Konzepte

Astra Control Center

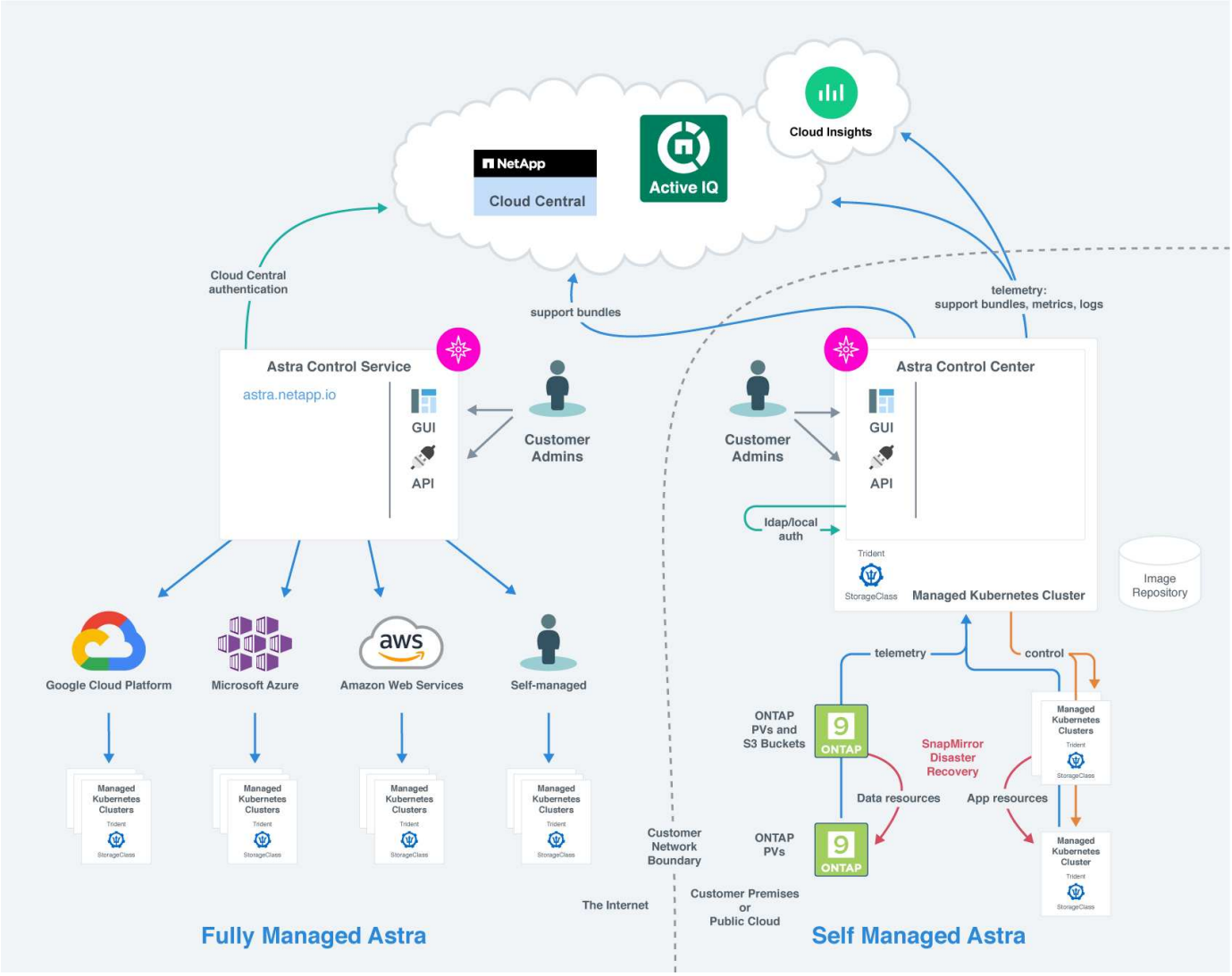
NetApp
November 21, 2023

Inhalt

Konzepte

Architektur und Komponenten

Hier ist ein Überblick über die verschiedenen Komponenten der Astra Control-Umgebung.



