



# Konzepte

## Astra Control Center

NetApp  
May 20, 2024

# Inhalt

- Konzepte ..... 1
  - Architektur und Komponenten ..... 1
  - Datensicherung ..... 6
  - Lizenzierung ..... 9
  - Applikationsmanagement ..... 11
  - Storage-Klassen und persistente Volume-Größe ..... 13
  - Benutzerrollen und Namespaces ..... 13

# Konzepte

## Architektur und Komponenten

Astra Control ist eine Kubernetes-Lösung für das übergreifende Lebenszyklusmanagement von Applikationsdaten. Sie vereinfacht den Betrieb zustandsbehafteter Applikationen und unterstützt Sie beim Speichern, Sichern und Verschieben Ihrer Kubernetes-Workloads zwischen Hybrid- und Multi-Cloud-Umgebungen.

### Sorgen

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

#### Store:

- Dynamische Storage-Bereitstellung für Container-Workloads
- Verschlüsselung der Daten auf der Übertragungstrecke aus Container zu persistenten Volumes
- Regionsübergreifende, zonenübergreifende Replizierung

#### Schutz:

- Automatische Erkennung und applikationsgerechte Sicherung einer gesamten Applikation und ihrer Daten
- Sofortige Wiederherstellung einer Applikation von einer beliebigen Snapshot-Version je nach den Anforderungen Ihres Unternehmens
- Schnelles Failover über Zonen, Regionen und Cloud-Provider hinweg

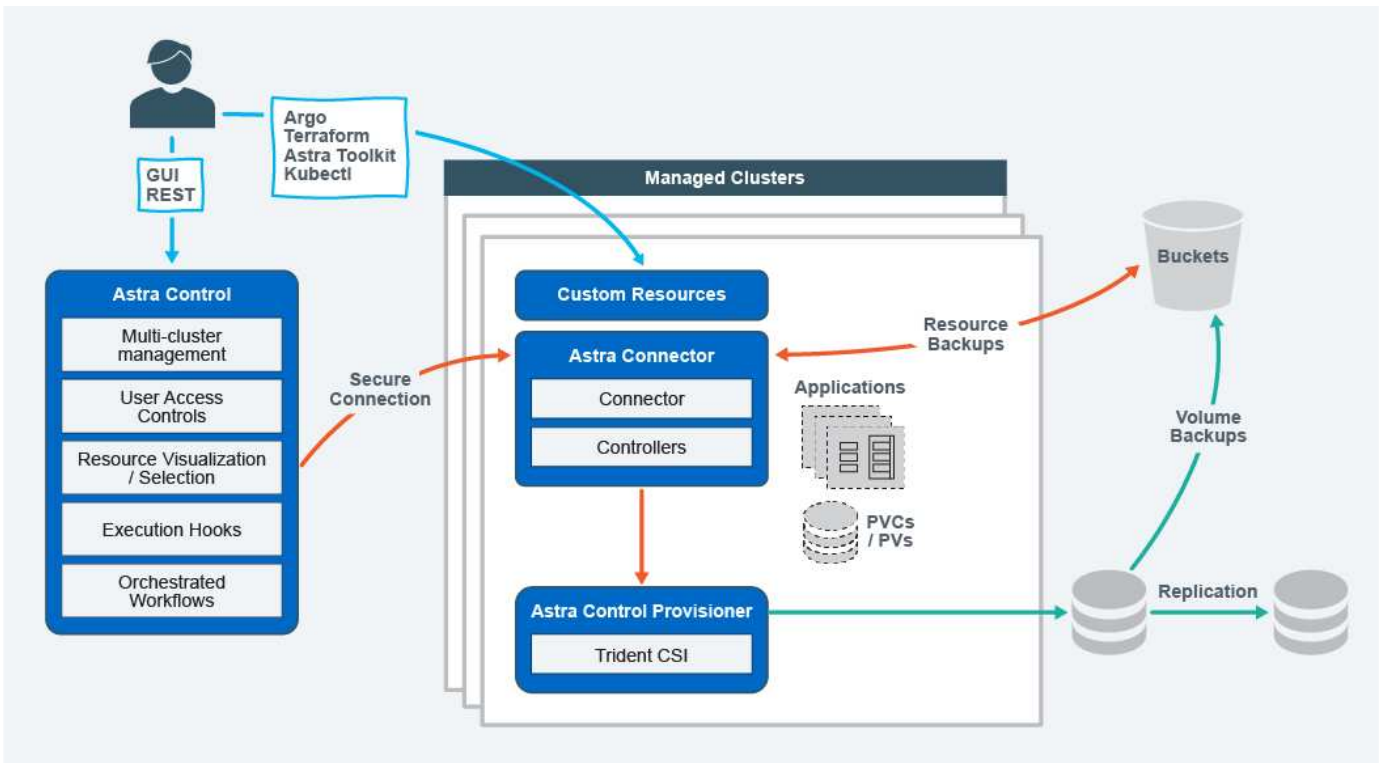
#### Verschieben:

- Vollständige Applikations- und Datenmobilität innerhalb und zwischen Kubernetes-Clustern und Clouds
- Sofortige Klone vollständiger Applikationen und Daten
- Migration von Anwendungen mit einem Klick über eine konsistente Web-UI und -API

## Der Netapp Architektur Sind

Mit der Architektur von Astra Control bietet die IT erweiterte Datenmanagementfunktionen, die sowohl die Funktionalität als auch die Verfügbarkeit von Kubernetes-Applikationen verbessern. Sie vereinfacht das Management, den Schutz und die Verschiebung von Container-Workloads in Public Clouds und On-Premises-Umgebungen. Die Software bietet Automatisierungsfunktionen über ihre REST-API und sein SDK und ermöglicht einen programmatischen Zugriff für eine nahtlose Integration in vorhandene Workflows.

