Référence du collecteur de données - Services

Data Infrastructure Insights

NetApp
February 19, 2026

Sommaire

Référence du collecteur de données - Services

Collecte de données de nœuds

Data Infrastructure Insights collecte les métriques du nœud sur lequel vous installez un agent.

Installation

1. Dans **Observabilité > Collecteurs**, choisissez un système d'exploitation/une plateforme. Notez que l'installation de n'importe quel collecteur de données d'intégration (Kubernetes, Docker, Apache, etc.) configurera également la collecte de données de nœud.
2. Suivez les instructions pour configurer l'agent. Les instructions varient en fonction du type de système d'exploitation ou de plate-forme que vous utilisez pour collecter des données.

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés en tant que métriques de nœud :

Objet:	Identifiants :	Attributs:	Points de données :
Système de fichiers Node	Type de chemin d'accès du périphérique UUID du nœud	IP du nœud Nom du nœud Mode du système d'exploitation du nœud	Inodes libres Inodes libres Total des inodes utilisés Total utilisé Total utilisé
Disque de nœud	Disque UUID du nœud	IP du nœud Nom du nœud Système d'exploitation du nœud	Temps d'E/S Total des IOPS en cours Octets lus (par seconde) Temps de lecture Total des lectures (par seconde) Temps d'E/S pondéré Total des octets d'écriture (par seconde) Temps d'écriture Total des écritures (par seconde) Longueur actuelle de la file d'attente du disque Temps d'écriture Temps de lecture Temps d'E/S
Nœud CPU	UUID du nœud CPU	IP du nœud Nom du nœud Système d'exploitation du nœud	Utilisation du processeur système Utilisation du processeur utilisateur Utilisation du processeur inactif Utilisation du processeur du processeur Utilisation du processeur d'interruption Utilisation du processeur DPC

Objet:	Identifiants :	Attributs:	Points de données :
Nœud	Nœud UUID	IP du nœud Nom du nœud Système d'exploitation du nœud	Temps de démarrage du noyau Changements de contexte du noyau (par seconde) Entropie du noyau disponible Interruptions du noyau (par seconde) Processus du noyau forkés (par seconde) Mémoire Mémoire active disponible Mémoire totale disponible Mémoire tamponnée Mémoire en cache Limite de validation Mémoire validée en tant que mémoire Mémoire sale Mémoire libre élevée Mémoire libre élevée Mémoire totale énorme Taille de page Mémoire Grandes pages Mémoire libre Grandes pages Mémoire totale faible Mémoire libre faible Mémoire totale Mémoire mappée Tables de pages Mémoire Mémoire partagée Mémoire en bloc Swap Mémoire en cache Swap Mémoire libre Swap Mémoire totale Mémoire totale utilisée Mémoire totale utilisée Mémoire Vmalloc Bloc de mémoire Vmalloc Mémoire totale Vmalloc Mémoire utilisée Mémoire câblée Écriture différée Mémoire totale Écriture différée Mémoire temporaire Défauts de cache Demande de mémoire Défauts de page mémoire Pages mémoire Mémoire non paginée Mémoire paginée Cache Mémoire principale Cache de secours Mémoire normale Cache de secours Réserve de mémoire Défauts de transition Processus Processus bloqués Processus morts Processus inactifs Processus de pagination

Objet:	Identifiants :	Attributs:	Points de données :
Réseau de nœuds	UUID du nœud d'interface réseau	Nom du nœud IP du nœud Système d'exploitation du nœud	Octets reçus Octets envoyés Paquets sortants Paquets rejetés Erreurs sortantes Paquets reçus Paquets rejetés Erreurs reçues Paquets reçus Paquets envoyés

Installation

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

Collecteur de données ActiveMQ

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

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez ActiveMQ.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
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 que vous utilisez pour collecter des données.

[Configuration d'ActiveMQ]

Installation

Des informations peuvent être trouvées dans le "Documentation d'ActiveMQ"

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
File d'attente ActiveMQ	Serveur de port de file d'attente d'espace de noms	Nom du nœud IP du nœud UUID du nœud	Nombre de consommateurs Nombre de sorties de file d'attente Nombre de mises en file 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 IP du nœud UUID du nœud Sélecteur de système d'exploitation du nœud Abonnement	Nombre de sorties de file d'attente Nombre de sorties expédiées Taille de la file d'attente expédiée Nombre de sorties de file d'attente Taille de la file d'attente en attente
Sujet ActiveMQ	Espace de noms du serveur de port de sujet	Nom du nœud IP du nœud UUID du nœud Système d'exploitation du nœud	Nombre de consommateurs Nombre de sorties de file d'attente Nombre de mises en file d'attente Taille

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Apache

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

Prérequis

- Votre serveur HTTP Apache doit être configuré et fonctionner correctement.
- Vous devez disposer des autorisations sudo ou administrateur sur votre hôte/VM d'agent
- En règle générale, 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, consultez la documentation du module Apache : https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Apache.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de

données, par exemple par système d'exploitation/plateforme.

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 que vous utilisez pour collecter des données.

[Configuration d'Apache]

Installation

Le plugin de Telegraf pour le serveur HTTP d'Apache s'appuie sur le module « mod_status » pour être activé. Lorsque cette option est activée, le serveur HTTP d'Apache exposera un point de terminaison HTML qui peut être visualisé sur votre navigateur ou récupéré pour l'extraction de l'état de toute la configuration du serveur HTTP d'Apache.

Compatibilité:

La configuration a été développée sur la version 2.4.38 du serveur HTTP d'Apache.

Activation de mod_status :

L'activation et l'exposition des modules « mod_status » impliquent deux étapes :

- Module d'activation
- Exposer les statistiques 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 décommentez les lignes suivantes :

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

Exposer les statistiques 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 d'avoir les éléments suivants dans ce fichier de configuration (au moins, d'autres directives seront présentes) :

```
# 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 des instructions détaillées sur le module « mod_status », consultez le"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 IP Nom du nœud Port Génération de configuration du serveur parent Génération MPM du serveur parent La disponibilité du serveur s’arrête	Travailleurs occupés Octets par requête Octets par seconde CPU Enfants CPU système Enfants Charge CPU utilisateur CPU système CPU utilisateur Connexions asynchrones Fermeture des connexions asynchrones Maintien en activité des connexions asynchrones Écriture des connexions Durée totale par requête Travailleurs inactifs Charge moyenne (dernier 1 min) Charge moyenne (derniers 15 min) Charge moyenne (derniers 5 min) Processus Requêtes par seconde Accès totaux Durée totale Total Ko Tableau de bord Fermeture Tableau de bord Recherches DNS Tableau de bord Fin Tableau de bord Nettoyage d’inactivité Tableau de bord Maintien en activité Tableau de bord Journalisation Tableau de bord Ouverture Tableau de bord Lecture Tableau de bord Envoi Tableau de bord Démarrage Tableau de bord Attente

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données consulaires

Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques auprès de Consul.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Consul.

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

Si vous avez déjà configuré un agent, sélectionnez le système d'exploitation ou la plateforme approprié et cliquez sur **Continuer**.

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

Installation

Des informations peuvent être trouvées dans le"Documentation du consul" .

Objets et compteurs pour consul

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Consul	Nœud de service d'identification de vérification d'espace de noms	IP du nœud OS du nœud UUID du nœud Nom du nœud Nom du service Nom de vérification ID du service Statut	Avertissement de dépassement critique

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Couchbase

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

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Couchbase.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
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 que vous utilisez pour collecter des données.

[Configuration de Couchbase]

Installation

Des informations peuvent être trouvées dans le"Documentation de Couchbase" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Nœud Couchbase	Espace de noms Cluster Couchbase Node Nom d'hôte	Nom du nœud IP du nœud	Mémoire libre Mémoire totale
Seau Couchbase	Cluster de compartiments d'espace de noms	Nom du nœud IP du nœud	Données utilisées Récupérations de données Disque utilisé Nombre d'éléments Mémoire utilisée Opérations par seconde Quota utilisé

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données CouchDB

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

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez CouchDB.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
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 que vous utilisez pour collecter des données.

[Configuration de CouchDB]

Installation

Des informations peuvent être trouvées dans le"Documentation de CouchDB" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
CouchDB	Serveur d'espace de noms	Nom du nœud IP du nœud	Authentification Cache Hits Authentification Cache Miss Lectures de base de données Écritures de base de données Bases de données Ouvrir Ouvrir Fichiers OS Durée maximale de la requête Durée minimale de la requête Méthodes de requête HTTP Copier Méthodes de requête HTTP Supprimer Méthodes de requête HTTP Obtenir Méthodes de requête HTTP En-tête Méthodes de requête HTTP Publier Méthodes de requête HTTP Mettre 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

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Docker

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

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Docker.

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

Si vous avez déjà configuré un agent, sélectionnez le système d'exploitation ou la plateforme approprié et cliquez sur **Continuer**.

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

[Configuration de Docker]

Installation

Le plugin d'entrée Telegraf pour Docker collecte des métriques via un socket UNIX spécifié ou un point de terminaison TCP.

Compatibilité

La configuration a été développée sur la version Docker 1.12.6.

Installation

Accéder à Docker via un socket UNIX

Si l'agent Telegraf s'exécute sur baremetal, ajoutez l'utilisateur Unix telegraf au groupe Unix docker 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 mappant le socket dans le pod en tant que volume, puis en
montant ce volume sur /var/run/docker.sock.  Par exemple, ajoutez ce qui
suit au PodSpec :
```

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

Ensuite, ajoutez les éléments suivants au conteneur :

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

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

Accéder à Docker via un point de terminaison TCP

Par défaut, Docker utilise le port 2375 pour l'accès non chiffré et le port 2376 pour l'accès chiffré.

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Moteur Docker	Espace de noms Docker Engine	Nom du nœud IP du nœud UUID du nœud Système d'exploitation du nœud Cluster Kubernetes Version Docker Unité	Conteneurs de mémoire Conteneurs Conteneurs en pause Conteneurs en cours d'exécution CPU arrêtés Routines Go Images Événements d'écoute utilisés Descripteurs de fichiers Données Données disponibles Données totales utilisées Métadonnées Métadonnées disponibles Métadonnées totales utilisées Taille de bloc du pool

Objet:	Identifiants :	Attributs:	Points de données :
Conteneur Docker	Espace de noms Nom du conteneur Moteur Docker	Hachage du conteneur Kubernetes Ports du conteneur Kubernetes Nombre de redémarrages du conteneur Kubernetes Chemin du message de fin du conteneur Kubernetes Politique de message de fin du conteneur Kubernetes Période de grâce de fin du pod Kubernetes Image du conteneur État du conteneur Version du conteneur Nom du nœud Chemin du journal du conteneur Kubernetes Nom du conteneur Kubernetes Type Docker Kubernetes Nom du pod Kubernetes Espace de noms du pod Kubernetes UID du pod Kubernetes ID du sandbox Kubernetes IP du nœud UUID du nœud Version Docker Configuration E/S Kubernetes vue Source de la configuration E/S Kubernetes OpenShift IO SCC Description Kubernetes Nom d'affichage Kubernetes Balises OpenShift Service Kompose Modèle de pod Contrôleur de hachage Révision du hachage Génération du modèle de pod Licence Date de build du schéma Nom du schéma de licence URL du schéma URL du VCS du schéma Fournisseur du schéma Version du schéma Schéma Responsable de la version du schéma Pod client Kubernetes StatefulSet Nom du pod Tenant Architecture de la console Web URL source faisant autorité Date de build Hôte de build RH Distribution des composants RH Portée	Mémoire active, anonyme, fichier actif, cache, limite hiérarchique, mémoire inactive, anonyme, fichier inactif, limite de mémoire, fichier mappé, mémoire, utilisation maximale, erreur de page, erreur majeure de page, mémoire paginée, mémoire paginée, mémoire sortante, taille de l'ensemble résident, mémoire, taille de l'ensemble résident, énorme mémoire, mémoire anonyme active totale, fichier actif, mémoire cache totale, mémoire anonyme inactive totale, fichier inactif, mémoire, fichier mappé, mémoire, erreur de page, erreur majeure de page, mémoire paginée, mémoire sortante, mémoire, taille de l'ensemble résident, mémoire, taille de l'ensemble résident, énorme mémoire, mémoire non supprimable, utilisation de la mémoire non supprimable, pourcentage d'utilisation de la mémoire, code de sortie, OOM, PID tué, commencé à la série d'échecs.

