Richten Sie Ihren Cloud-Provider ein

Astra Control Service

NetApp
March 28, 2023

Inhaltsverzeichnis

Richten Sie Ihren Cloud-Provider ein

Einrichten von Amazon Web Services

Zur Vorbereitung Ihres Amazon Web Services Projekts sind einige Schritte erforderlich, bevor Sie Amazon Elastic Kubernetes Service (EKS) Cluster mit Astra Control Service managen können.

Schnellstart für die Einrichtung von Amazon Web Services

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

[Eins] Astra Control Service-Anforderungen für Amazon Web Services überprüfen

Stellen Sie sicher, dass die Cluster ordnungsgemäß sind und eine unterstützte Version von Kubernetes ausführen, dass Worker-Nodes unter anderem Linux oder Windows online sind. Erfahren Sie mehr zu diesem Schritt.

[Zwei] Erstellen Sie ein Amazon-Konto

Wenn Sie noch kein Amazon-Konto haben, müssen Sie ein Konto erstellen, damit Sie EKS verwenden können. Erfahren Sie mehr zu diesem Schritt.

[Drittens] Installieren Sie die Amazon Web Services-CLI

Installieren Sie die AWS CLI, sodass Sie AWS über die Befehlszeile managen können. Befolgen Sie die Schritt-für-Schritt-Anweisungen.

[Vier] Optional: Erstellen Sie einen IAM-Benutzer

Erstellen Sie einen Amazon IAM-Benutzer (Identity and Access Management). Sie können diesen Schritt auch überspringen und einen vorhandenen IAM-Benutzer mit Astra Control Service verwenden.

Lesen Sie Schritt-für-Schritt-Anleitungen.

[Fünf] Erstellen Sie eine Berechtigungsrichtlinie und fügen Sie sie an

Erstellen einer Richtlinie mit den erforderlichen Berechtigungen für den Astra Control Service zur Interaktion mit Ihrem AWS Konto

Lesen Sie Schritt-für-Schritt-Anleitungen.

[Sechs] Speichern Sie die Anmeldeinformationen für den IAM-Benutzer

Speichern Sie die Anmeldeinformationen für den IAM-Benutzer, damit Sie die Anmeldeinformationen in den Astra Control Service importieren können.

Lesen Sie Schritt-für-Schritt-Anleitungen.

EKS-Clusteranforderungen

Ein Kubernetes-Cluster muss folgende Anforderungen erfüllen, damit Sie ihn über den Astra Control Service erkennen und managen können.

Kubernetes-Version

Auf einem Cluster muss eine Kubernetes-Version im Bereich von 1.22 bis 1.24 ausgeführt werden.

Bildtyp

Der Bildtyp für jeden Arbeiterknoten muss Linux sein.

Der Cluster-Status

Cluster müssen in einem ordnungsgemäßen Zustand ausgeführt werden und mindestens einen Online-Worker-Node ohne „Worker“-Nodes im ausgefallenen Status aufweisen.

Astra Trident für Amazon FSX für NetApp ONTAP

Wenn Sie das Backend von Amazon FSX für NetApp ONTAP Storage nutzen, müssen Sie Astra Trident installieren. Anweisungen finden Sie unter "Astra Trident – Übersicht über die Implementierung". Weitere Informationen zur Verwendung von Astra Trident mit FSX für NetApp ONTAP finden Sie unter "Setzen Sie Astra Trident mit Amazon FSX für NetApp ONTAP ein".

CSI-Treiber für Amazon Elastic Block Store (EBS)

Wenn Sie das Amazon EBS Storage-Backend verwenden, müssen Sie den Container Storage Interface (CSI)-Treiber für EBS installieren (dieser wird nicht automatisch installiert).

Anweisungen zur Installation des CSI-Treibers finden Sie in den Details.

Installieren Sie einen externen Schnappschussfilter

1. Erstellen von Volume Snapshot-CRDs.

   Verwenden Sie für Kubernetes ab Version 1.20 v1 Snapshot-CRDs mit Snapshot-Komponenten von v5.0.

```
$ cat snapshot-setup.sh
#!/bin/bash
# Create volume snapshot CRDs
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-5.0/client/config/crd/snapshot.storage.k8s.io_volumesnapshotclasses.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-5.0/client/config/crd/snapshot.storage.k8s.io_volumesnapshotcontents.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-5.0/client/config/crd/snapshot.storage.k8s.io_volumesnapshots.yaml
```

1. Erstellen Sie den Snapshot-Controller im gewünschten Namespace. Bearbeiten Sie die YAML-Manifeste unten, um den Namespace zu ändern.

   Für Kubernetes 1.20 und höher verwenden Sie v5.0.

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-5.0/deploy/kubernetes/snapshot-controller/rbac-snapshot-controller.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-5.0/deploy/kubernetes/snapshot-controller/setup-snapshot-controller.yaml
```

Den CSI-Treiber als Amazon EKS-Add-On installieren

1. Erstellen der IAM-Rolle des Amazon EBS CSI-Treibers für Service-Konten Befolgen Sie die Anweisungen "In der Amazon-Dokumentation", Verwenden der AWS CLI-Befehle in den Anweisungen.
2. Fügen Sie das Amazon EBS CSI-Add-on mit dem folgenden AWS-CLI-Befehl hinzu und ersetzen Sie Informationen in Klammern <> durch Werte speziell für Ihre Umgebung. Ersetzen Sie <DRIVER_ROLE> durch den Namen der EBS CSI-Treiberrolle, die Sie im vorherigen Schritt erstellt haben:

```
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>
```

Konfigurieren der EBS Storage-Klasse

1. Klonen Sie das GitHub Repository des Amazon EBS CSI-Treibers auf Ihrem System.

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

2. Navigieren Sie zum Beispielverzeichnis für dynamische Bereitstellung.

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

3. Implementierung der ebs-sc-Storage-Klasse und der ebs-Claim Persistent Volume Claim aus dem Manifeste Verzeichnis

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

4. ebs-sc Storage-Klasse beschreiben

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

   Sie sollten die Ausgabe sehen, in der die Attribute der Storage-Klasse beschrieben werden.

Erstellen Sie ein Amazon-Konto

Wenn Sie noch kein Amazon-Konto besitzen, müssen Sie ein Konto erstellen, um die Abrechnung für Amazon EKS zu aktivieren.

Schritte

1. Wechseln Sie zum "Amazon Homepage" Wählen Sie oben rechts **Anmelden** und wählen Sie **Hier starten**.
2. Befolgen Sie die Anweisungen, um ein Konto zu erstellen.

Installieren Sie die Amazon Web Services-CLI

Installieren Sie die AWS CLI, sodass Sie AWS Ressourcen über die Befehlszeile managen können.

Schritt

1. Gehen Sie zu "Erste Schritte mit der AWS CLI" Und befolgen Sie die Anweisungen zur Installation der CLI.

Optional: Erstellen Sie einen IAM-Benutzer

Erstellen Sie einen IAM-Benutzer, damit Sie AWS Services und Ressourcen mit erhöhter Sicherheit nutzen und managen können. Sie können diesen Schritt auch überspringen und einen vorhandenen IAM-Benutzer mit Astra Control Service verwenden.

Schritt

1. Gehen Sie zu "IAM-Benutzer werden erstellt" Und befolgen Sie die Anweisungen zum Erstellen eines IAM-Benutzers.

Erstellen Sie eine Berechtigungsrichtlinie und fügen Sie sie an

Erstellen einer Richtlinie mit den erforderlichen Berechtigungen für den Astra Control Service zur Interaktion mit Ihrem AWS Konto

Schritte

1. Erstellen Sie eine neue Datei mit dem Namen `policy.json`.
2. Kopieren Sie den folgenden JSON-Inhalt in die Datei:

```
{
    "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. Erstellen der Richtlinie:

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

4. Hängen Sie die Richtlinie an den IAM-Benutzer an. Austausch `<IAM-USER-NAME>` Entweder mit dem Benutzernamen des von Ihnen erstellten IAM-Benutzers oder mit einem vorhandenen IAM-Benutzer:

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

Speichern Sie die Anmeldeinformationen für den IAM-Benutzer

Speichern Sie die Anmeldeinformationen für den IAM-Benutzer, damit Sie den Astra Control Service auf den Benutzer aufmerksam machen können.

Schritte

1. Anmeldedaten herunterladen Austausch `<IAM-USER-NAME>` Mit dem Benutzernamen des IAM-Benutzers, den Sie verwenden möchten:

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

Ergebnis

Der `credential.json` Datei ist erstellt, und Sie können die Anmeldeinformationen in Astra Control Service importieren.

Google Cloud einrichten

Zur Vorbereitung Ihres Google Cloud-Projekts sind einige Schritte erforderlich, bevor Sie Google Kubernetes Engine-Cluster mit Astra Control Service verwalten können.

> Wenn Sie Google Cloud Volumes Service for Google Cloud nicht als Speicher-Backend nutzen, sondern zu einem späteren Zeitpunkt nutzen möchten, sollten Sie die notwendigen Schritte ausführen, um Google Cloud Volumes Service für Google Cloud jetzt zu konfigurieren. Das Erstellen eines Service-Kontos im späteren Verlauf bedeutet, dass der Zugriff auf die vorhandenen Storage-Buckets verloren geht.

Schnellstart für die Einrichtung von Google Cloud

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

[Eins] Astra Control Service-Anforderungen für Google Kubernetes Engine prüfen

Stellen Sie sicher, dass die Cluster ordnungsgemäß sind und eine unterstützte Kubernetes-Version ausführen, dass Worker-Nodes online sind und einen unterstützten Bildtyp ausführen, und vieles mehr. Erfahren Sie mehr zu diesem Schritt.

[Zwei] (Optional): Kaufen Sie Cloud Volumes Service für Google Cloud

Wenn Sie Cloud Volumes Service für Google Cloud als Storage-Back-End verwenden möchten, gehen Sie zur NetApp Cloud Volumes Service Seite im Google Cloud Marketplace und wählen Sie „Kaufen“. Erfahren Sie mehr zu diesem Schritt.

[Drittens] Aktivieren Sie APIs in Ihrem Google Cloud-Projekt

Aktivieren Sie die folgenden Google Cloud APIs:

- Google Kubernetes Engine

- Cloud-Storage
- Cloud Storage JSON API
- Nutzung Von Services
- Cloud Resource Manager API
- NetApp Cloud Volumes Service
  - Für Cloud Volumes Service für Google Cloud erforderlich
  - Optional (aber empfohlen) für Google Persistent Disk
- Service Consumer Management API
- Service Networking API
- Service-Management-API

Befolgen Sie die Schritt-für-Schritt-Anweisungen.

[Vier] Erstellen Sie ein Dienstkonto mit den erforderlichen Berechtigungen

Erstellen Sie ein Google Cloud-Servicekonto mit folgenden Berechtigungen:

- Kubernetes Engine-Administrator
- NetApp Cloud Volumes Admin
  - Für Cloud Volumes Service für Google Cloud erforderlich
  - Optional (aber empfohlen) für Google Persistent Disk
- Storage-Admin
- Viewer Für Die Nutzung Des Dienstes
- Network Viewer Für Computing

Lesen Sie Schritt-für-Schritt-Anleitungen.

[Fünf] Erstellen eines Service-Kontokonschlüssels

Erstellen Sie einen Schlüssel für das Servicekonto, und speichern Sie die Schlüsseldatei an einem sicheren Speicherort. Befolgen Sie die Schritt-für-Schritt-Anweisungen.

