



# **Nutzen Sie Astra**

## **Astra Control Center**

NetApp  
October 23, 2024

This PDF was generated from <https://docs.netapp.com/de-de/astra-control-center-2112/use/manage-apps.html> on October 23, 2024. Always check docs.netapp.com for the latest.

# Inhalt

- Nutzen Sie Astra. . . . . 1
  - Applikationsmanagement . . . . . 1
  - Schützen von Applikationen . . . . . 8
  - Zeigen Sie den Applikations- und Cluster-Zustand an . . . . . 32
  - Konto verwalten . . . . . 34
  - Buckets verwalten . . . . . 40
  - Management des Storage-Backends . . . . . 42
  - Überwachung und Sicherung der Infrastruktur . . . . . 44
  - Aktualisieren einer vorhandenen Lizenz . . . . . 51
  - Heben Sie das Management von Applikationen und Clustern auf . . . . . 52
  - Upgrade Astra Control Center . . . . . 53
  - Deinstallieren Sie Astra Control Center . . . . . 66

# Nutzen Sie Astra

## Applikationsmanagement

### 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 Apps in Astra Control zu starten, um die Apps und ihre Ressourcen zu verwalten.

### Anforderungen für das Applikationsmanagement

Astra Control verfügt über folgende Anforderungen an das Applikationsmanagement:

- **Lizenzierung:** Zur Verwaltung von Apps mit Astra Control Center benötigen Sie eine Astra Control Center-Lizenz.
- **Namespaces:** Astra Control erfordert, dass eine App nicht mehr als einen Single Namespace umfasst, aber ein Namespace kann mehr als eine App enthalten.
- **StorageClass:** Wenn Sie eine App mit einem explizit eingestellten StorageClass installieren und die App klonen müssen, muss das Zielcluster für den Klonvorgang die ursprünglich angegebene StorageClass haben. Das Klonen einer Applikation, deren StorageClass explizit auf ein Cluster festgelegt ist, das nicht über dieselbe StorageClass verfügt, schlägt fehl.
- **Kubernetes-Ressourcen:** Applikationen, die nicht von 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
  - KundenressourcenDefinition
  - Benutzerressource
  - DaemonSet
  - Einsatz
  - BereitstellungConfig
  - Eindringen
  - MutatingWebhook
  - PersistentVolumeClaim
  - Pod
  - ReplicaSet
  - Rollenverschwarten
  - Rolle
  - Route
  - Geheim
  - Service

- Service Account
- StatfulSet
- ValidierenWebhook

## Unterstützte Installationsmethoden für Anwendungen

Astra Control unterstützt folgende Installationsmethoden für Anwendungen:

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

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

- **Helm 3:** Wenn Sie Helm zur Installation von Apps verwenden, benötigt Astra Control Helm Version 3. Das Management und Klonen von Apps, die mit Helm 3 installiert sind (oder ein Upgrade von Helm 2 auf Helm 3), werden vollständig unterstützt. Das Verwalten von mit Helm 2 installierten Apps wird nicht unterstützt.
- **Vom Betreiber bereitgestellte Apps:** Astra Control unterstützt Apps, die mit Betreibern mit Namespace-Scoped installiert sind. Diese Betreiber sind in der Regel mit einer "Pass-by-Value"-Architektur statt "Pass-by-reference"-Architektur ausgelegt. Im Folgenden sind einige Bedieneranwendungen aufgeführt, die folgende Muster befolgen:
  - ["Apache K8ssandra"](#)
  - ["Jenkins CI"](#)
  - ["Percona XtraDB Cluster"](#)

Astra Control ist möglicherweise nicht in der Lage, einen Operator zu klonen, der mit einer „Pass-by-reference“-Architektur entworfen wurde (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.



Ein Operator und die von ihm zu installieren App müssen denselben Namespace verwenden. Möglicherweise müssen Sie die yaml-Bereitstellungsdatei ändern, um sicherzustellen, dass dies der Fall ist.

## Installation von Apps auf dem Cluster

Nachdem Sie jetzt Ihren Cluster zum Astra Control hinzugefügt haben, können Sie Apps installieren oder bestehende Apps auf dem Cluster managen. Jede Anwendung, die einem Namespace zugeordnet ist, kann verwaltet werden. Nachdem die Pods online sind, können Sie die App mit Astra Control verwalten.

Hilfe bei der Implementierung validierter Apps aus Helm Charts finden Sie in den folgenden Informationen:

- ["Implementieren Sie MariaDB aus einem Helm-Diagramm"](#)
- ["MySQL aus einem Helm Diagramm implementieren"](#)
- ["Postgres aus einem Helm-Diagramm bereitstellen"](#)
- ["Jenkins aus einem Helm-Diagramm implementieren"](#)

## Applikationsmanagement

Astra Control ermöglicht das Management von Applikationen auf Namespace-Ebene oder über Kubernetes-Label.



Mit Helm 2 installierte Apps werden nicht unterstützt.

Sie können die folgenden Aktivitäten zum Verwalten von Apps durchführen:

- Applikationsmanagement
  - [Applikationen nach Namespace managen](#)
  - [Apps nach Kubernetes Label managen](#)
- [Apps ignorieren](#)
- [Das Management von Apps wird aufgehoben](#)



Astra Control selbst ist keine Standard-App, sondern eine „System-App“. Sie sollten nicht versuchen, Astra Control selbst zu verwalten. Astra Control selbst wird für das Management nicht standardmäßig angezeigt. Verwenden Sie den Filter „System-Apps anzeigen“, um Systemanwendungen anzuzeigen.

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



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.

### Applikationen nach Namespace managen

Der Abschnitt **entdeckt** der Seite Apps zeigt Namensräume und alle Helm-installierten Apps oder benutzerdefinierte Apps in diesen Namespaces. Sie können jede Applikation einzeln oder auf Namespace-Ebene managen. All dies kommt auf die Granularität zurück, die Sie für Datensicherungsvorgänge benötigen.

Vielleicht möchten Sie beispielsweise 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. Je nach Anforderungen müssen die Applikationen separat gemanagt werden und nicht unter dem Single Namespace.

Während Astra Control ermöglicht Ihnen, beide Ebenen der Hierarchie (der Namespace und die Apps in diesem Namespace) getrennt zu verwalten, ist die beste Praxis, 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.

### Schritte

1. Wählen Sie in der linken Navigationsleiste die Option **Anwendungen**.
2. Wählen Sie **Entdeckt**.

| Name                | Ready | Cluster | Group               | Discovered           | Actions   |
|---------------------|-------|---------|---------------------|----------------------|-----------|
| default             |       |         | grp_default         | 2021/06/28 17:36 UTC | Managed   |
| default1            |       |         | grp1_default        | 2021/06/28 17:36 UTC | Unmanaged |
| default2            |       |         | grp2_default        | 2021/06/28 17:36 UTC | Unmanaged |
| netapp-acc-operator |       |         | netapp-acc-operator | 2021/07/13 12:36 UTC | Unmanaged |
| pcloud              |       |         | pcloud              | 2021/07/13 12:37 UTC | Unmanaged |

- Zeigen Sie die Liste der erkannten Namespaces an. Erweitern Sie den Namespace, um die Apps und zugehörigen Ressourcen anzuzeigen.

Astra Control zeigt Ihnen die Helm-Apps und benutzerdefinierte Apps im Namespace. Wenn Helm-Labels verfügbar sind, sind sie mit einem Tag-Symbol gekennzeichnet.

- Sehen Sie sich die Spalte **Gruppe** an, um zu sehen, in welchem Namespace die Anwendung ausgeführt wird (es ist mit dem Ordnersymbol gekennzeichnet).
- Entscheiden Sie, ob Sie jede Applikation einzeln oder auf Namespace-Ebene verwalten möchten.
- Suchen Sie die gewünschte App auf der gewünschten Ebene in der Hierarchie, und wählen Sie im Menü Aktionen die Option **Verwalten**.
- Wenn Sie keine App verwalten möchten, wählen Sie im Menü Aktionen neben der App die Option **Ignorieren** aus.

Wenn Sie beispielsweise alle Apps unter dem Namespace „maria“ verwalten möchten, so dass sie dieselben Snapshot- und Backup-Richtlinien haben, verwalten Sie den Namespace und ignorieren die Apps im Namespace.

- Um die Liste der verwalteten Apps anzuzeigen, wählen Sie **verwaltet** als Anzeigefilter aus.

| Name | Ready | Protected | Cluster | Group       | Discovered           | Actions  |
|------|-------|-----------|---------|-------------|----------------------|--|
| app1 |       |           |         | app-logging | 2021/06/28 17:36 UTC | Available<br>Snapshot<br>Backup<br>Clone<br>Unmanage |

Beachten Sie, dass die soeben hinzugefügte App unter der Spalte „geschützt“ ein Warnsymbol enthält, 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.

## Ergebnis

Apps, die Sie verwalten möchten, stehen jetzt auf der Registerkarte \* Managed\* zur Verfügung. Alle ignorierten Apps werden auf die Registerkarte **ignorierte** verschoben. Im Idealfall zeigt die Registerkarte „entdeckt“ keine Apps an, sodass neue Anwendungen leichter zu finden und zu verwalten sind.

## Apps nach Kubernetes Label managen

Astra Control beinhaltet eine Aktion oben auf der Seite Apps mit dem Namen **Define Custom App**. Sie können diese Aktion zum Verwalten von Apps verwenden, die mit einem Kubernetes-Etikett gekennzeichnet sind.

["Weitere Informationen über das Definieren benutzerdefinierter Applikationen nach dem Kubernetes Label"](#).

### Schritte

1. Wählen Sie in der linken Navigationsleiste die Option **Anwendungen**.
2. Wählen Sie **Definieren**.

The screenshot shows the 'Define custom application' dialog. It has a header 'Define custom application' with a close button. Below the header, there are two main sections: 'APPLICATION DETAILS' and 'SELECTED RESOURCES'. The 'APPLICATION DETAILS' section contains fields for 'New app application', 'Namespace', 'Cluster', and 'Label (optional)'. The 'SELECTED RESOURCES' section has a 'Filter by name' input and a table with columns 'Resources' and 'Created'. The table shows a list of resources: Deployment (1), ReplicaSet (1), Secret (4), and Pod (10). The 'UNSELECTED RESOURCES' section also has a 'Filter by name' input and a message: 'No selected resources. Every resource in the namespace is selected or matches a specified label.' On the right side, there is a sidebar titled 'DEFINE CUSTOM APPLICATION' with text: 'You can use this application builder to create a custom collection of Kubernetes resources based on a namespace and an optional label. Astra Control is aware of the relationships between resources and will use the guidance you provide here to create a complete set.' Below this text is a link: 'Read more in Define custom app'. At the bottom of the dialog, there are two buttons: 'Cancel' and 'Define custom application'.

3. Geben Sie im Dialogfeld **benutzerdefinierte Anwendung definieren** die erforderlichen Informationen zur Verwaltung der App an:
  - a. **Neue App**: Geben Sie den Anzeigenamen der App ein.
  - b. **Cluster**: Wählen Sie den Cluster aus, in dem sich die App befindet.
  - c. **Namespace**: Wählen Sie den Namespace für die App aus.
  - d. **Beschriftung**: Geben Sie eine Beschriftung ein oder wählen Sie eine Beschriftung aus den unten stehenden Ressourcen aus.
  - e. **Ausgewählte Ressourcen**: Zeigen Sie die ausgewählten Kubernetes-Ressourcen an, die Sie schützen möchten (Pods, Geheimnisse, persistente Volumes usw.) und managen Sie sie.
    - Zeigen Sie die verfügbaren Beschriftungen an, indem Sie eine Ressource erweitern und die Anzahl der Beschriftungen auswählen.
    - Wählen Sie eine der Beschriftungen aus.