Objet:	Identifiants :	Attributs:	Points de données :
Bloc d’E/S du conteneur Docker	Espace de noms Nom du conteneur Appareil Moteur Docker	Hachage du conteneur Kubernetes Ports du conteneur Kubernetes Nombre de redémarrages du conteneur Kubernetes Chemin du message de fin du conteneur Kubernetes Politique de message de fin du conteneur Kubernetes Période de grâce de fin du pod Kubernetes Image du conteneur État du conteneur Version du conteneur Nom du nœud Chemin du journal du conteneur Kubernetes Nom du conteneur Kubernetes Type Docker Kubernetes Nom du pod Kubernetes Espace de noms du pod Kubernetes UID du pod Kubernetes ID du sandbox Kubernetes IP du nœud UUID du nœud Version Docker Configuration Kubernetes vue Source de la configuration Kubernetes OpenShift SCC Description Kubernetes Nom d’affichage Kubernetes Balises OpenShift Schéma Version du schéma Modèle de pod Contrôleur de hachage Révision Génération du modèle de pod de hachage Service Kompose Date de build du schéma Licence du schéma Nom du schéma Fournisseur de schéma Pod client Kubernetes StatefulSet Nom du pod Tenant Console Web Date de build Licence Fournisseur Architecture URL source faisant autorité Hôte de build RH Distribution des composants RH Portée Installation Responsable Publication Résumé de l’exécution Désinstallation	Octets de service d’E/S récursifs asynchrones Octets de service d’E/S récursifs en lecture Octets de service d’E/S récursifs en synchronisation Octets de service d’E/S récursifs Total d’octets de service d’E/S récursifs en écriture Octets de service d’E/S récursifs asynchrones avec service d’E/S récursifs en lecture Octets de service d’E/S récursifs en synchronisation avec service d’E/S récursifs Total d’E/S récursifs en écriture

Objet:	Identifiants :	Attributs:	Points de données :
Réseau de conteneurs Docker	Espace de noms Conteneur Nom Réseau Moteur Docker	Image du conteneur État du conteneur Version du conteneur Nom du nœud IP du nœud UUID du nœud Système d'exploitation du nœud Cluster K8s Version Docker ID du conteneur	RX Octets RX supprimés Erreurs RX Paquets RX TX Octets TX supprimés Erreurs TX Paquets TX

Objet:	Identifiants :	Attributs:	Points de données :
Processeur du conteneur Docker	Espace de noms Nom du conteneur CPU Moteur Docker	Hachage du conteneur Kubernetes Ports du conteneur Kubernetes Nombre de redémarrages du conteneur Kubernetes Chemin du message de fin du conteneur Kubernetes Politique de message de fin du conteneur Kubernetes Période de grâce de fin du pod Kubernetes Configuration Kubernetes vue Source de la configuration Kubernetes Image conteneur SCC OpenShift État du conteneur Version du conteneur Nom du nœud Chemin du journal du conteneur Kubernetes Nom du conteneur Kubernetes Type Docker Kubernetes Nom du pod Kubernetes Espace de noms du pod Kubernetes UID du pod Kubernetes ID du sandbox Kubernetes IP du nœud UUID du nœud Système d'exploitation du nœud Cluster Kubernetes Version Docker Description Kubernetes Nom d'affichage Kubernetes Balises OpenShift Version du schéma Modèle de pod Contrôleur de hachage Révision Génération du modèle de pod de hachage Service Kompose Date de build du schéma Licence du schéma Nom du schéma Fournisseur de schéma Pod client Kubernetes StatefulSet Nom du pod Tenant Date de build de la console Web Licence Fournisseur Architecture URL source faisant autorité Hôte de build RH Distribution des composants RH Portée Installer Responsable de	Périodes de limitation Périodes de limitation Durée de limitation Utilisation en mode noyau Utilisation en mode utilisateur Pourcentage d'utilisation Utilisation du système Total

Dépannage

Problème:	Essayez ceci:
Je ne vois pas mes métriques Docker dans Data Infrastructure Insights après avoir suivi les instructions sur la page de configuration.	Vérifiez les journaux de l'agent Telegraf pour voir s'il signale l'erreur suivante : E! Erreur dans le plugin [inputs.docker] : l'autorisation a été refusée lors de la tentative de connexion au socket du démon Docker. Si c'est le cas, prenez les mesures nécessaires pour fournir à l'agent Telegraf l'accès au socket Docker Unix comme spécifié ci-dessus.

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Elasticsearch

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

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Elasticsearch.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
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 que vous utilisez pour collecter des données.

[Configuration d'Elasticsearch]

Installation

Des informations peuvent être trouvées dans le"Documentation d'Elasticsearch" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

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

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Flink

Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques de Flink.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Flink.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
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 que vous utilisez pour collecter des données.

[Configuration Flink]

Installation

Un déploiement Flink complet implique les composants suivants :

JobManager : le système principal de Flink. Coordonne une série de gestionnaires de tâches. Dans une configuration haute disponibilité, le système aura plus d'un JobManager. Gestionnaire des tâches : c'est ici que les opérateurs Flink sont exécutés. Le plugin Flink est basé sur le plugin Jolokia de Telegraf. En tant qu'exigence de collecte d'informations à partir de tous les composants 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.

Installation

Agent Jar Jolokia

Pour tous les composants individuels, une version du fichier jar de l'agent Jolokia doit être téléchargée. La version testée était"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/flink/lib/ ».

Gestionnaire de tâches

Pour configurer JobManager afin d'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 port différent pour Jolokia (8778).  Si vous
disposez d'une IP interne sur laquelle verrouiller Jolokia, vous pouvez
remplacer le « catch all » 0.0.0.0 par votre propre IP.  Notez que cette
IP doit être accessible depuis le plugin Telegraf.
```

Gestionnaire de tâches

Pour configurer les gestionnaires de tâches afin d'exposer l'API Jolokia, vous pouvez configurer la variable d'environnement suivante sur vos nœuds, puis redémarrer le gestionnaire de tâches :

```
 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 port différent pour Jolokia (8778).  Si vous
disposez d'une IP interne sur laquelle verrouiller Jolokia, vous pouvez
remplacer le « catch all » 0.0.0.0 par votre propre IP.  Notez que cette
IP doit être accessible depuis le plugin 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 réseau disponibles Segments de mémoire réseau totaux Nombre de nettoyages PS (nettoyage de la mémoire) Temps de nettoyage PS (nettoyage de la mémoire) Nombre de nettoyages PS (nettoyage de la mémoire) Temps de nettoyage PS (nettoyage de la mémoire) Mémoire du tas engagée Mémoire du tas d’initialisation Mémoire du tas max. utilisée Nombre de threads Nombre de threads du démon Nombre maximal de threads Nombre total de threads démarrés
Flink Job	ID de tâche du serveur d’espace de noms de cluster	Nom du nœud Nom du travail IP du nœud Dernier point de contrôle Chemin externe Heure de redémarrage	Temps d’arrêt Redémarrages complets Alignement du dernier point de contrôle Mise en mémoire tampon Durée du dernier point de contrôle Taille du dernier point de contrôle Nombre de points de contrôle terminés Nombre de points de contrôle échoués Nombre de points de contrôle en cours Nombre de points de contrôle Temps de disponibilité

Objet:	Identifiants :	Attributs:	Points de données :
Gestionnaire de tâches Flink	Serveur d’espace de noms de cluster	Nom du nœud IP du nœud	Nombre de nettoyages PS MarkSweep pour la collecte des déchets Temps de nettoyage PS MarkSweep Nombre de nettoyages PS pour la collecte des déchets Temps de nettoyage PS pour la collecte des déchets Mémoire du tas engagée Mémoire du tas d’initialisation Mémoire maximale du tas utilisée Nombre de gestionnaires de tâches enregistrés Nombre de tâches en cours d’exécution Emplacements de tâches disponibles Nombre total de threads Nombre de threads du démon Nombre maximal de threads Nombre total de threads démarrés

Objet:	Identifiants :	Attributs:	Points de données :
Tâche Flink	Espace de noms du cluster ID de travail ID de tâche	Nom du nœud du serveur Nom du travail Index des sous-tâches ID de tentative de tâche Numéro de tentative de tâche Nom de la tâche ID du gestionnaire de tâches IP du nœud Filigrane d'entrée actuel	Tampons dans le pool Utilisation Tampons dans la file d'attente Longueur Tampons en sortie du pool Utilisation Tampons en sortie Longueur de la file d'attente Nombre Tampons en local Nombre Tampons en local par seconde Nombre Tampons en local Taux par seconde Nombre Tampons en distant Nombre Tampons en distant par seconde Nombre Tampons en distant Taux par seconde Nombre Tampons en sortie Nombre Tampons en sortie par seconde Nombre Tampons en sortie par seconde Nombre Octets en local Nombre Octets en local par seconde Nombre Octets en local par seconde Nombre Octets en local par seconde Nombre Octets en distant Nombre Octets en distant par seconde Nombre Octets en distant par seconde Nombre Octets en sortie Nombre Octets en sortie par seconde Nombre Octets en sortie par seconde Nombre Enregistrements en entrée Nombre Enregistrements en entrée par seconde Nombre Enregistrements en entrée par seconde Nombre Enregistrements en sortie Nombre Enregistrements en sortie par seconde Nombre Enregistrements en sortie par seconde Nombre Enregistrements en sortie par seconde Nombre Enregistrements en sortie par seconde

Objet:	Identifiants :	Attributs:	Points de données :
Opérateur de tâche Flink	Espace de noms du cluster ID de travail ID d'opérateur ID de tâche	Nom du nœud du serveur Nom du travail Nom de l'opérateur Index des sous-tâches ID de tentative de tâche Numéro de tentative de tâche Nom de la tâche ID du gestionnaire de tâches IP du nœud	Filigrane d'entrée actuel Filigrane de sortie actuel Nombre d'enregistrements entrants Nombre d'enregistrements entrants par seconde Nombre d'enregistrements entrants par seconde Taux Nombre d'enregistrements sortants Nombre d'enregistrements sortants par seconde Taux Nombre d'enregistrements en retard abandonnés Partitions affectées Octets Taux de consommation Latence de validation Latence de validation moyenne Taux de validation maximal Validations échouées Validations réussies Taux de fermeture de connexion Nombre de connexions Taux de création de connexion Nombre Latence de récupération Latence de récupération moyenne Taux de récupération maximal Taille de récupération Taille moyenne de récupération maximale Délai de limitation de récupération Temps de limitation de récupération moyen Taux de pulsation maximal Taux d'octets entrants Rapport E/S Temps E/S moyen (ns) Rapport d'attente E/S Temps d'attente E/S moyen (ns) Taux de jointure Heure de jointure moyenne Il y a le dernier battement de cœur Taux E/S réseau Taux d'octets sortants Taux de consommation d'enregistrements Retard d'enregistrements Max Enregistrements par requête Taux de requête moyen Taille de requête Taille moyenne de requête

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Hadoop

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

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Hadoop.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
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 que vous utilisez pour collecter des données.

[Configuration Hadoop] [Configuration Hadoop]

Installation

Un déploiement Hadoop complet implique les composants suivants :

- NameNode : le système principal du système de fichiers distribué Hadoop (HDFS). Coordonne une série de DataNodes.
- NameNode secondaire : un basculement à chaud pour le NameNode principal. Dans Hadoop, la promotion vers NameNode ne se produit pas automatiquement. Le NameNode secondaire collecte les informations du NameNode pour être prêt à être promu en cas de besoin.
- DataNode : propriétaire actuel des données.
- ResourceManager : le système de calcul principal (Yarn). Coordonne une série de NodeManagers.
- NodeManager : la ressource pour le calcul. Emplacement réel d'exécution des applications.
- JobHistoryServer : responsable du traitement de toutes les demandes liées à l'historique des tâches.

Le plugin Hadoop est basé sur le plugin Jolokia de Telegraf. En tant qu'exigence de collecte d'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 sur la version Hadoop 2.9.2.

Installation

Agent Jar Jolokia

Pour tous les composants individuels, une version du fichier jar de l'agent Jolokia doit être téléchargée. La version testée était"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/hadoop/lib/ ».

NomNode

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 du nœud secondaire

Pour configurer le NameNode secondaire afin d'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 afin d'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.
```

Gestionnaire de ressources

Pour configurer le ResourceManager afin d'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 nœuds

Pour configurer les NodeManagers 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.
```

Serveur d'historique des tâches

Pour configurer le JobHistoryServer 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 du nœud secondaire Hadoop	Serveur d'espace de noms de cluster	Nom du nœud IP du nœud Informations de compilation Version
Gestionnaire de nœuds Hadoop	Serveur d'espace de noms de cluster	Nom du nœud IP du nœud
Gestionnaire de ressources Hadoop	Serveur d'espace de noms de cluster	Nom du nœud IP du nœud

Objet:	Identifiants :	Attributs:
Nœud de données Hadoop	Serveur d'espace de noms de cluster	Nom du nœud IP du nœud ID du cluster Version
Nom du nœud Hadoop	Serveur d'espace de noms de cluster	Nom du nœud IP du nœud ID de transaction Dernière heure d'écriture depuis le dernier chargement Modifications État HA État du système de fichiers ID du pool de blocs ID du cluster Informations de compilation Nombre de versions distinctes Version
Serveur d'historique des tâches Hadoop	Serveur d'espace de noms de cluster	Nom du nœud IP du nœud

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données HAProxy

Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de HAProxy.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez HAProxy.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
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 que vous utilisez pour collecter des données.

[Configuration de HAProxy]

Installation

Le plugin de Telegraf pour HAProxy repose sur l'activation de HAProxy Stats. Il s'agit d'une configuration intégrée à HAProxy, mais elle n'est pas activée par défaut. Lorsqu'il est activé, HAProxy exposera un point de terminaison HTML qui peut être visualisé sur votre navigateur ou récupéré pour l'extraction de l'état de toutes les configurations HAProxy.

Compatibilité:

La configuration a été développée par rapport à la version HAProxy 1.9.4.