Astra Control ist Kubernetes-nativ und ermöglicht Datensicherungs-Workflows, die benutzerdefinierte Ressourcen verwenden und gleichzeitig rückwärtskompatibel mit der vorhandenen API und dem SDK bleiben. Die native Datensicherung von Kubernetes bietet deutliche Vorteile. Durch die nahtlose Integration in Kubernetes-APIs und -Ressourcen kann die Datensicherung über die vorhandenen CI/CD- und/oder GitOps-Tools eines Unternehmens zu einem integrierenden Bestandteil des Applikationslebenszyklus werden.



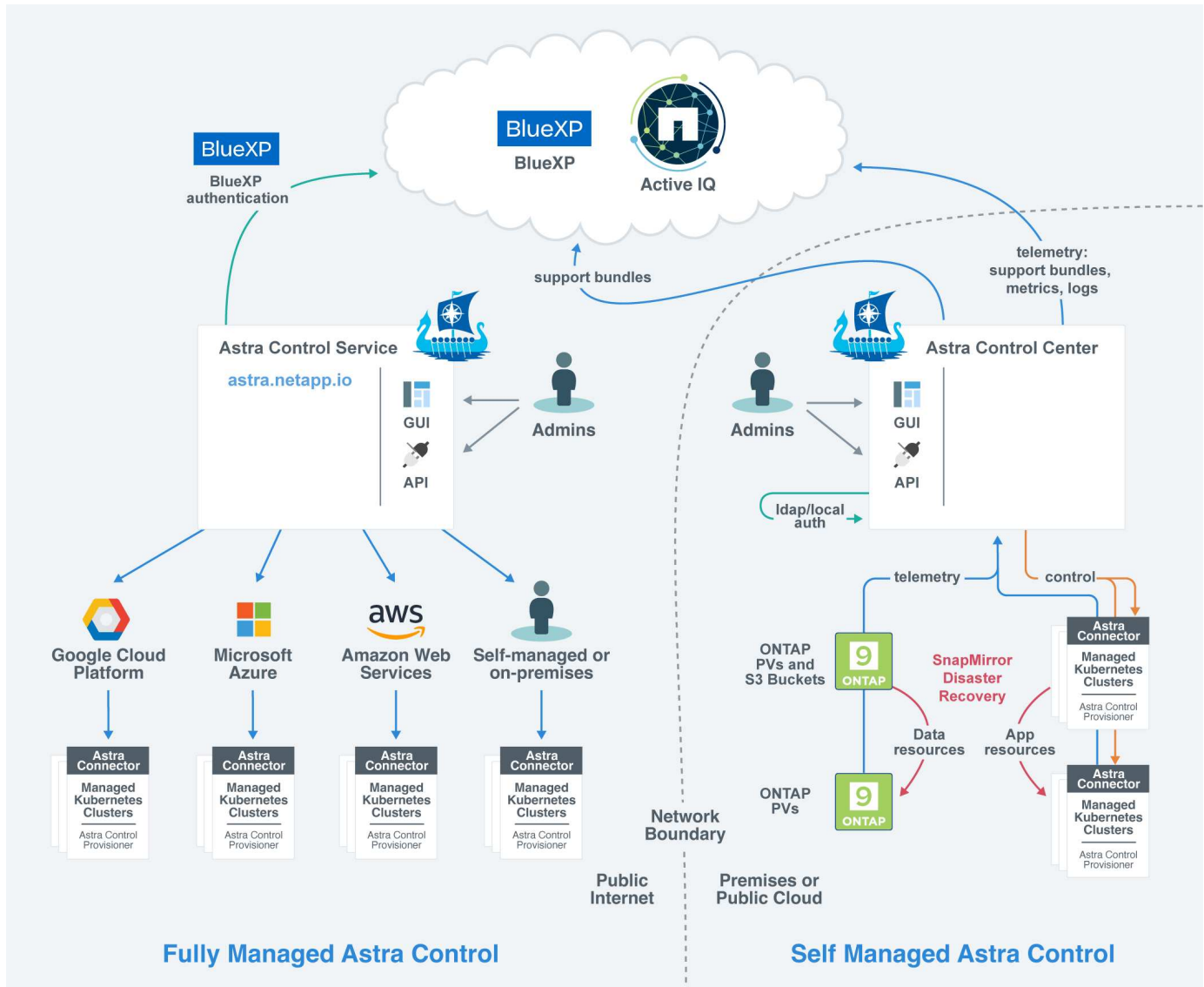
Astra Control basiert auf vier sich ergänzenden Komponenten:

- **Astra Control:** Astra Control ist der zentralisierte Management-Service für alle gemanagten Cluster und bietet orchestrierte Workloads für den Schutz und die Mobilität von Applikationen in der Cloud und On-Premises sowie folgende Funktionen:
  - Kombinierte Ansicht auf mehrere Cluster und Clouds
  - Schutz orchestrierter Workflows
  - Granulare Ressourcenvisualisierung und -Auswahl
- **Astra Connector:** Astra Connector arbeitet mit Astra Control zusammen, um eine sichere Verbindung zu jedem verwalteten Cluster bereitzustellen und so die lokale Ausführung geplanter Operationen unabhängig vom Verbindungsstatus sowie die folgenden Funktionen zu ermöglichen:
  - Lokale Ausführung geplanter Vorgänge unabhängig vom Verbindungsstatus
  - Lokale Abläufe, die die Nutzung von Astra Systemressourcen auf Cluster verteilen und optimieren
  - Lokale Installation, die den Zugriff auf das Cluster mit den geringsten Berechtigungen ermöglicht, um die Sicherheit zu erhöhen
- **Astra Control Provisioner:** Der Astra Control Provisioner bietet zentrale CSI-Bereitstellungsfunktionen und erweiterte Storage Management-Funktionen für zusätzliche Sicherheit und Disaster Recovery-Konfiguration sowie die folgenden Funktionen:
  - Dynamische Storage-Bereitstellung für Container-Workloads
  - Erweitertes Storage-Management:
    - Verschlüsselung der Daten während der Übertragung vom Container zum PV
    - SnapMirror Cloud Funktionalität mit regionsübergreifender Replizierung
- **Astra Custom-Ressourcen:** Auf jedem Cluster verwendete benutzerdefinierte Ressourcen bieten einen Kubernetes-nativen Ansatz für die lokale Ausführung von Vorgängen. Dies vereinfacht die Integration in andere Kubernetes-freundliche Tools und Automatisierungsfunktionen sowie folgende Funktionen:

- Direkte Integration und Workflows für die Automatisierung von Tools anderer Anbieter
- Primitive auf niedrigerer Ebene, die benutzerdefinierte Workflows ermöglichen

## Implementierungsmodelle

Astra Control ist in zwei Implementierungsmodellen verfügbar.



- **Astra Control Service:** Ein von NetApp gemanagter Service, der applikationskonsistentes Datenmanagement für Kubernetes-Cluster in Umgebungen mehrerer Cloud-Provider sowie selbstverwaltete Kubernetes-Cluster bietet.

["Dokumentation des Astra Control Service"](#)

- **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 Center-Dokumentation"](#)

	<b>Astra Control Service</b>	<b>Astra Control Center</b>
<b>Wie wird das angeboten?</b>	Vollständig gemanagter Cloud-Service von NetApp	Als Software, die Sie herunterladen, installieren und verwalten können
<b>Wo wird sie gehostet?</b>	In einer Public Cloud von NetApp ihrer Wahl	In Ihrem eigenen Kubernetes-Cluster
<b>Wie wird sie aktualisiert?</b>	Gemanagt von NetApp	Sie verwalten jegliche Updates
<b>Welche Kubernetes-Distributionen werden unterstützt?</b>	<ul style="list-style-type: none"> <li>• <b>Cloud-Provider</b> <ul style="list-style-type: none"> <li>◦ Amazon Web Services <ul style="list-style-type: none"> <li>▪ Amazon Elastic Kubernetes Service (EKS)</li> </ul> </li> <li>◦ Google Cloud <ul style="list-style-type: none"> <li>▪ Google Kubernetes Engine (GKE)</li> </ul> </li> <li>◦ Microsoft Azure <ul style="list-style-type: none"> <li>▪ Azure Kubernetes-Service (AKS)</li> </ul> </li> </ul> </li> <li>• <b>Selbstverwaltete Cluster</b> <ul style="list-style-type: none"> <li>◦ Kubernetes (Vorgelagert)</li> <li>◦ Rancher Kubernetes Engine (RKE)</li> <li>◦ Red hat OpenShift Container Platform</li> </ul> </li> <li>• <b>On-Premises-Cluster</b> <ul style="list-style-type: none"> <li>◦ Lokale Red hat OpenShift Container-Plattform</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Azure Kubernetes Service für Azure Stack HCI</li> <li>• Google Anthos</li> <li>• Kubernetes (Vorgelagert)</li> <li>• Rancher Kubernetes Engine (RKE)</li> <li>• Red hat OpenShift Container Platform</li> </ul>

