Configura il tuo cloud provider

Astra Control Service

NetApp
April 24, 2024

Sommario

Configura il tuo cloud provider

Configurare Amazon Web Services

Sono necessari alcuni passaggi per preparare il tuo progetto Amazon Web Services prima di poter gestire i cluster Amazon Elastic Kubernetes Service (EKS) con Astra Control Service.

Avvio rapido per la configurazione di Amazon Web Services

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

[Uno] Consulta i requisiti del servizio Astra Control per Amazon Web Services

Assicurarsi che i cluster siano integri e che eseguano una versione supportata di Kubernetes, che i nodi di lavoro siano online e che eseguano Linux o Windows e altro ancora. Scopri di più su questo passaggio.

[Due] Crea un account Amazon

Se non disponi già di un account Amazon, devi crearne uno per poter utilizzare EKS. Scopri di più su questo passaggio.

[Tre] Installare la CLI di Amazon Web Services

Installare la CLI AWS in modo da poter gestire AWS dalla riga di comando. Seguire le istruzioni dettagliate.

[Quattro] Facoltativo: Creare un utente IAM

Creare un utente Amazon Identity and Access Management (IAM). Puoi anche saltare questo passaggio e utilizzare un utente IAM esistente con Astra Control Service.

Leggi le istruzioni dettagliate.

[Cinque] Creare e allegare un criterio di autorizzazioni

Creare una policy con le autorizzazioni richieste per Astra Control Service per interagire con l'account AWS.

Leggi le istruzioni dettagliate.

[Sei] Salvare le credenziali per l'utente IAM

Salvare le credenziali per l'utente IAM in modo da poter importare le credenziali in Astra Control Service.

Leggi le istruzioni dettagliate.

Requisiti del cluster EKS

Un cluster Kubernetes deve soddisfare i seguenti requisiti per consentirne il rilevamento e la gestione da Astra Control Service.

Versione di Kubernetes

Un cluster deve eseguire una versione di Kubernetes compresa tra 1,25 e 1,28.

Tipo di immagine

Il tipo di immagine per ciascun nodo di lavoro deve essere Linux.

Stato del cluster

I cluster devono essere in esecuzione in uno stato integro e avere almeno un nodo di lavoro online senza nodi di lavoro in uno stato di errore.

Astra Control provisioner

Astra Control Provivisioner e un controller delle snapshot esterno sono necessari per le operazioni con backend di storage. Per attivare queste operazioni, procedere come segue:

1. "Installare gli snapshot CRD e lo snapshot controller".
2. "Abilita Astra Control Provisioner".
3. "Creare una classe VolumeSnapshotClass".

Driver CSI per Amazon Elastic Block Store (EBS)

Se si utilizza il backend dello storage Amazon EBS, è necessario installare il driver CSI (Container Storage Interface) per EBS (non viene installato automaticamente).

Per istruzioni sull'installazione del driver CSI, fare riferimento alla procedura.

Installare uno snap-shot esterno

Se non l'hai già fatto, "Installare gli snapshot CRD e lo snapshot controller".

Installare il driver CSI come add-on Amazon EKS

1. Creare il ruolo IAM del driver CSI Amazon EBS per gli account del servizio. Seguire le istruzioni "Nella documentazione Amazon", Utilizzando i comandi CLI di AWS nelle istruzioni.
2. Aggiungere il componente aggiuntivo Amazon EBS CSI utilizzando il seguente comando AWS CLI, sostituendo le informazioni tra parentesi <> con valori specifici per il proprio ambiente. Sostituire <DRIVER_ROLE> con il nome del ruolo del driver EBS CSI creato nel passaggio precedente:

```
aws eks create-addon \
  --cluster-name <CLUSTER_NAME> \
  --addon-name aws-ebs-csi-driver \
  --service-account-role-arn
arn:aws:iam::<ACCOUNT_ID>:role/<DRIVER_ROLE>
```

Configurare la classe di storage EBS

1. Clonare il repository GitHub del driver CSI di Amazon EBS nel sistema.

```
git clone https://github.com/kubernetes-sigs/aws-ebs-csi-
driver.git
```

2. Accedere alla directory di esempio del provisioning dinamico.

```
cd aws-ebs-csi-driver/examples/kubernetes/dynamic-provisioning/
```

3. Implementare la classe di storage ebs-sc e l'attestazione di volume persistente ebs-claim dalla directory manifests.

```
kubectl apply -f manifests/storageclass.yaml
kubectl apply -f manifests/claim.yaml
```

4. Descrivere la classe di storage ebs-sc.

```
kubectl describe storageclass ebs-sc
```

Viene visualizzato un output che descrive gli attributi della classe di storage.

Crea un account Amazon

Se non disponi già di un account Amazon, devi crearne uno per attivare la fatturazione per Amazon EKS.

Fasi

1. Accedere alla "Pagina principale Amazon" , Selezionare **Accedi** in alto a destra e selezionare **inizia qui**.
2. Seguire le istruzioni per creare un account.

Installare la CLI di Amazon Web Services

Installare la CLI AWS in modo da poter gestire le risorse AWS dalla riga di comando.

Fase

1. Passare a. "Introduzione a AWS CLI" E seguire le istruzioni per installare l'interfaccia CLI.

Facoltativo: Creare un utente IAM

Creare un utente IAM in modo da poter utilizzare e gestire i servizi e le risorse AWS con maggiore sicurezza. È inoltre possibile saltare questo passaggio e utilizzare un utente IAM esistente con Astra Control Service.