Installation :

Pour activer les statistiques, modifiez votre fichier de configuration haproxy et ajoutez les lignes suivantes après la section « defaults », en utilisant votre propre nom d'utilisateur/mot de passe et/ou URL haproxy :

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

Voici un exemple simplifié de fichier de configuration avec les 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 des instructions complètes et à jour, consultez le"Documentation HAProxy" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Interface HAProxy	Proxy d'adresse d'espace de noms	Nœud IP Nom du nœud ID proxy Mode ID de processus Limite de débit de sessions ID du serveur Limite de sessions Statut	Octets entrants Octets sortants Accès au cache Recherches dans le cache Compression Octets contournés Compression Octets entrants Compression Octets sortants Réponses Taux de connexion Taux de connexion Nombre maximal de connexions Nombre total de requêtes refusées par la règle de connexion Requêtes refusées par des problèmes de sécurité Réponses refusées par des problèmes de sécurité Requêtes refusées par la règle de session Erreurs de requêtes Réponses Réponses 1xx Réponses 2xx Réponses 3xx Réponses 4xx Réponses 5xx Autres requêtes Sessions interceptées Taux Sessions Taux Max Requêtes Taux Requêtes Taux Max Requêtes Total Sessions Sessions Max Sessions Total Requêtes Réécritures

Objet:	Identifiants :	Attributs:	Points de données :
Serveur HAProxy	Serveur proxy d'adresse d'espace de noms	Nœud IP Nom du nœud Heure de fin de vérification Configuration de chute Vérification de la valeur d'intégrité Vérification de la configuration de montée Statut ID proxy Heure de la dernière modification Heure de la dernière session Mode ID de processus ID du serveur Statut Poids	Serveurs actifs Serveurs de sauvegarde Octets entrants Octets sortants Vérifications échouées Abandons de vérification Client Connexions Temps moyen de connexion Temps d'arrêt Total des réponses refusées Erreurs de connexion Erreurs de réponse Réponses 1xx Réponses 2xx Réponses 3xx Réponses 4xx Réponses 5xx Autre serveur sélectionné File d'attente totale File d'attente actuelle Temps moyen maximal de la file d'attente Sessions par seconde Sessions par seconde Temps de réponse maximal de réutilisation de connexion Moyenne Sessions Sessions Transfert de serveur max. Abandons Sessions Total des sessions Temps total Moyenne des requêtes Redispatches Requêtes Nouvelles tentatives Requêtes Réécritures

Objet:	Identifiants :	Attributs:	Points de données :
Backend HAProxy	Proxy d'adresse d'espace de noms	Nœud IP Nom du nœud ID proxy Heure de la dernière modification Heure de la dernière session Mode ID du processus ID du serveur Limite de sessions Statut Poids	Serveurs actifs Serveurs de sauvegarde Octets entrants Octets sortants Accès au cache Consultations dans le cache Vérifications Abandons client Compression Octets contournés Compression Octets entrants Compression Octets sortants Réponses Connexions Temps moyen de connexion Temps d'arrêt Total des requêtes refusées pour des raisons de sécurité Réponses refusées pour des raisons de sécurité Erreurs de connexion Erreurs de réponse Réponses 1xx Réponses 2xx Réponses 3xx Réponses 4xx Réponses 5xx Autre serveur sélectionné File d'attente totale File d'attente actuelle Temps moyen de file d'attente Sessions par seconde Sessions par seconde Nombre maximal de requêtes Réutilisation totale des connexions Temps de réponse moyen Sessions Sessions Nombre maximal d'abandons de transfert de serveur Sessions Total des sessions Temps total Moyenne des requêtes Redispatches Requêtes Nouvelles tentatives Requêtes Réécritures

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données JVM

Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques

à partir de JVM.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez JVM.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
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 que vous utilisez pour collecter des données.

[Configuration JVM]

Installation

Des informations peuvent être trouvées dans"Documentation JVM" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
JVM	Espace de noms JVM	Architecture du système d'exploitation Nom du système d'exploitation Version du système d'exploitation Spécification d'exécution Fournisseur de spécifications d'exécution Version de spécification d'exécution Temps de disponibilité Nom de la machine virtuelle d'exécution Fournisseur de la machine virtuelle d'exécution Version de la machine virtuelle d'exécution Nom du nœud IP du nœud	Classe chargée Classe chargée Classe totale déchargée Tas de mémoire Mémoire engagée Tas de mémoire d'initialisation Mémoire utilisée maximale du tas de mémoire utilisée Mémoire non engagée Mémoire non engagée Mémoire non utilisée du tas Mémoire maximale non utilisée du tas Objets en attente de finalisation Processeurs du système d'exploitation disponibles Taille de la mémoire virtuelle engagée du système d'exploitation Taille de la mémoire physique libre du système d'exploitation Taille de l'espace d'échange libre du système d'exploitation Nombre maximal de descripteurs de fichiers du système d'exploitation Nombre de descripteurs de fichiers ouverts du système d'exploitation Charge CPU du processeur du système d'exploitation Temps CPU du processeur du système d'exploitation Charge CPU système du système d'exploitation Charge moyenne du système d'exploitation Taille totale de la mémoire physique du système d'exploitation Taille totale de l'espace d'échange du système d'exploitation Nombre de démons de threads Nombre de pics de threads Nombre de threads Nombre total de threads démarrés Nombre de copies de collecte du ramasse-miettes Heure de collecte des copies du ramasse-miettes Nombre de collectes de marquage-balayage du ramasse-

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Kafka

Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de Kafka.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Kafka.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
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 que vous utilisez pour collecter des données.

[Configuration de Kafka]

Installation

Le plugin Kafka est basé sur le plugin Jolokia de Telegraf. En tant qu'exigence de collecte d'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 sur la version 0.11.0.2 de Kafka.

Mise en place

Toutes les instructions ci-dessous supposent que votre emplacement d'installation pour Kafka est « /opt/kafka ». Vous pouvez adapter les instructions ci-dessous pour refléter votre emplacement d'installation.

Agent Jar Jolokia

Une version du 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/ ».

Courtiers Kafka

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 le cas de machines à plusieurs IP, cela devra être modifié pour collecter l'IP qui vous intéresse pour les connexions RMI.

Vous pouvez choisir un port différent pour JMX (9999 ci-dessus) et Jolokia (8778). Si vous disposez d'une IP interne sur laquelle verrouiller Jolokia, vous pouvez remplacer le « catch all » 0.0.0.0 par votre propre IP. Notez que cette IP doit être accessible depuis le plugin Telegraf. Vous pouvez utiliser l'option '-Dcom.sun.management.jmxremote.authenticate=false' si vous ne souhaitez pas vous authentifier. Utilisez-le 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	Nom du nœud IP du nœud

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Kibana

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

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Kibana.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de

données, par exemple par système d'exploitation/plateforme.

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 que vous utilisez pour collecter des données.

[Configuration de Kibana]

Installation

Des informations peuvent être trouvées dans le"Documentation de 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	Nœud IP Nom du nœud Version État	Connexions simultanées Tas Tas max. utilisé Requêtes par seconde Temps de réponse Temps de réponse moyen Temps de disponibilité maximal

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

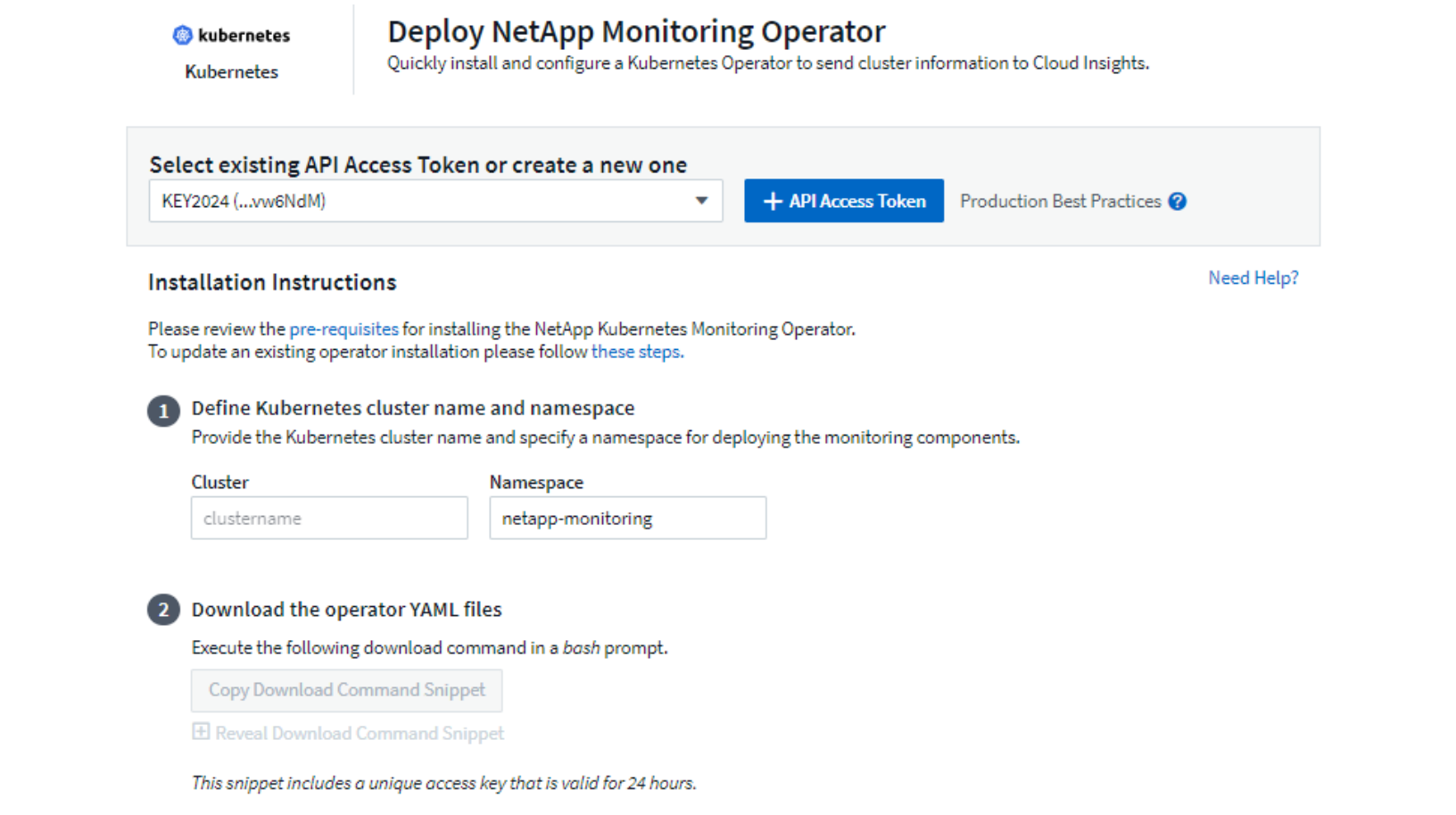
Installation et configuration de l'opérateur de surveillance Kubernetes

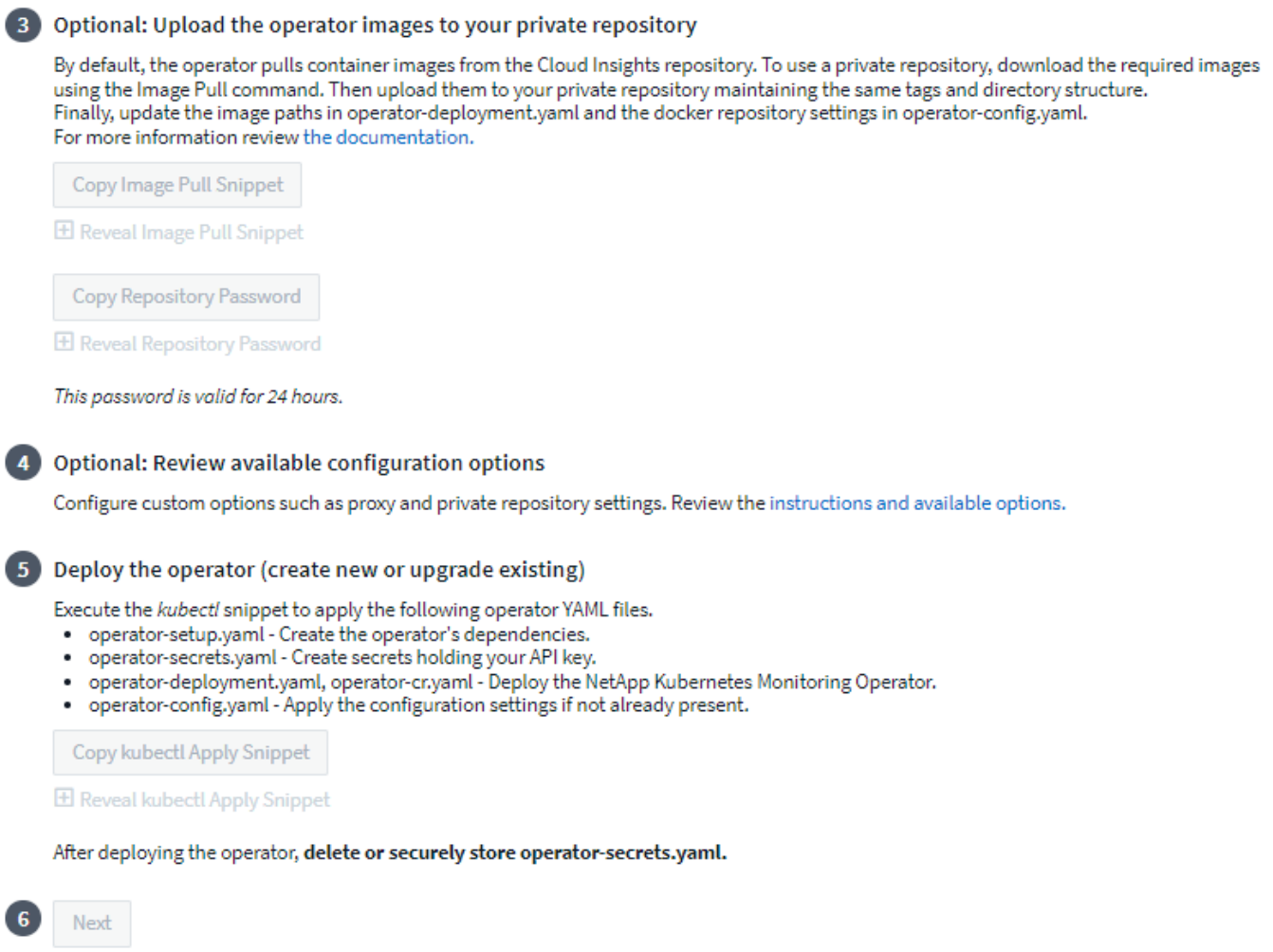
Data Infrastructure Insights propose l'opérateur de surveillance Kubernetes pour la collection Kubernetes. Accédez à **Kubernetes > Collecteurs > +Kubernetes Collector** pour déployer un nouvel opérateur.

Avant d'installer Kubernetes Monitoring Operator

Voir le"Prérequis" documentation avant d'installer ou de mettre à niveau Kubernetes Monitoring Operator.

