Los geht's

Astra Control Service

NetApp
March 07, 2023

Inhaltsverzeichnis

Los geht’s . . . 1
- Weitere Informationen zu Astra Control . . . 1
- Unterstützte Kubernetes-Implementierungen . . . 4
- Schnellstart für den Astra Control Service . . . 4
- Richten Sie Ihren Cloud-Provider ein . . . 5
- Registrieren Sie sich für ein Astra Control Service-Konto . . . 28
- Managen Sie Kubernetes Cluster über den Astra Control Service . . . 30
- Managen Sie private Cluster über den Astra Control Service . . . 42
- Was kommt als Nächstes? . . . 43
- Videos des Astra Control Service . . . 44
- Häufig gestellte Fragen zum Astra Control Service . . . 46

Los geht’s

Weitere Informationen zu Astra Control

Astra Control ist eine Kubernetes-Lösung für das Lifecycle-Management von Applikationsdaten, die den Betrieb zustandsorientierte Applikationen vereinfacht. Schutz, Backup und Migration von Kubernetes-Workloads und sofortige Erstellung von Applikationsklonen

Funktionen

Astra Control bietet entscheidende Funktionen für das Lifecycle Management von Kubernetes-Applikationsdaten:

- Automatisches Management von persistentem Storage
- Erstellen Sie applikationsorientierte Snapshots und Backups nach Bedarf
- Automatisierung von richtlinienbasierten Snapshot- und Backup-Vorgängen
- Migrieren Sie Applikationen und Daten von einem Kubernetes-Cluster zu einem anderen
- Klonen einer Applikation vom Staging zur Produktion
- Darstellung des Anwendungszustands und des Schutzstatus
- Verwenden Sie eine Web-Oberfläche oder eine API zur Implementierung Ihrer Backup- und Migration-Workflows

Implementierungsmodelle

Astra Control ist in zwei Implementierungsmodellen erhältlich:

- **Astra Control Service**: Ein von NetApp gemanagter Service, der applikationskonsistentes Datenmanagement von Kubernetes Clustern in Umgebungen mehrerer Cloud-Provider sowie selbst gemanagte Kubernetes Cluster bietet.
- **Astra Control Center**: Gemanagte Software für applikationsgerechtes Datenmanagement von Kubernetes-Clustern, die in Ihrer On-Premises-Umgebung ausgeführt werden. Astra Control Center kann auch auf mehreren Cloud-Provider-Umgebungen mit einem NetApp Cloud Volumes ONTAP Storage-Backend installiert werden.

	Astra Control Service	**Astra Control Center**
Wie wird das angeboten?	Vollständig gemanagter Cloud-Service von NetApp	Als Software, die Sie herunterladen, installieren und verwalten können
Wo wird sie gehostet?	In einer Public Cloud von NetApp ihrer Wahl	In Ihrem eigenen Kubernetes-Cluster
Wie wird sie aktualisiert?	Gemanagt von NetApp	Sie verwalten jegliche Updates

	Astra Control Service	Astra Control Center
Welche Storage-Back-Ends werden unterstützt?	• Amazon Web Services: ◦ Amazon EBS ◦ Amazon FSX für NetApp ONTAP ◦ "Cloud Volumes ONTAP" • Google Cloud: ◦ Google Persistent Disk ◦ NetApp Cloud Volumes Service ◦ "Cloud Volumes ONTAP" • Microsoft Azure: ◦ Über Azure Gemanagte Festplatten ◦ Azure NetApp Dateien ◦ "Cloud Volumes ONTAP" • Self-Managed Cluster: ◦ Amazon EBS ◦ Google Persistent Disk ◦ Über Azure Gemanagte Festplatten ◦ "Cloud Volumes ONTAP"	• NetApp ONTAP AFF und FAS Systeme • "Cloud Volumes ONTAP"

Funktionsweise des Astra Control Service

Astra Control Service ist ein von NetApp gemanagter Cloud-Service, der ständig verfügbar und mit den neuesten Funktionen aktualisiert ist. Verschiedene Komponenten unterstützen das Lifecycle-Management von Applikationsdaten.

Astra Control Service funktioniert auf hohem Niveau wie folgt:

- Starten Sie mit Astra Control Service, indem Sie Ihren Cloud-Provider einrichten und einen Astra Account anfordern.

+ ** für GKE Cluster, Astra Control Service verwendet "NetApp Cloud Volumes Service für Google Cloud" Oder Google Persistent Disks als Storage-Backend für Ihre persistenten Volumes.

+ ** für AKS-Cluster, Astra Control Service verwendet "Azure NetApp Dateien" Oder von Azure gemanagte Festplatten als Storage-Backend für Ihre persistenten Volumes.

+ ** für Amazon EKS Cluster, Astra Control Service verwendet "Amazon Elastic Block Store" Oder "Amazon FSX für NetApp ONTAP" Das Storage-Backend für Ihre persistenten Volumes

- Sie fügen Ihre ersten Kubernetes-Computing-Ressourcen in den Astra Control Service ein. Astra Control Service übernimmt dann Folgendes:
  - Erstellung eines Objektspeicher in Ihrem Cloud-Provider-Konto, an dem Backup-Kopien gespeichert werden

+ in Azure erstellt Astra Control Service außerdem eine Ressourcengruppe, ein Storage-Konto und Schlüssel für den Blob-Container.

- Erstellt eine neue Administratorrolle und ein Kubernetes-Servicekonto auf dem Cluster.
- Verwendet diese neue Administratorrolle für die Installation "Astra Trident" Auf dem Cluster und um eine oder mehrere Storage-Klassen zu erstellen.
- Wenn Sie ein Cloud-Service-Storage-Angebot von NetApp als Storage-Back-End verwenden, verwendet der Astra Control Service Astra Trident zur Bereitstellung persistenter Volumes für Ihre Applikationen. Wenn Sie von Amazon EBS oder Azure gemanagte Festplatten als Storage-Backend verwenden, müssen Sie einen Provider-spezifischen CSI-Treiber installieren. Installationsanweisungen finden Sie in "Einrichten von Amazon Web Services" Und "Richten Sie Microsoft Azure mit von Azure gemanagten Festplatten ein".
    - An diesem Punkt können Sie Apps aus Ihrem Cluster definieren. Persistente Volumes werden auf dem Storage-Back-End über die neue Standard-Storage-Klasse bereitgestellt.
    - Anschließend verwalten Sie diese Applikationen mithilfe des Astra Control Service und erstellen Snapshots, Backups und Klone.

Mit dem kostenlosen Plan von Astra Control können Sie bis zu 10 Namespaces in Ihrem Konto verwalten. Wenn Sie mehr als 10 Namespaces verwalten möchten, müssen Sie die Abrechnung durch ein Upgrade vom kostenlosen Plan auf den Premium-Plan einrichten.

So funktioniert Astra Control Center

Astra Control Center wird lokal in Ihrer eigenen Private Cloud ausgeführt.

Astra Control Center unterstützt Kubernetes-Cluster mit Trident-basiertem Storage mit einem Storage-Backend mit ONTAP 9.5 und höher.

In einer Cloud-vernetzten Umgebung nutzt Astra Control Center erweiterte Monitoring- und Telemetriedaten mithilfe von Cloud Insights. Liegt keine Cloud Insights-Verbindung vor, ist das Monitoring und die Telemetrie nur begrenzt (7 Tage Metriken) im Astra Control Center verfügbar und wird auch über offene Endpunkt in native Kubernetes-Monitoring-Tools (wie Prometheus und Grafana) exportiert.

Astra Control Center ist vollständig in das AutoSupport und Active IQ Ecosystem integriert, damit Benutzer und NetApp Support Fehlerbehebungs- und Verwendungsinformationen liefern können.