[Sechs] (Optional): Netzwerk-Peering für Ihr VPC einrichten

Wenn Sie Cloud Volumes Service für Google Cloud als Storage-Back-End verwenden möchten, richten Sie Netzwerk-Peering von Ihrem VPC zu Cloud Volumes Service für Google Cloud ein. Befolgen Sie die Schritt-für-Schritt-Anweisungen.

GKE-Clusteranforderungen

Ein Kubernetes-Cluster muss folgende Anforderungen erfüllen, damit Sie ihn über den Astra Control Service erkennen und managen können. Einige dieser Anforderungen gelten nur, wenn Sie Cloud Volumes Service für Google Cloud als Storage-Backend verwenden möchten.

Kubernetes-Version

Auf einem Cluster muss eine Kubernetes-Version im Bereich von 1.22 bis 1.24 ausgeführt werden.

Bildtyp

Der Bildtyp für jeden Arbeiterknoten muss sein `COS_CONTAINERD`.

Der Cluster-Status

Cluster müssen in einem ordnungsgemäßen Zustand ausgeführt werden und mindestens einen Online-Worker-Node ohne „Worker“-Nodes im ausgefallenen Status aufweisen.

Google Cloud-Region

Wenn Sie Cloud Volumes Service für Google Cloud als Storage-Back-End verwenden möchten, müssen Cluster in einem ausgeführt werden "Google Cloud-Region, in der Cloud Volumes Service für Google Cloud unterstützt wird." Der Astra Control Service unterstützt beide Servicetypen: CVS und CVS-Performance. Als Best Practice sollten Sie eine Region wählen, die Cloud Volumes Service für Google Cloud unterstützt, auch wenn Sie sie nicht als Storage-Backend verwenden. Dies vereinfacht die Verwendung von Cloud Volumes Service für Google Cloud als Storage-Backend, wenn sich Ihre Performance-Anforderungen ändern.

Netzwerkbetrieb

Wenn Sie Cloud Volumes Service für Google Cloud als Storage-Back-End verwenden möchten, muss der Cluster in einer VPC oder der mit Cloud Volumes Service für Google Cloud Peering durchgeführt werden. Dieser Schritt wird im Folgenden beschrieben.

Private Cluster

Wenn das Cluster privat ist, gilt das "Autorisierte Netzwerke" Die Astra Control Service-IP-Adresse muss zugelassen werden:

52.188.218.166/32

Betriebsmodus für ein GKE-Cluster

Sie sollten den Standardbetriebsmodus verwenden. Der Autopilot-Modus wurde derzeit nicht getestet. "Erfahren Sie mehr über Betriebsmodi".

Optional: Kauf von Cloud Volumes Service für Google Cloud

Astra Control Service kann Cloud Volumes Service für Google Cloud als Storage-Backend für Ihre persistenten Volumes nutzen. Wenn Sie diesen Service nutzen möchten, müssen Sie Cloud Volumes Service für Google Cloud über Google Cloud Marketplace erwerben, um die Abrechnung für persistente Volumes zu ermöglichen.

Schritt

1. Wechseln Sie zum "NetApp Cloud Volumes Service Seite" Wählen Sie im Google Cloud Marketplace die Option **Einkauf** aus, und folgen Sie den Anweisungen.

   "Befolgen Sie die Schritt-für-Schritt-Anweisungen in der Google Cloud-Dokumentation, um den Service zu erwerben und zu aktivieren".

Aktivieren Sie APIs in Ihrem Projekt

Für Ihr Projekt sind Berechtigungen erforderlich, um auf bestimmte Google Cloud-APIs zuzugreifen. APIs werden für die Interaktion mit Google Cloud-Ressourcen eingesetzt, beispielsweise mit Google Kubernetes Engine-Clustern (GKE) und NetApp Cloud Volumes Service Storage.

Schritt

1. "Verwenden Sie die Google Cloud-Konsole oder die gcloudbasierte CLI, um die folgenden APIs zu

aktivieren":

- Google Kubernetes Engine
- Cloud-Storage
- Cloud Storage JSON API
- Nutzung Von Services
- Cloud Resource Manager API
- NetApp Cloud Volumes Service (für Cloud Volumes Service für Google Cloud erforderlich)
- Service Consumer Management API
- Service Networking API
- Service-Management-API

Das folgende Video zeigt, wie die APIs über die Google Cloud-Konsole aktiviert werden.

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

Erstellen eines Dienstkontos

Astra Control Service nutzt ein Google Cloud-Service-Konto, um das Management von Kubernetes-Applikationsdaten in Ihrem Auftrag zu vereinfachen.

Schritte

1. Besuchen Sie Google Cloud und "Erstellen Sie ein Servicekonto, indem Sie die Konsole, den gcloudbasierten Befehl oder eine andere bevorzugte Methode verwenden".
2. Gewähren Sie dem Dienstkonto die folgenden Rollen:
   - **Kubernetes Engine Admin** - wird verwendet, um Cluster aufzulisten und Administratorzugriff zum Verwalten von Apps zu erstellen.
   - **NetApp Cloud Volumes Admin** - wird für das Management von persistentem Storage für Applikationen verwendet.
   - **Storage Admin** - zur Verwaltung von Buckets und Objekten für Backups von Apps.
   - **Service Usage Viewer** - wird verwendet, um zu überprüfen, ob die erforderlichen Cloud Volumes Service für Google Cloud APIs aktiviert sind.
   - **Computing Network Viewer** - wird verwendet, um zu prüfen, ob die Kubernetes VPC erlaubt ist, Cloud Volumes Service für Google Cloud zu erreichen.

Wenn Sie gcloudbasierte Lösungen verwenden möchten, können Sie im Astra Control Interface die gewünschten Schritte ausführen. Wählen Sie **Konto > Anmeldeinformationen > Anmeldeinformationen hinzufügen**, und wählen Sie dann **Anweisungen** aus.

Wenn Sie die Google Cloud-Konsole verwenden möchten, wird im folgenden Video gezeigt, wie Sie das Servicekonto über die Konsole erstellen.