	Astra Control Service	Astra Control Center
Welche Storage-Back-Ends werden unterstützt?	<ul style="list-style-type: none"> <li>• <b>Cloud-Provider</b> <ul style="list-style-type: none"> <li>◦ Amazon Web Services <ul style="list-style-type: none"> <li>▪ Amazon EBS</li> <li>▪ Amazon FSX für NetApp ONTAP</li> <li>▪ "Cloud Volumes ONTAP"</li> </ul> </li> <li>◦ Google Cloud <ul style="list-style-type: none"> <li>▪ Google Persistent Disk</li> <li>▪ NetApp Cloud Volumes Service</li> <li>▪ "Cloud Volumes ONTAP"</li> </ul> </li> <li>◦ Microsoft Azure <ul style="list-style-type: none"> <li>▪ Über Azure Gemanagte Festplatten</li> <li>▪ Azure NetApp Dateien</li> <li>▪ "Cloud Volumes ONTAP"</li> </ul> </li> </ul> </li> <li>• <b>Selbstverwaltete Cluster</b> <ul style="list-style-type: none"> <li>◦ Amazon EBS</li> <li>◦ Über Azure Gemanagte Festplatten</li> <li>◦ Google Persistent Disk</li> <li>◦ "Cloud Volumes ONTAP"</li> <li>◦ NetApp MetroCluster</li> <li>◦ "Longhorn"</li> </ul> </li> <li>• <b>On-Premises-Cluster</b> <ul style="list-style-type: none"> <li>◦ NetApp MetroCluster</li> <li>◦ NetApp ONTAP AFF und FAS Systeme</li> <li>◦ NetApp ONTAP Select</li> <li>◦ "Cloud Volumes ONTAP"</li> <li>◦ "Longhorn"</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• NetApp ONTAP AFF und FAS Systeme</li> <li>• NetApp ONTAP Select</li> <li>• "Cloud Volumes ONTAP"</li> <li>• "Longhorn"</li> </ul>

## Finden Sie weitere Informationen

- ["Dokumentation des Astra Control Service"](#)
- ["Astra Control Center-Dokumentation"](#)
- ["Astra Trident-Dokumentation"](#)
- ["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.

### Unveränderliche Backups

Ein unveränderliches Backup ist ein Backup, das innerhalb eines festgelegten Zeitraums nicht geändert oder gelöscht werden kann. Beim Erstellen eines unveränderlichen Backups überprüft Astra Control, ob es sich bei dem verwendeten Bucket um einen WORM-Bucket (Write Once Read Many) handelt. Falls ja, stellt er sicher, dass das Backup in Astra Control unveränderlich ist.

Astra Control Center unterstützt das Erstellen unveränderlicher Backups mit den folgenden Plattformen und Bucket-Typen:



- Amazon Web Services verwenden einen Amazon S3 Bucket mit konfigurierter S3 Object Lock
- NetApp StorageGRID mithilfe eines S3 Buckets mit konfigurierter S3 Object Lock-Funktion

Beachten Sie beim Arbeiten mit unveränderlichen Backups Folgendes:

- Wenn ein Backup auf einem WORM-Bucket in einer nicht unterstützten Plattform oder auf einem nicht unterstützten Bucket-Typ durchgeführt wird, können unvorhersehbare Ergebnisse wie das Löschen von Backups sogar dann angezeigt werden, wenn die Aufbewahrungszeit abgelaufen ist.
- Astra Control unterstützt keine Management-Richtlinien für den Daten-Lebenszyklus oder das manuelle Löschen von Objekten in den Buckets, die Sie mit unveränderlichen Backups verwenden. Stellen Sie sicher, dass Ihr Storage-Backend nicht für das Management des Lebenszyklus von Astra Control Snapshots oder gesicherten Daten konfiguriert ist.

## 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 zwischen Storage-Back-Ends

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). Nach der Konfiguration können Ihre Applikationen auf diese Weise Daten und Applikationsänderungen von einem Storage-Back-End auf ein anderes replizieren, sowohl im selben Cluster als auch zwischen verschiedenen Clustern.

Sie können zwischen zwei ONTAP SVMs auf demselben ONTAP Cluster oder in verschiedenen ONTAP Clustern replizieren.

