



# **Nutzen Sie Das Astra Control Center**

## **Astra Control Center**

NetApp  
November 21, 2023

# Inhalt

- Nutzen Sie Das Astra Control Center . . . . . 1
  - Starten Sie das Anwendungsmanagement . . . . . 1
  - Schützen von Applikationen . . . . . 7
  - Monitoring des Applikations- und Cluster-Systemzustands . . . . . 31
  - Konto verwalten . . . . . 33
  - Buckets verwalten . . . . . 44
  - Management des Storage-Backends . . . . . 47
  - Überwachen Sie laufende Aufgaben . . . . . 49
  - Infrastruktur mit Cloud Insights-, Prometheus- oder Fluentd-Verbindungen überwachen . . . . . 50
  - Heben Sie das Management von Applikationen und Clustern auf . . . . . 59
  - Upgrade Astra Control Center . . . . . 60
  - Deinstallieren Sie Astra Control Center . . . . . 69

# Nutzen Sie Das Astra Control Center

## Starten Sie das Anwendungsmanagement

Nach Ihnen "[Fügen Sie dem Astra Control Management einen Cluster hinzu](#)", Sie können Apps auf dem Cluster installieren (außerhalb von Astra Control) und dann auf der Seite Anwendungen in Astra Control, um die Apps und ihre Ressourcen zu definieren.

### Anforderungen für das Applikationsmanagement

Astra Control verfügt über folgende Anforderungen an das Applikationsmanagement:

- **Lizenzierung:** Zur Verwaltung von Anwendungen mit dem Astra Control Center benötigen Sie eine Astra Control Center-Lizenz.
- **Namespaces:** Apps können mit Astra Control innerhalb eines oder mehrerer spezifizierter Namespaces auf einem einzigen Cluster definiert werden. Eine App kann Ressourcen enthalten, die mehrere Namespaces innerhalb desselben Clusters umfassen. Astra Control unterstützt nicht die Möglichkeit, Applikationen über mehrere Cluster hinweg zu definieren.
- **Speicherklasse:** Wenn Sie eine Anwendung installieren, die eine Speicherklasse explizit festgelegt hat und Sie die App klonen müssen, muss das Zielcluster für den Klonvorgang die ursprünglich angegebene Speicherklasse haben. Das Klonen einer Applikation mit einer explizit festgelegten Storage-Klasse auf ein Cluster ohne dieselbe Storage-Klasse schlägt fehl.
- **Kubernetes-Ressourcen:** Applikationen, die nicht mit Astra Control gesammelte Kubernetes-Ressourcen verwenden, verfügen unter Umständen nicht über umfassende Funktionen zum App-Datenmanagement. Astra Control sammelt die folgenden Kubernetes-Ressourcen:

ClusterRole	ClusterRoleBinding	ConfigMap
CronJob	CustomResourceDefinition	CustomResource
DaemonSet	DeploymentConfig	HorizontalPodAutoscaler
Ingress	MutatingWebhook	NetworkPolicy
PersistentVolumeClaim	Pod	PodDisruptionBudget
PodTemplate	ReplicaSet	Role
RoleBinding	Route	Secret
Service	ServiceAccount	StatefulSet
ValidatingWebhook		

### Unterstützte Installationsmethoden für Anwendungen

Astra Control unterstützt folgende Installationsmethoden für Anwendungen:

- **Manifest-Datei:** Astra Control unterstützt Apps, die aus einer Manifest-Datei mit kubectl installiert wurden. Beispiel:

```
kubectl apply -f myapp.yaml
```

- **Helm 3:** Wenn Sie Helm zur Installation von Apps verwenden, benötigt Astra Control Helm Version 3. Das Management und Klonen von Apps, die mit Helm 3 installiert sind (oder ein Upgrade von Helm 2 auf Helm 3), werden vollständig unterstützt. Das Verwalten von mit Helm 2 installierten Apps wird nicht unterstützt.
- **Vom Betreiber implementierte Apps:** Astra Control unterstützt Apps, die mit Betreibern mit Namespace-Scoped installiert sind, die im Allgemeinen mit einer "Pass-by-Value"-Architektur statt mit "Pass-by-reference"-Architektur konzipiert sind. Ein Operator und die von ihm zu installierende App müssen denselben Namespace verwenden. Möglicherweise müssen Sie die yaml-Bereitstellungsdatei ändern, um sicherzustellen, dass dies der Fall ist.

Im Folgenden sind einige Bedieneranwendungen aufgeführt, die folgende Muster befolgen:

- ["Apache K8ssandra"](#)



Für K8ssandra werden in-Place-Wiederherstellungsvorgänge unterstützt. Für einen Restore-Vorgang in einem neuen Namespace oder Cluster muss die ursprüngliche Instanz der Applikation ausgefallen sein. Dadurch soll sichergestellt werden, dass die überführten Peer-Group-Informationen nicht zu einer instanzübergreifenden Kommunikation führen. Das Klonen der App wird nicht unterstützt.

- ["Jenkins CI"](#)
- ["Percona XtraDB Cluster"](#)

Astra Control kann einen Operator, der mit einer „Pass-by-reference“-Architektur entworfen wurde, möglicherweise nicht klonen (z.B. der CockroachDB-Operator). Während dieser Art von Klonvorgängen versucht der geklonte Operator, Kubernetes Secrets vom Quelloperator zu beziehen, obwohl er im Zuge des Klonens ein eigenes neues Geheimnis hat. Der Klonvorgang kann fehlschlagen, da Astra Control die Kubernetes-Geheimnisse im Quelloperator nicht kennt.

## Installation von Apps auf dem Cluster

Nachdem Sie den Cluster hinzugefügt haben, können Sie Apps installieren oder vorhandene Apps auf dem Cluster managen. Jede Anwendung, die einem oder mehreren Namespaces zugeordnet ist, kann verwaltet werden.

## Definieren von Apps

Nachdem Astra Control Namespaces auf den Clustern ermittelt hat, können Sie Anwendungen definieren, die Sie managen möchten. Sie können wählen [die als Applikation gemanagt werden sollen, Verwalten einer App, die einen oder mehrere Namespaces umfasst](#) Oder [der als App gemanagt werden soll, Management eines gesamten Namespace als einzelne Applikation](#). All dies kommt auf die Granularität zurück, die Sie für Datensicherungsvorgänge benötigen.

Astra Control ermöglicht es Ihnen zwar, beide Ebenen der Hierarchie (den Namespace und die Apps in diesem Namespace oder den überspannenden Namespaces) separat zu verwalten, aber die beste Vorgehensweise ist es, eine oder andere zu wählen. Aktionen, die Sie in Astra Control nehmen, können fehlschlagen, wenn die Aktionen gleichzeitig sowohl auf Namespace- als auch auf App-Ebene stattfinden.



Beispielsweise könnten Sie eine Backup-Policy für „maria“ setzen, die über ein wöchentliches Kadenz verfügt, aber vielleicht müssen Sie „mariadb“ (die sich im selben Namespace befindet) häufiger sichern. Basierend auf diesen Anforderungen müssen die Applikationen separat gemanagt werden und nicht als Single Namespace App.

### Was Sie benötigen

- Astra Control ist ein Kubernetes Cluster.
- Eine oder mehrere installierte Applikationen auf dem Cluster. [Weitere Informationen zu unterstützten App-Installationsmethoden](#).
- Ein oder mehrere aktive Pods.
- Namespaces sind auf dem Kubernetes-Cluster vorhanden, die Sie Astra Control hinzugefügt haben.
- (Optional) ein Kubernetes-Etikett auf jeder beliebigen ["Unterstützte Kubernetes-Ressourcen"](#).



Eine Bezeichnung ist ein Schlüssel-/Wertpaar, das Sie Kubernetes-Objekten zur Identifizierung zuweisen können. Etiketten erleichtern das Sortieren, Organisieren und Auffinden Ihrer Kubernetes-Objekte. Weitere Informationen zu Kubernetes-Labels: ["In der offiziellen Kubernetes-Dokumentation finden Sie weitere Informationen"](#).

### Über diese Aufgabe

- Bevor Sie beginnen, sollten Sie auch verstehen ["Verwalten von Standard- und Systemnames"](#).
- Wenn Sie in Astra Control mehrere Namespaces mit Ihren Apps verwenden möchten, ["Ändern Sie Benutzerrollen mit Namespace-Einschränkungen"](#) Nach dem Upgrade auf eine Astra Control Center-Version mit Unterstützung für mehrere Namespaces.
- Anweisungen zum Verwalten von Apps mit der Astra Control API finden Sie im ["Astra Automation und API-Informationen"](#).

### Optionen für Applikationsmanagement

- [die als Applikation gemanagt werden sollen](#)
- [der als App gemanagt werden soll](#)

### Definition von Ressourcen, die als Applikation gemanagt werden sollen

Sie können den angeben ["Kubernetes-Ressourcen bilden eine Applikation"](#) Die Sie mit Astra Control verwalten möchten. Durch die Definition einer App können Sie Elemente Ihres Kubernetes Clusters zu einer einzelnen Applikation gruppieren. Diese Sammlung von Kubernetes-Ressourcen ist nach Namespace und Auswahlkriterien für Labels organisiert.

Mit der Definition einer App haben Sie eine granularere Kontrolle über die Auswirkungen einer Astra Control Operation, einschließlich Klonen, Snapshots und Backups.



Stellen Sie bei der Definition von Applikationen sicher, dass Sie keine Kubernetes-Ressource in mehrere Applikationen mit Sicherungsrichtlinien aufnehmen. Überlappende Sicherungsrichtlinien für Kubernetes-Ressourcen können zu Datenkonflikten führen. [Lesen Sie mehr in einem Beispiel](#).

Die Durchführung einer in-Place-Wiederherstellung in einer Anwendung, in der Ressourcen mit einer anderen Anwendung geteilt werden, kann unbeabsichtigte Ergebnisse haben. Alle Ressourcen, die von den Applikationen gemeinsam genutzt werden, werden ersetzt, wenn eine in-Place-Wiederherstellung für eine der Applikationen durchgeführt wird. Das folgende Szenario führt zum Beispiel zu einer unerwünschten Situation bei der Verwendung der NetApp SnapMirror Replizierung:



1. Sie definieren die Anwendung `app1` Verwenden des Namespace `ns1`.
2. Sie konfigurieren eine Replikationsbeziehung für `app1`.
3. Sie definieren die Anwendung `app2` (Auf demselben Cluster) mit den Namespaces `ns1` Und `ns2`.
4. Sie konfigurieren eine Replikationsbeziehung für `app2`.
5. Die Replizierung wird für rückgängig gemacht `app2`. Das verursacht das `app1` App auf dem Quellcluster zu deaktivieren.

### **</strong> über das Hinzufügen von Ressourcen im Cluster-Umfang zu Ihren Namespaces für Apps.**

Außerdem können Sie Clusterressourcen importieren, die den Namespace-Ressourcen zugeordnet sind und die automatisch mit Astra Control integriert sind. Sie können eine Regel hinzufügen, die Ressourcen einer bestimmten Gruppe, Art, Version und optional eine Bezeichnung enthält. Dies sollten Sie tun, wenn Astra Control nicht automatisch Ressourcen enthält.

Sie können keine Ressourcen mit Cluster-Umfang ausschließen, die automatisch von Astra Control enthalten sind.

Sie können Folgendes hinzufügen `apiVersions` (Welche Gruppen sind mit der API-Version kombiniert):

RessourcArt	ApiVersions (Gruppe + Version)
ClusterRole	rbac.authorization.k8s.io/v1
ClusterRoleBinding	rbac.authorization.k8s.io/v1
CustomResource	Apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
CustomResourceDefinition	Apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
MutatingWebhookConfiguration	Zulassungsregistrierung.k8s.io/v1
ValidatingWebhookConfiguration	Zulassungsregistrierung.k8s.io/v1

### Schritte

1. Wählen Sie auf der Seite Anwendungen die Option **Definieren**.
2. Geben Sie im Fenster **Anwendung definieren** den App-Namen ein.
3. Wählen Sie den Cluster aus, auf dem Ihre Anwendung ausgeführt wird, in der Dropdown-Liste \* Cluster\* aus.
4. Wählen Sie aus der Dropdown-Liste **Namespace** einen Namespace für Ihre Anwendung aus.



Apps können mit Astra Control in einem oder mehreren festgelegten Namespaces auf einem einzigen Cluster definiert werden. Eine App kann Ressourcen enthalten, die mehrere Namespaces innerhalb desselben Clusters umfassen. Astra Control unterstützt nicht die Möglichkeit, Applikationen über mehrere Cluster hinweg zu definieren.

5. (Optional) Geben Sie in jedem Namespace ein Etikett für die Kubernetes-Ressourcen ein. Sie können ein einzelnes Etikett oder ein Label-Auswahlkriterium (Abfrage) festlegen.



Weitere Informationen zu Kubernetes-Labels: "[In der offiziellen Kubernetes-Dokumentation finden Sie weitere Informationen](#)".

6. (Optional) Fügen Sie zusätzliche Namespaces für die App hinzu, indem Sie **Namespace hinzufügen** und den Namespace aus der Dropdown-Liste auswählen.
7. (Optional) Geben Sie für alle weiteren Namespaces, die Sie hinzufügen, die Kriterien für eine einzelne Beschriftung oder eine Labelauswahl ein.
8. (Optional) um Ressourcen mit Cluster-Umfang zusätzlich zu den Ressourcen von Astra Control automatisch einzubeziehen, überprüfen Sie **zusätzliche Ressourcen mit Cluster-Umfang** und füllen Sie Folgendes aus:
  - a. Wählen Sie **Add include Rule**.
  - b. **Gruppe**: Wählen Sie aus der Dropdown-Liste die API-Ressourcengruppe aus.
  - c. **Art**: Wählen Sie aus der Dropdown-Liste den Namen des Objektschemas aus.
  - d. **Version**: Geben Sie die API-Version ein.
  - e. **Label selector**: Optional ein Etikett enthalten, das der Regel hinzugefügt werden soll. Mit diesem Etikett werden nur die Ressourcen abgerufen, die diesem Etikett entsprechen. Wenn Sie kein Etikett bereitstellen, sammelt Astra Control alle Instanzen der für diesen Cluster angegebenen Ressourcenkartart.
  - f. Überprüfen Sie die Regel, die auf Ihren Einträgen erstellt wird.
  - g. Wählen Sie **Hinzufügen**.



Sie können die gewünschten Ressourcenregeln mit dem Cluster-Umfang erstellen. Die Regeln werden in der Anwendungsübersicht definieren angezeigt.

9. Wählen Sie **Definieren**.
10. Nachdem Sie **Definieren** ausgewählt haben, wiederholen Sie den Vorgang für andere Apps, je nach Bedarf.

Nachdem Sie die Definition einer App abgeschlossen haben, wird die App in angezeigt **Healthy** Geben Sie in der Liste der Apps auf der Seite Anwendungen an. Sie können sie jetzt klonen und erstellen Backups und Snapshots.



Die gerade hinzugefügte App verfügt möglicherweise über ein Warnsymbol unter der Spalte „geschützt“, das angibt, dass sie nicht gesichert ist und noch keine Backups geplant sind.



Um Details zu einer bestimmten App anzuzeigen, wählen Sie den App-Namen aus.

Um die Ressourcen anzuzeigen, die dieser App hinzugefügt wurden, wählen Sie die Registerkarte **Ressourcen** aus. Wählen Sie in der Spalte Ressource die Nummer nach dem Ressourcennamen aus, oder

geben Sie den Ressourcennamen in die Suche ein, um die zusätzlichen Ressourcen anzuzeigen, die im Cluster enthalten sind.

## Definieren Sie einen Namespace, der als App gemanagt werden soll

Sie können alle Kubernetes-Ressourcen im Namespace zum Astra Control Management hinzufügen, indem Sie die Ressourcen dieses Namespace als Applikation definieren. Diese Methode ist es besser, Apps einzeln zu definieren, wenn Sie alle Ressourcen in einem bestimmten Namespace ähnlich und in gemeinsamen Abständen verwalten und schützen wollen.

### Schritte

1. Wählen Sie auf der Seite Cluster einen Cluster aus.
2. Wählen Sie die Registerkarte **Namespaces** aus.
3. Wählen Sie das Menü Aktionen für den Namespace aus, der die Anwendungsressourcen enthält, die Sie verwalten möchten, und wählen Sie **als Anwendung definieren** aus.



Wenn Sie mehrere Anwendungen definieren möchten, wählen Sie in der Namensliste die Schaltfläche **Aktionen** in der linken oberen Ecke aus und wählen Sie **als Anwendung definieren** aus. Damit werden mehrere einzelne Anwendungen in ihren einzelnen Namespaces definiert. Informationen zu Multi-Namespace-Anwendungen finden Sie unter [die als Applikation gemanagt werden sollen](#).



Aktivieren Sie das Kontrollkästchen **System-Namespaces**, um Systemnamenpaces anzuzeigen, die in der Regel nicht standardmäßig in der App-Verwaltung verwendet werden.



Show system namespaces

["Weitere Informationen"](#).

Nach Abschluss des Prozesses werden die dem Namespace zugeordneten Anwendungen im angezeigt Associated applications Spalte.

## Und wie sieht es mit System-Namespaces aus?

Astra Control erkennt auch Systemnames auf einem Kubernetes Cluster. Wir zeigen Ihnen diese System-Namespaces standardmäßig nicht, da es selten ist, dass Sie die Ressourcen der System-App sichern müssen.

Sie können Systemnames auf der Registerkarte Namespaces für ein ausgewähltes Cluster anzeigen, indem Sie das Kontrollkästchen **System-Namespaces** anzeigen auswählen.



Show system namespaces



Astra Control selbst ist keine Standard-App, sondern eine „System-App“. Sie sollten nicht versuchen, Astra Control selbst zu verwalten. Astra Control selbst wird für das Management nicht standardmäßig angezeigt.

## Beispiel: Separate Sicherheitsrichtlinie für verschiedene Versionen

In diesem Beispiel managt das devops Team eine Implementierung der Version „canary“. Der Cluster des Teams verfügt über drei Pods mit nginx. Zwei der Stative sind der stabilen Freisetzung gewidmet. Der dritte POD ist für den canary Release.



Der Kubernetes Administrator des devops-Teams fügt das Label hinzu `deployment=stable` Zu den stabilen Entriegelungstativen. Das Team fügt das Label hinzu `deployment=canary` Zum canary Release POD.

Die stabile Version des Teams umfasst eine Notwendigkeit für stündliche Snapshots und tägliche Backups. Die version von canary ist kurzlebig, deshalb wollen sie für alles, was gekennzeichnet ist, eine weniger aggressive, kurzfristige Schutzpolitik erstellen `deployment=canary`.

Um mögliche Datenkonflikte zu vermeiden, erstellt der Admin zwei Apps: Eine für die "canary"-Version und eine für die "Stable"-Version. Hierdurch werden Backups, Snapshots und Klonvorgänge für die beiden Gruppen von Kubernetes-Objekten getrennt.

## Weitere Informationen

- ["Verwenden Sie die Astra Control API"](#)
- ["Verwaltung einer Anwendung aufheben"](#)

# Schützen von Applikationen

## Sicherungsübersicht

Mit Astra Control Center können Sie Backups, Klone, Snapshots und Sicherungsrichtlinien für Ihre Applikationen erstellen. Durch das Backup Ihrer Applikationen sind Ihre Services und zugehörigen Daten so verfügbar wie möglich. Bei einem Disaster-Szenario ist durch die Wiederherstellung aus einem Backup die vollständige Recovery einer Applikation und der zugehörigen Daten bei minimalen Unterbrechungen sichergestellt. Backups, Klone und Snapshots schützen vor gängigen Bedrohungen wie Ransomware, versehentlichen Datenverlusten und Umweltnotfällen. ["Informieren Sie sich über die verfügbaren Arten von Datensicherung im Astra Control Center und wann Sie diese einsetzen können"](#).

Darüber hinaus können Sie Applikationen zur Vorbereitung auf das Disaster Recovery auf ein Remote-Cluster replizieren.

## Workflow für Applikationssicherung

Anhand des folgenden Beispielworkflows können Sie Ihre Apps schützen.

### [Eins] Sicherung aller Applikationen

Um sicherzustellen, dass Ihre Apps sofort geschützt sind, ["Erstellen Sie ein manuelles Backup aller Apps"](#).

### [Zwei] Konfigurieren Sie für jede Applikation eine Sicherungsrichtlinie

Zur Automatisierung zukünftiger Backups und Snapshots ["Konfigurieren Sie für jede Applikation eine Sicherungsrichtlinie"](#). Sie können beispielsweise mit wöchentlichen Backups und täglichen Snapshots beginnen und jeweils mit einer Monatsaufbewahrung beginnen. Für manuelle Backups und Snapshots wird dringend die Automatisierung von Backups und Snapshots mit einer Schutzrichtlinie empfohlen.

### [Drittens] Passen Sie die Sicherungsrichtlinien an

Wenn Applikationen und ihre Nutzungsmuster sich ändern, passen Sie die Sicherungsrichtlinien nach Bedarf

an, um einen bestmöglichen Schutz zu gewährleisten.

#### [Vier] Replizieren von Applikationen in einem Remote-Cluster

["Replizierung von Applikationen"](#) Zu einem Remote-Cluster mit NetApp SnapMirror Technologie Astra Control repliziert Snapshots in einen Remote-Cluster und bietet damit asynchrone Disaster Recovery-Funktion.

#### [Fünf] Stellen Sie im Notfall Ihre Applikationen mit dem neuesten Backup oder der neuesten Replizierung auf ein Remote-System wieder her

Im Falle eines Datenverlustes sind Recoverys bis möglich ["Wiederherstellung des aktuellen Backups"](#) Zuerst für jede Anwendung. Sie können dann den letzten Snapshot wiederherstellen (falls verfügbar). Sie können die Replikation zu einem Remote-System verwenden.

## Sichern von Applikationen durch Snapshots und Backups

Alle Applikationen werden gesichert, indem Snapshots und Backups über eine automatisierte Sicherungsrichtlinie oder im Ad-hoc-Verfahren erstellt werden. Sie können die Astra Control Center-UI oder verwenden ["Die Astra Control API"](#) Um Anwendungen zu schützen.

#### Über diese Aufgabe

- **Helm implementierte Apps:** Wenn Sie Helm zum Bereitstellen von Apps verwenden, benötigt Astra Control Center Helm Version 3. Das Management und Klonen von mit Helm 3 bereitgestellten Apps (oder ein Upgrade von Helm 2 auf Helm 3) werden vollständig unterstützt. Mit Helm 2 implementierte Apps werden nicht unterstützt.
- **(nur OpenShift-Cluster) Richtlinien hinzufügen:** Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder Kubernetes-Namespace) eine SecurityContext-UID zugewiesen. Um Astra Control Center zum Schutz Ihrer App zu aktivieren und die App in ein anderes Cluster oder Projekt in OpenShift zu verschieben, müssen Sie Richtlinien hinzufügen, mit denen die App als beliebige UID ausgeführt werden kann. Als Beispiel erteilen die folgenden OpenShift-CLI-Befehle der WordPress-App die entsprechenden Richtlinien.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Sie können die folgenden Aufgaben zum Schutz Ihrer Applikationsdaten ausführen:

- [Konfigurieren einer Sicherungsrichtlinie](#)
- [Erstellen Sie einen Snapshot](#)
- [Erstellen Sie ein Backup](#)
- [Anzeigen von Snapshots und Backups](#)
- [Snapshots löschen](#)
- [Abbrechen von Backups](#)
- [Backups löschen](#)

## 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.

Wenn Sie Backups oder Snapshots öfter als einmal pro Stunde benötigen, können Sie dies tun ["Erstellen Sie mithilfe der Astra Control REST API Snapshots und Backups"](#).

### Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie **Datenschutz**.
3. Wählen Sie **Schutzrichtlinie Konfigurieren**.
4. Legen Sie einen Sicherungszeitplan fest, indem Sie die Anzahl der Snapshots und Backups auswählen, die stündlich, täglich, wöchentlich und monatlich erstellt werden sollen.

Sie können die stündlichen, täglichen, wöchentlichen und monatlichen Zeitpläne gleichzeitig festlegen. Ein Zeitplan wird erst aktiviert, wenn Sie eine Aufbewahrungsstufe festlegen.

Wenn Sie ein Aufbewahrungsniveau für Backups festlegen, können Sie den Bucket auswählen, auf dem Sie die Backups speichern möchten.

Im folgenden Beispiel sind vier Sicherungspläne definiert: Stündlich, täglich, wöchentlich und monatlich für Snapshots und Backups.

**Configure protection policy** STEP 1/2: DETAILS

**PROTECTION SCHEDULE**

Hourly: Every hour on the 0th minute, keep the last 4 snapshots

Daily: Daily at 02:00 (UTC), keep the last 15 snapshots

Weekly: Weekly on Mondays at 02:00 (UTC), keep the last 26 snapshots

Monthly: Every 1st of the month at 02:00 (UTC), keep the last 12 backups

● Hourly ● Daily ● **Weekly** ● Monthly

Select Weekday(s) (optional): Monday X

Time (UTC) (optional): 02:00

– Snapshots to keep 26 +

– Backups to keep 0 +

**BACKUP DESTINATION**

Bucket: ntp-nautilus-bucket-10 - ntp-nautilus-bucket-10 Default

**OVERVIEW**

**Schedule and retention**

Define a policy to continuously protect your application on a schedule and configure a retention count to get started.

For select stateful applications, expect I/O to pause for a short time during a backup or snapshot operation.

Read more in [Protection policies](#)

Application cattle-logging

Namespace cattle-logging

Cluster se-openlab-astra-enterprise-05-se-openlab-astra-enterprise-05-mstr-1

Cancel Review →

5. Wählen Sie **Bewertung**.
6. Wählen Sie **Schutzrichtlinie Festlegen**.

## Ergebnis

Astra Control implementiert die Datensicherungsrichtlinien, indem Snapshots und Backups mithilfe der von Ihnen definierten Zeitplan und Aufbewahrungsrichtlinie erstellt und aufbewahrt werden.

## Erstellen Sie einen Snapshot

Sie können jederzeit einen On-Demand-Snapshot erstellen.

### Schritte

1. Wählen Sie **Anwendungen**.
2. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für die gewünschte App die Option **Snapshot** aus.
3. Passen Sie den Namen des Snapshots an und wählen Sie dann **Weiter**.
4. Überprüfen Sie die Snapshot-Zusammenfassung und wählen Sie **Snapshot**.

## Ergebnis

Der Snapshot-Prozess beginnt. Ein Snapshot ist erfolgreich, wenn der Status in der Spalte **Zustand** auf der Seite **Datenschutz > Snapshots** in der Spalte **Zustand** angegeben ist.

## Erstellen Sie ein Backup

Sie können eine App auch jederzeit sichern.



S3 Buckets im Astra Control Center berichten nicht über die verfügbare Kapazität. Bevor Sie Backups oder Klonanwendungen durchführen, die von Astra Control Center gemanagt werden, sollten Sie die Bucket-Informationen im ONTAP oder StorageGRID Managementsystem prüfen.

### Schritte

1. Wählen Sie **Anwendungen**.
2. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für die gewünschte App die Option **Sichern** aus.
3. Passen Sie den Namen des Backups an.
4. Wählen Sie aus, ob die Anwendung aus einem vorhandenen Snapshot gesichert werden soll. Wenn Sie diese Option auswählen, können Sie aus einer Liste vorhandener Snapshots auswählen.
5. Wählen Sie aus der Liste der Storage-Buckets einen Ziel-Bucket für das Backup aus.
6. Wählen Sie **Weiter**.
7. Überprüfen Sie die Backup-Zusammenfassung und wählen Sie **Backup**.

## Ergebnis

Astra Control erstellt ein Backup der App.



Wenn Ihr Netzwerk ausfällt oder ungewöhnlich langsam ist, kann es zu einer Zeit für einen Backup-Vorgang kommen. Dies führt zum Fehlschlagen der Datensicherung.



Wenn Sie eine laufende Sicherung abbrechen müssen, befolgen Sie die Anweisungen unter [Abbrechen von Backups](#). Um das Backup zu löschen, warten Sie, bis es abgeschlossen ist, und befolgen Sie die Anweisungen unter [Backups löschen](#).



Nach einer Datensicherungsoperation (Klonen, Backup, Restore) und einer anschließenden Anpassung des persistenten Volumes beträgt die Verzögerung bis zu zwanzig Minuten, bevor die neue Volume-Größe in der UI angezeigt wird. Der Datensicherungsvorgang ist innerhalb von Minuten erfolgreich und Sie können mit der Management Software für das Storage-Backend die Änderung der Volume-Größe bestätigen.

## Anzeigen von Snapshots und Backups

Sie können die Snapshots und Backups einer Anwendung auf der Registerkarte Datenschutz anzeigen.

### Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie **Datenschutz**.

Die Snapshots werden standardmäßig angezeigt.

3. Wählen Sie **Backups**, um die Liste der Backups anzuzeigen.

## Snapshots löschen

Löschen Sie die geplanten oder On-Demand Snapshots, die Sie nicht mehr benötigen.



Sie können keinen Snapshot löschen, der derzeit repliziert wird.

### Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie **Datenschutz**.
3. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für den gewünschten Snapshot die Option **Snapshot löschen** aus.
4. Geben Sie das Wort „Löschen“ ein, um das Löschen zu bestätigen und wählen Sie dann **Ja, Snapshot löschen** aus.

### Ergebnis

Astra Control löscht den Snapshot.

## Abbrechen von Backups

Sie können ein gerade einlaufenden Backup abbrechen.



Um ein Backup abzubrechen, muss sich das Backup befinden **Running** Bundesland. Sie können ein Backup, das sich in befindet, nicht abbrechen **Pending** Bundesland.

### Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie **Datenschutz**.
3. Wählen Sie **Backups**.
4. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für das gewünschte Backup die Option **Abbrechen** aus.

5. Geben Sie das Wort „Abbrechen“ ein, um den Vorgang zu bestätigen, und wählen Sie dann **Ja, Sicherung abbrechen** aus.

## Backups löschen

Löschen Sie die geplanten oder On-Demand-Backups, die Sie nicht mehr benötigen.



Wenn Sie eine laufende Sicherung abbrechen müssen, befolgen Sie die Anweisungen unter [Abbrechen von Backups](#). Um das Backup zu löschen, warten Sie, bis es abgeschlossen ist, und befolgen Sie diese Anweisungen.

### Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie **Datenschutz**.
3. Wählen Sie **Backups**.
4. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für das gewünschte Backup die Option **Backup löschen** aus.
5. Geben Sie das Wort „Löschen“ ein, um das Löschen zu bestätigen und wählen Sie dann **Ja, Sicherung löschen**.

### Ergebnis

Astra Control löscht das Backup.

## Wiederherstellung von Applikationen

Astra Control kann Ihre Applikation aus einem Snapshot oder einem Backup wiederherstellen. Das Wiederherstellen aus einem vorhandenen Snapshot erfolgt schneller, wenn die Anwendung auf dasselbe Cluster wiederhergestellt wird. Sie können die Astra Control UI oder verwenden ["Die Astra Control API"](#) Zur Wiederherstellung von Applikationen.



Wenn Sie eine in-Place-Wiederherstellung einer Applikation durchführen, die NetApp ONTAP Storage verwendet, kann der von der wiederhergestellten Applikation verwendete Speicherplatz verdoppelt werden. Nachdem Sie eine in-Place-Wiederherstellung durchgeführt haben, entfernen Sie alle unerwünschten Snapshots aus der wiederhergestellten Applikation, um Speicherplatz freizugeben.

### Über diese Aufgabe

- **Schützen Sie Ihre Apps zuerst:** Es wird dringend empfohlen, einen Schnappschuss von Ihrer Anwendung zu machen oder zu sichern, bevor Sie sie wiederherstellen. Dadurch können Sie den Snapshot oder die Datensicherung klonen, wenn die Wiederherstellung nicht erfolgreich war.
- **Zielvolumen prüfen:** Wenn Sie auf einem anderen Cluster wiederherstellen, stellen Sie sicher, dass der Cluster denselben Zugriffsmodus für persistente Volumes verwendet (z. B. ReadWriteManche). Der Wiederherstellungsvorgang schlägt fehl, wenn der Zugriffsmodus des Ziel-persistenten Volumes anders ist.
- **(nur OpenShift-Cluster) Richtlinien hinzufügen:** Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder Kubernetes-Namespace) eine SecurityContext-UID zugewiesen. Um Astra Control Center zum Schutz Ihrer App zu aktivieren und die App in ein anderes Cluster oder Projekt in OpenShift zu verschieben, müssen Sie Richtlinien hinzufügen, mit denen die App

als beliebige UID ausgeführt werden kann. Als Beispiel erteilen die folgenden OpenShift-CLI-Befehle der WordPress-App die entsprechenden Richtlinien.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

- **Helm implementierte Apps:** Mit Helm 3 implementierte Klon-Apps (oder ein Upgrade von Helm 2 auf Helm 3) werden vollständig unterstützt. Mit Helm 2 implementierte Apps werden nicht unterstützt.

## Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie **Datenschutz**.
3. Wenn Sie von einem Snapshot wiederherstellen möchten, lassen Sie das **Snapshots** -Symbol ausgewählt. Andernfalls wählen Sie das Symbol **Backups** aus, um aus einem Backup wiederherzustellen.
4. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für den Snapshot oder die Datensicherung, aus der Sie wiederherstellen möchten, **Anwendung wiederherstellen** aus.
5. Wählen Sie den Wiederherstellungstyp aus:
  - **Wiederherstellen auf ursprünglichen Namespaces:** Verwenden Sie dieses Verfahren, um die App an Ort und Stelle auf dem ursprünglichen Cluster wiederherzustellen.

Die Durchführung einer in-Place-Wiederherstellung in einer Anwendung, in der Ressourcen mit einer anderen Anwendung geteilt werden, kann unbeabsichtigte Ergebnisse haben. Alle Ressourcen, die von den Applikationen gemeinsam genutzt werden, werden ersetzt, wenn eine in-Place-Wiederherstellung für eine der Applikationen durchgeführt wird. Das folgende Szenario führt zum Beispiel zu einer unerwünschten Situation bei der Verwendung der NetApp SnapMirror Replizierung:



- i. Sie definieren die Anwendung `app1` Verwenden des Namespace `ns1`.
- ii. Sie konfigurieren eine Replikationsbeziehung für `app1`.
- iii. Sie definieren die Anwendung `app2` (Auf demselben Cluster) mit den Namespaces `ns1` Und `ns2`.
- iv. Sie konfigurieren eine Replikationsbeziehung für `app2`.
- v. Die Replizierung wird für rückgängig gemacht `app2`. Das verursacht das `app1` App auf dem Quellcluster zu deaktivieren.

- i. Wählen Sie den Snapshot aus, mit dem die Anwendung wiederhergestellt werden soll, die auf eine frühere Version von selbst zurückgesetzt wird.
- ii. Wählen Sie **Weiter**.



Wenn Sie in einem zuvor gelöschten Namespace wiederherstellen, wird im Rahmen des Wiederherstellungsprozesses ein neuer Namespace mit demselben Namen erstellt. Alle Benutzer, die über Berechtigungen zum Verwalten von Apps im zuvor gelöschten Namespace verfügen, müssen die Rechte für den neu erstellten Namespace manuell wiederherstellen.

- iii. Überprüfen Sie die Details zur Wiederherstellungsaktion, geben Sie „Wiederherstellen“ ein, und wählen Sie **Wiederherstellen**.



- **Wiederherstellen auf neuen Namespaces:** Verwenden Sie dieses Verfahren, um die App auf einem anderen Cluster oder mit verschiedenen Namespaces von der Quelle wiederherzustellen.
  - i. Wählen Sie das Ziel-Cluster für die Anwendung aus, die Sie wiederherstellen möchten.
  - ii. Geben Sie für jeden mit der App verknüpften Quell-Namespace einen Ziel-Namespace ein.



Astra Control erstellt als Teil dieser Wiederherstellungsoption neue Ziel-Namespaces. Die angegebenen Ziel-Namespaces dürfen nicht bereits im Ziel-Cluster vorhanden sein.

- iii. Wählen Sie **Weiter**.
- iv. Wählen Sie den Snapshot aus, mit dem die Anwendung wiederhergestellt werden soll.
- v. Wählen Sie **Weiter**.
- vi. Überprüfen Sie die Details zur Wiederherstellungsaktion und wählen Sie **Wiederherstellen**.

## Ergebnis

Astra Control stellt die App basierend auf den von Ihnen angegebenen Informationen wieder her. Wenn Sie die Applikation bereits wiederhergestellt haben, wird der Inhalt vorhandener persistenter Volumes durch den Inhalt persistenter Volumes aus der wiederhergestellten App ersetzt.



Nach einer Datensicherungsoperation (Klonen, Backup oder Wiederherstellung) und einer anschließenden Anpassung des persistenten Volumes beträgt die Verzögerung bis zu zwanzig Minuten, bevor die neue Volume-Größe in der Web-Benutzeroberfläche angezeigt wird. Der Datensicherungsvorgang ist innerhalb von Minuten erfolgreich und Sie können mit der Management Software für das Storage-Backend die Änderung der Volume-Größe bestätigen.



Jeder Mitgliedsbenutzer mit Namespace-Einschränkungen nach Namespace-Name/ID oder anhand von Namespace-Bezeichnungen kann eine Applikation in einem neuen Namespace im selben Cluster oder einem anderen Cluster in seinem Unternehmenskonto klonen oder wiederherstellen. Derselbe Benutzer kann jedoch nicht auf die geklonte oder wiederhergestellte Anwendung im neuen Namespace zugreifen. Nachdem ein neuer Namespace durch einen Klon- oder Wiederherstellungsvorgang erstellt wurde, kann der Account-Administrator/-Eigentümer das Mitglied-Benutzerkonto bearbeiten und Rolleneinschränkungen für den betroffenen Benutzer aktualisieren, um dem neuen Namespace Zugriff zu gewähren.

## Replizieren von Applikationen auf einem Remote-System mit SnapMirror Technologie

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.

Einen Vergleich zwischen Backups/Wiederherstellungen und der Replizierung finden Sie unter ["Konzepte zur Datensicherung"](#).

Applikationen lassen sich in unterschiedlichen Szenarien replizieren, z. B. nur on-Premises, in Hybrid- und Multi-Cloud-Szenarien:



- On-Premises-Standort A auf On-Premises-Standort B
- On-Premises- und Cloud-Umgebungen mit Cloud Volumes ONTAP
- Cloud mit Cloud Volumes ONTAP auf On-Premises-Umgebungen
- Cloud mit Cloud Volumes ONTAP in die Cloud (zwischen verschiedenen Regionen desselben Cloud-Providers oder verschiedener Cloud-Provider)

Astra Control kann Applikationen über On-Premises-Cluster, On-Premises-Cluster und Cloud (mithilfe von Cloud Volumes ONTAP) oder zwischen Clouds (Cloud Volumes ONTAP auf Cloud Volumes ONTAP) replizieren.



Sie können gleichzeitig eine andere Applikation (auf dem anderen Cluster oder Standort ausgeführt) in die entgegengesetzte Richtung replizieren. So können beispielsweise Applikationen A, B und C von Datacenter 1 nach Datacenter 2 repliziert werden. Applikationen X, Y und Z können von Datacenter 2 zu Datacenter 1 repliziert werden.

Mit Astra Control können Sie die folgenden Aufgaben für die Replikation von Anwendungen ausführen:

- [Richten Sie eine Replikationsbeziehung ein](#)
- [Online-Betrieb einer replizierten App auf dem Ziel-Cluster \(Failover\)](#)
- [Resynchronisierung einer fehlgeschlagenen Überreplikation](#)
- [Replizierung der Applikation wird rückgängig gemacht](#)
- [Führen Sie ein Failback von Anwendungen auf das ursprüngliche Quellcluster durch](#)
- [Löschen einer Replikationsbeziehung für Anwendungen](#)

## Replikationsvoraussetzungen

Die Astra Control Applikationsreplikierung erfordert, dass die folgenden Voraussetzungen erfüllt sein müssen, bevor Sie beginnen:

- Um eine nahtlose Disaster Recovery zu erreichen, empfehlen wir Ihnen, Astra Control Center in einer dritten Fehlerdomäne oder an einem sekundären Standort einzusetzen.
- Das Kubernetes-Cluster der Applikation, ein Ziel-Kubernetes-Cluster, muss zusammen mit den ONTAP-Clustern gemanagt werden, im Idealfall in verschiedenen Ausfall-Domains oder Standorten.
- ONTAP-Cluster und die Host-SVM müssen gekoppelt sein. Siehe ["Übersicht über Cluster- und SVM-Peering"](#).
- Die gepaarte Remote-SVM muss für Astra Trident auf dem Ziel-Cluster verfügbar sein.
- Astra Trident Version 22.07 oder höher muss sowohl auf den Quell- als auch Ziel-ONTAP Clustern vorhanden sein.
- Asynchrone ONTAP SnapMirror Lizenzen mit dem Datensicherungs-Bundle müssen sowohl auf den Quell- als auch auf den Ziel-ONTAP Clustern aktiviert werden. Siehe ["Übersicht über die SnapMirror Lizenzierung in ONTAP"](#).
- Wenn Sie dem Astra Control Center ein ONTAP-Speicher-Backend hinzufügen, wenden Sie die Benutzeranmeldeinformationen auf die Rolle „Admin“ an, die über Zugriffsmethoden verfügt `http` Und `ontapi` Sowohl auf ONTAP Quell- als auch auf Ziel-Clustern aktiviert. Siehe ["Managen von Benutzerkonten in der ONTAP Dokumentation"](#) Finden Sie weitere Informationen.
- Sowohl Quell- als auch Ziel-Kubernetes-Cluster als auch ONTAP-Cluster müssen von Astra Control gemanagt werden.



Sie können gleichzeitig eine andere Applikation (auf dem anderen Cluster oder Standort ausgeführt) in die entgegengesetzte Richtung replizieren. So können beispielsweise Applikationen A, B und C von Datacenter 1 nach Datacenter 2 repliziert werden. Applikationen X, Y und Z können von Datacenter 2 zu Datacenter 1 repliziert werden.

- **Astra Trident / ONTAP Konfiguration:** Astra Control Center erfordert, dass eine Storage-Klasse erstellt und als Standard-Storage-Klasse eingestellt wird. Astra Control Center unterstützt die folgenden ONTAP-Treiber von Astra Trident zur Replizierung:
  - ontap-nas
  - ontap-nas-Flexgroup
  - ontap-san

Erfahren Sie, wie Sie ["Replizieren von Applikationen auf einem Remote-System mit SnapMirror Technologie"](#).

### Richten Sie eine Replikationsbeziehung ein

Die Einrichtung einer Replikationsbeziehung umfasst Folgendes, die die Replikationsrichtlinie enthält;

- Wählen Sie, wie häufig Astra Control einen App Snapshot erstellen soll (einschließlich der Kubernetes-Ressourcen der Applikation und der Volume-Snapshots für die einzelnen Applikations-Volumes).
- Auswahl des Replizierungszeitplans (einschließlich Kubernetes-Ressourcen und persistente Volume-Daten)
- Einstellen der Zeit, die für die Erstellung des Snapshots verwendet werden soll

### Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie auf der Seite Anwendung die Registerkarte **Datenschutz > Replikation** aus.
3. Wählen Sie auf der Registerkarte Data Protection > Replication die Option **Configure Replication Policy** aus. Oder wählen Sie im Feld Anwendungsschutz die Option Aktionen aus, und wählen Sie **Replikationsrichtlinie konfigurieren** aus.
4. Geben Sie die folgenden Informationen ein, oder wählen Sie sie aus:
  - **Zielcluster:** Geben Sie einen Zielcluster ein, der sich von der Quelle unterscheidet.
  - **Zielspeicherklasse:** Wählen Sie die Speicherklasse aus, die die gekoppelte SVM auf dem Ziel-ONTAP-Cluster verwendet.
  - **Replikationstyp:** "Asynchron" ist derzeit der einzige verfügbare Replikationstyp.
  - **Ziel-Namespace:** Geben Sie neue oder vorhandene Ziel-Namespace für das Ziel-Cluster ein.
  - (Optional) Fügen Sie zusätzliche Namespaces hinzu, indem Sie **Namespace hinzufügen** und den Namespace aus der Dropdown-Liste auswählen.
  - **Frequenz der Replikation:** Legen Sie fest, wie oft Astra Control einen Snapshot machen und ihn an sein Ziel replizieren soll.
  - **Offset:** Stellen Sie die Anzahl der Minuten von der Stunde her, die Sie möchten, dass Astra Control einen Schnappschuss machen soll. Möglicherweise möchten Sie einen Offset verwenden, sodass er nicht mit anderen geplanten Vorgängen übereinstimmt. Wenn Sie beispielsweise den Snapshot alle 5 Minuten ab 10:02 Uhr aufnehmen möchten, geben Sie als Offset-Minuten „02“ ein. Das Ergebnis sind 10:02, 10:07, 10:12 usw.
5. Wählen Sie **Weiter**, lesen Sie die Zusammenfassung und wählen Sie **Speichern**.



Zunächst wird der Status „App-Mirror“ angezeigt, bevor der erste Zeitplan stattfindet.

Astra Control erstellt einen Applikations-Snapshot, der für die Replizierung verwendet wird.

6. Um den Snapshot-Status der Anwendung anzuzeigen, wählen Sie die Registerkarte **Anwendungen > Snapshots**.

Der Snapshot-Name verwendet das Format „Replication-Schedule-`<string>`“. Astra Control behält den letzten Snapshot, der für die Replizierung verwendet wurde. Alle älteren Replizierungs-Snapshots werden nach Abschluss der Replikation gelöscht.

## Ergebnis

Dadurch wird die Replikationsbeziehung erstellt.

Astra Control führt die folgenden Maßnahmen durch, die auf dem Aufbau der Beziehung resultieren:

- Erstellt einen Namespace auf dem Ziel (wenn er nicht vorhanden ist)
- Erstellt eine PVC auf dem Ziel-Namespace, der den PVCs der Quell-App entspricht.
- Ersten applikationskonsistenten Snapshot
- Legt mithilfe des ersten Snapshots die SnapMirror Beziehung für persistente Volumes fest

Auf der Seite Datensicherung werden der Status und der Status der Replikationsbeziehung angezeigt:  
<Status> <Lebenszyklus der Beziehung>

Zum Beispiel: Normal

Erfahren Sie am Ende dieses Themas mehr über Replikationszustände und -Status.