Komponenten des Astra Control

- **Kubernetes-Cluster**: Kubernetes ist eine portable, erweiterbare Open-Source-Plattform für das Management von Workloads und Services in Containern, die sowohl deklarative Konfigurationen als auch Automatisierung ermöglicht. Astra bietet Managementservices für Applikationen, die in einem Kubernetes-Cluster gehostet werden.
- **Astra Trident**: Trident ist eine vollständig unterstützte Open-Source-Storage-bereitstellung und -Orchestrierung mit Hilfe von NetApp. Mit Trident können Sie Storage Volumes für Container-Applikationen erstellen, die von Docker und Kubernetes verwaltet werden. Bei der Implementierung mit Astra Control Center umfasst Trident ein konfiguriertes ONTAP Storage-Back-End.
- **Speicher-Backend**:

- Astra Control Service nutzt folgende Storage-Back-Ends:
  - "NetApp Cloud Volumes Service für Google Cloud" Oder Google Persistent Disk als Speicher-Backend für GKE-Cluster
  - "Azure NetApp Dateien" Oder von Azure verwaltete Festplatten als Storage-Backend für AKS-Cluster.
  - "Amazon Elastic Block Store (EBS)" Oder "Amazon FSX für NetApp ONTAP" Als Back-End-Speicheroptionen für EKS-Cluster.
- Astra Control Center nutzt folgende Storage-Back-Ends:
  - ONTAP AFF, FAS und ASA. Als Storage-Software- und Hardware-Plattform bietet ONTAP wichtige Storage-Services, Unterstützung für mehrere Storage-Zugriffsprotokolle und Storage-Managementfunktionen wie Snapshots und Spiegelung.
  - Cloud Volumes ONTAP

- **Cloud Insights**: Mit Cloud Insights, einem Cloud-Infrastruktur-Monitoring-Tool, überwachen Sie die Performance und Auslastung Ihrer Kubernetes-Cluster und werden von Astra Control Center gemanagt. Cloud Insights korreliert die Storage-Auslastung mit Workloads. Wenn Sie die Cloud Insights-Verbindung im Astra Control Center aktivieren, werden Telemetriedaten auf den UI-Seiten des Astra Control Center angezeigt.

Astra Control-Schnittstellen

Sie können Aufgaben über verschiedene Schnittstellen ausführen:

- **Web-Benutzeroberfläche (UI)**: Sowohl Astra Control Service als auch Astra Control Center nutzen die gleiche webbasierte Benutzeroberfläche, in der Sie Apps verwalten, migrieren und schützen können. Verwenden Sie die UI auch zum Verwalten von Benutzerkonten und Konfigurationseinstellungen.
- **API**: Sowohl Astra Control Service als auch Astra Control Center nutzen die gleiche Astra Control API. Mit der API können Sie die gleichen Aufgaben ausführen, die Sie über die UI ausgeführt haben.

Mit Astra Control Center können Sie auch Kubernetes Cluster in VM-Umgebungen managen, migrieren und schützen.

Finden Sie weitere Informationen

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

Datensicherung

Lernen Sie die verfügbaren Datensicherungsarten im Astra Control Center kennen und erfahren Sie, wie Sie diese am besten für den Schutz Ihrer Applikationen nutzen.

Snapshots, Backups und Sicherungsrichtlinien

Sowohl Snapshots als auch Backups sichern die folgenden Datentypen:

- Der Applikation selbst.
- Alle persistenten Daten-Volumes, die mit der Applikation in Verbindung stehen
- Alle zu der Applikation gehörenden Ressourcenartefakte

A *Snapshot* ist eine zeitpunktgenaue Kopie einer Applikation, die auf demselben bereitgestellten Volume wie die Applikation gespeichert ist. In der Regel sind sie schnell. Sie können lokale Snapshots verwenden, um die Anwendung auf einen früheren Zeitpunkt wiederherzustellen. Snapshots sind nützlich für schnelle Klone. Snapshots enthalten alle Kubernetes-Objekte für die App, einschließlich Konfigurationsdateien. Snapshots sind nützlich zum Klonen oder Wiederherstellen einer Anwendung innerhalb desselben Clusters.

Ein *Backup* basiert auf einem Snapshot. Er wird im externen Objektspeicher gespeichert und kann daher im Vergleich zu lokalen Snapshots langsamer erstellt werden. Sie können ein Applikations-Backup in demselben Cluster wiederherstellen oder eine Applikation migrieren, indem Sie dessen Backup auf ein anderes Cluster wiederherstellen. Sie können auch eine längere Aufbewahrungsdauer für Backups wählen. Da diese im externen Objektspeicher gespeichert werden, bieten Backups in der Regel besseren Schutz als Snapshots bei Serverausfällen oder Datenverlusten.