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

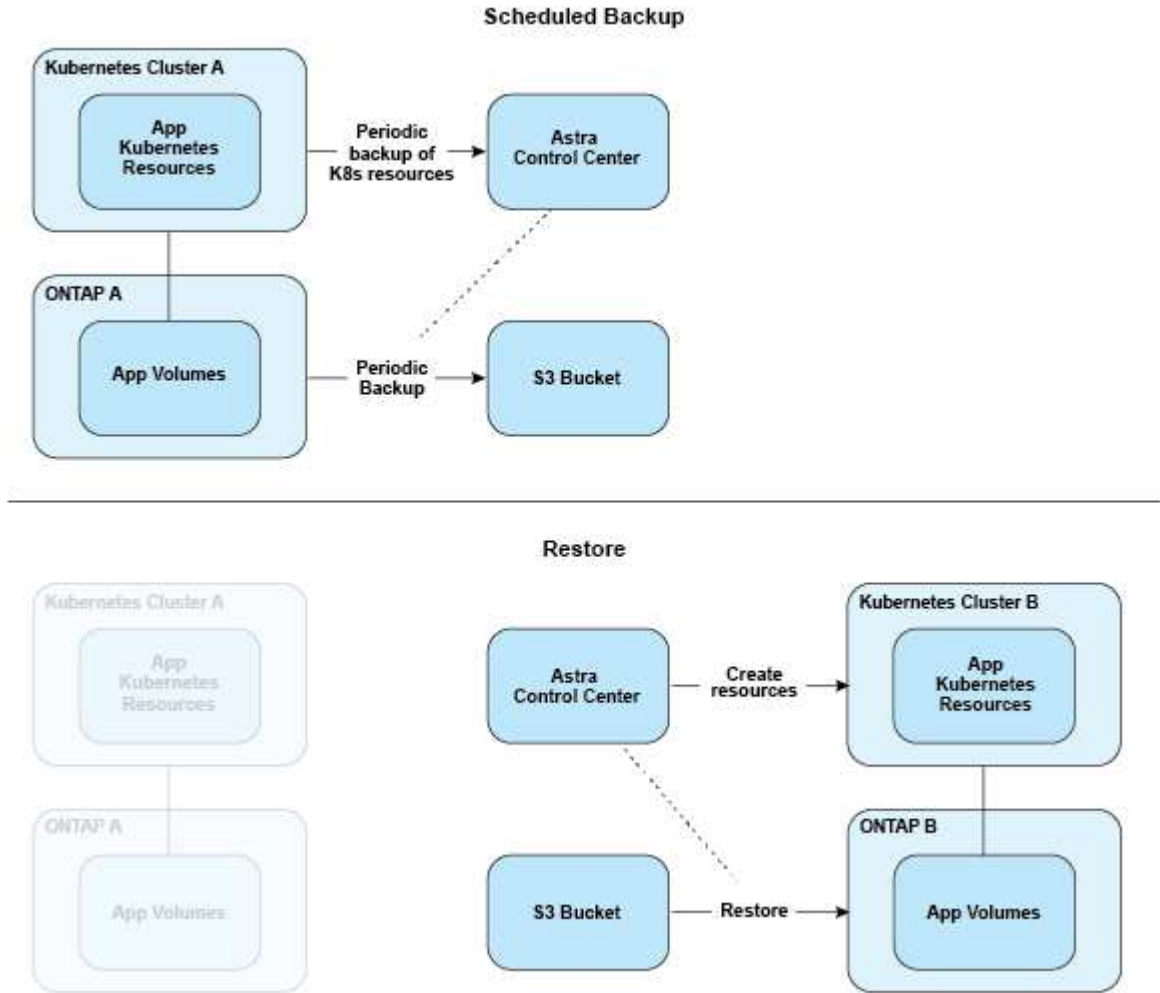
Die Replizierung von Applikationen unterscheidet sich folgendermaßen von Backup und Restore von Applikationen:

- **App-Replizierung:** Für Astra Control müssen die Kubernetes Quell- und Ziel-Cluster (die dasselbe Cluster sein können) verfügbar sein und mit ihren jeweiligen ONTAP Storage-Back-Ends gemanagt werden, die für die Aktivierung von NetApp SnapMirror konfiguriert sind. Astra Control repliziert den richtlinienbasierten Applikations-Snapshot auf das Ziel-Storage-Back-End. NetApp SnapMirror wird zur Replizierung der persistenten Volume-Daten eingesetzt. 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 persistenten Volume-Daten bereits auf dem Ziel-ONTAP-Cluster vorhanden sind, kann Astra Control schnelle Recovery-Zeiten für Failover bieten.
- **App-Backup und -Wiederherstellung:** Beim Backup von Anwendungen erstellt Astra Control einen Snapshot der App-Daten und speichert diesen 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 zum Replizieren von Apps finden Sie unter ["Replizieren von Applikationen auf einem Remote-System mit SnapMirror Technologie"](#).

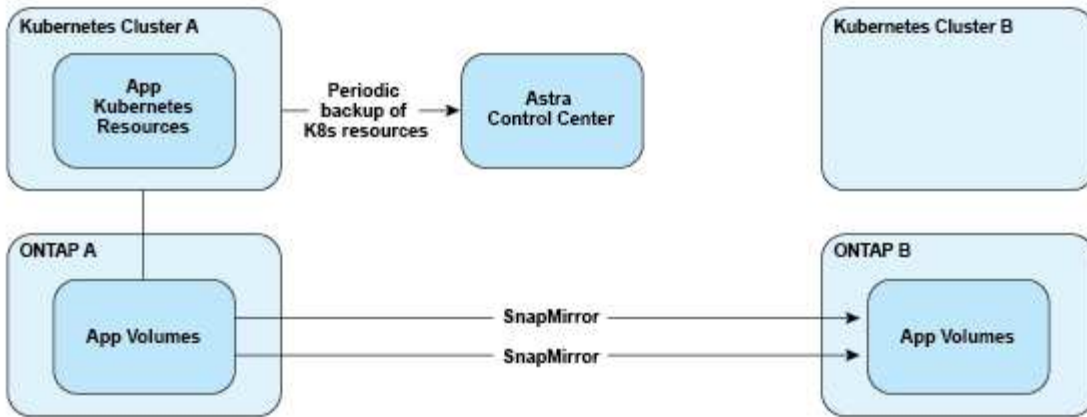
Die folgenden Images zeigen den geplanten Backup- und Wiederherstellungsprozess im Vergleich zum Replikationsprozess.

