# Nutzen Sie Das Astra Control Center

Astra Control Center

NetApp
August 11, 2025

# Inhalt

# 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.

Sie können Apps definieren und managen, die Storage-Ressourcen mit laufenden Pods umfassen, oder Applikationen mit Storage-Ressourcen, ohne laufende Pods auszuführen. Applikationen, auf denen keine Pods ausgeführt werden, werden als reine Daten-Applikationen bezeichnet.

### Anforderungen für das Applikationsmanagement

Astra Control verfügt über folgende Anforderungen an das Applikationsmanagement:

- **Lizenzierung**: Um Anwendungen mit Astra Control Center zu verwalten, benötigen Sie entweder die eingebettete Astra Control Center-Evaluierungslizenz oder eine Volllizenz.
- **Namesaces**: 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), wird vollständig unterstützt. Das Verwalten von mit Helm 2 installierten Apps wird nicht unterstützt.
- **Vom Betreiber bereitgestellte Apps**: Astra Control unterstützt Apps, die mit Namespace-Scoped Operatoren installiert sind und im Allgemeinen mit einer "Pass-by-value" anstatt einer "Pass-by-reference" Architektur konzipiert sind. Ein Operator und die App, die er installiert, müssen denselben Namespace verwenden. Möglicherweise müssen Sie die YAML-Bereitstellungsdatei für den Operator 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

Nach dem haben "Hat den Cluster hinzugefügt" Bei Astra Control 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.

**Bevor Sie beginnen**

- Astra Control ist ein Kubernetes Cluster.
- Eine oder mehrere installierte Applikationen auf dem Cluster. Weitere Informationen zu unterstützten App-Installationsmethoden.
- 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 Namespace.
- 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.

**Erweitern Sie, um weitere Informationen über das Hinzufügen von Ressourcen mit Clusterbereich zu Ihren App-Namespaces zu erhalten.**

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

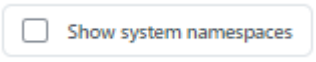
Sie können alle Kubernetes-Ressourcen im Namespace zum Astra Control Management hinzufügen, indem Sie die Ressourcen dieses Namespace als Applikation definieren. Diese Methode ist es besser, Apps einzeln zu definieren, wenn Sie alle Ressourcen in einem bestimmten Namespace ähnlich und in gemeinsamen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

#### Schritte

1. Wählen Sie auf der Seite Cluster einen Cluster aus.
2. Wählen Sie die Registerkarte **Namesaces** 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.



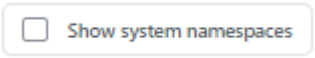

"Weitere Informationen".

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.




Astra Control Center wird standardmäßig nicht als eine Applikation angezeigt, die Sie managen können. Sie können jedoch eine Astra Control Center-Instanz sichern und wiederherstellen.

## Beispiel: Separate Sicherungsrichtlinie 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" Erstellen eines Remote-Clusters mithilfe von NetApp SnapMirror. 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
- Backup und Restore für den wirtschaftlichen Betrieb von ontap-nas
- Unveränderliches Backup erstellen
- 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".

> Wenn Sie eine Schutzrichtlinie definieren, die unveränderliche Backups für WORM-Buckets (Write Once Read Many) erstellt, stellen Sie sicher, dass die Aufbewahrungszeit für die Backups nicht kürzer ist als der für den Bucket konfigurierte Aufbewahrungszeitraum.

Verschieben Sie Backup- und Replikationspläne, um Zeitplanüberschneidungen zu vermeiden. Führen Sie beispielsweise jede Stunde Backups oben in der Stunde durch, und planen Sie die Replikation, um mit einem Offset von 5 Minuten und einem Intervall von 10 Minuten zu beginnen.

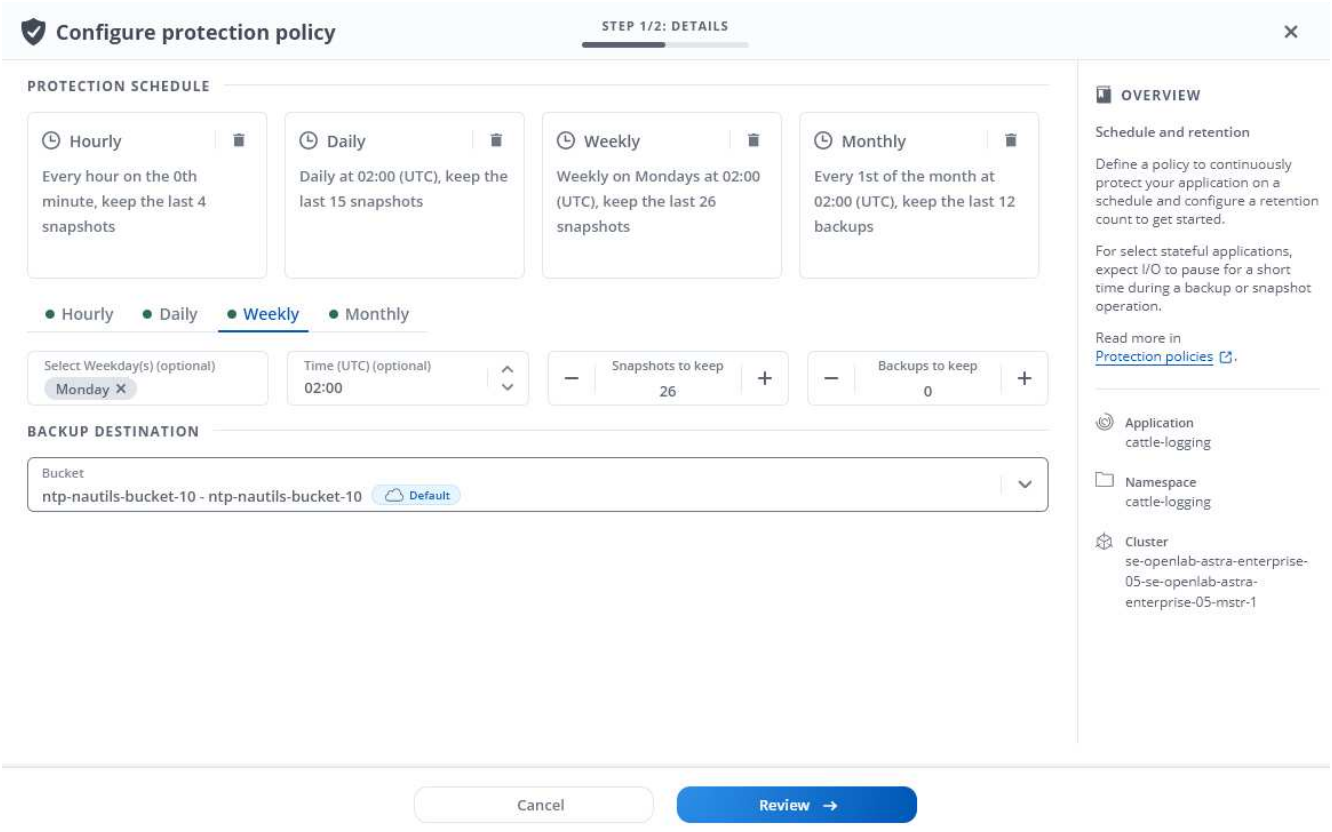
**Schritte**

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.




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.

#### Über diese Aufgabe

Astra Control unterstützt die Snapshot-Erstellung mithilfe von Storage-Klassen, die von den folgenden Treibern unterstützt werden:

- `ontap-nas`
- `ontap-san`
- `ontap-san-economy`

> Wenn Ihre App eine von der unterstützte Storage-Klasse verwendet `ontap-nas-economy` Treiber, Snapshots können nicht erstellt werden. Verwenden Sie eine alternative Storage-Klasse für Snapshots.

#### 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 jederzeit sichern.

#### Über diese Aufgabe

Buckets in Astra Control berichten nicht über die verfügbare Kapazität. Bevor Sie von Astra Control gemanagte Applikationen sichern oder klonen, überprüfen Sie Bucket-Informationen im entsprechenden Storage-Managementsystem.

Wenn Ihre App eine von der unterstützte Storage-Klasse verwendet `ontap-nas-economy` Fahrer, müssen Sie Aktivieren Sie Backup und Restore Funktionalität. Stellen Sie sicher, dass Sie einen definiert haben `backendType` Parameter in im "Kubernetes Storage-Objekt" Mit einem Wert von `ontap-nas-economy` Bevor Sie Schutzmaßnahmen durchführen.

Astra Control unterstützt die Backup-Erstellung mithilfe von Storage-Klassen, die von den folgenden Treibern unterstützt werden:

- `ontap-nas`
- `ontap-nas-economy`
- `ontap-san`
- `ontap-san-economy`

**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.

### Backup und Restore für den wirtschaftlichen Betrieb von ontap-nas

Astra Control Provisioner bietet Backup- und Restore-Funktionen für Storage-Back-Ends, die das verwenden `ontap-nas-economy` Storage-Klasse.

**Bevor Sie beginnen**

- Das ist schon "Astra Control Provisioner wurde aktiviert".
- Sie haben eine Anwendung in Astra Control definiert. Diese Anwendung verfügt nur über begrenzte Schutzfunktionen, bis Sie diesen Vorgang abgeschlossen haben.
- Das ist schon `ontap-nas-economy` Ausgewählt als Standard-Storage-Klasse für Ihr Storage-Back-End.

**Erweitern Sie für Konfigurationsschritte**

1. Gehen Sie auf dem ONTAP Storage Back-End folgendermaßen vor:

   a. Finden Sie die SVM, die den hostet `ontap-nas-economy`-Basierte Volumen der Anwendung.

   b. Melden Sie sich bei einem Terminal an, das mit ONTAP verbunden ist, wo die Volumes erstellt werden.

   c. Snapshot-Verzeichnis für SVM ausblenden:

   > Diese Änderung wirkt sich auf die gesamte SVM aus. Auf das verborgene Verzeichnis kann weiterhin zugegriffen werden.

   ```
   nfs modify -vserver <svm name> -v3-hide-snapshot enabled
   ```

   +

   > Vergewissern Sie sich, dass das Snapshot-Verzeichnis auf dem ONTAP-Speicher-Back-End verborgen ist. Das Ausblenden dieses Verzeichnisses kann zu einem Verlust des Zugriffs auf Ihre Anwendung führen, insbesondere wenn es NFSv3 verwendet.

2. Gehen Sie in Astra Trident wie folgt vor:

   a. Aktivieren Sie das Snapshot-Verzeichnis für jedes PV, das ist `ontap-nas-economy` Basiert und mit der Applikation verknüpft:

   ```
   tridentctl update volume <pv name> --snapshot-dir=true --pool
   -level=true -n trident
   ```

   b. Vergewissern Sie sich, dass das Snapshot-Verzeichnis für jedes zugeordnete PV aktiviert wurde:

   ```
   tridentctl get volume <pv name> -n trident -o yaml | grep
   snapshotDir
   ```

   Antwort:

   ```
   snapshotDirectory: "true"
   ```

3. Aktualisieren Sie in Astra Control die Applikation nach Aktivierung aller zugehörigen Snapshot-Verzeichnisse, damit Astra Control den geänderten Wert erkennt.

**Ergebnis**

Die Applikation ist bereit für Backups und Restores mit Astra Control. Jede PVC kann auch von anderen Anwendungen für Backups und Wiederherstellungen verwendet werden.

### Unveränderliches Backup erstellen

Ein unveränderliches Backup kann nicht geändert, gelöscht oder überschrieben werden, solange die Aufbewahrungsrichtlinie auf dem Bucket, der das Backup speichert, dies verbietet. Erstellen Sie unveränderliche Backups, indem Sie Applikationen in Buckets sichern, für die eine Aufbewahrungsrichtlinie konfiguriert ist. Siehe "Datensicherung" Finden Sie wichtige Informationen zum Arbeiten mit unveränderlichen Backups.

#### Bevor Sie beginnen

Sie müssen den Ziel-Bucket mit einer Aufbewahrungsrichtlinie konfigurieren. Je nachdem, welchen Storage-Anbieter Sie verwenden, hängt die Vorgehensweise davon ab. Weitere Informationen finden Sie in der Dokumentation des Speicheranbieters:

- **Amazon Web Services**: "Aktivieren Sie S3 Object Lock beim Erstellen des Buckets und legen Sie den Standardaufbewahrungsmodus „Governance“ mit einer Standardaufbewahrungszeit fest".
- **NetApp StorageGRID**: "Aktivieren Sie S3 Object Lock beim Erstellen des Buckets und legen Sie den Standardaufbewahrungsmodus „Compliance“ mit einer Standardaufbewahrungsdauer fest".

> Buckets in Astra Control berichten nicht über die verfügbare Kapazität. Bevor Sie von Astra Control gemanagte Applikationen sichern oder klonen, überprüfen Sie Bucket-Informationen im entsprechenden Storage-Managementsystem.

> Wenn Ihre App eine von der unterstützte Storage-Klasse verwendet `ontap-nas-economy` Treiber, stellen Sie sicher, dass Sie einen definiert haben `backendType` Parameter in im "Kubernetes Storage-Objekt" Mit einem Wert von `ontap-nas-economy` Bevor Sie Schutzmaßnahmen durchführen.

#### 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. Ein WORM-Bucket (Write Once Read Many) wird neben dem Bucket-Namen mit dem Status „gesperrt“ angezeigt.

   > Wenn es sich bei dem Bucket um einen nicht unterstützten Typ handelt, wird dies angezeigt, wenn Sie den Mauszeiger über den Bucket bewegen oder ihn auswählen.

6. Wählen Sie **Weiter**.
7. Überprüfen Sie die Backup-Zusammenfassung und wählen Sie **Backup**.

#### Ergebnis

Astra Control erstellt eine unveränderliche Sicherung 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 versuchen, zwei unveränderliche Backups derselben App gleichzeitig im selben Bucket zu erstellen, verhindert Astra Control, dass das zweite Backup gestartet wird. Warten Sie, bis die erste Sicherung abgeschlossen ist, bevor Sie eine andere starten.
- Sie können ein auslaufendes unveränderliches Backup nicht abbrechen.
- 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.

Ein unveränderliches Backup wird neben dem verwendeten Bucket mit dem Status „gesperrt“ angezeigt.

#### 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.

Sie können ein auslaufendes unveränderliches Backup nicht abbrechen.

**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. Sie können ein Backup, das an einem unveränderlichen Bucket erstellt wurde, erst dann löschen, wenn dies durch die Aufbewahrungsrichtlinie des Buckets möglich ist.

Sie können ein unveränderliches Backup nicht vor Ablauf der Aufbewahrungsfrist löschen.

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 "Astra Control API" Zur Wiederherstellung von Applikationen.