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

account.mp4 *(video)*

Konfigurieren des Service-Kontos für eine gemeinsame VPC

Um GKE-Cluster zu verwalten, die sich in einem Projekt befinden, aber ein VPC aus einem anderen Projekt (ein gemeinsames VPC) zu verwenden, müssen Sie das Astra-Servicekonto als Mitglied des Hostprojekts mit der Rolle **Compute Network Viewer** angeben.

Schritte

1. Wählen Sie von der Google Cloud-Konsole aus die Option **IAM & Admin** aus und wählen Sie **Servicekonten** aus.
2. Finden Sie das Astra-Servicekonto mit "Die erforderlichen Berechtigungen" Und dann kopieren Sie die E-Mail-Adresse.
3. Gehen Sie zu Ihrem Hostprojekt und wählen Sie dann **IAM & Admin** > **IAM**.
4. Wählen Sie **Hinzufügen** und fügen Sie einen Eintrag für das Servicekonto hinzu.
   a. **Neue Mitglieder**: Geben Sie die E-Mail-Adresse für das Service-Konto ein.
   b. **Rolle**: Wählen Sie **Compute Network Viewer**.
   c. Wählen Sie **Speichern**.

Ergebnis

Das Hinzufügen eines GKE-Clusters mithilfe einer gemeinsamen VPC wird mit Astra vollständig funktionieren.

Erstellen eines Service-Kontokonschlüssels

Statt dem Astra Control Service einen Benutzernamen und ein Passwort anzugeben, stellen Sie beim Hinzufügen des ersten Clusters einen Service-Account-Schlüssel bereit. Astra Control Service verwendet den Service-Account-Schlüssel, um die Identität des Service-Kontos zu ermitteln, das Sie gerade eingerichtet haben.

Der Dienstkontenschlüssel ist Klartext im JavaScript Object Notation (JSON) Format gespeichert. Es enthält Informationen zu den GCP-Ressourcen, auf die Sie Zugriff haben.

Sie können die JSON-Datei nur anzeigen oder herunterladen, wenn Sie den Schlüssel erstellen. Sie können jedoch jederzeit einen neuen Schlüssel erstellen.

Schritte

1. Besuchen Sie Google Cloud und "Erstellen Sie einen Service-Kontokschlüssel über die Konsole, den gcloudbasierten Befehl oder eine andere bevorzugte Methode".
2. Wenn Sie dazu aufgefordert werden, speichern Sie die Servicekontoschlüsseldatei an einem sicheren Ort.

Das folgende Video zeigt, wie der Service-Kontokschlüssel über die Google Cloud-Konsole erstellt wird.

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

key.mp4 *(video)*

Optional: Netzwerk-Peering für Ihr VPC einrichten

Wenn Sie Cloud Volumes Service für Google Cloud als Storage-Backend-Service nutzen möchten, besteht der letzte Schritt darin, Netzwerk-Peering von Ihrem VPC zum Cloud Volumes Service für Google Cloud einzurichten.

Die einfachste Möglichkeit, Netzwerk-Peering einzurichten, besteht darin, die gcloudbefehle direkt von Cloud Volumes Service zu beziehen. Die Befehle sind über Cloud Volumes Service verfügbar, wenn ein neues Dateisystem erstellt wird.

Schritte

1. "Gehen Sie zu den globalen Regions Maps von NetApp Cloud Central" Und geben Sie den Servicetyp an, den Sie in der Region Google Cloud verwenden möchten, in der sich Ihr Cluster befindet.

   Cloud Volumes Service bietet zwei Arten von Services: CVS und CVS-Performance. "Erfahren Sie mehr über diese Service-Typen".

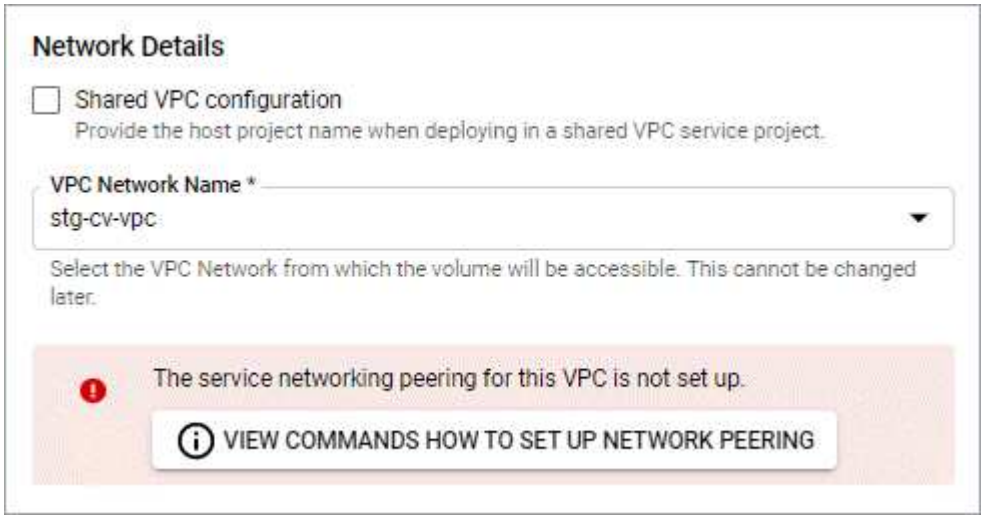
2. "Wechseln Sie zu Cloud Volumes in der Google Cloud Platform".
3. Wählen Sie auf der Seite **Bände** die Option **Erstellen**.
4. Wählen Sie unter **Diensttyp** entweder **CVS** oder **CVS-Performance** aus.

   Sie müssen den richtigen Servicetyp für Ihre Google Cloud-Region auswählen. Dies ist der Service-Typ, den Sie in Schritt 1 identifiziert haben. Nachdem Sie einen Servicetyp ausgewählt haben, wird die Liste der Regionen auf der Seite mit den Regionen aktualisiert, in denen dieser Servicetyp unterstützt wird.

