



# **Management und Sicherung von Applikationen**

## **Astra Control Service**

NetApp  
March 07, 2023

# Inhaltsverzeichnis

- Management und Sicherung von Applikationen ..... 1
  - Starten Sie das Anwendungsmanagement ..... 1
  - Sichern von Applikationen durch Snapshots und Backups ..... 6
  - Wiederherstellung von Applikationen ..... 10
  - Klonen und Migrieren von Applikationen ..... 12
  - Anwendungsausführungshaken verwalten ..... 14

# Management und Sicherung von Applikationen

## Starten Sie das Anwendungsmanagement

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

## Anforderungen für das Applikationsmanagement

Astra Control verfügt über folgende Anforderungen an das Applikationsmanagement:

- **Lizenzierung:** Um mehr als 10 Namespaces zu verwalten, benötigen Sie ein Astra Control Center-Abonnement.
- **Namespaces:** Apps können mit Astra Control innerhalb eines oder mehrerer spezifizierter Namespaces auf einem einzigen Cluster definiert werden. Eine App kann Ressourcen enthalten, die mehrere Namespaces innerhalb desselben Clusters umfassen. Astra Control unterstützt nicht die Möglichkeit, Applikationen über mehrere Cluster hinweg zu definieren.
- **Speicherklasse:** Wenn Sie eine App installieren, die eine Speicherklasse explizit festgelegt hat und Sie die App klonen müssen, muss das Zielcluster für den Klonvorgang die ursprünglich angegebene Speicherklasse haben. Das Klonen einer Applikation mit einer explizit festgelegten Storage-Klasse auf ein Cluster ohne dieselbe Storage-Klasse schlägt fehl.
- **Kubernetes-Ressourcen:** Applikationen, die nicht 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
CronJob	CustomResourceDefinition	CustomResource
DaemonSet	DeploymentConfig	HorizontalPodAutoscaler
Ingress	MutatingWebhook	NetworkPolicy
PersistentVolumeClaim	Pod	PodDisruptionBudget
PodTemplate	ReplicaSet	Role
RoleBinding	Route	Secret
Service	ServiceAccount	StatefulSet
ValidatingWebhook		

## Unterstützte Installationsmethoden für Anwendungen

Astra Control unterstützt folgende Installationsmethoden für Anwendungen:

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

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

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

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

- ["Apache K8ssandra"](#)



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

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

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

## Installation von Apps auf dem Cluster

Nachdem Sie ["Hat den Cluster hinzugefügt"](#) Bei Astra Control können Sie Apps installieren oder vorhandene Apps auf dem Cluster managen. Jede Anwendung, die einem oder mehreren Namespaces zugeordnet ist, kann verwaltet werden.

Astra Control verwaltet statusorientierte Applikationen nur dann, wenn sich der Storage auf einer Storage-Klasse befindet, die von Astra Control unterstützt wird. Astra Control Service unterstützt alle Storage-Klassen, die von Astra Trident oder einem generischen CSI-Treiber unterstützt werden.

- ["Erfahren Sie mehr über Speicherklassen für GKE-Cluster"](#)
- ["Erfahren Sie mehr über Speicherklassen für AKS-Cluster"](#)
- ["Erfahren Sie mehr über Storage-Klassen für AWS Cluster"](#)

## Definieren von Apps

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

Datensicherungsvorgänge benötigen.

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



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

### Was Sie benötigen

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



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

### Über diese Aufgabe

- Bevor Sie beginnen, sollten Sie auch verstehen ["Verwalten von Standard- und Systemnames"](#).
- Wenn Sie in Astra Control mehrere Namespaces mit Ihren Apps verwenden möchten, sollten Sie dies in Betracht ziehen ["Ändern von Benutzerrollen mit Namespace-Einschränkungen"](#) Vor dem Definieren von Apps.
- Anweisungen zum Verwalten von Apps mit der Astra Control API finden Sie im ["Astra Automation und API-Informationen"](#).

### Optionen für Applikationsmanagement

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

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

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

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



Stellen Sie bei der Definition von Applikationen sicher, dass Sie keine Kubernetes-Ressource in mehrere Applikationen mit Sicherheitsrichtlinien aufnehmen. Überlappende Sicherheitsrichtlinien für Kubernetes-Ressourcen können zu Datenkonflikten führen.



