Fügen Sie ein vom Anbieter verwaltetes Cluster hinzu

Astra Control Service

NetApp
April 24, 2024

Inhalt

Fügen Sie ein vom Anbieter verwaltetes Cluster hinzu 1
Fügen Sie Astra Control Service einen über einen öffentlichen Provider gemanagten Cluster hinzu 1
Fügen Sie dem Astra Control Service einen über privaten Provider gemanagten Cluster hinzu. 6

Fügen Sie ein vom Anbieter verwaltetes Cluster hinzu

Fügen Sie Astra Control Service einen über einen öffentlichen Provider gemanagten Cluster hinzu

Nachdem Sie Ihre Cloud-Umgebung eingerichtet haben, sind Sie bereit, ein Kubernetes-Cluster zu erstellen und dieses dann zu Astra Control Service hinzuzufügen.

- Erstellen eines Kubernetes-Clusters
- Fügen Sie das Cluster zu Astra Control Service hinzu
- 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.

Fügen Sie das Cluster zu Astra Control Service hinzu

Nachdem Sie sich beim Astra Control Service angemeldet haben, beginnen Sie zunächst mit dem Verwalten Ihrer Cluster. Bevor Sie Astra Control Service ein Cluster hinzufügen, müssen Sie bestimmte Aufgaben ausführen und sicherstellen, dass das Cluster bestimmte Anforderungen erfüllt.

Beachten Sie beim Management von Azure Kubernetes Service und Google Kubernetes Engine-Clustern, dass für die Installation von Astra Control und das Lifecycle Management zwei Optionen zur Verfügung stehen:

- Mit Astra Control Service können Sie den Lebenszyklus von Astra Control Provisioner automatisch managen. Vergewissern Sie sich dazu, dass Astra Trident nicht installiert ist und Astra Control Provisioner nicht auf dem Cluster aktiviert ist, den Sie mit Astra Control Service managen möchten. In diesem Fall aktiviert Astra Control Service automatisch die Astra Control-Bereitstellung, wenn Sie mit dem Cluster-Management beginnen. Upgrades für die Astra Control-Bereitstellung werden automatisch durchgeführt.
- Sie können den Lebenszyklus der Astra Control Provisionierung selbst managen. Aktivieren Sie hierfür die Astra Control-Provisionierung im Cluster, bevor Sie das Cluster mit Astra Control Service verwalten. In diesem Fall erkennt Astra Control Service, dass die Provisionierung von Astra Control bereits aktiviert ist. Es wird weder neu installiert noch Astra Control Provisioner-Upgrades gemanagt. Siehe "Astra Control Provisioner Aktivieren" Für die Schritte aktivieren Sie die Astra Control-Provisionierung.

Wenn Sie Amazon Web Services Cluster mit Astra Control Service managen, müssen Sie bei Bedarf Storage-

Back-Ends, die nur mit dem Astra Control Provisioner verwendet werden können, die Astra Control Service manuell im Cluster aktivieren, bevor Sie die Bereitstellung mit Astra Control Service managen. Siehe "Astra Control Provisioner Aktivieren" Enthält die Schritte zum Aktivieren der Astra Control-Bereitstellung.

Bevor Sie beginnen

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 Control Provisioner ist für Amazon FSX for NetApp ONTAP erforderlich. Wenn Sie Amazon FSX for NetApp ONTAP als Storage-Backend für Ihr EKS-Cluster verwenden möchten, finden Sie in den Informationen zur Astra Control-Bereitstellung 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.

- 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".

Schritte

1. (Optional) Wenn Sie einen Amazon EKS Cluster hinzufügen oder die Installation und Upgrades von Astra Control Provisioner selbst managen möchten, aktivieren Sie die Astra Control Provisioner-Funktion im Cluster. Siehe "Astra Control Provisioner Aktivieren" Für Enablement-Schritte.
2. Öffnen Sie die Web-UI des Astra Control Service in einem Browser.
3. Wählen Sie im Dashboard **Kubernetes Cluster managen** aus.

   Befolgen Sie die Aufforderungen zum Hinzufügen des Clusters.

4. **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.

5. **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.

6. **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.

7. **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.

8. **Andere**: Diese Registerkarte ist nur für die Verwendung mit selbst verwalteten Clustern vorgesehen.
   a. **Cloud-Instanzname**: Geben Sie einen Namen für die neue Cloud-Instanz an, die beim Hinzufügen dieses Clusters erstellt wird. Weitere Informationen zu "Cloud-Instanzen".
   b. Wählen Sie **Weiter**.