   Nach diesem Schritt müssen Sie nur Ihre Netzwerkinformationen eingeben, um die Befehle abzurufen.

5. Wählen Sie unter **Region** Ihre Region und Zone aus.
6. Wählen Sie unter **Netzwerkdetails** die VPC aus.

   Wenn Sie Netzwerk-Peering nicht eingerichtet haben, sehen Sie die folgende Benachrichtigung:



7. Wählen Sie die Schaltfläche aus, um die Befehle zum Einrichten von Netzwerk-Peering anzuzeigen.
8. Kopieren Sie die Befehle und führen Sie sie in Cloud Shell aus.

Weitere Informationen zur Verwendung dieser Befehle finden Sie im "QuickStart for Cloud Volumes Service for GCP".

"Erfahren Sie mehr über die Konfiguration des Zugriffs auf private Services und die Einrichtung von Netzwerk-Peering".

9. Nachdem Sie fertig sind, können Sie auf der Seite **Dateisystem erstellen** Abbrechen auswählen.

   Wir haben mit dem Erstellen dieses Volumes nur begonnen, um die Befehle für Netzwerk-Peering zu erhalten.

Microsoft Azure mit Azure NetApp Files einrichten

Einige Schritte sind zur Vorbereitung Ihres Microsoft Azure Abonnements erforderlich, bevor Sie Azure Kubernetes Service-Cluster mit Astra Control Service managen können. Folgen Sie diesen Anweisungen, wenn Sie Azure NetApp Files als Storage-Back-End verwenden möchten.

Schnellstart für die Einrichtung von Azure

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

[Eins] Astra Control Service-Anforderungen für Azure Kubernetes Service prüfen

Vergewissern Sie sich, dass die Cluster ordnungsgemäß sind und eine unterstützte Version von Kubernetes ausführen, dass Node-Pools unter Linux verfügbar sind und unter anderem. Erfahren Sie mehr zu diesem Schritt.

[Zwei] Melden Sie sich für Microsoft Azure an

Erstellen Sie ein Microsoft Azure Konto. Erfahren Sie mehr zu diesem Schritt.

[Drittens] Für Azure NetApp Files anmelden

Registrieren Sie den NetApp Resource Provider. Erfahren Sie mehr zu diesem Schritt.

[Vier] Erstellen Sie einen NetApp Account

Erstellen Sie im Azure-Portal unter Azure NetApp Files einen NetApp Account. Erfahren Sie mehr zu diesem Schritt.

[Fünf] Einrichten von Kapazitäts-Pools

Richten Sie einen oder mehrere Kapazitäts-Pools für Ihre persistenten Volumes ein. Erfahren Sie mehr zu diesem Schritt.

[Sechs] Delegieren eines Subnetzes an Azure NetApp Files

Delegieren Sie ein Subnetz an Azure NetApp Files, damit der Astra Control Service persistente Volumes in diesem Subnetz erstellen kann. Erfahren Sie mehr zu diesem Schritt.

[Sieben] Erstellen Sie einen Azure Service Principal

Erstellen Sie einen Azure-Serviceprincipal mit der Rolle „Contributor“. Erfahren Sie mehr zu diesem Schritt.

[Acht] Optional: Redundanz für Azure Backup Buckets konfigurieren

Standardmäßig verwendet der Buckets Astra Control Service für das Speichern von Azure Kubernetes Service-Backups die LRS-Redundanzoption (lokal Redundant Storage). Als optionaler Schritt können Sie einen langlebigen Grad an Redundanz für Azure Buckets konfigurieren. Erfahren Sie mehr zu diesem Schritt.

Anforderungen für den Azure Kubernetes Service-Cluster

Ein Kubernetes-Cluster muss folgende Anforderungen erfüllen, damit Sie ihn über den Astra Control Service erkennen und managen können.

Kubernetes-Version
: Auf Clustern muss die Kubernetes-Version 1.23 bis 1.25 ausgeführt werden.

Bildtyp
: Der Image-Typ für alle Node-Pools muss Linux sein.

Der Cluster-Status
: Cluster müssen in einem ordnungsgemäßen Zustand ausgeführt werden und mindestens einen Online-Worker-Node ohne „Worker“-Nodes im ausgefallenen Status aufweisen.

Azure Region
: Cluster müssen in einer Region residieren, in der Azure NetApp Files verfügbar ist. "Hier finden Sie Azure Produkte nach Region".

Abonnement
: Cluster müssen in einem Abonnement gespeichert werden, in dem Azure NetApp Files aktiviert ist. Sie wählen ein Abonnement, wenn Sie für Azure NetApp Files anmelden.

Vnet
: Folgende vnet-Anforderungen sind zu berücksichtigen:

- Cluster müssen sich in einem vnet befinden, das direkten Zugriff auf ein für Azure NetApp Files delegiertes Subnetz hat. Erfahren Sie, wie Sie ein delegiertes Subnetz einrichten.
- Wenn sich Ihre Kubernetes Cluster in einem vnet befinden, das über das von Azure NetApp Files delegierte Subnetz in einem anderen vnet verfügt, müssen beide Seiten der Peering-Verbindung online sein.
- Beachten Sie, dass die Standardgrenze für die Anzahl der IP-Adressen, die in einem vnet (einschließlich sofort gepedierter VNets) mit Azure NetApp Files verwendet werden, 1,000 ist. "Zeigen Sie Einschränkungen für Azure NetApp Files-Ressourcen an".

  Wenn Sie nahe am Limit sind, haben Sie zwei Möglichkeiten:

  - Das können Sie "Senden Sie eine Anfrage für eine Grenzerhöhung". Wenden Sie sich an Ihren NetApp Ansprechpartner, wenn Sie Hilfe benötigen.
  - Geben Sie bei der Erstellung eines neuen Amazon Kubernetes Service (AKS)-Clusters ein neues Netzwerk für den Cluster an. Sobald das neue Netzwerk erstellt wurde, stellen Sie ein neues Subnetz bereit und delegieren Sie das Subnetz an Azure NetApp Files.