Fase

1. Passare a. "Creazione di utenti IAM" E seguire le istruzioni per creare un utente IAM.

Creare e allegare un criterio di autorizzazioni

Creare una policy con le autorizzazioni richieste per Astra Control Service per interagire con l'account AWS.

Fasi

1. Creare un nuovo file chiamato `policy.json`.
2. Copiare il seguente contenuto JSON nel file:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData",
                "fsx:DescribeVolumes",
                "ec2:DescribeRegions",
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject",
                "iam:SimulatePrincipalPolicy",
                "s3:ListAllMyBuckets",
                "eks:DescribeCluster",
                "eks:ListNodegroups",
                "eks:DescribeNodegroup",
                "eks:ListClusters",
                "iam:GetUser",
                "s3:DeleteObject",
                "s3:DeleteBucket",
                "autoscaling:DescribeAutoScalingGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Creare la policy:

```
POLICY_ARN=$(aws iam create-policy  --policy-name <policy-name> --policy
-document file://policy.json  --query='Policy.Arn' --output=text)
```

4. Allegare il criterio all'utente IAM. Sostituire `<IAM-USER-NAME>` Con il nome utente dell'utente IAM creato o con un utente IAM esistente:

```
aws iam attach-user-policy --user-name <IAM-USER-NAME> --policy-arn
=$POLICY_ARN
```

Salvare le credenziali per l'utente IAM

Salvare le credenziali per l'utente IAM in modo da rendere Astra Control Service consapevole dell'utente.

Fasi

1. Scarica le credenziali. Sostituire `<IAM-USER-NAME>` Con il nome utente dell'utente IAM che si desidera utilizzare:

```
aws iam create-access-key --user-name <IAM-USER-NAME> --output json >
credential.json
```

Risultato

Il `credential.json` Il file viene creato ed è possibile importare le credenziali in Astra Control Service.

Configurare Google Cloud

Sono necessari alcuni passaggi per preparare il tuo progetto Google Cloud prima di poter gestire i cluster di Google Kubernetes Engine con Astra Control Service.

> Se non si inizia a utilizzare Google Cloud Volumes Service per Google Cloud come back-end di storage ma si prevede di utilizzarlo in un secondo momento, è necessario completare i passaggi necessari per configurare Google Cloud Volumes Service per Google Cloud ora. La creazione di un account di servizio in un secondo momento implica la perdita di accesso ai bucket di storage esistenti.

Avvio rapido per la configurazione di Google Cloud

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

[Uno] Consulta i requisiti del servizio Astra Control per Google Kubernetes Engine

Assicurarsi che i cluster siano integri e che eseguano una versione di Kubernetes supportata, che i nodi di lavoro siano online e che eseguano un tipo di immagine supportato e altro ancora. Scopri di più su questo passaggio.

[Due] (Facoltativo): Acquista Cloud Volumes Service per Google Cloud

Se si intende utilizzare Cloud Volumes Service per Google Cloud come back-end di storage, accedere alla pagina NetApp Cloud Volumes Service nel Google Cloud Marketplace e selezionare Acquista. Scopri di più su questo passaggio.

[Tre] Abilita le API nel tuo progetto Google Cloud

Abilitare le seguenti API di Google Cloud:

- Motore di Google Kubernetes
- Cloud Storage

- API JSON per lo storage cloud
- Utilizzo del servizio
- API Cloud Resource Manager
- NetApp Cloud Volumes Service
  - Richiesto per Cloud Volumes Service per Google Cloud
  - Opzionale (ma consigliato) per Google Persistent Disk
- API Service Consumer Management
- API di Service Networking
- API di gestione dei servizi

Seguire le istruzioni dettagliate.

[Quattro] Creare un account di servizio con le autorizzazioni richieste

Creare un account di servizio Google Cloud con le seguenti autorizzazioni:

- Amministratore del motore di Kubernetes
- NetApp Cloud Volumes Admin
  - Richiesto per Cloud Volumes Service per Google Cloud
  - Opzionale (ma consigliato) per Google Persistent Disk
- Amministratore dello storage
- Visualizzatore utilizzo servizio
- Visualizzatore di Compute Network

Leggi le istruzioni dettagliate.

[Cinque] Creare una chiave dell'account del servizio

Creare una chiave per l'account del servizio e salvare il file delle chiavi in una posizione sicura. Seguire le istruzioni dettagliate.

[Sei] (Facoltativo): Impostare il peering di rete per il VPC

Se intendi utilizzare Cloud Volumes Service per Google Cloud come back-end di storage, imposta il peering di rete dal tuo VPC a Cloud Volumes Service per Google Cloud. Seguire le istruzioni dettagliate.

Requisiti del cluster GKE

Un cluster Kubernetes deve soddisfare i seguenti requisiti per consentirne il rilevamento e la gestione da Astra Control Service. Alcuni di questi requisiti si applicano solo se si prevede di utilizzare Cloud Volumes Service per Google Cloud come back-end di storage.

Versione di Kubernetes

Un cluster deve eseguire una versione di Kubernetes compresa tra 1,26 e 1,28.

Tipo di immagine

Il tipo di immagine per ciascun nodo di lavoro deve essere `COS_CONTAINERD`.