## Online-Betrieb einer replizierten App auf dem Ziel-Cluster (Failover)

Mit Astra Control können Sie ein „Failover“ Ihrer replizierten Applikationen auf ein Ziel-Cluster ausführen. Durch dieses Verfahren wird die Replikationsbeziehung angehalten und die App wird auf dem Ziel-Cluster online geschaltet. Durch dieses Verfahren wird die App nicht auf dem Quell-Cluster angehalten, wenn sie betriebsbereit war.

## Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie auf der Seite Anwendung die Registerkarte **Datenschutz > Replikation** aus.
3. Wählen Sie auf der Registerkarte Datenschutz > Replikation im Menü Aktionen die Option **Failover** aus.
4. Überprüfen Sie auf der Seite Failover die Informationen, und wählen Sie **Failover**.

## Ergebnis

Die folgenden Aktionen ergeben sich aus dem Failover-Verfahren:

- Auf dem Ziel-Cluster wird die Applikation basierend auf dem zuletzt replizierten Snapshot gestartet.
- Das Quellcluster und die App (falls betriebsbereit) werden nicht angehalten und werden weiterhin ausgeführt.
- Der Replikationsstatus ändert sich zu „Failover“ und dann zu „Failover“, wenn er abgeschlossen ist.
- Die Schutzrichtlinie der Quell-App wird basierend auf den Zeitplänen in der Quell-App zum Zeitpunkt des

Failover in die Ziel-App kopiert.

- Astra Control zeigt die App sowohl auf den Quell- und Ziel-Clustern und deren jeweiligen Zustand.

## Resynchronisierung einer fehlgeschlagenen Überreplikation

Durch den Neusynchronisierung wird die Replikationsbeziehung wiederhergestellt. Sie können die Quelle der Beziehung auswählen, um die Daten im Quell- oder Ziel-Cluster aufzubewahren. Durch diesen Vorgang werden die SnapMirror Beziehungen neu erstellt, um die Volume-Replizierung in Richtung ihrer Wahl zu starten.

Dabei wird die App auf dem neuen Ziel-Cluster angehalten, bevor die Replizierung neu erstellt wird.



Während der Resynchronisierung wird der Lebenszyklusstatus als „Einrichten“ angezeigt.

### Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie auf der Seite Anwendung die Registerkarte **Datenschutz > Replikation** aus.
3. Wählen Sie auf der Registerkarte Datenschutz > Replikation im Menü Aktionen die Option **Resync** aus.
4. Wählen Sie auf der Seite Resync entweder die Quell- oder Ziel-App-Instanz aus, die die zu bewahrenden Daten enthält.



Wählen Sie die Quelle sorgfältig neu synchronisieren, da die Daten auf dem Ziel überschrieben werden.

5. Wählen Sie **Resync**, um fortzufahren.
6. Geben Sie zur Bestätigung „Resynchronisieren“ ein.
7. Wählen Sie **Ja, Resynchronisierung**, um den Vorgang abzuschließen.

### Ergebnis

- Die Seite „Replikation“ zeigt den Replikationsstatus „Einrichten“ an.
- Astra Control stoppt die Applikation auf dem neuen Ziel-Cluster.
- Astra Control stellt mithilfe der SnapMirror-Resynchronisierung die persistente Volume-Replikation in die ausgewählte Richtung wieder her.
- Auf der Seite Replikation wird die aktualisierte Beziehung angezeigt.

## Replizierung der Applikation wird rückgängig gemacht

Dies ist ein geplanter Vorgang, bei dem die Applikation zum Ziel-Cluster verschoben und anschließend wieder zurück auf das ursprüngliche Quell-Cluster repliziert wird. Astra Control stoppt die Applikation auf dem Quell-Cluster und repliziert die Daten zum Ziel, bevor ein Failover der App zum Ziel-Cluster erfolgt.

In dieser Situation tauschen Sie Quelle und Ziel aus. Der ursprüngliche Quellcluster wird zum neuen Ziel-Cluster, und das ursprüngliche Ziel-Cluster wird zum neuen Quellcluster.

### Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie auf der Seite Anwendung die Registerkarte **Datenschutz > Replikation** aus.
3. Wählen Sie auf der Registerkarte Datenschutz > Replikation im Menü Aktionen die Option **Replikation**

**umkehren** aus.

4. Überprüfen Sie auf der Seite „Replikation umkehren“ die Informationen und wählen Sie zum Fortfahren **Replikation umkehren** aus.

## Ergebnis

Die folgenden Aktionen sind auf das Ergebnis der umgekehrten Replikation zurückzuführen:

- Es wird ein Snapshot der Kubernetes-Ressourcen der ursprünglichen Quell-Applikation erstellt.
- Die PODs der ursprünglichen Quell-App werden mit sanfter Weise gestoppt, indem die Kubernetes-Ressourcen der App gelöscht werden (wodurch PVCs und PVS aktiviert bleiben).
- Nach dem Herunterfahren der Pods werden Snapshots der Volumes der Applikation erstellt und repliziert.
- Die SnapMirror Beziehungen sind beschädigt, wodurch die Zieldatenträger für Lese-/Schreibvorgänge bereit sind.
- Die Kubernetes-Ressourcen der Applikation werden aus dem vor dem Herunterfahren-Snapshot wiederhergestellt. Dabei werden die Volume-Daten repliziert, nachdem die ursprüngliche Quell-App heruntergefahren wurde.
- Die Replizierung wird in umgekehrter Richtung wieder hergestellt.

## Führen Sie ein Failback von Anwendungen auf das ursprüngliche Quellcluster durch

Mit Astra Control können Sie nach einem „Failover“-Vorgang „Failback“ erreichen, indem Sie die folgende Reihenfolge der Vorgänge verwenden. In diesem Workflow repliziert (neu synchronisiert) Astra Control alle Anwendungen, die in die ursprüngliche Replikationsrichtung geändert werden, zurück zum ursprünglichen Quell-Cluster, bevor die Replikationsrichtung umkehrt.

Dieser Prozess beginnt mit einer Beziehung, die ein Failover zu einem Ziel abgeschlossen hat und die folgenden Schritte umfasst:

- Starten Sie mit einem Failover-Status fehlgeschlagen.
- Beziehung neu synchronisieren.
- Die Replikation wird rückgängig gemacht.

## Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie auf der Seite Anwendung die Registerkarte **Datenschutz > Replikation** aus.
3. Wählen Sie auf der Registerkarte Datenschutz > Replikation im Menü Aktionen die Option **Resync** aus.
4. Für einen Fail-Back-Vorgang wählen Sie die Failover-App als Quelle für den Resynchronisierungsvorgang aus (wobei Daten nach dem Failover beim Schreiben beibehalten werden).
5. Geben Sie zur Bestätigung „Resynchronisieren“ ein.
6. Wählen Sie **Ja, Resynchronisierung**, um den Vorgang abzuschließen.
7. Nach Abschluss der Resynchronisierung wählen Sie im Menü Aktionen auf der Registerkarte Data Protection > Replication die Option **Replikation umkehren** aus.
8. Überprüfen Sie auf der Seite „Replikation umkehren“ die Informationen und wählen Sie **Replikation umkehren**.

## Ergebnis

Dies kombiniert die Ergebnisse aus den „Resync“- und „umgekehrten Beziehungs“-Vorgängen, um die

Applikation auf dem ursprünglichen Quell-Cluster online zu schalten und die Replizierung wieder auf das ursprüngliche Ziel-Cluster zu übertragen.

## Löschen einer Replikationsbeziehung für Anwendungen

Das Löschen der Beziehung führt zu zwei separaten Apps ohne Beziehung zwischen ihnen.

### Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie auf der Seite Anwendung die Registerkarte **Datenschutz > Replikation** aus.
3. Wählen Sie auf der Registerkarte Datenschutz > Replikation im Feld Anwendungsschutz oder im Beziehungsdiagramm die Option **Replikationsbeziehung löschen** aus.

### Ergebnis

Die folgenden Aktionen treten beim Löschen einer Replikationsbeziehung auf:

- Wenn die Beziehung aufgebaut ist, aber die App noch nicht auf dem Ziel-Cluster online gestellt wurde (Failover fehlgeschlagen), behält Astra Control während der Initialisierung erstellte PVCs bei, hinterlässt eine „leere“ gemanagte App auf dem Ziel-Cluster und behält die Ziel-App bei, alle Backups zu behalten, die möglicherweise erstellt wurden.
- Wenn die App auf dem Ziel-Cluster online geschaltet wurde (Failover), behält Astra Control PVCs und Ziel-Applikationen bei. Quell- und Zielapplikationen werden jetzt als unabhängige Apps behandelt. Die Backup-Zeitpläne bleiben auf beiden Applikationen, sind jedoch nicht miteinander verknüpft.

## Status des Integritätsstatus der Replikationsbeziehung und Lebenszyklusstatus der Beziehungen

Astra Control zeigt den Zustand der Beziehung und die Zustände des Lebenszyklus der Replikationsbeziehung an.

### Integritätsstatus von Replikationsbeziehungen

Die folgenden Status geben den Zustand der Replikationsbeziehung an:

- **Normal:** Die Beziehung wird entweder hergestellt oder hat sich etabliert, und der jüngste Snapshot wurde erfolgreich übertragen.
- **Warnung:** Die Beziehung wird entweder überschlagen oder ist gescheitert (und somit schützt die Quell-App nicht mehr).
- **\* Kritisch\***
  - Die Beziehung wird erstellt oder fehlgeschlagen, und der letzte Versuch der Abstimmung ist fehlgeschlagen.
  - Die Beziehung wird hergestellt, und der letzte Versuch, die Hinzufügung eines neuen PVC zu vereinbaren, ist gescheitert.
  - Die Beziehung steht fest (also, ein erfolgreicher Snapshot wurde repliziert, und ein Failover ist möglich), aber der neueste Snapshot ist ausgefallen oder zur Replizierung fehlgeschlagen.

### Lebenszyklusstatus der Replikation

Die folgenden Zustände spiegeln die verschiedenen Phasen des Replikationslebenszyklus wider:

- **Aufbau:** Es wird eine neue Replikationsbeziehung erstellt. Astra Control erstellt bei Bedarf einen Namespace, erstellt PVCs (persistente Volume Claims) auf neuen Volumes im Ziel-Cluster und erstellt

SnapMirror Beziehungen. Dieser Status kann auch darauf hinweisen, dass die Replikation neu synchronisiert wird oder die Replikation rückgängig gemacht wird.

- **Etabliert:** Es besteht eine Replikationsbeziehung. Astra Control überprüft regelmäßig, ob die PVCs verfügbar sind, überprüft die Replikationsbeziehung, erstellt regelmäßig Snapshots der App und identifiziert alle neuen Quell-VES in der App. Wenn ja, erstellt Astra Control die Ressourcen, die sie in die Replikation aufnehmen.
- **Failover:** Astra Control durchbricht die SnapMirror Beziehungen und stellt die Kubernetes-Ressourcen der App aus dem letzten erfolgreich replizierten App-Snapshot wieder her.
- **Failover:** Astra Control stoppt die Replizierung vom Quell-Cluster, verwendet den neuesten (erfolgreichen) replizierten App-Snapshot auf dem Ziel und stellt die Kubernetes-Ressourcen wieder her.
- **Resyncing:** Astra Control resynchronisiert die neuen Daten auf der Resynchronisierungsquelle mit SnapMirror Resynchronisierung auf das Resynchronisierungsziel. Bei diesem Vorgang werden möglicherweise einige Daten auf dem Ziel basierend auf der Synchronisationsrichtung überschrieben. Astra Control stoppt die Ausführung der Applikation auf dem Ziel-Namespace und entfernt die Kubernetes App. Während der Resynchronisierung wird der Status als „Einrichten“ angezeigt.
- **Umkehrung:** Der ist der geplante Vorgang, um die Anwendung auf das Ziel-Cluster zu verschieben, während die Replikation zurück zum ursprünglichen Quellcluster fortgesetzt wird. Astra Control stoppt die Anwendung auf dem Quell-Cluster, repliziert die Daten auf dem Ziel, bevor ein Failover über die App zum Ziel-Cluster erfolgt. Während der umgekehrten Replikation wird der Status als „Einrichten“ angezeigt.
- **Löschen:**
  - Wenn die Replikationsbeziehung hergestellt wurde, aber noch nicht Failover durchgeführt wurde, entfernt Astra Control PVCs, die während der Replikation erstellt wurden, und löscht die Ziel-verwaltete App.
  - Wenn die Replikation bereits gescheitert ist, behält Astra Control die PVCs und die Ziel-App bei.

## Klonen und Migrieren von Applikationen

Eine vorhandene Applikation kann geklont werden, um eine doppelte Applikation auf demselben Kubernetes-Cluster oder einem anderen Cluster zu erstellen. Wenn Astra Control eine Applikation klonen, wird ein Klon Ihrer Applikationskonfiguration und des persistenten Storage erstellt.

Das Klonen kann sich leisten, wenn Sie Applikationen und Storage von einem Kubernetes Cluster zu einem anderen verschieben müssen. So möchten Sie beispielsweise Workloads über eine CI/CD-Pipeline und über Kubernetes-Namespaces verschieben. Sie können die Astra Control Center-UI oder verwenden ["Die Astra Control API"](#) Zum Klonen und Migrieren von Applikationen

### Was Sie benötigen

- Um Applikationen in einem anderen Cluster zu klonen, müssen Sie sicherstellen, dass die Cloud-Instanzen, die die Quell- und Ziel-Cluster enthalten (wenn sie nicht identisch sind), einen Standard-Bucket haben. Für jede Cloud-Instanz müssen Sie einen Standard-Bucket zuweisen.
- Während Klonvorgängen müssen Applikationen, die eine Ressource oder Webhooks der ProgresClass benötigen, nicht über die Ressourcen verfügen, die bereits auf dem Ziel-Cluster definiert sind.

Beim Klonen von Applikationen in OpenShift-Umgebungen muss das Astra Control Center OpenShift erlauben, Volumes anzuhängen und die Eigentümerschaft von Dateien zu ändern. Daher müssen Sie eine ONTAP Volume Export-Richtlinie konfigurieren, damit diese Vorgänge möglich sind. Sie können dies mit folgenden Befehlen tun:



1. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sys`
2. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -anon 65534`

### Einschränkungen beim Klonen

- **Explicit Storage class:** Wenn Sie eine App mit einer explizit eingestellten Speicherklasse bereitstellen und die App klonen müssen, muss das Ziel-Cluster über die ursprünglich angegebene Speicherklasse verfügen. Das Klonen einer Applikation mit einer explizit festgelegten Storage-Klasse auf ein Cluster ohne dieselbe Storage-Klasse schlägt fehl.
- **Klone und Benutzerbeschränkungen:** Jeder Mitgliedsbenutzer mit Namespace-Beschränkungen durch Namespace-Name/ID oder durch Namespace-Labels kann eine Anwendung in einem neuen Namespace im selben Cluster oder einem anderen Cluster im Konto ihres Unternehmens klonen oder wiederherstellen. Derselbe Benutzer kann jedoch nicht auf die geklonte oder wiederhergestellte Anwendung im neuen Namespace zugreifen. Nachdem ein neuer Namespace durch einen Klon- oder Wiederherstellungsvorgang erstellt wurde, kann der Account-Administrator/-Eigentümer das Mitglied-Benutzerkonto bearbeiten und Rolleneinschränkungen für den betroffenen Benutzer aktualisieren, um dem neuen Namespace Zugriff zu gewähren.
- **Klone verwenden Standard-Buckets:** Während einer App-Sicherung oder App-Wiederherstellung können Sie optional eine Bucket-ID angeben. Ein Applikationsklonvorgang verwendet jedoch immer den definierten Standard-Bucket. Es besteht keine Möglichkeit, die Buckets für einen Klon zu ändern. Wenn Sie die Kontrolle darüber haben möchten, welcher Bucket verwendet wird, können Sie entweder "[Ändern Sie den Bucket-Standard](#)" Oder machen Sie ein "[Backup](#)" Gefolgt von A "[Wiederherstellen](#)" Separat.
- **Mit Jenkins CI:** Wenn Sie eine vom Betreiber implementierte Instanz von Jenkins CI klonen, müssen Sie die persistenten Daten manuell wiederherstellen. Dies ist eine Einschränkung des Bereitstellungsmodells der Applikation.
- **Mit S3 Buckets:** S3 Buckets im Astra Control Center melden keine verfügbare Kapazität. Bevor Sie Backups oder Klonanwendungen durchführen, die von Astra Control Center gemanagt werden, sollten Sie die Bucket-Informationen im ONTAP oder StorageGRID Managementsystem prüfen.


### OpenShift-Überlegungen

- **Cluster und OpenShift Versionen:** Wenn Sie eine App zwischen Clustern klonen, müssen die Quell- und Ziel-Cluster die gleiche Verteilung von OpenShift sein. Wenn Sie beispielsweise eine App aus einem OpenShift 4.7-Cluster klonen, verwenden Sie ein Ziel-Cluster, das auch OpenShift 4.7 ist.
- **Projekte und UIDs:** Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder Kubernetes-Namespace) eine SecurityContext-UID zugewiesen. Um Astra Control Center zum Schutz Ihrer App zu aktivieren und die App in ein anderes Cluster oder Projekt in OpenShift zu verschieben, müssen Sie Richtlinien hinzufügen, mit denen die App als beliebige UID ausgeführt werden kann. Als Beispiel erteilen die folgenden OpenShift-CLI-Befehle der WordPress-App die entsprechenden Richtlinien.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```



## Schritte

1. Wählen Sie **Anwendungen**.
  2. Führen Sie einen der folgenden Schritte aus:
    - Wählen Sie das Menü Optionen in der Spalte **Aktionen** für die gewünschte App aus.
    - Wählen Sie den Namen der gewünschten App aus, und wählen Sie rechts oben auf der Seite die Dropdown-Liste Status aus.
  3. Wählen Sie **Clone**.
  4. Geben Sie Details für den Klon an:
    - Geben Sie einen Namen ein.
    - Wählen Sie ein Ziel-Cluster für den Klon.
    - Geben Sie die Ziel-Namespaces für den Klon ein. Jeder mit der App verknüpfte Quell-Namespace ordnet den von Ihnen definierten Ziel-Namespace zu.
- 

Astra Control erstellt im Rahmen des Klonvorgangs neue Ziel-Namespaces. Die angegebenen Ziel-Namespaces dürfen nicht bereits im Ziel-Cluster vorhanden sein.
- Wählen Sie **Weiter**.
    - Wählen Sie aus, ob Sie den Klon aus einem vorhandenen Snapshot oder einem vorhandenen Backup erstellen möchten. Wenn Sie diese Option nicht wählen, erstellt Astra Control Center den Klon aus dem aktuellen Status der App.
      - Wenn Sie aus einem vorhandenen Snapshot oder Backup klonen möchten, wählen Sie den Snapshot oder das Backup aus, den Sie verwenden möchten.
  5. Wählen Sie **Weiter**.
  6. Überprüfen Sie die Informationen über den Klon und wählen Sie **Clone**.

## Ergebnis

Astra Control kloniert die App basierend auf den von Ihnen angegebenen Informationen. Der Klonvorgang ist erfolgreich, wenn der neue Applikationsklon ausgeführt wird `Healthy`. Geben Sie auf der Seite **Anwendungen** an.

Nachdem ein neuer Namespace durch einen Klon- oder Wiederherstellungsvorgang erstellt wurde, kann der Account-Administrator/-Eigentümer das Mitglied-Benutzerkonto bearbeiten und Rolleneinschränkungen für den betroffenen Benutzer aktualisieren, um dem neuen Namespace Zugriff zu gewähren.



Nach einer Datensicherungsoperation (Klonen, Backup oder Wiederherstellung) und einer anschließenden Größenanpassung des persistenten Volumes beträgt die Verzögerung bis zu zwanzig Minuten, bevor die neue Volume-Größe in der UI angezeigt wird. Der Datensicherungsvorgang ist innerhalb von Minuten erfolgreich und Sie können mit der Management Software für das Storage-Backend die Änderung der Volume-Größe bestätigen.

## Anwendungsausführungshaken verwalten

Ein Execution Hook ist eine benutzerdefinierte Aktion, die Sie so konfigurieren können, dass sie zusammen mit einem Datenschutzvorgang einer verwalteten App ausgeführt wird. Wenn Sie beispielsweise über eine Datenbank-App verfügen, können Sie mithilfe von Testsuiten alle Datenbanktransaktionen vor dem Snapshot anhalten und die

Transaktionen nach Abschluss des Snapshots fortsetzen. Dies gewährleistet applikationskonsistente Snapshots.

### Arten von Ausführungshaken

Astra Control unterstützt die folgenden Arten von Ausführungshaken, je nachdem, wann sie ausgeführt werden können:

- Vor dem Snapshot
- Nach dem Snapshot
- Vor dem Backup
- Nach dem Backup
- Nach dem Wiederherstellen

### Wichtige Hinweise zu benutzerdefinierten Testausführungshaken

Bei der Planung von Testausführungshooks für Ihre Apps sollten Sie Folgendes berücksichtigen:

- Ein Testsuite muss ein Skript verwenden, um Aktionen durchzuführen. Viele Testsuitehooks können auf dasselbe Skript verweisen.
- Astra Control erfordert, dass die Skripte, mit denen Ausführungshaken ausgeführt werden, im Format ausführbarer Shell-Skripte geschrieben werden.
- Die Skriptgröße ist auf 96 KB begrenzt.
- Astra Control verwendet Hook-Einstellungen für die Ausführung und alle übereinstimmenden Kriterien, um festzustellen, welche Haken für einen Snapshot-, Backup- oder Wiederherstellungsvorgang gelten.
- Alle Fehler bei den Testausführungshaken sind weiche Ausfälle, andere Haken und der Datenschutzvorgang werden immer noch versucht, auch wenn ein Haken ausfällt. Wenn ein Haken jedoch ausfällt, wird ein Warnereignis im Ereignisprotokoll der Seite \* aufgezeichnet.
- Um Testsuiten zu erstellen, zu bearbeiten oder zu löschen, müssen Sie Benutzer mit den Berechtigungen Eigentümer, Administrator oder Mitglied sein.
- Wenn ein Execution Hook länger als 25 Minuten dauert, schlägt der Hook fehl und erstellt einen Ereignisprotokolleintrag mit einem Rückgabecode von „N/A“. Jeder betroffene Snapshot wird als fehlgeschlagen markiert, und ein resultierender Eintrag im Ereignisprotokoll weist auf das Timeout hin.
- Bei Ad-hoc-Datenschutzvorgängen werden alle Hook-Ereignisse im Ereignisprotokoll auf der Seite \* erzeugt und gespeichert. Bei geplanten Datenschutzvorgängen werden jedoch nur Hook-Failure-Ereignisse im Ereignisprotokoll aufgezeichnet (Ereignisse, die von den geplanten Datenschutzvorgängen selbst generiert werden, werden noch aufgezeichnet).



- Wenn Sie einen Testsuite-Haken für eine Anwendung erstellen, die an einem Istio-Service-Netz teilnimmt, stellen Sie sicher, dass der Haken gegen den ursprünglichen Anwendungscontainer und nicht den Service-Mesh-Container ausgeführt wird. Sie können Istio Service-Mesh-Container ausschließen, indem Sie einen Filter-Regex auf jeden Ausführungshaken anwenden, der für Anwendungen ausgeführt wird, die ein Istio-Service-Mesh verwenden.
- Da die Testsuitehingel die Funktionalität der Anwendung, für die sie ausgeführt werden, oft reduzieren oder vollständig deaktivieren, sollten Sie immer versuchen, die Zeit zu minimieren, die Ihre benutzerdefinierten Testausführungshaken für die Ausführung benötigt.
- Wenn Sie eine Backup- oder Snapshot-Operation mit zugeordneten Testsuiten starten, diese aber dann abbrechen, können die Haken trotzdem ausgeführt werden, wenn der Backup- oder Snapshot-Vorgang bereits gestartet wurde. Das bedeutet, dass ein Testinaper nach dem Backup nicht davon ausgehen kann, dass die Sicherung abgeschlossen wurde.