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 pour installer l'agent Kubernetes Monitoring Operator sur Kubernetes :

1. Saisissez un nom de cluster et un espace de noms uniques. Si vous êtesmise à niveau à partir d'un opérateur Kubernetes précédent, utilisez le même nom de cluster et le même espace de noms.
2. Une fois ces informations saisies, vous pouvez copier l'extrait de commande de téléchargement dans le presse-papiers.
3. Collez l'extrait dans une fenêtre *bash* et exécutez-le. Les fichiers d'installation de l'opérateur seront téléchargés. Notez que l'extrait possède une clé unique et est valable 24 heures.
4. Si vous disposez d'un référentiel personnalisé ou privé, copiez l'extrait d'image facultatif, 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, examinez 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 l'extrait kubectl Apply, en le téléchargeant et en l'exécutant.
7. L'installation se déroule 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 disposez d'un référentiel personnalisé, lisez à proposen utilisant un référentiel Docker

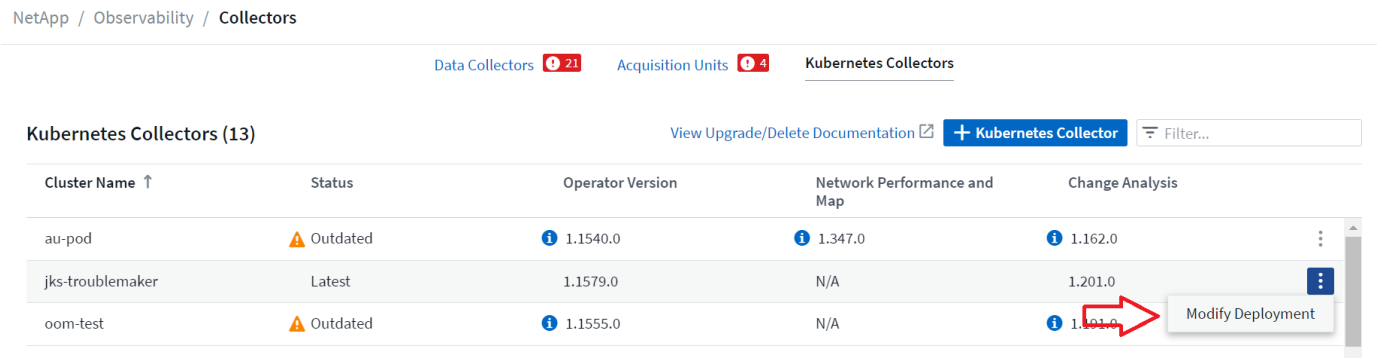
personnalisé/privé .

Composants de surveillance Kubernetes

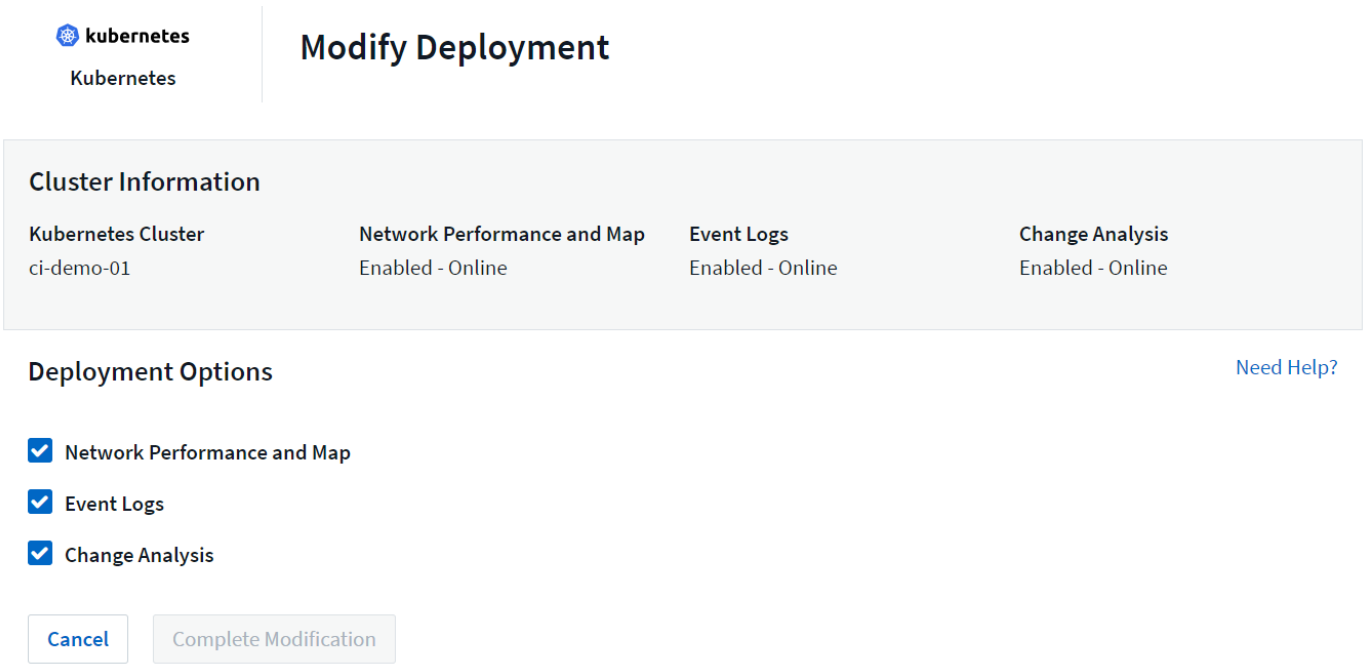
Data Infrastructure Insights Kubernetes Monitoring comprend quatre composants de surveillance :

- Mesures de cluster
- Performances et carte du réseau (facultatif)
- Journaux d'événements (facultatif)
- Analyse des changements (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 > Collecteurs** et en sélectionnant *Modifier le déploiement* 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 de ce collecteur selon vos besoins.



Mise à niveau vers la dernière version de Kubernetes Monitoring Operator

Mises à niveau du bouton-poussoir DII

Vous pouvez mettre à niveau l'opérateur de surveillance Kubernetes via la page Collecteurs Kubernetes DII. Cliquez sur le menu à côté du cluster que vous souhaitez mettre à niveau et sélectionnez *Mettre à niveau*. L'opérateur vérifiera les signatures d'image, effectuera un instantané de votre installation actuelle et effectuera la mise à niveau. Dans quelques minutes, vous devriez voir l'état de l'opérateur progresser de « Mise à niveau en cours » à « Dernière mise à jour ». Si vous rencontrez une erreur, vous pouvez sélectionner le statut d'erreur pour plus de détails et vous référer au tableau de dépannage des mises à niveau par bouton-poussoir ci-dessous.

Mises à niveau par simple pression d'un bouton avec des référentiels privés

Si votre opérateur est configuré pour utiliser un référentiel privé, assurez-vous que toutes les images requises pour exécuter l'opérateur et leurs signatures sont disponibles dans votre référentiel. Si vous rencontrez une erreur pendant le processus de mise à niveau pour des images manquantes, ajoutez-les simplement à votre référentiel et réessayez la mise à niveau. Pour télécharger les signatures d'image dans votre référentiel, veuillez utiliser l'outil de cosignature comme suit, en veillant à télécharger les signatures pour toutes les images spécifiées sous 3 Facultatif : Télécharger les images de l'opérateur dans votre référentiel privé > Extrait d'image

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

Revenir à une version précédemment exécutée

Si vous avez effectué une mise à niveau à l'aide de la fonction de mise à niveau par simple pression sur un bouton et que vous rencontrez des difficultés avec la version actuelle de l'opérateur dans les sept jours suivant la mise à niveau, vous pouvez rétrograder vers la version précédemment exécutée à l'aide de l'instantané créé pendant le processus de mise à niveau. Cliquez sur le menu à côté du cluster que vous souhaitez restaurer et sélectionnez *Restaurer*.

Mises à niveau manuelles

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

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
Si une _AgentConfiguration_ existe :
```

- Installationle dernier opérateur sur l'opérateur existant.
  - Assurez-vous que vous êtesextraire les dernières images de conteneurs si vous utilisez un référentiel personnalisé.

Si *AgentConfiguration* n'existe pas :

- Notez le nom de votre cluster tel qu'il est reconnu par Data Infrastructure Insights (si votre espace de noms n'est pas le netapp-monitoring par défaut, remplacez-le par l'espace de noms approprié) :

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Créez une sauvegarde de l'opérateur existant (si votre espace de noms
n'est pas le netapp-monitoring par défaut, remplacez-le par l'espace de
noms 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,Installation>>le
dernier opérateur.
```

  - Utilisez le même nom de cluster.
  - Après avoir téléchargé les derniers fichiers YAML de l'opérateur, reportez toutes les personnalisations trouvées dans *agent_backup.yaml* vers le fichier *operator-config.yaml* téléchargé avant le déploiement.
  - Assurez-vous que vous êtesextraire les dernières images de conteneurs si vous utilisez 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 pour l'opérateur de surveillance Kubernetes est « netapp-monitoring ». Si vous avez défini votre propre espace de noms, remplacez cet espace de noms dans ces commandes et fichiers et dans tous les suivants.

Les versions plus récentes de l'opérateur de surveillance peuvent être désinstallées avec les 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, supprimez l'espace de noms :

```
 kubectl delete ns <NAMESPACE>
Remarque : si la première commande renvoie « Aucune ressource trouvée »,
utilisez les instructions suivantes pour désinstaller les anciennes
versions de l'opérateur de surveillance.
```

Exécutez chacune des commandes suivantes dans l'ordre. 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 de Kube-state-metrics

L'opérateur de surveillance NetApp Kubernetes installe ses propres métriques d'état Kube pour éviter tout conflit avec d'autres instances.

Pour plus d'informations sur Kube-State-Metrics, voir"cette page" .

Configuration/Personnalisation de l'opérateur

Ces sections contiennent des informations sur la personnalisation de la configuration de votre opérateur, l'utilisation d'un 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 comprend des exemples de paramètres commentés. Voir la liste des"paramètres disponibles" pour la version la plus récente de 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 de la prise en charge du proxy

Il existe deux endroits où vous pouvez utiliser un proxy sur votre locataire afin d'installer Kubernetes Monitoring Operator. Il peut s'agir des mêmes systèmes proxy ou de systèmes proxy distincts :

- Proxy nécessaire lors de l'exécution de l'extrait de code d'installation (à l'aide de « curl ») pour connecter le système où l'extrait 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'un ou les deux, afin d'installer Kubernetes Operating Monitor, 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 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 Kubernetes Operating Monitor, avant d'installer l'opérateur, définissez les variables d'environnement *http_proxy/https_proxy*. Pour certains environnements proxy, vous devrez peut-être également définir la variable d'environnement *no_proxy*.

Pour définir la ou les variables, effectuez les étapes suivantes sur votre système **avant** d'installer Kubernetes Monitoring Operator :

1. Définissez les variables d'environnement *https_proxy* et/ou *http_proxy* pour l'utilisateur actuel :
    a. Si le proxy en cours de configuration ne dispose 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 cette
commande :
```

```
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 Kubernetes Monitoring Operator après avoir lu toutes ces instructions.

Configurez la section proxy de *AgentConfiguration* dans *operator-config.yaml* avant de déployer le Kubernetes Monitoring Operator.

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

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

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

Utiliser 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 disposez d'un cluster Kubernetes utilisé comme cible pour la surveillance et que ce cluster est configuré pour extraire uniquement des 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 nécessaires à l'opérateur de surveillance Kubernetes.

Exécutez « Image Pull Snippet » à partir de la mosaïque d'installation de NetApp Monitoring Operator. Cette commande se connectera au référentiel Data Infrastructure Insights , extraira toutes les dépendances d'image pour l'opérateur et se déconnectera du référentiel Data Infrastructure Insights . Lorsque vous y êtes invité, saisissez le mot de passe temporaire du référentiel fourni. Cette commande télécharge toutes les images utilisées par l'opérateur, y compris pour les fonctionnalités optionnelles. Voir ci-dessous pour les fonctionnalités pour lesquelles ces images sont utilisées.

Fonctionnalités de l'opérateur principal et surveillance de Kubernetes

- surveillance netapp
- proxy ci-kube-rbac
- ci-ksm
- ci-telegraf
- utilisateur root sans distribution

Journal des événements

- ci-fluent-bit
- exportateur d'événements ci-kubernetes

Performances et carte du réseau

- ci-net-observer

Poussez l'image Docker de l'opérateur vers votre référentiel Docker privé/local/d'entreprise conformément à vos politiques d'entreprise. Assurez-vous que les balises d'image et les chemins d'accès aux répertoires de 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 *AgentConfiguration* dans *operator-config.yaml* pour refléter le nouvel emplacement du dépôt docker. Créez un nouveau imagePullSecret pour votre dépôt privé, pour plus de détails, consultez *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
```

Jeton d'accès API pour les mots de passe à long terme

Certains environnements (par exemple, les dépôts proxy) exigent des mots de passe à long terme pour le dépôt docker de Data Infrastructure Insights. Le mot de passe fourni dans l'interface utilisateur lors de l'installation n'est valable que 24 heures. Au lieu de cela, on peut utiliser un jeton d'accès API comme mot de passe du dépôt docker. Ce mot de passe sera valable aussi longtemps que le jeton d'accès API est valide. On peut générer un nouveau jeton d'accès API à cette fin ou en utiliser un existant.

"Lire ici" pour obtenir des instructions sur la création d'un nouveau jeton d'accès API.

Pour extraire un jeton d'accès API existant à partir d'un fichier *operator-secrets.yaml* téléchargé, les utilisateurs peuvent exécuter la commande suivante :

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

Pour extraire un jeton d'accès API existant d'une installation d'opérateur en cours d'exécution, les utilisateurs peuvent exécuter la commande suivante :

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

Instructions OpenShift

Si vous utilisez OpenShift 4.6 ou une version ultérieure, vous devez modifier *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 souillures

Les DaemonSets *netapp-ci-telegraf-ds*, *netapp-ci-fluent-bit-ds* et *netapp-ci-net-observer-l4-ds* 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 certaines **souillures** bien connues. Si vous avez configuré des taches personnalisées sur vos nœuds, empêchant ainsi les pods de s'exécuter sur chaque nœud, vous pouvez créer une **tolérance** pour ces taches"dans *AgentConfiguration*" . Si vous avez appliqué des taches personnalisées 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 de l'opérateur.

En savoir plus sur Kubernetes"Souillures et tolérances" .

Retour à la"* Page d'installation de l'opérateur de surveillance NetApp Kubernetes*"

Une note sur les secrets

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

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

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'analyse des changements est activée, modifiez *AgentConfiguration* ou *operator-config.yaml* pour supprimer le commentaire de la section de gestion des changements et inclure *kindsToIgnoreFromWatch: '"secrets"'* sous la section de gestion des changements. 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'image 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 cosignature 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 : téléchargez les images de l'opérateur dans votre référentiel privé >*

Clé publique de signature d'image

Pour vérifier manuellement une signature d'image, procédez comme suit :

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 de cosign. Reportez-vous à l'exemple suivant d'utilisation de cosignature

```
$ 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

Quelques éléments à essayer si vous rencontrez des problèmes lors de la configuration de l'opérateur de surveillance Kubernetes :

Problème:	Essayez ceci:
Je ne vois pas d'hyperlien/connexion entre mon volume persistant Kubernetes et le périphérique de stockage back-end correspondant. Mon volume persistant Kubernetes est configuré à l'aide du nom d'hôte du serveur de stockage.	Suivez les étapes pour désinstaller l'agent Telegraf existant, puis réinstaller le dernier agent Telegraf. Vous devez utiliser Telegraf version 2.0 ou ultérieure et votre stockage de cluster Kubernetes doit être activement surveillé par Data Infrastructure Insights.