      Astra Control Service zeigt eine Liste von Clustern an, aus denen Sie auswählen können.

   c. **Cluster**: Wählen Sie einen Cluster aus der Liste aus, der zu Astra Control Service hinzugefügt werden soll.

      > Wenn Sie aus der Liste der Cluster auswählen, achten Sie auf die Spalte **Eligiblity**. Wenn ein Cluster „nicht berechtigt“ oder „teilweise berechtigt“ ist, bewegen Sie den Mauszeiger über den Status, um zu ermitteln, ob ein Problem im Cluster vorliegt. Beispielsweise kann sie erkennen, dass für das Cluster kein Worker Node vorhanden ist.

   d. Wählen Sie **Weiter**.
   e. (Optional) **Speicher**: Wählen Sie optional die Storage-Klasse aus, die Kubernetes-Anwendungen, die auf diesem Cluster bereitgestellt werden sollen, standardmäßig verwenden sollen.
9. Um eine neue Standard-Storage-Klasse für den Cluster auszuwählen, aktivieren Sie das Kontrollkästchen **Neue Standard-Storage-Klasse zuweisen**.
10. Wählen Sie eine neue Standard-Storage-Klasse aus der Liste aus.

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. Wählen Sie **Weiter**.
  b. **Überprüfen und genehmigen**: Überprüfen Sie die Konfigurationsdetails.
  c. Wählen Sie **Add**, um den Cluster zu Astra Control Service hinzuzufügen.

