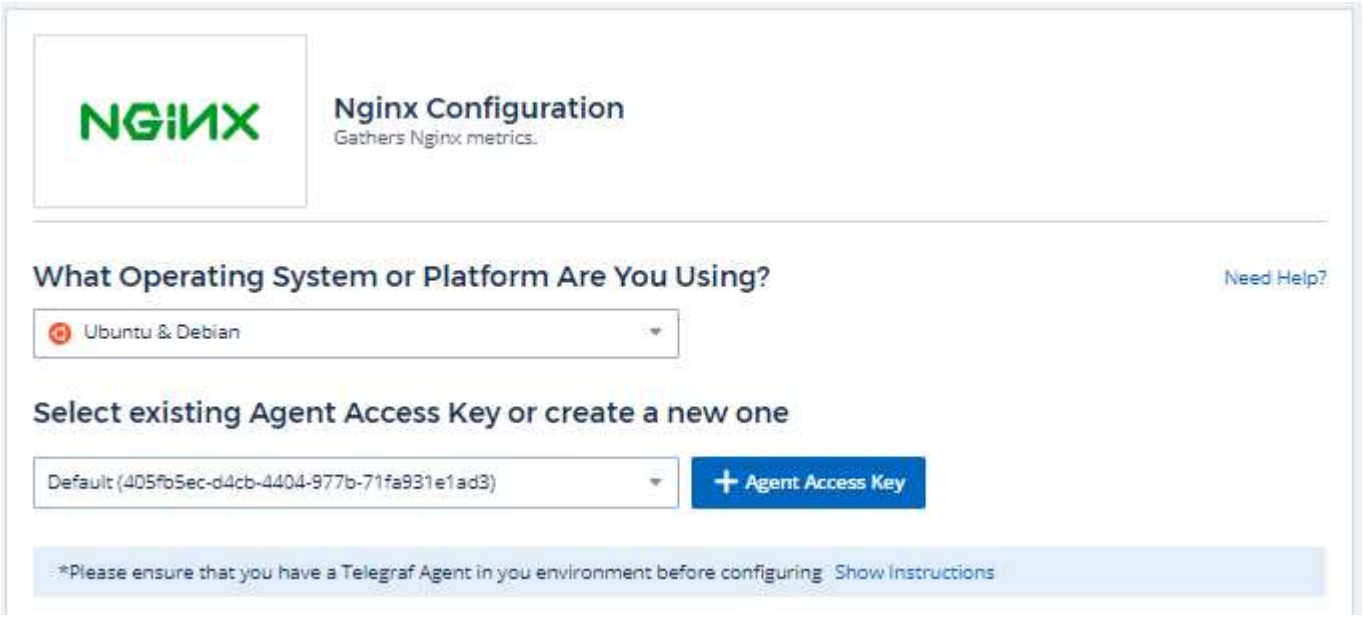
ce dernier.