### Ausführungsreihenfolge

Wenn ein Datenschutzvorgang ausgeführt wird, finden Hakenereignisse in der folgenden Reihenfolge statt:

1. Alle entsprechenden benutzerdefinierten Testhaken für die Ausführung vor dem Betrieb werden auf den entsprechenden Containern ausgeführt. Sie können beliebig viele benutzerdefinierte Hooks für die Vorbedienung erstellen und ausführen, aber die Reihenfolge der Ausführung dieser Haken vor der Operation ist weder garantiert noch konfigurierbar.
2. Der Vorgang der Datensicherung wird durchgeführt.
3. Alle entsprechenden benutzerdefinierten Testhaken für die Ausführung nach der Operation werden auf den entsprechenden Containern ausgeführt. Sie können beliebig viele benutzerdefinierte Haken für die Nachbearbeitung erstellen und ausführen, aber die Reihenfolge der Ausführung dieser Haken nach der Operation ist weder garantiert noch konfigurierbar.

Wenn Sie mehrere Testausführungshaken desselben Typs erstellen (z. B. Pre-Snapshot), ist die Reihenfolge der Ausführung dieser Haken nicht garantiert. Die Reihenfolge der Ausführung von Haken unterschiedlicher Art ist jedoch garantiert. So würde beispielsweise die Reihenfolge der Ausführung einer Konfiguration mit allen fünf verschiedenen Hooks aussehen:

1. Hooks vor dem Backup wurden ausgeführt
2. Hooks vor dem Snapshot wurden ausgeführt
3. Hooks nach dem Snapshot wurden ausgeführt
4. Hooks nach dem Backup ausgeführt
5. Haken nach der Wiederherstellung ausgeführt

Ein Beispiel für diese Konfiguration finden Sie in Szenario 2 aus der Tabelle in [ob ein Haken läuft](#).



Sie sollten Ihre Hook-Skripte immer testen, bevor Sie sie in einer Produktionsumgebung aktivieren. Mit dem Befehl 'kubectl exec' können Sie die Skripte bequem testen. Nachdem Sie die Testausführungshaken in einer Produktionsumgebung aktiviert haben, testen Sie die erstellten Snapshots und Backups, um sicherzustellen, dass sie konsistent sind. Dazu klonen Sie die Applikation in einem temporären Namespace, stellen den Snapshot oder das Backup wieder her und testen anschließend die App.

## Bestimmen Sie, ob ein Haken läuft

Verwenden Sie die folgende Tabelle, um zu ermitteln, ob ein benutzerdefinierter Testsuite für Ihre Anwendung ausgeführt wird.

Alle grundlegenden Applikationsvorgänge müssen eine der grundlegenden Vorgänge – Snapshot, Backup oder Wiederherstellung – ausgeführt werden. Je nach Szenario kann ein Klonvorgang aus verschiedenen Kombinationen dieser Operationen bestehen, sodass die Ausführungsooks für einen Klonvorgang variieren.

Für Wiederherstellungen ohne Backup ist ein vorhandener Snapshot oder Backup erforderlich, sodass bei diesen Vorgängen keine Snapshot- oder Backup-Hooks ausgeführt werden.



Wenn Sie starten, aber dann brechen Sie ein Backup, das einen Snapshot enthält und es sind zugewiesene Testausführungshaken, einige Haken laufen, und andere möglicherweise nicht. Das bedeutet, dass ein Testinaper nach dem Backup nicht davon ausgehen kann, dass die Sicherung abgeschlossen wurde. Beachten Sie die folgenden Punkte für abgebrochene Backups mit zugehörigen Testsuiten:

- Die Hooks vor dem Backup und nach dem Backup laufen immer.
- Wenn das Backup einen neuen Snapshot enthält und der Snapshot gestartet wurde, werden die Hooks vor dem Snapshot und nach dem Snapshot ausgeführt.
- Wenn die Sicherung vor dem Start des Snapshots abgebrochen wird, werden die Hooks vor dem Snapshot und nach dem Snapshot nicht ausgeführt.

Szenario	Betrieb	Vorhandener Snapshot	Vorhandenes Backup	Namespace	Cluster	Snapshot Hooks laufen	Backup Hooks laufen	Hooks Run wiederherstellen
1	Klon	N	N	Neu	Gleich	Y	N	Y
2	Klon	N	N	Neu	Anders	Y	Y	Y
3	Klonen oder Wiederherstellen	Y	N	Neu	Gleich	N	N	Y
4	Klonen oder Wiederherstellen	N	Y	Neu	Gleich	N	N	Y
5	Klonen oder Wiederherstellen	Y	N	Neu	Anders	N	Y	Y
6	Klonen oder Wiederherstellen	N	Y	Neu	Anders	N	N	Y
7	Wiederherstellen	Y	N	Vorhanden	Gleich	N	N	Y

Szenario	Betrieb	Vorhandener Snapshot	Vorhandenes Backup	Namespace	Cluster	Snapshot Hooks laufen	Backup Hooks laufen	Hooks Run wiederherstellen
8	Wiederherstellen	N	Y	Vorhanden	Gleich	N	N	Y
9	Snapshot	K. A.	K. A.	K. A.	K. A.	Y	K. A.	K. A.
10	Backup	N	K. A.	K. A.	K. A.	Y	Y	K. A.
11	Backup	Y	K. A.	K. A.	K. A.	N	Y	K. A.

## Beispiele für Testausführungshaken

Besuchen Sie das ["NetApp Verda GitHub Projekt"](#) Um Beispiele zu sehen und eine Vorstellung davon zu bekommen, wie Sie Ihre Ausführungshaken strukturieren. Sie können diese Beispiele als Vorlagen oder Testskripte verwenden.

## Vorhandene Testsuiten anzeigen

Sie können vorhandene benutzerdefinierte Testsuiten für eine App anzeigen.

### Schritte

1. Gehen Sie zu **Anwendungen** und wählen Sie dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.

In der Ergebnisliste können Sie alle aktivierten oder deaktivierten Testausführungshaken anzeigen. Sie sehen den Status, die Quelle und den Ablauf eines Hakens (vor oder nach dem Betrieb). Um Ereignisprotokolle zu den Testausführungshaken anzuzeigen, gehen Sie zur Seite **Aktivität** im linken Navigationsbereich.

## Vorhandene Skripte anzeigen

Sie können die bereits hochgeladenen Skripte anzeigen. Auf dieser Seite können Sie auch sehen, welche Skripte verwendet werden und welche Haken sie verwenden.

### Schritte

1. Gehen Sie zu **Konto**.
2. Wählen Sie die Registerkarte **Skripts** aus.

Auf dieser Seite sehen Sie eine Liste mit bereits hochgeladenen Skripten. Die Spalte **used by** zeigt an, welche Testsuitehooks die einzelnen Skripte verwenden.

## Fügen Sie ein Skript hinzu

Sie können einen oder mehrere Skripte hinzufügen, auf die Testausführungshaken verweisen können. Viele Testsuitehooks können auf dasselbe Skript verweisen. So können Sie viele Testsuiten aktualisieren, indem Sie nur ein Skript ändern.

### Schritte

1. Gehen Sie zu **Konto**.

2. Wählen Sie die Registerkarte **Skripts** aus.
3. Wählen Sie **Hinzufügen**.
4. Führen Sie einen der folgenden Schritte aus:
  - Laden Sie ein benutzerdefiniertes Skript hoch.
    - i. Wählen Sie die Option **Datei hochladen**.
    - ii. Navigieren Sie zu einer Datei, und laden Sie sie hoch.
    - iii. Geben Sie dem Skript einen eindeutigen Namen.
    - iv. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.
    - v. Wählen Sie **Skript speichern**.
  - Fügen Sie in ein benutzerdefiniertes Skript aus der Zwischenablage ein.
    - i. Wählen Sie die Option **Einfügen oder Typ** aus.
    - ii. Wählen Sie das Textfeld aus, und fügen Sie den Skripttext in das Feld ein.
    - iii. Geben Sie dem Skript einen eindeutigen Namen.
    - iv. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.
5. Wählen Sie **Skript speichern**.

## Ergebnis

Das neue Skript erscheint in der Liste auf der Registerkarte **Scripts**.

## Ein Skript löschen

Sie können ein Skript aus dem System entfernen, wenn es nicht mehr benötigt wird und nicht von Testsuiten verwendet wird.

## Schritte

1. Gehen Sie zu **Konto**.
2. Wählen Sie die Registerkarte **Skripts** aus.
3. Wählen Sie ein Skript aus, das Sie entfernen möchten, und wählen Sie das Menü in der Spalte **Aktionen** aus.
4. Wählen Sie **Löschen**.



Wenn das Skript mit einem oder mehreren Testsuiten verknüpft ist, ist die Aktion **Löschen** nicht verfügbar. Um das Skript zu löschen, bearbeiten Sie zunächst die zugehörigen Testausführungshaken und ordnen Sie sie einem anderen Skript zu.

## Erstellen Sie einen benutzerdefinierten Testsuite-Haken

Sie können einen benutzerdefinierten Testsuite-Haken für eine App erstellen. Siehe [Beispiele für Testausführungshaken](#) Beispiele für Haken. Sie müssen über die Berechtigungen Eigentümer, Administrator oder Mitglied verfügen, um Testausführungshaken zu erstellen.



Wenn Sie ein benutzerdefiniertes Shell-Skript erstellen, das als Execution Hook verwendet werden soll, denken Sie daran, die entsprechende Shell am Anfang der Datei anzugeben, es sei denn, Sie führen bestimmte Befehle aus oder geben den vollständigen Pfad zu einer ausführbaren Datei an.

## Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie **Hinzufügen**.
4. Legen Sie im Bereich **Hook Details** fest, wann der Haken ausgeführt werden soll, indem Sie im Dropdown-Menü **Operation** einen Operationstyp auswählen.
5. Geben Sie einen eindeutigen Namen für den Haken ein.
6. (Optional) Geben Sie alle Argumente ein, um während der Ausführung an den Haken weiterzuleiten. Drücken Sie nach jedem eingegebenen Argument die Eingabetaste, um jedes Argument aufzuzeichnen.
7. Wenn der Haken im Bereich **Container Images** auf alle Container-Bilder in der Anwendung laufen soll, aktivieren Sie das Kontrollkästchen **auf alle Container-Bilder** anwenden. Sollte der Haken stattdessen nur auf ein oder mehrere angegebene Container-Images wirken, geben Sie die Container-Bildnamen in das Feld **Container-Bildnamen ein, die mit** übereinstimmen.
8. Führen Sie im Bereich **Script** einen der folgenden Schritte aus:
  - Fügen Sie ein neues Skript hinzu.
    - i. Wählen Sie **Hinzufügen**.
    - ii. Führen Sie einen der folgenden Schritte aus:
      - Laden Sie ein benutzerdefiniertes Skript hoch.
        - I. Wählen Sie die Option **Datei hochladen**.
        - II. Navigieren Sie zu einer Datei, und laden Sie sie hoch.
        - III. Geben Sie dem Skript einen eindeutigen Namen.
        - IV. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.
        - V. Wählen Sie **Skript speichern**.
      - Fügen Sie in ein benutzerdefiniertes Skript aus der Zwischenablage ein.
        - I. Wählen Sie die Option **Einfügen oder Typ** aus.
        - II. Wählen Sie das Textfeld aus, und fügen Sie den Skripttext in das Feld ein.
        - III. Geben Sie dem Skript einen eindeutigen Namen.
        - IV. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.
    - Wählen Sie ein vorhandenes Skript aus der Liste aus.

Hiermit wird der Testsuitelink angewiesen, dieses Skript zu verwenden.

9. Wählen Sie **Haken hinzufügen**.

## Überprüfen Sie den Status eines Testablaufanhänges

Nachdem ein Snapshot-, Backup- oder Wiederherstellungsvorgang abgeschlossen wurde, können Sie den Status der Testsuiten überprüfen, die im Rahmen des Vorgangs ausgeführt wurden. Mit diesen Statusinformationen können Sie festlegen, ob der Testsuite beibehalten, geändert oder gelöscht werden soll.

## Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.

2. Wählen Sie die Registerkarte **Datenschutz** aus.
3. Wählen Sie **Snapshots** aus, um die laufenden Snapshots zu sehen, oder **Backups**, um die laufenden Backups zu sehen.

Der **Hook-Status** zeigt den Status der Ausführung Hakenlauf nach Abschluss des Vorgangs an. Sie können den Mauszeiger auf den Status bewegen, um weitere Details zu erhalten. Wenn z. B. beim Snapshot Fehler beim Ausführen von Hakenabfällen auftreten, wird beim Mauszeiger über den Hakenzustand für diesen Snapshot eine Liste mit fehlgeschlagenen Testsuitehaken angezeigt. Um die Gründe für jeden Fehler zu sehen, können Sie die Seite **Aktivität** im linken Navigationsbereich überprüfen.

## Skriptverwendung anzeigen

In der Web-Benutzeroberfläche von Astra Control können Sie sehen, welche Testausführungshaken ein bestimmtes Skript verwenden.

### Schritte

1. Wählen Sie **Konto**.
2. Wählen Sie die Registerkarte **Skripts** aus.

Die Spalte **used by** in der Liste der Skripte enthält Details darüber, welche Haken die einzelnen Skripte in der Liste verwenden.

3. Wählen Sie die Informationen in der Spalte **used by** für ein Skript aus, das Sie interessieren.

Eine detailliertere Liste mit den Namen der Haken, die das Skript verwenden, und der Art der Operation, mit der sie konfiguriert sind.

## Deaktivieren Sie einen Testsuite-Haken

Sie können einen Testsuite-Hook deaktivieren, wenn Sie ihn vorübergehend vor oder nach einem Snapshot einer App nicht ausführen möchten. Sie müssen über die Berechtigung Eigentümer, Administrator oder Mitglied verfügen, um Testsuiten zu deaktivieren.

### Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie in der Spalte **Aktionen** das Menü Optionen für einen Haken, den Sie deaktivieren möchten.
4. Wählen Sie **Deaktivieren**.

## Löschen Sie einen Testsuite-Haken

Sie können einen Execution Hook ganz entfernen, wenn Sie ihn nicht mehr benötigen. Sie müssen über die Berechtigung Eigentümer, Administrator oder Mitglied verfügen, um Testausführungshaken zu löschen.

### Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie in der Spalte **Aktionen** das Menü Optionen für einen Haken, den Sie löschen möchten.
4. Wählen Sie **Löschen**.



## Finden Sie weitere Informationen

- ["NetApp Verda GitHub Projekt"](#)

# Monitoring des Applikations- und Cluster-Systemzustands

## Zeigen Sie eine Zusammenfassung des Applikations- und Cluster-Zustands an

Wählen Sie das **Dashboard** aus, um eine übergeordnete Ansicht Ihrer Apps, Cluster, Storage-Back-Ends und deren Integrität anzuzeigen.

Dabei handelt es sich nicht nur um statische Zahlen oder Statusangaben, sondern Sie können von jedem einzelnen Detail aus darauf aufgehen. Wenn Apps beispielsweise nicht vollständig geschützt sind, können Sie mit dem Mauszeiger auf das Symbol zeigen, um zu ermitteln, welche Apps nicht vollständig geschützt sind. Dies gibt einen Grund dafür.

### Auf Applikationen Kachel

Mit der Kachel \* Applications\* können Sie Folgendes identifizieren:

- Wie viele Applikationen managen Sie aktuell mit Astra?
- Ob diese verwalteten Apps gesund sind.
- Gibt an, ob die Applikationen vollständig gesichert sind (sie sind geschützt, wenn neueste Backups verfügbar sind).
- Die Anzahl der Anwendungen, die erkannt, aber noch nicht verwaltet wurden.

Idealerweise wäre diese Zahl null, da Sie Apps nach dem Entstehen verwalten oder ignorieren würden. Anschließend sollten Sie die Anzahl der im Dashboard ermittelten Apps überwachen, um zu ermitteln, wann Entwickler neue Apps zu einem Cluster hinzufügen.

### Cluster-Tile

Die Kachel **Cluster** bietet ähnliche Details über die Integrität der Cluster, die Sie mit dem Astra Control Center verwalten, und Sie können detaillierte Informationen abrufen, wie Sie es mit einer App möglich sind.

### Storage Back-Ends

Die Kachel **Storage Back-Ends** enthält Informationen, die Ihnen bei der Identifizierung des Zustands von Storage-Back-Ends helfen. Dazu gehören:

- Wie viele Storage-Back-Ends werden gemanagt
- Gibt an, ob diese gemanagten Backends gesund sind
- Gibt an, ob die Back-Ends vollständig geschützt sind
- Die Anzahl der Back-Ends, die zwar erkannt, aber noch nicht gemanagt werden.

## Zeigen Sie den Cluster-Zustand an und managen Sie Storage-Klassen

Nachdem Sie Cluster hinzugefügt haben, die von Astra Control Center gemanagt werden können, können Sie Details zum Cluster anzeigen, beispielsweise den Speicherort, die

Worker-Nodes, die persistenten Volumes und die Storage-Klassen. Sie können auch die Standard-Storage-Klasse für verwaltete Cluster ändern.

### Zeigen Sie den Cluster-Zustand und die Details an

Sie können Details zum Cluster anzeigen, z. B. seinen Standort, die Worker-Nodes, persistente Volumes und Storage-Klassen.

#### Schritte

1. Wählen Sie in der Astra Control Center-Benutzeroberfläche **Cluster** aus.
2. Wählen Sie auf der Seite **Cluster** den Cluster aus, dessen Details Sie anzeigen möchten.



Wenn ein Cluster vorhanden ist `removed` Der Zustand der Cluster- und Netzwerk-Konnektivität erscheint jedoch ordnungsgemäß (externe Versuche, mit Kubernetes-APIs erfolgreich auf das Cluster zuzugreifen, sind dennoch erfolgreich), ist das Kubeconfig, das Sie Astra Control zur Verfügung gestellt haben, möglicherweise nicht mehr gültig. Dies kann an einer Zertifikatrotation oder einem Ablaufdatum im Cluster liegen. Um dieses Problem zu beheben, aktualisieren Sie die Anmeldeinformationen, die mit dem Cluster in Astra Control verbunden sind, mithilfe des ["Astra Control API"](#).

3. Zeigen Sie die Informationen auf den Registerkarten **Übersicht**, **Speicher** und **Aktivität** an, um die gewünschten Informationen zu finden.
  - **Übersicht**: Details zu den Arbeiterknoten, einschließlich ihres Status.
  - **Storage**: Die persistenten Volumes, die mit dem Computing verbunden sind, einschließlich der Speicherklasse und des Status.
  - **Aktivität**: Zeigt die Aktivitäten im Zusammenhang mit dem Cluster an.



Sie können auch Clusterinformationen anzeigen, die Sie über das Astra Control Center **Dashboard** starten. Auf der Registerkarte **Cluster** unter **Resource summary** können Sie die verwalteten Cluster auswählen, die Sie zur Seite **Cluster** führen. Nachdem Sie die Seite **Cluster** aufgerufen haben, befolgen Sie die oben beschriebenen Schritte.

### Ändern der Standard-Storage-Klasse

Sie können die Standard-Storage-Klasse für ein Cluster ändern. Wenn Astra Control einen Cluster verwaltet, wird die Standard-Storage-Klasse des Clusters überwacht.



Ändern Sie die Storage-Klasse nicht mit `kubectl`-Befehlen. Verwenden Sie stattdessen diese Prozedur. Astra Control setzt die Änderungen zurück, wenn sie mit `kubectl` vorgenommen werden.

#### Schritte

1. Wählen Sie in der Web-UI des Astra Control Center die Option **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**.

## Anzeigen des Funktionszustands und der Details einer App

Nachdem Sie mit dem Management einer Applikation begonnen haben, stellt Astra Control Details zur App bereit, mit der Sie ihren Status (unabhängig davon, ob sie sich gesund ist), ihren Sicherungsstatus (ob sie im Falle eines Ausfalls vollständig geschützt ist), die Behälter, den persistenten Storage und vieles mehr ermitteln können.

### Schritte

1. Wählen Sie in der Astra Control Center-UI **Anwendungen** und dann den Namen einer App aus.
2. Überprüfen Sie die Informationen.
  - **App-Status:** Gibt einen Status an, der den Status der App in Kubernetes wiedergibt. Sind Pods und persistente Volumes beispielsweise online? Wenn eine Applikation fehlerhaft ist, müssen Sie mit den Kubernetes-Protokollen zum Beheben des Problems im Cluster wechseln. Astra stellt keine Informationen zur Verfügung, die Ihnen bei der Behebung einer defekten App helfen.
  - **App Protection Status:** Gibt einen Status, wie gut die App geschützt ist:
    - **Vollständig geschützt:** Die App verfügt über einen aktiven Backup-Zeitplan und ein erfolgreiches Backup, das weniger als eine Woche alt ist
    - **Teilweise geschützt:** Die App verfügt über einen aktiven Backup-Zeitplan, einen aktiven Snapshot-Zeitplan oder einen erfolgreichen Backup oder Snapshot
    - **Ungeschützt:** Apps, die weder vollständig geschützt noch teilweise geschützt sind.

\_\_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 herauswischt und es sich um den persistenten Storage handelt, muss das Backup wiederhergestellt werden. Ein Snapshot würde es Ihnen nicht ermöglichen, eine Wiederherstellung durchzuführen.
  - **Übersicht:** Informationen über den Zustand der Pods, die mit der App verbunden sind.
  - **Datenschutz:** Ermöglicht die Konfiguration einer Datenschutzrichtlinie und die Anzeige der vorhandenen Snapshots und Backups.
  - **Storage:** Zeigt dir die persistenten Volumes auf App-Ebene. Der Zustand eines persistenten Volumes befindet sich aus der Perspektive des Kubernetes Clusters.
  - **Ressourcen:** Ermöglicht es Ihnen, zu überprüfen, welche Ressourcen gesichert und verwaltet werden.
  - **Aktivität:** Zeigt die Aktivitäten im Zusammenhang mit der App an.



Sie können auch App-Informationen ab dem Astra Control Center **Dashboard** anzeigen. Auf der Registerkarte **Anwendungen** unter **Ressourcenzusammenfassung** können Sie die verwalteten Apps auswählen, die Sie zur Seite **Anwendungen** führen. Nachdem Sie die Seite **Applikationen** aufgerufen haben, befolgen Sie die oben beschriebenen Schritte.

## Konto verwalten

### Managen Sie lokale Benutzer und Rollen

Sie können Benutzer Ihrer Astra Control Center-Installation über die Astra Control-

Benutzeroberfläche hinzufügen, entfernen und bearbeiten. Sie können die Astra Control UI oder verwenden ["Die Astra Control API"](#) Um Benutzer zu managen.

Sie können LDAP auch zur Authentifizierung für ausgewählte Benutzer verwenden.