Stato del cluster

I cluster devono essere in esecuzione in uno stato integro e avere almeno un nodo di lavoro online senza nodi di lavoro in uno stato di errore.

Regione di Google Cloud

Se si prevede di utilizzare Cloud Volumes Service per Google Cloud come backend di storage, i cluster devono essere eseguiti in un "Area di Google Cloud in cui è supportato Cloud Volumes Service per Google Cloud." Si noti che Astra Control Service supporta entrambi i tipi di servizio: CVS e CVS-Performance. Come Best practice, devi scegliere una regione che supporti Cloud Volumes Service per Google Cloud, anche se non la utilizzi come back-end di storage. In questo modo sarà più semplice utilizzare Cloud Volumes Service per Google Cloud come back-end di storage in futuro, se i requisiti di performance cambiano.

Networking

Se si intende utilizzare Cloud Volumes Service per Google Cloud come backend di storage, il cluster deve risiedere in un VPC con Cloud Volumes Service per Google Cloud. Questo passaggio è descritto di seguito.

Cluster privati

Se il cluster è privato, il "reti autorizzate" Deve consentire l'indirizzo IP di Astra Control Service:

52.188.218.166/32

Modalità operativa per un cluster GKE

Si consiglia di utilizzare la modalità operativa standard. La modalità Autopilot non è stata testata al momento. "Scopri di più sulle modalità operative".

Pool di storage

Se si utilizza NetApp Cloud Volumes Service come backend di storage con il tipo di servizio CVS, è necessario configurare i pool di storage prima di poter eseguire il provisioning dei volumi. Fare riferimento a. "Tipo di servizio, classi di storage e dimensione PV per cluster GKE" per ulteriori informazioni.

Opzionale: Acquista Cloud Volumes Service per Google Cloud

Il servizio di controllo Astra può utilizzare Cloud Volumes Service per Google Cloud come back-end di storage per i volumi persistenti. Se intendi utilizzare questo servizio, devi acquistare Cloud Volumes Service per Google Cloud da Google Cloud Marketplace per abilitare la fatturazione per volumi persistenti.

Fase

1. Accedere alla "Pagina Cloud Volumes Service di NetApp" In Google Cloud Marketplace, selezionare **Purchase** (Acquista) e seguire le istruzioni.

   "Seguire le istruzioni dettagliate nella documentazione di Google Cloud per acquistare e attivare il servizio".

Abilitare le API nel progetto

Il progetto richiede autorizzazioni per accedere a specifiche API di Google Cloud. Le API vengono utilizzate per interagire con le risorse cloud di Google, come i cluster GKE e lo storage NetApp Cloud Volumes Service.

Fase

1. "Utilizzare la console Google Cloud o la CLI gcloud per abilitare le seguenti API":

- Motore di Google Kubernetes
- Cloud Storage
- API JSON per lo storage cloud
- Utilizzo del servizio
- API Cloud Resource Manager
- NetApp Cloud Volumes Service (richiesto per Cloud Volumes Service per Google Cloud)
- API Service Consumer Management
- API di Service Networking
- API di gestione dei servizi

Il video seguente mostra come abilitare le API dalla console Google Cloud.

► https://docs.netapp.com/it-it/astra-control-service/media/get-started/video-enable-gcp-apis.mp4 *(video)*

Creare un account di servizio

Astra Control Service utilizza un account di servizio Google Cloud per facilitare la gestione dei dati dell'applicazione Kubernetes per conto dell'utente.

Fasi

1. Accedere a Google Cloud e. "creare un account di servizio utilizzando la console, il comando gcloud o un altro metodo preferito".
2. Assegnare all'account del servizio i seguenti ruoli:
   - **Kubernetes Engine Admin** - utilizzato per elencare i cluster e creare l'accesso amministratore per gestire le applicazioni.
   - **NetApp Cloud Volumes Admin** - utilizzato per gestire lo storage persistente per le applicazioni.
   - **Storage Admin** - utilizzato per gestire bucket e oggetti per il backup delle applicazioni.
   - **Visualizzatore utilizzo servizio** - consente di verificare se le API Cloud Volumes Service per Google Cloud richieste sono attivate.
   - **Visualizzatore di rete di calcolo** - utilizzato per verificare se il VPC Kubernetes è autorizzato a raggiungere Cloud Volumes Service per Google Cloud.

Se si desidera utilizzare gcloud, è possibile seguire i passaggi dall'interfaccia Astra Control. Selezionare **account > credenziali > Aggiungi credenziali**, quindi selezionare **istruzioni**.

Se si desidera utilizzare la console Google Cloud, il video seguente mostra come creare l'account del servizio dalla console.

► https://docs.netapp.com/it-it/astra-control-service/media/get-started/video-create-gcp-service-account.mp4

(video)

Configurare l’account di servizio per un VPC condiviso

Per gestire i cluster GKE che risiedono in un progetto, ma utilizzano un VPC di un progetto diverso (un VPC condiviso), è necessario specificare l’account del servizio Astra come membro del progetto host con il ruolo **Compute Network Viewer**.