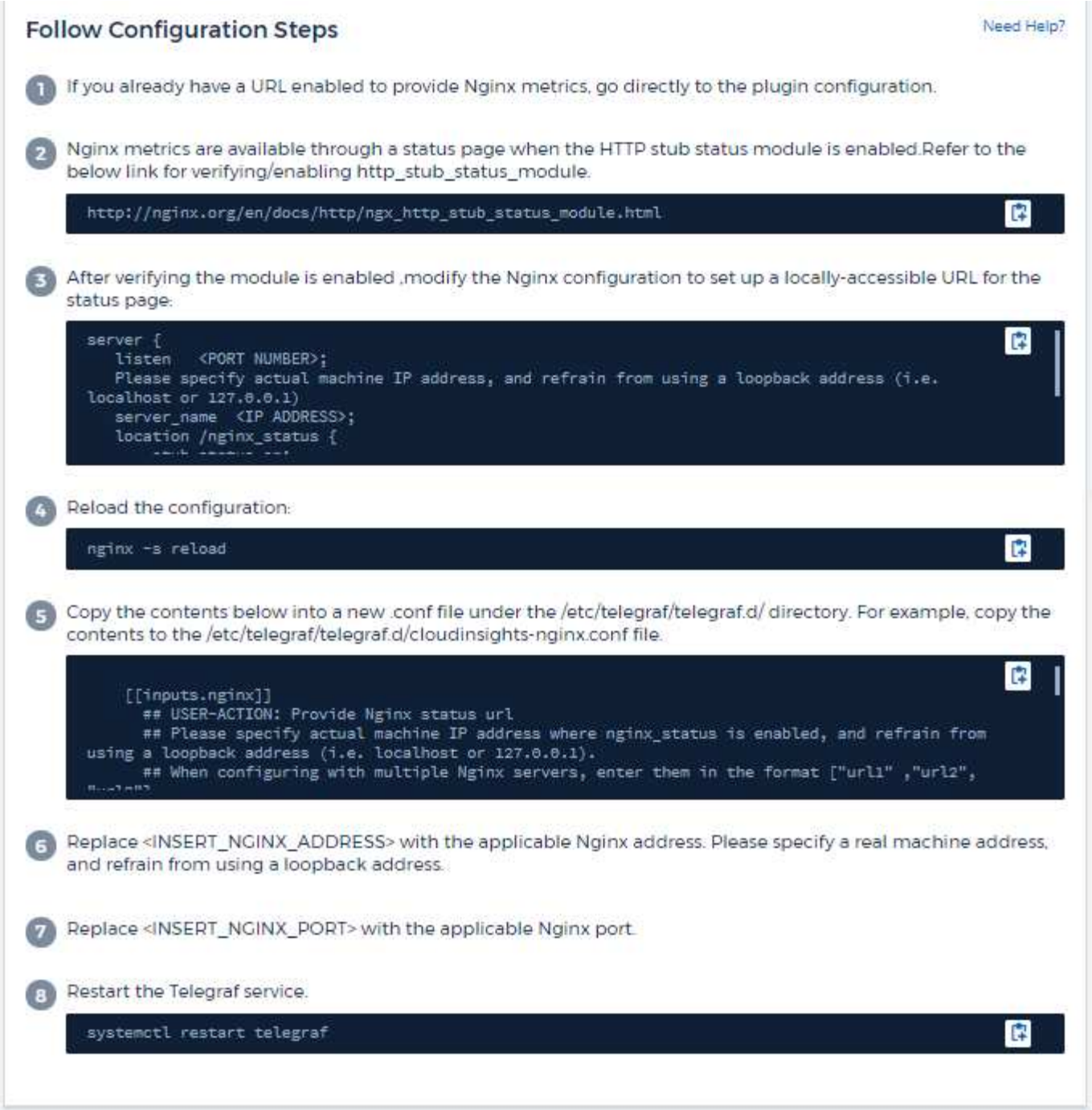
Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Nginx.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.





Configuration

La collecte des mesures NGINX requiert l'"http_stub_status_module"activation de ce dernier.

Vous trouverez des informations supplémentaires dans le "Documentation Nginx".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Nginx	Serveur d'espace de noms	Port du nom de nœud IP du nœud	Accepte les demandes de lecture traitées actives en attente d'écriture