Sie können Astra Control Center mit einer 90-Tage-Evaluierungslizenz ausprobieren. Die Evaluierungsversion wird durch E-Mail- und Community-Optionen unterstützt. Zudem haben Sie über das Dashboard für den Produktsupport Zugriff auf Knowledgebase-Artikel und -Dokumentation.

Um Astra Control Center zu installieren und zu verwenden, müssen Sie sicher sein "Anforderungen".

Astra Control Center funktioniert auf hohem Niveau wie folgt:

- Sie installieren Astra Control Center in Ihrer lokalen Umgebung. Erfahren Sie mehr darüber, wie Sie "Installieren Sie Astra Control Center".
- Sie führen einige Setup-Aufgaben wie die folgenden aus:
    - Lizenzierung einrichten.
    - Fügen Sie den ersten Cluster hinzu.
    - Fügen Sie ein Storage-Back-End hinzu, das beim Hinzufügen des Clusters erkannt wird.
    - Fügen Sie einen Objektspeicher-Bucket hinzu, der Ihre Applikations-Backups speichert.

Erfahren Sie mehr darüber, wie Sie "Einrichten des Astra Control Center".

Sie können Applikationen zu Ihrem Cluster hinzufügen. Wenn auch einige Applikationen bereits im Cluster gemanagt werden, können Sie sie mit Astra Control Center managen. Nutzen Sie dann das Astra Control Center, um Snapshots, Backups, Klone und Replizierungsbeziehungen zu erstellen.

Finden Sie weitere Informationen

- "Dokumentation für die NetApp Astra Produktfamilie"
- "Dokumentation des Astra Control Service"
- "Astra Control Center-Dokumentation"
- "Astra Trident-Dokumentation"
- "Verwenden Sie die Astra Control API"
- "Cloud Insights-Dokumentation"
- "ONTAP-Dokumentation"

Unterstützte Kubernetes-Implementierungen

Astra Control Service managt Applikationen, die auf einem gemanagten Kubernetes-Cluster in Amazon Elastic Kubernetes Service (EKS) ausgeführt werden, sowie Cluster, die Sie selbst managen.

Astra Control Service kann sowohl auf einem gemanagten Kubernetes-Cluster in der Google Kubernetes Engine (GKE) als auch auf Clustern, die Sie selbst managen, ausgeführte Applikationen managen.

Astra Control Service kann Apps managen, die auf einem gemanagten Kubernetes-Cluster in Azure Kubernetes Service (AKS) ausgeführt werden, sowie Cluster, die Sie selbst managen.

- "Erfahren Sie, wie Sie Amazon Web Services für Astra Control Service einrichten".
- "Erfahren Sie, wie Sie Google Cloud für Astra Control Service einrichten".
- "Erfahren Sie, wie Sie Microsoft Azure mit Azure NetApp Files für Astra Control Service einrichten".
- "Erfahren Sie, wie Sie Microsoft Azure mit gemanagten Azure Festplatten für den Astra Control Service einrichten".
- "Bereiten Sie selbst gemanagte Cluster vor, bevor Sie sie in den Astra Control Service hinzufügen".

Schnellstart für den Astra Control Service

Diese Seite bietet einen grundlegenden Überblick über die Schritte, die Sie für den Einstieg in den Astra Control Service benötigen. Die Links in den einzelnen Schritten führen zu einer Seite, die weitere Details enthält.

[Eins] Richten Sie Ihren Cloud-Provider ein

1. Google Cloud:
    - Google Kubernetes Engine-Cluster-Anforderungen prüfen.
    - Kaufen Sie Cloud Volumes Service für Google Cloud über den Google Cloud Marketplace.

- Aktivieren Sie die erforderlichen APIs.
- Erstellen eines Servicekontos und eines Servicekontenschlüssels.
- Netzwerk-Peering von Ihrem VPC zu Cloud Volumes Service für Google Cloud einrichten.

  "Erfahren Sie mehr über die Google Cloud Anforderungen".

2. Amazon Web Services:
   - Amazon Web Services-Cluster-Anforderungen prüfen.
   - Erstellen Sie ein Amazon-Konto.
   - Installieren Sie die Amazon Web Services-CLI.
   - Erstellen Sie einen IAM-Benutzer.
   - Erstellen Sie eine Berechtigungsrichtlinie und fügen Sie sie an.
   - Speichern Sie die Anmeldeinformationen für den IAM-Benutzer.

     "Erfahren Sie mehr über die Anforderungen von Amazon Web Services".
3. Microsoft Azure:
   - Azure Kubernetes Service-Cluster-Anforderungen für das Storage-Back-End prüfen, das Sie verwenden möchten.

     "Erfahren Sie mehr über Microsoft Azure und Azure NetApp Files Anforderungen".

   "Erfahren Sie mehr über die von Microsoft Azure und Azure gemanagten Festplattenanforderungen".

Wenn Sie ein eigenes Cluster managen und nicht von einem Cloud-Provider gehostet werden, prüfen Sie die Anforderungen für Self-Managed Cluster."Erfahren Sie mehr über Self-Managed-Cluster-Anforderungen".

[Zwei] Schließen Sie die Registrierung für den Astra Control ab

1. Erstellen Sie ein "NetApp Cloud Central" Konto.
2. Geben Sie Ihre NetApp Cloud Central E-Mail-ID an, wenn Sie Ihr Astra Control Konto erstellen "Von der Astra-Produktseite".

"Erfahren Sie mehr über den Registrierungsprozess".

[Drittens] Fügen Sie Cluster zum Astra Control hinzu

Nachdem Sie sich angemeldet haben, wählen Sie **Cluster hinzufügen**, um das Cluster mit Astra Control zu verwalten.

"Erfahren Sie mehr über das Hinzufügen von Clustern".

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".

Registrieren Sie sich für ein Astra Control Service-Konto

Zur Nutzung von Astra Control Service benötigen Sie ein Astra Control Service-Konto, das mit Ihrem NetApp Cloud Central Konto verknüpft ist. Füllen Sie den Astra Control Service-Registrierungsprozess aus und wenn Sie noch nicht über ein Cloud Central-Konto verfügen, melden Sie sich bei Cloud Central an, um auf den Astra Control Service zuzugreifen.

Registrieren Sie sich für ein Astra Control Konto

Bevor Sie sich beim Astra Control Service anmelden können, müssen Sie einen Registrierungsvorgang abschließen, um ein Astra Control Service-Konto zu erhalten.

Wenn Sie den Astra Control Service nutzen, verwalten Sie Ihre Apps über ein Konto. Ein Konto umfasst Benutzer, die die Apps im Konto anzeigen und verwalten können, sowie Ihre Rechnungsdaten.

Schritte

1. "Wechseln Sie zur Astra Control-Seite auf Cloud Central".
2. Wählen Sie **erste Schritte mit Astra Control** aus.
3. Wählen Sie die Registerkarte **FREIER PLAN**.

4. Geben Sie die erforderlichen Informationen in das Formular ein.

   Beim Ausfüllen des Formulars sind einige wichtige Punkte zu beachten:

   - Ihr Unternehmensname und Ihre Adresse müssen korrekt sein, da wir sie überprüfen, um die Anforderungen der Global Trade Compliance zu erfüllen.
   - Der **Astra-Kundenname** ist der Name Ihres Astra Control Service-Kontos. Diesen Namen sehen Sie in der Benutzeroberfläche des Astra Control Service. Beachten Sie, dass Sie bei Bedarf weitere Konten (bis zu 5) erstellen können.
   - Wenn Sie über ein NetApp Cloud Central Konto verfügen, geben Sie im Feld **Business E-Mail-Adresse** die E-Mail ein, die Sie für dieses Konto verwenden. Wenn Sie noch kein NetApp Cloud Central Konto haben, verwenden Sie die hier eingegebene E-Mail-Adresse, wenn Sie sich bei Cloud Central anmelden.

5. Wählen Sie **Senden**.

Melden Sie sich bei Cloud Central an

Wenn Sie noch keinen NetApp Cloud Central Account haben, melden Sie sich bei Cloud Central an. So können Sie auf den Astra Control Service und die anderen Cloud Services von NetApp zugreifen. Astra Control Service ist in den Authentifizierungsservice von NetApp Cloud Central integriert. Wenn Sie bereits über ein Cloud Central Konto verfügen und die Registrierung abgeschlossen haben, können Sie auf zugreifen "Astra Control Service" Cloud Central – die Zugangsdaten, die Sie selbst nutzen können

Sie können Single Sign-On verwenden, um sich mit den Zugangsdaten aus Ihrem Unternehmensverzeichnis (föderierte Identität) bei Cloud Central anzumelden. Weitere Informationen erhalten Sie im "Cloud Central Help Center" Und wählen Sie dann **Cloud Central Anmelde-Optionen**.

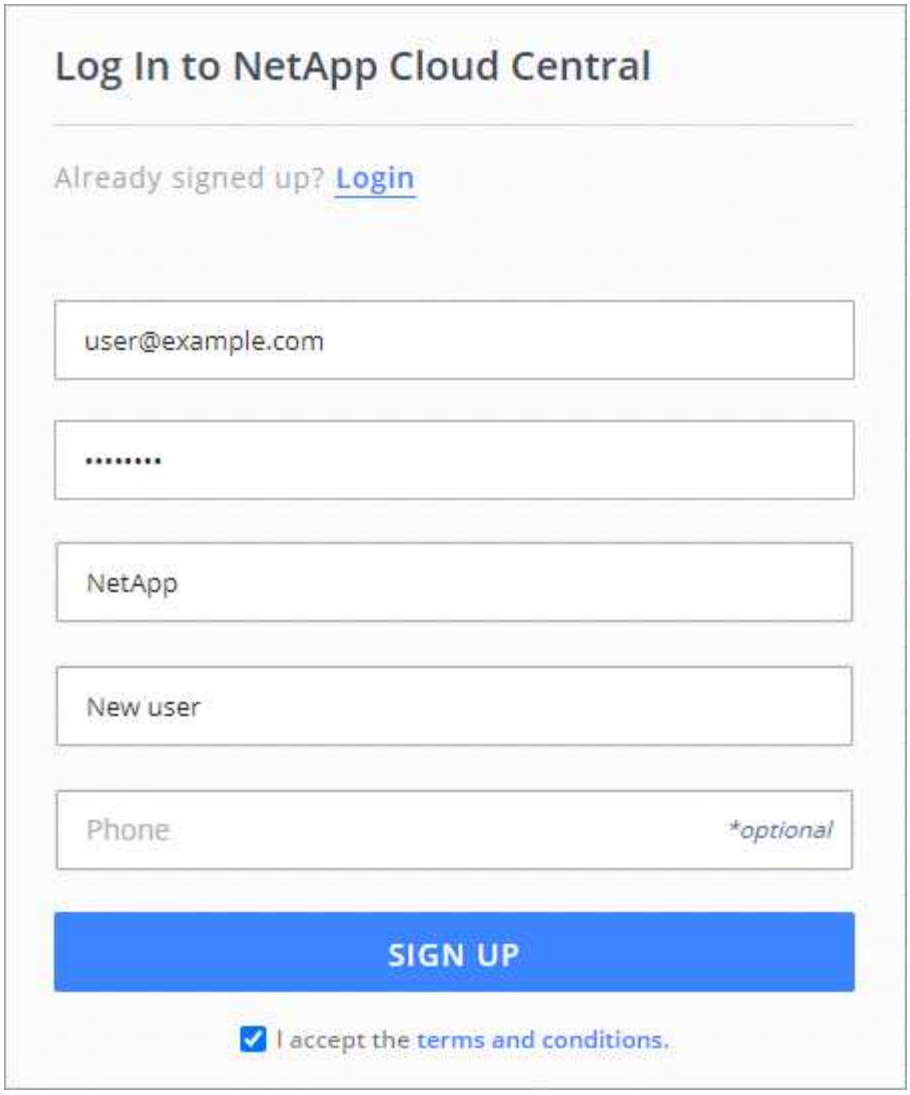
Schritte

1. Gehen Sie zu "NetApp Cloud Central".
2. Wählen Sie oben rechts die Option **Registrieren**.
3. Füllen Sie das Formular aus.

   Stellen Sie sicher, dass die hier eingegebene Telefonnummer und die E-Mail-Adresse identisch sind, die Sie im vorhergehenden Registrierungsformular für den kostenlosen Plan verwendet haben.

4. Wählen Sie **Registrieren**.

Die in dieses Formular eingegebene E-Mail-Adresse ist für Ihre NetApp Cloud Central Benutzer-ID. Verwenden Sie diese Cloud Central-Benutzer-ID, wenn Sie sich für ein neues Astra Control Service-Konto anmelden oder wenn ein Astra Control Service-Administrator Sie zu einem bestehenden Astra Control Service-Konto einlädt.



5. Warten Sie auf eine E-Mail von NetApp Cloud Central. Die E-Mail-Adresse stammt von saas.support@netapp.com und kann einige Minuten dauern. Überprüfen Sie Ihren Spam-Ordner.
6. Wenn die E-Mail eintrifft, wählen Sie den Link in der E-Mail aus, um Ihre E-Mail-Adresse zu überprüfen.

Ergebnis

Sie haben jetzt eine aktive Cloud Central-Benutzeranmeldung.

Nachdem Sie sich jetzt registriert haben, können Sie den Astra Control Service direkt mit Ihren Cloud Central Anmeldedaten über aufrufen https://astra.netapp.io.

Managen Sie Kubernetes Cluster über den Astra Control Service

Nach der Einrichtung der Umgebung erstellen Sie sofort einen Kubernetes Cluster und fügen ihn dann dem Astra Control Service hinzu.

- Erstellen eines Kubernetes-Clusters
- Verwalten Sie Kubernetes-Cluster

- Ändern der Standard-Storage-Klasse

Erstellen eines Kubernetes-Clusters

Wenn Sie noch keinen Cluster haben, können Sie ein Cluster erstellen, das erfüllt "Astra Control Service-Anforderungen für Amazon Elastic Kubernetes Service (EKS)". Wenn Sie noch keinen Cluster haben, können Sie ein Cluster erstellen, das erfüllt "Astra Control Service-Anforderungen für Google Kubernetes Engine (GKE)". Wenn Sie noch keinen Cluster haben, können Sie ein Cluster erstellen, das erfüllt "Astra Control Service-Anforderungen für Azure Kubernetes Service (AKS) mit Azure NetApp Files" Oder "Astra Control Service-Anforderungen für Azure Kubernetes Service (AKS) mit von Azure gemanagten Festplatten".

Astra Control Service unterstützt AKS-Cluster, die Azure Active Directory (Azure AD) zur Authentifizierung und Identitätsverwaltung nutzen. Wenn Sie das Cluster erstellen, befolgen Sie die Anweisungen im "Offizielle Dokumentation" Um den Cluster mit Azure AD zu konfigurieren. Stellen Sie sicher, dass Ihre Cluster die Anforderungen für die AKS-verwaltete Azure AD-Integration erfüllen.

Selbstverwaltete Cluster

Ein selbstverwalteter Cluster ist ein Cluster, den Sie direkt bereitstellen und managen können. Astra Control Service unterstützt selbst gemanagte Cluster, die in einer Public-Cloud-Umgebung ausgeführt werden. Sie können einen selbstverwalteten Cluster zum Astra Control Service hinzufügen, indem Sie ein hochladen `kubeconfig.yaml` Datei: Sie müssen sicherstellen, dass der Cluster die in aufgeführten Anforderungen erfüllt Verwalten Sie Kubernetes-Cluster.

Verwalten Sie Kubernetes-Cluster

Nachdem Sie sich beim Astra Control Service angemeldet haben, beginnen Sie zunächst mit dem Verwalten Ihrer Cluster. Sie können ein von einem Cloud-Provider gemanagtes Cluster oder einen Self-Managed Cluster hinzufügen. Bevor Sie Astra Control Service ein Cluster hinzufügen, müssen Sie bestimmte Aufgaben ausführen und sicherstellen, dass das Cluster bestimmte Anforderungen erfüllt.

Was Sie'll benötigen Cluster, die von einem Cloud-Provider verwaltet werden

Amazon Web Services

- Sie sollten die JSON-Datei mit den Anmeldedaten des IAM-Benutzers haben, der das Cluster erstellt hat. "Erfahren Sie, wie ein IAM-Benutzer erstellt wird".
- Astra Trident ist für Amazon FSX für NetApp ONTAP erforderlich. Wenn Sie Amazon FSX für NetApp ONTAP als Storage-Backend für Ihren EKS-Cluster verwenden möchten, finden Sie die Informationen zu Astra Trident im "EKS-Clusteranforderungen".
- (Optional) Wenn Sie angeben müssen `kubectl` Befehlszugriff für ein Cluster auf andere IAM-Benutzer, die nicht der Ersteller des Clusters sind, finden Sie in den Anweisungen unter "Wie erhalte ich Zugriff auf andere IAM-Benutzer und Rollen nach der Cluster-Erstellung in Amazon EKS?".
- Wenn Sie NetApp Cloud Volumes ONTAP als Storage-Backend verwenden möchten, müssen Sie Cloud Volumes ONTAP für die Nutzung mit Amazon Web Services konfigurieren. Weitere Informationen finden Sie im Cloud Volumes ONTAP "Setup-Dokumentation".

Microsoft Azure

- Sie sollten beim Erstellen des Service-Principal die JSON-Datei haben, die die Ausgabe aus der Azure CLI enthält. "Erfahren Sie, wie Sie einen Service-Principal einrichten".

  Außerdem benötigen Sie Ihre Azure Abonnement-ID, wenn Sie sie nicht zur JSON-Datei hinzugefügt haben.

- Informationen zu privaten AKS-Clustern finden Sie unter "Managen Sie private Cluster über den Astra Control Service".
- Wenn Sie NetApp Cloud Volumes ONTAP als Storage-Backend verwenden möchten, müssen Sie Cloud Volumes ONTAP für die Zusammenarbeit mit Microsoft Azure konfigurieren. Weitere Informationen finden Sie im Cloud Volumes ONTAP "Setup-Dokumentation".

Google Cloud

- Sie sollten die Servicekontoschlüsseldatei für ein Servicekonto haben, das über die erforderlichen Berechtigungen verfügt. "Erfahren Sie, wie Sie ein Service-Konto einrichten".
- Wenn Sie NetApp Cloud Volumes ONTAP als Storage-Backend verwenden möchten, müssen Sie Cloud Volumes ONTAP für die Zusammenarbeit mit Google Cloud konfigurieren. Weitere Informationen finden Sie im Cloud Volumes ONTAP "Setup-Dokumentation".

Was Sie'll benötigen für selbstverwaltete Cluster

Ein selbstverwalteter Cluster ist ein Cluster, den Sie direkt bereitstellen und managen können. Astra Control Service unterstützt selbst gemanagte Cluster, die in einer Public-Cloud-Umgebung ausgeführt werden. Selbstverwaltete Cluster können über Astra Trident eine Schnittstelle zu NetApp Storage-Services aufbauen oder über CSI-Treiber (Container Storage Interface) eine Schnittstelle zu Amazon Elastic Block Store (EBS), Azure Managed Disks und Google Persistent Disk aufbauen.

Astra Control Service unterstützt selbst gemanagte Cluster, die die folgenden Kubernetes-Distributionen verwenden:

- Red hat OpenShift Container Platform
- Rancher Kubernetes Engine
- Vorgelagerte Kubernetes-Systeme

Ihr Self-Managed-Cluster muss folgende Anforderungen erfüllen:

- Der Cluster muss über das Internet zugänglich sein.
- Der Cluster kann nicht in Ihrem On-Premises-Netzwerk gehostet werden, sondern muss in einer Public-Cloud-Umgebung gehostet werden.
- Wenn Sie Speicher mit CSI-Treibern verwenden oder planen, diese zu verwenden, müssen auf dem Cluster die entsprechenden CSI-Treiber installiert sein. Weitere Informationen zur Verwendung von CSI-Treibern zur Integration von Speicher finden Sie in der Dokumentation Ihres Speicherservices.
- Wenn Sie NetApp Storage nutzen oder nutzen möchten, stellen Sie sicher, dass Sie die neueste Version von Astra Trident installiert haben:

  > ⓘ Das können Sie "Implementieren Sie Astra Trident" Mit dem Trident-Operator (manuell oder mit Hilfe des Helm-Diagramms) oder `tridentctl`. Vor der Installation oder dem Upgrade von Astra Trident sollten Sie sich die "Unterstützte Frontends, Back-Ends und Host-Konfigurationen".

  - **Trident Storage Back-End konfiguriert**: Mindestens ein Astra Trident Storage-Back-End muss sein "Konfiguriert" Auf dem Cluster.
  - **Trident Storage-Klassen konfiguriert**: Mindestens ein Astra Trident Storage-Klasse muss sein "Konfiguriert" Auf dem Cluster. Wenn eine Standard-Storage-Klasse konfiguriert ist, stellen Sie sicher, dass nur eine Storage-Klasse diese Annotation aufweist.
  - **Astra Trident Volume Snapshot Controller und Volume Snapshot Klasse installiert und konfiguriert**: Der Volume Snapshot Controller muss sein "Installiert" Damit Snapshots in Astra Control erstellt werden können. Mindestens ein Astra Trident `VolumeSnapshotClass` Gewesen "Einrichtung" Durch einen Administrator.
- **Kubeconfig**: Sie haben Zugang zum Cluster kubeconfig Das umfasst nur ein Kontextseil.
- **Rancher only**: Ändern Sie beim Verwalten von Anwendungsclustern in einer Rancher-Umgebung den Standardkontext des Anwendungsclusters in der von Rancher bereitgestellten kubeconfig-Datei, um einen Steuerebenen-Kontext anstelle des Rancher API-Serverkontexts zu verwenden. So wird die Last auf dem Rancher API Server reduziert und die Performance verbessert.

(Optional) Überprüfen Sie die Astra Trident-Version

Wenn Ihr Cluster Astra Trident für Storage-Services verwendet, stellen Sie sicher, dass die aktuellste installierte Version von Astra Trident ist.

Schritte

1. Testen Sie die Version von Astra Trident.

```
kubectl get tridentversions -n trident
```

Wenn Astra Trident installiert ist, wird die Ausgabe wie folgt ausgegeben:

```
NAME      VERSION
trident   22.10.0
```

Wenn Astra Trident nicht installiert ist, wird die Ausgabe wie folgt angezeigt:

```
error: the server doesn't have a resource type "tridentversions"
```

> Wenn Astra Trident nicht oder nicht aktuell installiert ist und der Cluster Astra Trident für Storage-Services verwenden soll, müssen Sie vor dem Fortfahren die neueste Version von Astra Trident installieren. Siehe "Astra Trident-Dokumentation" Weitere Anweisungen.

2. Stellen Sie sicher, dass die Pods ausgeführt werden:

```
kubectl get pods -n trident
```

3. Prüfen Sie, ob die Storage-Klassen die unterstützten Astra Trident Treiber verwenden. Der bereitstellungsname sollte lauten `csi.trident.netapp.io`. Im folgenden Beispiel finden Sie weitere Informationen:

```
kubectl get sc
```

Beispielantwort:

```
NAME                    PROVISIONER                    RECLAIMPOLICY
VOLUMEBINDINGMODE   ALLOWVOLUMEEXPANSION   AGE
ontap-gold (default)   csi.trident.netapp.io          Delete
Immediate           true                   5d23h
```

Admin-Rolle kubeconfig erstellen (gilt für Cluster, die Rancher, OpenShift und Upstream Kubernetes ausführen)

Stellen Sie sicher, dass Sie die folgenden Schritte auf Ihrem Gerät ausführen:

- Kubectl v1.19 oder höher installiert

- Ein aktiver kubeconfig mit Clusteradministratorrechten für den aktiven Kontext

Schritte

1. Erstellen Sie ein Service-Konto wie folgt:

   a. Erstellen Sie eine Dienstkontendatei mit dem Namen `astracontrol-service-account.yaml`.

   Passen Sie Namen und Namespace nach Bedarf an. Wenn hier Änderungen vorgenommen werden, sollten Sie die gleichen Änderungen in den folgenden Schritten anwenden.

```
<strong>astracontrol-service-account.yaml</strong>
```

+

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: astracontrol-service-account
  namespace: default
```

   a. Wenden Sie das Servicekonto an:

```
kubectl apply -f astracontrol-service-account.yaml
```

2. Gewähren Sie Cluster-Admin-Berechtigungen wie folgt:

   a. Erstellen Sie ein `ClusterRoleBinding` Datei aufgerufen `astracontrol-clusterrolebinding.yaml`.

   Passen Sie bei Bedarf alle beim Erstellen des Dienstkontos geänderten Namen und Namespaces an.

```
<strong>astracontrol-clusterrolebinding.yaml</strong>
```

+

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astracontrol-admin
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- kind: ServiceAccount
  name: astracontrol-service-account
  namespace: default
```

a. Wenden Sie die Bindung der Cluster-Rolle an:

```
kubectl apply -f astracontrol-clusterrolebinding.yaml
```

3. Listen Sie die Geheimnisse des Dienstkontos auf, ersetzen Sie `<context>` Mit dem richtigen Kontext für Ihre Installation:

```
kubectl get serviceaccount astracontrol-service-account --context
<context> --namespace default -o json
```

Das Ende der Ausgabe sollte wie folgt aussehen:

```
"secrets": [
{ "name": "astracontrol-service-account-dockercfg-vhz87"},
{ "name": "astracontrol-service-account-token-r59kr"}
]
```

Die Indizes für jedes Element im `secrets` Array beginnt mit 0. Im obigen Beispiel der Index für `astracontrol-service-account-dockercfg-vhz87` Wäre 0 und der Index für `astracontrol-service-account-token-r59kr` Sind es 1. Notieren Sie in Ihrer Ausgabe den Index für den Namen des Dienstkontos, der das Wort „Token“ darin enthält.

4. Erzeugen Sie den kubeconfig wie folgt:

a. Erstellen Sie ein `create-kubeconfig.sh` Datei: Austausch `TOKEN_INDEX` Am Anfang des folgenden Skripts mit dem korrekten Wert.

```
<strong>create-kubeconfig.sh</strong>
```

```

```

```
# Update these to match your environment.
# Replace TOKEN_INDEX with the correct value
# from the output in the previous step. If you
# didn't change anything else above, don't change
# anything else here.

SERVICE_ACCOUNT_NAME=astracontrol-service-account
NAMESPACE=default
NEW_CONTEXT=astracontrol
KUBECONFIG_FILE='kubeconfig-sa'

CONTEXT=$(kubectl config current-context)

SECRET_NAME=$(kubectl get serviceaccount ${SERVICE_ACCOUNT_NAME}
\
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.secrets[TOKEN_INDEX].name}')
TOKEN_DATA=$(kubectl get secret ${SECRET_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.data.token}')

TOKEN=$(echo ${TOKEN_DATA} | base64 -d)

# Create dedicated kubeconfig
# Create a full copy
kubectl config view --raw > ${KUBECONFIG_FILE}.full.tmp

# Switch working context to correct context
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp config use-
context ${CONTEXT}

# Minify
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp \
  config view --flatten --minify > ${KUBECONFIG_FILE}.tmp

# Rename context
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  rename-context ${CONTEXT} ${NEW_CONTEXT}

# Create token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-credentials ${CONTEXT}-${NAMESPACE}-token-user \
  --token ${TOKEN}

# Set context to use token user
```

```
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token
-user

# Set context to correct namespace
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --namespace ${NAMESPACE}

# Flatten/minify kubeconfig
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  view --flatten --minify > ${KUBECONFIG_FILE}

# Remove tmp
rm ${KUBECONFIG_FILE}.full.tmp
rm ${KUBECONFIG_FILE}.tmp
```

b. Geben Sie die Befehle an, um sie auf Ihren Kubernetes-Cluster anzuwenden.

```
source create-kubeconfig.sh
```

5. (Optional) Umbenennen Sie die kubeconfig auf einen aussagekräftigen Namen für Ihr Cluster. Schützen Sie die Cluster-Anmeldedaten.

```
chmod 700 create-kubeconfig.sh
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

Schritte

1. Wählen Sie im Dashboard **Kubernetes Cluster managen** aus.

   Befolgen Sie die Aufforderungen zum Hinzufügen des Clusters.

2. **Provider**: Wählen Sie Ihren Cloud-Provider aus und geben Sie dann entweder die erforderlichen Anmeldedaten für die Erstellung einer neuen Cloud-Instanz an, oder wählen Sie eine vorhandene Cloud-Instanz aus.
3. **Amazon Web Services**: Geben Sie Details über Ihr Amazon Web Services IAM-Benutzerkonto an, indem Sie eine JSON-Datei hochladen oder den Inhalt dieser JSON-Datei aus Ihrer Zwischenablage einfügen.

   Die JSON-Datei sollte die Anmeldeinformationen des IAM-Benutzers enthalten, der das Cluster erstellt hat.

4. **Microsoft Azure**: Geben Sie Details zu Ihrem Azure Service Principal an, indem Sie eine JSON-Datei hochladen oder den Inhalt dieser JSON-Datei aus Ihrer Zwischenablage einfügen.

   Die JSON-Datei sollte beim Erstellen des Service-Principal die Ausgabe aus der Azure CLI enthalten. Sie können auch Ihre Abonnement-ID angeben, damit sie automatisch in den Astra aufgenommen wird. Andernfalls müssen Sie die ID manuell eingeben, nachdem Sie den JSON bereitgestellt haben.

5. **Google Cloud Platform**: Stellen Sie die Service-Konto-Schlüsseldatei entweder durch das Hochladen der Datei oder durch Einfügen der Inhalte aus Ihrer Zwischenablage bereit.

   Astra Control Service nutzt das Service-Konto, um Cluster zu erkennen, die in der Google Kubernetes Engine ausgeführt werden.

6. **Other**: Geben Sie Details über Ihren selbstverwalteten Cluster durch das Hochladen eines `kubeconfig.yaml` Datei oder durch Einfügen des Inhalts des `kubeconfig.yaml` Datei aus der Zwischenablage.

   Wenn Sie Ihre eigenen erstellen `kubeconfig` Datei, Sie sollten nur ein **ein**-Kontext -Element darin definieren. Siehe "Kubernetes-Dokumentation" Weitere Informationen zum Erstellen `kubeconfig` Dateien:

   a. **Cloud-Instanzname** (für vom Provider verwaltete Cluster): Geben Sie einen Namen für die neue Cloud-Instanz an, die beim Hinzufügen dieses Clusters erstellt wird. Weitere Informationen zu "Cloud-Instanzen".

      Wenn Sie aus der Cluster-Liste auswählen, achten Sie auf die entsprechende Registerkarte. Wenn eine Warnung angezeigt wird, fahren Sie mit der Warnmeldung über die Warnmeldung, um festzustellen, ob es ein Problem mit dem Cluster gibt. Beispielsweise kann sie erkennen, dass für das Cluster kein Worker Node vorhanden ist.

Wenn Sie einen Cluster auswählen, der mit einem „Private“-Symbol gekennzeichnet ist, verwendet er private IP-Adressen, und der Astra Connector ist erforderlich, damit Astra Control den Cluster verwalten kann. Wenn Sie eine Meldung sehen, dass Sie den Astra Connector installieren müssen, "Beachten Sie diese Anweisungen" Um den Astra Connector zu installieren und die Verwaltung des Clusters zu ermöglichen. Nach der Installation des Astra Connectors sollte der Cluster geeignet sein und Sie können das Hinzufügen des Clusters fortsetzen.

1. **Credential Name** (für selbstverwaltete Cluster): Geben Sie einen Namen für die selbst verwalteten Cluster-Anmeldeinformationen an, die Sie auf Astra Control hochladen. Standardmäßig wird der Name der Anmeldeinformationen automatisch als Name des Clusters ausgefüllt.
2. (Optional) **Storage**: Wählen Sie die Storage-Klasse aus, die Kubernetes-Anwendungen in diesem Cluster standardmäßig verwenden sollen.

Jeder Storage-Service eines Cloud-Providers enthält die folgenden Informationen zu Preis, Performance und Ausfallsicherheit:

- Cloud Volumes Service für Google Cloud: Informationen zu Preis, Performance und Ausfallsicherheit
- Google Persistent Disk: Keine Informationen über Preis, Performance oder Ausfallsicherheit verfügbar
- Azure NetApp Files: Informationen zu Performance und Ausfallsicherheit
- Azure Managed Disks: Es sind weder Preis-, Performance- oder Resilience-Informationen verfügbar
- Amazon Elastic Block Store: Keine Informationen zu Preis, Performance oder Ausfallsicherheit verfügbar
- Amazon FSX für NetApp ONTAP: Keine Informationen zu Preis, Performance und Ausfallsicherheit verfügbar
- NetApp Cloud Volumes ONTAP: Keine Informationen zu Preis, Performance oder Ausfallsicherheit verfügbar

Jede Storage-Klasse kann einen der folgenden Services nutzen:

- "Cloud Volumes Service für Google Cloud"
- "Google Persistent Disk"
- "Azure NetApp Dateien"
- "Von Azure gemanagte Festplatten"
- "Amazon Elastic Block Store"
- "Amazon FSX für NetApp ONTAP"
- "NetApp Cloud Volumes ONTAP"

Weitere Informationen zu "Storage-Klassen für Amazon Web Services Cluster". Weitere Informationen zu "Speicherklassen für AKS-Cluster". Weitere Informationen zu "Speicherklassen für GKE-Cluster".

a. **Überprüfen & Genehmigen**: Prüfen Sie die Konfigurationsdetails und wählen Sie **Cluster hinzufügen**.

Ergebnis

Für Provider-verwaltete Cluster: Wenn dies der erste Cluster ist, den Sie für diesen Cloud-Provider hinzugefügt haben, erstellt Astra Control Service einen Objektspeicher für den Cloud-Provider für Backups von Anwendungen, die auf geeigneten Clustern ausgeführt werden. (Wenn Sie nachfolgende Cluster für diesen Cloud-Provider hinzufügen, werden keine weiteren Objektspeicher erstellt.) Wenn Sie eine Standard-Storage-Klasse angegeben haben, setzt Astra Control Service die von Ihnen angegebene Standard-Storage-Klasse ein. Für Cluster, die in Amazon Web Services oder Google Cloud Platform gemanagt werden, erstellt Astra Control Service auch ein Administratorkonto auf dem Cluster. Diese Vorgänge können mehrere Minuten dauern.

Ändern der Standard-Storage-Klasse

Sie können die Standard-Storage-Klasse für ein Cluster ändern.

Ändern Sie die Standard-Storage-Klasse mit Astra Control

Sie können die Standard-Storage-Klasse für ein Cluster aus Astra Control ändern. Wenn Ihr Cluster einen zuvor installierten Speicher-Backend-Service verwendet, können Sie diese Methode möglicherweise nicht verwenden, um die Standard-Speicherklasse zu ändern (die Aktion **default** ist nicht wählbar). In diesem Fall können Sie Ändern Sie die Standard-Storage-Klasse über die Befehlszeile.

Schritte

1. Wählen Sie in der Astra Control Service-UI **Cluster** aus.
2. Wählen Sie auf der Seite **Cluster** den Cluster aus, den Sie ändern möchten.
3. Wählen Sie die Registerkarte **Storage** aus.
4. Wählen Sie die Kategorie **Speicherklassen** aus.
5. Wählen Sie das Menü **Aktionen** für die Speicherklasse aus, die Sie als Standard festlegen möchten.
6. Wählen Sie **als Standard**.

Ändern Sie die Standard-Storage-Klasse über die Befehlszeile

Sie können die Standard-Storage-Klasse für ein Cluster mit Kubernetes-Befehlen ändern. Diese Methode funktioniert unabhängig von der Konfiguration Ihres Clusters.

Schritte

1. Melden Sie sich bei Ihrem Kubernetes Cluster an.
2. Listen Sie die Storage-Klassen in Ihrem Cluster auf:

```
kubectl get storageclass
```

3. Entfernen Sie die Standardbezeichnung aus der Standardspeicherklasse. Ersetzen Sie <SC_NAME> durch den Namen der Speicherklasse:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Markieren Sie standardmäßig eine andere Storage-Klasse. Ersetzen Sie <SC_NAME> durch den Namen der Speicherklasse:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Bestätigen Sie die neue Standard-Speicherklasse:

```
kubectl get storageclass
```

Finden Sie weitere Informationen

- "Verwalten eines privaten Clusters"

Managen Sie private Cluster über den Astra Control Service

Sie können Astra Control Service verwenden, um private AKS-Cluster zu verwalten. In diesen Anweisungen wird davon ausgegangen, dass Sie bereits einen privaten AKS-Cluster erstellt und eine sichere Methode für den Remote-Zugriff vorbereitet haben. Weitere Informationen zum Erstellen und Abrufen privater AKS-Cluster finden Sie im "Azure-Dokumentation".

- Installieren Sie den Astra Connector Operator
- Einrichtung von persistentem Storage
- Fügen Sie den privaten Cluster zum Astra Control Service hinzu

Installieren Sie den Astra Connector Operator

Sie müssen den Astra Connector Operator auf privaten AKS Cluster installieren. Wenn Sie einen Bastion-Host verwenden, geben Sie diese Befehle über die Befehlszeile des Bastion-Hosts aus.

Schritte

1. Klonen des GitHub-Repositorys des Astra Connector-Betreibers:

```
git clone https://github.com/NetApp/astra-connector-operator.git
```

2. Ändern Sie die Verzeichnisse auf die oberste Ebene des entpackten Bedienerpakets, damit Sie die sehen können `astraconnector_operator.yaml` Datei mit `ls` Befehl.
3. Erstellen Sie einen Namespace für den Astra Connector Operator.

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

4. Anwenden des `astraconnector_operator.yaml` Datei zum Namespace des Bedieners.

```
kubectl apply -f astraconnector_operator.yaml -n astra-connector-
operator
```

5. Erstellen Sie einen Namespace für die privaten Clusterkomponenten.

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

6. Generieren Sie mithilfe der Anweisungen im ein Astra Control API-Token "Dokumentation von Astra Automation".

7. Ändern Sie die Beispielkonfigurationsdatei im config/Samples-Verzeichnis des Astra Connector Operator Repository, um Ihre Anforderungen zu erfüllen.
8. Wenden Sie die Astra Connector Custom Resource Definition (CRD) an.

```
kubectl apply -f config/samples/astraconnector_v1.yaml -n astra-
connector
```

9. Überprüfen Sie den Status des Astra Connectors.

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

Sie sollten sich auf die Ausgabe beziehen, die der folgenden ähnelt:

```
NAME              REGISTERED   ASTRACONNECTORID
astra-connector   true         22b839aa-8b85-445a-85dd-0b1f53b5ea19
```

Einrichtung von persistentem Storage

Konfigurieren Sie persistenten Storage für das Cluster. Sie können gemanagte Azure NetApp Files oder Azure Festplatten verwenden. Weitere Informationen zur Konfiguration von Azure mit diesen Optionen finden Sie in der Dokumentation zu Einstieg:

- "Microsoft Azure mit Azure NetApp Files einrichten"
- "Richten Sie Microsoft Azure mit von Azure gemanagten Festplatten ein"

Fügen Sie den privaten Cluster zum Astra Control Service hinzu

Sie können jetzt den privaten AKS-Cluster zum Astra Control Service hinzufügen. Folgen Sie dem Standard-Workflow, um dem Astra Control Service ein Cluster hinzuzufügen: "Managen Sie Kubernetes Cluster über den Astra Control Service".

Was kommt als Nächstes?

Nachdem Sie sich angemeldet haben und Astra Control um einen Cluster erweitert haben, können Sie die Anwendungsdatenmanagement-Funktionen von Astra Control nutzen.

- "Starten Sie das Anwendungsmanagement"
- "Schützen von Applikationen"
- "Applikationen klonen"
- "Abrechnung einrichten"
- "Benutzer einladen und managen"
- "Management der Anmeldedaten von Cloud-Providern"

- "Benachrichtigungen verwalten"

Videos des Astra Control Service

Viele der Seiten auf dieser doc-Site enthalten Videos, die Ihnen zeigen, wie Sie eine Aufgabe für den Astra Control Service erledigen können. Wenn Sie nur an Videos interessiert sind, haben wir es Ihnen leicht gemacht, indem Sie alle Videos auf dieser einzelnen Seite sammeln (ähnlich einer Playlist).

Videos zum Einrichten von Google Cloud

In den folgenden Videos wird gezeigt, wie die Einrichtung in Google Cloud abgeschlossen wird, bevor Kubernetes Cluster in GCP erkannt werden können.

Aktivieren Sie APIs

Für Ihr Projekt sind Berechtigungen erforderlich, um auf bestimmte Google Cloud-APIs zuzugreifen. Das folgende Video zeigt, wie die APIs über die Google Cloud-Konsole aktiviert werden. "Erfahren Sie mehr über die Aktivierung von APIs".

► 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. Das folgende Video zeigt, wie Sie das Servicekonto über die Google Cloud-Konsole erstellen. "Erfahren Sie mehr über das Erstellen eines Servicekontos".

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

account.mp4 *(video)*

Erstellen eines Service-Kontokonschlüssels

Astra Control Service verwendet einen Service-Account-Schlüssel, um die Identität des Service-Kontos zu ermitteln, das Sie gerade eingerichtet haben. Das folgende Video zeigt, wie der Service-Kontokschlüssel über die Google Cloud-Konsole erstellt wird. "Erfahren Sie mehr über das Erstellen eines Service-Kontokonschlüssels".

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

key.mp4 *(video)*

Videos zur Verwendung von Astra Control

In den folgenden Videos wird gezeigt, wie Sie gängige Aufgaben mit Astra Control ausführen.

Management von Clustern über Astra Control

Nachdem Sie sich beim Astra Control Service angemeldet haben, müssen Sie zunächst Kubernetes-Computing hinzufügen. "Erfahren Sie mehr über das Managen von Clustern".

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

Konfigurieren einer Sicherungsrichtlinie

Eine Sicherungsrichtlinie sichert eine Applikation, indem Snapshots, Backups oder beides nach einem definierten Zeitplan erstellt werden. Sie können Snapshots und Backups stündlich, täglich, wöchentlich und monatlich erstellen. Außerdem können Sie die Anzahl der beizubehaltenden Kopien festlegen. "Weitere Informationen zum Konfigurieren von Sicherungsrichtlinien".

► https://docs.netapp.com/de-de/astra-control-service/media/use/video-set-protection-policy.mp4 *(video)*

Häufig gestellte Fragen zum Astra Control Service

Diese FAQ kann Ihnen helfen, wenn Sie nur nach einer schnellen Antwort auf eine Frage suchen.

Überblick

Astra Control zielt darauf ab, das Lifecycle Management von Applikationsdaten für native Kubernetes-Applikationen zu vereinfachen. Astra Control Service unterstützt Kubernetes-Cluster, die in Umgebungen mehrerer Cloud-Provider ausgeführt werden.

In den folgenden Abschnitten finden Sie Antworten auf einige zusätzliche Fragen, die Sie bei der Verwendung von Astra Control beantworten können. Bei weiteren Klarstellungen wenden Sie sich bitte an astra.feedback@netapp.com

Zugang zum Astra Control

Warum muss ich bei der Registrierung für Astra Control so viele Details angeben?

Astra Control erfordert genaue Kundeninformationen bei der Registrierung. Diese Informationen sind erforderlich, um eine Prüfung auf Global Trade Compliance (GTC) durchgehen zu können.

Warum erhalte ich einen Fehler bei der Registrierung für Astra Control?

Astra Control verlangt von Ihnen, im Abschnitt „Onboarding“ genaue Kundeninformationen bereitzustellen. Wenn Sie falsche Informationen angegeben haben, wird ein Fehler bei der Registrierung angezeigt. Andere Konten, für die Sie Mitglied sind, werden ebenfalls gesperrt.

Was ist die Astra Control Service URL?

Sie können auf den Astra Control Service zugreifen unter https://astra.netapp.io.

Ich habe eine E-Mail-Einladung an einen Kollegen geschickt, aber sie haben sie nicht erhalten. Was soll ich tun?

Bitten Sie sie, ihren Spam-Ordner auf eine E-Mail von do-not-reply@netapp.com zu prüfen, oder suchen Sie in ihrem Posteingang nach „Einladung“. Sie können den Benutzer auch entfernen und versuchen, ihn erneut hinzuzufügen.

Ich habe einen Upgrade auf den Premium PAYGO Plan aus dem Free Plan. Werde ich die ersten 10 Namensräume in Rechnung stellen?

Ja. Nach dem Upgrade auf den Premium-Plan beginnt Astra Control Sie mit dem Aufladen aller verwalteten Namespaces in Ihrem Konto.

Mitte eines Monats habe ich einen Upgrade auf den Premium PAYGO Plan durchgeführt. Werde ich den ganzen Monat in Rechnung stellen?

Nein. Die Abrechnung beginnt mit dem Zeitpunkt, an dem Sie auf den Premium-Plan aktualisiert haben.

Ich verwende den Freiplan, wird mir die Persistent Volume Claims berechnet?

Ja, die von den Clustern Ihres Cloud-Providers verwendeten persistenten Volumes werden Ihnen Rechnung gestellt.

Kubernetes Cluster werden registriert

Muss ich CSI-Treiber auf meinem Cluster installieren, bevor ich den Astra Control Service hinzufüge?