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

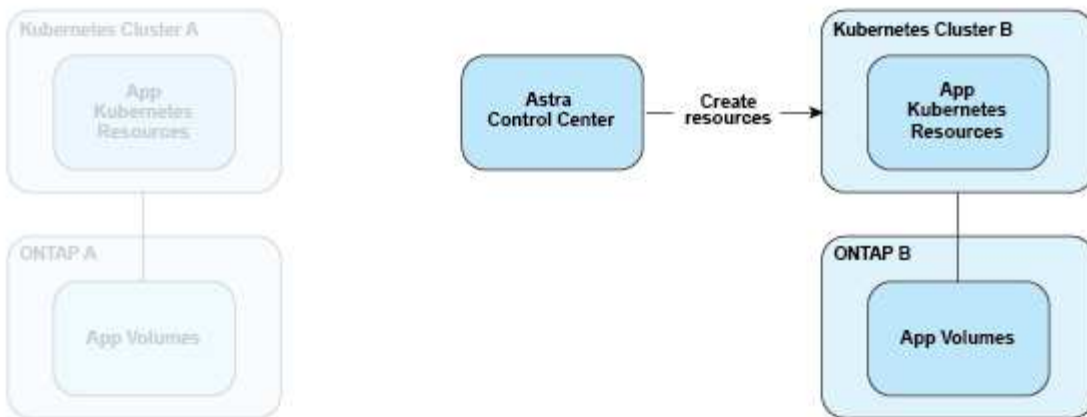


Andererseits wird die Replizierung zu ONTAP durchgeführt. Durch ein Failover werden die Kubernetes-Ressourcen erzeugt:

### Replication Relationship



### Fail over



## Backups, Snapshots und Klone mit abgelaufener Lizenz

Wenn Ihre Lizenz abläuft, können Sie nur dann eine neue Applikation hinzufügen oder Vorgänge zum Schutz von Applikationen (wie Snapshots, Backups, Klone und Wiederherstellungsvorgänge) durchführen, wenn die hinzugefügte oder zu schützende Applikation eine weitere Astra Control Center-Instanz ist.

## Lizenzierung

Bei der Bereitstellung von Astra Control Center wird es mit einer eingebetteten 90-Tage-Evaluierungslizenz für 4,800 CPU-Einheiten installiert. Wenn Sie mehr Kapazität oder einen längeren Evaluierungszeitraum benötigen oder auf eine komplette Lizenz aktualisieren möchten, können Sie eine andere Evaluierungslizenz oder eine komplette Lizenz von NetApp beziehen.

Sie erhalten eine Lizenz auf eine der folgenden Arten:

- Wenn Sie Astra Control Center evaluieren und andere Evaluierungsbedingungen als in der eingebetteten Evaluierungslizenz benötigen, wenden Sie sich an NetApp, um eine andere Evaluierungslizenzdatei zu anfordern.
- ["Wenn Sie Astra Control Center bereits gekauft haben, generieren Sie Ihre NetApp Lizenzdatei \(NLF\)."](#) Melden Sie sich dazu auf der NetApp Support-Website an und navigieren Sie zu Ihren Softwarelizenzen im

Menü „Systeme“.

Details zu Lizenzen, die für ONTAP Storage Back-Ends erforderlich sind, finden Sie unter ["Unterstützte Storage-Back-Ends"](#).



Stellen Sie sicher, dass Ihre Lizenz mindestens so viele CPU-Einheiten wie erforderlich aktiviert. Wenn die Anzahl der CPU-Einheiten, die Astra Control Center derzeit verwaltet, die verfügbaren CPU-Einheiten in der neuen Lizenz überschreitet, können Sie die neue Lizenz nicht anwenden.

## Evaluierungslizenzen und Volllizenzen

Eine eingebettete Evaluierungslizenz wird mit der neuen Astra Control Center-Installation bereitgestellt. Eine Evaluierungslizenz ermöglicht über einen begrenzten Zeitraum (90 Tage) dieselben Funktionen und Funktionen wie eine Volllizenz. Nach dem Evaluierungszeitraum ist eine vollständige Lizenz erforderlich, um mit voller Funktionalität fortzufahren.

## Ablauf der Lizenz

Wenn die aktive Astra Control Center-Lizenz abläuft, sind die UI- und API-Funktionen für die folgenden Funktionen nicht verfügbar:

- Manuelle lokale Snapshots und Backups
- Geplante lokale Snapshots und Backups
- Wiederherstellen aus einem Snapshot oder einem Backup
- Klonen aus einem Snapshot oder aktuellem Status
- Managen neuer Applikationen
- Konfigurieren von Replikationsrichtlinien

## 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 verwalten, sind alle CPU-Einheiten dieses Clusters im Lizenzverbrauch von Astra Control Center enthalten, mit Ausnahme der CPU-Einheiten des Red hat OpenShift-Cluster-Node, die von einem mit dem Label gemeldet werden `node-role.kubernetes.io/infra: ""`.



Red hat OpenShift Infrastruktur-Nodes nutzen keine Lizenzen in Astra Control Center. Um einen Node als Infrastruktur-Node zu markieren, wenden Sie die Beschriftung an `node-role.kubernetes.io/infra: ""` Auf den Node.