Fasi

1. Dalla console di Google Cloud, accedere a **IAM & Admin** e selezionare **Service Accounts**.
2. Individuare l’account di servizio Astra "le autorizzazioni richieste" quindi copiare l’indirizzo e-mail.
3. Accedere al progetto host e selezionare **IAM & Admin** > **IAM**.
4. Selezionare **Aggiungi** e aggiungere una voce per l’account del servizio.
   a. **Nuovi membri**: Inserire l’indirizzo e-mail dell’account del servizio.
   b. **Ruolo**: Selezionare **Compute Network Viewer**.
   c. Selezionare **Salva**.

Risultato

L’aggiunta di un cluster GKE utilizzando un VPC condiviso funziona perfettamente con Astra.

Creare una chiave dell’account del servizio

Invece di fornire un nome utente e una password ad Astra Control Service, fornirai una chiave account del servizio quando Aggiungi il tuo primo cluster. Astra Control Service utilizza la chiave dell’account del servizio per stabilire l’identità dell’account del servizio appena configurato.

La chiave dell’account del servizio è in formato non crittografato e memorizzata nel formato JSON (JavaScript Object Notation). Contiene informazioni sulle risorse GCP a cui si dispone dei diritti di accesso.

È possibile visualizzare o scaricare il file JSON solo quando si crea la chiave. Tuttavia, è possibile creare una nuova chiave in qualsiasi momento.

Fasi

1. Accedere a Google Cloud e. "creare una chiave dell’account di servizio utilizzando la console, il comando gcloud o un altro metodo preferito".
2. Quando richiesto, salvare il file delle chiavi dell’account di servizio in una posizione sicura.

Il video seguente mostra come creare la chiave dell’account di servizio dalla console Google Cloud.

► https://docs.netapp.com/it-it/astra-control-service/media/get-started/video-create-gcp-service-account-

key.mp4 *(video)*

Opzionale: Configurare il peering di rete per il VPC

Se intendi utilizzare Cloud Volumes Service per Google Cloud come servizio di back-end per lo storage, il passaggio finale è configurare il peering di rete dal tuo VPC a Cloud Volumes Service per Google Cloud.

Il modo più semplice per configurare il peering di rete è ottenere i comandi gcloud direttamente da Cloud Volumes Service. I comandi sono disponibili da Cloud Volumes Service quando si crea un nuovo file system.

Fasi

1. "Vai alle mappe delle regioni globali BlueXP di NetApp" E identificare il tipo di servizio che si utilizza nell'area di Google Cloud in cui risiede il cluster.

   Cloud Volumes Service offre due tipi di servizio: CVS e CVS-Performance. "Scopri di più su questi tipi di servizi".

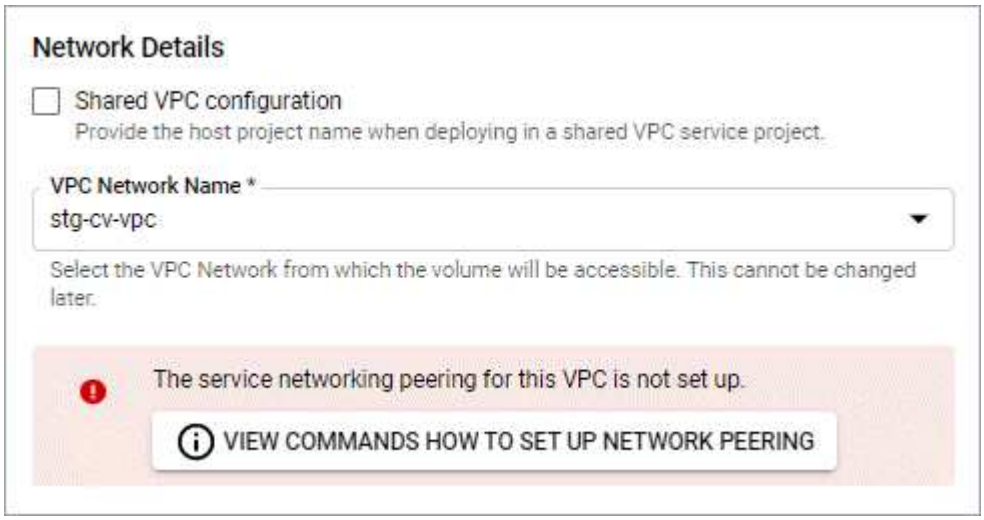
2. "Vai a Cloud Volumes in Google Cloud Platform".
3. Nella pagina **volumi**, selezionare **Crea**.
4. In **tipo di servizio**, selezionare **CVS** o **CVS-Performance**.

   Devi scegliere il tipo di servizio corretto per la tua area geografica Google Cloud. Questo è il tipo di servizio identificato al punto 1. Dopo aver selezionato un tipo di servizio, l'elenco delle regioni nella pagina viene aggiornato con le regioni in cui tale tipo di servizio è supportato.

   Dopo questa fase, è sufficiente inserire le informazioni di rete per ottenere i comandi.

5. In **Regione**, selezionare la propria regione e zona.
6. In **Dettagli rete**, selezionare il VPC.

   Se non hai configurato il peering di rete, verrà visualizzata la seguente notifica:



7. Selezionare il pulsante per visualizzare i comandi di configurazione del peering di rete.
8. Copiare i comandi ed eseguirli in Cloud Shell.

   Per ulteriori informazioni sull'utilizzo di questi comandi, fare riferimento a. "Guida rapida per Cloud Volumes Service per GCP".

"Scopri di più sulla configurazione dell'accesso ai servizi privati e sulla configurazione del peering di rete".