Melden Sie sich für Microsoft Azure an

Wenn Sie kein Microsoft Azure Konto haben, melden Sie sich zunächst bei Microsoft Azure an.

Schritte

1. Wechseln Sie zum "Azure-Abonnementseite" Um den Azure Service zu abonnieren.
2. Wählen Sie einen Plan aus, und befolgen Sie die Anweisungen, um das Abonnement abzuschließen.

Für Azure NetApp Files anmelden

Erhalten Sie Zugriff auf Azure NetApp Files, indem Sie den NetApp Resource Provider registrieren.

Schritte

1. Melden Sie sich beim Azure Portal an.
2. "Registrieren Sie den NetApp Ressourcenanbieter mithilfe der Azure NetApp Files Dokumentation".

Erstellen Sie einen NetApp Account

Erstellen Sie einen NetApp Account in Azure NetApp Files.

Schritt

1. "Erstellen Sie mit der Azure NetApp Files Dokumentation ein NetApp Konto aus dem Azure Portal".

Richten Sie einen Kapazitäts-Pool ein

Ein oder mehrere Kapazitäts-Pools sind erforderlich, damit der Astra Control Service persistente Volumes in einem Kapazitäts-Pool bereitstellen kann. Astra Control Service erstellt keine Kapazitäts-Pools.

Berücksichtigen Sie bei der Einrichtung von Kapazitäts-Pools für Ihre Kubernetes-Applikationen folgende Punkte:

- Die Kapazitätspools müssen in derselben Region Azure erstellt werden, in der die AKS-Cluster mit Astra Control Service verwaltet werden.
- Ein Kapazitäts-Pool kann ein Ultra-, Premium- oder Standard-Service-Level haben. Jedes dieser Service-Level ist für unterschiedliche Performance-Anforderungen konzipiert. Astra Control Service unterstützt alle drei.

  Sie müssen für jedes Service-Level, das Sie mit Ihren Kubernetes Clustern verwenden möchten, einen Kapazitäts-Pool einrichten.

  "Erfahren Sie mehr über Service-Level für Azure NetApp Files".

- Bevor Sie einen Kapazitäts-Pool für die Applikationen erstellen, die Sie mit dem Astra Control Service schützen möchten, wählen Sie die erforderliche Performance und Kapazität für diese Anwendungen.

  Durch die Bereitstellung der richtigen Kapazität wird sichergestellt, dass Benutzer persistente Volumes nach Bedarf erstellen können. Wenn keine Kapazität verfügbar ist, können die persistenten Volumes nicht bereitgestellt werden.

- Ein Azure NetApp Files-Kapazitäts-Pool kann den manuellen oder automatischen QoS-Typ verwenden. Astra Control Service unterstützt automatische QoS-Kapazitäts-Pools. Manuelle QoS-Kapazitätspools werden nicht unterstützt.

Schritt

1. "Folgen Sie der Azure NetApp Files Dokumentation, um einen automatischen QoS-Kapazitätspool einzurichten".

Delegieren eines Subnetzes an Azure NetApp Files

Sie müssen ein Subnetz an Azure NetApp Files delegieren, damit der Astra Control Service persistente Volumes in diesem Subnetz erstellen kann. Beachten Sie, dass Sie mit Azure NetApp Files nur ein delegiertes Subnetz in einem vnet haben können.

Wenn Sie Peered VNets verwenden, müssen beide Seiten der Peering-Verbindung online sein: Die vnet, in der sich Ihre Kubernetes-Cluster befinden, und das vnet mit dem Azure NetApp Files delegierten Subnetz.

Schritt

1. "Folgen Sie der Azure NetApp Files-Dokumentation, um ein Subnetz an Azure NetApp Files zu delegieren".

Nachdem Sie fertig sind

Warten Sie ungefähr 10 Minuten, bevor Sie den im delegierten Subnetz ausgeführten Cluster ermitteln.

Erstellen Sie einen Azure Service Principal

Astra Control Service erfordert einen Azure-Service-Principal, dem die Rolle „Contributor“ zugewiesen wird. Astra Control Service nutzt diesen Service-Principal, um das Management von Kubernetes-Applikationsdaten in Ihrem Auftrag zu vereinfachen.

Ein Service-Principal ist eine Identität, die speziell für die Verwendung mit Anwendungen, Services und Tools erstellt wurde. Durch die Zuweisung einer Rolle zum Service-Principal wird der Zugriff auf bestimmte Azure-Ressourcen beschränkt.

Führen Sie die folgenden Schritte aus, um einen Service-Principal mithilfe der Azure CLI zu erstellen. Sie müssen die Ausgabe in einer JSON-Datei speichern und später den Astra Control Service bereitstellen. "Weitere Details zur Verwendung der CLI finden Sie in der Azure Dokumentation".

Bei den folgenden Schritten wird davon ausgegangen, dass Sie die Berechtigung zum Erstellen eines Service-Principal haben und dass das Microsoft Azure SDK (az-Befehl) auf Ihrem Computer installiert ist.

Anforderungen

- Der Service-Principal muss die regelmäßige Authentifizierung verwenden. Zertifikate werden nicht unterstützt.
- Dem Service Principal muss ein Zugriff auf Ihr Azure Abonnement für Mitarbeiter oder Eigentümer gewährt werden.
- Das Abonnement oder die Ressourcengruppe, die Sie für den Umfang auswählen, muss die AKS-Cluster und Ihr Azure NetApp Files-Konto enthalten.

Schritte

1. Geben Sie die Abonnement- und Mandanten-ID an, in der sich Ihre AKS-Cluster befinden (dies sind die Cluster, die Sie im Astra Control Service verwalten möchten).

