Installa Astra Connector per gestire i cluster

Astra Control Service

NetApp
September 23, 2024

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

Sommario

Installa Astra Connector per gestire i cluster 1
Installare la versione precedente del connettore Astra 1
(Anteprima tecnica) Installa il connettore dichiarativo di Kubernetes Astra 4

Installa Astra Connector per gestire i cluster

Astra Connector è un software che risiede nei cluster gestiti e facilita la comunicazione tra il cluster gestito e Astra Control. Per i cluster gestiti mediante Astra Control Service, sono disponibili due versioni di Astra Connector:

- **Versione precedente del connettore Astra**: "Installare la versione precedente del connettore Astra" Sul tuo cluster, se intendi gestire il cluster con flussi di lavoro non nativi di Kubernetes.
- [Tech preview] * connettore dichiarativo di Kubernetes Astra*: "Installa Astra Connector per i cluster gestiti con flussi di lavoro Kubernetes dichiarativi" Sul cluster, se si intende gestire il cluster utilizzando flussi di lavoro Kubernetes dichiarativi. Dopo aver installato Astra Connector sul cluster, il cluster viene aggiunto automaticamente ad Astra Control.

> Il connettore dichiarativo Kubernetes Astra è disponibile solo come parte del programma Astra Control Early Adopter Program (EAP). Per informazioni sulla partecipazione al programma EAP, contattare il rappresentante commerciale NetApp di zona.

Installare la versione precedente del connettore Astra

Astra Control Service utilizza la versione precedente di Astra Connector per consentire la comunicazione tra Astra Control Service e i cluster privati gestiti con flussi di lavoro non nativi per Kubernetes. Devi installare Astra Connector su cluster privati che vuoi gestire con flussi di lavoro non nativi di Kubernetes.

La versione precedente di Astra Connector supporta i seguenti tipi di cluster privati gestiti con flussi di lavoro non nativi di Kubernetes:

- Amazon Elastic Kubernetes Service (EKS)
- Servizio Azure Kubernetes (AKS)
- Google Kubernetes Engine (GKE)
- Red Hat OpenShift Service su AWS (ROSA)
- ROSA con AWS PrivateLink
- Piattaforma Red Hat OpenShift Container all'interno dell'hotel

A proposito di questa attività

- Per eseguire questi passaggi, esegui questi comandi sul cluster privato che desideri gestire con Astra Control Service.
- Se si utilizza un host Bastion, eseguire questi comandi dalla riga di comando dell'host Bastion.

Prima di iniziare

- Devi accedere al cluster privato da gestire con Astra Control Service.
- Sono necessarie autorizzazioni di amministratore di Kubernetes per installare l'operatore Astra Connector sul cluster.

Fasi

1. Installa l'operatore Astra Connector precedente sul cluster privato che desideri gestire con flussi di lavoro non nativi di Kubernetes. Quando si esegue questo comando, lo spazio dei nomi `astra-connector-`

`operator` viene creato e la configurazione viene applicata allo spazio dei nomi:

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

2. Verificare che l'operatore sia installato e pronto:

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

3. Ottieni un token API da Astra Control. Fare riferimento a. "Documentazione di Astra Automation" per istruzioni.
4. Creare lo spazio dei nomi astra-Connector:

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

5. Creare il file Astra Connector CR e assegnargli un nome `astra-connector-cr.yaml`. Aggiorna i valori tra parentesi <> per farli corrispondere all'ambiente Astra Control e alla configurazione del cluster:
   - **<ASTRA_CONTROL_SERVICE_URL>**: L'URL dell'interfaccia utente web del servizio di controllo Astra. Ad esempio:

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

   - **<ASTRA_CONTROL_SERVICE_API_TOKEN>**: Il token dell'API di controllo Astra ottenuto nel passaggio precedente.
   - **<PRIVATE_AKS_CLUSTER_NAME>**: (Solo cluster AKS) - il nome del cluster del cluster privato Azure Kubernetes Service. Annullare il commento e popolare questa riga solo se si aggiunge un cluster AKS privato.
   - **<ASTRA_CONTROL_ACCOUNT_ID>**: Ottenuto dall'interfaccia utente web Astra Control. Selezionare l'icona a forma di figura in alto a destra nella pagina e selezionare **accesso API**.

```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. Dopo aver popolato il `astra-connector-cr.yaml` File con i valori corretti, applicare il CR:

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

7. Verificare che il connettore Astra sia completamente distribuito:

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

8. Verifica che il cluster sia registrato con Astra Control:

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

L'output dovrebbe essere simile a quanto segue:

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

Prendere nota di ASTRACONNECTORID; sarà necessario quando si aggiunge il cluster ad Astra Control.

Quali sono le prossime novità?

Una volta installato Astra Connector, puoi aggiungere il cluster privato ad Astra Control Service.

- "Aggiungere un cluster gestito da provider privato ad Astra Control Service": Utilizzare questa procedura per aggiungere un cluster che dispone di un indirizzo IP privato ed è gestito da un provider cloud. È necessario disporre dell'account Service Principal, dell'account del servizio o dell'account utente per il provider cloud.
- "Aggiungere un cluster privato autogestato ad Astra Control Service": Utilizzare questa procedura per aggiungere un cluster con un indirizzo IP privato e gestito dall'organizzazione. Sarà necessario creare un file kubeconfig per il cluster che si desidera aggiungere.

Per ulteriori informazioni

- "Aggiungere un cluster"

(Anteprima tecnica) Installa il connettore dichiarativo di Kubernetes Astra

I cluster gestiti utilizzando flussi di lavoro Kubernetes dichiarativi utilizzano Astra Connector per consentire la comunicazione tra il cluster gestito e Astra Control. Devi installare Astra Connector su tutti i cluster che verranno gestiti con flussi di lavoro Kubernetes dichiarativi.

Viene installato il connettore Astra dichiarativo di Kubernetes utilizzando i comandi di Kubernetes e i file Custom Resource (CR).

A proposito di questa attività

- Quando esegui questi passaggi, esegui questi comandi sul cluster che desideri gestire con Astra Control.
- Se si utilizza un host Bastion, eseguire questi comandi dalla riga di comando dell'host Bastion.

Prima di iniziare

- Devi accedere al cluster da gestire con Astra Control.
- Sono necessarie autorizzazioni di amministratore di Kubernetes per installare l'operatore Astra Connector sul cluster.

> Se il cluster è configurato con l'imposizione dell'ammissione di sicurezza pod, che è l'impostazione predefinita per i cluster Kubernetes 1,25 e versioni successive, è necessario abilitare le restrizioni PSA sugli spazi dei nomi appropriati. Fare riferimento a. "Prepara il tuo ambiente per la gestione dei cluster utilizzando Astra Control" per istruzioni.

Fasi

1. Installare l'operatore Astra Connector sul cluster che si desidera gestire con flussi di lavoro Kubernetes dichiarativi. Quando si esegue questo comando, lo spazio dei nomi `astra-connector-operator` viene creato e la configurazione viene applicata allo spazio dei nomi:

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

2. Verificare che l'operatore sia installato e pronto:

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

3. Ottieni un token API da Astra Control. Fare riferimento a. "Documentazione di Astra Automation" per istruzioni.
4. Creare un segreto utilizzando il token. Sostituisci <API_TOKEN> con il token ricevuto da Astra Control:

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

5. Crea un Docker Secret da usare per estrarre l'immagine di Astra Connector. Sostituire i valori tra parentesi <> con le informazioni dell'ambiente:

> Puoi trovare il <ASTRA_CONTROL_ACCOUNT_ID> nell'interfaccia utente web di Astra Control. Nell'interfaccia utente Web, selezionare l'icona della figura in alto a destra nella pagina e selezionare **accesso 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. Creare il file Astra Connector CR e assegnargli un nome `astra-connector-cr.yaml`. Aggiorna i valori tra parentesi <> per farli corrispondere all'ambiente Astra Control e alla configurazione del cluster:
   - <ASTRA_CONTROL_ACCOUNT_ID>: Ottenuto dall'interfaccia utente web Astra Control durante la fase precedente.
   - <CLUSTER_NAME>: Il nome che il cluster deve essere assegnato in Astra Control.
   - <ASTRA_CONTROL_URL>: L'URL dell'interfaccia utente web di Astra Control. Ad esempio:

```
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. Dopo aver popolato il `astra-connector-cr.yaml` File con i valori corretti, applicare il CR:

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

8. Verificare che il connettore Astra sia completamente distribuito:

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

9. Verifica che il cluster sia registrato con Astra Control:

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

L'output dovrebbe essere simile a quanto segue:

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

10. Verificare che il cluster compaia nell'elenco dei cluster gestiti nella pagina **cluster** dell'interfaccia utente Web Astra Control.

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

Informazioni sul marchio commerciale

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