Problème:	Essayez ceci:
Je vois des messages dans les journaux ressemblant à ce qui suit : E0901 15:21:39.962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Failed to list *v1.MutatingWebhookConfiguration: the server could not find the requested resource E0901 15:21:43.168161 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Failed to list *v1.Lease: the server could not find the requested resource (get leases.coordination.k8s.io) etc.	Ces messages peuvent se produire si vous exécutez kube-state-metrics version 2.0.0 ou supérieure avec des versions de Kubernetes inférieures à 1.20. Pour obtenir la version de Kubernetes : *kubectl version* Pour obtenir la version de kube-state-metrics : *kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* Pour éviter que ces messages ne se produisent, les utilisateurs peuvent modifier leur déploiement kube-state-metrics pour désactiver les baux suivants : *mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources* Plus précisément, ils peuvent utiliser l'argument CLI suivant : resources=certificatesigningrequests,configmaps,cronjobs,daemonsets, deployments,endpoints,horizontalpodautoscalers,ingresses,jobs,limitranges, namespaces,networkpolicies,nodes,persistentvolumeclaims,persistentvolumes, poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas, La liste de ressources par défaut est : « certificatesigningrequests,configmaps,cronjobs,daemonsets,deployments,endpoints,horizontalpodautoscalers,ingresses,jobs,leases,limitranges,mutatingwebhookconfigurations,namespaces,networkpolicies,nodes, persistentvolumeclaims,persistentvolumes,poddisruptionbudgets,pods,replicasets,replicationcontrollers,resourcequotas,secrets,services,statefulsets,storageclasses,validatingwebhookconfigurations,volumeattachments »
Je vois des messages d'erreur de Telegraf ressemblant à ce qui suit, mais Telegraf démarre et s'exécute : 11 oct. 14:23:41 ip-172-31-39-47 systemd[1] : Démarré L'agent serveur piloté par plug-in pour la création de rapports de métriques dans InfluxDB. 11 oct. 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="échec de la création du répertoire de cache. /etc/telegraf/.cache/snowflake, err : mkdir /etc/telegraf/.ca che : permission refusée. ignoré\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" Oct 11 14:23:41 ip-172-31-39-47 telegraf[1827] : time="2021-10-11T14:23:41Z" level=error msg="échec d'ouverture. Ignoré. ouvrez /etc/telegraf/.cache/snowflake/ocsp_response_cache.json : aucun fichier ou répertoire de ce type\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" 11 oct. 14:23:41 ip-172-31-39-47 telegraf[1827] : 2021-10-11T14:23:41Z Je ! Démarrage de Telegraf 1.19.3	Il s'agit d'un problème connu. Se référer à"Cet article GitHub" pour plus de détails. Tant que Telegraf est opérationnel, les utilisateurs peuvent ignorer ces messages d'erreur.

Problème:	Essayez ceci:
Sur Kubernetes, mes pods Telegraf signalent l'erreur suivante : « Erreur lors du traitement des informations mountstats : échec d'ouverture du fichier mountstats : /hostfs/proc/1/mountstats, erreur : ouverture de /hostfs/proc/1/mountstats : autorisation refusée »	Si SELinux est activé et appliqué, il empêche probablement les pods Telegraf d'accéder au fichier /proc/1/mountstats sur le nœud Kubernetes. Pour surmonter cette restriction, modifiez la configuration de l'agent et activez le paramètre runPrivileged. Pour plus de détails, reportez-vous aux instructions OpenShift.
Sur Kubernetes, mon pod Telegraf ReplicaSet signale l'erreur suivante : [inputs.prometheus] Erreur dans le plugin : impossible de charger la paire de clés /etc/kubernetes/pki/etcd/server.crt:/etc/kubernetes/pki/etcd/server.key : ouvrir /etc/kubernetes/pki/etcd/server.crt : aucun fichier ou répertoire de ce type	Le pod Telegraf ReplicaSet est destiné à 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 obtiendrez ces erreurs. Vérifiez si vos nœuds maître/etcd sont contaminés. Si c'est le cas, ajoutez les tolérances nécessaires au Telegraf ReplicaSet, telegraf-rs. Par exemple, modifiez le ReplicaSet… kubectl edit rs telegraf-rs … et ajoutez les tolérances appropriées à la spécification. Ensuite, redémarrez 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 stratégie de sécurité des pods (PSP) ou l'admission de sécurité des pods (PSA) en place, vous devez effectuer une mise à niveau vers la dernière version de Kubernetes Monitoring Operator. Suivez ces étapes pour mettre à niveau vers l'opérateur actuel avec prise en charge de PSP/PSA : 1. Désinstaller l'opérateur de surveillance précédent : kubectl delete agent agent-monitoring-netapp -n netapp-monitoring kubectl delete ns netapp-monitoring kubectl delete crd agents.monitoring.netapp.com kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding 2. Installation la dernière version de l'opérateur de surveillance.
J'ai rencontré des problèmes lors du déploiement de l'opérateur et j'utilise PSP/PSA.	1. Modifiez l'agent à l'aide de la commande suivante : kubectl -n <name-space> edit agent 2. Marquer « security-policy-enabled » comme « faux ». Cela désactivera les politiques de sécurité des pods et l'admission de sécurité des pods et permettra à l'opérateur de se déployer. Confirmez en utilisant les commandes suivantes : kubectl get psp (devrait indiquer que la politique de sécurité du pod a été supprimée) kubectl get all -n <namespace>
grep -i psp (devrait indiquer que rien n'est trouvé)	Erreurs « ImagePullBackoff » observées
Ces erreurs peuvent être observées si vous disposez d'un référentiel Docker personnalisé ou privé et que vous n'avez pas encore configuré l'opérateur de surveillance Kubernetes pour le reconnaître correctement. En savoir plus à propos de la configuration pour un 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:	Essayez ceci:

Capturez ou notez autrement la sortie des commandes suivantes et contactez 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-observer (Workload Map) dans l'espace de noms Operator sont dans CrashLoopBackOff

Ces pods correspondent au collecteur de données Workload Map pour l'observabilité du réseau. Essayez ceci : • Vérifiez les journaux de l'un des pods pour confirmer la version minimale du noyau. Par exemple : ---- {"ci-tenant-id":"votre-id-de-tenant","collector-cluster":"votre-nom-de-cluster-k8s","environment":"prod","level":"error","msg":"échec de validation. Raison : la version du noyau 3.10.0 est inférieure à la version minimale du noyau 4.18.0","time":"2022-11-09T08:23:08Z"} ---- • Les pods Net-observer nécessitent 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'elle est >= 4.18.0	Les pods s'exécutent dans l'espace de noms de l'opérateur (par défaut : netapp-monitoring), mais aucune donnée n'est affichée dans l'interface utilisateur pour la carte de charge de travail ou les métriques Kubernetes dans les requêtes.
Vérifiez le réglage de l'heure sur les nœuds du cluster K8S. Pour un audit et des rapports de données précis, il est fortement recommandé de synchroniser l'heure sur la machine Agent à l'aide du protocole Network Time Protocol (NTP) ou du protocole Simple Network Time Protocol (SNTP).	Certains des pods d'observateur réseau dans l'espace de noms Operator sont en état d'attente
Net-observer est un DaemonSet et exécute un pod dans chaque nœud du cluster k8s. • Notez le pod qui est en état d'attente et vérifiez s'il rencontre un problème de ressources 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 Kubernetes Monitoring Operator : [inputs.prometheus] Erreur dans le plugin : erreur lors de la requête HTTP vers http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics : obtenir http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics : numérotation TCP : recherche kube-state-metrics.<namespace>.svc.cluster.local : aucun hôte de ce type

Problème:	Essayez ceci:
Ce message n'apparaît généralement que lorsqu'un nouvel opérateur est installé et que le pod *telegraf-rs* est opérationnel avant le pod *ksm*. Ces messages devraient cesser une fois que tous les pods sont en cours d'exécution.	Je ne vois aucune métrique collectée pour les CronJobs Kubernetes qui existent dans mon cluster.
Vérifiez votre version de Kubernetes (c'est-à-dire `kubectl version`). S'il s'agit de la version 1.20.x ou d'une version antérieure, il s'agit d'une limitation attendue. La version kube-state-metrics déployée avec l'opérateur de surveillance Kubernetes prend uniquement en charge la version v1.CronJob. Avec Kubernetes 1.20.x et versions antérieures, la ressource CronJob se trouve dans v1beta.CronJob. Par conséquent, kube-state-metrics ne peut pas trouver la ressource CronJob.	Après l'installation de l'opérateur, les pods telegraf-ds entrent dans CrashLoopBackOff et les journaux des pods indiquent « su : échec d'authentification ».
Modifiez la section telegraf dans *AgentConfiguration*, et définissez *dockerMetricCollectionEnabled* sur false. Pour plus de détails, consultez le "options de configuration" de l'opérateur. … spec: … telegraf: … - name: docker run-mode: - DaemonSet substitutions: - key: DOCKER_UNIX_SOCK_PLACEHOLDER value: unix:///run/docker.sock … …	Je vois des messages d'erreur répétés ressemblant à ce qui suit dans mes journaux Telegraf : E! [agent] Erreur lors de l'écriture dans outputs.http : Post "https://<tenant_url>/rest/v1/lake/ingest/influxdb" : délai de contexte dépassé (Client.Timeout dépassé lors de l'attente des en-têtes)
Modifiez la section Telegraf dans *AgentConfiguration* et augmentez *outputTimeout* à 10 s. Pour plus de détails, reportez-vous au manuel de l'opérateur."options de configuration" .	Il me manque des données *involvedobject* pour certains journaux d'événements.
Assurez-vous d'avoir suivi les étapes décrites dans la"Autorisations" section ci-dessus.	Pourquoi est-ce que je vois deux pods d'opérateurs de surveillance en cours d'exécution, l'un nommé netapp-ci-monitoring-operator-<pod> et l'autre nommé monitoring-operator-<pod> ?
À compter du 12 octobre 2023, Data Infrastructure Insights a remanié l'opérateur pour mieux servir nos utilisateurs ; pour que ces changements soient pleinement adoptés, vous devezsupprimer l'ancien opérateur etinstaller le nouveau .	Mes événements Kubernetes ont cessé de manière inattendue d'être signalés à Data Infrastructure Insights.
Récupérer le nom du pod exportateur d'événements : `kubectl -n netapp-monitoring get pods`	grep event-exporter

Problème:	Essayez ceci:
awk '{print $1}'	sed 's/event-exporter./event-exporter/'` Il doit s'agir soit de « netapp-ci-event-exporter » soit de « event-exporter ». Ensuite, modifiez l'agent de surveillance `kubectl -n netapp-monitoring edit agent` et définissez la valeur de LOG_FILE pour refléter 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-exporter.log » ou « /var/log/containers/event-exporter*.log » …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. Alternativement, on peut aussidésinstaller etréinstaller l'agent.
Je vois que des pods déployés par l'opérateur de surveillance Kubernetes se bloquent en raison de ressources insuffisantes.	Consultez l'opérateur de surveillance Kubernetes"options de configuration" pour augmenter les limites du processeur et/ou de la mémoire selon les besoins.
Une image manquante ou une configuration non valide a entraîné l'échec du démarrage ou de la préparation des pods netapp-ci-kube-state-metrics. Désormais, le StatefulSet est bloqué et les modifications de configuration ne sont pas appliquées aux pods netapp-ci-kube-state-metrics.	Le StatefulSet est dans un"cassé" État. Après avoir résolu les problèmes de configuration, faites rebondir les pods netapp-ci-kube-state-metrics.
Les pods netapp-ci-kube-state-metrics ne parviennent pas à démarrer après l'exécution d'une mise à niveau de l'opérateur Kubernetes, générant ErrImagePull (échec de l'extraction de l'image).	Essayez de réinitialiser les pods manuellement.
Les messages « Événement rejeté car plus ancien que maxEventAgeSeconds » sont observés pour mon cluster Kubernetes sous Analyse des journaux.	Modifiez l'opérateur *agentconfiguration* et augmentez *event-exporter-maxEventAgeSeconds* (c'est-à-dire à 60 s), *event-exporter-kubeQPS* (c'est-à-dire à 100) et *event-exporter-kubeBurst* (c'est-à-dire à 500). Pour plus de détails sur ces options de configuration, consultez le"options de configuration" page.

Problème:	Essayez ceci:
Telegraf avertit ou plante à cause 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'agent NKMO et définissez *unprotected* sur *true*. Cela indiquera 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 le disque, cela permet l'exécution dans des environnements où la réservation de mémoire verrouillée n'est pas possible. Pour plus de détails sur les options de configuration *non protégées*, 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 de lecture de /dev/vdc : aucun fichier ou répertoire de ce type*	Pour l'opérateur de surveillance Kubernetes, ces messages d'avertissement sont sans conséquence et peuvent être ignorés. Vous pouvez également modifier la section telegraf dans AgentConfiguration et définir *runDsPrivileged* sur true. Pour plus de détails, consultez le "options de configuration de l'opérateur".