Nachdem Sie eine Bezeichnung ausgewählt haben, wird sie im Feld **Etikett** angezeigt. Astra Control aktualisiert außerdem den Abschnitt **nicht ausgewählte Ressourcen**, um die Ressourcen

anzuzeigen, die nicht mit dem ausgewählten Etikett übereinstimmen.

- f. **Nicht ausgewählte Ressourcen:** Überprüfen Sie die App-Ressourcen, die Sie nicht schützen möchten.

4. Wählen Sie **benutzerdefinierte Anwendung definieren**.

### Ergebnis

Astra Control ermöglicht das Management der App. Sie finden es jetzt auf der Registerkarte **verwaltet**.

### Apps ignorieren

Wenn eine App entdeckt wurde, wird sie in der Liste entdeckt angezeigt. In diesem Fall können Sie die entdeckte Liste aufräumen, damit neue, neu installierte Apps einfacher zu finden sind. Oder Sie haben unter Umständen Anwendungen, die Sie verwalten und entscheiden später, dass Sie sie nicht mehr verwalten möchten. Wenn Sie diese Apps nicht verwalten möchten, können Sie angeben, dass sie ignoriert werden sollen.

Möglicherweise möchten Sie auch Apps unter einem Namespace zusammen managen (Namespace-verwaltet). Sie können Apps ignorieren, die Sie vom Namespace ausschließen möchten.

### Schritte

1. Wählen Sie in der linken Navigationsleiste die Option **Anwendungen**.
2. Wählen Sie als Filter \* entdeckt\* aus.
3. Wählen Sie die App aus.
4. Wählen Sie im Menü Aktionen die Option **Ignorieren** aus.
5. Um das ignorieren rückgängig zu machen, wählen Sie im Menü Aktionen die Option **Unignore**.

### Das Management von Apps wird aufgehoben

Wenn Sie keine Backups, Snapshots oder Klone mehr erstellen möchten, können Sie deren Management beenden.



Wenn Sie die Verwaltung einer Anwendung aufheben, gehen alle Backups oder Snapshots verloren, die zuvor erstellt wurden.

### Schritte

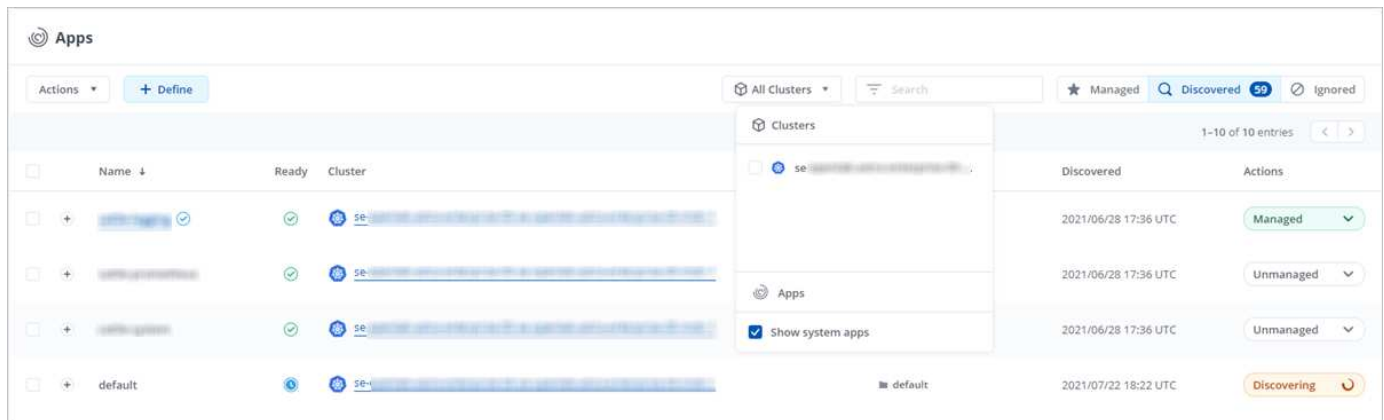
1. Wählen Sie in der linken Navigationsleiste die Option **Anwendungen**.
2. Wählen Sie als Filter \* verwaltet\* aus.
3. Wählen Sie die App aus.
4. Wählen Sie im Menü Aktionen die Option **Verwaltung aufheben** aus.
5. Überprüfen Sie die Informationen.
6. Geben Sie zur Bestätigung „nicht verwalten“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

### Wie sieht es mit System-Applikationen aus?

Astra Control erkennt auch die System-Applikationen, die auf einem Kubernetes Cluster ausgeführt werden. Sie können Systemanwendungen anzeigen, indem Sie in der Symbolleiste unter dem Clusterfilter das



Kontrollkästchen **System-Apps anzeigen** aktivieren.



Wir zeigen Ihnen diese System-Apps standardmäßig nicht, da es selten ist, dass Sie sie sichern müssen.



Astra Control selbst ist keine Standard-App, sondern eine „System-App“. Sie sollten nicht versuchen, Astra Control selbst zu verwalten. Astra Control selbst wird für das Management nicht standardmäßig angezeigt. Verwenden Sie den Filter „System-Apps anzeigen“, um Systemanwendungen anzuzeigen.

## Weitere Informationen

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

## Definieren Sie ein Beispiel für eine benutzerdefinierte Anwendung

Wenn Sie eine benutzerdefinierte App erstellen, können Sie Elemente Ihres Kubernetes Clusters zu einer einzelnen Applikation gruppieren.

Eine benutzerdefinierte App bietet Ihnen mehr granulare Kontrolle darüber, was in einem Astra Control-Betrieb enthalten ist, darunter:

- Klon
- Snapshot
- Backup
- Sicherungsrichtlinie

In den meisten Fällen möchten Sie die Funktionen von Astra Control in Ihrer gesamten App nutzen. Sie können jedoch auch eine benutzerdefinierte App erstellen, die diese Funktionen durch die Beschriftungen verwendet, die Sie Kubernetes-Objekten in einem Namespace zuweisen.

Um eine benutzerdefinierte App zu erstellen, gehen Sie zur Seite Apps und wählen **+ Definieren**.

Während Sie Ihre Auswahl treffen, zeigt Ihnen das Fenster Benutzerdefinierte App an, welche Ressourcen in Ihre benutzerdefinierte App aufgenommen oder von dieser ausgeschlossen werden. Dadurch können Sie sicherstellen, dass Sie die richtigen Kriterien für die Definition Ihrer benutzerdefinierten App auswählen.



Benutzerdefinierte Applikationen können nur innerhalb eines bestimmten Namespace auf einem einzelnen Cluster erstellt werden. Astra Control bietet keine Unterstützung für eine benutzerdefinierte App, die mehrere Namespaces oder Cluster umfasst.

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"](#).



Überlappende Richtlinien für dieselbe Ressource unter verschiedenen Namen können Datenkonflikte verursachen. Wenn Sie eine benutzerdefinierte App für eine Ressource erstellen, müssen Sie sicher sein, dass sie nicht unter anderen Richtlinien geklont oder gesichert wird.

### Beispiel: Separate Schutzpolitik für kanarische Veröffentlichung

In diesem Beispiel managt das devops-Team eine Implementierung für kanarische Versionen. Im Cluster befinden sich 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 benutzerdefinierte Apps: Eine für die canary-Version und eine für die stabile Version. Hierdurch werden Backups, Snapshots und Klonvorgänge für die beiden Gruppen von Kubernetes-Objekten getrennt.

#### Schritte

1. Nachdem das Team den Cluster zu Astra Control hinzugefügt hat, besteht der nächste Schritt darin, eine benutzerdefinierte App zu definieren. Dazu wählt das Team auf der Seite Apps die Schaltfläche **+ Definieren** aus.
2. Im daraufhin angezeigten Pop-up-Fenster setzt das Team ein `devops-canary-deployment` Als App-Name. Das Team wählt den Cluster im Drop-down-Menü **Namespace Cluster** aus, dann der Namensraum der App aus dem Drop-down **\*\***.
3. Das Team kann entweder eingeben `deployment=canary` Wählen Sie im Feld **Labels** das Etikett aus den unten aufgeführten Ressourcen aus.
4. Nach der Definition der benutzerdefinierten App für die canary-Bereitstellung wiederholt das Team den Prozess für die stabile Bereitstellung.

Wenn das Team die beiden benutzerdefinierten Apps erstellt hat, können diese Ressourcen als jede andere Astra Control Anwendung behandelt werden. Sie können sie klonen, Backups und Snapshots erstellen und für jede Gruppe von Ressourcen auf der Basis der Kubernetes-Labels eine individuelle Sicherungsrichtlinie erstellen.

## 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"](#).

### Workflow für Applikationssicherung

Anhand des folgenden Beispielworkflows können Sie Ihre Apps schützen.

#### [Eins] Backup 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] Optional: Passen Sie die Schutzrichtlinien an

Wenn Applikationen und ihre Nutzungsmuster sich ändern, passen Sie die Sicherungsrichtlinien nach Bedarf an, um einen bestmöglichen Schutz zu gewährleisten.

#### [Vier] Stellen Sie Ihre Applikationen bei einem Notfall 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).

## Sichern von Applikationen durch Snapshots und Backups

Schützen Sie Ihre Applikationen, indem Sie Snapshots und Backups über eine automatisierte Sicherungsrichtlinie oder Ad-hoc-Erstellung erstellen. Sie können die Astra UI oder verwenden ["Die Astra Control API"](#) Um Anwendungen zu schützen.



Wenn Sie Helm zur Implementierung von Apps verwenden, erfordert 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.



Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder dem 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
```

## 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. Eine Sicherungsrichtlinie kann beispielsweise wöchentliche Backups und tägliche Snapshots erstellen und die Backups und Snapshots einen Monat lang aufbewahren. Wie oft Sie Snapshots und Backups erstellen und wie lange Sie sie behalten, hängt von den Anforderungen Ihres Unternehmens ab.

### 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.

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

**Configure protection policy**

STEP 1/2: DETAILS

✕

PROTECTION SCHEDULE

🕒 Hourly

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

🕒 Daily

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

🕒 Weekly

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

🕒 Monthly

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

● Hourly

● Daily

● **Weekly**

● Monthly

Select Weekday(s) (optional)

Monday X

Time (UTC) (optional)

02:00

– Snapshots to keep +

26

– Backups to keep +

0

BACKUP DESTINATION

Bucket

ntp-nautilus-bucket-10 - ntp-nautilus-bucket-10

Default

OVERVIEW

Schedule and retention

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

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

Read more in [Protection policies](#)

🔗 Application

cattle-logging

📁 Namespace

cattle-logging

🌐 Cluster

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

Cancel

Review →

5. Wählen Sie **Bewertung**.

6. Wählen Sie **Schutzrichtlinie Festlegen**.

## Ergebnis

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

## Erstellen Sie einen Snapshot

Sie können jederzeit einen On-Demand-Snapshot erstellen.

### Schritte

1. Wählen Sie **Anwendungen**.
2. Wählen Sie die Dropdown-Liste in der Spalte **Aktionen** für die gewünschte App aus.
3. Wählen Sie **Snapshot**.
4. Passen Sie den Namen des Snapshots an und wählen Sie dann **Review**.
5. Überprüfen Sie die Snapshot-Zusammenfassung und wählen Sie **Snapshot**.

## Ergebnis

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

## Erstellen Sie ein Backup

Sie können eine App auch jederzeit sichern.



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

## Schritte

1. Wählen Sie **Anwendungen**.
2. Wählen Sie die Dropdown-Liste in der Spalte **Aktionen** für die gewünschte App aus.
3. Wählen Sie **Backup**.
4. Passen Sie den Namen des Backups an.
5. 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.
6. Wählen Sie ein Ziel für das Backup aus der Liste der Speicher-Buckets aus.
7. Wählen Sie **Bewertung**.
8. Überprüfen Sie die Backup-Zusammenfassung und wählen Sie **Backup**.

## Ergebnis

Astra Control Center 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.



Es gibt keine Möglichkeit, ein ausgelaufenes Backup zu stoppen. Wenn Sie das Backup löschen müssen, warten Sie, bis es abgeschlossen ist, und befolgen Sie die Anweisungen unter [Backups löschen](#). So löschen Sie ein fehlgeschlagenes Backup: "[Verwenden Sie die Astra Control API](#)".



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

## Anzeigen von Snapshots und Backups

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

### Schritte

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

Die Snapshots werden standardmäßig angezeigt.

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

## Snapshots löschen

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

## Schritte

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

## Ergebnis

Astra Control Center löscht den Snapshot.

## Backups löschen

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



Es gibt keine Möglichkeit, ein ausgelaufenes Backup zu stoppen. Wenn Sie das Backup löschen müssen, warten Sie, bis es abgeschlossen ist, und befolgen Sie diese Anweisungen. So löschen Sie ein fehlgeschlagenes Backup: "[Verwenden Sie die Astra Control API](#)".

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

## Ergebnis

Astra Control Center löscht das Backup.

## Wiederherstellung von Applikationen

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



Wenn Sie Helm zur Implementierung von Apps verwenden, erfordert 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.



Wenn Sie ein anderes Cluster wiederherstellen, stellen Sie sicher, dass das Cluster denselben Zugriffsmodus für persistente Volumes verwendet (z. B. ReadWriteManche). Der Wiederherstellungsvorgang schlägt fehl, wenn der Zugriffsmodus des Ziel-persistenten Volumes anders ist.



Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder dem 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** und dann den Namen einer App aus.
2. Wählen Sie **Datenschutz**.
3. Wenn Sie von einem Snapshot wiederherstellen möchten, lassen Sie das **Snapshots** -Symbol ausgewählt. Andernfalls wählen Sie das Symbol **Backups** aus, um aus einem Backup wiederherzustellen.
4. Wählen Sie die Dropdown-Liste in der Spalte **Aktionen** für den Snapshot oder die Sicherung aus, aus der Sie wiederherstellen möchten.
5. Wählen Sie **Anwendung wiederherstellen**.
6. **Restore Details**: Geben Sie Details für die wiederhergestellte App an. Standardmäßig werden das aktuelle Cluster und der aktuelle Namespace angezeigt. Lassen Sie diese Werte intakt, um eine App an Ort und Stelle wiederherzustellen, die die App auf eine frühere Version von selbst zurücksetzt. Ändern Sie diese Werte, wenn Sie die Daten in einem anderen Cluster oder Namespace wiederherstellen möchten.
  - Geben Sie einen Namen und einen Namespace für die App ein.
  - Wählen Sie das Ziel-Cluster für die App aus.
  - Wählen Sie **Bewertung**.
7. **Zusammenfassung wiederherstellen**: Überprüfen Sie die Details über die Wiederherstellungsaktion, geben Sie "wiederherstellen" ein und wählen Sie **Wiederherstellen**.

## Ergebnis

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



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.

## Klonen und Migrieren von Applikationen

Eine vorhandene Applikation klonen, um eine doppelte Applikation auf demselben Kubernetes-Cluster oder einem anderen Cluster zu erstellen. 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 UI



## oder verwenden "Die Astra Control API" Zum Klonen und Migrieren von Applikationen



Wenn Sie eine App implementieren, die explizit auf StorageClass gesetzt ist und Sie die Applikation klonen müssen, muss das Ziel-Cluster über die ursprünglich angegebene StorageClass verfügen. Das Klonen einer Applikation, deren StorageClass explizit auf ein Cluster festgelegt ist, das nicht über dieselbe StorageClass verfügt, schlägt fehl.



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.



Wenn Sie eine App zwischen Clustern klonen, müssen die Quell- und Ziel-Cluster dieselbe Verteilung von OpenShift aufweisen. Wenn Sie beispielsweise eine App aus einem OpenShift 4.7-Cluster klonen, verwenden Sie ein Ziel-Cluster, das auch OpenShift 4.7 ist.

Wenn Astra Control Center eine Applikation geklont, wird ein Klon Ihrer Applikationskonfiguration und des persistenten Storage erstellt.



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.



Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder dem 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
```

### Was Sie benötigen

Zum Klonen von Applikationen auf einem anderen Cluster benötigen Sie einen Standard-Bucket. Wenn Sie einen ersten Bucket hinzufügen, wird dieser zum Standard-Bucket.

### Schritte

1. Wählen Sie **Anwendungen**.
2. Führen Sie einen der folgenden Schritte aus:
  - Wählen Sie die Dropdown-Liste 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. **Clone Details**: Geben Sie Details für den Klon an:
  - Geben Sie einen Namen ein.
  - Geben Sie einen Namespace für den Klon ein.

- Wählen Sie ein Ziel-Cluster für den Klon.
  - Wählen Sie aus, ob Sie den Klon aus einem vorhandenen Snapshot oder einem vorhandenen Backup erstellen möchten. Wenn Sie diese Option nicht wählen, erstellt Astra Control Center den Klon aus dem aktuellen Status der App.
5. **Quelle:** Wenn Sie sich für das Klonen aus einem vorhandenen Snapshot oder Backup entscheiden, wählen Sie den Snapshot oder die Sicherung, die Sie verwenden möchten.
6. Wählen Sie **Bewertung**.
7. **Clone Summary:** Überprüfen Sie die Details über den Klon und wählen Sie **Clone**.

## Ergebnis

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



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.

## Anwendungsausführungshaken verwalten

Ein Execution Hook ist ein benutzerdefiniertes Skript, das Sie vor oder nach einem Snapshot einer verwalteten App ausführen können. Wenn Sie beispielsweise über eine Datenbank-App verfügen, können Sie mithilfe von Testsuiten alle Datenbanktransaktionen vor dem Snapshot anhalten und die Transaktionen nach Abschluss des Snapshots fortsetzen. Dies gewährleistet applikationskonsistente Snapshots.

### Standard-Ausführungshaken und reguläre Ausdrücke

Für einige Applikationen verfügt Astra Control über Standard-Testhooks von NetApp, die für Frost- und Thaw-Vorgänge vor und nach Snapshots sorgen. Astra Control verwendet regelmäßige Ausdrücke, um das Container-Image einer App mit diesen Apps zu kombinieren:

- MariaDB
  - Übereinstimmende reguläre Ausdrücke: `\Bmariadb\b`
- MySQL
  - Übereinstimmende reguläre Ausdrücke: `\Bmysql\b`
- PostgreSQL
  - Übereinstimmende reguläre Ausdrücke: `\Bpostgresql\b`

Bei Übereinstimmung werden die von NetApp bereitgestellten Standard-Testsuite für die Applikation in der Liste der aktiven Testhooks der Applikation angezeigt. Die Haken werden automatisch ausgeführt, wenn Snapshots der App erstellt werden. Wenn eine Ihrer benutzerdefinierten Apps einen ähnlichen Bildnamen hat, der mit einem der regulären Ausdrücke übereinstimmt (und Sie nicht die standardmäßigen Testsuiten verwenden möchten), können Sie entweder den Bildnamen ändern. Oder deaktivieren Sie den Standard-Testsuite-Haken für diese App und verwenden Sie stattdessen einen benutzerdefinierten Haken.

Sie können die standardmäßigen Testsuiten nicht löschen oder ändern.

## Wichtige Hinweise zu benutzerdefinierten Testausführungshaken

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

- Astra Control erfordert das Schreiben von Testsuiten im Format ausführbarer Shell-Skripte.
- Die Skriptgröße ist auf 128 KB beschränkt.
- Astra Control verwendet die Einstellungen für Testausführungshaken und die zugehörigen Kriterien, um zu bestimmen, welche Haken für einen Snapshot gelten.
- Bei allen Verbindungsausfällen handelt es sich um weiche Fehler. Andere Haken und der Snapshot 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.



Da die Testsuitehingel die Funktionalität der Anwendung, für die sie ausgeführt werden, oft reduzieren oder vollständig deaktivieren, sollten Sie immer versuchen, die Zeit zu minimieren, die Ihre benutzerdefinierten Testausführungshaken für die Ausführung benötigt.

Wenn ein Snapshot ausgeführt wird, finden Ereignisse zum Ausführen von Testinsuiten in der folgenden Reihenfolge statt:

1. Auf den entsprechenden Containern werden alle relevanten, von NetApp zur Verfügung gestellten Standard-Hooks für die Snapshot-Ausführung ausgeführt.
2. Alle entsprechenden benutzerdefinierten Hooks für die vor-Snapshot-Ausführung werden auf den entsprechenden Containern ausgeführt. Sie können beliebig viele benutzerdefinierte Pre-Snapshot Hooks erstellen und ausführen, aber die Reihenfolge der Ausführung dieser Hooks vor dem Snapshot ist weder garantiert noch konfigurierbar.
3. Der Snapshot wird durchgeführt.
4. Alle entsprechenden benutzerdefinierten Hooks für die Ausführung nach dem Snapshot werden auf den entsprechenden Containern ausgeführt. Sie können beliebig viele benutzerdefinierte Haken für die Nachbearbeitung erstellen und ausführen, aber die Reihenfolge der Ausführung dieser Hooks nach dem Snapshot ist weder garantiert noch konfigurierbar.
5. Auf den entsprechenden Containern werden alle relevanten, von NetApp bereitgestellten Standard-Hooks für die Nachbearbeitung ausgeführt.



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

## Vorhandene Testsuiten anzeigen

Sie können vorhandene benutzerdefinierte oder von NetApp bereitgestellte Standard-Testhooks 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 können den Status, die Quelle und die Ausführung eines Hakens (vor oder nach dem Schnappschuss) sehen. Um Ereignisprotokolle zu den Testausführungshaken anzuzeigen, gehen Sie zur Seite **Aktivität** im linken Navigationsbereich.