## LDAP verwenden

LDAP ist ein branchenübliches Protokoll für den Zugriff auf verteilte Verzeichnisinformationen und eine beliebte Wahl für die Unternehmensauthentifizierung. Sie können Astra Control Center mit einem LDAP-Server verbinden, um die Authentifizierung für ausgewählte Astra Control-Benutzer durchzuführen. Auf hohem Niveau beinhaltet die Konfiguration die Integration von Astra mit LDAP und die Definition der Astra Control Benutzer und Gruppen entsprechend der LDAP-Definitionen. Sie können die Astra Control API oder die Web-Benutzeroberfläche verwenden, um die LDAP-Authentifizierung und LDAP-Benutzer und -Gruppen zu konfigurieren. Weitere Informationen finden Sie in der folgenden Dokumentation:

- ["Mit der Astra Control API können Sie die Remote-Authentifizierung und -Benutzer verwalten"](#)
- ["Verwenden Sie die Astra Control-Benutzeroberfläche, um Remote-Benutzer und -Gruppen zu verwalten"](#)
- ["Verwenden Sie die Astra Control-Benutzeroberfläche, um die Remote-Authentifizierung zu verwalten"](#)

## Benutzer hinzufügen

Kontoinhaber und -Administratoren können weitere Benutzer zur Installation des Astra Control Center hinzufügen.

### Schritte

1. Wählen Sie im Navigationsbereich \* Konto verwalten\* die Option **Konto**.
2. Wählen Sie die Registerkarte **Benutzer** aus.
3. Wählen Sie **Benutzer Hinzufügen**.
4. Geben Sie den Namen des Benutzers, die E-Mail-Adresse und ein temporäres Kennwort ein.

Der Benutzer muss das Passwort bei der ersten Anmeldung ändern.

5. Wählen Sie eine Benutzerrolle mit den entsprechenden Systemberechtigungen aus.

Jede Rolle bietet die folgenden Berechtigungen:

- 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.
6. Um einem Benutzer mit einer Mitglied- oder Viewer-Rolle Einschränkungen hinzuzufügen, aktivieren Sie das Kontrollkästchen \* Rolle auf Einschränkungen beschränken\*.

Weitere Informationen zum Hinzufügen von Einschränkungen finden Sie unter ["Managen Sie lokale Benutzer und Rollen"](#).

7. Wählen Sie **Hinzufügen**.

## Passwörter verwalten

Sie können Passwörter für Benutzerkonten im Astra Control Center verwalten.

### Passwort ändern

Sie können das Passwort Ihres Benutzerkontos jederzeit ändern.

#### Schritte

1. Klicken Sie oben rechts auf dem Bildschirm auf das Symbol Benutzer.
2. Wählen Sie **Profil**.
3. Wählen Sie im Menü Optionen in der Spalte **Aktionen** die Option **Passwort ändern** aus.
4. Geben Sie ein Passwort ein, das den Anforderungen des Passworts entspricht.
5. Geben Sie das Kennwort zur Bestätigung erneut ein.
6. Wählen Sie **Passwort ändern**.

### Kennwort eines anderen Benutzers zurücksetzen

Wenn Ihr Konto über Berechtigungen für die Administrator- oder Eigentümerrolle verfügt, können Sie Passwörter für andere Benutzerkonten sowie für Ihre eigenen zurücksetzen. Wenn Sie ein Kennwort zurücksetzen, weisen Sie ein temporäres Kennwort zu, das der Benutzer bei der Anmeldung ändern muss.

#### Schritte

1. Wählen Sie im Navigationsbereich \* Konto verwalten\* die Option **Konto**.
2. Wählen Sie die Dropdown-Liste **Aktionen** aus.
3. Wählen Sie **Passwort Zurücksetzen**.
4. Geben Sie ein temporäres Kennwort ein, das den Anforderungen des Passworts entspricht.
5. Geben Sie das Kennwort zur Bestätigung erneut ein.



Wenn sich der Benutzer beim nächsten Mal anmeldet, wird er aufgefordert, das Passwort zu ändern.

6. Wählen Sie **Passwort zurücksetzen**.

## Benutzer entfernen

Benutzer mit der Eigentümer- oder Administratorrolle können jederzeit andere Benutzer aus dem Konto entfernen.

#### Schritte

1. Wählen Sie im Navigationsbereich \* Konto verwalten\* die Option **Konto**.
2. Aktivieren Sie auf der Registerkarte **Benutzer** das Kontrollkästchen in der Zeile jedes Benutzers, den Sie entfernen möchten.
3. Wählen Sie im Menü Optionen in der Spalte **Aktionen** die Option **Benutzer/s entfernen** aus.
4. Wenn Sie aufgefordert werden, bestätigen Sie den Löschvorgang, indem Sie das Wort "Entfernen" eingeben und dann **Ja, Benutzer entfernen** wählen.

## Ergebnis

Astra Control Center entfernt den Benutzer aus dem Konto.

## Rollen managen

Sie können Rollen managen, indem Sie Namespace-Einschränkungen hinzufügen und Benutzerrollen auf diese Einschränkungen beschränken. So können Sie den Zugriff auf Ressourcen in Ihrem Unternehmen kontrollieren. Sie können die Astra Control UI oder verwenden ["Die Astra Control API"](#) Rollen managen.

### Fügen Sie einer Rolle eine Namespace-Einschränkung hinzu

Ein Administrator oder Benutzer des Eigentümers kann den Mitglied- oder Viewer-Rollen Namespace-Einschränkungen hinzufügen.

#### Schritte

1. Wählen Sie im Navigationsbereich \* Konto verwalten\* die Option **Konto**.
2. Wählen Sie die Registerkarte **Benutzer** aus.
3. Wählen Sie in der Spalte **Actions** die Menü-Schaltfläche für einen Benutzer mit der Rolle Mitglied oder Viewer.
4. Wählen Sie **Rolle bearbeiten**.
5. Aktivieren Sie das Kontrollkästchen \* Rolle auf Einschränkungen beschränken\*.

Das Kontrollkästchen ist nur für Mitglieder- oder Viewer-Rollen verfügbar. Aus der Dropdown-Liste **Rolle** können Sie eine andere Rolle auswählen.

6. Wählen Sie **Bedingung hinzufügen**.

Sie können die Liste der verfügbaren Einschränkungen nach Namespace oder Namensraum-Bezeichnung anzeigen.

7. Wählen Sie in der Dropdown-Liste **Constraint type** je nach Konfiguration Ihrer Namespaces entweder **Kubernetes Namespace** oder **Kubernetes Namespace Label** aus.
8. Wählen Sie eine oder mehrere Namespaces oder Labels aus der Liste aus, um eine Beschränkung zu erstellen, die Rollen auf diese Namespaces beschränkt.
9. Wählen Sie **Bestätigen**.

Auf der Seite \* Rolle bearbeiten\* wird die Liste der für diese Rolle ausgewählten Einschränkungen angezeigt.

10. Wählen Sie **Bestätigen**.

Auf der Seite **Konto** können Sie die Einschränkungen für beliebige Mitglieder- oder Viewer-Rollen in der Spalte **Role** anzeigen.



Wenn Sie Einschränkungen für eine Rolle aktivieren und **Bestätigen** wählen, ohne dass Einschränkungen hinzugefügt werden müssen, gilt die Rolle als uneingeschränkt eingeschränkt (die Rolle wird dem Zugriff auf alle Ressourcen verweigert, die Namespaces zugewiesen sind).

### Entfernen Sie eine Namespace-Beschränkung aus einer Rolle

Ein Administrator oder Benutzer eines Eigentümers kann eine Namespace-Einschränkung aus einer Rolle entfernen.

## Schritte

1. Wählen Sie im Navigationsbereich \* Konto verwalten\* die Option **Konto**.
2. Wählen Sie die Registerkarte **Benutzer** aus.
3. Wählen Sie in der Spalte **Aktionen** die Menütaste für einen Benutzer mit der Rolle Mitglied oder Viewer mit aktiven Einschränkungen.
4. Wählen Sie **Rolle bearbeiten**.

Im Dialogfeld **Rolle bearbeiten** werden die aktiven Einschränkungen für die Rolle angezeigt.

5. Wählen Sie das **X** rechts neben der Bedingung aus, die Sie entfernen müssen.
6. Wählen Sie **Bestätigen**.

## Finden Sie weitere Informationen

- ["Benutzerrollen und Namespaces"](#)

## Managen Sie die Remote-Authentifizierung

LDAP ist ein branchenübliches Protokoll für den Zugriff auf verteilte Verzeichnisinformationen und eine beliebte Wahl für die Unternehmensauthentifizierung. Sie können Astra Control Center mit einem LDAP-Server verbinden, um die Authentifizierung für ausgewählte Astra Control-Benutzer durchzuführen.

Auf hohem Niveau beinhaltet die Konfiguration die Integration von Astra mit LDAP und die Definition der Astra Control Benutzer und Gruppen entsprechend der LDAP-Definitionen. Sie können die Astra Control API oder die Web-Benutzeroberfläche verwenden, um die LDAP-Authentifizierung und LDAP-Benutzer und -Gruppen zu konfigurieren.



Astra Control Center verwendet die E-Mail-Adresse im LDAP-Attribut „Mail“, um Remote-Benutzer zu suchen und zu verfolgen. Dieses Attribut kann ein optionales oder leeres Feld in Ihrem Verzeichnis sein. In diesem Feld muss für alle Remote-Benutzer, die im Astra Control Center erscheinen sollen, eine E-Mail-Adresse vorhanden sein. Diese E-Mail-Adresse wird als Benutzername im Astra Control Center zur Authentifizierung verwendet.

## Fügen Sie ein Zertifikat für die LDAPS-Authentifizierung hinzu

Fügen Sie das private TLS-Zertifikat für den LDAP-Server hinzu, damit sich Astra Control Center bei Verwendung einer LDAPS-Verbindung mit dem LDAP-Server authentifizieren kann. Sie müssen dies nur einmal tun, oder wenn das Zertifikat, das Sie installiert haben, abläuft.

## Schritte

1. Gehen Sie zu **Konto**.
2. Wählen Sie die Registerkarte **Zertifikate** aus.
3. Wählen Sie **Hinzufügen**.
4. Laden Sie entweder die hoch .pem Datei oder fügen Sie den Inhalt der Datei aus der Zwischenablage ein.
5. Aktivieren Sie das Kontrollkästchen \* Trusted\*.
6. Wählen Sie **Zertifikat hinzufügen**.

## Aktivieren Sie die Remote-Authentifizierung

Sie können die LDAP-Authentifizierung aktivieren und die Verbindung zwischen Astra Control und dem Remote LDAP-Server konfigurieren.

### Was Sie benötigen

Wenn Sie LDAPS verwenden möchten, stellen Sie sicher, dass das private TLS-Zertifikat für den LDAP-Server im Astra Control Center installiert ist, damit sich Astra Control Center mit dem LDAP-Server authentifizieren kann. Siehe [Fügen Sie ein Zertifikat für die LDAPS-Authentifizierung hinzu](#) Weitere Anweisungen.

### Schritte

1. Gehen Sie zu **Konto > Verbindungen**.
2. Wählen Sie im Fenster **Remote Authentication** das Konfigurationsmenü aus.
3. Wählen Sie **Verbinden**.
4. Geben Sie die IP-Adresse, den Port und das bevorzugte Verbindungsprotokoll (LDAP oder LDAPS) des Servers ein.



Verwenden Sie als Best Practice LDAPS, wenn Sie eine Verbindung zum LDAP-Server herstellen. Vor der Verbindung mit LDAPS müssen Sie das private TLS-Zertifikat des LDAP-Servers in Astra Control Center installieren.

5. Geben Sie die Anmeldeinformationen für das Servicekonto im E-Mail-Format ein ([administrator@example.com](#)). Astra Control verwendet diese Anmeldeinformationen, wenn Sie eine Verbindung mit dem LDAP-Server herstellen.
6. Geben Sie im Abschnitt **User Match** den Basis-DN und einen entsprechenden Benutzersuchfilter ein, der beim Abrufen von Benutzerinformationen vom LDAP-Server verwendet werden soll.
7. Geben Sie im Abschnitt **Gruppenvergleich** den Gruppen-Suchsocket-DN und einen entsprechenden benutzerdefinierten Gruppensuchfilter ein.



Verwenden Sie unbedingt den richtigen Basisnamen (DN) und einen entsprechenden Suchfilter für **User Match** und **Group Match**. Der Basis-DN teilt Astra Control mit, auf welcher Ebene der Verzeichnisstruktur die Suche gestartet werden soll, und der Suchfilter begrenzt die Teile des Verzeichnisbaums Astra Control Suchanfragen.

8. Wählen Sie **Senden**.

### Ergebnis

Der Fensterstatus **Remote-Authentifizierung** wechselt zu **Ausstehend** und dann zu **verbunden**, wenn die Verbindung zum LDAP-Server hergestellt wird.

## Deaktivieren Sie die Remote-Authentifizierung

Sie können eine aktive Verbindung zum LDAP-Server vorübergehend deaktivieren.



Wenn Sie eine Verbindung zu einem LDAP-Server deaktivieren, werden alle Einstellungen gespeichert und alle Remote-Benutzer und -Gruppen, die von diesem LDAP-Server zu Astra Control hinzugefügt wurden, bleiben erhalten. Sie können jederzeit eine Verbindung zu diesem LDAP-Server herstellen.

### Schritte



1. Gehen Sie zu **Konto > Verbindungen**.
2. Wählen Sie im Fenster **Remote Authentication** das Konfigurationsmenü aus.
3. Wählen Sie **Deaktivieren**.

### Ergebnis

Der Status des Fensterbereichs **Remote Authentication** wechselt zu **deaktivierte**. Alle Einstellungen für die Remote-Authentifizierung, Remote-Benutzer und Remote-Gruppen bleiben erhalten, und Sie können die Verbindung jederzeit wieder aktivieren.

### Remote-Authentifizierungseinstellungen bearbeiten

Wenn Sie die Verbindung zum LDAP-Server deaktiviert haben oder sich der Fensterbereich **Remote Authentication** im Status „Verbindungsfehler“ befindet, können Sie die Konfigurationseinstellungen bearbeiten.



Sie können die URL oder IP-Adresse des LDAP-Servers nicht bearbeiten, wenn sich der Bereich **Remote Authentication** im Status „deaktiviert“ befindet. Sie müssen [Trennen Sie die Remote-Authentifizierung](#) Zunächst.

### Schritte

1. Gehen Sie zu **Konto > Verbindungen**.
2. Wählen Sie im Fenster **Remote Authentication** das Konfigurationsmenü aus.
3. Wählen Sie **Bearbeiten**.
4. Nehmen Sie die erforderlichen Änderungen vor, und wählen Sie **Bearbeiten**.

### Trennen Sie die Remote-Authentifizierung

Sie können die Verbindung zu einem LDAP-Server trennen und die Konfigurationseinstellungen von Astra Control entfernen.



Wenn Sie die Verbindung zum LDAP-Server trennen, werden alle Konfigurationseinstellungen für diesen LDAP-Server aus Astra Control sowie alle Remote-Benutzer und -Gruppen entfernt, die diesem LDAP-Server hinzugefügt wurden.

### Schritte

1. Gehen Sie zu **Konto > Verbindungen**.
2. Wählen Sie im Fenster **Remote Authentication** das Konfigurationsmenü aus.
3. Wählen Sie **Trennen**.

### Ergebnis

Der Status des Fensterbereichs **Remote Authentication** wechselt zu **nicht verbunden**. Remote-Authentifizierungseinstellungen, Remote-Benutzer und Remote-Gruppen werden aus Astra Control entfernt.

### Verwalten von Remote-Benutzern und -Gruppen

Wenn Sie die LDAP-Authentifizierung auf Ihrem Astra Control System aktiviert haben, können Sie nach LDAP-Benutzern und -Gruppen suchen und diese in die genehmigten Benutzer des Systems aufnehmen.

## Fügen Sie einen Remote-Benutzer hinzu

Kontoinhaber und -Administratoren können Remote-Benutzer zu Astra Control hinzufügen.



Remote-Benutzer können nicht hinzugefügt werden, wenn bereits ein lokaler Benutzer mit derselben E-Mail-Adresse im System vorhanden ist. Um den Benutzer als Remote-Benutzer hinzuzufügen, löschen Sie zuerst den lokalen Benutzer aus dem System.



Astra Control Center verwendet die E-Mail-Adresse im LDAP-Attribut „Mail“, um Remote-Benutzer zu suchen und zu verfolgen. Dieses Attribut kann ein optionales oder leeres Feld in Ihrem Verzeichnis sein. In diesem Feld muss für alle Remote-Benutzer, die im Astra Control Center erscheinen sollen, eine E-Mail-Adresse vorhanden sein. Diese E-Mail-Adresse wird als Benutzername im Astra Control Center zur Authentifizierung verwendet.

### Schritte

1. Gehen Sie zum Bereich **Konto**.
2. Wählen Sie die Registerkarte **Benutzer & Gruppen** aus.
3. Wählen Sie rechts auf der Seite die Option **Remote Users**.
4. Wählen Sie **Hinzufügen**.
5. Sie können auch nach einem LDAP-Benutzer suchen, indem Sie die E-Mail-Adresse des Benutzers im Feld **Filtern nach E-Mail** eingeben.
6. Wählen Sie einen oder mehrere Benutzer aus der Liste aus.
7. Weisen Sie dem Benutzer eine Rolle zu.



Wenn Sie einem Benutzer und der Gruppe des Benutzers verschiedene Rollen zuweisen, hat die Rolle eine größere Priorität.

8. Weisen Sie diesem Benutzer optional eine oder mehrere Namespace-Einschränkungen zu und wählen Sie **Rolle auf Einschränkungen beschränken** aus, um sie durchzusetzen. Sie können eine neue Namespace-Einschränkung hinzufügen, indem Sie **Bedingung hinzufügen** auswählen.



Wenn einem Benutzer mehrere Rollen durch die LDAP-Gruppenmitgliedschaft zugewiesen werden, sind die Einschränkungen in der am stärksten permissivsten Rolle die einzigen, die wirksam werden. Wenn z. B. ein Benutzer mit einer lokalen Viewer-Rolle drei Gruppen verbindet, die an die Rolle Mitglied gebunden sind, wird die Summe der Einschränkungen aus den Mitgliederrollen wirksam, und alle Einschränkungen aus der Viewer-Rolle werden ignoriert.

9. Wählen Sie **Hinzufügen**.

### Ergebnis

Der neue Benutzer wird in der Liste der Remote-Benutzer angezeigt. In dieser Liste können Sie aktive Einschränkungen für den Benutzer sehen und den Benutzer über das Menü **Aktionen** verwalten.

## Fügen Sie eine externe Gruppe hinzu

Wenn Sie viele Remote-Benutzer gleichzeitig hinzufügen möchten, können Kontoinhaber und -Administratoren Remote-Gruppen zu Astra Control hinzufügen. Wenn Sie eine Remote-Gruppe hinzufügen, werden alle Remote-Benutzer in dieser Gruppe zu Astra Control hinzugefügt und übernehmen die gleiche Rolle.

## Schritte

1. Gehen Sie zum Bereich **Konto**.
2. Wählen Sie die Registerkarte **Benutzer & Gruppen** aus.
3. Wählen Sie rechts auf der Seite **Remote-Gruppen** aus.
4. Wählen Sie **Hinzufügen**.

In diesem Fenster sehen Sie eine Liste der gemeinsamen Namen und Distinguished Names der LDAP-Gruppen, die Astra Control aus dem Verzeichnis abgerufen hat.

5. Suchen Sie optional nach einer LDAP-Gruppe, indem Sie den gemeinsamen Namen der Gruppe in das Feld **Filter nach gemeinsamem Namen** eingeben.
6. Wählen Sie eine oder mehrere Gruppen aus der Liste aus.
7. Weisen Sie den Gruppen eine Rolle zu.



Die ausgewählte Rolle ist allen Benutzern in dieser Gruppe zugewiesen. Wenn Sie einem Benutzer und der Gruppe des Benutzers verschiedene Rollen zuweisen, hat die Rolle eine größere Priorität.

8. Weisen Sie dieser Gruppe optional eine oder mehrere Namespace-Einschränkungen zu und wählen Sie **Rolle auf Einschränkungen beschränken** aus, um sie durchzusetzen. Sie können eine neue Namespace-Einschränkung hinzufügen, indem Sie **Bedingung hinzufügen** auswählen.



Wenn einem Benutzer mehrere Rollen durch die LDAP-Gruppenmitgliedschaft zugewiesen werden, sind die Einschränkungen in der am stärksten permissivsten Rolle die einzigen, die wirksam werden. Wenn z. B. ein Benutzer mit einer lokalen Viewer-Rolle drei Gruppen verbindet, die an die Rolle Mitglied gebunden sind, wird die Summe der Einschränkungen aus den Mitgliederrollen wirksam, und alle Einschränkungen aus der Viewer-Rolle werden ignoriert.

9. Wählen Sie **Hinzufügen**.

## Ergebnis

Die neue Gruppe wird in der Liste der Remote-Gruppen angezeigt, und alle Remote-Benutzer in dieser Gruppe werden in der Liste der Remote-Benutzer angezeigt. In dieser Liste können Sie Details über die Gruppe anzeigen und die Gruppe über das Menü **Aktionen** verwalten.

## Anzeigen und Managen von Benachrichtigungen

Astra benachrichtigt Sie, wenn Aktionen abgeschlossen oder fehlgeschlagen sind. Beispielsweise wird eine Benachrichtigung angezeigt, wenn ein Backup einer Anwendung erfolgreich abgeschlossen wurde.

Sie können diese Benachrichtigungen oben rechts auf der Schnittstelle verwalten:



## Schritte

1. Wählen Sie oben rechts die Anzahl der ungelesenen Benachrichtigungen aus.
2. Überprüfen Sie die Benachrichtigungen und wählen Sie dann **als gelesen markieren** oder **Alle Benachrichtigungen anzeigen**.

Wenn Sie **Alle Benachrichtigungen anzeigen** ausgewählt haben, wird die Seite Benachrichtigungen geladen.

3. Zeigen Sie auf der Seite **Benachrichtigungen** die Benachrichtigungen an, wählen Sie die Benachrichtigungen aus, die Sie als gelesen markieren möchten, wählen Sie **Aktion** und wählen Sie **als gelesen markieren**.

## Anmeldeinformationen hinzufügen und entfernen

Fügen Sie Anmeldedaten für lokale Private-Cloud-Provider wie ONTAP S3, mit OpenShift gemanagte Kubernetes-Cluster oder nicht gemanagte Kubernetes-Cluster jederzeit in Ihrem Konto hinzu und entfernen Sie sie. Astra Control Center verwendet diese Zugangsdaten, um Kubernetes-Cluster und die Applikationen auf den Clustern zu erkennen und Ressourcen in Ihrem Auftrag bereitzustellen.

Beachten Sie, dass alle Benutzer im Astra Control Center dieselben Anmeldedaten verwenden.

### Anmeldedaten hinzufügen

Wenn Sie Cluster verwalten, können Sie Astra Control Center Anmeldeinformationen hinzufügen. Informationen zum Hinzufügen von Anmeldeinformationen durch Hinzufügen eines neuen Clusters finden Sie unter ["Fügen Sie einen Kubernetes-Cluster hinzu"](#).



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:

### Anmeldedaten entfernen

Entfernen Sie die Anmeldeinformationen jederzeit aus einem Konto. Sie sollten erst nach dem Entfernen von Anmeldeinformationen verwenden ["Verwalten aller zugehörigen Cluster wird aufgehoben"](#).



