Installez Astra Connector pour gérer les clusters

Astra Control Service

NetApp
September 23, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/astra-control-service/get-started/install-astra-connector-previous.html on September 23, 2024. Always check docs.netapp.com for the latest.

Sommaire

Installez Astra Connector pour gérer les clusters 1
Installer la version précédente du connecteur Astra 1
(Préversion technique) installez le connecteur Kubernetes Astra déclaratif 4

Installez Astra Connector pour gérer les clusters

ASTRA Connector est un logiciel qui réside sur vos clusters gérés et qui facilite la communication entre le cluster géré et Astra Control. Pour les clusters gérés à l'aide d'Astra Control Service, deux versions d'Astra Connector sont disponibles :

- **Version précédente du connecteur Astra** : "Installer la version précédente du connecteur Astra" Sur votre cluster si vous prévoyez de gérer un cluster avec des workflows non natifs Kubernetes.
- [Aperçu technique] **Declarative Kubernetes Astra Connector** : "Installez Astra Connector pour les clusters gérés avec des workflows Kubernetes déclaratifs" Sur votre cluster si vous prévoyez de gérer le cluster à l'aide de workflows Kubernetes déclaratifs. Une fois que vous avez installé Astra Connector sur votre cluster, celui-ci est automatiquement ajouté à Astra Control.

> Le connecteur Kubernetes Astra déclaratif est disponible uniquement dans le cadre du programme Astra Control Early Adopter Program (EAP). Pour plus d'informations sur l'adhésion au programme EAP, contactez votre ingénieur commercial NetApp.

Installer la version précédente du connecteur Astra

ASTRA Control Service utilise la version précédente d'Astra Connector pour permettre la communication entre Astra Control Service et les clusters privés gérés avec des workflows non natifs Kubernetes. Vous devez installer Astra Connector sur des clusters privés que vous souhaitez gérer avec des workflows non natifs Kubernetes.

La version précédente d'Astra Connector prend en charge les types suivants de clusters privés gérés avec des workflows non natifs Kubernetes :

- Amazon Elastic Kubernetes Service (EKS)
- Azure Kubernetes Service (AKS)
- Google Kubernetes Engine (GKE)
- Red Hat OpenShift Service sur AWS (ROSA)
- ROSA avec AWS PrivateLink
- Red Hat OpenShift Container Platform sur site

Description de la tâche

- Lorsque vous effectuez ces étapes, exécutez ces commandes sur le cluster privé que vous souhaitez gérer avec Astra Control Service.
- Si vous utilisez un hôte bastion, exécutez ces commandes à partir de la ligne de commande de l'hôte bastion.

Avant de commencer

- Vous devez accéder au cluster privé que vous souhaitez gérer avec Astra Control Service.
- Vous devez disposer des autorisations d'administrateur Kubernetes pour installer l'opérateur Astra Connector sur le cluster.

Étapes

1. Installez l'ancien opérateur Astra Connector sur le cluster privé que vous souhaitez gérer avec des workflows non natifs Kubernetes. Lorsque vous exécutez cette commande, le namespace `astra-connector-operator` est créé et la configuration est appliquée au namespace :

```
kubectl apply -f https://github.com/NetApp/astra-connector-operator/releases/download/23.07.0-202310251519/astraconnector_operator.yaml
```

2. Vérifiez que l'opérateur est installé et prêt :

```
kubectl get all -n astra-connector-operator
```

3. Obtenez un jeton API d'Astra Control. Reportez-vous à la "Documentation relative à l'automatisation d'Astra" pour obtenir des instructions.
4. Créez le namespace astra-Connector :

```
kubectl create ns astra-connector
```

5. Créez le fichier CR du connecteur Astra et nommez-le `astra-connector-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour correspondre à votre environnement Astra Control et à la configuration du cluster :
   - **<ASTRA_CONTROL_SERVICE_URL>** : l'URL de l'interface utilisateur Web d'Astra Control Service. Par exemple :