## Erstellen Sie einen benutzerdefinierten Testsuite-Haken

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



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

### Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie **Neuen Haken hinzufügen**.
4. Wählen Sie im Bereich **Hook Details**, je nachdem, wann der Haken laufen soll, **Pre-Snapshot** oder **Post-Snapshot**.
5. Geben Sie einen eindeutigen Namen für den Haken ein.
6. (Optional) Geben Sie alle Argumente ein, um während der Ausführung an den Haken weiterzuleiten. Drücken Sie nach jedem eingegebenen Argument die Eingabetaste, um jedes Argument aufzuzeichnen.
7. Wenn der Haken im Bereich **Container Images** auf alle Container-Bilder in der Anwendung laufen soll, aktivieren Sie das Kontrollkästchen **auf alle Container-Bilder** anwenden. Sollte der Haken stattdessen nur auf ein oder mehrere angegebene Container-Images wirken, geben Sie die Container-Bildnamen in das Feld **Container-Bildnamen ein, die mit** übereinstimmen.
8. Führen Sie im Bereich **Script** einen der folgenden Schritte aus:
  - 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.
  - Fügen Sie in ein benutzerdefiniertes Skript aus der Zwischenablage ein.
    - i. Wählen Sie die Option **aus Zwischenablage einfügen**.

- 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.
9. Wählen Sie **Haken hinzufügen**.

### 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 die Dropdown-Liste **Aktionen** 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 die Dropdown-Liste **Aktionen** für einen Haken, den Sie löschen möchten.
4. Wählen Sie **Löschen**.

### Beispiele für Testausführungshaken

Nutzen Sie die folgenden Beispiele, um eine Vorstellung davon zu erhalten, wie Sie Ihre Testausführungshaken strukturieren. Sie können diese Haken als Vorlagen oder als Testskripte verwenden.

#### Einfaches Erfolgsbeispiel

Dies ist ein Beispiel für einen einfachen Haken, der erfolgreich ist und eine Nachricht in die Standardausgabe und Standardfehler schreibt.

```
#!/bin/sh

# success_sample.sh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#
```

```

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}

#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}

#
# main
#

# log something to stdout
info "running success_sample.sh"

# exit with 0 to indicate success
info "exit 0"
exit 0

```

### Einfaches Erfolgsbeispiel (Bash-Version)

Dies ist ein Beispiel für einen einfachen Haken, der erfolgreich ist und eine Nachricht in die Standardausgabe und Standardfehler schreibt, für bash geschrieben.

```
#!/bin/bash

# success_sample.bash
#
# A simple noop success hook script for testing purposes.
#
# args: None

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}

#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}

#
# main
#

# log something to stdout
info "running success_sample.bash"

# exit with 0 to indicate success
info "exit 0"
```

```
exit 0
```

### Einfaches Erfolgsbeispiel (zsh-Version)

Dies ist ein Beispiel für einen einfachen Haken, der erfolgreich ist und eine Nachricht in Standardausgabe und Standardfehler schreibt, geschrieben für Z Shell.

```
#!/bin/zsh

# success_sample.zsh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}

#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}

#
```



```
# main
#

# log something to stdout
info "running success_sample.zsh"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

### Erfolg mit Argumenten Beispiel

Das folgende Beispiel zeigt, wie Sie in einem Haken Aargliste verwenden können.

```
#!/bin/sh

# success_sample_args.sh
#
# A simple success hook script with args for testing purposes.
#
# args: Up to two optional args that are echoed to stdout
#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}

#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
```

```

error() {
    msg "ERROR: $" 1>&2
}

#
# main
#

# log something to stdout
info "running success_sample_args.sh"

# collect args
arg1=$1
arg2=$2

# output args and arg count to stdout
info "number of args: $#
info "arg1 ${arg1}"
info "arg2 ${arg2}"

# exit with 0 to indicate success
info "exit 0"
exit 0

```

### Beispiel für Haken vor dem Snapshot/nach dem Snapshot

Das folgende Beispiel zeigt, wie dasselbe Skript sowohl für einen Pre-Snapshot als auch für einen Post-Snapshot-Haken verwendet werden kann.

```

#!/bin/sh

# success_sample_pre_post.sh
#
# A simple success hook script example with an arg for testing purposes
# to demonstrate how the same script can be used for both a prehook and
# posthook
#
# args: [pre|post]

# unique error codes for every error case
ebase=100
eusage=$((ebase+1))
ebadstage=$((ebase+2))
epre=$((ebase+3))

```

```

epost=$((ebase+4))

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}

#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}

#
# Would run prehook steps here
#
prehook() {
    info "Running noop prehook"
    return 0
}

#
# Would run posthook steps here
#
posthook() {
    info "Running noop posthook"
    return 0
}

```

```

}

#
# main
#

# check arg
stage=$1
if [ -z "${stage}" ]; then
    echo "Usage: $0 <pre|post>"
    exit ${eusage}
fi

if [ "${stage}" != "pre" ] && [ "${stage}" != "post" ]; then
    echo "Invalid arg: ${stage}"
    exit ${ebadstage}
fi

# log something to stdout
info "running success_sample_pre_post.sh"

if [ "${stage}" = "pre" ]; then
    prehook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during prehook"
    fi
fi

if [ "${stage}" = "post" ]; then
    posthook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during posthook"
    fi
fi

exit ${rc}

```

### Fehlerbeispiel

Das folgende Beispiel zeigt, wie Sie Fehler in einem Haken handhaben können.

```
#!/bin/sh
```

```

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}

#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}

#
# main
#

# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr

```

```
error "script failed, returning exit code ${argexitcode}"
```

```
# exit with specified exit code  
exit ${argexitcode}
```

### Beispiel für ausführlichen Fehler

Das folgende Beispiel zeigt, wie Sie Fehler in einem Haken mit detaillierteren Protokollierung behandeln können.

```
#!/bin/sh  
  
# failure_sample_verbose.sh  
#  
# A simple failure hook script with args for testing purposes.  
#  
# args: [The number of lines to output to stdout]  
  
#  
# Writes the given message to standard output  
#  
# $* - The message to write  
#  
msg() {  
    echo "$*"  
}  
  
#  
# Writes the given information message to standard output  
#  
# $* - The message to write  
#  
info() {  
    msg "INFO: $*"  
}  
  
#  
# Writes the given error message to standard error  
#  
# $* - The message to write  
#  
error() {  
    msg "ERROR: $*" 1>&2  
}
```

```

#
# main
#

# log something to stdout
info "running failure_sample_verbose.sh"


# output arg value to stdout
linecount=$1
info "line count ${linecount}"


# write out a line to stdout based on line count arg
i=1
while [ "$i" -le ${linecount} ]; do
    info "This is line ${i} from failure_sample_verbose.sh"
    i=$(( i + 1 ))
done

error "exiting with error code 8"
exit 8

```

### Fehler bei einem Beispiel für den Exit-Code

Das folgende Beispiel zeigt, dass ein Haken mit einem Exit-Code ausfällt.

```

#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}

```

```

#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}

#
# main
#

# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}

```

### Beispiel Erfolg nach Ausfall

Das folgende Beispiel zeigt, dass bei der ersten Ausführung ein Haken versagt, der jedoch nach dem zweiten Lauf erfolgreich ist.

```

#!/bin/sh

# failure_then_success_sample.sh
#
# A hook script that fails on initial run but succeeds on second run for

```



```

testing purposes.
#
# Helpful for testing retry logic for post hooks.
#
# args: None
#

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}

#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}

#
# main
#

# log something to stdout
info "running failure_success sample.sh"

if [ -e /tmp/hook-test.junk ] ; then
    info "File does exist. Removing /tmp/hook-test.junk"

```