9. Al termine, selezionare Annulla nella pagina **Crea file system**.

   Abbiamo iniziato a creare questo volume solo per ottenere i comandi per il peering di rete.

Configurare Microsoft Azure con Azure NetApp Files

Sono necessari alcuni passaggi per preparare l'abbonamento a Microsoft Azure prima di poter gestire i cluster di servizi Azure Kubernetes con Astra Control Service. Seguire queste istruzioni se si intende utilizzare Azure NetApp Files come backend di storage.

Avvio rapido per la configurazione di Azure

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

[Uno] Esaminare i requisiti del servizio di controllo Astra per Azure Kubernetes Service

Assicurarsi che i cluster siano integri e che eseguano una versione supportata di Kubernetes, che i pool di nodi siano online e che eseguano Linux e altro ancora. Scopri di più su questo passaggio.

[Due] Iscriviti a Microsoft Azure

Creare un account Microsoft Azure. Scopri di più su questo passaggio.

[Tre] Registrati a Azure NetApp Files

Registrare il NetApp Resource Provider. Scopri di più su questo passaggio.

[Quattro] Creare un account NetApp

Accedere a Azure NetApp Files nel portale Azure e creare un account NetApp. Scopri di più su questo passaggio.

[Cinque] Configurare i pool di capacità

Configurare uno o più pool di capacità per i volumi persistenti. Scopri di più su questo passaggio.

[Sei] Delegare una subnet a Azure NetApp Files

Delegare una subnet a Azure NetApp Files in modo che il servizio di controllo Astra possa creare volumi persistenti in tale subnet. Scopri di più su questo passaggio.

[Sette] Creare un'entità del servizio Azure

Creare un'entità del servizio Azure con il ruolo di collaboratore. Scopri di più su questo passaggio.

[Otto] Opzionale: Configurare la ridondanza per i bucket di backup di Azure

Per impostazione predefinita, i bucket Astra Control Service utilizzati per memorizzare i backup di Azure Kubernetes Service utilizzano l'opzione di ridondanza LRS (Redundant Storage) locale. Come passaggio

opzionale, è possibile configurare un livello di ridondanza più duraturo per i bucket Azure. Scopri di più su questo passaggio.

Azure Kubernetes Service Cluster Requirements

Un cluster Kubernetes deve soddisfare i seguenti requisiti per consentirne il rilevamento e la gestione da Astra Control Service.

Versione di Kubernetes

I cluster devono eseguire Kubernetes versione 1,26 - 1,28.

Tipo di immagine

Il tipo di immagine per tutti i pool di nodi deve essere Linux.

Stato del cluster

I cluster devono essere in esecuzione in uno stato integro e avere almeno un nodo di lavoro online senza nodi di lavoro in uno stato di errore.

Regione di Azure

I cluster devono risiedere in una regione in cui è disponibile Azure NetApp Files. "Visualizza i prodotti Azure per regione".

Iscrizione

I cluster devono risiedere in un abbonamento in cui Azure NetApp Files è attivato. Scegli un abbonamento quando lo desideri Registrati a Azure NetApp Files.

VNET

Considerare i seguenti requisiti VNET:

- I cluster devono risiedere in una rete virtuale con accesso diretto a una subnet delegata da Azure NetApp Files. Scopri come configurare una subnet delegata.
- Se i cluster Kubernetes si trovano in un VNET collegato alla subnet delegata Azure NetApp Files di un altro VNET, entrambi i lati della connessione di peering devono essere in linea.
- Tenere presente che il limite predefinito per il numero di IP utilizzati in una rete virtuale (inclusi i VNet con peering immediato) con Azure NetApp Files è 1,000. "Visualizza i limiti delle risorse Azure NetApp Files".

  Se sei vicino al limite, hai due opzioni:

  - È possibile "inviare una richiesta di aumento del limite". Per assistenza, contatta il tuo rappresentante NetApp.
  - Quando si crea un nuovo cluster Amazon Kubernetes Service (AKS), specificare una nuova rete per il cluster. Una volta creata la nuova rete, eseguire il provisioning di una nuova subnet e delegare la subnet a Azure NetApp Files.

Iscriviti a Microsoft Azure

Se non disponi di un account Microsoft Azure, inizia iscrivendoti a Microsoft Azure.

Fasi

1. Accedere alla "Pagina di iscrizione Azure" Per iscriversi al servizio Azure.

2. Selezionare un piano e seguire le istruzioni per completare l'abbonamento.

Registrati a Azure NetApp Files

Ottieni l'accesso a Azure NetApp Files registrando il provider di risorse NetApp.

Fasi

1. Accedere al portale Azure.
2. "Seguire la documentazione di Azure NetApp Files per registrare il provider di risorse NetApp".

Creare un account NetApp

Creare un account NetApp in Azure NetApp Files.

Fase

1. "Seguire la documentazione di Azure NetApp Files per creare un account NetApp dal portale Azure".

Impostare un pool di capacità

Sono necessari uno o più pool di capacità per consentire ad Astra Control Service di eseguire il provisioning di volumi persistenti in un pool di capacità. Astra Control Service non crea pool di capacità per te.