Problème:	Essayez ceci:

Mon pod Fluent-bit échoue avec les erreurs suivantes : [2024/10/16 14:16:23] [error] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno=24] Trop de fichiers ouverts [2024/10/16 14:16:23] [error] échec d'initialisation de l'entrée tail.0 [2024/10/16 14:16:23] [error] [engine] échec d'initialisation de l'entrée	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 après chaque redémarrage du 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:	Essayez ceci:
Les pods DS de Telegraf signalent des erreurs liées au fait que le plug-in d’entrée Kubernetes ne parvient pas à effectuer des requêtes HTTP en raison de l’impossibilité de valider le certificat TLS. Par exemple : E! [inputs.kubernetes] Erreur dans le plugin : erreur lors de la requête HTTP vers"<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 vérification du certificat : x509 : impossible de valider le certificat pour <kubelet_IP> car il ne contient aucun 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 *Subject Alternative Name* des certificats. Pour résoudre ce problème, l'utilisateur peut modifier le"configuration de l'agent" , et définissez *telegraf:insecureK8sSkipVerify* sur *true*. Cela configurera le plugin d'entrée Telegraf pour ignorer la vérification. Alternativement, l'utilisateur peut configurer le kubelet pour"serveurTLSBootstrap" , ce qui déclenchera une demande de certificat à partir de l'API « certificates.k8s.io ».
Je rencontre l'erreur suivante dans les pods Fluent-bit et le pod ne peut pas démarrer : [2026/01/12 20:20:32] [error] [sqldb] error=unable to open database file [2026/01/12 20:20:32] [error] [input:tail:tail.0] db: could not create 'in_tail_files' table [2026/01/12 20:20:32] [error] [input:tail:tail.0] could not open/create database [2026/01/12 20:20:32] [error] failed initialize input tail.0 [2026/01/12 20:20:32] [error] [engine] input initialization failed	Assurez-vous que le répertoire hôte dans lequel le fichier DB réside dispose des permissions de lecture/écriture appropriées. Plus précisément, le répertoire hôte doit accorder des permissions de lecture/écriture aux utilisateurs non-root. L'emplacement par défaut du fichier DB est /var/log/ sauf si cela est remplacé par l'option fluent-bit-dbFile *agentconfiguration*. Si SELinux est activé, essayez de définir l'option fluent-bit-seLinuxOptionsType agentconfiguration sur 'spc_t'.

Des informations complémentaires peuvent être trouvées à partir du"Support" page ou dans le"Matrice de support du collecteur de données" .

Collecteur de données Memcached

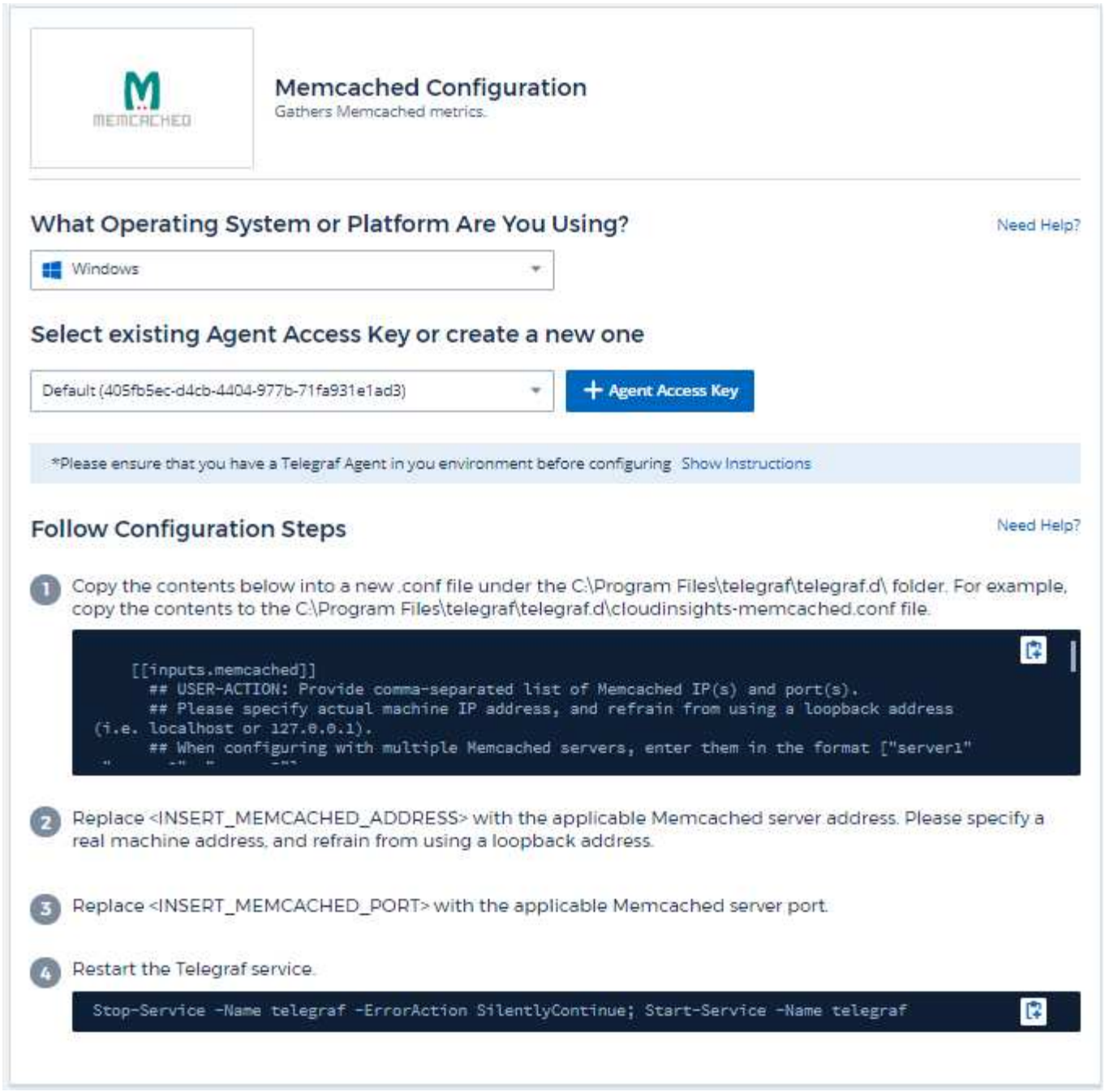
Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de Memcached.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Memcached.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
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 que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées dans le"Wiki Memcached" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :
Memcached	Serveur d’espace de noms	IP du nœud Nom du nœud	Acceptation des connexions Requêtes d’authentification traitées Authentifications échouées Octets utilisés Octets lus (par seconde) Octets écrits (par seconde) CAS Badval Succès CAS Échecs CAS Demandes de vidage (par seconde) Demandes d’obtention (par seconde) Demandes de définition (par seconde) Demandes tactiles (par seconde) Rendements de connexion (par seconde) Structures de connexion Connexions ouvertes Éléments stockés actuels Demandes de diminution Succès (par seconde) Demandes de diminution Échecs (par seconde) Demandes de suppression Succès (par seconde) Demandes de suppression Échecs (par seconde) Éléments expulsés Expulsions valides Éléments expirés Obtenir Succès (par seconde) Obtenir Échecs (par seconde) Octets de hachage utilisés Le hachage est en expansion Niveau de puissance de hachage Augmentation des requêtes Succès (par seconde) Augmentation des requêtes Échecs (par seconde) Serveur Nombre max. d’octets Écoute désactivée Nombre de threads de travail récupérés Nombre total de connexions ouvertes Nombre total d’éléments stockés Touch Succès Touch Échecs Temps de disponibilité du serveur

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données MongoDB

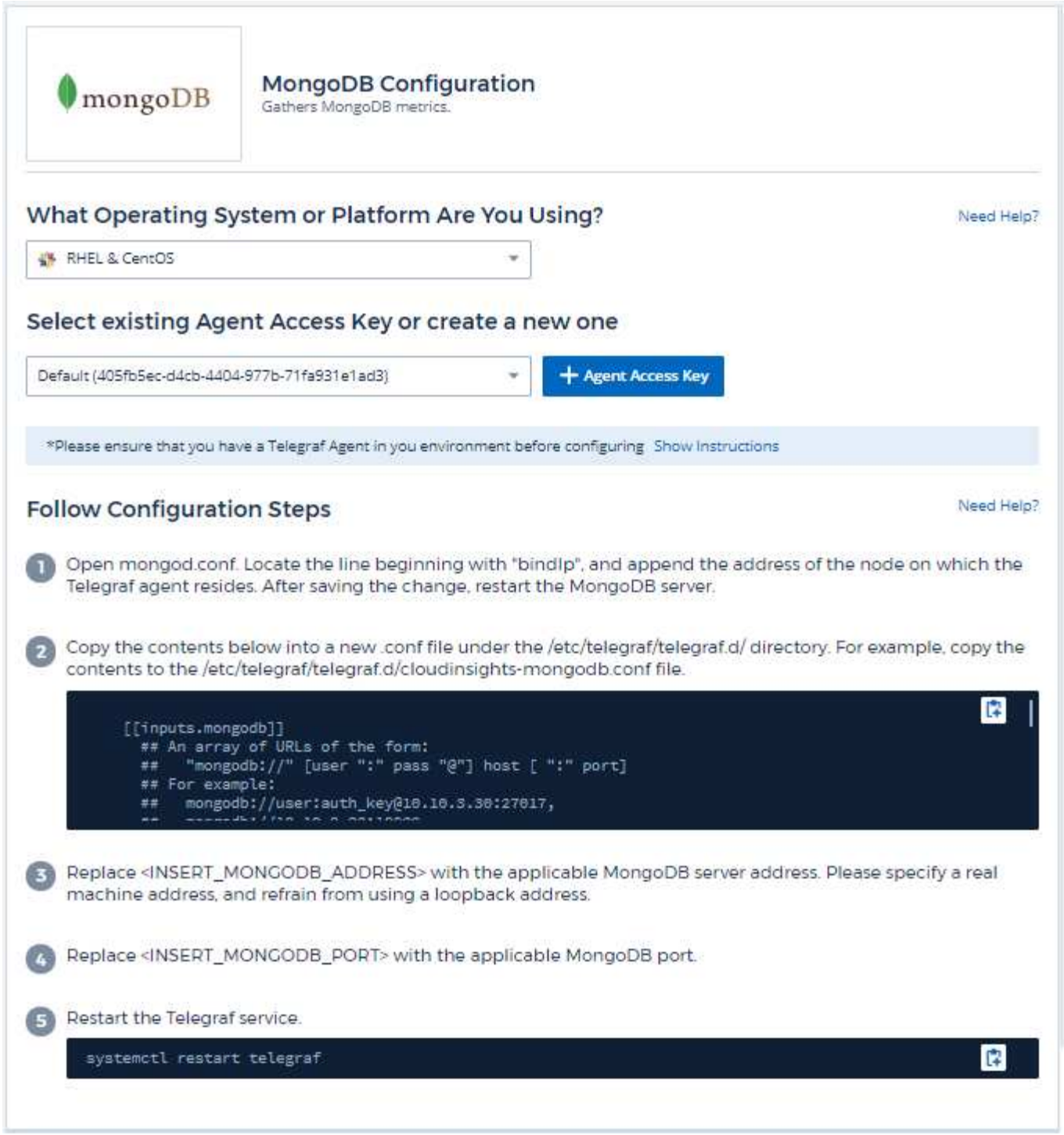
Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de MongoDB.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez MongoDB.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
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 que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées dans le"Documentation de MongoDB" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

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

Dépannage

Des informations peuvent être trouvées à partir du"Support" page.