Der erste Satz von Anmeldeinformationen, die Sie dem Astra Control Center hinzufügen, wird immer verwendet, da Astra Control Center die Zugangsdaten für die Authentifizierung beim Backup-Bucket verwendet. Diese Anmeldedaten sollten am besten nicht entfernt werden.

### Schritte

1. Wählen Sie **Konto**.
2. Wählen Sie die Registerkarte **Anmeldeinformationen** aus.
3. Wählen Sie in der Spalte **Status** das Menü Optionen für die Anmeldeinformationen aus, die Sie entfernen möchten.
4. Wählen Sie **Entfernen**.
5. Geben Sie das Wort „Entfernen“ ein, um den Löschvorgang zu bestätigen, und wählen Sie dann **Ja, Anmeldedaten entfernen** aus.

## Ergebnis

Astra Control Center entfernt die Anmeldeinformationen aus dem Konto.

## Überwachen der Kontoaktivität

Details zu den Aktivitäten können Sie in Ihrem Astra Control Konto anzeigen. Beispiel: Beim Einladen neuer Benutzer, beim Hinzufügen eines Clusters oder beim Erstellen eines Snapshots. Sie haben auch die Möglichkeit, Ihre Kontoaktivität in eine CSV-Datei zu exportieren.



Wenn Sie Kubernetes-Cluster über Astra Control verwalten und Astra Control mit Cloud Insights verbunden ist, sendet Astra Control Ereignisprotokolle an Cloud Insights. Die Protokollinformationen, einschließlich Informationen über die Pod-Implementierung und PVC-Anhänge, werden im Astra Control Activity Log angezeigt. Mithilfe dieser Informationen können Sie alle zu verwaltenden Kubernetes-Cluster Fehler ermitteln.

### Alle Kontoaktivitäten in Astra Control anzeigen

1. Wählen Sie **Aktivität**.
2. Verwenden Sie die Filter, um die Liste der Aktivitäten einzugrenzen, oder verwenden Sie das Suchfeld, um das gesuchte zu finden.
3. Wählen Sie **in CSV exportieren** aus, um Ihre Kontoaktivität in eine CSV-Datei herunterzuladen.

### Zeigen Sie die Kontoaktivität für eine bestimmte App an

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie **Aktivität**.

### Zeigen Sie die Kontoaktivität für Cluster an

1. Wählen Sie **Cluster** und dann den Namen des Clusters aus.
2. Wählen Sie **Aktivität**.

### Ergreifen Sie Maßnahmen, um Ereignisse zu lösen, die Aufmerksamkeit erfordern

1. Wählen Sie **Aktivität**.
2. Wählen Sie ein Ereignis aus, das Aufmerksamkeit erfordert.
3. Wählen Sie die Dropdown-Option **Aktion** aus.

In dieser Liste finden Sie mögliche Korrekturmaßnahmen, die Sie ergreifen können, eine Dokumentation zum Problem anzeigen und Support zur Behebung des Problems erhalten.

## Aktualisieren einer vorhandenen Lizenz

Sie können eine Evaluierungslizenz in eine vollständige Lizenz umwandeln oder eine bestehende Evaluierung oder Volllizenz mit einer neuen Lizenz aktualisieren. Wenn Sie keine vollständige Lizenz besitzen, wenden Sie sich an Ihren NetApp Ansprechpartner, um eine vollständige Lizenz und eine Seriennummer zu erhalten. Sie können die Astra Control Center-UI oder verwenden ["Die Astra Control API"](#) Um eine vorhandene Lizenz zu aktualisieren.

## Schritte

1. Melden Sie sich bei an ["NetApp Support Website"](#).
2. Rufen Sie die Download-Seite des Astra Control Center auf, geben Sie die Seriennummer ein und laden Sie die vollständige NetApp Lizenzdatei (NLF) herunter.
3. Melden Sie sich in der UI des Astra Control Center an.
4. Wählen Sie in der linken Navigationsleiste **Konto > Lizenz**.
5. Wählen Sie auf der Seite **Konto > Lizenz** das Dropdown-Menü Status der vorhandenen Lizenz aus und wählen Sie **Replace**.
6. Navigieren Sie zu der Lizenzdatei, die Sie heruntergeladen haben.
7. Wählen Sie **Hinzufügen**.

Auf der Seite **Konto > Lizenzen** werden Lizenzinformationen, Ablaufdatum, Lizenzseriennummer, Konto-ID und verwendete CPU-Einheiten angezeigt.

## Finden Sie weitere Informationen

- ["Astra Control Center-Lizenzierung"](#)

# Buckets verwalten

Ein Objektspeicher-Bucket-Provider ist äußerst wichtig, wenn Sie Ihre Applikationen und Ihren persistenten Storage sichern möchten oder Applikationen über Cluster hinweg klonen möchten. Fügen Sie mithilfe des Astra Control Center einen Objektspeicher-Provider als externes Backup-Ziel für Ihre Applikationen hinzu.

Sie benötigen keinen Bucket, wenn Sie die Applikationskonfiguration und Ihren persistenten Storage auf dasselbe Cluster klonen.

Verwenden Sie einen der folgenden Amazon Simple Storage Service (S3) Bucket-Provider:

- NetApp ONTAP S3
- NetApp StorageGRID S3
- Microsoft Azure
- Allgemein S3



Amazon Web Services (AWS) und Google Cloud Platform (GCP) verwenden den Bucket-Typ Generic S3.



Obwohl Astra Control Center Amazon S3 als Generic S3 Bucket-Provider unterstützt, unterstützt Astra Control Center unter Umständen nicht alle Objektspeicher-Anbieter, die die Unterstützung von Amazon S3 beanspruchen.

Ein Bucket kann sich in einem dieser Zustände befinden:

- Ausstehend: Der Bucket ist für die Erkennung geplant.
- Verfügbar: Der Bucket ist zur Verwendung verfügbar.

- Entfernt: Auf den Bucket ist derzeit nicht zugegriffen werden können.

Anweisungen zum Verwalten von Buckets mithilfe der Astra Control API finden Sie im ["Astra Automation und API-Informationen"](#).

Sie können die folgenden Aufgaben zum Verwalten von Buckets ausführen:

- ["Fügen Sie einen Bucket hinzu"](#)
- [Bearbeiten eines Buckets](#)
- [Legen Sie den Standard-Bucket fest](#)
- [Bucket-Anmeldedaten drehen oder entfernen](#)
- [Entfernen Sie einen Bucket](#)



S3 Buckets im Astra Control Center berichten nicht über die verfügbare Kapazität. Bevor Sie Backups oder Klonanwendungen durchführen, die von Astra Control Center gemanagt werden, sollten Sie die Bucket-Informationen im ONTAP oder StorageGRID Managementsystem prüfen.

## Bearbeiten eines Buckets

Sie können die Zugangsdaten für einen Bucket ändern und ändern, ob ein ausgewählter Bucket der Standard-Bucket ist.



Wenn Sie einen Bucket hinzufügen, wählen Sie den richtigen Bucket-Provider aus und geben die richtigen Anmeldedaten für diesen Provider an. Beispielsweise akzeptiert die UI NetApp ONTAP S3 als Typ und akzeptiert StorageGRID-Anmeldedaten. Dies führt jedoch dazu, dass alle künftigen Applikations-Backups und -Wiederherstellungen, die diesen Bucket verwenden, fehlschlagen. Siehe ["Versionshinweise"](#).

### Schritte

1. Wählen Sie in der linken Navigationsleiste **Buckets** aus.
2. Wählen Sie im Menü in der Spalte **Aktionen** die Option **Bearbeiten**.
3. Ändern Sie alle Informationen außer dem Bucket-Typ.



Sie können den Bucket-Typ nicht ändern.

4. Wählen Sie **Aktualisieren**.

## Legen Sie den Standard-Bucket fest

Wenn Sie einen Cluster-übergreifenden Klon durchführen, benötigt Astra Control einen Standard-Bucket. Führen Sie diese Schritte aus, um einen Standard-Bucket für alle Cluster festzulegen.

### Schritte

1. Gehen Sie zu **Cloud-Instanzen**.
2. Wählen Sie das Menü in der Spalte **Aktionen** für die Cloud-Instanz in der Liste aus.
3. Wählen Sie **Bearbeiten**.
4. Wählen Sie in der Liste **Bucket** den Bucket aus, der als Standard verwendet werden soll.

5. Wählen Sie **Speichern**.

## Bucket-Anmeldedaten drehen oder entfernen

Astra Control verwendet Bucket-Zugangsdaten, um Zugriff zu erhalten und geheime Schlüssel für einen S3-Bucket bereitzustellen, damit Astra Control Center mit dem Bucket kommunizieren kann.

### Bucket-Anmeldedaten rotieren

Wenn Sie die Anmeldeinformationen drehen, drehen Sie sie während eines Wartungsfensters, wenn keine Backups ausgeführt werden (geplant oder auf Anforderung).

### Schritte zum Bearbeiten und Drehen von Anmeldeinformationen

1. Wählen Sie in der linken Navigationsleiste **Buckets** aus.
2. Wählen Sie im Menü Optionen in der Spalte **Aktionen** die Option **Bearbeiten** aus.
3. Erstellen Sie die neuen Anmeldedaten.
4. Wählen Sie **Aktualisieren**.

### Bucket-Anmeldedaten entfernen

Sie sollten die Bucket-Anmeldedaten nur entfernen, wenn auf einen Bucket neue Zugangsdaten angewendet wurden oder der Bucket nicht mehr aktiv verwendet wird.



Der erste Satz von Anmeldeinformationen, die Sie Astra Control hinzufügen, wird immer verwendet, da Astra Control zur Authentifizierung des Backup-Buckets die Zugangsdaten verwendet. Entfernen Sie diese Anmeldedaten nicht, wenn der Bucket aktiv ist, da dies zu Backup-Ausfällen und Nichtverfügbarkeit von Backups führen kann.



Wenn Sie die aktiven Bucket-Anmeldedaten entfernen, finden Sie unter "[Fehlerbehebung beim Entfernen der Bucket-Anmeldeinformationen](#)".

Anweisungen zum Entfernen von S3-Anmeldeinformationen mithilfe der Astra Control API finden Sie im "[Astra Automation und API-Informationen](#)".

## Entfernen Sie einen Bucket

Sie können einen Eimer entfernen, der nicht mehr verwendet wird oder nicht ordnungsgemäß ist. Dies könnte Sie nutzen, um die Konfiguration Ihres Objektspeicher einfach und aktuell zu halten.



Sie können keinen Standard-Bucket entfernen. Wenn Sie diesen Bucket entfernen möchten, wählen Sie zuerst einen anderen Bucket als Standard aus.

### Was Sie benötigen

- Sie sollten vor Beginn sicherstellen, dass keine Backups für diesen Bucket ausgeführt oder abgeschlossen wurden.
- Sie sollten prüfen, ob der Bucket nicht in einer aktiven Schutzrichtlinie verwendet wird.

Wenn dies der Fall ist, können Sie nicht fortfahren.

### Schritte



1. Wählen Sie in der linken Navigationsleiste **Buckets** aus.
2. Wählen Sie im Menü **Aktionen** die Option **Entfernen**.



Astra Control stellt zunächst sicher, dass es keine Planungsrichtlinien gibt, die den Bucket für Backups verwenden und dass keine aktiven Backups im Bucket vorhanden sind, den Sie entfernen möchten.

3. Geben Sie „Entfernen“ ein, um die Aktion zu bestätigen.
4. Wählen Sie **Ja, entfernen Sie den Eimer**.

## Weitere Informationen

- ["Verwenden Sie die Astra Control API"](#)

## Management des Storage-Backends

Durch das Management von Storage-Clustern in Astra Control als Storage-Backend können Sie Verbindungen zwischen persistenten Volumes (PVS) und dem Storage-Backend sowie zusätzliche Storage-Kennzahlen abrufen. Sie können Storage-Kapazität und -Integritätsdetails überwachen, beispielsweise die Performance, wenn Astra Control Center mit Cloud Insights verbunden ist.

Eine Anleitung zum Managen von Storage-Back-Ends mithilfe der Astra Control API finden Sie im ["Astra Automation und API-Informationen"](#).

Sie können die folgenden Aufgaben zur Verwaltung eines Storage-Backends ausführen:

- ["Fügen Sie ein Storage-Back-End hinzu"](#)
- [Details zum Storage-Back-End](#)
- [Unmanagement eines Storage-Backends](#)
- [Entfernen Sie ein Speicher-Back-End](#)

## Details zum Storage-Back-End

Sie können Speicher-Backend-Informationen über das Dashboard oder über die Option Back-Ends anzeigen.

### Details zum Storage-Back-End können Sie über das Dashboard anzeigen

#### Schritte

1. Wählen Sie in der linken Navigationsleiste **Dashboard** aus.
2. Überprüfen Sie den Back-End-Bereich Speicher des Dashboards, der den Status anzeigt:
  - **Ungesund:** Die Lagerung befindet sich nicht im optimalen Zustand. Dies kann durch ein Latenzproblem oder eine Applikation aufgrund eines Container-Problems, z. B., beeinträchtigt sein.
  - **Alles gesund:** Die Lagerung wurde verwaltet und ist in einem optimalen Zustand.
  - **Entdeckt:** Der Speicher wurde entdeckt, aber nicht von Astra Control verwaltet.

## Details zum Speicher-Backend über die Option „Backend“ anzeigen

Informationen zum Zustand, Kapazität und Performance des Backend (IOPS-Durchsatz und/oder Latenz)

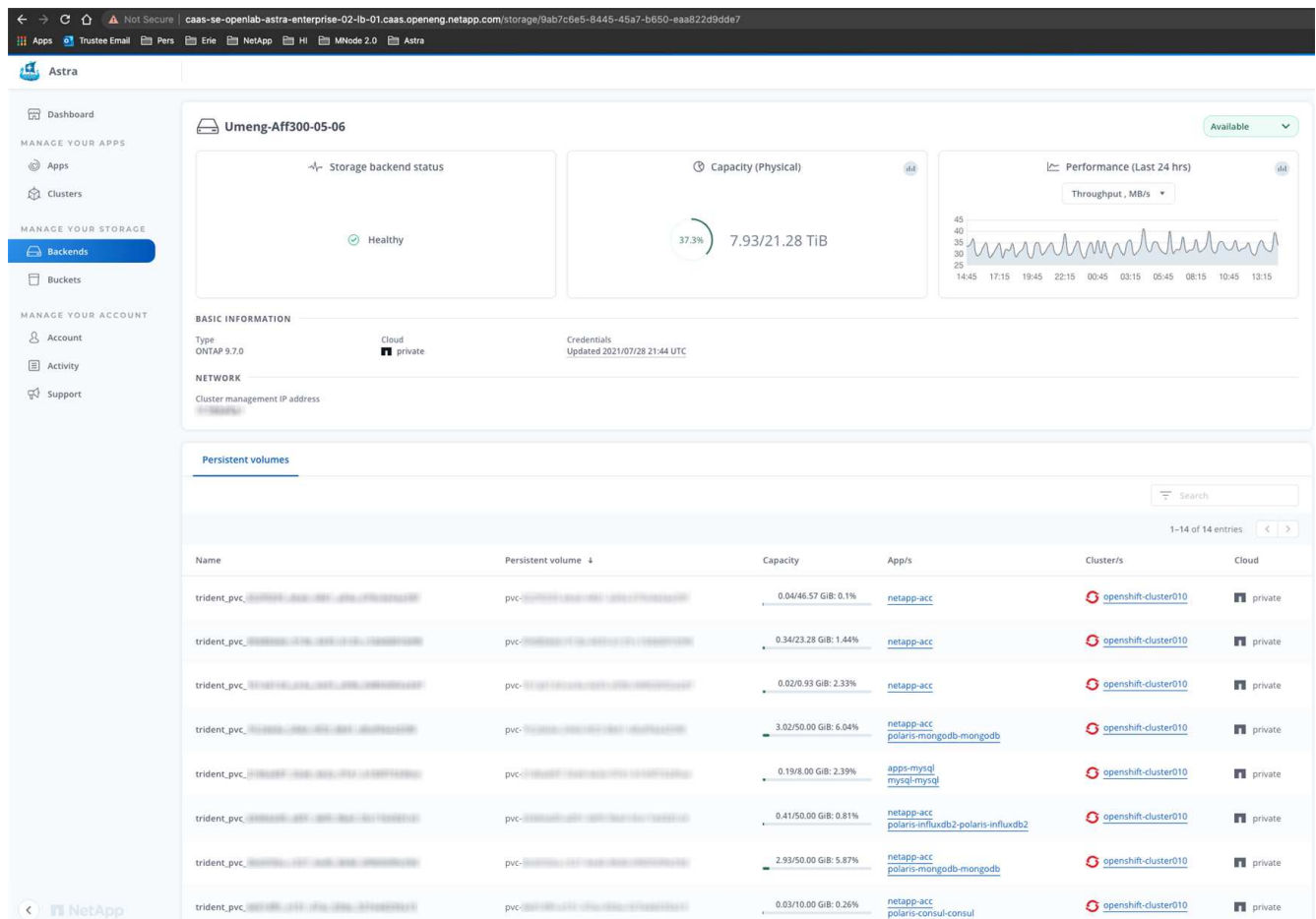
Sie sehen die Volumes, die die Kubernetes-Apps verwenden, die in einem ausgewählten Storage-Backend gespeichert sind. Mit Cloud Insights werden zusätzliche Informationen angezeigt. Siehe "[Cloud Insights-Dokumentation](#)".

### Schritte

1. Wählen Sie im linken Navigationsbereich **Backend** aus.
2. Wählen Sie das Storage-Back-End aus.



Wenn Sie eine Verbindung zum NetApp Cloud Insights hergestellt haben, werden auf der Seite „Back-Ends“ Auszüge aus Cloud Insights angezeigt.



3. Um direkt zu Cloud Insights zu gelangen, wählen Sie neben dem Kennzahlenbild das Symbol **Cloud Insights** aus.

## Unmanagement eines Storage-Backends

Sie können das Backend verwalten.

### Schritte

1. Wählen Sie in der linken Navigationsleiste **Backend** aus.

2. Wählen Sie das Storage-Back-End aus.
3. Wählen Sie im Menü Optionen in der Spalte **Aktionen** die Option **Verwaltung aufheben** aus.
4. Geben Sie „unverwalten“ ein, um die Aktion zu bestätigen.
5. Wählen Sie **Ja, verwalten Sie das Speicher-Backend**.

## Entfernen Sie ein Speicher-Back-End

Sie können ein nicht mehr verwendendes Storage-Back-End entfernen. Nutzen Sie dies, um Ihre Konfiguration auf dem neuesten Stand zu halten.

### Was Sie benötigen

- Stellen Sie sicher, dass das Storage-Back-End nicht gemanagt wird.
- Stellen Sie sicher, dass dem Cluster keine Volumes im Speicher-Backend zugewiesen sind.

### Schritte

1. Wählen Sie in der linken Navigationsleiste **Backend** aus.
2. Wenn das Backend verwaltet wird, managen Sie es rückgängig.
  - a. Wählen Sie **Verwaltet**.
  - b. Wählen Sie das Storage-Back-End aus.
  - c. Wählen Sie aus der Option **Aktionen** die Option **Verwaltung aufheben** aus.
  - d. Geben Sie „unverwalten“ ein, um die Aktion zu bestätigen.
  - e. Wählen Sie **Ja, verwalten Sie das Speicher-Backend**.
3. Wählen Sie **Entdeckt**.
  - a. Wählen Sie das Storage-Back-End aus.
  - b. Wählen Sie aus der Option **Aktionen** die Option **Entfernen**.
  - c. Geben Sie „Entfernen“ ein, um die Aktion zu bestätigen.
  - d. Wählen Sie **Ja, Speicher-Backend entfernen**.

### Weitere Informationen

- ["Verwenden Sie die Astra Control API"](#)

## Überwachen Sie laufende Aufgaben

Sie können Details über die Ausführung von Aufgaben und Aufgaben anzeigen, die in den letzten 24 Stunden in Astra Control abgeschlossen, fehlgeschlagen oder abgebrochen wurden. Beispielsweise können Sie den Status eines laufenden Backups, Restores oder Klonvorgangs anzeigen, und Details wie den Prozentsatz abgeschlossen und die geschätzte verbleibende Zeit angezeigt werden. Sie können den Status eines geplanten Vorgangs anzeigen, der ausgeführt wurde, oder einen manuell gestarteten Vorgang.

Während Sie eine laufende oder abgeschlossene Aufgabe anzeigen, können Sie die Aufgabendetails erweitern, um den Status der einzelnen Unteraufgaben anzuzeigen. Die Fortschrittsleiste der Aufgabe ist grün

für laufende oder abgeschlossene Aufgaben, blau für stornierte Aufgaben und rot für Aufgaben, die aufgrund eines Fehlers fehlgeschlagen sind.



Bei Klonvorgängen bestehen die Unteraufgaben der Aufgabe aus einem Snapshot und einem Snapshot-Wiederherstellungsvorgang.

Weitere Informationen zu fehlgeschlagenen Aufgaben finden Sie unter ["Überwachen der Kontoaktivität"](#).

#### Schritte

1. Während eine Aufgabe ausgeführt wird, gehen Sie zu **Anwendungen**.
2. Wählen Sie den Namen einer Anwendung aus der Liste aus.
3. Wählen Sie in den Details der Anwendung die Registerkarte **Aufgaben** aus.

Sie können Details zu aktuellen oder früheren Aufgaben anzeigen und nach Aufgabenstatus filtern.



Aufgaben werden bis zu 24 Stunden in der Liste **Aufgaben** aufbewahrt. Sie können diese Begrenzung und andere Einstellungen für die Aufgabenüberwachung mit dem konfigurieren ["Astra Control API"](#).

## Infrastruktur mit Cloud Insights-, Prometheus- oder Fluentd-Verbindungen überwachen

Sie können mehrere optionale Einstellungen konfigurieren, um Ihre Astra Control Center-Erfahrung zu verbessern. Um Ihre komplette Infrastruktur zu überwachen und Erkenntnisse zu erhalten, stellen Sie eine Verbindung zu NetApp Cloud Insights her, konfigurieren Sie Prometheus oder fügen Sie eine Fluentd-Verbindung hinzu.

Wenn das Netzwerk, in dem Astra Control Center ausgeführt wird, einen Proxy für die Verbindung zum Internet benötigt (um Support-Bundles auf die NetApp Support Site hochzuladen oder eine Verbindung zu Cloud Insights herzustellen), sollten Sie einen Proxy Server in Astra Control Center konfigurieren.

- [Verbinden Sie sich mit Cloud Insights](#)
- [Verbinden Sie sich mit Prometheus](#)
- [Mit Fluentd verbinden](#)

### Fügen Sie einen Proxy-Server für Verbindungen zu Cloud Insights oder zur NetApp Support-Website hinzu

Wenn das Netzwerk, in dem Astra Control Center ausgeführt wird, einen Proxy für die Verbindung zum Internet benötigt (um Support-Bundles auf die NetApp Support Site hochzuladen oder eine Verbindung zu Cloud Insights herzustellen), sollten Sie einen Proxy Server in Astra Control Center konfigurieren.



Astra Control Center überprüft nicht die von Ihnen eingegebenen Details für Ihren Proxy-Server. Stellen Sie sicher, dass Sie korrekte Werte eingeben.

#### Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin/Owner**-Berechtigung an.