     ```
     https://astra.netapp.io
     ```

   - **<ASTRA_CONTROL_SERVICE_API_TOKEN>** : jeton API Astra Control que vous avez obtenu à l'étape précédente.
   - **<PRIVATE_AKS_CLUSTER_NAME>**: (Clusters AKS uniquement) - le nom du cluster du cluster privé Azure Kubernetes Service. Supprimez le commentaire et remplissez cette ligne uniquement si vous ajoutez un cluster AKS privé.
   - **<ASTRA_CONTROL_ACCOUNT_ID>** : obtenu à partir de l'interface utilisateur Web d'Astra Control. Sélectionnez l'icône de figure en haut à droite de la page et sélectionnez **API Access**.

```yaml
apiVersion: netapp.astraconnector.com/v1
kind: AstraConnector
metadata:
  name: astra-connector
  namespace: astra-connector
spec:
  natssync-client:
    cloud-bridge-url: <ASTRA_CONTROL_SERVICE_URL>
  imageRegistry:
    name: theotw
    secret: ""
  astra:
    token: <ASTRA_CONTROL_SERVICE_API_TOKEN>
    #clusterName: <PRIVATE_AKS_CLUSTER_NAME>
    accountId: <ASTRA_CONTROL_ACCOUNT_ID>
    acceptEULA: yes
```

6. Après avoir renseigné le `astra-connector-cr.yaml` Fichier avec les valeurs correctes, appliquer la CR :

```
kubectl apply -f astra-connector-cr.yaml
```

7. Vérifier que le connecteur Astra est entièrement déployé :

```
kubectl get all -n astra-connector
```

8. Vérifier que le cluster est enregistré avec Astra Control :

```
kubectl get astraconnector -n astra-connector
```

Vous devez voir les résultats similaires à ce qui suit :

```
NAME               REGISTERED   ASTRACONNECTORID
STATUS
astra-connector    true         be475ae5-1511-4eaa-9b9e-712f09b0d065
Registered with Astra
```

Notez l'ASTRACONNECTORID ; vous en aurez besoin lorsque vous ajouterez le cluster à Astra Control.

Et la suite ?

Maintenant que vous avez installé Astra Connector, vous êtes prêt à ajouter votre cluster privé à Astra Control Service.

- "Ajoutez un cluster géré par un fournisseur privé à Astra Control Service": Procédez comme suit pour ajouter un cluster qui a une adresse IP privée et qui est géré par un fournisseur de cloud. Vous aurez besoin du compte principal de service, du compte de service ou du compte utilisateur du fournisseur cloud.
- "Ajoutez un cluster privé autogéré à Astra Control Service": Utilisez ces étapes pour ajouter un cluster qui a une adresse IP privée et qui est géré par votre organisation. Vous devrez créer un fichier kubeconfig pour le cluster que vous souhaitez ajouter.

Pour en savoir plus

- "Ajouter un cluster"

(Préversion technique) installez le connecteur Kubernetes Astra déclaratif

Les clusters gérés à l'aide de workflows Kubernetes déclaratifs utilisent Astra Connector pour permettre la communication entre le cluster géré et Astra Control. Vous devez installer Astra Connector sur tous les clusters que vous allez gérer avec des workflows Kubernetes déclaratifs.

Vous installez le connecteur Kubernetes Astra déclaratif à l'aide des commandes Kubernetes et des fichiers de ressources personnalisées (CR).

Description de la tâche

- Lorsque vous effectuez ces étapes, exécutez ces commandes sur le cluster que vous souhaitez gérer avec Astra Control.
- Si vous utilisez un hôte bastion, exécutez ces commandes à partir de la ligne de commande de l'hôte bastion.

Avant de commencer

- Vous devez accéder au cluster que vous souhaitez gérer avec Astra Control.
- Vous devez disposer des autorisations d'administrateur Kubernetes pour installer l'opérateur Astra Connector sur le cluster.