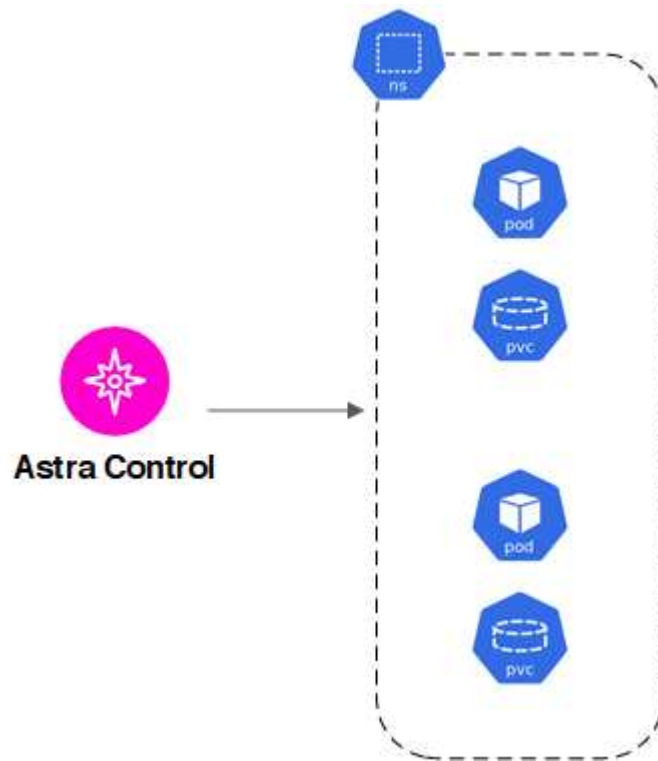
## Weitere Informationen

- ["Fügen Sie beim ersten Einrichten des Astra Control Center eine Lizenz hinzu"](#)
- ["Aktualisieren einer vorhandenen Lizenz"](#)