Die Durchführung einer in-Place-Wiederherstellung in einer Anwendung, in der Ressourcen mit einer anderen Anwendung geteilt werden, kann unbeabsichtigte Ergebnisse haben. Alle Ressourcen, die von den Applikationen gemeinsam genutzt werden, werden ersetzt, wenn eine in-Place-Wiederherstellung für eine der Applikationen durchgeführt wird.

**Erfahren Sie mehr über das Hinzufügen von Ressourcen im Cluster-Umfang zu Ihren Applikationsnamensräumen.**

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

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

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

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

**Schritte**

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



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

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



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

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



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

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

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



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



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

Um die Ressourcen anzuzeigen, die dieser App hinzugefügt wurden, wählen Sie die Registerkarte **Ressourcen** aus. Wählen Sie in der Spalte „Ressource“ die Nummer nach dem Ressourcennamen aus, oder geben Sie den Ressourcennamen in „Suche“ ein, um die zusätzlichen Ressourcen anzuzeigen, die im Cluster-Umfang enthalten sind.

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

Sie können alle Kubernetes-Ressourcen im Namespace zum Astra Control Management hinzufügen, indem Sie die Ressourcen dieses Namespace als Applikation definieren. Diese Methode ist vorzuziehen, Apps einzeln zu definieren, wenn Sie ["Alle Ressourcen in einem bestimmten Namespace managen und schützen sollen"](#) Auf ähnliche Weise und in gemeinsamen Abständen.

## Schritte

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



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



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

Show system namespaces

["Weitere Informationen"](#).

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

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

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

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

Show system namespaces



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

## 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.

### Snapshots und Backups

A *Snapshot* ist eine zeitpunktgenaue Kopie einer Applikation, die auf demselben bereitgestellten Volume wie die Applikation gespeichert ist. In der Regel sind sie schnell. Lokale Snapshots werden verwendet, um die Applikation zu einem früheren Zeitpunkt wiederherzustellen.

Ein *Backup* wird im Objekt-Storage in der Cloud gespeichert. Das Backup kann im Vergleich zu den lokalen Snapshots langsamer erstellt werden. Allerdings ist der Zugriff über Regionen in der Cloud hinweg möglich, um



Applikationsmigrationen zu ermöglichen. Sie können auch eine längere Aufbewahrungsdauer für Backups wählen.



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. Falls ein Ausfall des Clusters und der persistente Storage beschädigt werden, muss ein Backup wiederhergestellt werden. Ein Snapshot würde es Ihnen nicht ermöglichen, eine Wiederherstellung durchzuführen.



Wenn Sie einen Snapshot oder eine Sicherung durchführen, aber der Vorgang mit dem Fehler „die Ressource wurde nicht wegen eines internen Serverproblems erstellt“ fehlschlägt, überprüfen Sie, ob im verwendeten Speicher-Backend die richtigen Treiber installiert sind. Einige Storage-Back-Ends benötigen Container-CSI-Treiber (Storage Interface), während andere einen externen Snapshot-Controller benötigen.

Sie können die folgenden Aufgaben zum Schutz Ihrer Applikationsdaten ausführen:

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

## Konfigurieren einer Sicherungsrichtlinie

Eine Sicherungsrichtlinie sichert eine Applikation, indem Snapshots, Backups oder beides nach einem definierten Zeitplan erstellt werden. Sie können Snapshots und Backups stündlich, täglich, wöchentlich und monatlich erstellen. Außerdem können Sie die Anzahl der beizubehaltenden Kopien festlegen. Wenn Sie Backups oder Snapshots öfter als einmal pro Stunde benötigen, können Sie dies tun "[Erstellen Sie mithilfe der Astra Control REST API Snapshots und Backups](#)".