Collecteur de données MySQL

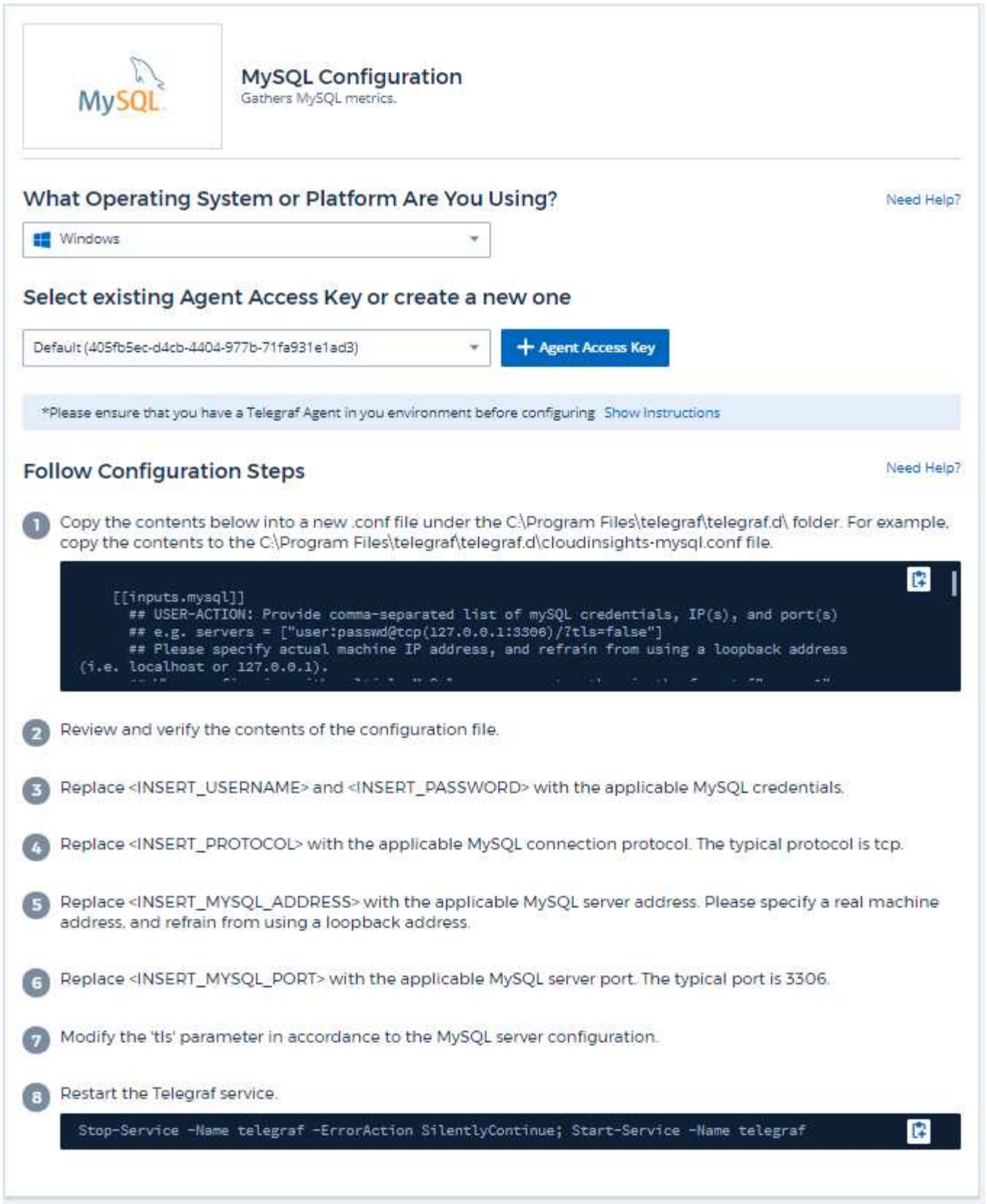
Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de MySQL.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez MySQL.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
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 que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées 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 du serveur MySQL	IP du nœud Nom du nœud	Clients abandonnés (par seconde) Connexions abandonnées (par seconde) Octets RX (par seconde) Octets TX (par seconde) Commandes Admin (par seconde) Commandes Alter Event Commandes Alter Function Commandes Alter Instance Commandes Alter Procedure Commandes Alter Server Commandes Alter Table Commandes Alter Tablespace Commandes Alter User Commandes Analyze Commandes Assign To Keycache Commandes Begin Commandes Binlog Commandes Call Procedure Commandes Change DB Commandes Change Master Commandes Change Repl Filter Commandes Check Commandes Checksum Commandes Commit Commandes Create DB Commandes Create Event Commandes Create Function Commandes Create Index Commandes Create Procedure Commandes Create Server Commandes Create Table Commandes Create Trigger Commandes Create UDF Commandes Create User Commandes Create View Commandes Dealloc Erreurs de connexion SQL Accept Create Tmp Disk Tables Erreurs différées Commandes Flush Handler Commit Innodb Buffer Pool Octets Données Blocs de clés non vidés Requêtes de lecture de clé Requêtes d'écriture de clé Écritures de clé Temps d'exécution maximal Dépassement du

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Netstat

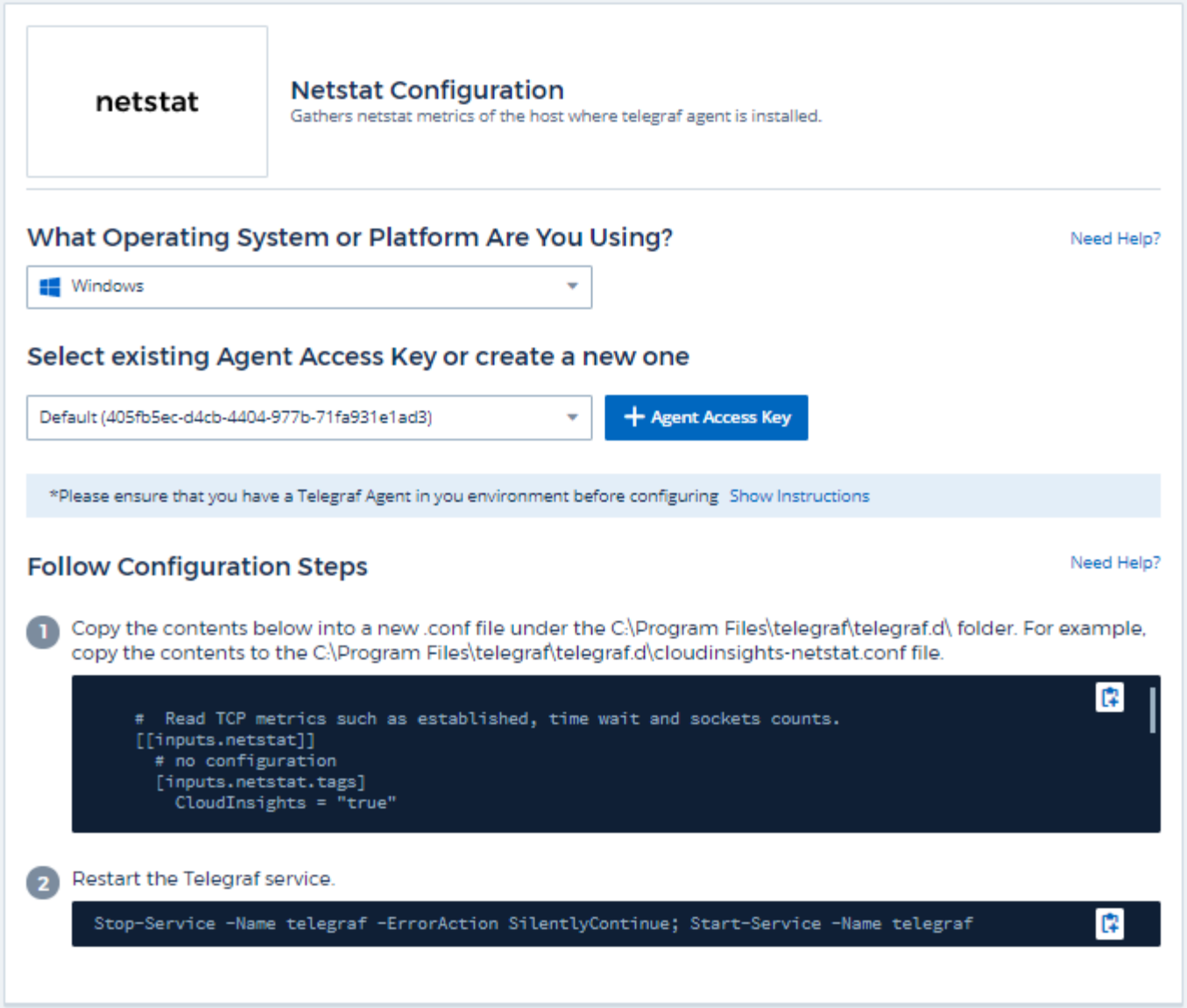
Data Infrastructure Insights utilise ce collecteur de données pour collecter les métriques Netstat.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Netstat.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
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 que vous utilisez pour collecter des données.



Installation

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

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

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Nginx

Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques

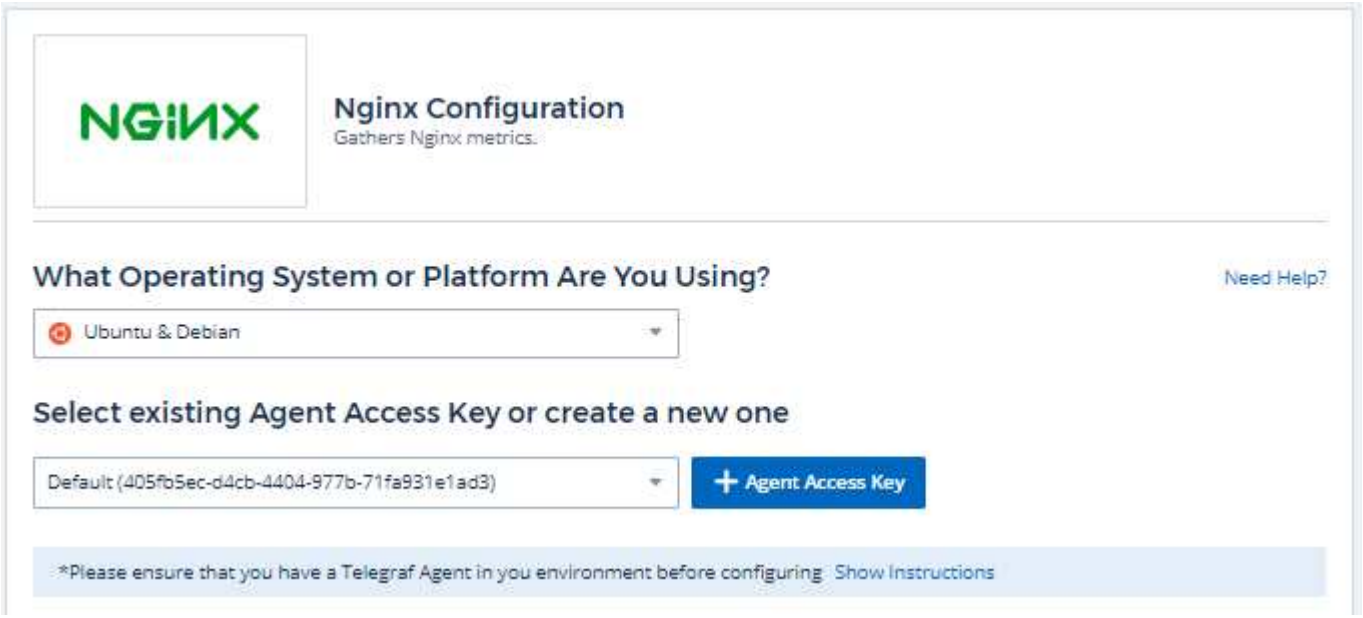
à partir de Nginx.

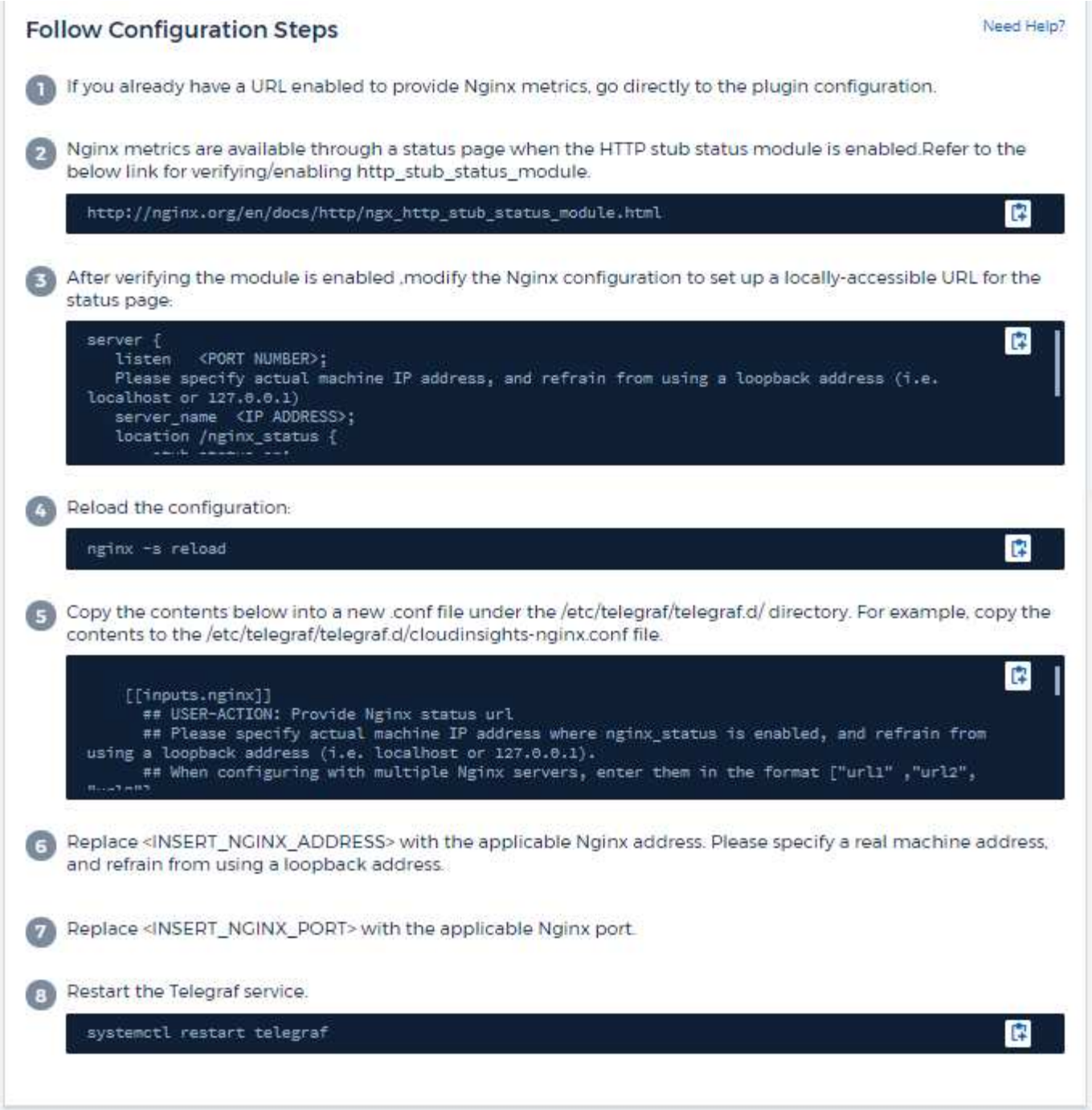
Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Nginx.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
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 que vous utilisez pour collecter des données.





Installation

La collecte de métriques Nginx nécessite que Nginx"module d'état http_stub" être activé.