Durante la configurazione dei pool di capacità per le applicazioni Kubernetes, prendere in considerazione quanto segue:

- I pool di capacità devono essere creati nella stessa regione di Azure in cui i cluster AKS saranno gestiti con Astra Control Service.
- Un pool di capacità può avere un livello di servizio Ultra, Premium o Standard. Ciascuno di questi livelli di servizio è progettato per soddisfare diverse esigenze di performance. Astra Control Service supporta tutti e tre.

  È necessario impostare un pool di capacità per ciascun livello di servizio che si desidera utilizzare con i cluster Kubernetes.

  "Scopri di più sui livelli di servizio per Azure NetApp Files".

- Prima di creare un pool di capacità per le applicazioni che si intende proteggere con Astra Control Service, scegliere le prestazioni e la capacità richieste per tali applicazioni.

  Il provisioning della giusta quantità di capacità garantisce agli utenti la possibilità di creare volumi persistenti in base alle esigenze. Se la capacità non è disponibile, non è possibile eseguire il provisioning dei volumi persistenti.

- Un pool di capacità Azure NetApp Files può utilizzare il tipo di QoS manuale o automatico. Astra Control Service supporta i pool di capacità QoS automatici. I pool di capacità QoS manuali non sono supportati.

Fase

1. "Seguire la documentazione di Azure NetApp Files per impostare un pool di capacità QoS automatico".

Delegare una subnet a Azure NetApp Files

È necessario delegare una subnet a Azure NetApp Files in modo che il servizio di controllo Astra possa creare

volumi persistenti in tale subnet. Tenere presente che Azure NetApp Files consente di avere una sola subnet delegata in una rete virtuale.

Se si utilizzano reti virtuali peering, entrambi i lati della connessione di peering devono essere online: La rete virtuale in cui risiedono i cluster Kubernetes e la rete virtuale con la subnet delegata Azure NetApp Files.

Fase

1. "Seguire la documentazione di Azure NetApp Files per delegare una subnet a Azure NetApp Files".

Al termine

Attendere circa 10 minuti prima di rilevare il cluster in esecuzione nella subnet delegata.

Creare un'entità del servizio Azure

Astra Control Service richiede un'entità del servizio Azure a cui viene assegnato il ruolo di collaboratore. Astra Control Service utilizza questo principio del servizio per facilitare la gestione dei dati delle applicazioni Kubernetes per conto dell'utente.

Un service principal è un'identità creata appositamente per l'utilizzo con applicazioni, servizi e strumenti. L'assegnazione di un ruolo all'entità del servizio limita l'accesso a risorse Azure specifiche.

Seguire la procedura riportata di seguito per creare un'entità servizio utilizzando la CLI di Azure. Sarà necessario salvare l'output in un file JSON e fornirlo successivamente ad Astra Control Service. "Fare riferimento alla documentazione di Azure per ulteriori dettagli sull'utilizzo della CLI".

I seguenti passaggi presuppongono che si disponga dell'autorizzazione per creare un'entità servizio e che Microsoft Azure SDK (comando az) sia installato sul computer.

Requisiti

- L'entità del servizio deve utilizzare l'autenticazione regolare. I certificati non sono supportati.
- All'entità del servizio deve essere concesso l'accesso al tuo abbonamento Azure da parte di Contributor o Owner.
- L'abbonamento o il gruppo di risorse scelto per l'ambito deve contenere i cluster AKS e l'account Azure NetApp Files.

Fasi

1. Identificare l'abbonamento e l'ID tenant in cui risiedono i cluster AKS (si tratta dei cluster che si desidera gestire in Astra Control Service).

   ```
   az configure --list-defaults
   az account list --output table
   ```

2. Eseguire una delle seguenti operazioni, a seconda che si utilizzi un'intera sottoscrizione o un gruppo di risorse:
   - Creare l'entità del servizio, assegnare il ruolo di collaboratore e specificare l'ambito dell'intera sottoscrizione in cui risiedono i cluster.

```
az ad sp create-for-rbac --name service-principal-name --role
contributor --scopes /subscriptions/SUBSCRIPTION-ID
```

- Creare l'entità del servizio, assegnare il ruolo di collaboratore e specificare il gruppo di risorse in cui risiedono i cluster.

```
az ad sp create-for-rbac --name service-principal-name --role
contributor --scopes /subscriptions/SUBSCRIPTION-
ID/resourceGroups/RESOURCE-GROUP-ID
```

3. Memorizzare l'output della CLI Azure risultante come file JSON.

   Dovrai fornire questo file in modo che Astra Control Service possa rilevare i tuoi cluster AKS e gestire le operazioni di gestione dei dati Kubernetes. "Scopri di più sulla gestione delle credenziali in Astra Control Service".

4. Facoltativo: Aggiungere l'ID di abbonamento al file JSON in modo che Astra Control Service compili automaticamente l'ID quando si seleziona il file.

   In caso contrario, dovrai inserire l'ID dell'abbonamento in Astra Control Service quando richiesto.

   Esempio

```
{
  "appId": "0db3929a-bfb0-4c93-baee-aaf8",
  "displayName": "sp-example-dev-sandbox",
  "name": "http://sp-example-dev-sandbox",
  "password": "mypassword",
  "tenant": "011cdf6c-7512-4805-aaf8-7721afd8ca37",
  "subscriptionId": "99ce999a-8c99-99d9-a9d9-99cce99f99ad"
}
```

5. Facoltativo: Verificare l'entità del servizio. Scegliere tra i seguenti comandi di esempio a seconda dell'ambito utilizzato dall'entità del servizio.