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données PostgreSQL

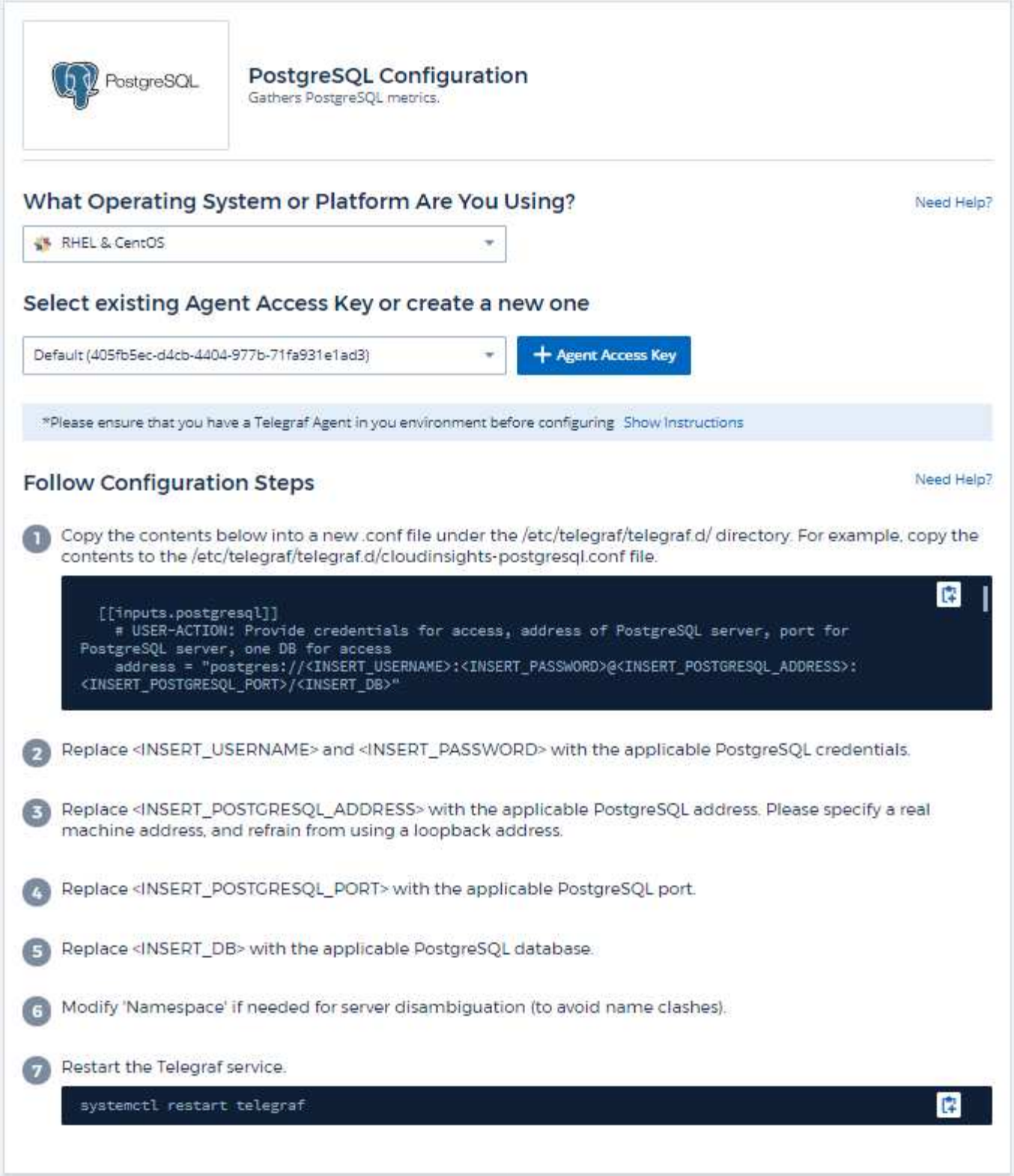
Data Infrastructure Insights utilise ce collecteur de données pour collecter les metrics de PostgreSQL.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez PostgreSQL.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Documentation PostgreSQL".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Serveur PostgreSQL	Serveur de base de données d'espace de noms	IP du nœud de nom de nœud	Tampons alloués tampons tampons Backend Buffers Backend File Sync tampons point de contrôle tampon nettoyage points de contrôle temps de synchronisation points de contrôle temps d'écriture demandes points de contrôle délai maximum écriture nettoyage
Base de données PostgreSQL	Serveur de base de données d'espace de noms	ID objet de la base de données Nom du nœud IP	Blocs blocs de temps de lecture blocs de temps d'écriture nombre de blocs de lectures nombre de conflits nombre de fichiers temporaires octets fichiers temporaires nombre de lignes supprimées lignes extraites lignes extraites lignes retournées lignes retournées transactions mises à jour validées Rollened transactions

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Collecteur de données Puppet Agent