**Bevor Sie beginnen**

- **Schützen Sie Ihre Anwendungen zuerst**: Es wird dringend empfohlen, dass Sie einen Snapshot oder ein Backup Ihrer Anwendung vor der Wiederherstellung machen. Auf diese Weise können Sie aus dem Snapshot oder Backup klonen, wenn die Wiederherstellung nicht erfolgreich war.
- **Zieldatenträger prüfen**: Wenn Sie eine andere Speicherklasse wiederherstellen, stellen Sie sicher, dass die Speicherklasse den gleichen persistenten Zugriffsmodus für Volumes verwendet (z. B. ReadWriteMany). Der Wiederherstellungsvorgang schlägt fehl, wenn der Zugriffsmodus des Ziel-persistenten Volumes anders ist. Wenn das persistente Quell-Volume beispielsweise den RWX-Zugriffsmodus verwendet, wählen Sie eine Ziel-Storage-Klasse aus, die RWX nicht bereitstellen kann, wie z. B. Azure Managed Disks, AWS EBS, Google Persistent Disk oder `ontap-san`Wird dazu führen, dass der Wiederherstellungsvorgang fehlschlägt. Weitere Informationen zu den Zugriffsmodi für persistente Volumes finden Sie im "Kubernetes" Dokumentation.
- **Planung des Platzbedarfs**: Wenn Sie eine in-Place-Wiederherstellung einer Applikation durchführen, die NetApp ONTAP Storage nutzt, kann sich der von der wiederhergestellten Applikation genutzte Speicherplatz verdoppeln. Nachdem Sie eine in-Place-Wiederherstellung durchgeführt haben, entfernen Sie alle unerwünschten Snapshots aus der wiederhergestellten Applikation, um Speicherplatz freizugeben.
- **(nur Red hat 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
```

- **Unterstützte Storage Class Treiber**: Astra Control unterstützt die Wiederherstellung von Backups mit Speicherklassen, die von den folgenden Treibern unterstützt werden:
  - `ontap-nas`
  - `ontap-nas-economy`
  - `ontap-san`
  - `ontap-san-economy`
- **(nur ontap-nas-Economy-Treiber) Backups und Wiederherstellungen**: Vor dem Backup oder der Wiederherstellung einer App, die eine von der unterstützte Storage-Klasse verwendet `ontap-nas-economy` Überprüfen Sie, ob der "Das snapshot Verzeichnis auf dem ONTAP Storage-Backend ist verborgen". Das Ausblenden dieses Verzeichnisses kann zu einem Verlust des Zugriffs auf Ihre Anwendung führen, insbesondere wenn es NFSv3 verwendet.
- **Helm bereitgestellte Apps**: Apps, die mit Helm 3 (oder von Helm 2 auf Helm 3 aktualisiert) bereitgestellt werden, werden vollständig unterstützt. Mit Helm 2 implementierte Apps werden nicht unterstützt.

> 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. Weitere Informationen finden Sie unter bei der Ressourcen mit einer anderen App geteilt werden,Dieses Beispiel.

**Schritte**

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie im Menü Optionen in der Spalte Aktionen die Option **Wiederherstellen** aus.
3. 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.

     > Wenn Ihre App eine von der unterstützte Storage-Klasse verwendet `ontap-nas-economy` Treiber, müssen Sie die App mithilfe der ursprünglichen Speicherklassen wiederherstellen. Sie können keine andere Storage-Klasse angeben, wenn Sie die App im gleichen Namespace wiederherstellen.

     i. Wählen Sie den Snapshot oder das Backup aus, mit dem die App direkt wiederhergestellt werden soll. Dadurch wird die App auf eine frühere Version von selbst zurückgesetzt.

     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.

   - **Wiederherstellen auf neuen Namespaces**: Verwenden Sie dieses Verfahren, um die App auf einem anderen Cluster oder mit verschiedenen Namespaces von der Quelle wiederherzustellen.

     i. Geben Sie den Namen für die wiederhergestellte App an.

     ii. Wählen Sie das Ziel-Cluster für die Anwendung aus, die Sie wiederherstellen möchten.

     iii. 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.

     iv. Wählen Sie **Weiter**.

     v. Wählen Sie den Snapshot oder das Backup aus, mit dem die App wiederhergestellt werden soll.

     vi. Wählen Sie **Weiter**.

     vii. Folgenden Optionen wählbar:

     - **Wiederherstellung unter Verwendung der ursprünglichen Speicherklassen**: Die Anwendung verwendet die ursprünglich zugeordnete Speicherklasse, es sei denn, sie existiert nicht auf dem Zielcluster. In diesem Fall wird die Standard-Storage-Klasse für das Cluster verwendet.
     - **Wiederherstellen mit einer anderen Storage-Klasse**: Wählen Sie eine Storage-Klasse aus, die auf dem Ziel-Cluster vorhanden ist. Alle Applikations-Volumes, unabhängig von den ursprünglich zugewiesenen Storage-Klassen, werden im Rahmen der Wiederherstellung in diese andere Storage-Klasse migriert.

     viii. Wählen Sie **Weiter**.
4. Wählen Sie die Ressourcen aus, die gefiltert werden sollen:
   - **Alle Ressourcen wiederherstellen**: Alle mit der ursprünglichen App verknüpften Ressourcen

wiederherstellen.

- **Ressourcen filtern**: Geben Sie Regeln an, um einen Untersatz der ursprünglichen Anwendungsressourcen wiederherzustellen:
  i. Wählen Sie diese Option, um Ressourcen aus der wiederhergestellten Anwendung einzuschließen oder auszuschließen.
  ii. Wählen Sie entweder **Include rule** oder **Add exclude rule** aus und konfigurieren Sie die Regel, um die richtigen Ressourcen während der Anwendungswiederherstellung zu filtern. Sie können eine Regel bearbeiten oder entfernen und eine Regel erneut erstellen, bis die Konfiguration korrekt ist.

> Weitere Informationen zum Konfigurieren von Einschließen- und Ausschlussregeln finden Sie unter Filtern Sie Ressourcen während einer Anwendungswiederherstellung.

5. Wählen Sie **Weiter**.
6. Lesen Sie die Details zur Wiederherstellungsaktion sorgfältig durch, geben Sie „Restore“ ein (falls Sie dazu aufgefordert werden), und wählen Sie **Restore**.

**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 durch einen Klon- oder Wiederherstellungsvorgang ein neuer Namespace erstellt wurde, kann der Kontoadministrator/Kontoinhaber das Mitgliedskonto bearbeiten und Rolleneinschränkungen aktualisieren, damit der betroffene Benutzer Zugriff auf den neuen Namespace gewährt.

### Filtern Sie Ressourcen während einer Anwendungswiederherstellung

Sie können eine Filterregel zu einem hinzufügen "Wiederherstellen" Vorgang, bei dem vorhandene Anwendungsressourcen angegeben werden, die in die wiederhergestellte Anwendung einbezogen oder von ihr ausgeschlossen werden sollen. Sie können Ressourcen basierend auf einem bestimmten Namespace, Label oder GVK (GroupVersionRind) ein- oder ausschließen.

**Erweitern Sie die Erweiterung, um weitere Informationen über ein- und Ausschlussszenarien zu erhalten**

- **Sie wählen eine Include-Regel mit ursprünglichen Namespaces (in-Place-Wiederherstellung)**: Vorhandene Anwendungsressourcen, die Sie in der Regel definieren, werden gelöscht und durch jene aus dem ausgewählten Snapshot oder Backup ersetzt, den Sie für die Wiederherstellung verwenden. Alle Ressourcen, die Sie nicht in der Include-Regel angeben, bleiben unverändert.
- **Sie wählen eine Include-Regel mit neuen Namespaces**: Verwenden Sie die Regel, um die spezifischen Ressourcen auszuwählen, die Sie in der wiederhergestellten Anwendung benötigen. Alle Ressourcen, die Sie nicht in der Include-Regel angeben, werden nicht in die wiederhergestellte Anwendung aufgenommen.
- **Sie wählen eine Ausschlussregel mit ursprünglichen Namespaces (in-Place-Wiederherstellung)**: Die von Ihnen angegebenen Ressourcen werden nicht wiederhergestellt und bleiben unverändert. Ressourcen, die Sie nicht ausschließen möchten, werden vom Snapshot oder Backup wiederhergestellt. Alle Daten auf persistenten Volumes werden gelöscht und neu erstellt, wenn das entsprechende StatefulSet Teil der gefilterten Ressourcen ist.
- **Sie wählen eine Ausschlussregel mit neuen Namespaces** aus: Wählen Sie mit der Regel die Ressourcen aus, die Sie aus der wiederhergestellten Anwendung entfernen möchten. Ressourcen, die Sie nicht ausschließen möchten, werden vom Snapshot oder Backup wiederhergestellt.

Regeln sind entweder Einschließen oder Ausschließen von Typen. Regeln, die Ressourceneinschluss und -Ausschluss kombinieren, sind nicht verfügbar.

**Schritte**

1. Nachdem Sie die Option Ressourcen filtern und im Assistenten zum Wiederherstellen von Apps eine Option ein- oder ausschließen ausgewählt haben, wählen Sie **Einschlussregel hinzufügen** oder **Ausschlussregel hinzufügen** aus.

   Sie können keine im Cluster enthaltenen Ressourcen ausschließen, die von Astra Control automatisch berücksichtigt werden.

2. Konfigurieren Sie die Filterregel:

   Sie müssen mindestens einen Namespace, eine Bezeichnung oder GVK angeben. Stellen Sie sicher, dass alle Ressourcen, die Sie behalten, nachdem die Filterregeln angewendet wurden, ausreichend sind, um die wiederhergestellte Anwendung in einem ordnungsgemäßen Zustand zu halten.

   a. Wählen Sie einen bestimmten Namespace für die Regel aus. Wenn Sie keine Auswahl treffen, werden alle Namespaces im Filter verwendet.

      Wenn Ihre Anwendung ursprünglich mehrere Namespaces enthielt und Sie sie in neuen Namespaces wiederherstellen, werden alle Namespaces erstellt, auch wenn sie keine Ressourcen enthalten.

   b. (Optional) Geben Sie einen Ressourcennamen ein.

   c. (Optional) **Etikettenauswahl**: A einschließen "Etikettenauswahl" Um der Regel hinzuzufügen. Mit der Etikettenauswahl werden nur die Ressourcen gefiltert, die der ausgewählten Bezeichnung entsprechen.

   d. (Optional) Wählen Sie **Use GVK (GroupVersionRind) Set, um Ressourcen zu filtern**, um weitere

Filteroptionen zu erhalten.

> Wenn Sie einen GVK-Filter verwenden, müssen Sie Version und Art angeben.

i. (Optional) **Gruppe**: Wählen Sie aus der Dropdown-Liste die Kubernetes API-Gruppe aus.
ii. **Kind**: Wählen Sie aus der Dropdown-Liste das Objektschema für den Kubernetes-Ressourcentyp aus, der im Filter verwendet werden soll.
iii. **Version**: Wählen Sie die Kubernetes API Version.

3. Überprüfen Sie die Regel, die auf Ihren Einträgen erstellt wird.
4. Wählen Sie **Hinzufügen**.

> Sie können beliebig viele Regeln für ein- und Ausschlussressourcen erstellen. Die Regeln werden in der Zusammenfassung der Wiederherstellungsanwendung angezeigt, bevor Sie den Vorgang starten.

#### In-Place-Wiederherstellungskomplikationen für eine App, bei der Ressourcen mit einer anderen App geteilt werden

Sie können einen in-Place-Wiederherstellungsvorgang für eine App durchführen, die Ressourcen mit einer anderen App teilt und unbeabsichtigte Ergebnisse liefert. Alle Ressourcen, die von den Applikationen gemeinsam genutzt werden, werden ersetzt, wenn eine in-Place-Wiederherstellung für eine der Applikationen durchgeführt wird.

Im Folgenden sehen Sie ein Beispielszenario, das eine unerwünschte Situation verursacht, wenn die NetApp SnapMirror Replizierung für eine Wiederherstellung verwendet wird:

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.

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

Einen Vergleich zwischen Backups/Wiederherstellungen und Replikation finden Sie unter "Konzepte zur Datensicherung".

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

Multi-Cloud-Szenarien:

- Standort A vor Ort zu Standort A
- 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 App 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-Funktion einer replizierten Anwendung 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

Für die Replizierung der Astra Control Applikation müssen vor Beginn die folgenden Voraussetzungen erfüllt sein:

#### ONTAP Cluster

- **Astra Trident**: Astra Trident Version 22.10 oder höher muss sowohl auf den Quell- als auch auf den Ziel-Kubernetes-Clustern vorhanden sein, die ONTAP als Backend nutzen. Astra Control unterstützt die Replizierung mit NetApp SnapMirror Technologie unter Verwendung von Storage-Klassen, die von den folgenden Treibern unterstützt werden:
  - `ontap-nas`
  - `ontap-san`
- **Lizenzen**: Asynchrone Lizenzen von ONTAP SnapMirror, die das Datensicherungspaket verwenden, müssen sowohl auf den Quell- als auch auf den Ziel-ONTAP-Clustern aktiviert sein. Siehe "Übersicht über die SnapMirror Lizenzierung in ONTAP" Finden Sie weitere Informationen.

#### Peering

- **Cluster und SVM**: Die ONTAP Speicher-Back-Ends müssen aktiviert werden. Siehe "Übersicht über Cluster- und SVM-Peering" Finden Sie weitere Informationen.

Vergewissern Sie sich, dass die in der Replizierungsbeziehung zwischen zwei ONTAP-Clustern verwendeten SVM-Namen eindeutig sind.

- **Astra Trident und SVM**: Die Peering von Remote-SVMs müssen für Astra Trident auf dem Ziel-Cluster verfügbar sein.

**Astra Control Center**

- **Managed Back-Ends**: Sie müssen ONTAP Storage Back-Ends in Astra Control Center hinzufügen und verwalten, um eine Replikationsbeziehung zu erstellen.

  ***nur Astra Control Provisioner***: Das Hinzufügen und Managen von ONTAP-Storage-Back-Ends in Astra Control Center ist optional, wenn Sie die Astra Control Provisioner für Astra Control Center 23.10 oder höher aktiviert haben.

- **Verwaltete Cluster**: Fügen Sie mit Astra Control die folgenden Cluster hinzu und verwalten Sie sie idealerweise an verschiedenen Ausfalldomänen oder Standorten:
  - Quell-Kubernetes-Cluster
  - Kubernetes Ziel-Cluster
  - Zugeordnete ONTAP-Cluster
- **Benutzerkonten**: Wenn Sie ein ONTAP-Speicher-Backend zu Astra Control Center hinzufügen, wenden Sie die Anmeldeinformationen des Benutzers mit der Rolle "admin" an. Diese Rolle verfügt über Zugriffsmethoden `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.

  ***nur Astra Control Provisioner***: Wenn Sie die Astra Control Provisioner-Funktion aktiviert haben, müssen Sie zum Managen von Clustern in Astra Control Center keine spezielle „Admin“-Rolle mehr definieren, da diese Zugangsdaten in Astra Control Center nicht mehr erforderlich sind.

"Implementieren Sie Astra Control Center" In einer dritten Fehlerdomäne oder an einem sekundären Standort für nahtloses Disaster Recovery

Astra Control Center unterstützt keine NetApp SnapMirror Replizierung für Storage-Back-Ends, die das NVMe-over-TCP-Protokoll verwenden.

**Konfiguration von Astra Trident/ONTAP**

Für Astra Control Center müssen Sie mindestens ein Storage-Back-End konfigurieren, das die Replizierung sowohl für die Quell- als auch für die Ziel-Cluster unterstützt. Wenn die Quell- und Ziel-Cluster identisch sind, sollte die Zielanwendung ein anderes Speicher-Back-End als die Quellanwendung verwenden, um die beste Ausfallsicherheit zu erreichen.

Die Astra Control Replizierung unterstützt Applikationen, die eine einzige Storage-Klasse verwenden. Wenn Sie eine App zu einem Namespace hinzufügen, stellen Sie sicher, dass die App dieselbe Storage-Klasse wie andere Apps im Namespace hat. Wenn Sie eine PVC zu einer replizierten App hinzufügen, stellen Sie sicher, dass die neue PVC die gleiche Speicherklasse hat wie andere VES im Namespace.

### Richten Sie eine Replikationsbeziehung ein

Die Einrichtung einer Replikationsbeziehung umfasst Folgendes:

- Festlegen der Häufigkeit, mit der Astra Control einen App-Snapshot erstellen soll (einschließlich der Kubernetes-Ressourcen der Applikation sowie der Volume-Snapshots für die jeweiligen Volumes der Applikation)
- Auswahl des Replizierungszeitplans (einschließlich Kubernetes-Ressourcen und persistente Volume-Daten)
- Einstellen der Uhrzeit für die Erstellung des Snapshots