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

2. Führen Sie einen der folgenden Schritte aus, je nachdem, ob Sie ein gesamtes Abonnement oder eine Ressourcengruppe verwenden:
   - Erstellen Sie den Service-Principal, weisen Sie die Rolle Contributor zu und geben Sie den Umfang dem gesamten Abonnement an, in dem sich die Cluster befinden.

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

   - Erstellen Sie den Service-Principal, weisen Sie die Contributor-Rolle zu und geben Sie die Ressourcengruppe an, in der sich die Cluster befinden.

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

3. Speichern Sie die resultierende Azure CLI-Ausgabe als JSON-Datei.

   Sie müssen diese Datei bereitstellen, damit Astra Control Service Ihre AKS-Cluster erkennen und Kubernetes-Datenmanagement-Vorgänge managen kann. "Erfahren Sie mehr über das Management von Anmeldeinformationen im Astra Control Service".

4. Optional: Fügen Sie die Abonnement-ID der JSON-Datei hinzu, damit der Astra Control Service beim Auswählen der Datei automatisch die ID füllt.

   Andernfalls müssen Sie die Abonnement-ID in Astra Control Service eingeben, wenn Sie dazu aufgefordert werden.

   Beispiel

   ```
   {
     "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. Optional: Testen Sie Ihren Service-Principal. Wählen Sie je nach Umfang, den Ihr Service Principal verwendet, die folgenden Beispielbefehle aus.

Abonnement-Umfang

```
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
```

Umfang der Ressourcengruppen

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

Optional: Redundanz für Azure Backup Buckets konfigurieren

Es besteht die Möglichkeit, eine robuenere Redundanzstufe für Azure Backup Buckets zu konfigurieren. Standardmäßig verwendet der Buckets Astra Control Service für das Speichern von Azure Kubernetes Service-Backups die LRS-Redundanzoption (lokal Redundant Storage). Um eine langlebige Redundanzoption für Azure Buckets zu verwenden, müssen Sie Folgendes tun:

Schritte

1. Erstellen Sie ein Azure-Storage-Konto, das die erforderliche Redundanzstufe verwendet "Diese Anweisungen".
2. Erstellen Sie einen Azure-Container auf dem neuen Storage-Konto mit "Diese Anweisungen".
3. Fügen Sie den Container als Eimer zum Astra Control Service hinzu. Siehe "Fügen Sie einen zusätzlichen Bucket hinzu".
4. (Optional) um den neu erstellten Bucket als Standard-Bucket für Azure Backups zu verwenden, setzen Sie ihn als Standard-Bucket für Azure fest. Siehe "Ändern des Standard-Bucket".

Richten Sie Microsoft Azure mit von Azure gemanagten Festplatten ein

Einige Schritte sind zur Vorbereitung Ihres Microsoft Azure Abonnements erforderlich, bevor Sie Azure Kubernetes Service-Cluster mit Astra Control Service managen können. Befolgen Sie diese Anweisungen, wenn Sie die von Azure verwalteten Laufwerke als Storage-Back-End verwenden möchten.

Schnellstart für die Einrichtung von Azure

Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

[Eins] Astra Control Service-Anforderungen für Azure Kubernetes Service prüfen

Vergewissern Sie sich, dass die Cluster ordnungsgemäß sind und eine unterstützte Version von Kubernetes ausführen, dass Node-Pools unter Linux verfügbar sind und unter anderem. Erfahren Sie mehr zu diesem Schritt.

[Zwei] Melden Sie sich für Microsoft Azure an

Erstellen Sie ein Microsoft Azure Konto. Erfahren Sie mehr zu diesem Schritt.

[Drittens] Erstellen Sie einen Azure Service Principal

Erstellen Sie einen Azure-Serviceprincipal mit der Rolle „Contributor“. Erfahren Sie mehr zu diesem Schritt.

[Vier] Konfigurieren Sie die Treiberdetails für die Container-Storage-Schnittstelle (CSI)

Sie müssen Ihr Azure-Abonnement und das Cluster konfigurieren, damit Sie mit den CSI-Treibern arbeiten können. Erfahren Sie mehr zu diesem Schritt.

[Fünf] Optional: Redundanz für Azure Backup Buckets konfigurieren

Standardmäßig verwendet der Buckets Astra Control Service für das Speichern von Azure Kubernetes Service-Backups die LRS-Redundanzoption (lokal Redundant Storage). Als optionaler Schritt können Sie einen langlebigen Grad an Redundanz für Azure Buckets konfigurieren. Erfahren Sie mehr zu diesem Schritt.

Anforderungen für den Azure Kubernetes Service-Cluster

Ein Kubernetes-Cluster muss folgende Anforderungen erfüllen, damit Sie ihn über den Astra Control Service erkennen und managen können.

Kubernetes-Version
: Auf Clustern muss die Kubernetes-Version 1.23 bis 1.25 ausgeführt werden.

Bildtyp
: Der Image-Typ für alle Node-Pools muss Linux sein.

Der Cluster-Status
: Cluster müssen in einem ordnungsgemäßen Zustand ausgeführt werden und mindestens einen Online-Worker-Node ohne „Worker“-Nodes im ausgefallenen Status aufweisen.

Azure Region
: Als Best Practice sollte eine Region gewählt werden, die Azure NetApp Files unterstützt, auch wenn Sie sie nicht als Storage-Backend verwenden. Dadurch ist es einfacher, Azure NetApp Files zukünftig als Storage-Backend zu verwenden, wenn sich Ihre Performance-Anforderungen ändern. "Hier finden Sie Azure Produkte nach Region".

CSI-Treiber
: Auf Clustern müssen die entsprechenden CSI-Treiber installiert sein.

Melden Sie sich für Microsoft Azure an

Wenn Sie kein Microsoft Azure Konto haben, melden Sie sich zunächst bei Microsoft Azure an.

Schritte

1. Wechseln Sie zum "Azure-Abonnementseite" Um den Azure Service zu abonnieren.
2. Wählen Sie einen Plan aus, und befolgen Sie die Anweisungen, um das Abonnement abzuschließen.

Erstellen Sie einen Azure Service Principal

Astra Control Service erfordert einen Azure-Service-Principal, dem die Rolle „Contributor“ zugewiesen wird. Astra Control Service nutzt diesen Service-Principal, um das Management von Kubernetes-Applikationsdaten in Ihrem Auftrag zu vereinfachen.

Ein Service-Principal ist eine Identität, die speziell für die Verwendung mit Anwendungen, Services und Tools erstellt wurde. Durch die Zuweisung einer Rolle zum Service-Principal wird der Zugriff auf bestimmte Azure-Ressourcen beschränkt.

Führen Sie die folgenden Schritte aus, um einen Service-Principal mithilfe der Azure CLI zu erstellen. Sie müssen die Ausgabe in einer JSON-Datei speichern und später den Astra Control Service bereitstellen. "Weitere Details zur Verwendung der CLI finden Sie in der Azure Dokumentation".

Bei den folgenden Schritten wird davon ausgegangen, dass Sie die Berechtigung zum Erstellen eines Service-Principal haben und dass das Microsoft Azure SDK (az-Befehl) auf Ihrem Computer installiert ist.

Anforderungen

- Der Service-Principal muss die regelmäßige Authentifizierung verwenden. Zertifikate werden nicht unterstützt.
- Dem Service Principal muss ein Zugriff auf Ihr Azure Abonnement für Mitarbeiter oder Eigentümer gewährt werden.
- Das Abonnement oder die Ressourcengruppe, die Sie für den Umfang auswählen, muss die AKS-Cluster und Ihr Azure NetApp Files-Konto enthalten.

Schritte

1. Geben Sie die Abonnement- und Mandanten-ID an, in der sich Ihre AKS-Cluster befinden (dies sind die Cluster, die Sie im Astra Control Service verwalten möchten).

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

2. Führen Sie einen der folgenden Schritte aus, je nachdem, ob Sie ein gesamtes Abonnement oder eine Ressourcengruppe verwenden:
   - Erstellen Sie den Service-Principal, weisen Sie die Rolle Contributor zu und geben Sie den Umfang dem gesamten Abonnement an, in dem sich die Cluster befinden.

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

   - Erstellen Sie den Service-Principal, weisen Sie die Contributor-Rolle zu und geben Sie die Ressourcengruppe an, in der sich die Cluster befinden.

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

3. Speichern Sie die resultierende Azure CLI-Ausgabe als JSON-Datei.

   Sie müssen diese Datei bereitstellen, damit Astra Control Service Ihre AKS-Cluster erkennen und Kubernetes-Datenmanagement-Vorgänge managen kann. "Erfahren Sie mehr über das Management von Anmeldeinformationen im Astra Control Service".

4. Optional: Fügen Sie die Abonnement-ID der JSON-Datei hinzu, damit der Astra Control Service beim Auswählen der Datei automatisch die ID füllt.

   Andernfalls müssen Sie die Abonnement-ID in Astra Control Service eingeben, wenn Sie dazu aufgefordert werden.

   Beispiel