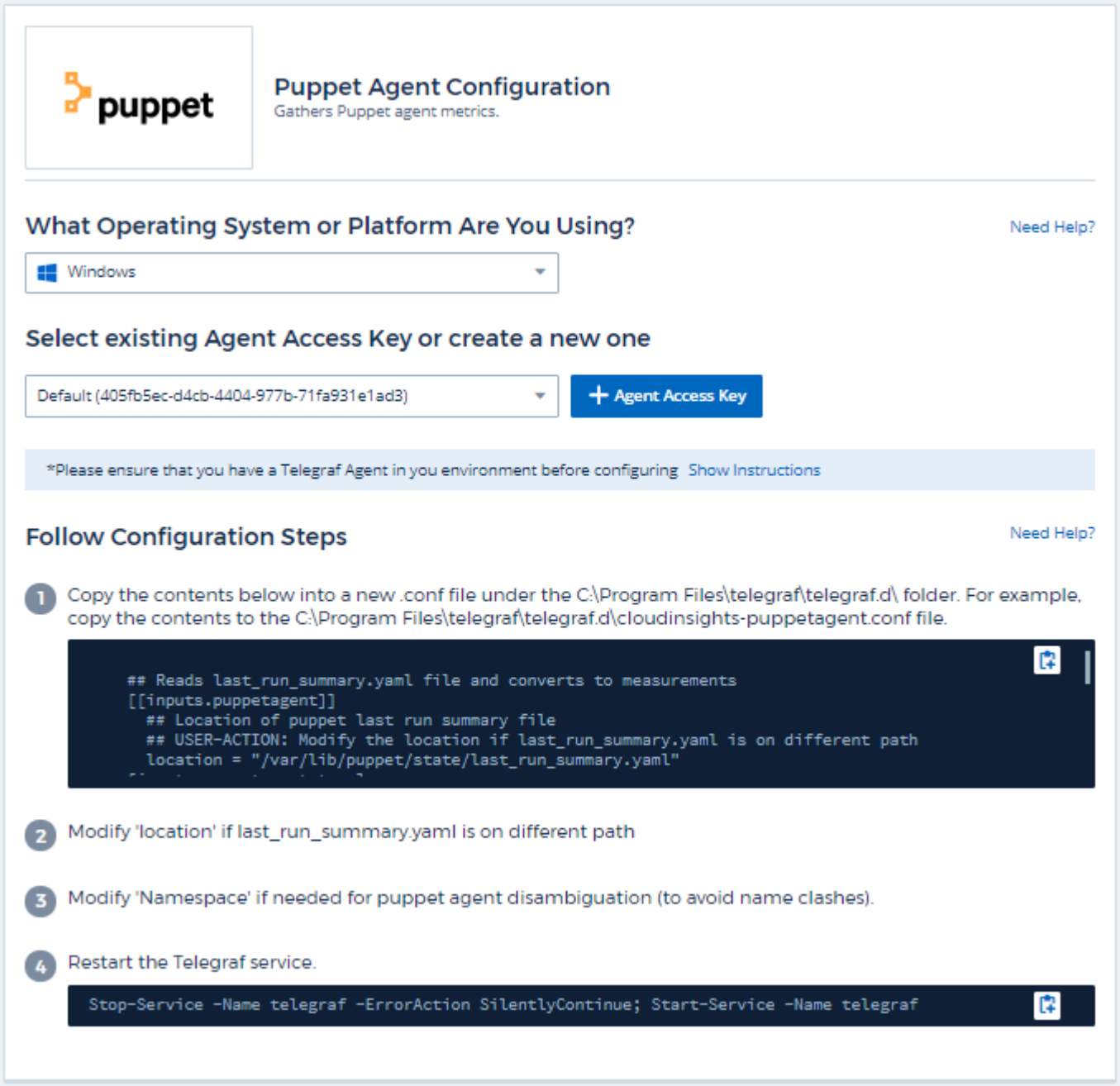
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de l'agent Puppet.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Puppet.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Documentation Puppet"

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :

Agent Puppet	UUID de nœud de namespace	Nom du nœud emplacement nœud version IP de la chaîne de configuration version Puppet	Changements Total des événements échec événements succès événements Total des ressources modifiées Ressources non modifiées Ressources non activées redémarrer les ressources désync Ressources redémarrées Ressources planifiées Ressources ignorées Ressources Total temps d'ancrage temps d'extraction temps d'extraction Cron Time Exec Time File Time Filebucket Time LASTRUN temps temps du temps du temps du temps du temps de service Sshauthorizedkey Time Total Utilisateur de temps

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.