2. Wählen Sie **Konto > Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Verbinden** aus, um einen Proxyserver hinzuzufügen.



4. Geben Sie den Proxy-Servernamen oder die IP-Adresse und die Proxy-Portnummer ein.
5. Wenn Ihr Proxy-Server eine Authentifizierung erfordert, aktivieren Sie das Kontrollkästchen, und geben Sie den Benutzernamen und das Kennwort ein.
6. Wählen Sie **Verbinden**.

### Ergebnis

Wenn die eingegebenen Proxydaten gespeichert wurden, zeigt der Abschnitt **HTTP Proxy** der Seite **Konto > Verbindungen** an, dass sie verbunden sind, und zeigt den Servernamen an.



### Proxy-Server-Einstellungen bearbeiten

Sie können die Proxy-Server-Einstellungen bearbeiten.

#### Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin/Owner**-Berechtigung an.
2. Wählen Sie **Konto > Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Bearbeiten** aus, um die Verbindung zu bearbeiten.
4. Bearbeiten Sie die Serverdetails und die Authentifizierungsinformationen.
5. Wählen Sie **Speichern**.

### Deaktivieren Sie die Proxy-Serververbindung

Sie können die Proxy-Server-Verbindung deaktivieren. Bevor Sie diese Option deaktivieren, werden Sie gewarnt, dass mögliche Unterbrechungen bei anderen Verbindungen auftreten können.

#### Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin/Owner**-Berechtigung an.
2. Wählen Sie **Konto > Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Trennen** aus, um die Verbindung zu deaktivieren.

4. Bestätigen Sie im Dialogfeld, das geöffnet wird, den Vorgang.

## Verbinden Sie sich mit Cloud Insights

Überwachen Sie Ihre komplette Infrastruktur, und verschaffen Sie sich so einen Überblick über Ihre komplette Infrastruktur. Verbinden Sie NetApp Cloud Insights mit Ihrer Astra Control Center Instanz. Cloud Insights ist in Ihrer Astra Control Center-Lizenz enthalten.

Cloud Insights sollte über das Netzwerk, das Astra Control Center verwendet, oder indirekt über einen Proxy-Server zugänglich sein.

Wenn Astra Control Center mit Cloud Insights verbunden ist, wird ein Pod für die Akquisitionseinheit erstellt. Dieser POD sammelt Daten aus den Storage-Back-Ends, die vom Astra Control Center gemanagt werden, und schiebt diese an Cloud Insights. Dieser POD benötigt 8 GB RAM und 2 CPU-Kerne.



Nach Aktivierung der Cloud Insights-Verbindung können Sie Durchsatzinformationen auf der Seite **Backend** anzeigen sowie von hier aus eine Verbindung zu Cloud Insights herstellen, nachdem Sie ein Speicher-Backend ausgewählt haben. Die Informationen finden Sie auch auf dem **Dashboard** im Clusterbereich, und von dort aus können Sie auch eine Verbindung zu Cloud Insights herstellen.

### Was Sie benötigen

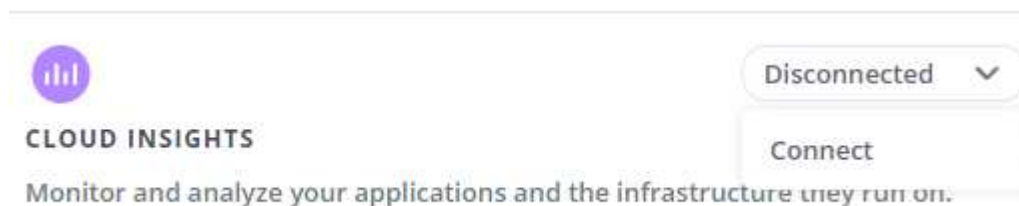
- Ein Astra Control Center-Konto mit **admin/Owner** Privilegien.
- Eine gültige Astra Control Center-Lizenz.
- Ein Proxy-Server, wenn das Netzwerk, in dem Sie Astra Control Center verwenden, einen Proxy für die Verbindung zum Internet benötigt.



Falls Sie neu bei Cloud Insights sind, sollten Sie sich mit den Funktionen und Features vertraut machen. Siehe "[Cloud Insights-Dokumentation](#)".

### Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin/Owner**-Berechtigung an.
2. Wählen Sie **Konto > Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Verbinden**, wo es **getrennt** angezeigt wird, um die Verbindung hinzuzufügen.



4. Geben Sie die Cloud Insights-API-Token und die Mandanten-URL ein. Die Mandanten-URL weist beispielsweise das folgende Format auf:

```
https://<environment-name>.c01.cloudinsights.netapp.com/
```

Sie erhalten die Mandanten-URL, wenn Sie die Cloud Insights-Lizenz erhalten. Wenn die Mandanten-URL nicht vorhanden ist, lesen Sie den "[Cloud Insights-Dokumentation](#)".

- Um die zu bekommen "[API-Token](#)", Loggen Sie sich bei Ihrer Cloud Insights-Mandanten-URL ein.
- Generieren Sie in Cloud Insights durch Klicken auf **Admin > API-Zugriff** sowohl ein **Lesen/Schreiben** als auch ein **schreibgeschütztes** API-Zugriffstoken.

The screenshot shows the Cloud Insights (Trial) Admin interface. The breadcrumb path is 'nmm95sx / Admin / API Access'. The main section is titled 'API Access Tokens (4)' and contains a table with the following data:

<input type="checkbox"/>	Name ↑	Description	Token	API Type	Permission
<input type="checkbox"/>	astra_...		...zBskB1	All Categories	Read/Write
<input type="checkbox"/>	astra_...		...xKOel_	All Categories	Read/Write
<input type="checkbox"/>	astra_...		...Z_A6HP	All Categories	Read Only
<input type="checkbox"/>	astra_...		...8BTkYY	All Categories	Read/Write

On the left sidebar, the 'ADMIN' menu item is highlighted. At the top right of the table, there is a '+ API Access Token' button and a 'Bulk Actions' dropdown.

- Kopieren Sie die Taste \* nur Lesen\*. Sie müssen es in das Fenster Astra Control Center einfügen, um die Cloud Insights-Verbindung zu aktivieren. Wählen Sie für die Hauptberechtigungen Lese-API-Zugriffstoken die Option Assets, Alerts, Acquisition Unit und Data Collection aus.
- Kopieren Sie die Taste **Lesen/Schreiben**. Sie müssen es in das Astra Control Center **Connect Cloud Insights** Fenster einfügen. Wählen Sie für die Hauptberechtigungen Lese-/Schreib-API-Zugriffstoken die Option Datenaufnahme, Protokollaufnahme, Erfassungseinheit und Datenerfassung aus.



Wir empfehlen Ihnen, einen **Read Only**-Schlüssel und einen **Read/Write**-Schlüssel zu generieren und nicht den gleichen Schlüssel für beide Zwecke zu verwenden. Standardmäßig ist der Ablauf des Tokens auf ein Jahr festgelegt. Wir empfehlen, dass Sie die Standardauswahl beibehalten, um dem Token die maximale Dauer zu geben, bevor es abläuft. Wenn Ihr Token abläuft, wird die Telemetrie angehalten.

- Fügen Sie die Tasten ein, die Sie von Cloud Insights in Astra Control Center kopiert haben.

## 5. Wählen Sie **Verbinden**.



Nach der Auswahl von **Verbinden** ändert sich der Status der Verbindung auf der Seite **Konto > Verbindungen** auf der Seite **Cloud Insights** auf **ausstehend**. Es kann einige Minuten dauern, bis die Verbindung aktiviert ist und der Status auf **verbunden** geändert wird.



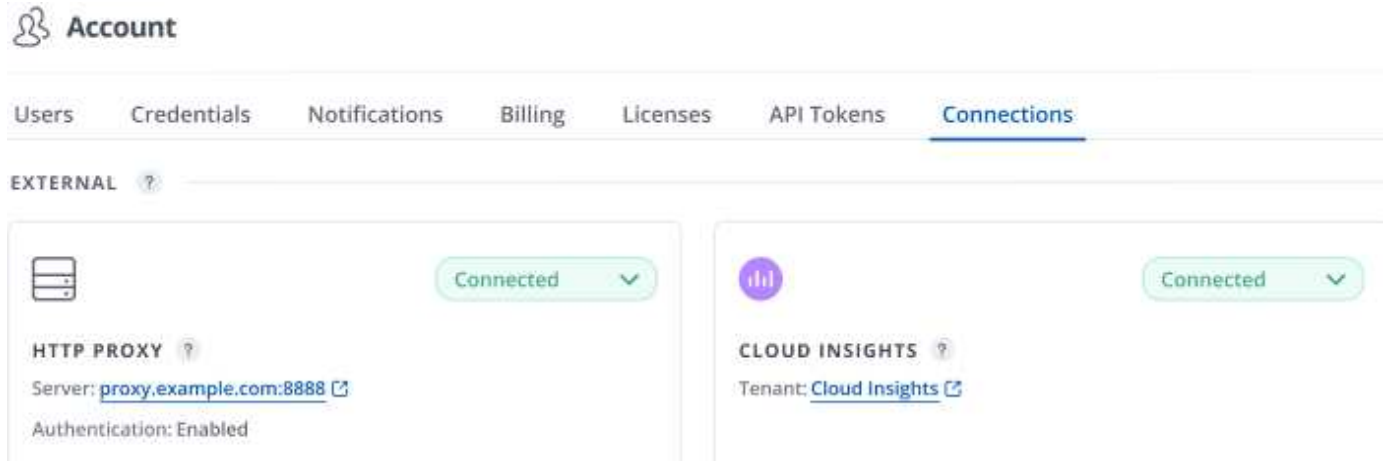
Um zwischen dem Astra Control Center und den Cloud Insights UIs hin und her zu gehen, stellen Sie sicher, dass Sie bei beiden angemeldet sind.

## Daten im Cloud Insights anzeigen

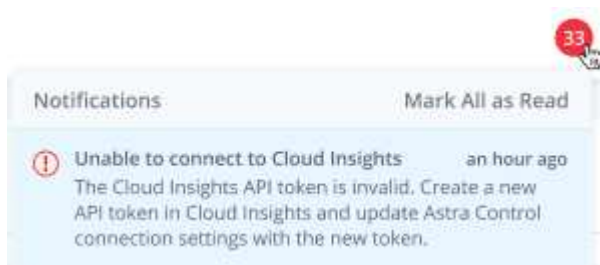
Wenn die Verbindung erfolgreich war, zeigt der Abschnitt **Cloud Insights** auf der Seite **Konto >**



**Verbindungen** an, dass sie verbunden ist, und zeigt die Mandanten-URL an. Sie können Cloud Insights besuchen, um zu sehen, dass Daten erfolgreich empfangen und angezeigt werden.

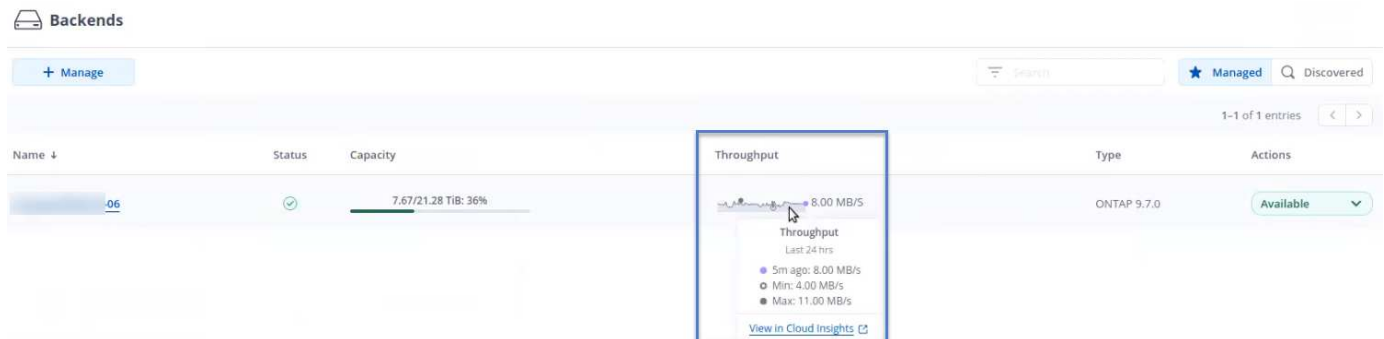


Wenn die Verbindung aus irgendeinem Grund fehlgeschlagen ist, wird im Status **failed** angezeigt. Den Grund für Fehlschlag finden Sie unter **Benachrichtigungen** auf der rechten oberen Seite des UI.



Die gleichen Informationen finden Sie auch unter **Konto > Benachrichtigungen**.

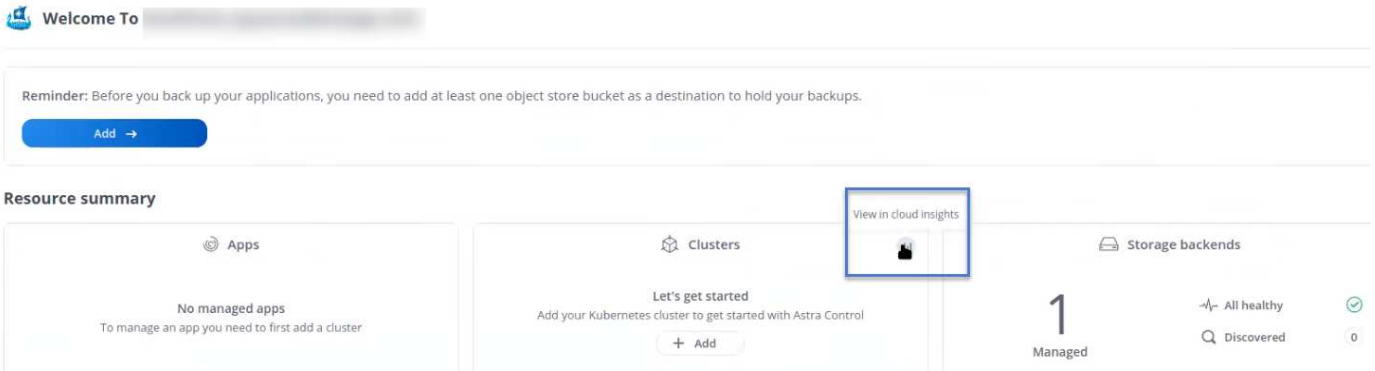
Vom Astra Control Center können Sie Durchsatzinformationen auf der Seite **Backend** anzeigen sowie von hier aus eine Verbindung zu Cloud Insights herstellen, nachdem Sie ein Storage-Backend ausgewählt haben.



Um direkt zu Cloud Insights zu gelangen, wählen Sie neben dem Kennzahlenbild das Symbol **Cloud Insights** aus.

Die Informationen finden Sie auch auf dem **Dashboard**.





Wenn Sie nach Aktivierung der Cloud Insights-Verbindung die Back-Ends entfernen, die Sie im Astra Control Center hinzugefügt haben, werden die Back-Ends nicht mehr an Cloud Insights gemeldet.

## Cloud Insights-Verbindung bearbeiten

Sie können die Cloud Insights-Verbindung bearbeiten.



Sie können nur die API-Schlüssel bearbeiten. Um die Cloud Insights-Mandanten-URL zu ändern, sollten Sie die Cloud Insights-Verbindung trennen und eine Verbindung mit der neuen URL herstellen.

### Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin/Owner**-Berechtigung an.
2. Wählen Sie **Konto > Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Bearbeiten** aus, um die Verbindung zu bearbeiten.
4. Bearbeiten Sie die Cloud Insights-Verbindungseinstellungen.
5. Wählen Sie **Speichern**.

## Deaktivieren Sie die Cloud Insights-Verbindung

Sie können die Cloud Insights-Verbindung für einen Kubernetes Cluster deaktivieren, der von Astra Control Center gemanagt wird. Wenn Sie die Cloud Insights-Verbindung deaktivieren, werden die bereits auf Cloud Insights hochgeladenen Telemetriedaten nicht gelöscht.

### Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin/Owner**-Berechtigung an.
2. Wählen Sie **Konto > Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Trennen** aus, um die Verbindung zu deaktivieren.
4. Bestätigen Sie im Dialogfeld, das geöffnet wird, den Vorgang. Nachdem Sie den Vorgang bestätigt haben, ändert sich der Cloud Insights-Status auf der Seite **Konto > Verbindungen** in **Ausstehend**. Es dauert ein paar Minuten, bis der Status in **nicht verbunden** geändert wird.

## Verbinden Sie sich mit Prometheus

Sie können Astra Control Center Daten mit Prometheus überwachen. Sie können Prometheus so konfigurieren, dass Kennzahlen vom Kubernetes Cluster-Metriken-Endpunkt erfasst werden, und Sie können Prometheus auch zur Visualisierung der Kennzahlendaten verwenden.

Weitere Informationen zur Verwendung von Prometheus finden Sie in der Dokumentation unter ["Erste Schritte mit Prometheus"](#).

### Was Sie benötigen

Stellen Sie sicher, dass Sie das Prometheus-Paket auf dem Astra Control Center-Cluster oder einem anderen Cluster heruntergeladen und installiert haben, der mit dem Astra Control Center-Cluster kommunizieren kann.

Befolgen Sie die Anweisungen in der offiziellen Dokumentation zu ["Installation Von Prometheus"](#).

Prometheus muss in der Lage sein, mit dem Astra Control Center Kubernetes Cluster zu kommunizieren. Wenn Prometheus nicht auf dem Astra Control Center Cluster installiert ist, müssen Sie sicherstellen, dass sie mit dem Kennzahlendienst kommunizieren können, der auf dem Astra Control Center Cluster ausgeführt wird.

### Konfigurieren Sie Prometheus

Astra Control Center stellt einen Kennzahlungsservice für TCP-Port 9090 im Kubernetes-Cluster bereit. Sie müssen Prometheus konfigurieren, um Kennzahlen aus diesem Service zu sammeln.

#### Schritte

1. Melden Sie sich beim Prometheus-Server an.
2. Fügen Sie den Cluster-Eintrag in das `prometheus.yml` Datei: Im `yml` Fügen Sie im einen Eintrag wie der folgende für Ihr Cluster hinzu `scrape_configs` section:

```
job_name: '<Add your cluster name here. You can abbreviate. It just
needs to be a unique name>'
metrics_path: /accounts/<replace with your account ID>/metrics
authorization:
  credentials: <replace with your API token>
tls_config:
  insecure_skip_verify: true
static_configs:
  - targets: ['<replace with your astraAddress. If using FQDN, the
prometheus server has to be able to resolve it>']
```



Wenn Sie die einstellen `tls_config insecure_skip_verify` Bis `true`, Das TLS-Verschlüsselungsprotokoll ist nicht erforderlich.

3. Starten Sie den Prometheus-Service neu:

```
sudo systemctl restart prometheus
```

### Zugang Prometheus

Rufen Sie die Prometheus-URL auf.

#### Schritte

1. Geben Sie in einem Browser die Prometheus-URL mit Port 9090 ein.

2. Überprüfen Sie Ihre Verbindung, indem Sie **Status > Ziele** wählen.

## Daten in Prometheus anzeigen

Sie können Prometheus verwenden, um Astra Control Center-Daten anzuzeigen.

### Schritte

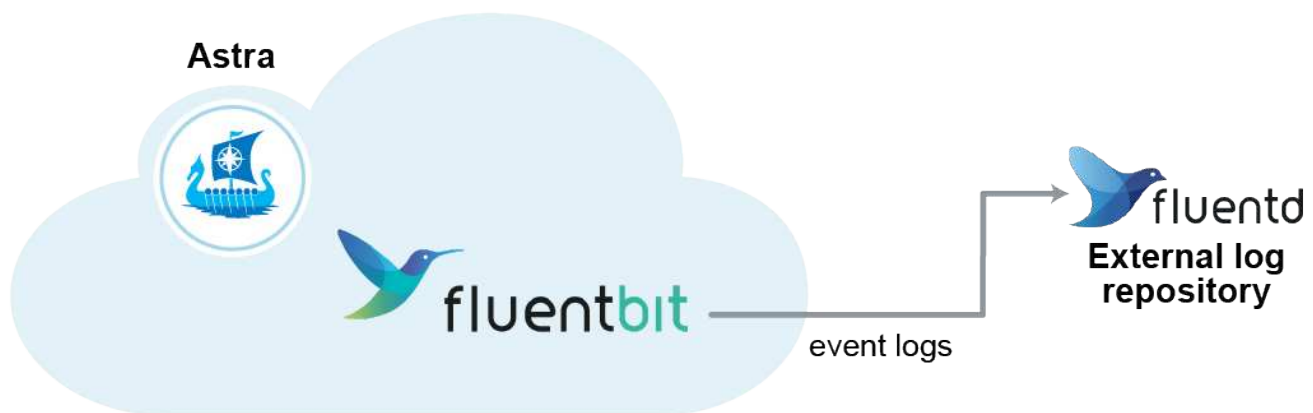
1. Geben Sie in einem Browser die Prometheus-URL ein.
2. Wählen Sie im Menü Prometheus die Option **Grafik** aus.
3. Um den Metrics Explorer zu verwenden, wählen Sie das Symbol neben **Ausführen** aus.
4. Wählen Sie `scrape_samples_scraped` Und wählen Sie **Ausführen**.
5. Wenn Sie das Scraping von Proben im Laufe der Zeit anzeigen möchten, wählen Sie **Grafik**.



Wenn mehrere Cluster-Daten erfasst wurden, werden die Metriken jedes Clusters in einer anderen Farbe angezeigt.

## Mit Fluentd verbinden

Sie können Protokolle (Kubernetes-Ereignisse) von einem vom Astra Control Center überwachten System an Ihren Fluentd Endpunkt senden. Die Fluentd-Verbindung ist standardmäßig deaktiviert.



Nur die Ereignisprotokolle von verwalteten Clustern werden an Fluentd weitergeleitet.

### Was Sie benötigen

- Ein Astra Control Center-Konto mit **admin/Owner** Privilegien.
- Astra Control Center ist auf einem Kubernetes-Cluster installiert und läuft.

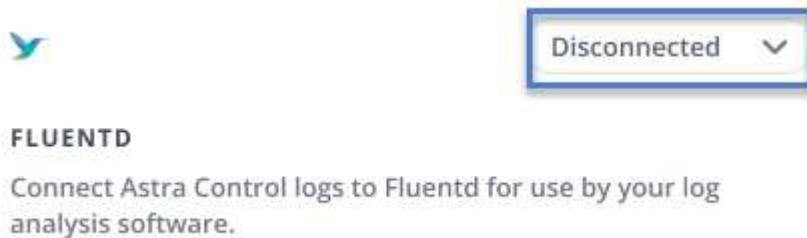


Astra Control Center überprüft nicht die Details, die Sie für Ihren Fluentd-Server eingeben. Stellen Sie sicher, dass Sie die richtigen Werte eingeben.

### Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin/Owner**-Berechtigung an.
2. Wählen Sie **Konto > Verbindungen**.

3. Wählen Sie in der Dropdown-Liste **nicht verbunden** aus, um die Verbindung hinzuzufügen.



4. Geben Sie die Host-IP-Adresse, die Portnummer und den freigegebenen Schlüssel für Ihren Fluentd-Server ein.
5. Wählen Sie **Verbinden**.

### Ergebnis

Wenn die für den Fluentd-Server eingegebenen Details gespeichert wurden, zeigt der Abschnitt **Fluentd** auf der Seite **Konto > Verbindungen** an, dass er verbunden ist. Jetzt können Sie den Fluentd-Server besuchen, mit dem Sie verbunden sind, und die Ereignisprotokolle anzeigen.