Eine *Schutzrichtlinie* ist eine Möglichkeit zum Schutz einer App, indem automatisch Snapshots, Backups oder beides gemäß einem von Ihnen für die App definierten Zeitplan erstellt werden. Eine Sicherungsrichtlinie erlaubt Ihnen außerdem festzulegen, wie viele Snapshots und Backups im Zeitplan aufbewahrt werden sollen, und verschiedene granulare Zeitplanebenen festzulegen. Die Automatisierung von Backups und Snapshots mit einer Sicherungsrichtlinie ist die beste Methode, um sicherzustellen, dass jede Applikation gemäß den Anforderungen Ihres Unternehmens und der SLA-Anforderungen (Service Level Agreement) geschützt ist.

> _Sie können erst dann vollständig geschützt sein, wenn Sie ein kürzlich gesichertes Backup haben. Das ist wichtig, da Backups abseits der persistenten Volumes in einem Objektspeicher gespeichert werden. Wenn ein Ausfall das Cluster und der damit verbundene persistente Storage entfernt, muss ein Backup wiederhergestellt werden. Ein Snapshot würde es Ihnen nicht ermöglichen, eine Wiederherstellung durchzuführen.

Klone

Ein *Clone* ist ein exaktes Duplikat einer App, ihrer Konfiguration und ihrer persistenten Daten-Volumes. Sie können einen Klon entweder manuell auf demselben Kubernetes-Cluster oder auf einem anderen Cluster erstellen. Das Klonen einer Applikation kann nützlich sein, wenn Sie Applikationen und Storage von einem Kubernetes Cluster zu einem anderen verschieben müssen.

Replizierung in ein Remote-Cluster

Mithilfe von Astra Control können Sie mit den asynchronen Replizierungsfunktionen der NetApp SnapMirror Technologie Business Continuity für Ihre Applikationen erzielen: Mit Low-RPO (Recovery Point Objective) und Low-RTO (Recovery Time Objective). Sobald Ihre Applikationen konfiguriert sind, können sie Daten und Applikationsänderungen von einem Cluster auf ein anderes replizieren.

Astra Control repliziert asynchron App-Snapshot-Kopien in einem Remote-Cluster. Der Replizierungsprozess umfasst Daten in den persistenten Volumes, die von SnapMirror repliziert werden, und die durch Astra Control geschützten App-Metadaten.

Die Replizierung von Applikationen unterscheidet sich folgendermaßen von Backup und Restore von

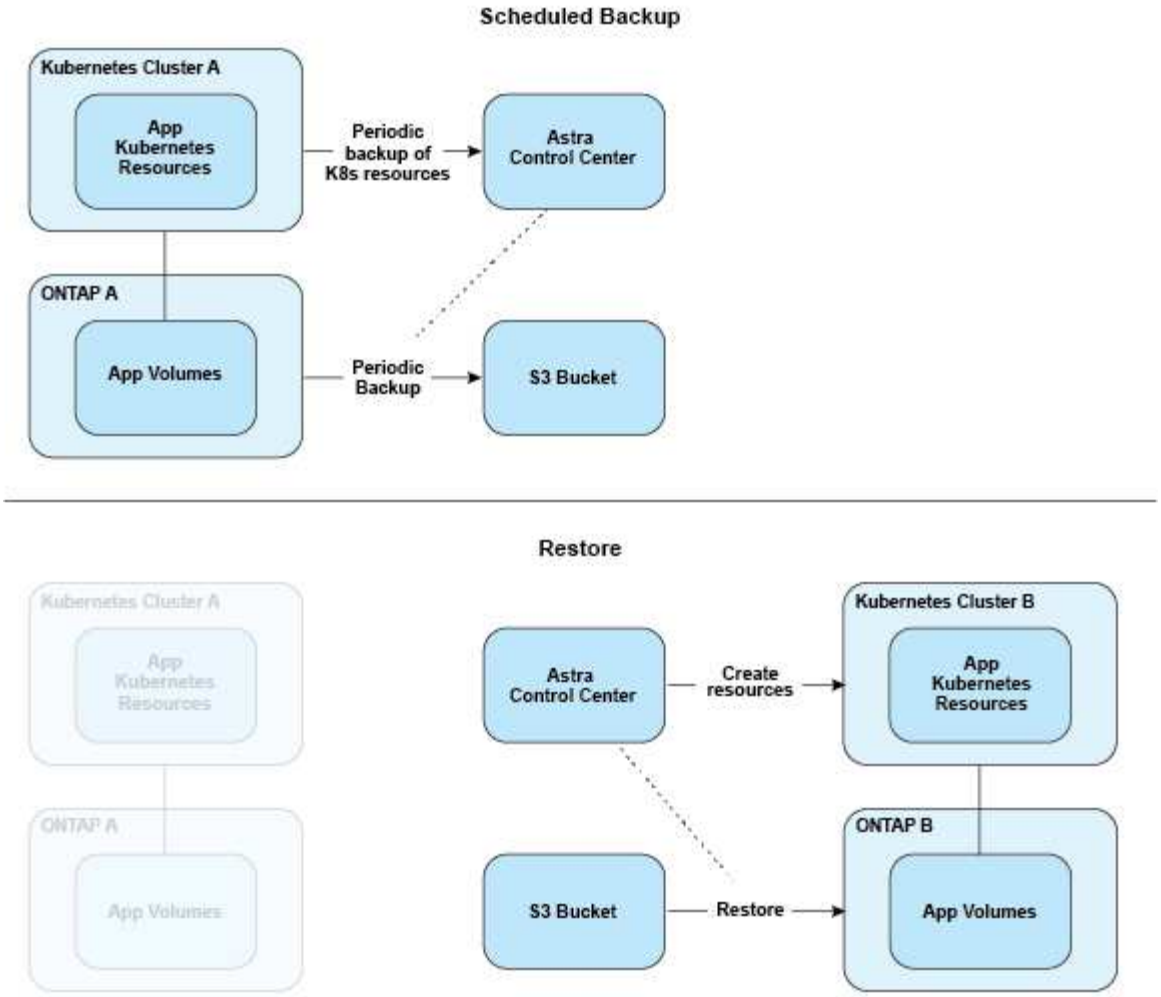
Applikationen:

- **App-Replizierung**: Astra Control erfordert, dass die Quell- und Ziel-Kubernetes-Cluster mit den entsprechenden ONTAP Storage-Back-Ends verfügbar und gemanagt werden, die für NetApp SnapMirror konfiguriert sind. Astra Control repliziert den richtlinienbasierten Applikations-Snapshot auf dem Remote-Cluster. NetApp SnapMirror Technologie wird zur Replizierung der Daten des persistenten Volumes verwendet. Zum Failover kann Astra Control die replizierte Applikation online schalten, indem die Applikationsobjekte auf dem Kubernetes Ziel-Cluster mit den replizierten Volumes auf dem ONTAP Ziel-Cluster neu erstellt werden. Da die Daten des persistenten Volumes bereits auf dem Ziel-ONTAP Cluster vorhanden sind, bietet Astra Control kurze Recovery-Zeiten für Failover.
- **App-Backup und -Restore**: Beim Backup von Applikationen erstellt Astra Control einen Snapshot der Applikationsdaten und speichert diese in einem Objekt-Storage-Bucket. Wenn eine Wiederherstellung erforderlich ist, müssen die Daten in dem Bucket auf ein persistentes Volume auf dem ONTAP Cluster kopiert werden. Der Backup-/Restore-Vorgang erfordert nicht, dass der sekundäre Kubernetes/ONTAP Cluster verfügbar und gemanagt wird. Die zusätzliche Datenkopie kann jedoch zu längeren Restore-Zeiten führen.