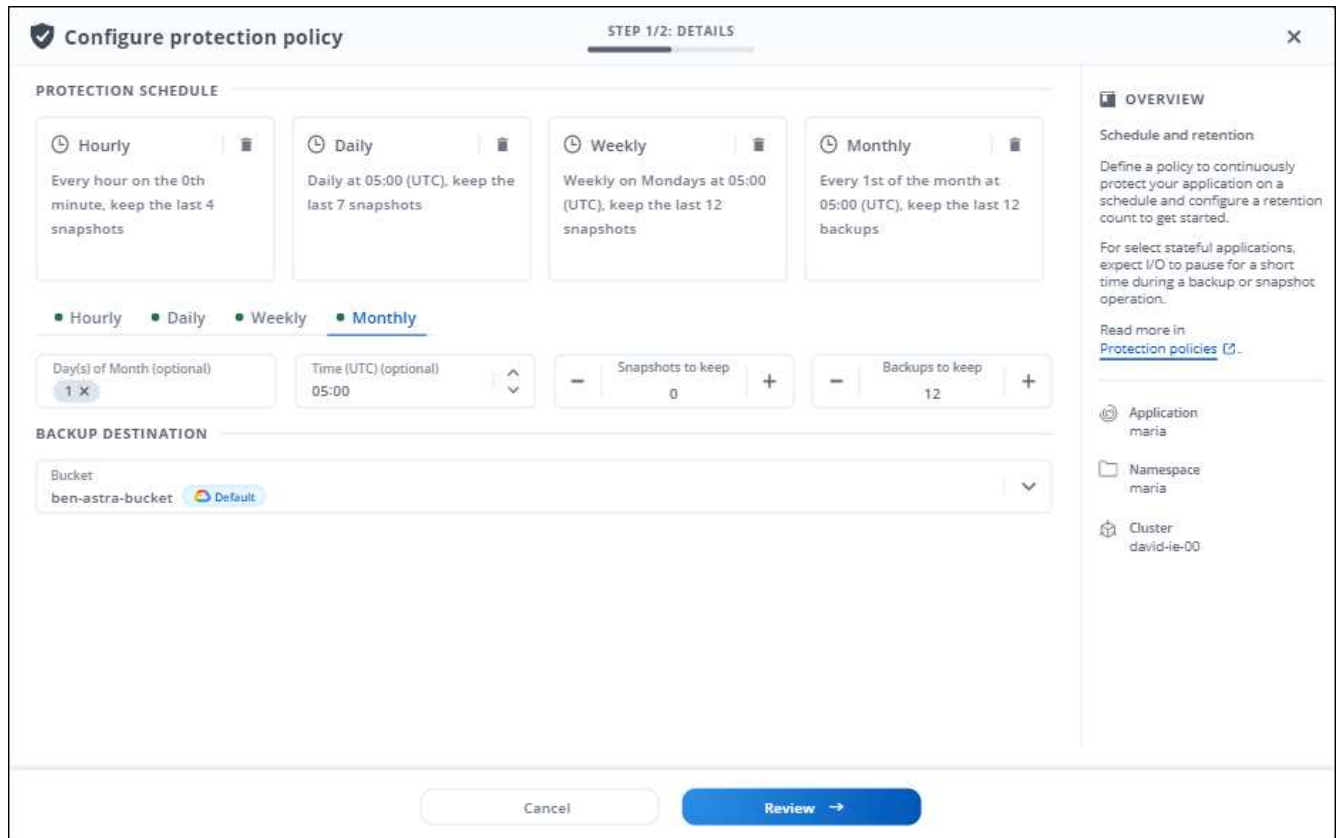
### Schritte

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

Sie können die stündlichen, täglichen, wöchentlichen und monatlichen Zeitpläne gleichzeitig festlegen. Ein Zeitplan wird nicht aktiv umschalten, bis Sie ein Aufbewahrungsniveau für Schnappschüsse und Backups festlegen.

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

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



5. Wählen Sie **Bewertung**.

6. Wählen Sie **Schutzrichtlinie Festlegen**.

### Ergebnis

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

## Erstellen Sie einen Snapshot

Sie können jederzeit einen On-Demand-Snapshot erstellen.

### Schritte

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

### Ergebnis

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

## Erstellen Sie ein Backup

Sie können eine App auch jederzeit sichern.

### Schritte

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

### Ergebnis

Astra Control erstellt ein Backup der App.



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

## 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 verwalteten App aus.
2. Wählen Sie **Datenschutz**.

Die Snapshots werden standardmäßig angezeigt.

3. Wählen Sie **Backups** aus, um auf die Liste der Backups zu verweisen.

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

### Ergebnis

Astra Control löscht den Snapshot.

## Abbrechen von Backups

Sie können ein gerade einlaufenden Backup abbrechen.



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

### Schritte

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

## Backups löschen

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



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

### Schritte

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

### Ergebnis

Astra Control löscht das Backup.