```

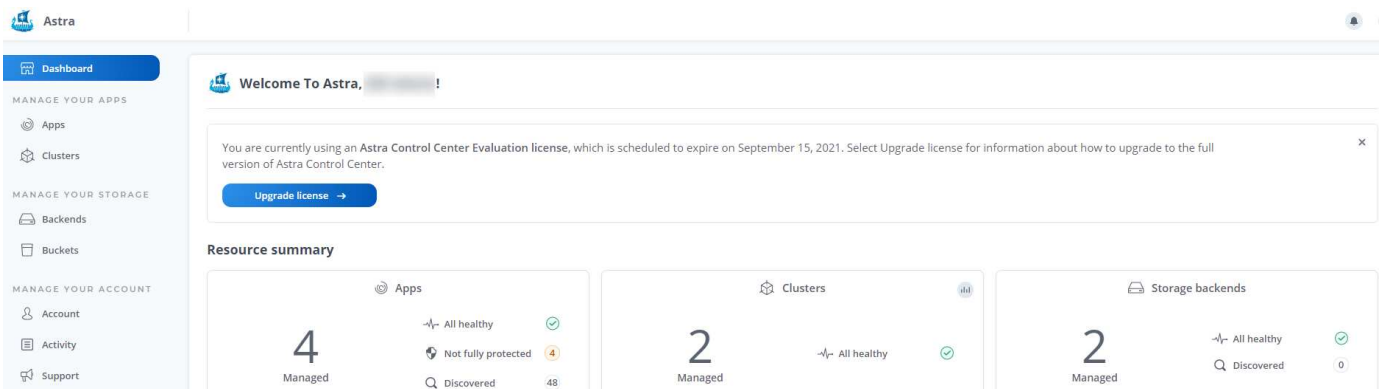
rm /tmp/hook-test.junk
info "Second run so returning exit code 0"
exit 0
else
info "File does not exist. Creating /tmp/hook-test.junk"
echo "test" > /tmp/hook-test.junk
error "Failed first run, returning exit code 5"
exit 5
fi

```

## Zeigen Sie den Applikations- und Cluster-Zustand an

### 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 dieser Faktoren heruntergehen. 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.

## Anzeigen des Systemzustands und der Details von Clustern

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.

### 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.
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.

## Anzeigen des Funktionszustands und der Details einer App

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

### Schritte

1. Wählen Sie in der Astra Control Center-UI **Anwendungen** und dann den Namen einer App aus.
2. Hier finden Sie die gewünschten Informationen:

## Anwendungsstatus

Gibt einen Status an, der den Status der App in Kubernetes wiedergibt. Sind Pods und persistente Volumes beispielsweise online? Wenn eine Applikation fehlerhaft ist, müssen Sie mit den Kubernetes-Protokollen zum Beheben des Problems im Cluster wechseln. Astra stellt keine Informationen zur Verfügung, die Ihnen bei der Behebung einer defekten App helfen.

## App-Schutzstatus

Gibt den Status an, 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.

## Überblick

Informationen über den Status der Pods, die mit der App verknüpft sind.

## Datensicherung

Hiermit können Sie eine Datenschutzrichtlinie konfigurieren und die vorhandenen Snapshots und Backups anzeigen.

## Storage

Zeigt Ihnen die persistenten Volumes auf App-Ebene. Der Zustand eines persistenten Volumes befindet sich aus der Perspektive des Kubernetes Clusters.

## Ressourcen

Hiermit können Sie überprüfen, welche Ressourcen gesichert und gemanagt 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

## Benutzer managen

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

## 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, aber Apps oder Cluster nicht verwalten oder Snapshots oder 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. 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 die Dropdown-Liste **Aktionen** aus, und wählen Sie **Passwort ändern**.
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 auf der Registerkarte **Benutzer** die Dropdown-Liste in der Spalte **Status** für den Benutzer 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**.

## Ändern Sie die Rolle eines Benutzers

Benutzer mit der Rolle „Eigentümer“ können die Rolle aller Benutzer ändern, während Benutzer mit der Administratorrolle die Rolle von Benutzern ändern können, die die Rolle „Administrator“, „Mitglied“ oder „Viewer“ haben.

### Schritte

1. Wählen Sie im Navigationsbereich \* Konto verwalten\* die Option **Konto**.
2. Wählen Sie auf der Registerkarte **Benutzer** die Dropdown-Liste in der Spalte **Rolle** für den Benutzer aus.
3. Wählen Sie eine neue Rolle aus, und wählen Sie dann **Rolle ändern**, wenn Sie dazu aufgefordert werden.

### Ergebnis

Astra Control Center aktualisiert die Benutzerberechtigungen auf der Grundlage der neuen Rolle, die Sie ausgewählt haben.

## 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 **Aktionen** und wählen Sie **Benutzer entfernen**.
4. Wenn Sie aufgefordert werden, bestätigen Sie den Löschvorgang, indem Sie das Wort "Entfernen" eingeben und dann **Ja, Benutzer entfernen** wählen.

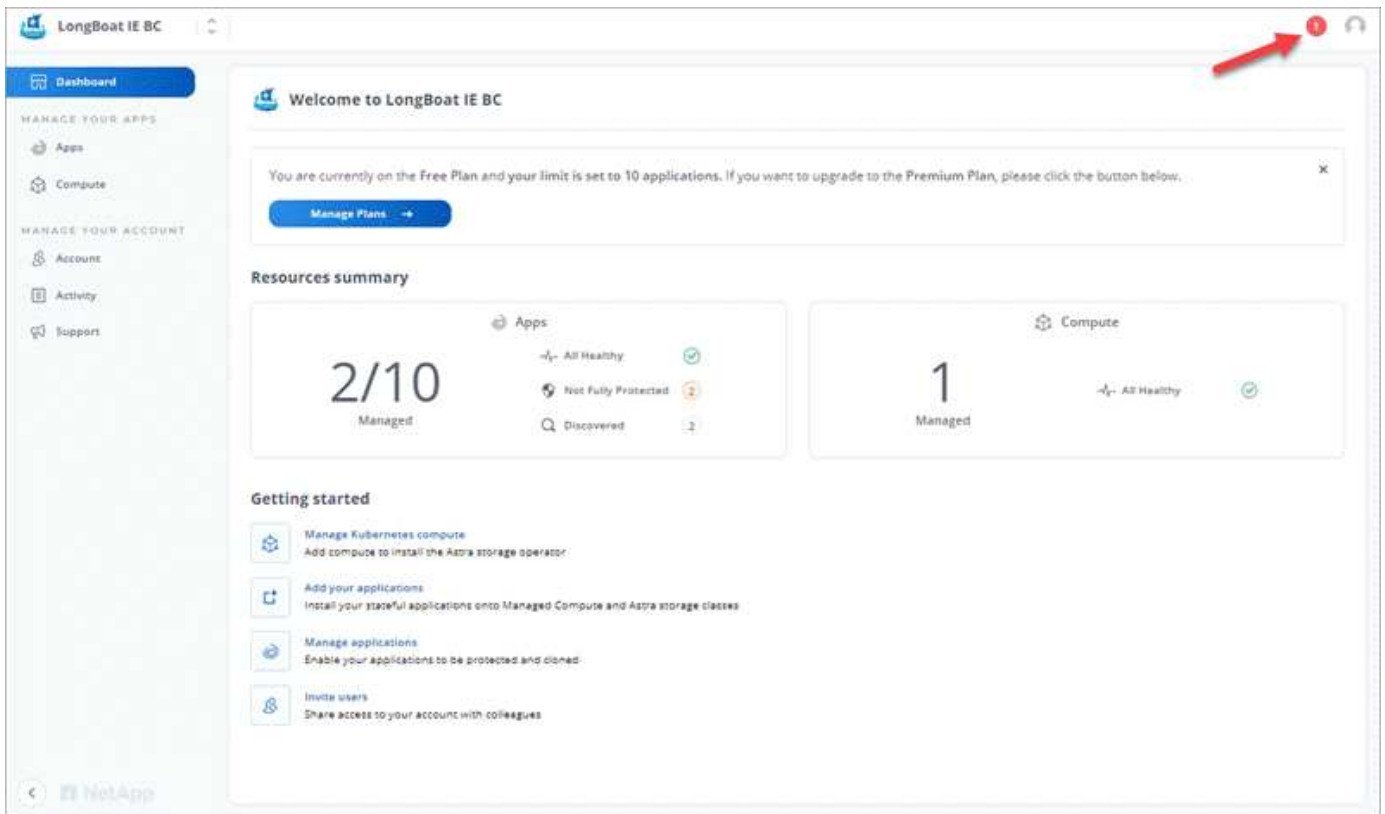
### Ergebnis

Astra Control Center entfernt den Benutzer aus dem Konto.

## 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.

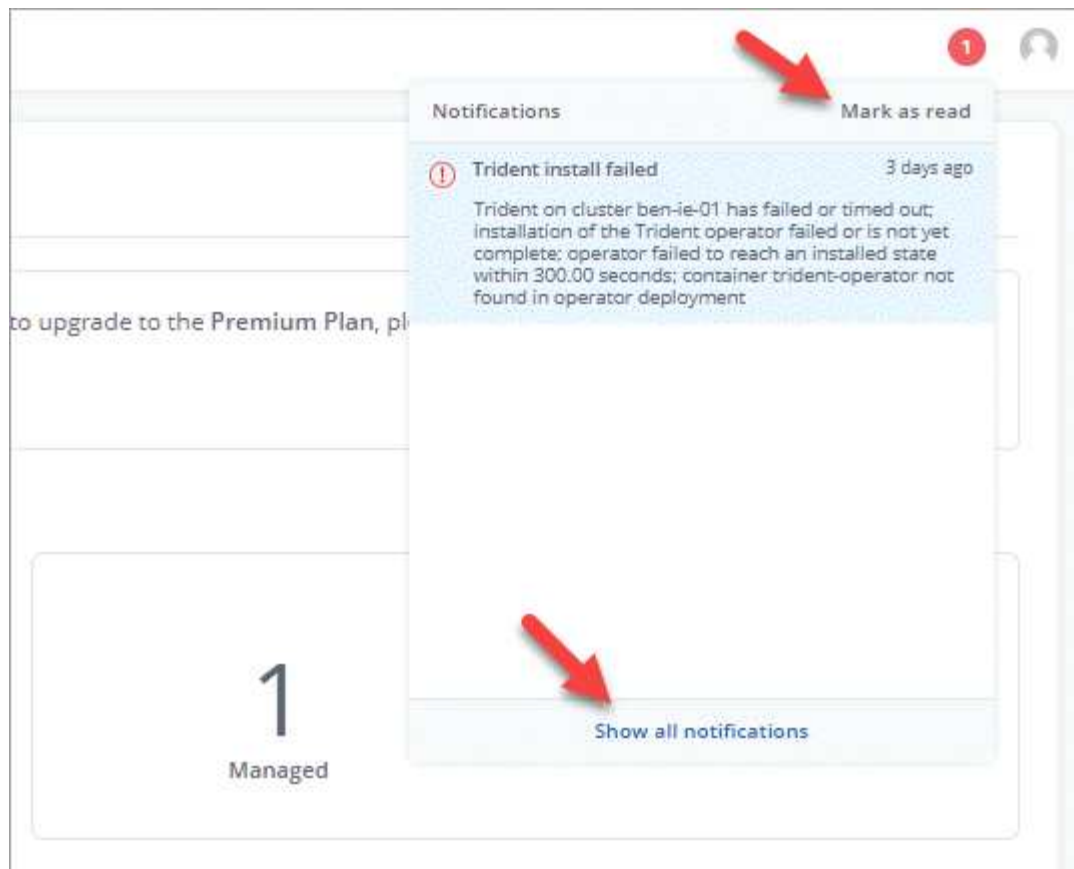
Die Anzahl der ungelesenen Benachrichtigungen ist oben rechts auf der Schnittstelle verfügbar:



Sie können diese Benachrichtigungen anzeigen und als gelesen markieren (dies kann nützlich sein, wenn Sie ungelesenen Benachrichtigungen löschen möchten, wie wir tun).

### Schritte

1. Wählen Sie oben rechts die Anzahl der ungelesenen Benachrichtigungen aus.



- 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.

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

## Anmeldeinformationen hinzufügen und entfernen

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

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

### Anmeldedaten hinzufügen

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





Wenn Sie Ihre eigenen erstellen kubeconfig Datei, Sie sollten nur ein **ein**-Kontext-Element darin definieren. Siehe "[Kubernetes-Dokumentation](#)" Weitere Informationen zum Erstellen kubeconfig Dateien:

## Anmeldedaten entfernen

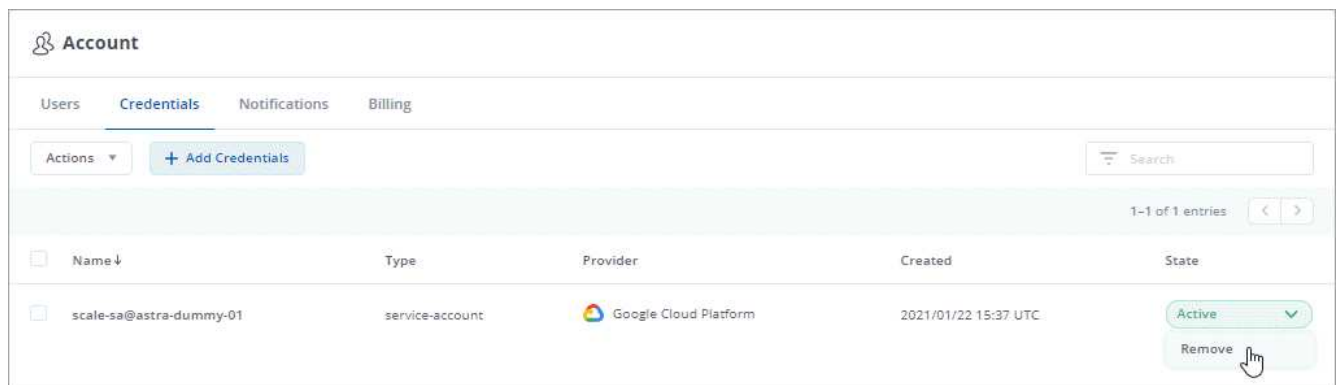
Entfernen Sie die Anmeldeinformationen jederzeit aus einem Konto. Sie sollten erst nach dem Entfernen von Anmeldeinformationen verwenden "[Verwalten aller zugehörigen Cluster wird aufgehoben](#)".



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

## Schritte

1. Wählen Sie **Konto > Anmeldeinformationen**.
2. Wählen Sie die Dropdown-Liste in der Spalte **Status** für die Anmeldeinformationen aus, die Sie entfernen möchten.
3. Wählen Sie **Entfernen**.



4. 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.

### 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 UI oder verwenden ["Die Astra Control API"](#) Um eine vorhandene Lizenz zu aktualisieren.

### Schritte

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

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

## 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 brauchen keinen Eimer, wenn Sie Ihre Anwendungskonfiguration und Ihren persistenten Storage im selben Cluster klonen.

Nutzen Sie einen der folgenden Bucket-Provider:

- NetApp ONTAP S3
- NetApp StorageGRID S3
- Allgemein S3



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

Ein Bucket kann nicht gelöscht werden, Sie können ihn jedoch bearbeiten.

Ein Bucket kann sich in einem dieser Zustände befinden:

- Ausstehend: Der Bucket ist für die Erkennung geplant.
- Verfügbar: Der Bucket ist zur Verwendung verfügbar.
- Entfernt: Auf den Bucket ist derzeit nicht zugegriffen werden können.

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

Sie können die folgenden Aufgaben zum Verwalten von Buckets ausführen:

- ["Fügen Sie einen Bucket hinzu"](#)
- [Bearbeiten eines Buckets](#)



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.

## Anmeldedaten entfernen

Entfernen Sie jederzeit S3-Anmeldeinformationen mithilfe der Astra Control API aus einem Konto.

Weitere Informationen finden Sie unter ["Verwenden Sie die Astra Control API"](#).



Der erste Satz von Anmeldeinformationen, die Sie Astra Control hinzufügen, wird immer verwendet, da Astra Control zur Authentifizierung des Backup-Buckets die Zugangsdaten verwendet. Es ist am besten, diese Anmeldeinformationen nicht zu entfernen.

## 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 Aktionen die Option **Bearbeiten**.
3. Ändern Sie alle Informationen außer dem Bucket-Typ.



Sie können den Bucket-Typ nicht ändern.

4. Wählen Sie **Aktualisieren**.

## Weitere Informationen

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

# Management des Storage-Backends

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

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

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

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

## 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 Abschnitt Storage Backend, 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)

Bei der Verbindung zu Cloud Insights sehen Sie die Volumes, die die Kubernetes-Apps verwenden, die in einem ausgewählten Storage-Back-End gespeichert sind.

## 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.

**Umeng-Aff300-05-06** Available

Storage backend status: Healthy

Capacity (Physical): 37.3% 7.93/21.28 TiB

Performance (Last 24 hrs): Throughput, MB/s

**BASIC INFORMATION**

Type: ONTAP 9.7.0 Cloud private Credentials: Updated 2021/07/28 21:44 UTC

**NETWORK**

Cluster management IP address: 10.10.10.10

**Persistent volumes**

| Name            | Persistent volume | Capacity              | App/s   | Cluster/s            | Cloud   |
|-----------------|-------------------|-----------------------|---|----------------------|---------|
| trident_pvc_... | pvc-...           | 0.04/46.57 GiB: 0.1%  | netapp-acc  | openshift-cluster010 | private |
| trident_pvc_... | pvc-...           | 0.34/23.28 GiB: 1.44% | netapp-acc  | openshift-cluster010 | private |
| trident_pvc_... | pvc-...           | 0.02/0.93 GiB: 2.33%  | netapp-acc  | openshift-cluster010 | private |
| trident_pvc_... | pvc-...           | 3.02/50.00 GiB: 6.04% | netapp-acc<br>polaris-mongodb-mongodb             | openshift-cluster010 | private |
| trident_pvc_... | pvc-...           | 0.19/8.00 GiB: 2.39%  | apps-mysql<br>mysql-mysql                         | openshift-cluster010 | private |