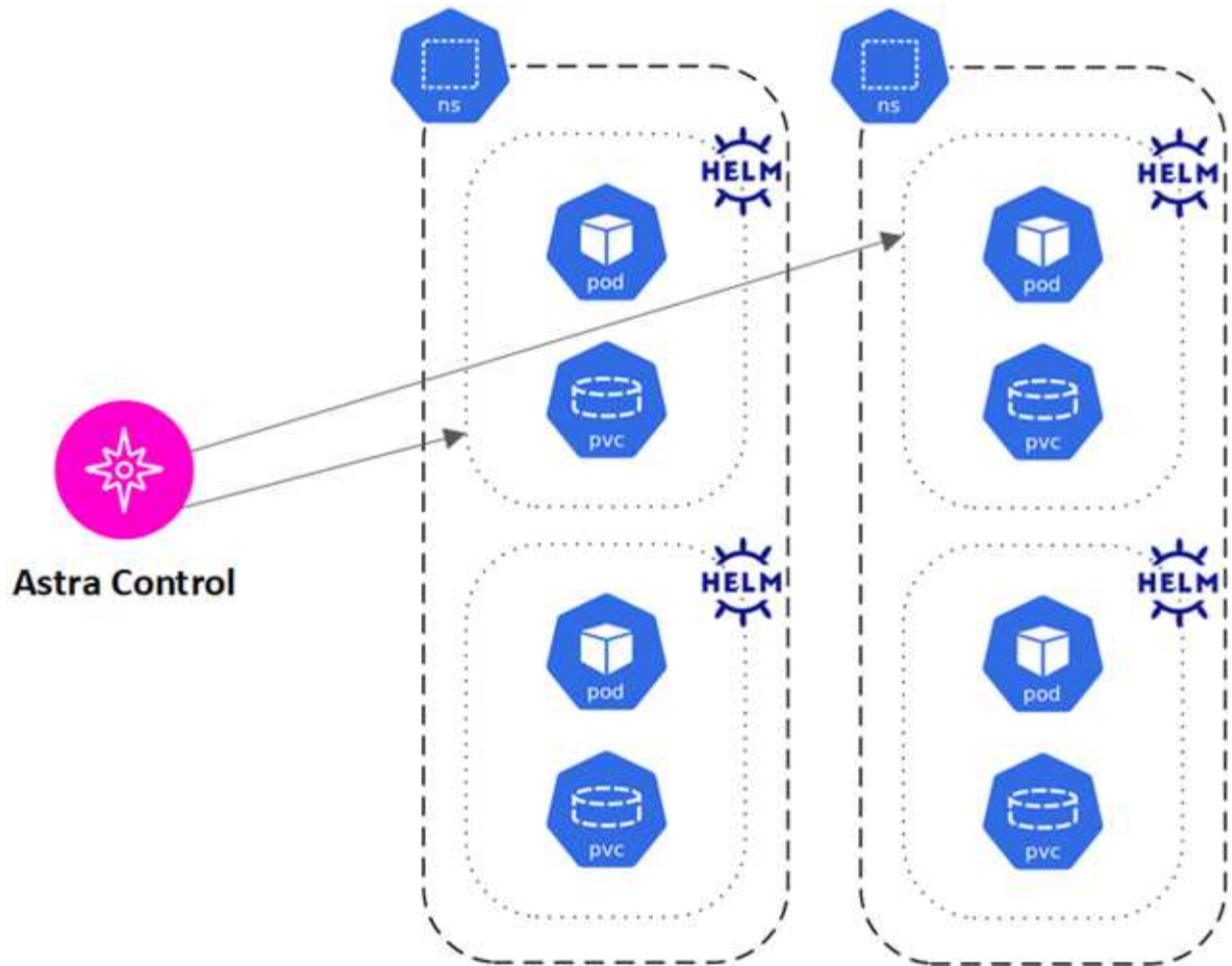
# Applikationsmanagement

Wenn Astra Control Ihre Cluster erkennt, werden die Apps auf diesen Clustern solange nicht verwaltet, bis Sie das gewünschte Management wählen. Eine verwaltete Anwendung in Astra Control kann eine der folgenden sein:

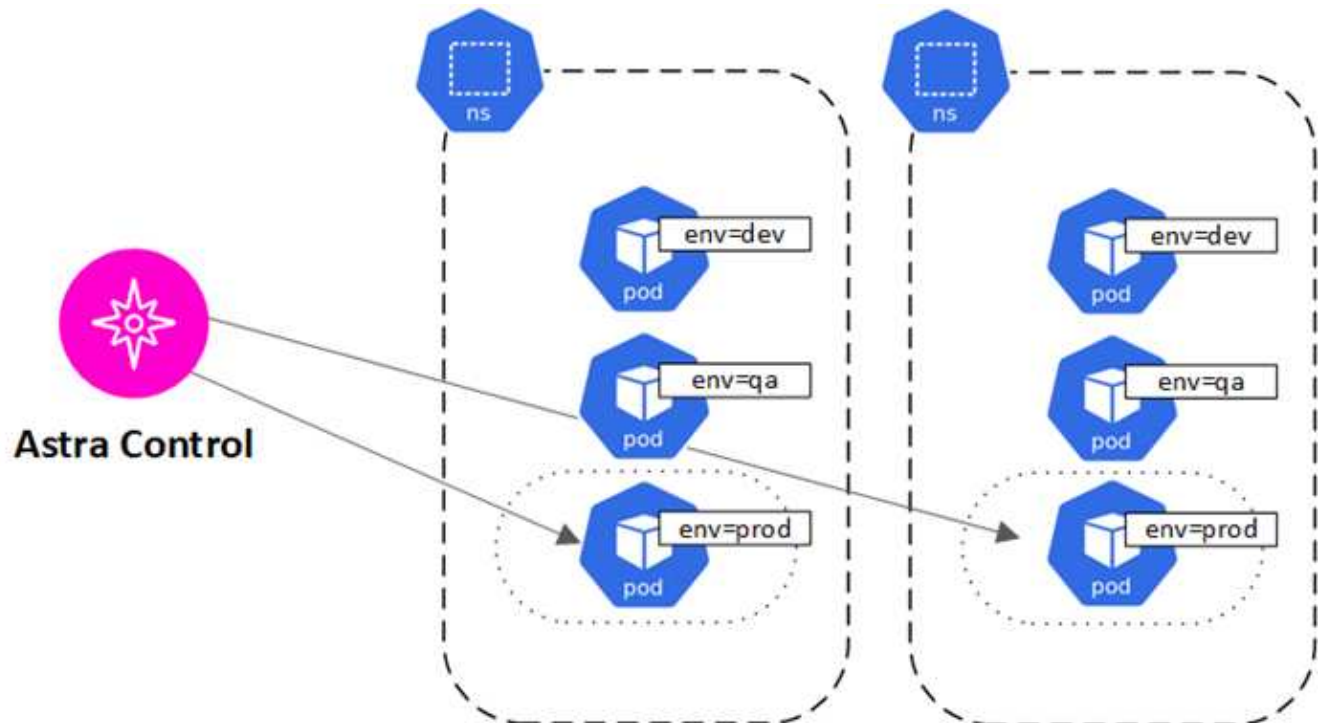
- Einen Namespace, einschließlich aller Ressourcen in diesem Namespace



- Eine individuelle Anwendung, die innerhalb einer oder mehrerer Namespaces bereitgestellt wird (in diesem Beispiel wird helm3 verwendet)



- Eine Gruppe von Ressourcen, die innerhalb eines oder mehrerer Namespaces durch ein Kubernetes-Label identifiziert werden



# Storage-Klassen und persistente Volume-Größe

Astra Control Center unterstützt NetApp ONTAP und Longhorn als Storage-Back-Ends.

## Überblick

Das Astra Control Center unterstützt Folgendes:

- **Von ONTAP-Speicher unterstützte Speicherklassen:** Wenn Sie ein ONTAP-Backend verwenden, bietet Astra Control Center die Möglichkeit, das ONTAP-Backend zu importieren, um Überwachungsinformationen zu melden.
- **CSI-basierte Speicherklassen mit Longhorn:** Sie können Longhorn mit dem Longhorn Container Storage Interface (CSI) Treiber verwenden.



Speicherklassen sollten sein "**Konfiguriert**" Verwenden von Astra Control Provisioner.

## 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.

## 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"](#)



## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.