## Wiederherstellung von Applikationen

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



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



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

## Über diese Aufgabe

- **Schützen Sie Ihre Apps zuerst:** Es wird dringend empfohlen, einen Schnappschuss von Ihrer Anwendung zu machen oder zu sichern, bevor Sie sie wiederherstellen. Dadurch können Sie den Snapshot oder die Datensicherung klonen, wenn die Wiederherstellung nicht erfolgreich war.
- **Zielspeicherklasse** prüfen: Wenn Sie auf einem anderen Cluster wiederherstellen, stellen Sie sicher, dass die Speicherklasse des Zielclusters denselben persistenten Zugriffsmodus (z. B. ReadWriteManche) verwendet, wie die Speicherklasse auf dem Quellcluster. Der Wiederherstellungsvorgang schlägt fehl, wenn der Zugriffsmodus des Ziel-persistenten Volumens anders ist.

## Schritte

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



Die Durchführung einer in-Place-Wiederherstellung in einer Anwendung, in der Ressourcen mit einer anderen Anwendung geteilt werden, kann unbeabsichtigte Ergebnisse haben. Alle Ressourcen, die von den Applikationen gemeinsam genutzt werden, werden ersetzt, wenn eine in-Place-Wiederherstellung für eine der Applikationen durchgeführt wird.

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



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

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



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

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

## Ergebnis

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



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

## Klonen und Migrieren von Applikationen

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

Das Klonen kann sich leisten, wenn Sie Applikationen und Storage von einem Kubernetes Cluster zu einem anderen verschieben müssen. So möchten Sie beispielsweise Workloads über eine CI/CD-Pipeline und über Kubernetes-Namespaces verschieben.



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

### Was Sie benötigen

- Um Apps einem anderen Cluster zu klonen, müssen Sie sicherstellen, dass Sie einen Standard-Bucket für die Cloud-Instanz zugewiesen haben, die das Quell-Cluster enthält. Wenn die Quell-Cloud-Instanz keinen Standard-Bucket-Satz hat, schlägt der Cluster-übergreifende Klonvorgang fehl.
- Während Klonvorgängen müssen Applikationen, die eine Ressource oder Webhooks der ProgresClass benötigen, nicht über die Ressourcen verfügen, die bereits auf dem Ziel-Cluster definiert sind.

### Einschränkungen beim Klonen

- **Explicit Storage Classes:** Wenn Sie eine App mit einer explizit eingestellten Speicherklasse bereitstellen und die App klonen müssen, muss der Zielcluster über die ursprünglich angegebene Speicherklasse

verfügen. Das Klonen einer Applikation mit einer explizit festgelegten Storage-Klasse auf ein Cluster ohne dieselbe Storage-Klasse schlägt fehl.

- **Klone und Benutzerbeschränkungen:** Jeder Mitgliedsbenutzer mit Namespace-Beschränkungen durch Namespace-Name/ID oder durch Namespace-Labels kann eine Anwendung in einem neuen Namespace im selben Cluster oder einem anderen Cluster im Konto ihres Unternehmens klonen oder wiederherstellen. Derselbe Benutzer kann jedoch nicht auf die geklonte oder wiederhergestellte Anwendung im neuen Namespace zugreifen. Nachdem ein neuer Namespace durch einen Klon- oder Wiederherstellungsvorgang erstellt wurde, kann der Account-Administrator/-Eigentümer das Mitglied-Benutzerkonto bearbeiten und Rolleneinschränkungen für den betroffenen Benutzer aktualisieren, um dem neuen Namespace Zugriff zu gewähren.
- **Klone verwenden Standardcontainer:**
  - Während eines Applikations-Backups oder Applikations-Restores können Sie einen Bucket angeben, der verwendet werden soll. Sie müssen einen Standard-Bucket angeben, wenn Sie über die Cluster hinweg klonen, aber die Angabe eines Buckets ist optional, wenn Sie innerhalb desselben Clusters klonen.
  - Wenn Sie über Cluster hinweg klonen, muss die Cloud-Instanz, die das Quell-Cluster des Klonvorgangs enthält, einen Standard-Bucket-Satz aufweisen.
  - Es besteht keine Möglichkeit, die Buckets für einen Klon zu ändern. Wenn Sie die Kontrolle darüber haben möchten, welcher Bucket verwendet wird, können Sie entweder ["Ändern Sie den Bucket-Standard"](#) Oder machen Sie ein ["Backup"](#) Gefolgt von A ["Wiederherstellen"](#) Separat.
- **Mit Jenkins CI:** Wenn Sie eine vom Betreiber implementierte Instanz von Jenkins CI klonen, müssen Sie die persistenten Daten manuell wiederherstellen. Dies ist eine Einschränkung des Bereitstellungsmodells der Applikation.