Redis Data Collector

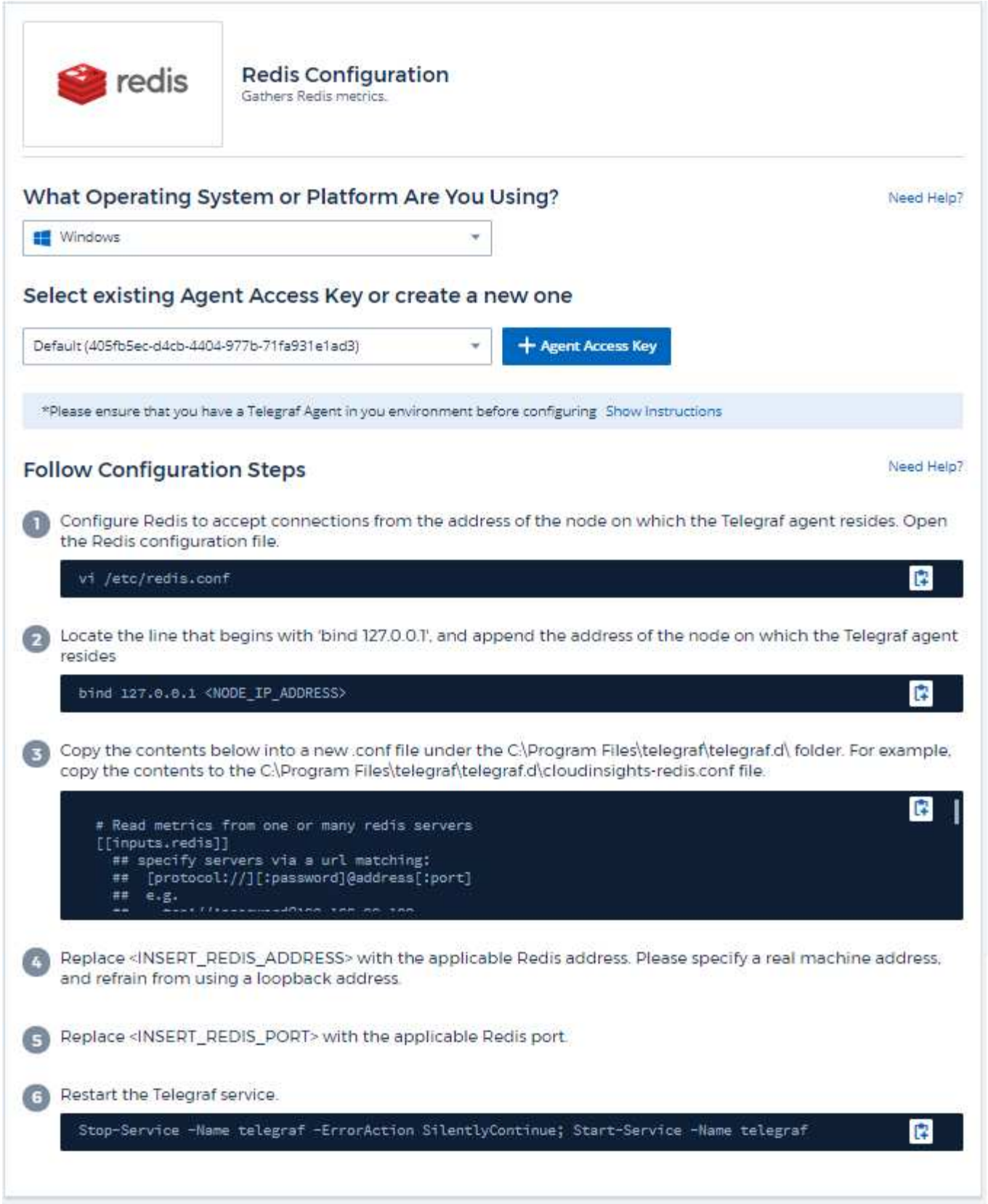
Data Infrastructure Insights utilise ce collecteur de données pour collecter des metrics à partir de Redis. Redis est un magasin de structure de données in-memory open source utilisé comme base de données, cache, et courtier en messages, prenant en charge les structures de données suivantes : chaînes, hachages, listes, jeux, etc.

Installation

1. Dans **observabilité > Collectors**, cliquez sur **+Data Collector**. Choisissez Redis.

   Sélectionnez le système d'exploitation ou la plate-forme sur laquelle l'agent Telegraf est installé.

2. Si vous n'avez pas déjà installé un agent pour la collecte ou si vous souhaitez installer un agent pour un autre système d'exploitation ou une autre plate-forme, cliquez sur *Afficher les instructions* pour développer les "Installation de l'agent"instructions.
3. Sélectionnez la clé d'accès de l'agent à utiliser avec ce collecteur de données. Vous pouvez ajouter une nouvelle clé d'accès à l'agent en cliquant sur le bouton * + clé d'accès à l'agent*. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple, par OS/plate-forme.
4. Suivez les étapes de configuration pour configurer le collecteur de données. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme utilisé pour collecter des données.



Configuration

Vous trouverez des informations dans le "Redis documentation".

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet :	Identifiants :	Attributs :	Points de données :
Redis	Serveur d’espace de noms		

Dépannage

Vous trouverez des informations supplémentaires sur la "Assistance" page.