Wenn die Verbindung aus irgendeinem Grund fehlgeschlagen ist, wird im Status **failed** angezeigt. Den Grund für Fehlschlag finden Sie unter **Benachrichtigungen** auf der rechten oberen Seite des UI.

Die gleichen Informationen finden Sie auch unter **Konto > Benachrichtigungen**.



Wenn Sie Probleme mit der Protokollerfassung haben, sollten Sie sich bei Ihrem Worker-Knoten anmelden und sicherstellen, dass Ihre Protokolle in verfügbar sind `/var/log/containers/`.

### Bearbeiten Sie die Fluentd-Verbindung

Sie können die Fluentd-Verbindung zu Ihrer Astra Control Center-Instanz bearbeiten.

#### Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin/Owner**-Berechtigung an.
2. Wählen Sie **Konto > Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Bearbeiten** aus, um die Verbindung zu bearbeiten.
4. Ändern Sie die Einstellungen für den Fluentd-Endpunkt.
5. Wählen Sie **Speichern**.

### Deaktivieren Sie die Fluentd-Verbindung

Sie können die Fluentd-Verbindung zu Ihrer Astra Control Center-Instanz deaktivieren.

#### Schritte

1. Melden Sie sich bei Astra Control Center mit einem Konto mit **admin/Owner**-Berechtigung an.
2. Wählen Sie **Konto > Verbindungen**.
3. Wählen Sie in der Dropdown-Liste **Trennen** aus, um die Verbindung zu deaktivieren.
4. Bestätigen Sie im Dialogfeld, das geöffnet wird, den Vorgang.

# Heben Sie das Management von Applikationen und Clustern auf

Entfernen Sie alle Apps oder Cluster, die Sie nicht mehr über das Astra Control Center managen möchten.

## Verwaltung einer Anwendung aufheben

Sie müssen nicht mehr Apps managen, die Sie nicht mehr Backups, Snapshots oder Klone von Astra Control Center erstellen möchten.

Wenn Sie die Verwaltung einer Anwendung aufheben:

- Alle bestehenden Backups und Snapshots werden gelöscht.
- Applikationen und Daten sind weiterhin verfügbar.

### Schritte

1. Wählen Sie in der linken Navigationsleiste die Option **Anwendungen**.
2. Wählen Sie die App aus.
3. Wählen Sie im Menü Optionen in der Spalte Aktionen die Option **Verwaltung aufheben** aus.
4. Überprüfen Sie die Informationen.
5. Geben Sie zur Bestätigung „nicht verwalten“ ein.
6. Wählen Sie **Ja, Anwendung verwalten** aus.

### Ergebnis

Astra Control Center beendet die Verwaltung der App.

## Aufheben des Managements eines Clusters

Sie müssen den Cluster nicht mehr über das Astra Control Center managen.



Bevor Sie das Management des Clusters aufheben, sollten Sie die dem Cluster zugeordnete Applikationen aufheben.

Wenn Sie das Management eines Clusters aufheben:

- Dadurch wird das Management des Clusters durch das Astra Control Center verhindert. Die Konfiguration des Clusters ändert sich nicht, und das Cluster wird nicht gelöscht.
- Trident wird nicht vom Cluster deinstalliert. ["Lesen Sie, wie Trident deinstalliert wird"](#).

### Schritte

1. Wählen Sie in der linken Navigationsleiste **Cluster** aus.
2. Aktivieren Sie das Kontrollkästchen für den Cluster, den Sie nicht mehr managen möchten.
3. Wählen Sie im Menü Optionen in der Spalte **Aktionen** die Option **Verwaltung aufheben** aus.
4. Bestätigen Sie, dass Sie die Verwaltung des Clusters aufheben möchten und wählen Sie dann **Ja, Cluster verwalten** aus.

## Ergebnis

Der Status des Clusters ändert sich in **Entfernen**. Danach wird der Cluster aus der Seite **Cluster** entfernt und wird nicht mehr vom Astra Control Center verwaltet.



**Wenn Astra Control Center und Cloud Insights nicht verbunden sind**, entfernt die Unverwaltung des Clusters alle Ressourcen, die zum Senden von Telemetriedaten installiert wurden. **Wenn Astra Control Center und Cloud Insights verbunden sind**, löscht die Entsteuerung des Clusters nur das `fluentbit` Und `event-exporter` Behälter.

## Upgrade Astra Control Center

Laden Sie zum Upgrade des Astra Control Center das Installationspaket von der NetApp Support Site herunter, und füllen Sie die folgenden Anweisungen aus. Mit diesem Verfahren können Sie das Astra Control Center in internetverbundenen oder luftgekapderten Umgebungen aktualisieren.

### Was Sie benötigen

- Bevor Sie ein Upgrade durchführen, lesen Sie "[Anforderungen an die Betriebsumgebung](#)". Damit Ihre Umgebung die Mindestanforderungen für die Implementierung von Astra Control Center erfüllt. Ihre Umgebung sollte Folgendes haben:
  - Eine unterstützte Astra Trident-Version um die Version zu bestimmen, die Sie ausführen, führen Sie den folgenden Befehl gegen Ihr vorhandenes Astra Control Center aus:

```
kubectl get tridentversion -n trident
```

Siehe "[Astra Trident-Dokumentation](#)" Zum Upgrade von einer älteren Version.



Sie müssen ein Upgrade auf Astra Trident 22.10 \* VOR\* auf Kubernetes 1.25 durchführen.

- Eine unterstützte Kubernetes-Distribution, um zu bestimmen, welche Version Sie ausführen, führen Sie den folgenden Befehl gegen Ihr bestehendes Astra Control Center aus: `kubectl get nodes -o wide`
- Ausreichende Cluster-Ressourcen zur Ermittlung von Cluster-Ressourcen: Führen Sie den folgenden Befehl in Ihrem vorhandenen Astra Control Center-Cluster aus: `kubectl describe node <node name>`
- Eine Registrierung, mit der Sie Bilder des Astra Control Centers übertragen und hochladen können
- Führen Sie als Standard-Storage-Klasse den folgenden Befehl für Ihr vorhandenes Astra Control Center aus, um Ihre Standard-Storage-Klasse zu bestimmen: `kubectl get storageclass`
- (Nur OpenShift) Stellen Sie sicher, dass sich alle Clusterbetreiber in einem gesunden Zustand befinden und verfügbar sind.

```
kubectl get clusteroperators
```

- Stellen Sie sicher, dass alle API-Services in einem gesunden Zustand und verfügbar sind.

```
kubectl get apiservices
```

- Melden Sie sich von der Astra Control Center-Benutzeroberfläche ab, bevor Sie das Upgrade starten.

### Über diese Aufgabe

Der Astra Control Center Upgrade-Prozess führt Sie durch die folgenden grundlegenden Schritte:

- [Laden Sie das Astra Control Center herunter und extrahieren Sie es](#)
- [Entfernen Sie das NetApp Astra kubectl Plugin und installieren Sie es erneut](#)
- [Fügen Sie die Bilder Ihrer lokalen Registrierung hinzu](#)
- [Installieren Sie den aktualisierten Astra Control Center-Operator](#)
- [Upgrade Astra Control Center](#)
- [Überprüfen Sie den Systemstatus](#)



Löschen Sie den Operator Astra Control Center nicht (z. B. `kubectl delete -f astra_control_center_operator_deploy.yaml`) Zu jeder Zeit während des Astra Control Center Upgrades oder Betrieb, um zu vermeiden, dass Pods gelöscht werden.



Führen Sie Upgrades in einem Wartungsfenster durch, wenn Zeitpläne, Backups und Snapshots nicht ausgeführt werden.

## Laden Sie das Astra Control Center herunter und extrahieren Sie es

1. Wechseln Sie zum "[Astra Control Center: Seite zum Herunterladen von Produkten](#)" Auf der NetApp Support Site Sie können die neueste Version oder eine andere Version aus dem Dropdown-Menü auswählen.
2. Laden Sie das Bundle mit Astra Control Center herunter (`astra-control-center-[version].tar.gz`).
3. (Empfohlen, aber optional) Laden Sie das Zertifikaten- und Unterschriftenpaket für Astra Control Center herunter (`astra-control-center-certs-[version].tar.gz`) Um die Signatur des Pakets zu überprüfen:

```
tar -vxzf astra-control-center-certs-[version].tar.gz
```

```
openssl dgst -sha256 -verify certs/AstraControlCenter-public.pub  
-signature certs/astra-control-center-[version].tar.gz.sig astra-  
control-center-[version].tar.gz
```

Die Ausgabe wird angezeigt `Verified OK` Nach erfolgreicher Überprüfung.

4. Extrahieren Sie die Bilder aus dem Astra Control Center Bundle:

```
tar -vxzf astra-control-center-[version].tar.gz
```

## Entfernen Sie das NetApp Astra kubectl Plugin und installieren Sie es erneut

Das NetApp Astra kubectl Kommandozeilen-Plug-in spart Zeit, wenn es gängige Aufgaben im Zusammenhang mit der Bereitstellung und dem Upgrade des Astra Control Center ausführt.

1. Ermitteln Sie, ob das Plug-in installiert ist:

```
kubectl astra
```

2. Führen Sie eine der folgenden Aktionen durch:

- Falls das Plugin installiert ist, sollte der Befehl die kubectl Plugin-Hilfe zurückgeben. Führen Sie folgenden Befehl aus, um eine vorhandene Version von kubectl-astra zu entfernen: `delete /usr/local/bin/kubectl-astra`.
- Wenn der Befehl einen Fehler zurückgibt, ist das Plugin nicht installiert und Sie können mit dem nächsten Schritt fortfahren, um es zu installieren.

3. Installieren Sie das Plugin:

- a. Geben Sie die verfügbaren Plug-ins-Binärdateien von NetApp Astra kubectl an und notieren Sie sich den Namen der für Ihr Betriebssystem und die CPU-Architektur erforderlichen Datei:



Die kubectl Plugin-Bibliothek ist Teil des tar-Bündels und wird in den Ordner extrahiert `kubectl-astra`.

```
ls kubectl-astra/
```

- a. Verschieben Sie die richtige Binärdatei in den aktuellen Pfad, und benennen Sie sie in um `kubectl-astra`:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

## Fügen Sie die Bilder Ihrer lokalen Registrierung hinzu

1. Führen Sie die entsprechende Schrittfolge für Ihre Container-Engine durch:



## Docker

1. Wechseln Sie in das Stammverzeichnis des Tarballs. Sie sollten diese Datei und das Verzeichnis sehen:

```
acc.manifest.bundle.yaml
acc/
```

2. Übertragen Sie die Paketbilder im Astra Control Center-Bildverzeichnis in Ihre lokale Registrierung. Führen Sie die folgenden Ersetzungen durch, bevor Sie den ausführen `push-images` Befehl:

- Ersetzen Sie `<BUNDLE_FILE>` durch den Namen der Astra Control Bundle-Datei (`acc.manifest.bundle.yaml`).
- `&lt;MY_FULL_REGISTRY_PATH&gt;` durch die URL des Docker Repositorys ersetzen, beispielsweise "`<a href='\"https://&lt;docker-registry&gt;\"' class='\"bare\">https://&lt;docker-registry&gt;\"</a>`".
- Ersetzen Sie `<MY_REGISTRY_USER>` durch den Benutzernamen.
- Ersetzen Sie `<MY_REGISTRY_TOKEN>` durch ein autorisiertes Token für die Registrierung.

```
kubectl astra packages push-images -m <BUNDLE_FILE> -r
<MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
<MY_REGISTRY_TOKEN>
```

## Podman

1. Wechseln Sie in das Stammverzeichnis des Tarballs. Sie sollten diese Datei und das Verzeichnis sehen:

```
acc.manifest.bundle.yaml
acc/
```

2. Melden Sie sich bei Ihrer Registrierung an:

```
podman login <YOUR_REGISTRY>
```

3. Vorbereiten und Ausführen eines der folgenden Skripts, das für die von Ihnen verwendete Podman-Version angepasst ist. Ersetzen Sie `<MY_FULL_REGISTRY_PATH>` durch die URL Ihres Repositorys, die alle Unterverzeichnisse enthält.

```
<strong>Podman 4</strong>
```

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=22.11.0-82
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```

**Podman 3**

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=22.11.0-82
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```



Der Bildpfad, den das Skript erstellt, sollte abhängig von Ihrer Registrierungskonfiguration wie folgt aussehen:

<https://netappdownloads.jfrog.io/docker-astra-control-prod/netapp/astra/acc/22.11.0-82/image:version>

## Installieren Sie den aktualisierten Astra Control Center-Operator

### 1. Telefonbuch ändern:

```
cd manifests
```

2. Bearbeiten Sie die yaml-Implementierung des Astra Control Center-Bedieners (astra\_control\_center\_operator\_deploy.yaml) Zu Ihrem lokalen Register und Geheimnis zu verweisen.

```
vim astra_control_center_operator_deploy.yaml
```

- a. Wenn Sie eine Registrierung verwenden, die eine Authentifizierung erfordert, ersetzen oder bearbeiten Sie die Standardzeile von imagePullSecrets: [] Mit folgenden Optionen:

```
imagePullSecrets:
- name: <astra-registry-cred_or_custom_name_of_secret>
```

- b. Ändern [your\_registry\_path] Für das kube-rbac-proxy Bild zum Registrierungspfad, in dem Sie die Bilder in ein geschoben haben [Vorheriger Schritt](#).
- c. Ändern [your\_registry\_path] Für das acc-operator Bild zum Registrierungspfad, in dem Sie die Bilder in ein geschoben haben [Vorheriger Schritt](#).
- d. Fügen Sie dem die folgenden Werte hinzu env Abschnitt:

```
- name: ACCOP_HELM_UPGRADE_TIMEOUT
  value: 300m
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
    name: acc-operator-controller-manager
    namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
        - args:
            - --secure-listen-address=0.0.0.0:8443
```

```

- --upstream=http://127.0.0.1:8080/
- --logtostderr=true
- --v=10
image: [your_registry_path]/kube-rbac-proxy:v4.8.0
name: kube-rbac-proxy
ports:
- containerPort: 8443
  name: https
- args:
- --health-probe-bind-address=:8081
- --metrics-bind-address=127.0.0.1:8080
- --leader-elect
env:
- name: ACCOP_LOG_LEVEL
  value: "2"
- name: ACCOP_HELM_UPGRADE_TIMEOUT
  value: 300m
image: [your_registry_path]/acc-operator:[version x.y.z]
imagePullPolicy: IfNotPresent
livenessProbe:
  httpGet:
    path: /healthz
    port: 8081
    initialDelaySeconds: 15
    periodSeconds: 20
name: manager
readinessProbe:
  httpGet:
    path: /readyz
    port: 8081
    initialDelaySeconds: 5
    periodSeconds: 10
resources:
  limits:
    cpu: 300m
    memory: 750Mi
  requests:
    cpu: 100m
    memory: 75Mi
securityContext:
  allowPrivilegeEscalation: false
imagePullSecrets: []
securityContext:
  runAsUser: 65532
terminationGracePeriodSeconds: 10

```

### 3. Installieren Sie den aktualisierten Astra Control Center-Operator:

```
kubectl apply -f astra_control_center_operator_deploy.yaml
```

Beispielantwort:

```
namespace/netapp-acc-operator unchanged
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.astra.
netapp.io configured
role.rbac.authorization.k8s.io/acc-operator-leader-election-role
unchanged
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role
configured
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
unchanged
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role unchanged
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding unchanged
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding configured
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding unchanged
configmap/acc-operator-manager-config unchanged
service/acc-operator-controller-manager-metrics-service unchanged
deployment.apps/acc-operator-controller-manager configured
```

### 4. Überprüfen Sie, ob Pods ausgeführt werden:

```
kubectl get pods -n netapp-acc-operator
```

## Upgrade Astra Control Center

#### 1. Bearbeiten der benutzerdefinierten Ressource des Astra Control Center (CR):

```
kubectl edit AstraControlCenter -n [netapp-acc or custom namespace]
```

#### 2. Ändern Sie die Versionsnummer des Astra (astraVersion Innerhalb von spec) Zu der Version, auf die Sie aktualisieren:

```
spec:
  accountName: "Example"
  astraVersion: "[Version number]"
```

3. Überprüfen Sie, ob Ihr Image-Registrierungspfad mit dem von Ihnen gedrückten Registrierungspfad übereinstimmt [Vorheriger Schritt](#). Aktualisierung imageRegistry Innerhalb von Spec Wenn sich die Registrierung seit Ihrer letzten Installation geändert hat.

```
imageRegistry:
  name: "[your_registry_path]"
```

4. Fügen Sie Folgendes zu Ihrem hinzu CRDs Konfiguration in Spec:

```
crds:
  shouldUpgrade: true
```

5. Fügen Sie die folgenden Zeilen in hinzu additionalValues Innerhalb von Spec Im Astra Control Center CR:

```
additionalValues:
  nautilus:
    startupProbe:
      periodSeconds: 30
      failureThreshold: 600
```

Nachdem Sie den Datei-Editor gespeichert und beendet haben, werden die Änderungen übernommen und das Upgrade wird gestartet.

6. (Optional) Stellen Sie sicher, dass die Pods beendet werden und wieder verfügbar sind:

```
watch kubectl get pods -n [netapp-acc or custom namespace]
```

7. Warten Sie, bis die Statusbedingungen des Astra Control angezeigt werden, um anzuzeigen, dass das Upgrade abgeschlossen und bereit ist (True):

```
kubectl get AstraControlCenter -n [netapp-acc or custom namespace]
```

Antwort:

NAME	UUID	VERSION	ADDRESS
READY			
astra	9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f	22.11.0-82	
10.111.111.111	True		



Führen Sie den folgenden Befehl aus, um den Upgrade-Status während des Vorgangs zu überwachen: `kubectl get AstraControlCenter -o yaml -n [netapp-acc or custom namespace]`



Führen Sie den folgenden Befehl aus, um die Bedienerprotokolle des Astra Control Center zu überprüfen:

`kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f`

## Überprüfen Sie den Systemstatus

1. Melden Sie sich beim Astra Control Center an.
2. Überprüfen Sie, ob die Version aktualisiert wurde. Weitere Informationen finden Sie auf der Seite **Support** in der Benutzeroberfläche.
3. Vergewissern Sie sich, dass alle gemanagten Cluster und Applikationen weiterhin vorhanden und geschützt sind.

## Deinstallieren Sie Astra Control Center

Möglicherweise müssen Sie die Komponenten des Astra Control Center entfernen, wenn Sie ein Upgrade von einer Testversion auf eine Vollversion des Produkts durchführen. Um Astra Control Center und den Astra Control Center Operator zu entfernen, führen Sie die in diesem Verfahren beschriebenen Befehle nacheinander aus.

Wenn Sie Probleme mit der Deinstallation haben, lesen Sie [Fehlerbehebung bei Deinstallationsproblemen](#).

### Was Sie benötigen

- Verwenden Sie die Benutzeroberfläche von Astra Control Center, um das Management aller zu lösen "Cluster".

### Schritte

1. Löschen Sie Das Astra Control Center. Der folgende Beispielbefehl basiert auf einer Standardinstallation. Ändern Sie den Befehl, wenn Sie benutzerdefinierte Konfigurationen erstellt haben.

```
kubectl delete -f astra_control_center.yaml -n netapp-acc
```

Ergebnis:

```
astracontrolcenter.astra.netapp.io "astra" deleted
```

2. Löschen Sie den mit dem folgenden Befehl `netapp-acc` Namespace:

```
kubectl delete ns netapp-acc
```

Ergebnis:

```
namespace "netapp-acc" deleted
```

3. Löschen Sie die Komponenten des Astra Control Center-Bediensystems mit dem folgenden Befehl:

```
kubectl delete -f astra_control_center_operator_deploy.yaml
```

Ergebnis:

```
namespace/netapp-acc-operator deleted
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.astra.
netapp.io deleted
role.rbac.authorization.k8s.io/acc-operator-leader-election-role deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role deleted
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding deleted
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding deleted
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding deleted
configmap/acc-operator-manager-config deleted
service/acc-operator-controller-manager-metrics-service deleted
deployment.apps/acc-operator-controller-manager deleted
```

## Fehlerbehebung bei Deinstallationsproblemen

Verwenden Sie die folgenden Problemumgehungen, um Probleme bei der Deinstallation von Astra Control Center zu beheben.



## Bei der Deinstallation des Astra Control Center wird der Monitor-Operator POD im Managed Cluster nicht bereinigt

Wenn Sie das Management Ihrer Cluster nicht rückgängig gemacht haben, bevor Sie Astra Control Center deinstalliert haben, können Sie die Pods im netapp-Monitoring Namespace und den Namespace manuell mit den folgenden Befehlen löschen:

### Schritte

1. Löschen `acc-monitoring` Agent:

```
kubectl delete agents acc-monitoring -n netapp-monitoring
```

Ergebnis:

```
agent.monitoring.netapp.com "acc-monitoring" deleted
```

2. Löschen Sie den Namespace:

```
kubectl delete ns netapp-monitoring
```

Ergebnis:

```
namespace "netapp-monitoring" deleted
```

3. Bestätigen der entfernten Ressourcen:

```
kubectl get pods -n netapp-monitoring
```

Ergebnis:

```
No resources found in netapp-monitoring namespace.
```

4. Bestätigen Sie, dass der Monitoring Agent entfernt wurde:

```
kubectl get crd|grep agent
```

Beispielergebnis:

```
agents.monitoring.netapp.com                2021-07-21T06:08:13Z
```

## 5. Informationen zur benutzerdefinierten Ressourcendefinition löschen:

```
kubectl delete crds agents.monitoring.netapp.com
```

Ergebnis:

```
customresourcedefinition.apiextensions.k8s.io  
"agents.monitoring.netapp.com" deleted
```

## Bei der Deinstallation von Astra Control Center werden die Traefik CRDs nicht bereinigt

Sie können die Traefik-CRDs manuell löschen. CRDs sind globale Ressourcen, und das Löschen kann sich auf andere Anwendungen auf dem Cluster auswirken.

### Schritte

1. Führen Sie die auf dem Cluster installierten Traefik-CRDs auf:

```
kubectl get crds |grep -E 'traefik'
```

Antwort

ingressroutes.traefik.containo.us	2021-06-23T23:29:11Z
ingressroutetcps.traefik.containo.us	2021-06-23T23:29:11Z
ingressrouteudps.traefik.containo.us	2021-06-23T23:29:12Z
middlewares.traefik.containo.us	2021-06-23T23:29:12Z
middlewareetcps.traefik.containo.us	2021-06-23T23:29:12Z
serverstransports.traefik.containo.us	2021-06-23T23:29:13Z
tlsoptions.traefik.containo.us	2021-06-23T23:29:13Z
tlsstores.traefik.containo.us	2021-06-23T23:29:14Z
traefikservices.traefik.containo.us	2021-06-23T23:29:15Z

2. Löschen Sie die CRDs:

```
kubectl delete crd ingressroutes.traefik.containo.us  
ingressroutetcps.traefik.containo.us  
ingressrouteudps.traefik.containo.us middlewares.traefik.containo.us  
serverstransports.traefik.containo.us tlsoptions.traefik.containo.us  
tlsstores.traefik.containo.us traefikservices.traefik.containo.us  
middlewareetcps.traefik.containo.us
```

## Weitere Informationen

- ["Bekannte Probleme bei der Deinstallation"](#)

## Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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.