> Si le cluster est configuré avec l'application d'admission de la sécurité du pod, c'est-à-dire la configuration par défaut pour les clusters Kubernetes 1.25 et versions ultérieures, vous devez activer les restrictions PSA sur les espaces de noms appropriés. Reportez-vous à la section "Préparez votre environnement à la gestion des clusters avec Astra Control" pour obtenir des instructions.

Étapes

1. Installez l'opérateur Astra Connector sur le cluster que vous souhaitez gérer avec des workflows Kubernetes déclaratifs. Lorsque vous exécutez cette commande, le namespace `astra-connector-operator` est créé et la configuration est appliquée au namespace :

```
kubectl apply -f https://github.com/NetApp/astra-connector-
operator/releases/download/24.02.0-
202403151353/astraconnector_operator.yaml
```

2. Vérifiez que l'opérateur est installé et prêt :

```
kubectl get all -n astra-connector-operator
```

3. Obtenez un jeton API d'Astra Control. Reportez-vous à la "Documentation relative à l'automatisation d'Astra" pour obtenir des instructions.
4. Créez un secret à l'aide du jeton. Remplacez <API_TOKEN> par le jeton que vous avez reçu d'Astra Control :

```
kubectl create secret generic astra-token \
--from-literal=apiToken=<API_TOKEN> \
-n astra-connector
```

5. Créez un secret Docker à utiliser pour extraire l'image du connecteur Astra. Remplacez les valeurs entre parenthèses <> par les informations de votre environnement :

> <ASTRA_CONTROL_ACCOUNT_ID> est disponible dans l'interface utilisateur web d'Astra Control. Dans l'interface utilisateur Web, sélectionnez l'icône figure en haut à droite de la page et sélectionnez **accès API**.

```
kubectl create secret docker-registry regcred \
--docker-username=<ASTRA_CONTROL_ACCOUNT_ID> \
--docker-password=<API_TOKEN> \
-n astra-connector \
--docker-server=cr.astra.netapp.io
```

6. Créez le fichier CR du connecteur Astra et nommez-le `astra-connector-cr.yaml`. Mettez à jour les valeurs entre parenthèses <> pour correspondre à votre environnement Astra Control et à la configuration du cluster :
   - <ASTRA_CONTROL_ACCOUNT_ID> : obtenu à partir de l'interface utilisateur web d'Astra Control au cours de l'étape précédente.
   - <CLUSTER_NAME> : nom que ce cluster doit être attribué dans Astra Control.
   - <ASTRA_CONTROL_URL> : l'URL de l'interface utilisateur Web d'Astra Control. Par exemple :

```
https://astra.control.url
```

```yaml
apiVersion: astra.netapp.io/v1
kind: AstraConnector
metadata:
  name: astra-connector
  namespace: astra-connector
spec:
  astra:
    accountId: <ASTRA_CONTROL_ACCOUNT_ID>
    clusterName: <CLUSTER_NAME>
    #Only set `skipTLSValidation` to `true` when using the default
self-signed
    #certificate in a proof-of-concept environment.
    skipTLSValidation: false #Should be set to false in production
environments
    tokenRef: astra-token
  natsSyncClient:
    cloudBridgeURL: <ASTRA_CONTROL_HOST_URL>
  imageRegistry:
    name: cr.astra.netapp.io
    secret: regcred
```

7. Après avoir renseigné le `astra-connector-cr.yaml` Fichier avec les valeurs correctes, appliquer la CR :

```
kubectl apply -n astra-connector -f astra-connector-cr.yaml
```

8. Vérifier que le connecteur Astra est entièrement déployé :

```
kubectl get all -n astra-connector
```

9. Vérifier que le cluster est enregistré avec Astra Control :

```
kubectl get astraconnectors.astra.netapp.io -A
```

Vous devez voir les résultats similaires à ce qui suit :

```
NAMESPACE         NAME              REGISTERED   ASTRACONNECTORID
STATUS
astra-connector   astra-connector   true         00ac8-2cef-41ac-8777-
ed0583e   Registered with Astra
```

10. Vérifiez que le cluster s’affiche dans la liste des clusters gérés sur la page **clusters** de l’interface utilisateur Web d’Astra Control.

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.