   Scopo dell'abbonamento

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az group list --subscription SUBSCRIPTION-ID
az aks list --subscription SUBSCRIPTION-ID
az storage container list --account-name STORAGE-ACCOUNT-NAME
```

Ambito del gruppo di risorse

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az aks list --subscription SUBSCRIPTION-ID --resource-group RESOURCE-
GROUP-ID
```

Opzionale: Configurare la ridondanza per i bucket di backup di Azure

È possibile configurare un livello di ridondanza più duraturo per i bucket di backup di Azure. Per impostazione predefinita, i bucket Astra Control Service utilizzati per memorizzare i backup di Azure Kubernetes Service utilizzano l'opzione di ridondanza LRS (Redundant Storage) locale. Per utilizzare un'opzione di ridondanza più durevole per i bucket Azure, è necessario eseguire le seguenti operazioni:

Fasi

1. Creare un account di storage Azure che utilizzi il livello di ridondanza necessario "queste istruzioni".
2. Creare un container Azure nel nuovo account storage utilizzando "queste istruzioni".
3. Aggiungere il container come bucket ad Astra Control Service. Fare riferimento a. "Aggiungere un bucket aggiuntivo".
4. (Facoltativo) per utilizzare il bucket appena creato come bucket predefinito per i backup di Azure, impostarlo come bucket predefinito per Azure. Fare riferimento a. "Modificare il bucket predefinito".

Configurare Microsoft Azure con dischi gestiti Azure

Sono necessari alcuni passaggi per preparare l'abbonamento a Microsoft Azure prima di poter gestire i cluster di servizi Azure Kubernetes con Astra Control Service. Seguire queste istruzioni se si intende utilizzare i dischi gestiti da Azure come backend di storage.

Avvio rapido per la configurazione di Azure

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

[Uno] Esaminare i requisiti del servizio di controllo Astra per Azure Kubernetes Service

Assicurarsi che i cluster siano integri e che eseguano una versione supportata di Kubernetes, che i pool di nodi siano online e che eseguano Linux e altro ancora. Scopri di più su questo passaggio.

[Due] Iscriviti a Microsoft Azure

Creare un account Microsoft Azure. Scopri di più su questo passaggio.

[Tre] Creare un'entità del servizio Azure

Creare un'entità del servizio Azure con il ruolo di collaboratore. Scopri di più su questo passaggio.

[Quattro] Configurare i dettagli del driver CSI (Container Storage Interface)

È necessario configurare l'abbonamento Azure e il cluster per il funzionamento con i driver CSI. Scopri di più su questo passaggio.

[Cinque] Opzionale: Configurare la ridondanza per i bucket di backup di Azure

Per impostazione predefinita, i bucket Astra Control Service utilizzati per memorizzare i backup di Azure Kubernetes Service utilizzano l'opzione di ridondanza LRS (Redundant Storage) locale. Come passaggio opzionale, è possibile configurare un livello di ridondanza più duraturo per i bucket Azure. Scopri di più su questo passaggio.

Azure Kubernetes Service Cluster Requirements

Un cluster Kubernetes deve soddisfare i seguenti requisiti per consentirne il rilevamento e la gestione da Astra Control Service.

Versione di Kubernetes

I cluster devono eseguire Kubernetes versione 1,26 - 1,28.

Tipo di immagine

Il tipo di immagine per tutti i pool di nodi deve essere Linux.

Stato del cluster

I cluster devono essere in esecuzione in uno stato integro e avere almeno un nodo di lavoro online senza nodi di lavoro in uno stato di errore.

Regione di Azure

Come Best practice, è necessario scegliere una regione che supporti Azure NetApp Files, anche se non viene utilizzata come back-end di storage. In questo modo sarà più semplice utilizzare Azure NetApp Files come back-end di storage in futuro se i requisiti di performance cambiano. "Visualizza i prodotti Azure per regione".

Driver CSI

I cluster devono avere installati i driver CSI appropriati.

Iscriviti a Microsoft Azure

Se non disponi di un account Microsoft Azure, inizia iscrivendoti a Microsoft Azure.

Fasi

1. Accedere alla "Pagina di iscrizione Azure" Per iscriversi al servizio Azure.
2. Selezionare un piano e seguire le istruzioni per completare l'abbonamento.

Creare un'entità del servizio Azure

Astra Control Service richiede un'entità del servizio Azure a cui viene assegnato il ruolo di collaboratore. Astra Control Service utilizza questo principio del servizio per facilitare la gestione dei dati delle applicazioni Kubernetes per conto dell'utente.

Un service principal è un'identità creata appositamente per l'utilizzo con applicazioni, servizi e strumenti. L'assegnazione di un ruolo all'entità del servizio limita l'accesso a risorse Azure specifiche.

Seguire la procedura riportata di seguito per creare un'entità servizio utilizzando la CLI di Azure. Sarà necessario salvare l'output in un file JSON e fornirlo successivamente ad Astra Control Service. "Fare riferimento alla documentazione di Azure per ulteriori dettagli sull'utilizzo della CLI".

I seguenti passaggi presuppongono che si disponga dell'autorizzazione per creare un'entità servizio e che Microsoft Azure SDK (comando az) sia installato sul computer.