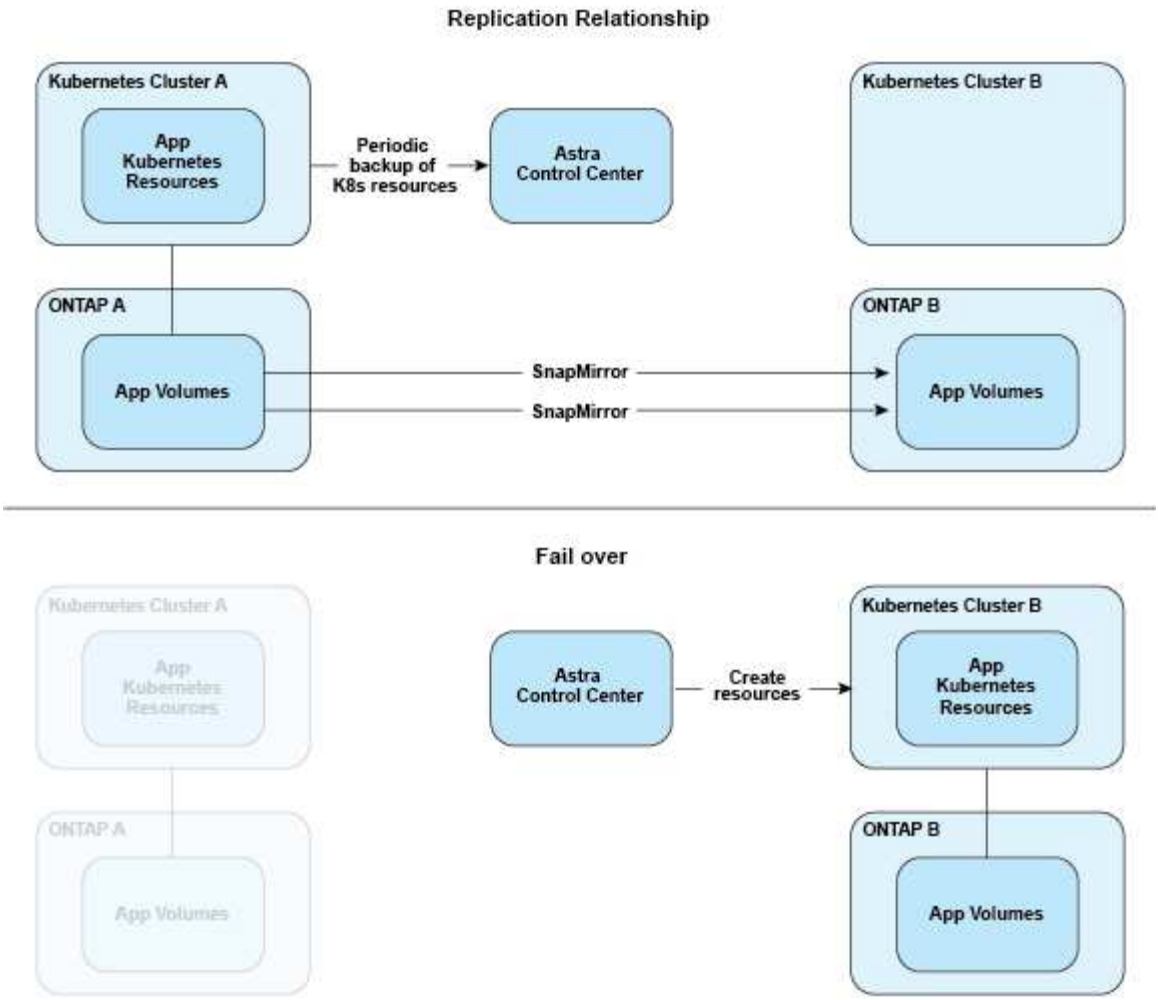
Weitere Informationen zur Replizierung von Applikationen finden Sie unter "Replizieren von Applikationen auf einem Remote-System mit SnapMirror Technologie".

Die folgenden Images zeigen den geplanten Backup- und Wiederherstellungsprozess im Vergleich zum Replikationsprozess.

Der Backup-Prozess kopiert Daten in S3 Buckets und Restores aus S3 Buckets:



Zum anderen erfolgt die Replizierung auf ONTAP. Bei einem Failover werden die Kubernetes-Ressourcen erstellt:



Lizenzierung

Astra Control Center erfordert die Installation einer Lizenz, damit die vollständige App-Datenmanagement-Funktion aktiviert werden kann. Wenn Sie Astra Control Center ohne Lizenz bereitstellen, wird in der Web-UI ein Banner angezeigt, in dem Sie darauf hingewiesen werden, dass die Systemfunktionalität begrenzt ist.

Sie erhalten eine Lizenz auf eine der folgenden Arten:

- "Wenn Sie Astra Control Center evaluieren, laden Sie die Evaluierungslizenzdatei herunter". Mit einer Evaluierungslizenz können Sie das Astra Control Center 90 Tage ab dem Datum, an dem Sie die Lizenz herunterladen, verwenden.
- "Wenn Sie Astra Control Center bereits gekauft haben, generieren Sie Ihre NetApp Lizenzdatei (NLF)." Von der NetApp Support Site aus. Nach dem Kauf des Produkts erhalten Sie eine Seriennummer und eine Lizenz, die Sie auf der Support-Website verwenden.

Details zu Lizenzen, die für ONTAP Storage Back-Ends erforderlich sind, finden Sie unter "Unterstützte Storage-Back-Ends".

> Sie können ohne Lizenz ein Cluster hinzufügen, einen Bucket hinzufügen und ein Storage-Backend verwalten.