**Schritte**

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie die Registerkarte **Data Protection** > **Replication** aus.
3. Wählen Sie **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:
   - **Ziel-Cluster**: Geben Sie einen Ziel-Cluster ein (dies kann mit dem Quell-Cluster identisch sein).
   - **Ziel-Storage-Klasse**: Wählen oder geben Sie die Storage-Klasse ein, die die Peering-SVM auf dem Ziel-ONTAP-Cluster verwendet. Als Best Practice sollte die Ziel-Storage-Klasse auf ein anderes Storage-Back-End verweisen als die Quell-Storage-Klasse.
   - **Replikationstyp**: `Asynchronous` Ist derzeit der einzige verfügbare Replikationstyp.
   - **Ziel-Namespace**: Geben Sie neue oder vorhandene Ziel-Namespaces für das Ziel-Cluster ein.
   - (Optional) Fügen Sie zusätzliche Namespaces hinzu, indem Sie **Namespace hinzufügen** und den Namespace aus der Dropdown-Liste auswählen.
   - **Replikationsfrequenz**: Legen Sie fest, wie oft Astra Control einen Snapshot erstellen und an das Ziel replizieren soll.
   - **Offset**: Legen Sie die Anzahl der Minuten von der Spitze der Stunde fest, die Astra Control für einen Snapshot verwenden soll. Möglicherweise möchten Sie einen Offset verwenden, sodass er nicht mit anderen geplanten Vorgängen übereinstimmt.

   Verschieben Sie Backup- und Replikationspläne, um Zeitplanüberschneidungen zu vermeiden. Führen Sie beispielsweise jede Stunde Backups oben in der Stunde durch, und planen Sie die Replikation, um mit einem Offset von 5 Minuten und einem Intervall von 10 Minuten zu beginnen.

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** aus.

   Der Snapshot-Name verwendet das Format von `replication-schedule-<string>`. Astra Control behält den letzten Snapshot bei, der für die Replizierung verwendet wurde. Alle älteren Replikations-Snapshots werden nach erfolgreichem 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.
- Erstellt einen ersten applikationskonsistenten Snapshot.
- Erstellt mithilfe des ersten Snapshots die SnapMirror Beziehung für persistente Volumes.

Die Seite **Data Protection** zeigt den Status und den Status der Replikationsbeziehung an:
<Health status>, <Relationship life cycle state>

Beispiel:
Normal

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

### Online-Funktion einer replizierten Anwendung auf dem Ziel-Cluster (Failover)

Mit Astra Control können Sie ein Failover replizierter Applikationen auf ein Ziel-Cluster durchführen. 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 die Registerkarte **Data Protection** > **Replication** aus.
3. Wählen Sie im Menü Aktionen die Option **Failover**.
4. Überprüfen Sie auf der Seite Failover die Informationen, und wählen Sie **Failover**.

#### Ergebnis

Die folgenden Aktionen werden als Ergebnis des Failover-Verfahrens durchgeführt:

- Die Zielanwendung wird 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 auf Basis der zum Zeitpunkt des Failovers auf der Quell-App vorhandenen Zeitpläne in die Ziel-App kopiert.
- Wenn in der Quell-App mindestens eine Ausführungshaken nach der Wiederherstellung aktiviert ist, werden diese Ausführungshaken für die Ziel-App ausgeführt.
- 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 die Registerkarte **Data Protection** > **Replication** aus.
3. Wählen Sie im Menü Aktionen die Option **Resync**.
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 der geplante Vorgang, mit dem die Applikation auf das Ziel-Storage Back-End verschoben und gleichzeitig weiterhin zurück auf das ursprüngliche Quell-Storage Back-End repliziert werden soll. Astra Control stoppt die Quellapplikation und repliziert die Daten zum Ziel, bevor ein Failover zur Ziel-App durchgeführt wird.

In dieser Situation tauschen Sie Quelle und Ziel aus.

**Schritte**

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie die Registerkarte **Data Protection** > **Replication** aus.
3. Wählen Sie im Menü Aktionen die Option **Reverse Replication**.
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:

- Von den Kubernetes-Ressourcen der ursprünglichen Quell-Applikation wird ein Snapshot 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 App erstellt und repliziert.

- Die SnapMirror Beziehungen sind beschädigt, wodurch die Zieldatenträger für Lese-/Schreibvorgänge bereit sind.
- Die Kubernetes-Ressourcen der App werden aus dem Snapshot vor dem Herunterfahren wiederhergestellt. Dabei werden die Volume-Daten verwendet, die nach dem Herunterfahren der ursprünglichen Quell-App repliziert wurden.
- 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 mithilfe der folgenden Sequenz von Vorgängen „Failback“ erreichen. In diesem Workflow zur Wiederherstellung der ursprünglichen Replikationsrichtung repliziert (synchronisiert) Astra Control alle Anwendungsänderungen zurück zur ursprünglichen Quellanwendung, bevor die Replikationsrichtung umkehrt.

Dieser Prozess beginnt mit einer Beziehung, bei der ein Failover zu einem Ziel durchgeführt wurde, und umfasst die folgenden Schritte:

- 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 die Registerkarte **Data Protection** > **Replication** aus.
3. Wählen Sie im Menü Aktionen die Option **Resync**.
4. Wählen Sie für einen Failback-Vorgang die Failoveranwendung als Quelle für den Resync-Vorgang aus (unter Beibehaltung der nach dem Failover geschriebenen Daten).
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 die Registerkarte **Data Protection** > **Replication** aus.
3. Wählen Sie im Feld Anwendungsschutz oder im Beziehungsdiagramm **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 aufgebaut oder hat sich etabliert, und der letzte 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 wird hergestellt (so dass ein erfolgreicher Snapshot repliziert wurde und Failover möglich ist), aber der aktuelle Snapshot ist fehlgeschlagen oder konnte nicht repliziert werden.

### 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 VES verfügbar sind, überprüft die Replizierungsbeziehung, erstellt regelmäßig Snapshots der App und identifiziert neue Quell-VES in der App. Wenn ja, erstellt Astra Control die Ressourcen, die sie in die Replikation aufnehmen.
- **Failover**: Astra Control bricht die SnapMirror-Beziehungen und stellt die Kubernetes-Ressourcen der App aus dem zuletzt erfolgreich replizierten App-Snapshot wieder her.
- **Failover**: Astra Control stoppt die Replikation vom Quellcluster, 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 "Astra Control API" Zum Klonen und Migrieren von Applikationen

**Bevor Sie beginnen**

- **Zieldatenträger prüfen**: Wenn Sie in eine andere Speicherklasse klonen, stellen Sie sicher, dass die Speicherklasse den gleichen persistenten Zugriffsmodus für Volumes verwendet (z. B. ReadWriteMany). Der Klonvorgang schlägt fehl, wenn der Zugriffsmodus des persistenten Volume-Ziels anders ist. Wenn das persistente Quell-Volume beispielsweise den RWX-Zugriffsmodus verwendet, wählen Sie eine Ziel-Storage-Klasse aus, die RWX nicht bereitstellen kann, wie z. B. Azure Managed Disks, AWS EBS, Google Persistent Disk oder `ontap-san`, Führt dazu, dass der Klonvorgang fehlschlägt. Weitere Informationen zu den Zugriffsmodi für persistente Volumes finden Sie im "Kubernetes" Dokumentation.
- 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.
- **Anwendungen mit Unterstützung der ontap-nas-Wirtschaft**: Klonvorgänge können nicht verwendet werden, wenn die Storage-Klasse Ihrer Applikation von unterstützt wird `ontap-nas-economy` Treiber. Sie können es jedoch "Backup und Restore für den wirtschaftlichen Betrieb von ontap-nas".
- **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 durch einen Klon- oder Wiederherstellungsvorgang ein neuer Namespace erstellt wurde, kann der Kontoadministrator/Kontoinhaber das Mitgliedskonto bearbeiten und Rolleneinschränkungen aktualisieren, damit der betroffene Benutzer Zugriff auf den neuen Namespace gewährt.
- **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.
- **Mit einer bestimmten Version von PostgreSQL**: App-Klone innerhalb desselben Clusters schlagen mit dem Bitnami PostgreSQL 11.5.0-Chart konsequent fehl. Um erfolgreich zu klonen, verwenden Sie eine frühere oder höhere Version des Diagramms.

**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 die der App zugeordnete ursprüngliche Storage-Klasse beibehalten oder eine andere Storage-Klasse ausgewählt werden soll.

     Sie können die Storage-Klasse einer App zu einer Storage-Klasse eines nativen Cloud-Providers oder einer anderen unterstützten Storage-Klasse migrieren und eine App von einer Storage-Klasse migrieren, die von unterstützt wird `ontap-nas-economy` Zu einer Storage-Klasse, die von unterstützt wird `ontap-nas` Oder kopieren Sie die App in ein anderes Cluster mit einer Storage-Klasse, die von der unterstützt wird `ontap-nas-economy` Treiber.

   Wenn Sie eine andere Storage-Klasse auswählen und diese Storage-Klasse zum Zeitpunkt der Wiederherstellung nicht vorhanden ist, wird ein Fehler zurückgegeben.

5. Wählen Sie **Weiter**.
6. Überprüfen Sie die Informationen über den Klon und wählen Sie **Clone**.

**Ergebnis**

Astra Control klont 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 durch einen Klon- oder Wiederherstellungsvorgang ein neuer Namespace erstellt wurde, kann der Kontoadministrator/Kontoinhaber das Mitgliedskonto bearbeiten und Rolleneinschränkungen aktualisieren, damit der betroffene Benutzer Zugriff auf den neuen Namespace gewährt.

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 mit einem Execution-Hook alle Datenbanktransaktionen vor einem Snapshot anhalten und die Transaktionen nach Abschluss des Snapshots wieder aufnehmen. Dies gewährleistet applikationskonsistente Snapshots.

### Arten von Ausführungshaken

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

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

### Filter für Testausführungshaken

Wenn Sie einer Anwendung einen Ausführungshaken hinzufügen oder bearbeiten, können Sie einem Ausführungshaken Filter hinzufügen, um zu verwalten, mit welchen Containern der Hook übereinstimmt. Filter sind für Applikationen nützlich, die in allen Containern dasselbe Container-Image nutzen. Jedes Image kann jedoch für einen anderen Zweck (wie Elasticsearch) verwendet werden. Mit Filtern können Sie Szenarien erstellen, in denen Ausführungshaken auf einigen, aber nicht unbedingt allen identischen Containern ausgeführt werden. Wenn Sie mehrere Filter für einen einzelnen Testausführungshaken erstellen, werden diese mit einem logischen UND einem Operator kombiniert. Pro Testsuite können Sie bis zu 10 aktive Filter haben.

Jeder Filter, den Sie einem Execution Hook hinzufügen, verwendet einen regulären Ausdruck, um Container in Ihrem Cluster zu entsprechen. Wenn ein Haken einem Container entspricht, führt der Haken sein zugehöriges Skript auf diesem Container aus. Reguläre Ausdrücke für Filter verwenden die Syntax des regulären Ausdrucks 2 (RE2), die das Erstellen eines Filters nicht unterstützt, der Container aus der Liste der Übereinstimmungen ausschließt. Informationen zur Syntax, die Astra Control für regelmäßige Ausdrücke in Hook-Filter unterstützt, finden Sie unter "Syntaxunterstützung für regulären Ausdruck 2 (RE2)".

> Wenn Sie einem Ausführungs-Hook einen Namespace-Filter hinzufügen, der nach einer Wiederherstellung oder einem Klonvorgang ausgeführt wird, und die Wiederherstellungs- oder Klonquelle und das Ziel in verschiedenen Namespaces liegen, wird der Namespace-Filter nur auf den Ziel-Namespace angewendet.

### Wichtige Hinweise zu benutzerdefinierten Testausführungshaken

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

Da 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 die in einem Testsuite nach dem Backup verwendete Logik nicht davon ausgehen kann, dass das Backup abgeschlossen wurde.

- Die Ausführungshaken-Funktion ist bei neuen Astra Control-Bereitstellungen standardmäßig deaktiviert.
  - Sie müssen die Funktion „Ausführungshaken“ aktivieren, bevor Sie Ausführungshaken verwenden können.
  - Benutzer von Eigentümer oder Administrator können die Funktion „Ausführungshaken“ für alle Benutzer aktivieren oder deaktivieren, die im aktuellen Astra Control-Konto definiert sind. Siehe Aktivieren Sie die Funktion „Ausführungshaken“ Und Deaktivieren Sie die Funktion Ausführungshaken Weitere Anweisungen.
  - Der Status der Funktionsunterstützung bleibt bei Astra Control Upgrades erhalten.
- Ein Testsuite muss ein Skript verwenden, um Aktionen durchzuführen. Viele Testsuitehaoks 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.
- Für Ad-hoc-Datenschutzvorgänge werden alle Hook-Ereignisse generiert und im Ereignisprotokoll der Seite **Aktivität** 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 Astra Control Center einen Failover über eine replizierte Quell-App an die Ziel-App ausführt, werden nach dem Failover alle für die Quell-App aktivierten Ausführungs-Hooks für die Ziel-App ausgeführt.

Wenn Sie nach der Wiederherstellung Hooks mit Astra Control Center 23.04 ausgeführt und Ihr Astra Control Center auf 23.07 oder höher aktualisiert haben, werden die Hooks für die Ausführung nach der Wiederherstellung nach einer Failover-Replizierung nicht mehr ausgeführt. Sie müssen neue Ausführungshaken nach dem Failover für Ihre Apps erstellen. Alternativ können Sie den Operationstyp vorhandener Hooks nach der Wiederherstellung ändern, die für Failover von „nach der Wiederherstellung“ zu „nach dem Failover“ gedacht sind.

#### 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. Die Reihenfolge der Ausführung einer Konfiguration mit allen verschiedenen Hooks sieht beispielsweise folgendermaßen aus:

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 | Failover Hooks werden ausgeführt |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Klon | N | N | Neu | Gleich | Y | N | Y | N |
| 2 | Klon | N | N | Neu | Anders | Y | Y | Y | N |
| 3 | Klonen oder Wiederherstellen | Y | N | Neu | Gleich | N | N | Y | N |
| 4 | Klonen oder Wiederherstellen | N | Y | Neu | Gleich | N | N | Y | N |
| 5 | Klonen oder Wiederherstellen | Y | N | Neu | Anders | N | N | Y | N |
| 6 | Klonen oder Wiederherstellen | N | Y | Neu | Anders | N | N | Y | N |
| 7 | Wiederherstellen | Y | N | Vorhanden | Gleich | N | N | Y | N |
| 8 | Wiederherstellen | N | Y | Vorhanden | Gleich | N | N | Y | N |
| 9 | Snapshot | K. A. | K. A. | K. A. | K. A. | Y | K. A. | K. A. | N |
| 10 | Backup | N | K. A. | K. A. | K. A. | Y | Y | K. A. | N |
| 11 | Backup | Y | K. A. | K. A. | K. A. | N | N | K. A. | N |
| 12 | Failover | Y | K. A. | Durch Replikation erstellt | Anders | N | N | N | Y |

| Szenario | Betrieb | Vorhandener Snapshot | Vorhandenes Backup | Namespace | Cluster | Snapshot Hooks laufen | Backup Hooks laufen | Hooks Run wiederherstellen | Failover Hooks werden ausgeführt |
|---|---|---|---|---|---|---|---|---|---|
| 13 | Failover | Y | K. A. | Durch Replikation erstellt | Gleich | N | N | N | Y |

### Beispiele für Testausführungshaken

Besuchen Sie das "NetApp Verda GitHub Projekt" Zum Herunterladen von Real-Execution-Hooks für beliebte Apps wie Apache Cassandra und Elasticsearch. Sie können auch Beispiele sehen und Ideen für die Strukturierung Ihrer eigenen benutzerdefinierten Execution Hooks erhalten.