Requisiti

- L'entità del servizio deve utilizzare l'autenticazione regolare. I certificati non sono supportati.
- All'entità del servizio deve essere concesso l'accesso al tuo abbonamento Azure da parte di Contributor o Owner.
- L'abbonamento o il gruppo di risorse scelto per l'ambito deve contenere i cluster AKS e l'account Azure NetApp Files.

Fasi

1. Identificare l'abbonamento e l'ID tenant in cui risiedono i cluster AKS (si tratta dei cluster che si desidera gestire in Astra Control Service).

   ```
   az configure --list-defaults
   az account list --output table
   ```

2. Eseguire una delle seguenti operazioni, a seconda che si utilizzi un'intera sottoscrizione o un gruppo di risorse:
   - Creare l'entità del servizio, assegnare il ruolo di collaboratore e specificare l'ambito dell'intera sottoscrizione in cui risiedono i cluster.

     ```
     az ad sp create-for-rbac --name service-principal-name --role
     contributor --scopes /subscriptions/SUBSCRIPTION-ID
     ```

   - Creare l'entità del servizio, assegnare il ruolo di collaboratore e specificare il gruppo di risorse in cui risiedono i cluster.

     ```
     az ad sp create-for-rbac --name service-principal-name --role
     contributor --scopes /subscriptions/SUBSCRIPTION-
     ID/resourceGroups/RESOURCE-GROUP-ID
     ```

3. Memorizzare l'output della CLI Azure risultante come file JSON.

   Dovrai fornire questo file in modo che Astra Control Service possa rilevare i tuoi cluster AKS e gestire le operazioni di gestione dei dati Kubernetes. "Scopri di più sulla gestione delle credenziali in Astra Control Service".

4. Facoltativo: Aggiungere l'ID di abbonamento al file JSON in modo che Astra Control Service compili automaticamente l'ID quando si seleziona il file.

   In caso contrario, dovrai inserire l'ID dell'abbonamento in Astra Control Service quando richiesto.

Esempio

```
{
  "appId": "0db3929a-bfb0-4c93-baee-aaf8",
  "displayName": "sp-example-dev-sandbox",
  "name": "http://sp-example-dev-sandbox",
  "password": "mypassword",
  "tenant": "011cdf6c-7512-4805-aaf8-7721afd8ca37",
  "subscriptionId": "99ce999a-8c99-99d9-a9d9-99cce99f99ad"
}
```

5. Facoltativo: Verificare l'entità del servizio. Scegliere tra i seguenti comandi di esempio a seconda dell'ambito utilizzato dall'entità del servizio.

Scopo dell'abbonamento

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az group list --subscription SUBSCRIPTION-ID
az aks list --subscription SUBSCRIPTION-ID
az storage container list --account-name STORAGE-ACCOUNT-NAME
```

Ambito del gruppo di risorse

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az aks list --subscription SUBSCRIPTION-ID --resource-group RESOURCE-
GROUP-ID
```

Configurare i dettagli del driver CSI (Container Storage Interface)

Per utilizzare i dischi gestiti Azure con Astra Control Service, è necessario installare i driver CSI richiesti.

Attivare la funzione del driver CSI nell'abbonamento Azure

Prima di installare i driver CSI, è necessario attivare la funzionalità del driver CSI nell'abbonamento Azure.

Fasi

1. Aprire l'interfaccia della riga di comando di Azure.
2. Eseguire il seguente comando per registrare il driver:

```
az feature register --namespace "Microsoft.ContainerService" --name
"EnableAzureDiskFileCSIDriver"
```

3. Eseguire il seguente comando per assicurarsi che la modifica venga propagata:

```
az provider register -n Microsoft.ContainerService
```

L'output dovrebbe essere simile a quanto segue:

```
{
"id": "/subscriptions/b200155f-001a-43be-87be-
3edde83acef4/providers/Microsoft.Features/providers/Microsoft.ContainerSer
vice/features/EnableAzureDiskFileCSIDriver",
"name": "Microsoft.ContainerService/EnableAzureDiskFileCSIDriver",
"properties": {
   "state": "Registering"
},
"type": "Microsoft.Features/providers/features"
}
```

Installare i driver CSI del disco gestito Azure nel cluster Azure Kubernetes Service

È possibile installare i driver di Azure CSI per completare la preparazione.

Fase

1. Passare a. "La documentazione del driver Microsoft CSI".
2. Seguire le istruzioni per installare i driver CSI richiesti.

Opzionale: Configurare la ridondanza per i bucket di backup di Azure

È possibile configurare un livello di ridondanza più duraturo per i bucket di backup di Azure. Per impostazione predefinita, i bucket Astra Control Service utilizzati per memorizzare i backup di Azure Kubernetes Service utilizzano l'opzione di ridondanza LRS (Redundant Storage) locale. Per utilizzare un'opzione di ridondanza più durevole per i bucket Azure, è necessario eseguire le seguenti operazioni:

Fasi

1. Creare un account di storage Azure che utilizzi il livello di ridondanza necessario "queste istruzioni".
2. Creare un container Azure nel nuovo account storage utilizzando "queste istruzioni".
3. Aggiungere il container come bucket ad Astra Control Service. Fare riferimento a. "Aggiungere un bucket aggiuntivo".
4. (Facoltativo) per utilizzare il bucket appena creato come bucket predefinito per i backup di Azure, impostarlo come bucket predefinito per Azure. Fare riferimento a. "Modificare il bucket predefinito".