## Schritte

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



Astra Control erstellt im Rahmen des Klonvorgangs neue Ziel-Namespace. Die angegebenen Ziel-Namespace dürfen nicht bereits im Ziel-Cluster vorhanden sein.

- Wählen Sie **Weiter**.
- Wählen Sie aus, ob Sie den Klon aus einem vorhandenen Snapshot oder einem vorhandenen Backup erstellen möchten. Wenn Sie diese Option nicht wählen, erstellt Astra Control den Klon aus dem aktuellen Status der App.
  - Wenn Sie aus einem vorhandenen Snapshot oder Backup klonen möchten, wählen Sie den Snapshot oder das Backup aus, den Sie verwenden möchten.



5. Wählen Sie **Weiter**.

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

## Ergebnis

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

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

# Anwendungsausführungshaken verwalten

Ein Execution Hook ist eine benutzerdefinierte Aktion, die Sie so konfigurieren können, dass sie zusammen mit einem Datenschutzvorgang einer verwalteten App ausgeführt wird. Wenn Sie beispielsweise über eine Datenbank-App verfügen, können Sie mit einem Execution-Hook alle Datenbanktransaktionen vor einem Snapshot anhalten und die Transaktionen nach Abschluss des Snapshots wieder aufnehmen. Dies gewährleistet applikationskonsistente Snapshots.

## Arten von Ausführungshaken

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

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

## Filter für Testausführungshaken

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

Jeder Filter, den Sie einem Execution Hook hinzufügen, verwendet einen regulären Ausdruck, um Container in Ihrem Cluster zu entsprechen. Wenn ein Haken einem Container entspricht, führt der Haken sein zugehöriges Skript auf diesem Container aus.



Reguläre Ausdrücke für Filter verwenden die Syntax des regulären Ausdrucks 2 (RE2), die das Erstellen eines Filters nicht unterstützt, der Container aus der Liste der Übereinstimmungen ausschließt.



Informationen zur Syntax, die Astra Control für regelmäßige Ausdrücke in Hook-Filter unterstützt, finden Sie unter "[Syntaxunterstützung für regulären Ausdruck 2 \(RE2\)](#)".

## Wichtige Hinweise zu benutzerdefinierten Testausführungshaken

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

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



Da die Testsuitehingel die Funktionalität der Anwendung, für die sie ausgeführt werden, oft reduzieren oder vollständig deaktivieren, sollten Sie immer versuchen, die Zeit zu minimieren, die Ihre benutzerdefinierten Testausführungshaken für die Ausführung benötigt. Wenn Sie eine Backup- oder Snapshot-Operation mit zugeordneten Testsuiten starten, diese aber dann abbrechen, können die Haken trotzdem ausgeführt werden, wenn der Backup- oder Snapshot-Vorgang bereits gestartet wurde. Das bedeutet, dass die in einem Testsuite nach dem Backup verwendete Logik nicht davon ausgehen kann, dass das Backup abgeschlossen wurde.

### Ausführungsreihenfolge

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

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

Nachbearbeitung erstellen und ausführen, aber die Reihenfolge der Ausführung dieser Haken nach der Operation ist weder garantiert noch konfigurierbar.

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

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

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



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

### Bestimmen Sie, ob ein Haken läuft

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

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

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



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

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

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

## Beispiele für Testausführungshaken

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

## Vorhandene Testsuiten anzeigen

Sie können vorhandene benutzerdefinierte Testsuiten für eine App anzeigen.