Ergebnis

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
```

Fügen Sie dem Astra Control Service einen über privaten Provider gemanagten Cluster hinzu

Mit Astra Control Service können Sie private GKE-Cluster (Google Kubernetes Engine) managen. In diesen Anweisungen wird davon ausgegangen, dass Sie bereits einen privaten AKS- oder OpenShift-Cluster erstellt und eine sichere Methode für den Remote-Zugriff darauf vorbereitet haben. Weitere Informationen zum Erstellen und Zugreifen auf private AKS- oder OpenShift-Cluster finden Sie in der folgenden Dokumentation:

- "Azure-Dokumentation für private AKS-Cluster"
- "Azure-Dokumentation für private OpenShift-Cluster"

Mit Astra Control Service können Sie private Azure Kubernetes Service (AKS)-Cluster sowie private Red hat OpenShift-Cluster in AKS managen. In diesen Anweisungen wird davon ausgegangen, dass Sie bereits einen privaten AKS- oder OpenShift-Cluster erstellt und eine sichere Methode für den Remote-Zugriff darauf vorbereitet haben. Weitere Informationen zum Erstellen und Zugreifen auf private AKS- oder OpenShift-Cluster finden Sie in der folgenden Dokumentation:

- "Azure-Dokumentation für private AKS-Cluster"
- "Azure-Dokumentation für private OpenShift-Cluster"

Mit Astra Control Service können Sie private EKS-Cluster (Amazon Elastic Kubernetes Service) managen. In diesen Anweisungen wird davon ausgegangen, dass Sie bereits einen privaten EKS-Cluster erstellt und eine sichere Methode für den Remote-Zugriff darauf vorbereitet haben. Weitere Informationen zum Erstellen und Zugreifen auf private EKS-Cluster finden Sie im "Amazon EKS-Dokumentation".

Führen Sie die folgenden Aufgaben aus, um Ihren privaten Cluster zum Astra Control Service hinzuzufügen:

1. Astra Connector Installieren
2. Einrichtung von persistentem Storage
3. Fügen Sie den über den privaten Provider gemanagten Cluster zu Astra Control Service hinzu

Astra Connector Installieren

Bevor Sie einen privaten Cluster hinzufügen, müssen Sie Astra Connector im Cluster installieren, damit Astra Control damit kommunizieren kann. Siehe "Installieren Sie die vorherige Version von Astra Connector für private Cluster, die mit nicht-Kubernetes-nativen Workflows gemanagt werden" Weitere Anweisungen.

Einrichtung von persistentem Storage

Konfigurieren Sie persistenten Storage für das Cluster. In der Dokumentation „erste Schritte“ finden Sie weitere Informationen zum Konfigurieren von persistentem Storage:

- "Microsoft Azure mit Azure NetApp Files einrichten"
- "Richten Sie Microsoft Azure mit von Azure gemanagten Festplatten ein"
- "Einrichten von Amazon Web Services"
- "Google Cloud einrichten"

Fügen Sie den über den privaten Provider gemanagten Cluster zu Astra Control Service hinzu

Sie können den privaten Cluster jetzt dem Astra Control Service hinzufügen.

Beachten Sie beim Management von Azure Kubernetes Service und Google Kubernetes Engine-Clustern, dass für die Installation von Astra Control und das Lifecycle Management zwei Optionen zur Verfügung stehen:

- Mit Astra Control Service können Sie den Lebenszyklus von Astra Control Provisioner automatisch managen. Vergewissern Sie sich dazu, dass Astra Trident nicht installiert ist und Astra Control Provisioner nicht auf dem Cluster aktiviert ist, den Sie mit Astra Control Service managen möchten. In diesem Fall aktiviert Astra Control Service automatisch die Astra Control-Bereitstellung, wenn Sie mit dem Cluster-Management beginnen. Upgrades für die Astra Control-Bereitstellung werden automatisch durchgeführt.
- Sie können den Lebenszyklus der Astra Control Provisionierung selbst managen. Aktivieren Sie hierfür die Astra Control-Provisionierung im Cluster, bevor Sie das Cluster mit Astra Control Service verwalten. In diesem Fall erkennt Astra Control Service, dass die Provisionierung von Astra Control bereits aktiviert ist. Es wird weder neu installiert noch Astra Control Provisioner-Upgrades gemanagt. Siehe "Astra Control Provisioner Aktivieren" Für die Schritte aktivieren Sie die Astra Control-Provisionierung.

Wenn Sie Amazon Web Services Cluster mit Astra Control Service managen, müssen Sie bei Bedarf Storage-Back-Ends, die nur mit dem Astra Control Provisioner verwendet werden können, die Astra Control Service manuell im Cluster aktivieren, bevor Sie die Bereitstellung mit Astra Control Service managen. Siehe "Astra Control Provisioner Aktivieren" Enthält die Schritte zum Aktivieren der Astra Control-Bereitstellung.

Bevor Sie beginnen

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 Control Provisioner ist für Amazon FSX for NetApp ONTAP erforderlich. Wenn Sie Amazon FSX for NetApp ONTAP als Storage-Backend für Ihr EKS-Cluster verwenden möchten, finden Sie in den Informationen zur Astra Control-Bereitstellung 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.

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

  52.188.218.166/32

- 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".

Schritte

1. (Optional) Wenn Sie einen Amazon EKS Cluster hinzufügen oder die Installation und Upgrades von Astra Control Provisioner selbst managen möchten, aktivieren Sie die Astra Control Provisioner-Funktion im Cluster. Siehe "Astra Control Provisioner Aktivieren" Für Enablement-Schritte.
2. Öffnen Sie die Web-UI des Astra Control Service in einem Browser.
3. Wählen Sie im Dashboard **Kubernetes Cluster managen** aus.

   Befolgen Sie die Aufforderungen zum Hinzufügen des Clusters.

4. **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.

5. **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.

6. **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.

7. **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.

8. **Andere**: Diese Registerkarte ist nur für die Verwendung mit selbst verwalteten Clustern vorgesehen.
   a. **Cloud-Instanzname**: Geben Sie einen Namen für die neue Cloud-Instanz an, die beim Hinzufügen dieses Clusters erstellt wird. Weitere Informationen zu "Cloud-Instanzen".
   b. Wählen Sie **Weiter**.

      Astra Control Service zeigt eine Liste von Clustern an, aus denen Sie auswählen können.

   c. **Cluster**: Wählen Sie einen Cluster aus der Liste aus, der zu Astra Control Service hinzugefügt werden soll.

      > Wenn Sie aus der Liste der Cluster auswählen, achten Sie auf die Spalte **Eligiblity**. Wenn ein Cluster „nicht berechtigt“ oder „teilweise berechtigt“ ist, bewegen Sie den Mauszeiger über den Status, um zu ermitteln, ob ein Problem im Cluster vorliegt. Beispielsweise kann sie erkennen, dass für das Cluster kein Worker Node vorhanden ist.

9. Wählen Sie **Weiter**.
10. (Optional) **Speicher**: Wählen Sie optional die Storage-Klasse aus, die Kubernetes-Anwendungen, die auf diesem Cluster bereitgestellt werden sollen, standardmäßig verwenden sollen.
    a. Um eine neue Standard-Storage-Klasse für den Cluster auszuwählen, aktivieren Sie das Kontrollkästchen **Neue Standard-Storage-Klasse zuweisen**.
    b. Wählen Sie eine neue Standard-Storage-Klasse aus der Liste aus.

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".

c. Wählen Sie **Weiter**.

d. **Überprüfen und genehmigen**: Überprüfen Sie die Konfigurationsdetails.

e. Wählen Sie **Add**, um den Cluster zu Astra Control Service hinzuzufügen.

Ergebnis

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
```