Des informations complémentaires peuvent être trouvées 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	IP du nœud Nom du nœud Port	Accepte les demandes de lecture traitées actives en attente d'écriture

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données PostgreSQL

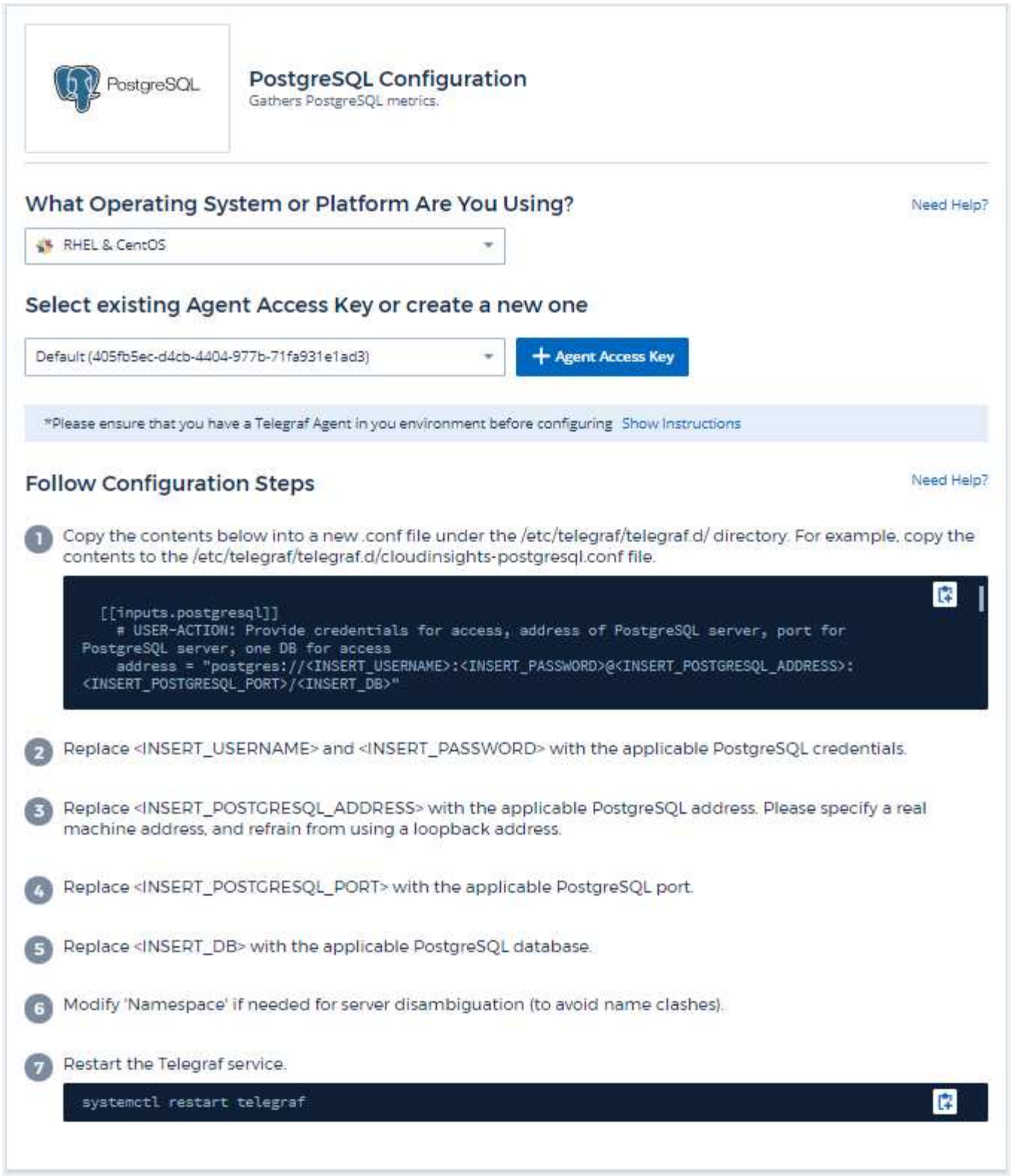
Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de PostgreSQL.

Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez PostgreSQL.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.
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 que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées 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	Nom du nœud IP du nœud	Tampons alloués Tampons backend Tampons de synchronisation de fichiers backend Tampons de point de contrôle Points de contrôle propres Temps de synchronisation Points de contrôle Temps d'écriture Points de contrôle Requêtes Points de contrôle chronométrés Max Écrit Propre
Base de données PostgreSQL	Serveur de base de données d'espace de noms	Base de données OID Nom du nœud IP du nœud	Blocs Temps de lecture Blocs Temps d'écriture Blocs Hits Blocs Lectures Conflits Blocs Interblocs Numéro de client Fichiers temporaires Octets Numéro de fichiers temporaires Lignes Lignes supprimées Lignes extraites Lignes insérées Lignes renvoyées Transactions mises à jour Transactions validées Annulées

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données d'agent de marionnettes

Data Infrastructure Insights utilise ce collecteur de données pour collecter des métriques à partir de Puppet Agent.

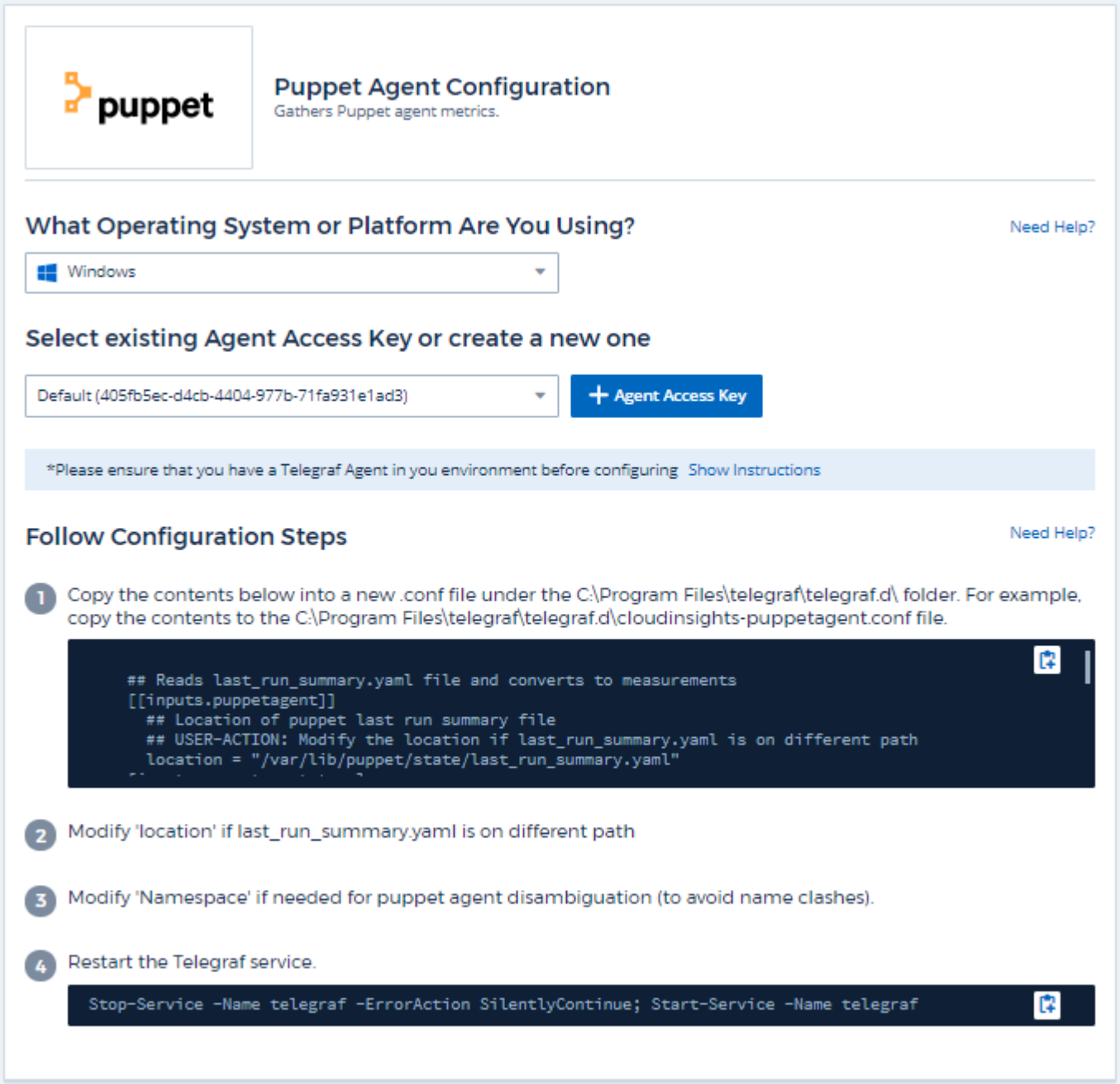
Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Puppet.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.

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 que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées dans le "Documentation des marionnettes"

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

Objet:	Identifiants :	Attributs:	Points de données :

Agent marionnette	UUID du nœud d'espace de noms	Nom du nœud Emplacement IP du nœud Version Chaîne de configuration Version Puppet	Modifications Total des événements Échecs Succès Ressources Total Ressources modifiées Ressources échouées Échec du redémarrage des ressources Ressources désynchronisées Ressources redémarrées Ressources planifiées Ressources ignorées Temps total Heure d'ancrage Heure de récupération de la configuration Heure cron Heure d'exécution Heure du fichier Heure du compartiment de fichiers Heure de la dernière exécution Heure du package Heure de planification Heure du service Heure de la clé Sshauthorized Heure totale Utilisateur

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.

Collecteur de données Redis

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

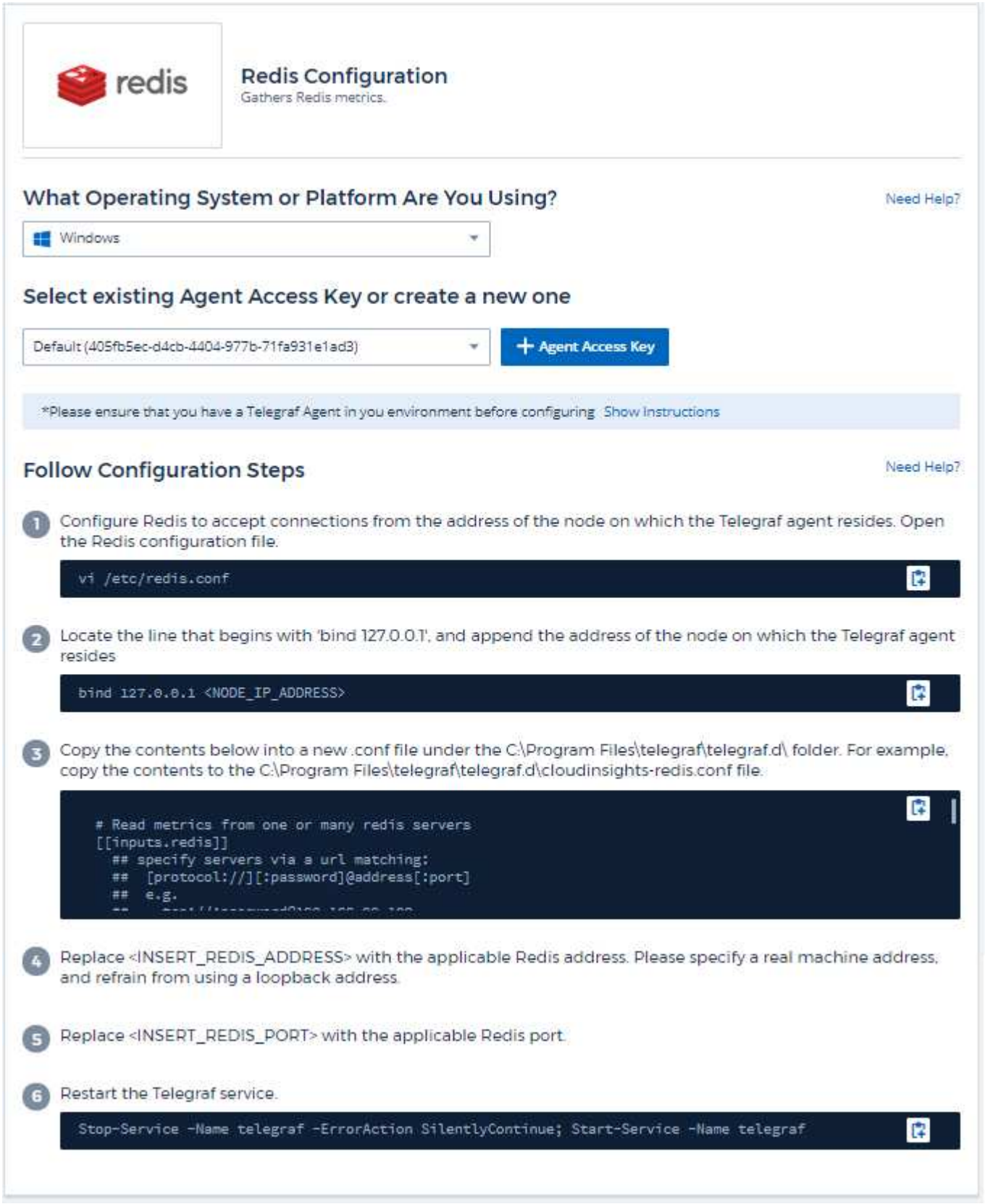
Installation

1. Depuis **Observabilité > Collecteurs**, cliquez sur **+Collecteur de données**. Choisissez Redis.

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

2. Si vous n'avez pas encore installé d'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 le"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 d'agent en cliquant sur le bouton **+ Clé d'accès d'agent**. Meilleure pratique : utilisez une clé d'accès d'agent différente uniquement lorsque vous souhaitez regrouper des collecteurs de données, par exemple par système d'exploitation/plateforme.

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 que vous utilisez pour collecter des données.



Installation

Des informations peuvent être trouvées dans le"Documentation Redis" .

Objets et compteurs

Les objets suivants et leurs compteurs sont collectés :

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

Dépannage

Des informations complémentaires peuvent être trouvées à partir du"Support" page.