```
{
  "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. Optional: Testen Sie Ihren Service-Principal. Wählen Sie je nach Umfang, den Ihr Service Principal verwendet, die folgenden Beispielbefehle aus.

   Abonnement-Umfang

```
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
```

   Umfang der Ressourcengruppen

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

Konfigurieren Sie die Treiberdetails für die Container-Storage-Schnittstelle (CSI)

Wenn Sie verwaltete Azure-Festplatten mit dem Astra Control Service verwenden möchten, müssen Sie die erforderlichen CSI-Treiber installieren.

Aktivieren Sie die CSI-Treiber-Funktion in Ihrem Azure-Abonnement

Bevor Sie die CSI-Treiber installieren, müssen Sie die CSI-Treiberfunktion in Ihrem Azure-Abonnement aktivieren.

Schritte

1. Öffnen Sie die Azure-Befehlszeilenschnittstelle.
2. Führen Sie den folgenden Befehl aus, um den Treiber zu registrieren:

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

3. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die Änderung propagiert wird:

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

Sie sollten eine Ausgabe wie die folgende sehen:

```
{
"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"
}
```

Installieren Sie die von Azure gemanagten CSI-Treiber in Ihrem Azure Kubernetes Service-Cluster

Sie können die Azure CSI Treiber installieren, um Ihre Vorbereitung abzuschließen.

Schritt

1. Gehen Sie zu "Die Microsoft CSI-Treiberdokumentation".
2. Befolgen Sie die Anweisungen zur Installation der erforderlichen CSI-Treiber.

Optional: Redundanz für Azure Backup Buckets konfigurieren

Es besteht die Möglichkeit, eine robuenere Redundanzstufe für Azure Backup Buckets zu konfigurieren.

Standardmäßig verwendet der Buckets Astra Control Service für das Speichern von Azure Kubernetes Service-Backups die LRS-Redundanzoption (lokal Redundant Storage). Um eine langlebige Redundanzoption für Azure Buckets zu verwenden, müssen Sie Folgendes tun:

Schritte

1. Erstellen Sie ein Azure-Storage-Konto, das die erforderliche Redundanzstufe verwendet "Diese Anweisungen".
2. Erstellen Sie einen Azure-Container auf dem neuen Storage-Konto mit "Diese Anweisungen".
3. Fügen Sie den Container als Eimer zum Astra Control Service hinzu. Siehe "Fügen Sie einen zusätzlichen Bucket hinzu".
4. (Optional) um den neu erstellten Bucket als Standard-Bucket für Azure Backups zu verwenden, setzen Sie ihn als Standard-Bucket für Azure fest. Siehe "Ändern des Standard-Bucket".