### Schritte

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

In der Ergebnisliste können Sie alle aktivierten oder deaktivierten Testausführungshaken anzeigen. Sie sehen den Status eines Hakens, die Anzahl der passenden Container, die Erstellungszeit und den Ablauf

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

## Vorhandene Skripte anzeigen

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

### Schritte

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

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

## Fügen Sie ein Skript hinzu

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

### Schritte

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

### Ergebnis

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

## Ein Skript löschen

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

### Schritte

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



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

## Erstellen Sie einen benutzerdefinierten Testsuite-Haken

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



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

### Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie **Hinzufügen**.
4. Im Bereich **Klettdetails**:
  - a. Bestimmen Sie, wann der Haken ausgeführt werden soll, indem Sie im Dropdown-Menü \* Operation\* einen Operationstyp auswählen.
  - b. Geben Sie einen eindeutigen Namen für den Haken ein.
  - c. (Optional) Geben Sie alle Argumente ein, um während der Ausführung an den Haken weiterzuleiten. Drücken Sie nach jedem eingegebenen Argument die Eingabetaste, um jedes Argument aufzuzeichnen.
5. (Optional) im Bereich **Hook Filter Details** können Sie Filter hinzufügen, um zu steuern, auf welchen Behältern der Execution Hook läuft:
  - a. Wählen Sie **Filter hinzufügen**.
  - b. Wählen Sie in der Spalte **Hook Filtertyp** ein Attribut aus, nach dem Sie im Dropdown-Menü filtern möchten.
  - c. Geben Sie in der Spalte **Regex** einen regulären Ausdruck ein, der als Filter verwendet werden soll. Astra Control verwendet den "[Regex-Syntax für regulären Ausdruck 2 \(RE2\)](#)".



Wenn Sie den genauen Namen eines Attributs (z. B. einen Pod-Namen) ohne anderen Text im Feld „regulärer Ausdruck“ filtern, wird ein Teilstring-Match durchgeführt. Verwenden Sie zum Abgleich eines genauen Namens und nur des Namens die exakte Syntax für die Übereinstimmung der Zeichenfolge (z. B. `^exact_podname$`).

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



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

6. Wählen Sie anschließend **Weiter** aus.

7. Führen Sie im Bereich **Script** einen der folgenden Schritte aus:

- Fügen Sie ein neues Skript hinzu.
  - i. Wählen Sie **Hinzufügen**.
  - ii. Führen Sie einen der folgenden Schritte aus:
    - Laden Sie ein benutzerdefiniertes Skript hoch.
      - I. Wählen Sie die Option **Datei hochladen**.
      - II. Navigieren Sie zu einer Datei, und laden Sie sie hoch.
      - III. Geben Sie dem Skript einen eindeutigen Namen.
      - IV. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.
      - V. Wählen Sie **Skript speichern**.
    - Fügen Sie in ein benutzerdefiniertes Skript aus der Zwischenablage ein.
      - I. Wählen Sie die Option **Einfügen oder Typ** aus.
      - II. Wählen Sie das Textfeld aus, und fügen Sie den Skripttext in das Feld ein.
      - III. Geben Sie dem Skript einen eindeutigen Namen.
      - IV. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.
- Wählen Sie ein vorhandenes Skript aus der Liste aus.

Hiermit wird der Testsuitelink angewiesen, dieses Skript zu verwenden.

8. Wählen Sie **Weiter**.

9. Überprüfen Sie die Konfiguration der Testsuite.

10. Wählen Sie **Hinzufügen**.

## Überprüfen Sie den Status eines Testablaufhängees

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

### Schritte

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

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

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

## Skriptverwendung anzeigen

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

### Schritte

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

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

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

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

## Bearbeiten Sie einen Testsuite-Haken

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

### Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie in der Spalte **Aktionen** das Menü Optionen für einen Haken, den Sie bearbeiten möchten.
4. Wählen Sie **Bearbeiten**.
5. Nehmen Sie alle erforderlichen Änderungen vor, und wählen Sie nach Abschluss jedes Abschnitts **Weiter** aus.
6. Wählen Sie **Speichern**.

## Deaktivieren Sie einen Testsuite-Haken

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

### Schritte

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

## Löschen Sie einen Testsuite-Haken

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

### Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie in der Spalte **Aktionen** das Menü Optionen für einen Haken, den Sie löschen möchten.
4. Wählen Sie **Löschen**.
5. Geben Sie im Dialogfeld „Ergebnis“ zur Bestätigung „Löschen“ ein.
6. Wählen Sie **Ja, Testsuite löschen**.

## Finden Sie weitere Informationen

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



## Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

## Markeninformationen

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