Nein Wenn Ihr Cluster Astra Control hinzugefügt wird, installiert der Service automatisch den Trident Container Storage Interface (CSI)-Treiber (Trident Container Storage Interface) auf dem Kubernetes Cluster. Dieser CSI-Treiber wird für die Bereitstellung persistenter Volumes für von Ihrem Cloud-Provider unterstützte Cluster verwendet.

Nach dem Hinzufügen zum Astra Control Service muss ich den Worker-Knoten zu meinem Cluster hinzufügen. Was soll ich tun?

Neue Worker-Nodes können vorhandenen Pools hinzugefügt oder neue Pools erstellt werden, solange sie der sind `COS_CONTAINERD` Bildtyp. Diese werden automatisch von Astra Control entdeckt. Wenn die neuen Knoten in Astra Control nicht sichtbar sind, prüfen Sie, ob auf den neuen Worker Nodes der unterstützte Bildtyp ausgeführt wird. Sie können den Zustand der neuen Worker-Nodes auch mit überprüfen `kubectl get nodes` Befehl.

Registrieren von Elastic Kubernetes Service (EKS) Clustern

Kann ich einen privaten EKS-Cluster zum Astra Control Service hinzufügen?

Private EKS-Cluster werden derzeit im Astra Control Service nicht unterstützt.

Azure Kubernetes Service-Cluster (AKS) werden registriert

Kann ich einen privaten AKS-Cluster zum Astra Control Service hinzufügen?

Ja, Sie können private AKS-Cluster zu Astra Control Service hinzufügen. Informationen zum Hinzufügen eines privaten AKS-Clusters finden Sie unter "Managen Sie Kubernetes Cluster über den Astra Control Service".

Kann ich Active Directory zur Verwaltung der Authentifizierung für meine AKS-Cluster verwenden?

Ja, Sie können Ihre AKS-Cluster so konfigurieren, dass sie Azure Active Directory (Azure AD) zur Authentifizierung und Identitätsverwaltung verwenden. Wenn Sie das Cluster erstellen, befolgen Sie die Anweisungen im "Offizielle Dokumentation" Um den Cluster mit Azure AD zu konfigurieren. Stellen Sie sicher, dass Ihre Cluster die Anforderungen für die AKS-verwaltete Azure AD-Integration erfüllen.

Google Kubernetes Engine (GKE)-Cluster werden registriert

Kann ich einen privaten GKE-Cluster zum Astra Control Service hinzufügen?

Ja, Sie können private GKE-Cluster zum Astra Control Service hinzufügen. Um ein privates GKE-Cluster zu erstellen, "Folgen Sie den Anweisungen in diesem Knowledgebase-Artikel".

Private Cluster müssen über die verfügen "Autorisierte Netzwerke" Einstellen, um die Astra Control-IP-Adresse zuzulassen:

52.188.218.166/32

Kann mein GKE-Cluster auf einem gemeinsamen VPC residieren?

Ja, Astra Control kann Cluster managen, die in einer gemeinsamen VPC residieren. "Erfahren Sie, wie Sie den Astra-Service-Account für eine Shared VPC-Konfiguration einrichten".

Wo finde ich meine Service-Konto-Anmeldeinformationen auf GCP?

Nachdem Sie sich beim angemeldet haben "Google Cloud Console", Ihre Angaben zu Ihrem Servicekonto finden Sie im Bereich **IAM und Admin**. Weitere Informationen finden Sie unter "So richten Sie Google Cloud für Astra Control ein".

Ich möchte verschiedene GKE-Cluster aus verschiedenen GCP-Projekten hinzufügen. Wird dies in Astra Control unterstützt?

Nein, dies ist keine unterstützte Konfiguration. Es wird nur ein einziges GCP-Projekt unterstützt.

Cluster werden entfernt

Wie kann ich die Registrierung richtig aufheben, einen Cluster herunterholen und die zugehörigen Volumes löschen?

1. "Lösen Sie die Anwendungen von Astra Control".
2. "Lösen Sie das Cluster von Astra Control".
3. "Löschen Sie die Anträge für das persistente Volume".
4. Löschen des Clusters.

Was passiert mit meinen Anwendungen und Daten, nachdem ich den Cluster aus Astra Control entfernt habe?

Das Entfernen eines Clusters aus Astra Control führt keine Änderungen an der Cluster-Konfiguration (Applikationen und persistenter Storage) durch. Astra Control Snapshots oder Backups, die von Applikationen auf diesem Cluster erstellt werden, sind zur Wiederherstellung nicht verfügbar. Volume-Snapshot-Daten, die im Storage-Back-End gespeichert sind, werden nicht entfernt. Persistente Storage Backups von Astra Control verbleiben im Objektspeicher Ihres Cloud-Providers, sind aber nicht für die Wiederherstellung verfügbar.

Entfernen Sie immer einen Cluster aus Astra Control, bevor Sie ihn über GCP löschen. Das Löschen eines Clusters von GCP aus, während dessen Management noch von Astra Control durchgeführt wird, kann Ihr Astra Control Konto Probleme bereiten.

Wird Astra Trident deinstalliert, wenn ich einen Cluster aus Astra Control entferne?

Astra Trident wird nicht aus einem Cluster deinstalliert, wenn Sie den Cluster aus Astra Control entfernen.

Management von Applikationen

Kann Astra Control eine Anwendung bereitstellen?

Astra Control implementiert keine Applikationen. Applikationen müssen außerhalb von Astra Control bereitgestellt werden.

Ich sehe keine PVCs meiner Anwendung, die an GCP CVS gebunden sind. Was ist falsch?

Der Operator Astra Trident setzt die Standard-Storage-Klasse auf `netapp-cvs-perf-premium` Nach dem erfolgreichen Hinzufügen zum Astra Control. Wenn PVCs einer Anwendung nicht an Cloud Volumes Service für Google Cloud gebunden sind, gibt es einige Schritte, die Sie durchführen können:

- Laufen `kubectl get sc` Und überprüfen Sie die Standard-Speicherklasse.
- Prüfen Sie die yaml-Datei oder das Helm-Diagramm, das zum Bereitstellen der Anwendung verwendet wurde, und sehen Sie, ob eine andere Speicherklasse definiert ist.
- GKE Version 1.24 und höher unterstützt keine Docker-basierten Node-Images. Überprüfen Sie, ob der Bildtyp des Arbeiterknotens in GKE lautet `COS_CONTAINERD` Und dass der NFS-Mount erfolgreich war.

Was passiert mit Anwendungen, nachdem ich sie von Astra Control aus verwaltet habe?

Alle bestehenden Backups oder Snapshots werden gelöscht. Applikationen und Daten sind weiterhin verfügbar. Datenmanagement-Vorgänge stehen nicht für nicht verwaltete Anwendungen oder für Backups oder Snapshots zur Verfügung, die dazu gehören.

Datenmanagement-Vorgänge

Wo erstellt Astra Control den Objektspeichereimer?

Die Geografie des ersten verwalteten Clusters bestimmt den Standort des Objektspeichers. Wenn sich beispielsweise der erste Cluster, den Sie hinzufügen, in einer europäischen Zone befindet, wird der Bucket in derselben Region erstellt. Wenn nötig, können Sie "Weitere Buckets hinzufügen".

Es gibt Schnappschüsse in meinem Konto, die ich nicht erstellt habe. Woher kamen sie?

In manchen Situationen erstellt Astra Control automatisch einen Snapshot im Rahmen eines anderen Prozesses. Wenn diese Snapshots älter als ein paar Minuten sind, können Sie sie sicher löschen.

Meine Anwendung verwendet mehrere PVS. Wird Astra Control Snapshots und Backups all dieser VES machen?

Ja. Ein Snapshot-Vorgang auf einer Anwendung von Astra Control umfasst die Momentaufnahme aller VES, die an die VES der Anwendung gebunden sind.

Kann ich die von Astra Control erstellten Snapshots direkt über meinen Cloud-Provider managen?

Nein Snapshots und Backups von Astra Control können nur mit Astra Control verwaltet werden.