| trident_pvc_... | pvc-...           | 0.41/50.00 GiB: 0.81% | netapp-acc<br>polaris-influxdb2-polaris-influxdb2 | openshift-cluster010 | private |
| trident_pvc_... | pvc-...           | 2.93/50.00 GiB: 5.87% | netapp-acc<br>polaris-mongodb-mongodb             | openshift-cluster010 | private |
| trident_pvc_... | pvc-...           | 0.03/10.00 GiB: 0.26% | netapp-acc<br>polaris-consul-consul               | openshift-cluster010 | private |

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

## Unmanagement eines Storage-Backends

Sie können das Backend verwalten.

### Schritte

1. Wählen Sie in der linken Navigationsleiste **Backend** aus.
2. Wählen Sie das Storage-Back-End aus.
3. Wählen Sie im Menü Aktionen die Option **Verwaltung aufheben** aus.
4. Geben Sie „unmanage“ ein, um das Entfernen zu bestätigen.
5. Wählen Sie **Ja, Speicher-Backend entfernen**.

## Weitere Informationen

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

# Überwachung und Sicherung der Infrastruktur

Sie können mehrere optionale Einstellungen konfigurieren, um Ihre Astra Control Center-Erfahrung zu verbessern. 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 im Astra Control Center konfigurieren. Um Ihre gesamte Infrastruktur zu überwachen und Erkenntnisse zu erhalten, verwenden Sie eine Verbindung zu NetApp Cloud Insights. Um Kubernetes-Ereignisse von Systemen zu erfassen, die vom Astra Control Center überwacht werden, fügen Sie eine Fluentd-Verbindung hinzu.

## Fügen Sie einen Proxyserver 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 im Astra Control Center konfigurieren.



Astra Control Center überprüft nicht die von Ihnen eingegebenen Details für Ihren Proxy-Server. 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 **Verbinden** aus, um einen Proxyserver hinzuzufügen.



#### HTTP PROXY

Configure Astra Control to send traffic through a proxy server.

Disconnected



Connect

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.



Connected



## HTTP PROXY ?

Server: proxy.example.com:8888

Authentication: Enabled

### Proxy-Server-Einstellungen bearbeiten

Sie können die Proxy-Server-Einstellungen bearbeiten.

#### Schritte

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

### Deaktivieren Sie die Proxy-Serververbindung

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

#### Schritte

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

### Verbinden Sie sich mit Cloud Insights

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

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

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



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

## Was Sie benötigen

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



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

## Schritte

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



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

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

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

- 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.



Cloud Insights (Trial) Tutorial 0% Complete Getting Started

MONITOR & OPTIMIZE nmm95sx / Admin / API Access

API Access Tokens (4)

| Name      | Description | Token     | API Type       | Permission |
|-----------|-------------|-----------|----------------|------------|
| astra_... |             | ...zBskB1 | All Categories | Read/Write |
| astra_... |             | ...xKOel_ | All Categories | Read/Write |
| astra_... |             | ...2_A6HP | All Categories | Read Only  |
| astra_... |             | ...8BTkYY | All Categories | Read/Write |

- 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. Für die Hauptberechtigungen Lese-/Schreibzugriff auf API-Zugriffstoken wählen Sie: Assets, Datenaufnahme, Log-Ingestion, Acquisition Unit, Und Datenerfassung.



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.

EXTERNAL ?





Connected 

**HTTP PROXY** ?


Server: [proxy.example.com:8888](#) 

Authentication: Enabled




Connected 

**CLOUD INSIGHTS** ?

Tenant: [Cloud Insights](#) 

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.


Notifications Mark All as Read

 **Unable to connect to Cloud Insights** an hour ago

The Cloud Insights API token is invalid. Create a new API token in Cloud Insights and update Astra Control connection settings with the new token.





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.

 **Backends**

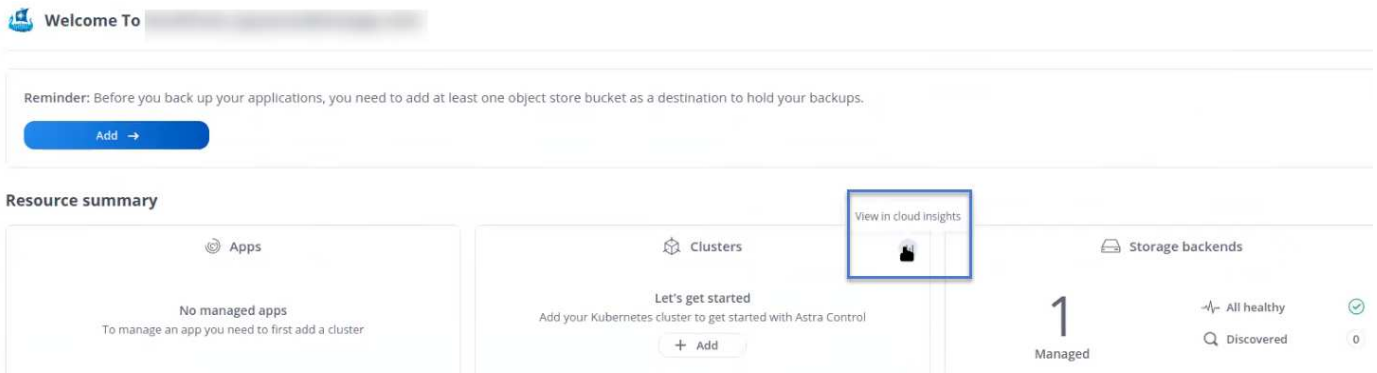
[+ Manage](#) Search ★ Managed 🔍 Discovered

1-1 of 1 entries < >

| Name | Status  | Capacity            | Throughput   | Type        | Actions   |
|------|---|---------------------|--|-------------|---|
| .06  |  | 7.67/21.28 TiB: 36% |  8.00 MB/s<br>Throughput<br>Last 24 hrs<br>● 5m ago: 8.00 MB/s<br>○ Min: 4.00 MB/s<br>● Max: 11.00 MB/s<br><a href="#">View in Cloud Insights</a>  | ONTAP 9.7.0 | Available  |

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

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



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

## Cloud Insights-Verbindung bearbeiten

Sie können die Cloud Insights-Verbindung bearbeiten.



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

### Schritte

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

## Deaktivieren Sie die Cloud Insights-Verbindung

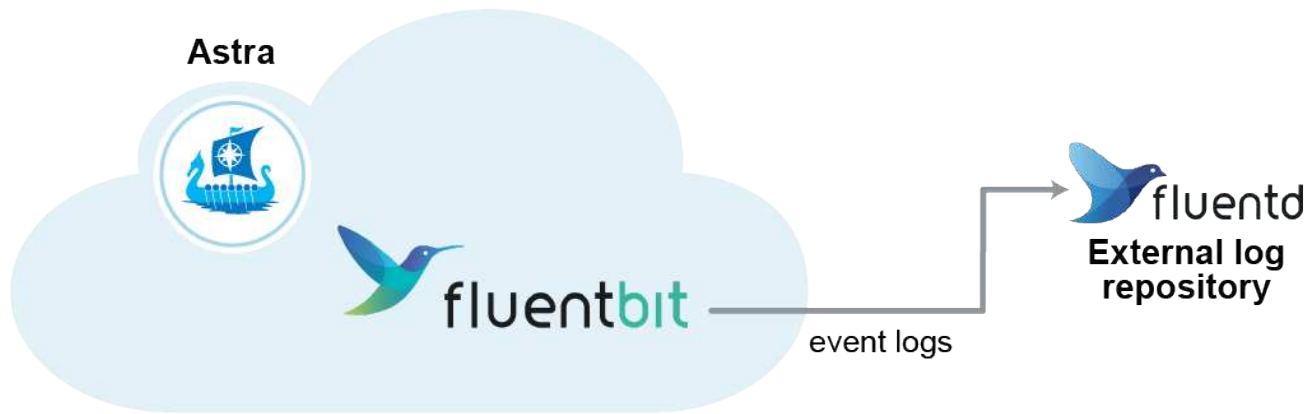
Sie können die Cloud Insights-Verbindung für einen Kubernetes Cluster deaktivieren, der von Astra Control Center gemanagt wird. Wenn Sie die Cloud Insights-Verbindung deaktivieren, werden die bereits auf Cloud Insights hochgeladenen Telemetriedaten nicht gelöscht.

### Schritte

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

## Mit Fluentd verbinden

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



Nur die Ereignisprotokolle von verwalteten Clustern werden an Fluentd weitergeleitet.

### Was Sie benötigen

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



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

### Schritte

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



#### FLUENTD

Connect Astra Control logs to Fluentd for use by your log analysis software.

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

### Ergebnis

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

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

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



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

## Bearbeiten Sie die Fluentd-Verbindung

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

### Schritte

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

## Deaktivieren Sie die Fluentd-Verbindung

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

### Schritte

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

# 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 UI oder verwenden "[Die Astra Control API](#)" Um eine vorhandene Lizenz zu aktualisieren.

### Schritte

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

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

# 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.

- 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. Aktivieren Sie das Kontrollkästchen für die Apps, die Sie nicht mehr verwalten möchten.
3. Wählen Sie im Menü **Aktion** die Option **Entverwalten**.
4. Geben Sie zur Bestätigung „nicht verwalten“ ein.
5. Bestätigen Sie, dass Sie die Verwaltung der Apps aufheben möchten, und wählen Sie dann **Ja, Anwendung verwalten** aus.

### Ergebnis

Astra Control Center beendet die Verwaltung der App.

## Aufheben des Managements eines Clusters

Entmanagement des Clusters, den Sie nicht mehr über das Astra Control Center managen möchten.

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



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

### Schritte

1. Wählen Sie in der linken Navigationsleiste **Cluster** aus.
2. Aktivieren Sie das Kontrollkästchen für den Cluster, den Sie in Astra Control Center nicht mehr verwalten möchten.
3. Wählen Sie im Menü **Aktionen** die Option **nicht verwalten**.
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 **removing** und danach wird der Cluster von der Seite **Clusters** entfernt und wird nicht mehr von 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 führen Sie diese Anweisungen aus, um die Komponenten des Astra Control Center in Ihrer Umgebung zu aktualisieren. Mit diesem Verfahren können Sie das Astra Control Center in internetverbundenen oder luftgekaperten Umgebungen aktualisieren.

### Was Sie benötigen

- "Bevor Sie mit dem Upgrade beginnen, stellen Sie sicher, dass Ihre Umgebung auch die [Mindestanforderungen für die Implementierung des Astra Control Center erfüllt](#)".
- Stellen Sie sicher, dass alle Cluster Operator in einem ordnungsgemäßen Zustand und verfügbar sind.

OpenShift-Beispiel:

```
oc get clusteroperators
```

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

OpenShift-Beispiel:

```
oc get apiservices
```

- Melden Sie sich von Ihrem Astra Control Center ab.

### Über diese Aufgabe

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

- [Laden Sie das Astra Control Center Bundle herunter](#)
- [Packen Sie das Paket aus und ändern Sie das Verzeichnis](#)
- [Fügen Sie die Bilder Ihrer lokalen Registrierung hinzu](#)
- [Installieren Sie den aktualisierten Astra Control Center-Operator](#)
- [Upgrade Astra Control Center](#)
- [Upgrade von Drittanbieter-Services](#)
- [Überprüfen Sie den Systemstatus](#)



Führen Sie den folgenden Befehl während der gesamten Dauer des Upgrades nicht aus, um zu vermeiden, dass alle Astra Control Center Pods gelöscht werden: `kubectl delete -f astra_control_center_operator_deploy.yaml`



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



Podman-Befehle können anstelle von Docker-Befehlen verwendet werden, wenn Sie den Podman von Red hat anstelle von Docker Engine verwenden.

## Laden Sie das Astra Control Center Bundle herunter

1. Laden Sie das Astra Control Center-Upgrade-Bundle herunter (astra-control-center-[version].tar.gz) Vom ["NetApp Support Website"](#).
2. (Optional) Überprüfen Sie mit dem folgenden Befehl die Signatur des Pakets:

```
openssl dgst -sha256 -verify astra-control-center[version].pub  
-signature <astra-control-center[version].sig astra-control-  
center[version].tar.gz
```

## Packen Sie das Paket aus und ändern Sie das Verzeichnis

1. Extrahieren Sie die Bilder:

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

2. Wechseln Sie in das Astra-Verzeichnis.

```
cd astra-control-center-[version]
```

## Fügen Sie die Bilder Ihrer lokalen Registrierung hinzu

1. Fügen Sie die Dateien im Astra Control Center-Bildverzeichnis Ihrer lokalen Registrierung hinzu.



Siehe ein Beispielskript für das automatische Laden von Bildern unten.

- a. Melden Sie sich bei Ihrer Docker Registrierung an:

```
docker login [your_registry_path]
```

- b. Laden Sie die Images in Docker.
- c. Markieren Sie die Bilder.
- d. Schieben Sie die Bilder in Ihre lokale Registrierung.



```

export REGISTRY=[your_registry_path]
for astraImageFile in $(ls images/*.tar)
  # Load to local cache. And store the name of the loaded image
  trimming the 'Loaded images: '
  do astraImage=$(docker load --input ${astraImageFile} | sed
's/Loaded image: //' )
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done

```

## Installieren Sie den aktualisierten Astra Control Center-Operator

1. 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, für die eine Authentifizierung erforderlich ist, ersetzen Sie die Standardzeile von imagePullSecrets: [] Mit folgenden Optionen:

```

imagePullSecrets:
- name: <name_of_secret_with_creds_to_local_registry>

```

- b. Ändern [your\_registry\_path] Für das kube-rbac-proxy Bild zum Registrierungspfad, in dem Sie die Bilder in ein geschoben haben [Vorheriger Schritt](#).
- c. Ändern [your\_registry\_path] Für das acc-operator-controller-manager Bild zum Registrierungspfad, in dem Sie die Bilder in ein geschoben haben [Vorheriger Schritt](#).

```

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
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
        - args:
            - --secure-listen-address=0.0.0.0:8443
            - --upstream=http://127.0.0.1:8080/
            - --logtostderr=true
            - --v=10
            image: [your_registry_path]/kube-rbac-proxy:v4.8.0
          name: kube-rbac-proxy
          ports:
            - containerPort: 8443
              name: https
        - args:
            - --health-probe-bind-address=:8081
            - --metrics-bind-address=127.0.0.1:8080
            - --leader-elect
          command:
            - /manager
          env:
            - name: ACCOP_LOG_LEVEL
              value: "2"
            image: [your_registry_path]/acc-operator:[version x.y.z]
          imagePullPolicy: IfNotPresent
      imagePullSecrets: []

```

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

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

Beispielantwort:

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

## Upgrade Astra Control Center

1. Bearbeiten Sie die benutzerdefinierte Astra Control Center-Ressource (CR) und ändern Sie die Astra-Version (astraVersion Innerhalb von Spec) Nummer auf die neueste:

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



Eine Änderung der Astra-Version ist die einzige Voraussetzung für ein Upgrade des Astra Control Center. Ihr Registrierungspfad muss mit dem Registrierungspfad übereinstimmen, in dem Sie die Bilder in A verschoben haben [Vorheriger Schritt](#).

2. Überprüfen Sie, ob die Pods enden und wieder verfügbar sind:

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

3. Überprüfen Sie, ob alle Systemkomponenten erfolgreich aktualisiert wurden.

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

Jeder Pod sollte einen Status von haben Running Und Age Das ist die letzte. Es kann mehrere Minuten dauern, bis die System-Pods implementiert sind.

Beispielantwort:

| NAME  | READY | STATUS  | RESTARTS |
|---|-------|---------|----------|
| AGE   |       |         |          |
| acc-helm-repo-5f75c5f564-bzqmt<br>11m             | 1/1   | Running | 0        |
| activity-6b8f7cccb9-mlrn4<br>9m2s                 | 1/1   | Running | 0        |
| api-token-authentication-6hznt<br>8m50s           | 1/1   | Running | 0        |
| api-token-authentication-qpfgb<br>8m50s           | 1/1   | Running | 0        |
| api-token-authentication-sqnb7<br>8m50s           | 1/1   | Running | 0        |
| asup-5578bbdd57-dxkbp<br>9m3s                     | 1/1   | Running | 0        |
| authentication-56bff4f95d-mspmq<br>7m31s          | 1/1   | Running | 0        |
| bucket-service-6f7968b95d-9rrrl<br>8m36s          | 1/1   | Running | 0        |
| cert-manager-5f6cf4bc4b-82khn<br>6m19s            | 1/1   | Running | 0        |
| cert-manager-cainjector-76cf976458-sdrbc<br>6m19s | 1/1   | Running | 0        |
| cert-manager-webhook-5b7896bfd8-2n45j<br>6m19s    | 1/1   | Running | 0        |
| cloud-extension-749d9f684c-8bdhq<br>9m6s          | 1/1   | Running | 0        |
| cloud-insights-service-7d58687d9-h5tzw<br>8m56s   | 1/1   | Running | 2        |
| composite-compute-968c79cb5-nv714<br>9m11s        | 1/1   | Running | 0        |
| composite-volume-7687569985-jg9gg<br>8m33s        | 1/1   | Running | 0        |
| credentials-5c9b75f4d6-nx9cz<br>8m42s             | 1/1   | Running | 0        |
| entitlement-6c96fd8b78-zt7f8<br>8m28s             | 1/1   | Running | 0        |
| features-5f7bfc9f68-gsjnl<br>8m57s                | 1/1   | Running | 0        |
| fluent-bit-ds-h88p7<br>7m22s                      | 1/1   | Running | 0        |
| fluent-bit-ds-krhnj<br>7m23s                      | 1/1   | Running | 0        |
| fluent-bit-ds-l5bjj<br>7m22s                      | 1/1   | Running | 0        |

|  |     |         |   |
|--|-----|---------|---|
| fluent-bit-ds-lrclb<br>7m23s                 | 1/1 | Running | 0 |
| fluent-bit-ds-s5t4n<br>7m23s                 | 1/1 | Running | 0 |
| fluent-bit-ds-zpr6v<br>7m22s                 | 1/1 | Running | 0 |
| graphql-server-5f5976f4bd-vbb4z<br>7m13s     | 1/1 | Running | 0 |
| identity-56f78b8f9f-8h9p9<br>8m29s           | 1/1 | Running | 0 |
| influxdb2-0<br>11m                           | 1/1 | Running | 0 |
| krakend-6f8d995b4d-5khkl<br>7m7s             | 1/1 | Running | 0 |
| license-5b5db87c97-jmxzc<br>9m               | 1/1 | Running | 0 |
| login-ui-57b57c74b8-6xtv7<br>7m10s           | 1/1 | Running | 0 |
| loki-0<br>11m                                | 1/1 | Running | 0 |
| monitoring-operator-9dbc9c76d-8znck<br>7m33s | 2/2 | Running | 0 |
| nats-0<br>11m                                | 1/1 | Running | 0 |
| nats-1<br>10m                                | 1/1 | Running | 0 |
| nats-2<br>10m                                | 1/1 | Running | 0 |
| nautilus-6b9d88bc86-h8kfb<br>8m6s            | 1/1 | Running | 0 |
| nautilus-6b9d88bc86-vn68r<br>8m35s           | 1/1 | Running | 0 |
| openapi-b87d77dd8-5dz9h<br>9m7s              | 1/1 | Running | 0 |
| polaris-consul-consul-5ljfb<br>11m           | 1/1 | Running | 0 |
| polaris-consul-consul-s5d5z<br>11m           | 1/1 | Running | 0 |
| polaris-consul-consul-server-0<br>11m        | 1/1 | Running | 0 |
| polaris-consul-consul-server-1<br>11m        | 1/1 | Running | 0 |
| polaris-consul-consul-server-2<br>11m        | 1/1 | Running | 0 |
| polaris-consul-consul-twmpq<br>11m           | 1/1 | Running | 0 |

|   |     |         |   |
|---|-----|---------|---|
| polaris-mongodb-0<br>11m                          | 2/2 | Running | 0 |
| polaris-mongodb-1<br>10m                          | 2/2 | Running | 0 |
| polaris-mongodb-2<br>10m                          | 2/2 | Running | 0 |
| polaris-ui-84dc87847f-zrg8w<br>7m12s              | 1/1 | Running | 0 |
| polaris-vault-0<br>11m                            | 1/1 | Running | 0 |
| polaris-vault-1<br>11m                            | 1/1 | Running | 0 |
| polaris-vault-2<br>11m                            | 1/1 | Running | 0 |
| public-metrics-657698b66f-67pgt<br>8m47s          | 1/1 | Running | 0 |
| storage-backend-metrics-6848b9fd87-w7x8r<br>8m39s | 1/1 | Running | 0 |
| storage-provider-5ff5868cd5-r9hj7<br>8m45s        | 1/1 | Running | 0 |
| telegraf-ds-dw4hg<br>7m23s                        | 1/1 | Running | 0 |
| telegraf-ds-k92gn<br>7m23s                        | 1/1 | Running | 0 |
| telegraf-ds-mmxjl<br>7m23s                        | 1/1 | Running | 0 |
| telegraf-ds-nhs8s<br>7m23s                        | 1/1 | Running | 0 |
| telegraf-ds-rj7lw<br>7m23s                        | 1/1 | Running | 0 |
| telegraf-ds-tqrkb<br>7m23s                        | 1/1 | Running | 0 |
| telegraf-rs-9mwgj<br>7m23s                        | 1/1 | Running | 0 |
| telemetry-service-56c49d689b-ffrzx<br>8m42s       | 1/1 | Running | 0 |
| tenancy-767c77fb9d-g9ctv<br>8m52s                 | 1/1 | Running | 0 |
| traefik-5857d87f85-7pmx8<br>6m49s                 | 1/1 | Running | 0 |
| traefik-5857d87f85-cpxgv<br>5m34s                 | 1/1 | Running | 0 |
| traefik-5857d87f85-lvmlb<br>4m33s                 | 1/1 | Running | 0 |
| traefik-5857d87f85-t2x1k<br>4m33s                 | 1/1 | Running | 0 |

|                                   |     |         |   |
|-----------------------------------|-----|---------|---|
| traefik-5857d87f85-v9wpf          | 1/1 | Running | 0 |
| 7m3s                              |     |         |   |
| trident-svc-595f84dd78-zb8l6      | 1/1 | Running | 0 |
| 8m54s                             |     |         |   |
| vault-controller-86c94fbf4f-krttq | 1/1 | Running | 0 |
| 9m24s                             |     |         |   |

4. Vergewissern Sie sich, dass die Statusbedingungen des Astra darauf hindeuten, dass das Upgrade abgeschlossen und bereit ist:

```
kubectl get -o yaml -n [netapp-acc or custom namespace]
astracontrolcenters.astra.netapp.io astra
```

Antwort:

```
conditions:
  - lastTransitionTime: "2021-10-25T18:49:26Z"
    message: Astra is deployed
    reason: Complete
    status: "True"
    type: Ready
  - lastTransitionTime: "2021-10-25T18:49:26Z"
    message: Upgrading succeeded.
    reason: Complete
    status: "False"
    type: Upgrading
```

## Upgrade von Drittanbieter-Services

Die Drittanbieter-Services Traefik und Cert-Manager werden während früherer Aktualisierungsschritte nicht aktualisiert. Sie können sie optional mithilfe der hier beschriebenen Vorgehensweise aktualisieren oder vorhandene Servicestversionen beibehalten, wenn es vom System benötigt wird. Im Folgenden finden Sie die empfohlene Upgrade-Sequenz für Traefik und Certs-Manager:

1. [um Traefik und Cert-Manager zu aktualisieren](#)
2. [Traefik-Dienst mit ACC-Helm-repo aktualisieren](#)
3. [Aktualisieren Sie den Cert-Manager-Service](#)

## Richten Sie ACC-Helm-repo ein, um Traefik und Cert-Manager zu aktualisieren

1. Finden Sie die enterprise-helm-repo Die in Ihren lokalen Docker Cache geladen sind:

```
docker images enterprise-helm-repo
```

Antwort:

| REPOSITORY           | TAG       | IMAGE ID     | CREATED      | SIZE  |
|----------------------|-----------|--------------|--------------|-------|
| enterprise-helm-repo | 21.10.218 | 7a182d6b30f3 | 20 hours ago | 464MB |

2. Starten eines Containers mit dem Tag aus dem vorherigen Schritt:

```
docker run -dp 8082:8080 enterprise-helm-repo:21.10.218
```

Antwort:

```
940436e67fa86d2c4559ac4987b96bb35588313c2c9ddc9cec195651963f08d8
```

3. Fügen Sie den Helm repo zu Ihren lokalen Host-Repositorys hinzu:

```
helm repo add acc-helm-repo http://localhost:8082/
```

Antwort:

```
"acc-helm-repo" has been added to your repositories
```

4. Speichern Sie das folgende Python-Skript als Datei, z. B. `set_previous_values.py`:



Dieses Python-Skript erstellt zwei Dateien, die in späteren Aktualisierungsschritten verwendet werden, um Steuerwerte beizubehalten.



```
#!/usr/bin/env python3
import json
import os

NAMESPACE = "netapp-acc"

os.system(f"helm get values traefik -n {NAMESPACE} -o json >
traefik_values.json")
os.system(f"helm get values cert-manager -n {NAMESPACE} -o json >
cert_manager_values.json")

# reformat traefik values
f = open("traefik_values.json", "r")
traefik_values = {'traefik': json.load(f)}
f.close()

with open('traefik_values.json', 'w') as output_file:
    json.dump(traefik_values, output_file)

# reformat cert-manager values
f = open("cert_manager_values.json", "r")
cm_values = {'cert-manager': json.load(f)}
f.close()

cm_values['global'] = cm_values['cert-manager']['global']
del cm_values['cert-manager']['global']

with open('cert_manager_values.json', 'w') as output_file:
    json.dump(cm_values, output_file)

print('Done')
```

5. Führen Sie das Skript aus:

```
python3.7 ./set_previous_values.py
```

## Traefik-Dienst mit ACC-Helm-repo aktualisieren



Dies muss bereits geschehen [um Traefik und Cert-Manager zu aktualisieren](#), ACC-Helm-Repo [einrichten](#) Vor dem Abschluss des folgenden Verfahrens.

1. Laden Sie das Traefik-Paket mit einem sicheren Dateiübertragungstool wie GNU wget herunter:

```
wget http://localhost:8082/traefik-0.2.0.tgz
```

2. Extrahieren Sie die Bilder:

```
tar -vxzf traefik-0.2.0.tgz
```

3. Anwenden der Traefik-CRDs:

```
kubectl apply -f ./traefik/charts/traefik/crds/
```

4. Suchen Sie die Helmchartenversion, die Sie mit Ihrem aktualisierten Traefik verwenden können:

```
helm search repo acc-helm-repo/traefik
```

Antwort:

| NAME                                 | CHART VERSION | APP VERSION |
|--------------------------------------|---------------|-------------|
| DESCRIPTION                          |               |             |
| acc-helm-repo/traefik                | 0.2.0         | 2.5.3       |
| chart for Traefik Ingress controller |               | Helm        |
| acc-helm-repo/traefik-ingressroutes  | 0.2.0         | 2.5.3       |
| chart for Kubernetes                 |               | A Helm      |

5. Überprüfen Sie die Datei „traefik\_values.json“ für das Upgrade:

- Öffnen Sie die Datei traefik\_values.json.
- Prüfen Sie, ob ein Wert für das vorhandene `imagePullSecret` Feld. Wenn er leer ist, entfernen Sie den folgenden Text aus der Datei:

```
"imagePullSecrets": [{"name": ""}],
```

- Stellen Sie sicher, dass das Traefik-Bild an den richtigen Ort geleitet wird und den richtigen Namen hat:

```
image: [your_registry_path]/traefik
```

6. Aktualisieren Sie Ihre Traefik-Konfiguration:

```
helm upgrade --version 0.2.0 --namespace netapp-acc -f  
traefik_values.json traefik acc-helm-repo/traefik
```

Antwort:

```
Release "traefik" has been upgraded. Happy Helming!  
NAME: traefik  
LAST DEPLOYED: Mon Oct 25 22:53:19 2021  
NAMESPACE: netapp-acc  
STATUS: deployed  
REVISION: 2  
TEST SUITE: None
```

## Aktualisieren Sie den Cert-Manager-Service



Sie müssen bereits den abgeschlossen haben [Traefik-Update](#) Und [um Traefik und Cert-Manager zu aktualisieren,ACC-Helm-repo in Helm hinzugefügt](#) Vor dem Abschluss des folgenden Verfahrens.

1. Suchen Sie die Version des Steuerrads, die Sie mit Ihrem aktualisierten Cert-Manager verwenden möchten:

```
helm search repo acc-helm-repo/cert-manager
```

Antwort:

```
NAME CHART VERSION APP VERSION DESCRIPTION  
acc-helm-repo/cert-manager 0.3.0 v1.5.4 A Helm chart for cert-manager  
acc-helm-repo/cert-manager-certificates 0.1.0 1.16.0 A Helm chart for  
Kubernetes
```

2. Überprüfen Sie die Datei `cert_Manager_values.json` für ein Upgrade:
  - a. Öffnen Sie die Datei `cert_Manager_values.json`.
  - b. Prüfen Sie, ob ein Wert für das vorhanden ist `imagePullSecret` Feld. Wenn er leer ist, entfernen Sie den folgenden Text aus der Datei:

```
"imagePullSecrets": [{"name": ""}],
```

- c. Stellen Sie sicher, dass die drei Bilder des Zertifikaten-Managers an den richtigen Ort geleitet werden und die richtigen Namen haben.
3. Aktualisieren Sie Ihre Cert-Manager-Konfiguration:

```
helm upgrade --version 0.3.0 --namespace netapp-acc -f  
cert_manager_values.json cert-manager acc-helm-repo/cert-manager
```

Antwort:

```
Release "cert-manager" has been upgraded. Happy Helming!  
NAME: cert-manager  
LAST DEPLOYED: Tue Nov 23 11:20:05 2021  
NAMESPACE: netapp-acc  
STATUS: deployed  
REVISION: 2  
TEST SUITE: None
```

## Überprüfen Sie den Systemstatus

1. Melden Sie sich beim Astra Control Center an.
2. Vergewissern Sie sich, dass alle gemanagten Cluster und Applikationen weiterhin vorhanden und geschützt sind.

## Deinstallieren Sie Astra Control Center

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

### Was Sie benötigen

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

### Schritte

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

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

Ergebnis:

```
astracenter.astra.netapp.io "astra" deleted
```

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

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

Ergebnis:

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

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

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

Ergebnis:

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

## Weitere Informationen

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

## Copyright-Informationen

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

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

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

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

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

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

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

## Markeninformationen

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