### Aktivieren Sie die Funktion „Ausführungshaken“

Wenn Sie Eigentümer oder Admin-Benutzer sind, können Sie die Funktion Ausführungshaken aktivieren. Wenn Sie die Funktion aktivieren, können alle in diesem Astra Control-Konto definierten Benutzer Ausführungshaken verwenden und vorhandene Ausführungshaken und Hook-Skripte anzeigen.

#### Schritte

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

   Die Registerkarte **Account** > **feature settings** wird angezeigt.
4. Wählen Sie im Bereich **Ausführungshaken** das Einstellungsmenü aus.
5. Wählen Sie **Enable**.
6. Beachten Sie die Sicherheitswarnung, die angezeigt wird.
7. Wählen Sie **Ja, Ausführungshaken aktivieren**.

### Deaktivieren Sie die Funktion Ausführungshaken

Wenn Sie ein Benutzer von Eigentümer oder Administrator sind, können Sie die Funktion „Ausführungshaken“ für alle Benutzer deaktivieren, die in diesem Astra Control-Konto definiert sind. Sie müssen alle vorhandenen Ausführungshaken löschen, bevor Sie die Funktion „Ausführungshaken“ deaktivieren können. Siehe Löschen Sie einen Testsuite-Haken Für Anweisungen zum Löschen einer vorhandenen Ausführungsöse.

#### Schritte

1. Gehen Sie zu **Account** und wählen Sie dann die Registerkarte **Feature settings**.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie im Bereich **Ausführungshaken** das Einstellungsmenü aus.
4. Wählen Sie **Deaktivieren**.
5. Beachten Sie die Warnmeldung, die angezeigt wird.
6. Typ `disable` Um zu bestätigen, dass Sie die Funktion für alle Benutzer deaktivieren möchten.

7. Wählen Sie **Ja, deaktivieren**.

### 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 eines Hakens, die Anzahl der passenden Container, die Erstellungszeit und den Ablauf (vor- oder Nachbetrieb). Sie können die auswählen + Symbol neben dem Hook-Namen, um die Liste der Container, auf denen es ausgeführt wird, zu erweitern. Um die Ereignisprotokolle zu den Testausführungshaken für diese Anwendung anzuzeigen, gehen Sie zur Registerkarte **Aktivität**.

### 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 Testsuitehaoks die einzelnen Skripte verwenden.

### Fügen Sie ein Skript hinzu

Jeder Execution Hook muss ein Skript verwenden, um Aktionen durchzuführen. Sie können einen oder mehrere Skripte hinzufügen, auf die Testausführungshaken verweisen können. Viele Ausführungshaken können auf dasselbe Skript verweisen. Dadurch können Sie viele Ausführungshaken aktualisieren, indem Sie nur ein Skript ändern.

**Schritte**

1. Stellen Sie sicher, dass die Funktion Ausführungshaken aktiviert ist Aktiviert.
2. Gehen Sie zu **Konto**.
3. Wählen Sie die Registerkarte **Skripts** aus.
4. Wählen Sie **Hinzufügen**.
5. 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.

6. 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 Ausführungshaken für eine App erstellen und ihn zu Astra Control hinzufügen. 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. Stellen Sie sicher, dass die Funktion Ausführungshaken aktiviert ist Aktiviert.
2. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
3. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
4. Wählen Sie **Hinzufügen**.
5. Im Bereich **Klettdetails**:
   a. Bestimmen Sie, wann der Haken ausgeführt werden soll, indem Sie im Dropdown-Menü * Operation* einen Operationstyp auswählen.
   b. Geben Sie einen eindeutigen Namen für den Haken ein.

c. (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.

6. (Optional) im Bereich **Hook Filter Details** können Sie Filter hinzufügen, um zu steuern, auf welchen Behältern der Execution Hook läuft:
   a. Wählen Sie **Filter hinzufügen**.
   b. Wählen Sie in der Spalte **Hook Filtertyp** ein Attribut aus, nach dem Sie im Dropdown-Menü filtern möchten.
   c. Geben Sie in der Spalte **Regex** einen regulären Ausdruck ein, der als Filter verwendet werden soll. Astra Control verwendet den "Regex-Syntax für regulären Ausdruck 2 (RE2)".

      Wenn Sie nach dem genauen Namen eines Attributs (z. B. einem Pod-Namen) filtern, ohne dass im Feld Regulärer Ausdruck ein anderer Text enthalten ist, wird eine Substring-Übereinstimmung durchgeführt. Verwenden Sie zum Abgleich eines genauen Namens und nur des Namens die exakte Syntax für die Übereinstimmung der Zeichenfolge (z. B. `^exact_podname$`).

   d. Um weitere Filter hinzuzufügen, wählen Sie **Filter hinzufügen**.

      Mehrere Filter für einen Execution Hook werden mit einem logischen UND einem Operator kombiniert. Pro Testsuite können Sie bis zu 10 aktive Filter haben.

7. Wählen Sie anschließend **Weiter** aus.
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 **Weiter**.
10. Überprüfen Sie die Konfiguration der Testsuite.
11. Wählen Sie **Hinzufügen**.

### Überprüfen Sie den Status eines Testablaufanhängees

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 Testsuitelhaken 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.

### Bearbeiten Sie einen Testsuite-Haken

Sie können einen Testsuite-Haken bearbeiten, wenn Sie die Attribute, Filter oder das verwendete Skript ändern möchten. Sie müssen über die Berechtigungen Eigentümer, Administrator oder Mitglied verfügen, um Testausführungshaken bearbeiten zu können.

#### 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 bearbeiten möchten.

4. Wählen Sie **Bearbeiten**.
5. Nehmen Sie alle erforderlichen Änderungen vor, und wählen Sie nach Abschluss jedes Abschnitts **Weiter** aus.
6. Wählen Sie **Speichern**.

#### 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**.
5. Geben Sie im Dialogfeld „Ergebnis“ zur Bestätigung „Löschen“ ein.
6. Wählen Sie **Ja, Testsuite löschen**.

#### Finden Sie weitere Informationen

- "NetApp Verda GitHub Projekt"

## Astra Control Center kann über Astra Control Center geschützt werden

Schützen Sie die Astra Control Center-Anwendung selbst, um die Ausfallsicherheit im Kubernetes-Cluster, auf dem Astra Control Center ausgeführt wird, besser vor schwerwiegenden Fehlern zu schützen. Sie können für ein Backup und Restore von Astra Control Center eine sekundäre Astra Control Center-Instanz verwenden oder die Astra-Replizierung verwenden, wenn der zugrunde liegende Storage ONTAP verwendet.

In diesen Szenarien wird eine zweite Instanz von Astra Control Center in einer anderen Fehlerdomäne bereitgestellt und konfiguriert und auf einem anderen zweiten Kubernetes-Cluster ausgeführt als die primäre Astra Control Center-Instanz. Die zweite Astra Control Instanz wird verwendet, um Backups und potenziell die primäre Astra Control Center Instanz wiederherzustellen. Eine wiederhergestellte oder replizierte Astra Control Center Instanz stellt weiterhin das Management von Applikationsdaten für die Applikations-Cluster-Applikationen bereit und stellt den Zugriff auf Backups und Snapshots dieser Applikationen wieder her.

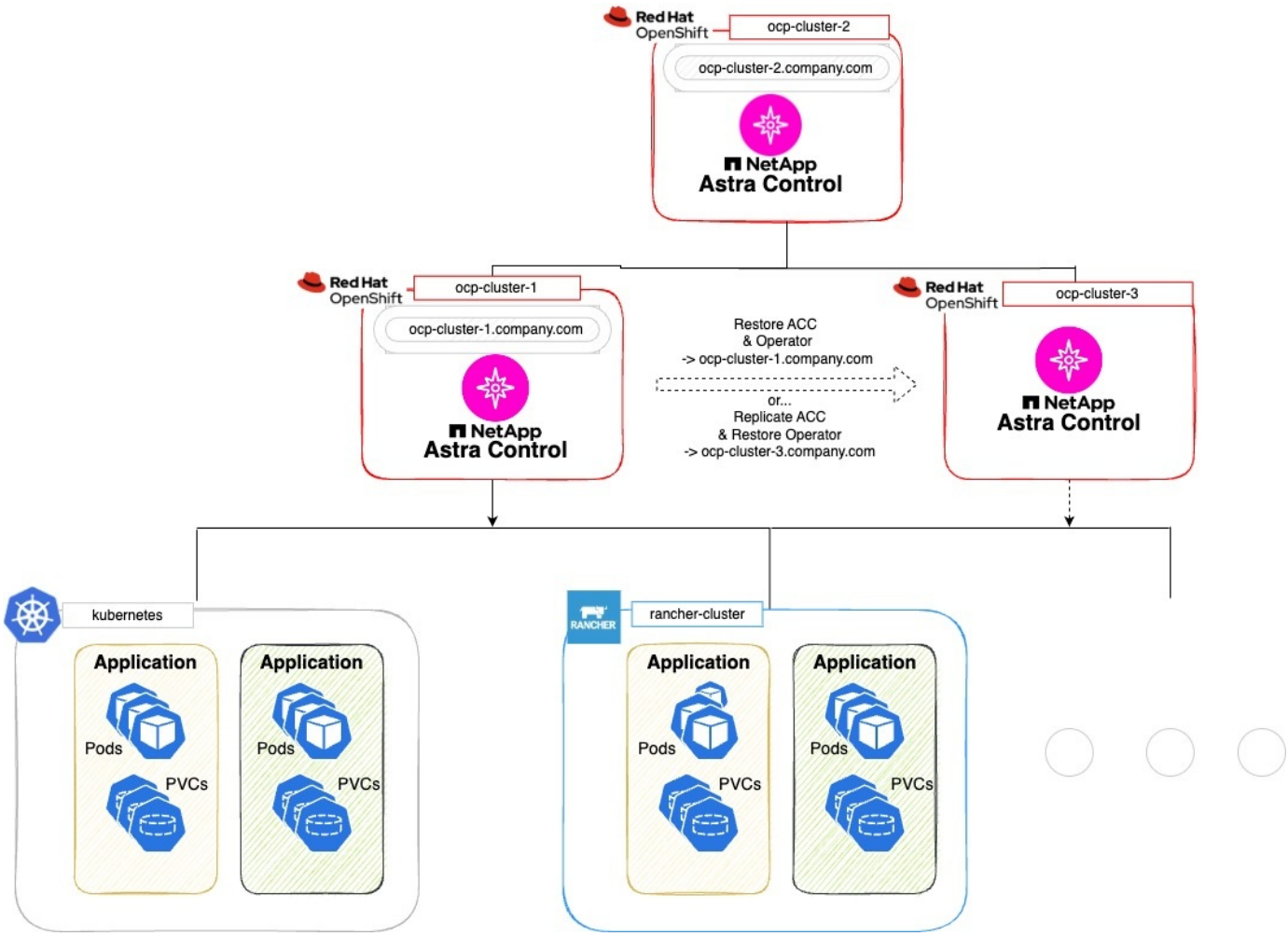
**Bevor Sie beginnen**

Stellen Sie sicher, dass Sie die folgenden Informationen haben, bevor Sie Schutzszenarien für Astra Control Center einrichten:

- **Ein Kubernetes-Cluster, auf dem die primäre Astra Control Center-Instanz ausgeführt wird**: Dieser Cluster hostet die primäre Astra Control Center-Instanz, die Anwendungscluster verwaltet.
- **Ein zweiter Kubernetes-Cluster desselben Kubernetes-Verteilungstyps wie der primäre, auf dem die sekundäre Astra Control Center-Instanz ausgeführt wird**: Dieser Cluster hostet die Astra Control Center-Instanz, die die primäre Astra Control Center-Instanz verwaltet.
- **Ein dritter Kubernetes-Cluster desselben Kubernetes-Verteilungstyps wie der primäre**: In diesem Cluster wird die wiederhergestellte oder replizierte Instanz von Astra Control Center gehostet. Er muss denselben Astra Control Center Namespace zur Verfügung haben, der derzeit auf dem primären System bereitgestellt wird. Wenn beispielsweise Astra Control Center im Namespace bereitgestellt wird `netapp-acc` Auf dem Quellcluster, dem Namespace `netapp-acc` Der Service muss verfügbar und nicht von Applikationen auf dem Kubernetes-Ziel-Cluster verwendet werden.
- **S3-kompatible Buckets**: Jede Astra Control Center Instanz verfügt über einen zugänglichen S3-kompatiblen Objektspeicher-Bucket.
- **Ein konfigurierter Load Balancer**: Der Load Balancer stellt eine IP-Adresse für Astra bereit und muss über eine Netzwerkverbindung zu den Anwendungsclustern und beiden S3 Buckets verfügen.
- **Cluster erfüllen die Anforderungen für Astra Control Center**: Jeder Cluster, der in Astra Control Center verwendet wird, erfüllt "Allgemeine Anforderungen für Astra Control Center".

**Über diese Aufgabe**

In diesen Verfahren werden die erforderlichen Schritte beschrieben, um Astra Control Center mithilfe eines der beiden Cluster auf einem neuen Cluster wiederherzustellen Backup und Restore Oder Replizierung. Die Schritte basieren auf der hier dargestellten Beispielkonfiguration:




In dieser Beispielkonfiguration wird Folgendes angezeigt:

- **Ein Kubernetes-Cluster, auf dem die primäre Astra Control Center-Instanz ausgeführt wird**:
  - OpenShift-Cluster: `ocp-cluster-1`
  - Primäre Astra Control Center-Instanz: `ocp-cluster-1.company.com`
  - Dieser Cluster verwaltet die Anwendungscluster.
- **Der zweite Kubernetes-Cluster desselben Kubernetes-Distributionstyps wie der primäre, auf dem die sekundäre Astra Control Center-Instanz ausgeführt wird**:
  - OpenShift-Cluster: `ocp-cluster-2`
  - Sekundäre Astra Control Center-Instanz: `ocp-cluster-2.company.com`
  - Dieser Cluster wird verwendet, um die primäre Astra Control Center-Instanz zu sichern oder die Replikation in einem anderen Cluster zu konfigurieren (in diesem Beispiel der `ocp-cluster-3` Cluster).
- **Ein dritter Kubernetes-Cluster mit demselben Kubernetes-Verteilungstyp wie der primäre, der für Wiederherstellungsvorgänge verwendet wird**:
  - OpenShift-Cluster: `ocp-cluster-3`
  - Astra Control Center dritte Instanz: `ocp-cluster-3.company.com`
  - Dieser Cluster wird für die Wiederherstellung oder das Replizierungs-Failover von Astra Control Center

verwendet.

> Idealerweise sollte sich der Applikations-Cluster außerhalb der drei Astra Control Center Cluster befinden, wie in der Abbildung oben in kubernetes und Rancher Clustern dargestellt.

Nicht im Diagramm dargestellt:

- Auf allen Clustern sind ONTAP-Back-Ends mit installiertem Trident installiert.
- In dieser Konfiguration verwenden die OpenShift-Cluster MetalLB als Load Balancer.
- Der Snapshot-Controller und die VolumeSnapshotClass sind auch auf allen Clustern installiert, wie in beschrieben "Voraussetzungen".

### Schritt 1 Option: Backup und Wiederherstellung von Astra Control Center

In diesem Verfahren werden die erforderlichen Schritte beschrieben, um Astra Control Center mithilfe von Backup und Restore auf einem neuen Cluster wiederherzustellen.

In diesem Beispiel wird Astra Control Center immer unter installiert `netapp-acc` Namespace und der Operator wird unter installiert `netapp-acc-operator` Namespace.

> Obwohl nicht beschrieben, kann der Astra Control Center-Operator auch im selben Namespace wie der Astra CR eingesetzt werden.

#### Bevor Sie beginnen

- Sie haben das primäre Astra Control Center auf einem Cluster installiert.
- Sie haben das sekundäre Astra Control Center auf einem anderen Cluster installiert.

#### Schritte

1. Management der primären Astra Control Center-Applikation und des Ziel-Clusters über die sekundäre Astra Control Center-Instanz (auf der ausgeführt wird `ocp-cluster-2` Cluster):
   a. Melden Sie sich bei der sekundären Astra Control Center-Instanz an.
   b. "Fügen Sie das primäre Astra Control Center-Cluster hinzu" (`ocp-cluster-1`).
   c. "Fügen Sie das dritte Zielcluster hinzu" (`ocp-cluster-3`), die für die Wiederherstellung verwendet werden.
2. Astra Control Center und den Astra Control Center Betreiber im sekundären Astra Control Center managen:
   a. Wählen Sie auf der Seite Anwendungen die Option **Definieren**.
   b. Geben Sie im Fenster **Anwendung definieren** den neuen Anwendungsnamen ein (`netapp-acc`).
   c. Wählen Sie den Cluster aus, auf dem das primäre Astra Control Center ausgeführt wird (`ocp-cluster-1`) Aus der Dropdown-Liste **Cluster**.
   d. Wählen Sie die aus `netapp-acc` Namespace für Astra Control Center aus der Dropdown-Liste **Namespace**.
   e. Aktivieren Sie auf der Seite „Cluster-Ressourcen“ die Option **zusätzliche Cluster-Ressourcen einschließen**.
   f. Wählen Sie **Add include Rule**.

g. Wählen Sie diese Einträge aus, und wählen Sie **Hinzufügen**:
   - Etikettenauswahl: <label name>
   - Gruppe: Apiextensions.k8s.io
   - Stand: v1
   - Art: CustomResourceDefinition

h. Bestätigen Sie die Anwendungsinformationen.

i. Wählen Sie **Definieren**.

   Nachdem Sie **define** ausgewählt haben, wiederholen Sie den Prozess Anwendung definieren für den Operator `netapp-acc-operator`) Und wählen Sie die aus `netapp-acc-operator` Namespace im Assistenten „Anwendung definieren“.

3. Astra Control Center und den Bediener sichern:
   a. Navigieren Sie im sekundären Astra Control Center zur Seite Anwendungen, indem Sie die Registerkarte Anwendungen auswählen.
   b. "Backup" Astra Control Center (`netapp-acc`).
   c. "Backup" Der Bediener (`netapp-acc-operator`).
4. Nachdem Sie Astra Control Center und den Operator gesichert haben, simulieren Sie durch ein Disaster Recovery-Szenario (DR) "Astra Control Center wird deinstalliert" Vom primären Cluster aus.

   Sie stellen Astra Control Center in einem neuen Cluster (dem dritten in diesem Verfahren beschriebenen Kubernetes-Cluster) wieder her und verwenden denselben DNS wie das primäre Cluster für das neu installierte Astra Control Center.

5. Mit dem sekundären Astra Control Center "Wiederherstellen" Die primäre Instanz der Astra Control Center-Anwendung aus ihrem Backup:
   a. Wählen Sie **Applications** aus und wählen Sie dann den Namen der Astra Control Center-Anwendung aus.
   b. Wählen Sie im Menü Optionen in der Spalte Aktionen die Option **Wiederherstellen** aus.
   c. Wählen Sie als Wiederherstellungstyp die Option **in neue Namespaces wiederherstellen**.
   d. Geben Sie den Wiederherstellungsnamen ein (`netapp-acc`).
   e. Wählen Sie das dritte Zielcluster aus (`ocp-cluster-3`).
   f. Aktualisieren Sie den Ziel-Namespace so, dass es sich um den gleichen Namespace wie das Original handelt.
   g. Wählen Sie auf der Seite Quelle wiederherstellen das Anwendungsbackup aus, das als Wiederherstellungsquelle verwendet werden soll.
   h. Wählen Sie **Restore using original Storage classes**.
   i. Wählen Sie **Alle Ressourcen wiederherstellen**.
   j. Überprüfen Sie die Restore-Informationen und wählen Sie dann **Restore** aus, um den Wiederherstellungsprozess zu starten, der Astra Control Center auf dem Ziel-Cluster wiederherstellt (`ocp-cluster-3`). Die Wiederherstellung ist abgeschlossen, wenn die Anwendung eingibt `available` Bundesland.
6. Astra Control Center auf dem Ziel-Cluster konfigurieren:

a. Öffnen Sie ein Terminal, und stellen Sie mithilfe von kubeconfig eine Verbindung zum Ziel-Cluster her (`ocp-cluster-3`), das das wiederhergestellte Astra Control Center enthält.

b. Bestätigen Sie das `ADDRESS` Spalte in der Astra Control Center-Konfiguration verweist auf den DNS-Namen des primären Systems:

```
kubectl get acc -n netapp-acc
```

Antwort:

```
NAME  UUID                                   VERSION    ADDRESS
READY
astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.10.0-68 ocp-cluster-
1.company.com           True
```

a. Wenn der `ADDRESS` Feld in der obigen Antwort weist nicht den FQDN der primären Astra Control Center-Instanz auf. Aktualisieren Sie die Konfiguration, um auf den Astra Control Center-DNS zu verweisen:

```
kubectl edit acc -n netapp-acc
```

i. Ändern Sie das `astraAddress` Unter `spec:` Zum FQDN (`ocp-cluster-1.company.com` In diesem Beispiel) der primären Astra Control Center-Instanz.

ii. Speichern Sie die Konfiguration.

iii. Bestätigen Sie, dass die Adresse aktualisiert wurde:

```
kubectl get acc -n netapp-acc
```

b. Wechseln Sie zum Stellen Sie den Astra Control Center Operator wieder her Abschnitt dieses Dokuments, um den Wiederherstellungsprozess abzuschließen.

### Schritt 1: Astra Control Center mit Replizierung schützen

Dieses Verfahren beschreibt die erforderlichen Schritte zur Konfiguration "Astra Control Center-Replizierung" Zum Schutz der primären Astra Control Center-Instanz.

In diesem Beispiel wird Astra Control Center immer unter installiert `netapp-acc` Namespace und der Operator wird unter installiert `netapp-acc-operator` Namespace.

#### Bevor Sie beginnen

- Sie haben das primäre Astra Control Center auf einem Cluster installiert.
- Sie haben das sekundäre Astra Control Center auf einem anderen Cluster installiert.

#### Schritte

1. Management der primären Astra Control Center-Applikation und des Ziel-Clusters über die sekundäre

Astra Control Center-Instanz:

a. Melden Sie sich bei der sekundären Astra Control Center-Instanz an.

b. "Fügen Sie das primäre Astra Control Center-Cluster hinzu" (`ocp-cluster-1`).

c. "Fügen Sie das dritte Zielcluster hinzu" (`ocp-cluster-3`), das für die Replikation verwendet wird.

2. Astra Control Center und den Astra Control Center Betreiber im sekundären Astra Control Center managen:

a. Wählen Sie **Cluster** aus und wählen Sie den Cluster aus, der das primäre Astra Control Center enthält (`ocp-cluster-1`).

b. Wählen Sie die Registerkarte **Namesaces** aus.

c. Wählen Sie `netapp-acc` Und `netapp-acc-operator` Namespaces.

d. Wählen Sie im Menü Aktionen die Option **als Anwendungen definieren**.

e. Wählen Sie **in Anwendungen anzeigen**, um die definierten Anwendungen anzuzeigen.

3. Back-Ends für Replikation konfigurieren:

> Für die Replizierung sind das primäre Astra Control Center-Cluster und das Ziel-Cluster erforderlich (`ocp-cluster-3`) Verwenden Sie verschiedene peered ONTAP-Speicher-Backends.
> Nachdem jedes Backend zu Astra Control hinzugefügt wurde, erscheint das Backend auf der Seite Backends auf der Registerkarte **Discovered**.

a. "Fügen Sie ein Peering-Backend hinzu" Zum Astra Control Center auf dem primären Cluster.

b. "Fügen Sie ein Peering-Backend hinzu" Zum Astra Control Center auf dem Ziel-Cluster.

4. Replikation konfigurieren:

a. Wählen Sie im Bildschirm Anwendungen die aus `netapp-acc` Applikation.

b. Wählen Sie **Configure Replication Policy** aus.

c. Wählen Sie `ocp-cluster-3` Als Ziel-Cluster.

d. Wählen Sie die Storage-Klasse aus.

e. Eingabe `netapp-acc` Als Ziel-Namespace.

f. Ändern Sie bei Bedarf die Replizierungshäufigkeit.

g. Wählen Sie **Weiter**.

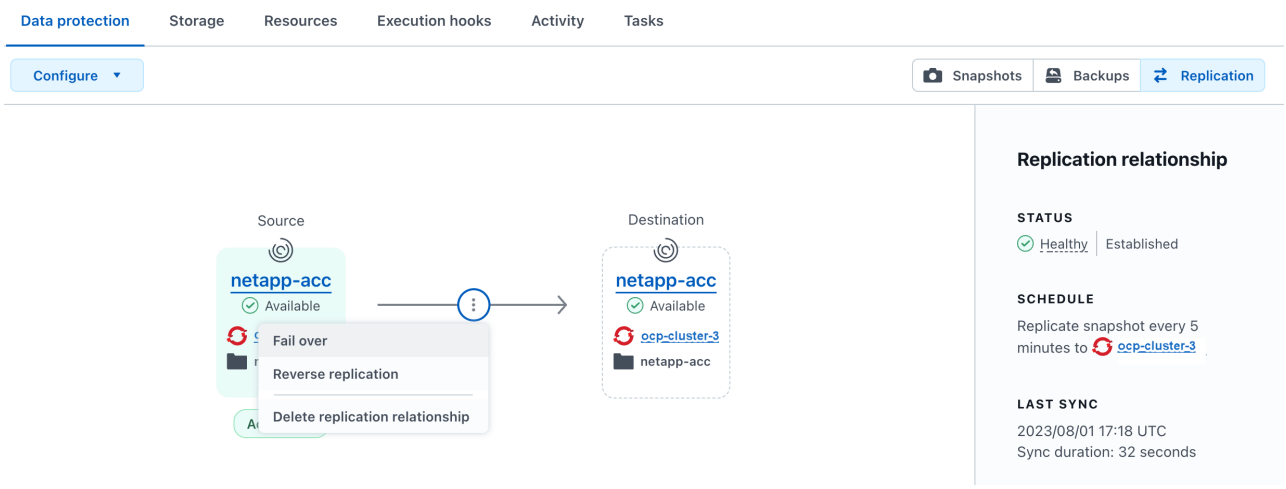
h. Bestätigen Sie, dass die Konfiguration korrekt ist, und wählen Sie **Speichern**.

Die Replikationsbeziehung wechselt von `Establishing` Bis `Established`. Wenn diese Replikation aktiv ist, erfolgt sie alle fünf Minuten, bis die Replikationskonfiguration gelöscht wird.

5. Failover der Replikation auf den anderen Cluster, wenn das primäre System beschädigt ist oder nicht mehr darauf zugegriffen werden kann:

> Stellen Sie sicher, dass auf dem Ziel-Cluster Astra Control Center nicht installiert ist, um einen erfolgreichen Failover zu gewährleisten.

a. Wählen Sie das Symbol für vertikale Ellipsen und dann **Failover**.




b. Bestätigen Sie die Details, und wählen Sie **Failover**, um den Failover-Prozess zu starten.

   Der Status der Replikationsbeziehung ändert sich in `Failing over` Und dann `Failed over` Nach Abschluss.

6. Schließen Sie die Failover-Konfiguration ab:

   a. Öffnen Sie ein Terminal, und verbinden Sie es mit dem kubeconfig des dritten Clusters (`ocp-cluster-3`). Auf diesem Cluster ist jetzt Astra Control Center installiert.

   b. Bestimmen Sie den FQDN des Astra Control Center auf dem dritten Cluster (`ocp-cluster-3`).

   c. Aktualisieren Sie die Konfiguration, um auf den Astra Control Center-DNS zu verweisen:

```
kubectl edit acc -n netapp-acc
```

      i. Ändern Sie das `astraAddress` Unter `spec:` Mit dem FQDN (`ocp-cluster-3.company.com`) Des dritten Zielclusters.

      ii. Speichern Sie die Konfiguration.

      iii. Bestätigen Sie, dass die Adresse aktualisiert wurde:

```
kubectl get acc -n netapp-acc
```

   d. Bestätigen Sie, dass alle erforderlichen traefik-CRDs vorhanden sind:

```
kubectl get crds | grep traefik
```

   Erforderliche Traefik CRDS:

```
ingressroutes.traefik.containo.us
ingressroutes.traefik.io
ingressroutetcps.traefik.containo.us
ingressroutetcps.traefik.io
ingressrouteudps.traefik.containo.us
ingressrouteudps.traefik.io
middlewares.traefik.containo.us
middlewares.traefik.io
middlewaretcps.traefik.containo.us
middlewaretcps.traefik.io
serverstransports.traefik.containo.us
serverstransports.traefik.io
tlsoptions.traefik.containo.us
tlsoptions.traefik.io
tIsstores.traefik.containo.us
tIsstores.traefik.io
traefikservices.traefik.containo.us
traefikservices.traefik.io
```

a. Wenn einige der oben genannten CRDs fehlen:
   i. Gehen Sie zu "Traefik-Dokumentation".
   ii. Kopieren Sie den Bereich „Definitionen“ in eine Datei.
   iii. Änderungen übernehmen:

```
kubectl apply -f <file name>
```

   iv. Traefik neu starten:

```
kubectl get pods -n netapp-acc | grep -e "traefik" | awk '{print
$1}' | xargs kubectl delete pod -n netapp-acc
```

b. Wechseln Sie zum Stellen Sie den Astra Control Center Operator wieder her Abschnitt dieses Dokuments, um den Wiederherstellungsprozess abzuschließen.

**Schritt 2: Wiederherstellen des Bedieners des Astra Control Centers**

Stellen Sie mithilfe des sekundären Astra Control Center den primären Astra Control Center-Operator aus dem Backup wieder her. Der Ziel-Namespace muss mit dem Quell-Namespace übereinstimmen. Wenn Astra Control Center aus dem primären Quell-Cluster gelöscht wurde, sind Backups weiterhin vorhanden, um dieselben Wiederherstellungsschritte auszuführen.

**Schritte**

1. Wählen Sie **Anwendungen** und dann den Namen der Operator-App aus (`netapp-acc-operator`).

2. Wählen Sie im Menü Optionen in der Spalte Aktionen die Option **Wiederherstellen** aus
3. Wählen Sie als Wiederherstellungstyp die Option **in neue Namespaces wiederherstellen**.
4. Wählen Sie das dritte Zielcluster aus (`ocp-cluster-3`).
5. Ändern Sie den Namespace so, dass er mit dem Namespace identisch ist, der mit dem primären Quellcluster verknüpft ist (`netapp-acc-operator`).
6. Wählen Sie das Backup aus, das zuvor als Wiederherstellungsquelle erstellt wurde.
7. Wählen Sie **Restore using original Storage classes**.
8. Wählen Sie **Alle Ressourcen wiederherstellen**.
9. Überprüfen Sie die Details und klicken Sie dann auf * Wiederherstellen*, um den Wiederherstellungsprozess zu starten.

   Auf der Seite Anwendungen wird der Astra Control Center-Operator angezeigt, der auf dem dritten Zielcluster wiederhergestellt wird (`ocp-cluster-3`). Wenn der Prozess abgeschlossen ist, wird der Status als angezeigt `Available`. Innerhalb von zehn Minuten sollte die DNS-Adresse auf der Seite aufgelöst werden.

**Ergebnis**

Astra Control Center, die registrierten Cluster sowie gemanagte Applikationen mit ihren Snapshots und Backups sind jetzt auf dem Ziel-Third-Cluster verfügbar (`ocp-cluster-3`). Alle Sicherungsrichtlinien, die Sie auf dem Original hatten, sind auch auf der neuen Instanz vorhanden. Sie können weiterhin geplante oder On-Demand-Backups und Snapshots erstellen.

**Fehlerbehebung**

Bestimmen Sie den Systemzustand und ob die Schutzprozesse erfolgreich waren.

- **Pods laufen nicht**: Vergewissern Sie sich, dass alle Pods ausgeführt werden:

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

  Wenn sich einige Pods im befinden `CrashLookBackOff` Geben Sie den Status ein, und starten Sie sie neu. Sie sollten dann zu wechseln `Running` Bundesland.

- **Systemstatus bestätigen**: Bestätigen Sie, dass sich das Astra Control Center-System in befindet `ready` Bundesland:

  ```
  kubectl get acc -n netapp-acc
  ```

  Antwort:

  ```
  NAME  UUID                                   VERSION    ADDRESS
  READY
  astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.10.0-68 ocp-cluster-
  1.company.com           True
  ```

- **Bereitstellungsstatus bestätigen**: Zeigt Informationen zur Astra Control Center-Bereitstellung an, um dies zu bestätigen `Deployment State` Ist `Deployed`.

```
kubectl describe acc astra -n netapp-acc
```

- **Wiederhergestellte Astra Control Center UI gibt einen 404 Fehler** zurück: Wenn dies geschieht, wenn Sie ausgewählt haben `AccTraefik` Aktivieren Sie als Eindringen die Option Traefik-CRDs Um sicherzustellen, dass alle installiert sind.

# 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 Kubeconsg, 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

Astra Control bietet nach dem Management einer App Details zu der App, mit der Sie den Kommunikationsstatus (ob Astra Control mit der App kommunizieren kann), den Sicherungsstatus (unabhängig davon, ob die App bei Ausfällen vollständig geschützt ist), die Pods, persistenten Storage usw. 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.

   **Anwendungsstatus**
   Zeigt einen Status an, der angibt, ob Astra Control mit der Applikation kommunizieren kann.

   - **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 "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 "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 das bei aktivierter Remote-Authentifizierung konfigurierte Attribut für die Benutzeranmeldung, um Remote-Benutzer zu suchen und zu verfolgen. Für jeden Remote-Benutzer, den Sie im Astra Control Center anzeigen möchten, muss in diesem Feld ein Attribut einer E-Mail-Adresse („Mail“) oder eines Hauptnamens des Benutzers („userPrincipalName“) vorhanden sein. Dieses Attribut wird als Benutzername in Astra Control Center für die Authentifizierung und bei der Suche nach Remote-Benutzern 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.

**Bevor Sie beginnen**

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. Gehen Sie im Abschnitt **User Match** wie folgt vor:
   a. Geben Sie den Basis-DN und einen entsprechenden Benutzersuchfilter ein, der beim Abrufen von Benutzerinformationen vom LDAP-Server verwendet werden soll.
   b. (Optional) Wenn Ihr Verzeichnis das Benutzeranmeldungsattribut verwendet `userPrincipalName` Statt `mail`, Geben Sie ein `userPrincipalName` Geben Sie im Feld **Benutzer-Login-Attribut** das richtige Attribut ein.
7. Geben Sie im Abschnitt **Gruppenvergleich** den Gruppen-Suchsockel-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 ein LDAP-Benutzer sind und die Verbindung trennen, wird Ihre Sitzung sofort beendet 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. Astra Control Center unterstützt bis zu 10,000 LDAP Remote-Benutzer.

> Astra Control Center verwendet das bei aktivierter Remote-Authentifizierung konfigurierte Attribut für die Benutzeranmeldung, um Remote-Benutzer zu suchen und zu verfolgen. Für jeden Remote-Benutzer, den Sie im Astra Control Center anzeigen möchten, muss in diesem Feld ein Attribut einer E-Mail-Adresse („Mail“) oder eines Hauptnamens des Benutzers („userPrincipalName“) vorhanden sein. Dieses Attribut wird als Benutzername in Astra Control Center für die Authentifizierung und bei der Suche nach Remote-Benutzern verwendet.

> Sie können keinen Remote-Benutzer hinzufügen, wenn bereits ein lokaler Benutzer mit derselben E-Mail-Adresse (basierend auf dem Attribut „Mail“ oder „user principal Name“) auf dem System vorhanden ist. Um den Benutzer als Remote-Benutzer hinzuzufügen, löschen Sie zuerst den lokalen Benutzer aus dem System.

**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, können sich alle Remote-Benutzer in dieser Gruppe bei Astra Control anmelden und übernehmen die gleiche Rolle wie die Gruppe.

Astra Control Center unterstützt bis zu 5,000 LDAP-Remote-Gruppen.

**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. Remote-Benutzer in dieser Gruppe werden erst dann in der Liste der Remote-Benutzer angezeigt, wenn sich jeder Remote-Benutzer anmeldet. 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 eigene kubeconfig-Datei erstellen, sollten Sie nur **ein** Kontextelement in ihr definieren. Siehe "Kubernetes-Dokumentation" Für Informationen über das Erstellen von 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 "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: Der Bucket ist derzeit nicht zugänglich.

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.
- Sie können einen WORM-Bucket (Write Once Read Many) nicht entfernen, bevor die Aufbewahrungsfrist des Cloud-Providers abgelaufen ist. WORM-Buckets werden neben dem Bucket-Namen mit „gesperrt“ gekennzeichnet.

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

**Bevor Sie beginnen**

- 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
- Bearbeiten Sie die Details der Storage-Back-End-Authentifizierung
- Management eines erkannten Storage-Backends
- 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

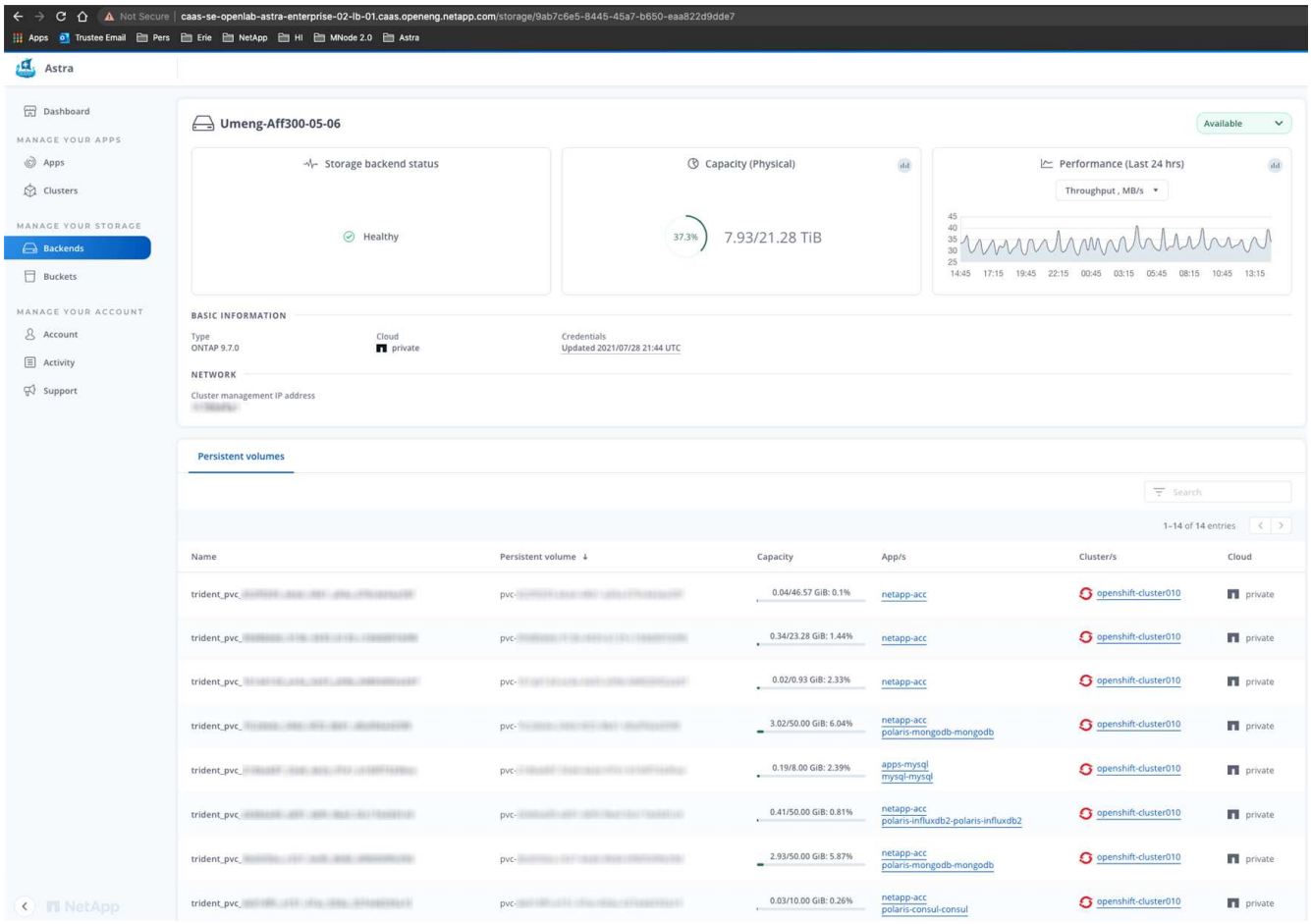
Informationen zum Zustand, Kapazität und Performance des Backend (IOPS-Durchsatz und/oder Latenz)

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.

## Bearbeiten Sie die Details der Storage-Back-End-Authentifizierung

Astra Control Center bietet zwei Arten der Authentifizierung eines ONTAP-Backends.

- **Credential-basierte Authentifizierung**: Der Benutzername und das Passwort an einen ONTAP-Benutzer mit den erforderlichen Berechtigungen. Sie sollten eine vordefinierte Sicherheits-Login-Rolle wie admin verwenden, um maximale Kompatibilität mit ONTAP-Versionen zu gewährleisten.
- **Zertifikatbasierte Authentifizierung**: Astra Control Center kann auch mit einem ONTAP-Cluster kommunizieren, indem ein auf dem Backend installiertes Zertifikat verwendet wird. Verwenden Sie gegebenenfalls das Clientzertifikat, den Schlüssel und das Zertifikat der vertrauenswürdigen Zertifizierungsstelle (empfohlen).

Sie können vorhandene Back-Ends aktualisieren, um von einem Authentifizierungstyp zu einer anderen zu wechseln. Es wird jeweils nur eine Authentifizierungsmethode unterstützt.

Weitere Informationen zum Aktivieren der zertifikatbasierten Authentifizierung finden Sie unter "Aktivieren Sie die Authentifizierung auf dem ONTAP Storage Back-End".

**Schritte**

1. Wählen Sie in der linken Navigationsleiste **Backend** aus.
2. Wählen Sie das Storage-Back-End aus.

3. Wählen Sie im Feld Anmeldeinformationen das Symbol **Bearbeiten** aus.
4. Wählen Sie auf der Seite Bearbeiten eine der folgenden Optionen aus.
   - **Administrator-Anmeldeinformationen verwenden**: Geben Sie die ONTAP Cluster Management IP-Adresse und die Admin-Anmeldeinformationen ein. Die Anmeldedaten müssen Cluster-weite Anmeldedaten aufweisen.

     Der Benutzer, dessen Anmeldeinformationen Sie hier eingeben, muss über den verfügen `ontapi` Aktivieren der Zugriffsmethode für die Anmeldung beim Benutzer in ONTAP System Manager auf dem ONTAP Cluster. Wenn Sie Vorhaben, SnapMirror Replizierung zu verwenden, wenden Sie Benutzeranmeldeinformationen auf die Rolle „Admin“ an, die über die Zugriffsmethoden verfügt `ontapi` Und `http`, Auf Quell- und Ziel-ONTAP Clustern. Siehe "Managen von Benutzerkonten in der ONTAP Dokumentation" Finden Sie weitere Informationen.

   - **Ein Zertifikat** verwenden: Das Zertifikat hochladen `.pem` Datei, dem Zertifikatschlüssel `.key` Datei und optional die Zertifizierungsdatei.
5. Wählen Sie **Speichern**.

## Management eines erkannten Storage-Backends

Sie können auswählen, wie ein nicht verwaltetes, aber dennoch ermitteltes Storage-Back-End verwaltet werden soll. Wenn Sie ein Storage-Backend verwalten, gibt Astra Control an, ob ein Authentifizierungszertifikat abgelaufen ist.

**Schritte**

1. Wählen Sie in der linken Navigationsleiste **Backend** aus.
2. Wählen Sie die Option **entdeckt**.
3. Wählen Sie das Storage-Back-End aus.
4. Wählen Sie im Menü Optionen in der Spalte **Aktionen Verwalten** aus.
5. Nehmen Sie die Änderungen vor.
6. Wählen Sie **Speichern**.

## 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 verwendenden Storage-Back-End entfernen. Nutzen Sie dies, um Ihre Konfiguration auf dem neuesten Stand zu halten.

**Bevor Sie beginnen**

- 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 in der Option **actions Unmanage** 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 in der Option **actions** die Option **Remove** aus.
   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 **Bearbeiten** aus der Dropdown-Liste, 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.

Wenn Astra Control Center mit Cloud Insights gekoppelt ist, sollten Sie die Option **Bereitstellung ändern** in Cloud Insights nicht verwenden.

Nachdem Sie die Cloud Insights-Verbindung aktiviert haben, können Sie die Durchsatzinformationen auf der Seite **Backends** anzeigen sowie nach Auswahl eines Storage-Backends eine Verbindung zu Cloud Insights herstellen. Sie können auch die Informationen im **Dashboard** im Bereich Cluster finden und sich von dort mit Cloud Insights verbinden.

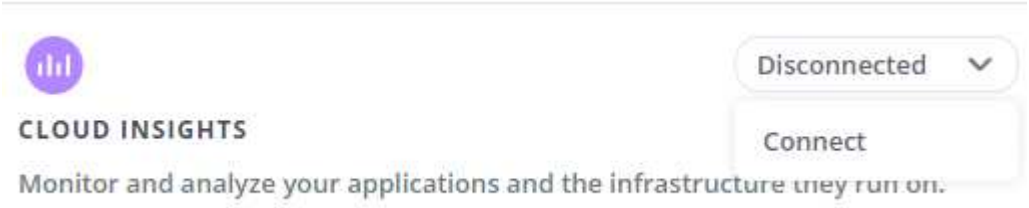
**Bevor Sie beginnen**

- 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.



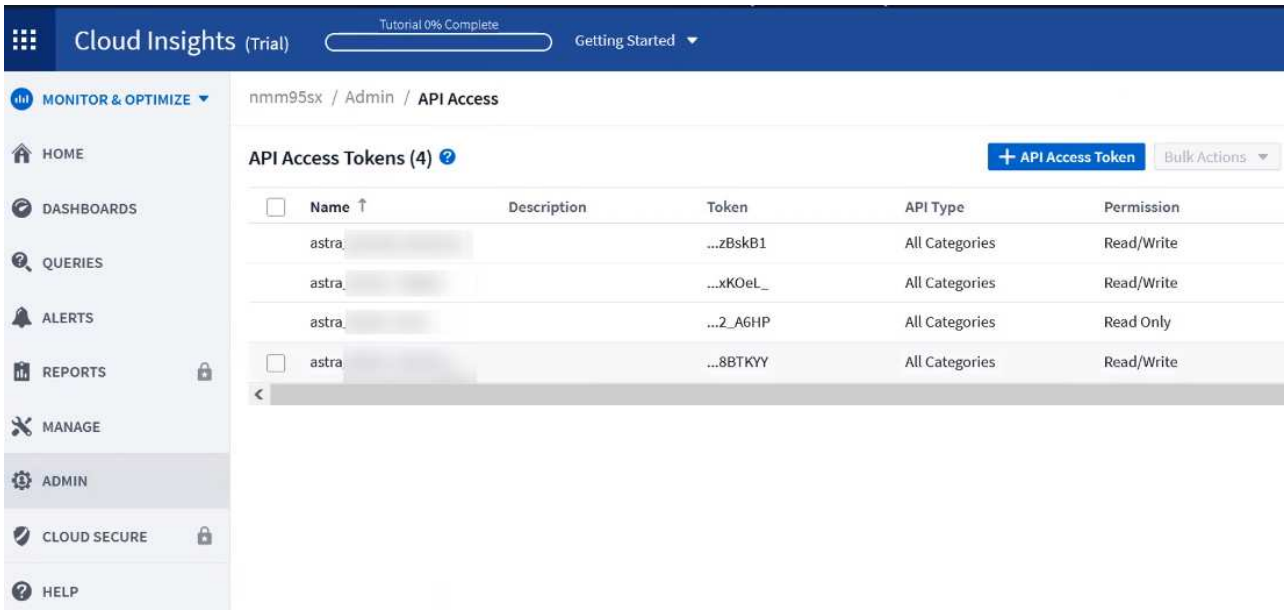

4. Geben Sie die Cloud Insights-API-Token und die Mandanten-URL ein. Die Mandanten-URL weist beispielsweise das folgende Format auf:

```
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".

a. Um die zu bekommen "API-Token", Loggen Sie sich bei Ihrer Cloud Insights-Mandanten-URL ein.

b. Generieren Sie in Cloud Insights durch Klicken auf **Admin** > **API-Zugriff** sowohl ein **Lesen/Schreiben** als auch ein **schreibgeschütztes** API-Zugriffstoken.




c. 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.

d. 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.

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

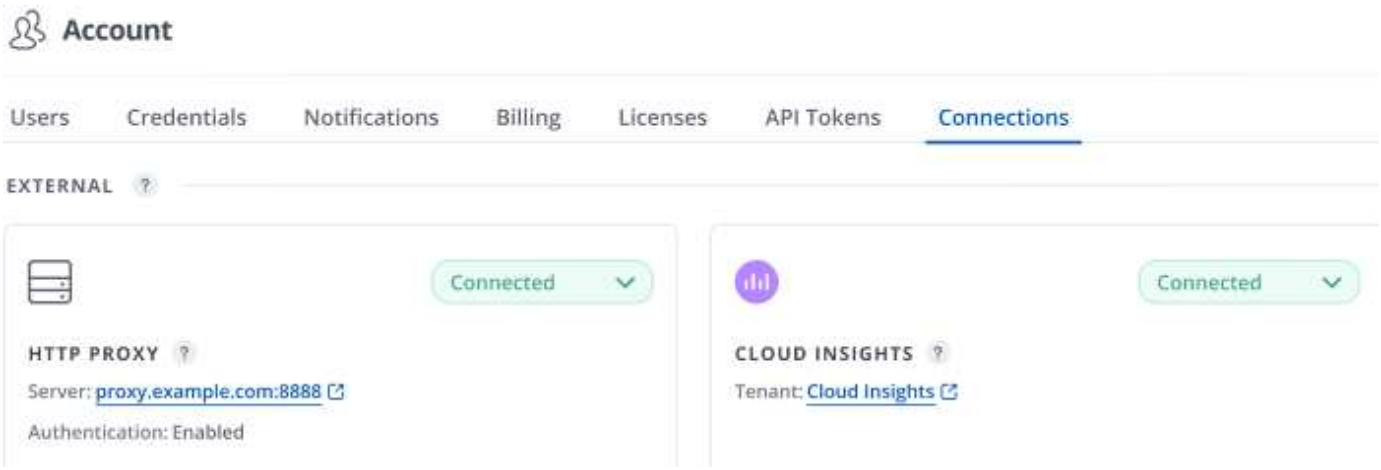
5. Wählen Sie **Verbinden**.

> 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.

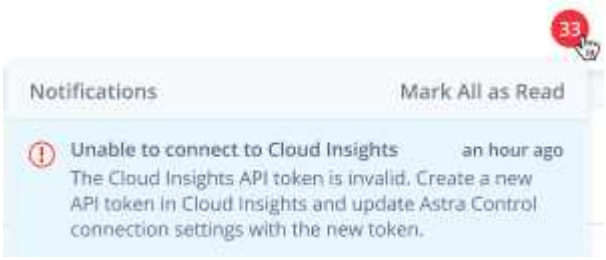
> Um zwischen dem Astra Control Center und den Cloud Insights UIs hin und her zu gehen, stellen Sie sicher, dass Sie bei beiden angemeldet sind.

### 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.

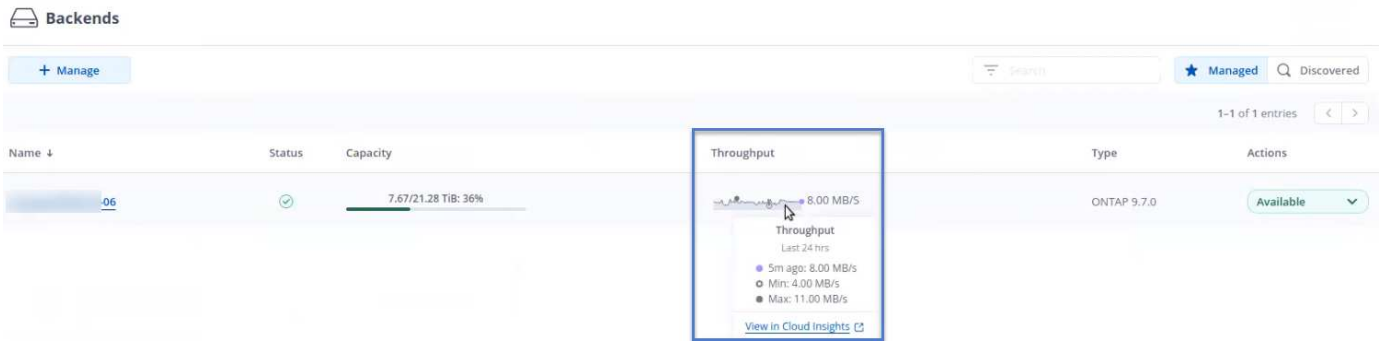



Wenn die Verbindung aus irgendeinem Grund fehlgeschlagen ist, wird im Status **failed** angezeigt. Den Grund für Fehlschlag finden Sie unter **Benachrichtigungen** auf der rechten oberen Seite des UI.



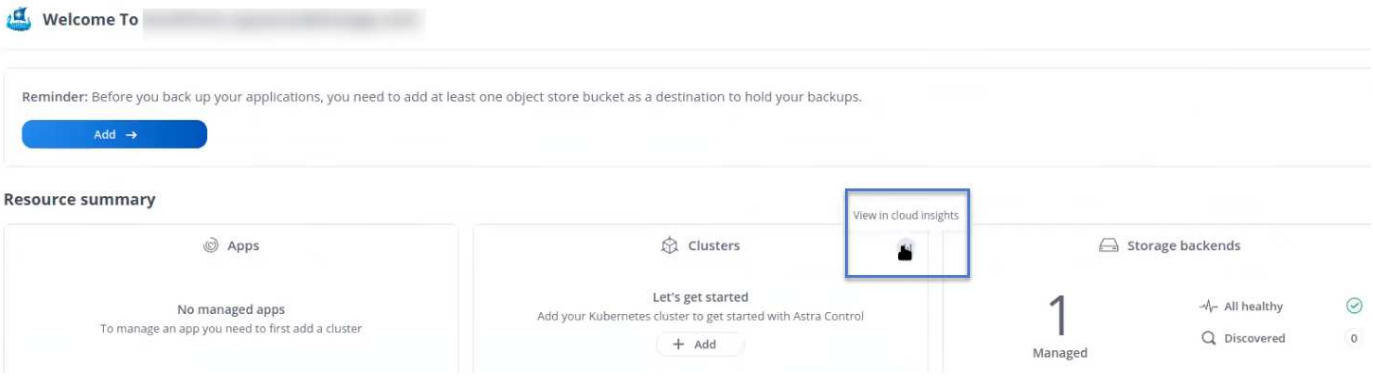

Die gleichen Informationen finden Sie auch unter **Konto** > **Benachrichtigungen**.

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 **Bearbeiten** aus der Dropdown-Liste, 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 hinzu `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.

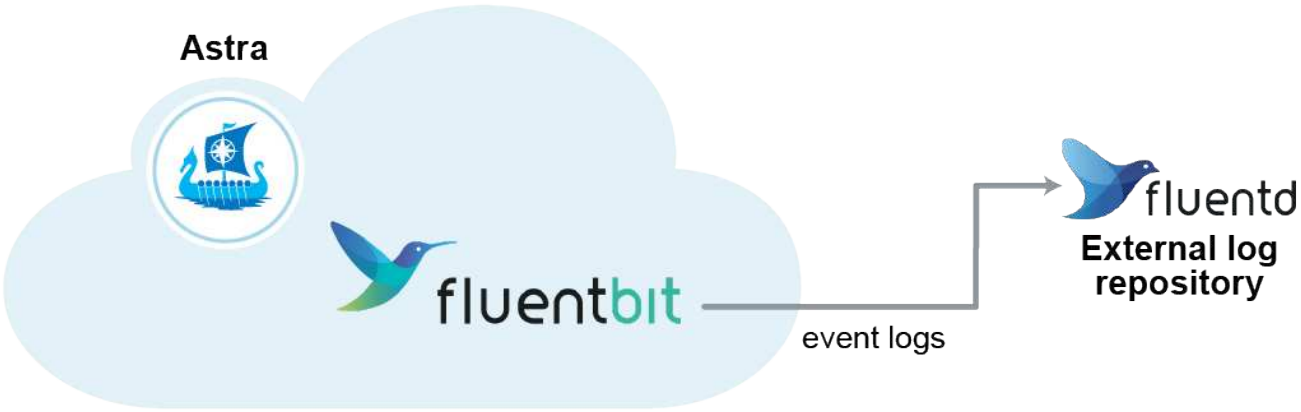
**Schritte**

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 System, das von Astra Control Center überwacht wird, an Ihren Fluentd-Endpunkt senden. Die Fluentd-Verbindung ist standardmäßig deaktiviert.




Nur die Ereignisprotokolle von verwalteten Clustern werden an Fluentd weitergeleitet.

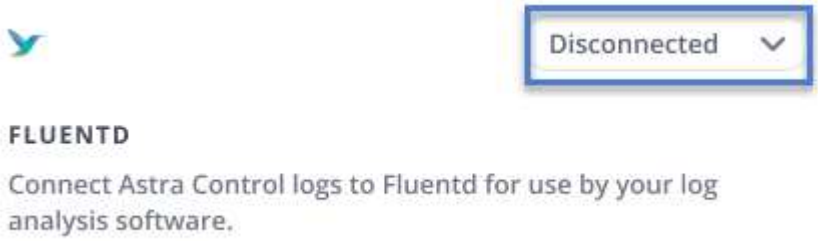
**Bevor Sie beginnen**

- 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 **Bearbeiten** aus der Dropdown-Liste, 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.
- Astra Trident wird nicht vom Cluster deinstalliert. "Erfahren Sie, wie Sie Astra Trident deinstallieren".

**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.

Diese Anweisungen beschreiben den Upgrade-Prozess für Astra Control Center von der zweitneuesten Version auf diese aktuelle Version. Sie können kein direktes Upgrade von einer Version durchführen, die zwei oder mehr Versionen hinter der aktuellen Version enthält. Wenn Ihre installierte Astra Control Center-Version viele Versionen hinter der aktuellen Version zurückliegt, müssen Sie möglicherweise Kettenaktualisierungen auf neuere Versionen durchführen, bis Ihr installiertes Astra Control Center nur eine Version hinter der neuesten Version zurückliegt. Eine vollständige Liste der freigegebenen Versionen finden Sie im "Versionshinweise".

**Bevor Sie beginnen**

Stellen Sie vor dem Upgrade sicher, dass Ihre Umgebung weiterhin die Anforderungen erfüllt "Mindestanforderungen für die Implementierung des Astra Control Center". Ihre Umgebung sollte Folgendes haben:

- **A "Unterstützt" Die Version Astra Trident**

  **Für Schritte erweitern**

  Bestimmen Sie die ausgeführte Trident-Version:

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

  > Führen Sie bei Bedarf ein Upgrade von Astra Trident durch. Verwenden Sie diese "Anweisungen".

Version 23.10 ist die letzte Version von Astra Control Center, die Astra Trident unterstützt. Es wird dringend empfohlen, dass Sie "Astra Control Provisioner aktivieren" Zugriff auf Funktionen für erweitertes Management und Storage-Bereitstellung, die über die von Astra Trident hinausgehen Zur Nutzung dieser erweiterten Funktion müssen Sie sowohl ein Upgrade auf Astra Control Center 23.10 als auch Astra Control Provisioner aktivieren. Astra Control Provisioner ist nicht mit älteren Versionen von Astra Control Center möglich.

- **Eine unterstützte Kubernetes-Distribution**

  **Für Schritte erweitern**

  Bestimmen Sie die Kubernetes-Version, die Sie ausführen:

  ```
  kubectl get nodes -o wide
  ```

- **Ausreichende Clusterressourcen**

  **Für Schritte erweitern**

  Ermitteln der verfügbaren Clusterressourcen:

  ```
  kubectl describe node <node name>
  ```

- **Eine Registrierung, mit der Sie Astra Control Center-Bilder per Push und Upload hochladen können**
- **Eine Standard-Speicherklasse**

  **Für Schritte erweitern**

  Bestimmen Sie Ihre Standard-Storage-Klasse:

  ```
  kubectl get storageclass
  ```

- **Gesunde und verfügbare API-Dienste**

  **Für Schritte erweitern**

  Stellen Sie sicher, dass alle API-Services in einem ordnungsgemäßen Zustand und verfügbar sind:

  ```
  kubectl get apiservices
  ```

- **(nur OpenShift) gesunde und verfügbare Clusteroperatoren**

**Für Schritte erweitern**

Stellen Sie sicher, dass alle Cluster Operator in einem ordnungsgemäßen Zustand und verfügbar sind.

```
kubectl get clusteroperators
```

- **Zugriff auf die NetApp Astra Control Image Registry**:
  Sie haben die Möglichkeit, Installations-Images und Funktionserweiterungen für Astra Control, wie z. B. Astra Control Provisioner, aus der NetApp-Image-Registrierung zu beziehen.

  **Für Schritte erweitern**

  a. Notieren Sie Ihre Astra Control Account-ID, die Sie zur Anmeldung in der Registrierung benötigen.

     Ihre Konto-ID wird in der Web-UI des Astra Control Service angezeigt. Wählen Sie das Symbol oben rechts auf der Seite aus, wählen Sie **API Access** aus und notieren Sie sich Ihre Konto-ID.

  b. Wählen Sie auf derselben Seite **API-Token generieren** aus und kopieren Sie die API-Token-Zeichenfolge in die Zwischenablage und speichern Sie sie in Ihrem Editor.

  c. Melden Sie sich in der Astra Control Registry an:

     ```
     docker login cr.astra.netapp.io -u <account-id> -p <api-token>
     ```

**Über diese Aufgabe**

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

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

- 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

Sie können das Bundle von Astra Control Center von der NetApp Support-Website herunterladen oder das Bundle mithilfe von Docker aus der Image-Registrierung des Astra Control Service abrufen.

**NetApp Support Website**

1. Laden Sie das Bundle mit Astra Control Center herunter (`astra-control-center-[version].tar.gz`) Vom "Download-Seite für Astra Control Center".
2. (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 Bündels zu überprüfen.

   **Erweitern Sie, um Details anzuzeigen**

   ```
   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.

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

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

**Astra Control-Image-Registrierung**

1. Melden Sie sich beim Astra Control Service an.
2. Wählen Sie im Dashboard **Deploy a self-Managed Instance of Astra Control** aus.
3. Folgen Sie den Anweisungen, um sich bei der Astra Control-Image-Registrierung anzumelden, das Astra Control Center-Installationsabbild zu ziehen und das Image zu extrahieren.

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

Sie können das NetApp Astra kubectl Befehlszeilenschnittstelle-Plug-in verwenden, um Images in ein lokales Docker Repository zu verschieben.

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

   ```
   kubectl astra
   ```

2. Führen Sie eine der folgenden Aktionen durch:
   - Wenn das Plugin installiert ist, sollte der Befehl die kubectl Plugin-Hilfe zurückgeben und Sie können die vorhandene Version von kubectl-astra 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 den sehen `acc.manifest.bundle.yaml` Datei und diese Verzeichnisse:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

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`).
   - <MY_FULL_REGISTRY_PATH> durch die URL des Docker Repositorys ersetzen, beispielsweise "<a href="https://<docker-registry>"" class="bare">https://<docker-registry>"</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/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

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=23.10.0-68
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
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
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://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/23.10.0-68/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}]
```

   b. Ändern `ASTRA_IMAGE_REGISTRY` Für das `kube-rbac-proxy` Bild zum Registrierungspfad, in dem Sie die Bilder in ein geschoben haben Vorheriger Schritt.

   c. Ändern `ASTRA_IMAGE_REGISTRY` 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_UPGRADETIMEOUT
  value: 300m
```

**Beispiel für astra_Control_Center_Operator_deploy.yaml:**

```
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: ASTRA_IMAGE_REGISTRY/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_UPGRADETIMEOUT
          value: 300m
        image: ASTRA_IMAGE_REGISTRY/acc-operator:23.10.72
        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.as
tra.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`) Aus Richtung `23.07.0` Bis `23.10.0`:

> Sie können kein direktes Upgrade von einer Version durchführen, die zwei oder mehr Versionen hinter der aktuellen Version enthält. Eine vollständige Liste der freigegebenen Versionen finden Sie im "Versionshinweise".

```
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
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
```

6. Speichern und beenden Sie den Dateieditor. Die Änderungen werden übernommen und das Upgrade beginnt.
7. (Optional) Stellen Sie sicher, dass die Pods beendet werden und wieder verfügbar sind:

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

8. 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   23.10.0-68
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.

# Astra Control Provisioner Aktivieren

In Astra Trident Version 23.10 und höher können Sie Astra Control Provisioner verwenden, damit lizenzierte Benutzer von Astra Control auf erweiterte Storage-Bereitstellungsfunktionen zugreifen können. Astra Control Provisioner bietet diese erweiterte Funktionalität zusätzlich zu den auf Astra Trident basierenden Standardfunktionen.

Bei den nächsten Updates für Astra Control wird der Provisioner Astra Trident als Storage-bereitstellung und -Orchestrierung in der Architektur von Astra Control ersetzen. Aus diesem Grund wird dringend empfohlen, Astra Control Benutzer für die Astra Control-Bereitstellung zu verwenden. Astra Trident wird weiterhin Open Source bleiben und mit neuen CSI- und anderen Funktionen von NetApp veröffentlicht, gepflegt, unterstützt und auf dem neuesten Stand sein.

**Über diese Aufgabe**

Befolgen Sie dieses Verfahren, wenn Sie als lizenzierter Astra Control Center-Benutzer die Astra Control Provisioner-Funktion verwenden möchten. Wenn Sie Astra Trident verwenden und die zusätzlichen Funktionen von Astra Control Provisioner verwenden möchten, sollten Sie dieses Verfahren auch befolgen.

In allen Fällen ist die bereitstellungsfunktion in Astra Trident 23.10 standardmäßig nicht aktiviert, kann jedoch mit diesem Prozess aktiviert werden.

**Bevor Sie beginnen**

Wenn Sie die Astra Control Provisioner aktivieren, gehen Sie wie folgt vor:

**Astra Control Provisioniert Benutzer mit Astra Control Center**

- **Bewirke eine Astra Control Center Lizenz**: Du benötigst eine "Astra Control Center-Lizenz" Um Astra Control Provisioner zu aktivieren und auf die enthaltenen Funktionen zuzugreifen.
- **Installation oder Upgrade auf Astra Control Center 23.10**: Sie benötigen diese Version, wenn Sie Astra Control Provisioner mit Astra Control verwenden möchten.
- **Bestätigen Sie, dass Ihr Cluster über eine AMD64-Systemarchitektur verfügt**: Das Astra Control Provisioner-Image wird sowohl in AMD64- als auch in ARM64-CPU-Architekturen bereitgestellt, aber nur AMD64 wird von Astra Control Center unterstützt.
- **Erhalten Sie ein Astra Control Service-Konto für den Registrierungszugriff**: Wenn Sie beabsichtigen, die Astra Control-Registrierung anstelle der NetApp-Support-Website zu verwenden, um das Astra Control-Provisioner-Image herunterzuladen, schließen Sie die Registrierung für einen ab "Astra Control Service Konto". Nachdem Sie das Formular ausgefüllt, übermittelt und ein BlueXP Konto erstellt haben, erhalten Sie eine Willkommens-E-Mail für Astra Control Service.
- **Wenn Sie Astra Trident installiert haben, bestätigen Sie, dass seine Version innerhalb eines Fensters mit vier Versionen ist**: Sie können ein direktes Upgrade auf Astra Trident 23.10 mit Astra Control Provisioner durchführen, wenn Ihr Astra Trident innerhalb eines Fensters mit vier Versionen von Version 23.10 ist. Sie können beispielsweise direkt von Astra Trident 22.10 auf 23.10 aktualisieren.

**Astra Control Provisioner nur Benutzer**

- **Bewirke eine Astra Control Center Lizenz**: Du benötigst eine "Astra Control Center-Lizenz" Um Astra Control Provisioner zu aktivieren und auf die enthaltenen Funktionen zuzugreifen.
- **Wenn Sie Astra Trident installiert haben, bestätigen Sie, dass seine Version innerhalb eines Fensters mit vier Versionen ist**: Sie können ein direktes Upgrade auf Astra Trident 23.10 mit Astra Control Provisioner durchführen, wenn Ihr Astra Trident innerhalb eines Fensters mit vier Versionen von Version 23.10 ist. Sie können beispielsweise direkt von Astra Trident 22.10 auf 23.10 aktualisieren.
- **Sie können ein Astra Control Service-Konto für den Registrierungszugriff abrufen**: Sie benötigen Zugriff auf die Registrierung, um Astra Control Provisioner-Bilder herunterladen zu können. Um zu beginnen, füllen Sie die Registrierung für einen aus "Astra Control Service Konto". Nachdem Sie das Formular ausgefüllt, übermittelt und ein BlueXP Konto erstellt haben, erhalten Sie eine Willkommens-E-Mail für Astra Control Service.

## (Schritt 1) Laden Sie die Astra Control Provisioner herunter und extrahieren Sie sie

Benutzer von Astra Control Center können das Image entweder über die NetApp Support Site oder die Astra Control Registry-Methode herunterladen. Für Astra Trident Benutzer, die Astra Control Provisioner ohne Astra Control verwenden möchten, sollte die Registrierungsmethode verwendet werden.

### (Optional) NetApp Support-Website

1. Laden Sie das Bundle für die Astra Control Bereitstellung herunter (`trident-acp-[version].tar`) Vom "Download-Seite für Astra Control Center".
2. (Empfohlen, aber optional) Laden Sie das Paket Zertifikate und Signaturen für Astra Control Center (astra-control-Center-certs-[Version].tar.gz) herunter, um die Signatur des tar-Bundles tar von trident-acp-[Version] zu überprüfen.

**Erweitern Sie, um Details anzuzeigen**

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

```
openssl dgst -sha256 -verify certs/AstraControlCenterDockerImages-public.pub -signature certs/trident-acp-[version].tar.sig trident-acp-[version].tar
```

3. Laden Sie das Astra Control Provisioner-Bild:

```
docker load < trident-acp-23.10.0.tar
```

Antwort:

```
Loaded image: trident-acp:23.10.0-linux-amd64
```

4. Markieren Sie das Bild:

```
docker tag trident-acp:23.10.0-linux-amd64 <my_custom_registry>/trident-acp:23.10.0
```

5. Laden Sie das Bild in Ihre benutzerdefinierte Registrierung:

```
docker push <my_custom_registry>/trident-acp:23.10.0
```

### (Optional) Astra Control-Image-Registrierung

Bei diesem Verfahren können Sie Podman anstelle von Docker für die Befehle verwenden. Wenn Sie eine Windows-Umgebung verwenden, wird PowerShell empfohlen.

1. Rufen Sie die NetApp Astra Control Image-Registry auf:
   a. Melden Sie sich bei der Astra Control Service Web-UI an, und wählen Sie das Symbol oben rechts auf der Seite aus.
   b. Wählen Sie **API-Zugriff**.
   c. Notieren Sie sich Ihre Konto-ID.
   d. Wählen Sie auf derselben Seite **API-Token generieren** aus und kopieren Sie die API-Token-Zeichenfolge in die Zwischenablage und speichern Sie sie in Ihrem Editor.
   e. Melden Sie sich über Ihre bevorzugte Methode in der Astra Control Registry an:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

```
crane auth login cr.astra.netapp.io -u <account-id> -p <api-token>
```

2. Wenn Sie über eine benutzerdefinierte Registrierung verfügen, führen Sie die folgenden Schritte aus, um das Bild in Ihre benutzerdefinierte Registrierung zu verschieben. Wenn Sie keine Registrierung verwenden, befolgen Sie die Schritte des Trident-Operators in "Nächster Abschnitt".

> Sie können Podman anstelle von Docker für die folgenden Befehle verwenden. Wenn Sie eine Windows-Umgebung verwenden, wird PowerShell empfohlen.

**Docker**

a. Rufen Sie das Astra Control Provisioner-Image aus der Registrierung ab:

> Das abgezogene Image unterstützt nicht mehrere Plattformen und unterstützt nur die gleiche Plattform wie der Host, der das Image gezogen hat, wie z. B. Linux AMD64.

```
docker pull cr.astra.netapp.io/astra/trident-acp:23.10.0
--platform <cluster platform>
```

Beispiel:

```
docker pull cr.astra.netapp.io/astra/trident-acp:23.10.0
--platform linux/amd64
```

b. Markieren Sie das Bild:

```
docker tag cr.astra.netapp.io/astra/trident-acp:23.10.0
<my_custom_registry>/trident-acp:23.10.0
```

c. Laden Sie das Bild in Ihre benutzerdefinierte Registrierung:

```
docker push <my_custom_registry>/trident-acp:23.10.0
```

**Kran**

a. Kopieren Sie das Astra Control Provisioner-Manifest in Ihre benutzerdefinierte Registry:

```
crane copy cr.astra.netapp.io/astra/trident-acp:23.10.0
<my_custom_registry>/trident-acp:23.10.0
```

## (Schritt 2) Aktivieren Sie die Astra Control-Bereitstellung in Astra Trident

Stellen Sie fest, ob die ursprüngliche Installationsmethode einen verwendet hat Und führen Sie die entsprechenden Schritte entsprechend Ihrer ursprünglichen Methode durch.

> Verwenden Sie Helm nicht, um die Astra Control Provisioner zu aktivieren. Wenn Sie Helm für die ursprüngliche Installation verwendet haben und ein Upgrade auf 23.10 durchführen, müssen Sie entweder den Trident-Operator oder tridentctl verwenden, um die Aktivierung von Astra Control Provisioner durchzuführen.

**Astra Trident Betreiber**

1. "Laden Sie das Astra Trident Installationsprogramm herunter und extrahieren Sie es".
2. Führen Sie diese Schritte aus, wenn Sie Astra Trident noch nicht installiert haben oder den Operator aus der ursprünglichen Astra Trident-Implementierung entfernt haben:
   a. Erstellen des CRD:

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.y
aml
```

   b. Erstellen Sie den Namespace für Trident (`kubectl create namespace trident`) Oder bestätigen Sie, dass der Namensraum Dreizack noch existiert (`kubectl get all -n trident`). Wenn der Namespace entfernt wurde, erstellen Sie ihn erneut.
3. Update von Astra Trident auf 23.10.0:

> Verwenden Sie für Cluster mit Kubernetes 1.24 oder früheren Versionen `bundle_pre_1_25.yaml`. Verwenden Sie für Cluster mit Kubernetes 1.25 oder höher `bundle_post_1_25.yaml`.

```
kubectl -n trident apply -f trident-installer-
23.10.0/deploy/<bundle-name.yaml>
```

4. Überprüfen Sie, ob Astra Trident ausgeführt wird:

```
kubectl get torc -n trident
```

   Antwort:

```
NAME      AGE
trident   21m
```

5. Wenn Sie eine Registry mit Geheimnissen haben, erstellen Sie ein Geheimnis, mit dem Sie das Astra Control Provisioner-Bild abrufen können:

```
kubectl create secret docker-registry <secret_name> -n trident
--docker-server=<my_custom_registry> --docker-username=<username>
--docker-password=<token>
```

6. Bearbeiten Sie den TridentOrchestrator CR, und nehmen Sie die folgenden Änderungen vor:

```
kubectl edit torc trident -n trident
```

a. Legen Sie einen benutzerdefinierten Registrierungsport für das Astra Trident Image fest oder ziehen Sie es aus der Astra Control Registry (`tridentImage: <my_custom_registry>/trident:23.10.0` Oder `tridentImage: netapp/trident:23.10.0`).

b. Astra Control Provisioner Aktivieren (`enableACP: true`).

c. Legen Sie den benutzerdefinierten Registrierungsport für das Astra Control Provisioner-Image fest oder ziehen Sie es aus der Astra Control Registry (`acpImage: <my_custom_registry>/trident-acp:23.10.0` Oder `acpImage: cr.astra.netapp.io/astra/trident-acp:23.10.0`).

d. Wenn Sie sich etabliert haben Geheimnisse der Bildausziehung Sie können diese hier einstellen (`imagePullSecrets: - <secret_name>`). Verwenden Sie den gleichen geheimen Namen, den Sie in den vorherigen Schritten festgelegt haben.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  tridentImage: <registry>/trident:23.10.0
  enableACP: true
  acpImage: <registry>/trident-acp:23.10.0
  imagePullSecrets:
  - <secret_name>
```

7. Speichern und beenden Sie die Datei. Der Bereitstellungsprozess wird automatisch gestartet.
8. Überprüfen Sie, ob der Operator, die Bereitstellung und Replikasets erstellt wurden.

```
kubectl get all -n trident
```

Es sollte nur eine Instanz* des Operators in einem Kubernetes-Cluster geben. Erstellen Sie nicht mehrere Implementierungen des Astra Trident Operators.

9. Überprüfen Sie die `trident-acp` Container läuft und das `acpVersion` Ist `23.10.0` Mit dem Status `Installed`:

```
kubectl get torc -o yaml
```

Antwort:

```
status:
  acpVersion: 23.10.0
  currentInstallationParams:
    ...
    acpImage: <registry>/trident-acp:23.10.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

**Tridentctl**

1. "Laden Sie das Astra Trident Installationsprogramm herunter und extrahieren Sie es".
2. "Wenn Sie bereits Astra Trident verwenden, deinstallieren Sie ihn aus dem Cluster, das ihn hostet".
3. Installieren Sie Astra Trident mit aktiviertem Astra Control Provisioner (`--enable-acp=true`):

```
./tridentctl -n trident install --enable-acp=true --acp
-image=mycustomregistry/trident-acp:23.10
```

4. Aktivieren Sie die Astra Control Provisioner-Funktion:

```
./tridentctl -n trident version
```

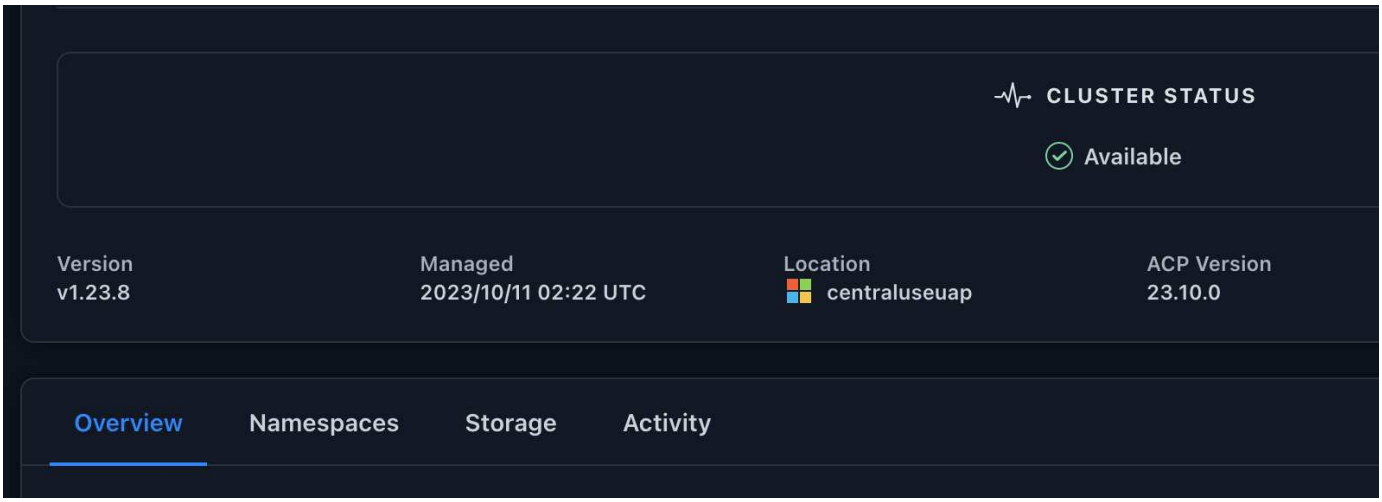
Antwort:

```
+----------------+----------------+-------------+ | SERVER VERSION |
CLIENT VERSION | ACP VERSION | +----------------+----------------
+-------------+ | 23.10.0 | 23.10.0 | 23.10.0. | +----------------
+----------------+-------------+
```

## Ergebnis

Die Bereitstellungsfunktion von Astra Control ist aktiviert und Sie können alle Funktionen der verwendeten Version verwenden.

(Nur für Astra Control Center Benutzer) nach der Installation von Astra Control wird für das Cluster, das die provisionierung in der Astra Control Center UI hostet, ein angezeigt `ACP version` Und nicht `Trident version` Feld und aktuelle installierte Versionsnummer.




**Finden Sie weitere Informationen**

- "Dokumentation für Astra Trident Upgrades"

# 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.

**Bevor Sie beginnen**

1. "Heben Sie die Verwaltung aller Apps auf" Auf den Clustern.
2. "Heben Sie die Verwaltung aller Cluster auf".

**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` (Oder benutzerdefinierter Name) Namespace:

   ```
   kubectl delete ns [netapp-acc or custom namespace]
   ```

   Beispielergebnis:

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

3. Löschen Sie die Komponenten des Astra Control Center-Bedienersystems 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
middlewaretcps.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
middlewaretcps.traefik.containo.us
```

## Weitere Informationen

- "Bekannte Probleme bei der Deinstallation"