Berechnung der Lizenznutzung

Wenn Sie dem Astra Control Center einen neuen Cluster hinzufügen, zählen diese nicht auf verbrauchte Lizenzen, bis mindestens eine auf dem Cluster ausgeführte Applikation vom Astra Control Center verwaltet wird.

Wenn Sie eine App auf einem Cluster managen, sind alle CPU-Einheiten des Clusters im Lizenzverbrauch des Astra Control Center enthalten.

Weitere Informationen

- "Fügen Sie beim ersten Einrichten des Astra Control Center eine Lizenz hinzu"
- "Aktualisieren einer vorhandenen Lizenz"

=
:allow-uri-read:

Storage-Klassen und persistente Volume-Größe

Astra Control Center unterstützt ONTAP als Storage-Backend.

Überblick

Das Astra Control Center unterstützt Folgendes:

- **Trident Storage-Klassen mit ONTAP-Storage**: Wenn Sie ein ONTAP-Back-End verwenden, bietet Astra Control Center die Möglichkeit, das ONTAP-Back-End zu importieren, um verschiedene Monitoring-Informationen zu melden.

> Trident Storage-Kurse sollten außerhalb des Astra Control Center vorkonfiguriert sein.

Speicherklassen

Wenn Sie dem Astra Control Center einen Cluster hinzufügen, werden Sie aufgefordert, eine zuvor konfigurierte Storage-Klasse auf diesem Cluster als Standard-Storage-Klasse auszuwählen. Diese Storage-Klasse wird verwendet, wenn in einem persistent Volume Claim (PVC) keine Storage-Klasse angegeben ist. Die Standard-Speicherklasse kann jederzeit im Astra Control Center geändert werden und jede Speicherklasse kann jederzeit verwendet werden, indem der Name der Speicherklasse im PVC- oder Helm-Diagramm angegeben wird. Stellen Sie sicher, dass nur eine einzelne Standard-Storage-Klasse für Ihr Kubernetes-Cluster definiert ist.

Finden Sie weitere Informationen

- "Astra Trident-Dokumentation"

Benutzerrollen und Namespaces

Informieren Sie sich über Benutzerrollen und Namespaces in Astra Control und darüber, wie Sie mit ihnen den Zugriff auf Ressourcen in Ihrem Unternehmen steuern können.

Benutzerrollen

Sie können Rollen verwenden, um den Zugriff von Benutzern auf Ressourcen oder Funktionen von Astra Control zu steuern. Im Folgenden sind die Benutzerrollen in Astra Control aufgeführt:

- Ein **Viewer** kann Ressourcen anzeigen.
- Ein **Mitglied** verfügt über Berechtigungen für Viewer-Rollen und kann Apps und Cluster verwalten, Apps verwalten und Snapshots und Backups löschen.
- Ein **Admin** verfügt über Berechtigungen für die Mitgliederrolle und kann alle anderen Benutzer außer dem Eigentümer hinzufügen und entfernen.
- Ein **Owner** hat Administratorrechte und kann beliebige Benutzerkonten hinzufügen und entfernen.

Sie können einem Mitglied oder Viewer-Benutzer Einschränkungen hinzufügen, um den Benutzer auf einen oder mehrere Benutzer zu beschränken Namespaces.

Namespaces

Ein Namespace ist ein Umfang, den Sie bestimmten Ressourcen innerhalb eines von Astra Control gemanagten Clusters zuweisen können. Astra Control erkennt Namespaces eines Clusters, wenn Sie das Cluster zu Astra Control hinzufügen. Sobald die Namespaces erkannt wurden, können sie Benutzern als Bedingungen zuweisen. Nur Mitglieder, die Zugriff auf diesen Namespace haben, können diese Ressource nutzen. Sie können Namespaces verwenden, um den Zugriff auf Ressourcen anhand eines Paradigmas zu steuern, das für Ihr Unternehmen sinnvoll ist, z. B. nach physischen Regionen oder Abteilungen innerhalb eines Unternehmens. Wenn Sie einem Benutzer Einschränkungen hinzufügen, können Sie diesen Benutzer so konfigurieren, dass er Zugriff auf alle Namespaces oder nur auf bestimmte Namespaces hat. Sie können auch Namespace-Einschränkungen mithilfe von Namespace-Etiketten zuweisen.

Weitere Informationen

"Managen Sie lokale Benutzer und Rollen"

=
:allow-uri-read: