



# **Management und Sicherung von Applikationen**

## **Astra Control Service**

NetApp  
July 29, 2024

# Inhalt

- Management und Sicherung von Applikationen ..... 1
  - Starten Sie das Anwendungsmanagement ..... 1
  - Sichern von Applikationen durch Snapshots und Backups ..... 9
  - [Tech Preview] Schützen Sie einen gesamten Cluster ..... 21
  - Wiederherstellung von Applikationen ..... 23
  - Klonen und Migrieren von Applikationen ..... 31
  - Anwendungsausführungshaken verwalten ..... 33

# 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.

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

## Anforderungen für das Applikationsmanagement

Astra Control verfügt über folgende Anforderungen an das Applikationsmanagement:

- **Lizenzierung:** Um mehr als 10 Namespaces zu verwalten, benötigen Sie ein Astra Control 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 haben ["Hat den Cluster hinzugefügt"](#) Bei Astra Control können Sie Apps installieren oder vorhandene Apps auf dem Cluster managen. Jede Anwendung, die einem oder mehreren Namespaces zugeordnet ist, kann verwaltet werden.

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 Control Provisioner oder einem allgemeinen 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.

### Bevor Sie beginnen

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



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

### Über diese Aufgabe

- Bevor Sie beginnen, sollten Sie auch verstehen ["Verwalten von Standard- und Systemnames"](#).
- Wenn Sie in Astra Control mehrere Namespaces mit Ihren Apps verwenden möchten, 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 Sicherungsrichtlinien aufnehmen. Überlappende Sicherungsrichtlinien für Kubernetes-Ressourcen können zu Datenkonflikten führen.

## 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 Systemnamespaces 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.

### **[Tech Preview] Definieren Sie eine Applikation mithilfe einer benutzerdefinierten Kubernetes-Ressource**

Sie können die Kubernetes-Ressourcen angeben, die Sie mit Astra Control managen möchten, indem Sie sie als Applikation mithilfe einer benutzerdefinierten Ressource definieren. Sie können Ressourcen mit Cluster-Umfang hinzufügen, wenn Sie diese Ressourcen einzeln oder alle Kubernetes-Ressourcen in einem Namespace managen möchten, wenn Sie beispielsweise alle Ressourcen in einem bestimmten Namespace auf ähnliche Weise und in gängigen Intervallen managen und schützen möchten.

#### **Schritte**

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie (z. B. `astra_mysql_app.yaml`).
2. Benennen Sie die Anwendung in `metadata.name`.
3. Definieren Sie die zu verwaltenden Anwendungsressourcen:



### **spec.includedClusterScopedResources**

Hinzufügen von Ressourcentypen mit Cluster-Umfang zusätzlich zu den von Astra Control automatisch enthaltenen Ressourcen:

- **spec.includedClusterScopedResources:** *(Optional)* Eine Liste der im Cluster enthaltenen Ressourcentypen.
  - **GroupVersionRind:** *(Optional)* eindeutig identifiziert eine Art.
    - **Group:** *(erforderlich, wenn groupVersionRind verwendet wird)* API-Gruppe der einzuschließen Ressource.
    - **Version:** *(erforderlich, wenn groupVersionRind verwendet wird)* API-Version der einzubauenden Ressource.
    - **Kind:** *(erforderlich, wenn groupVersionRind verwendet wird)* Art der Ressource, die einbezogen werden soll.
  - **LabelSelector:** *(Optional)* Eine Label-Abfrage für eine Gruppe von Ressourcen. Es wird verwendet, um nur die Ressourcen abzurufen, die der Bezeichnung entsprechen. Wenn Sie kein Etikett bereitstellen, sammelt Astra Control alle Instanzen der für diesen Cluster angegebenen Ressourcenkartart. Das Ergebnis von matchLabels und matchExpressions ist ANDed.
  - **MatchLabels:** *(Optional)* Eine Karte von {key,value} Paaren. Ein einzelner {key,value} in der matchLabels-Karte entspricht einem Element von matchExpressions, das ein Schlüsselfeld von "key", Operator als "in" und Values-Array enthält, das nur "value" enthält. Die Anforderungen sind ANDed.
  - **MatchExpressions:** *(Optional)* Eine Liste der Anforderungen an die Etikettenauswahl. Die Anforderungen sind ANDed.
    - **Key:** *(erforderlich, wenn matchExpressions verwendet wird)* der Label-Schlüssel, der mit dem Label-Selektor verknüpft ist.
    - **Operator:** *(erforderlich, wenn matchExpressions verwendet wird)* stellt die Beziehung eines Schlüssels zu einem Satz von Werten dar. Gültige Operatoren sind In, NotIn, Exists Und DoesNotExist.
    - **Values:** *(erforderlich, wenn matchExpressions verwendet wird)* ein Array von String-Werten. Wenn der Operator ist In Oder NotIn, Das Wertearray darf \_Not\_ leer sein. Wenn der Operator ist Exists Oder DoesNotExist, Das Werte-Array muss leer sein.

### **spec.includedNamespaces**

Fügen Sie Namespaces und Ressourcen in diesen Ressourcen in der Anwendung ein:

- **spec.includedNamespaces:** *\_(required)\_* definiert den Namespace und optionale Filter für die Ressourcenauswahl.
  - **Namespace:** *(erforderlich)* der Namespace, der die App-Ressourcen enthält, die Sie mit Astra Control managen möchten.
  - **LabelSelector:** *(Optional)* Eine Label-Abfrage für eine Gruppe von Ressourcen. Es wird verwendet, um nur die Ressourcen abzurufen, die der Bezeichnung entsprechen. Wenn Sie kein Etikett bereitstellen, sammelt Astra Control alle Instanzen der für diesen Cluster angegebenen Ressourcenkartart. Das Ergebnis von matchLabels und matchExpressions ist ANDed.
    - **MatchLabels:** *(Optional)* Eine Karte von {key,value} Paaren. Ein einzelner {key,value} in

der matchLabels-Karte entspricht einem Element von matchExpressions, das ein Schlüsselfeld von "key", Operator als "in" und Values-Array enthält, das nur "value" enthält. Die Anforderungen sind ANDed.

- **MatchExpressions:** (*Optional*) Eine Liste der Anforderungen an die Etikettenauswahl. key Und operator Erforderlich sind. Die Anforderungen sind ANDed.
  - **Key:** (*erforderlich, wenn matchExpressions verwendet wird*) der Label-Schlüssel, der mit dem Label-Selektor verknüpft ist.
  - **Operator:** (*erforderlich, wenn matchExpressions verwendet wird*) stellt die Beziehung eines Schlüssels zu einem Satz von Werten dar. Gültige Operatoren sind In, NotIn, Exists Und DoesNotExist.
  - **Values:** (*erforderlich, wenn matchExpressions verwendet wird*) ein Array von String-Werten. Wenn der Operator ist In Oder NotIn, Das Wertearray darf *Not* leer sein. Wenn der Operator ist Exists Oder DoesNotExist, Das Werte-Array muss leer sein.

Beispiel YAML:

```
apiVersion: astra.netapp.io/v1
kind: Application
metadata:
  name: astra_mysql_app
spec:
  includedNamespaces:
  - namespace: astra_mysql_app
  labelSelector:
    matchLabels:
      app: nginx
      env: production
  matchExpressions:
  - key: tier
    operator: In
    values:
      - frontend
      - backend
```

4. Nachdem Sie das ausgefüllt haben astra\_mysql\_app.yaml Datei mit den richtigen Werten, CR anwenden:

```
kubectl apply -f astra_mysql_app.yaml -n astra-connector
```

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

Astra Control erkennt auch Systemnames auf einem Kubernetes Cluster. Wir zeigen Ihnen diese System-Namespace 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.

Weitere Informationen zu "[Datensicherung in Astra Control](#)".

Sie können die folgenden Aufgaben zum Schutz Ihrer Applikationsdaten ausführen:

- [Konfigurieren einer Sicherungsrichtlinie](#)
- [Erstellen Sie einen Snapshot](#)
- [Erstellen Sie ein Backup](#)
- [Backup und Restore für den wirtschaftlichen Betrieb von ontap-nas](#)
- [Unveränderliches Backup erstellen](#)
- [Anzeigen von Snapshots und Backups](#)
- [Snapshots löschen](#)
- [Abbrechen von Backups](#)
- [Backups löschen](#)

### Konfigurieren einer Sicherungsrichtlinie

Eine Sicherungsrichtlinie sichert eine Applikation, indem Snapshots, Backups oder beides nach einem definierten Zeitplan erstellt werden. Sie können Snapshots und Backups stündlich, täglich, wöchentlich und monatlich erstellen. Außerdem können Sie die Anzahl der beizubehaltenden Kopien festlegen. Sie können eine Schutzrichtlinie entweder über die Astra Control Web-UI oder über eine benutzerdefinierte Ressourcendatei (CR) definieren.

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



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



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

## Konfigurieren Sie eine Schutzrichtlinie über die Web-Benutzeroberfläche

### 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. 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 erst aktiviert, wenn Sie eine Aufbewahrungsstufe festlegen.

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

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

[Einen Screenshot einer Beispielkonfigurationsrichtlinie, in der Sie Snapshots und Backups stündlich, täglich, wöchentlich oder monatlich erstellen können.]

5. **[Tech Preview]** Wählen Sie einen Ziel-Bucket für die Backups oder Snapshots aus der Liste der Speicher-Buckets.
6. Wählen Sie **Bewertung**.
7. Wählen Sie **Schutzrichtlinie Festlegen**.

### [Tech Preview] Konfigurieren Sie eine Schutzrichtlinie mit einem CR

#### Schritte

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie `astra-control-schedule-cr.yaml`. Aktualisieren Sie die Werte in Klammern `<>`, um sie an die Anforderungen Ihrer Astra Control-Umgebung, Cluster-Konfiguration und Datensicherung anzupassen:
  - `<CR_NAME>`: Der Name dieser benutzerdefinierten Ressource; wählen Sie einen eindeutigen und vernünftigen Namen für Ihre Umgebung.
  - `<APPLICATION_NAME>`: Der Kubernetes-Name der zu Back-up-Applikation.
  - `<APPVAULT_NAME>`: Der Name des AppVault, in dem der Backup-Inhalt gespeichert werden soll.
  - `<BACKUPS_RETAINED>`: Die Anzahl der beizubehaltenden Backups. Null bedeutet, dass keine Backups erstellt werden sollen.
  - `<SNAPSHOTS_RETAINED>`: Die Anzahl der beizubehaltenden Snapshots. Null bedeutet, dass keine Snapshots erstellt werden sollen.
  - `<GRANULARITY>`: Die Häufigkeit, mit der der Zeitplan ausgeführt werden soll. Mögliche Werte, zusammen mit den erforderlichen zugeordneten Feldern:
    - `hourly` (Erfordert, dass Sie angeben `spec.minute`)
    - `daily` (Erfordert, dass Sie angeben `spec.minute` Und `spec.hour`)
    - `weekly` (Erfordert, dass Sie angeben `spec.minute`, `spec.hour`, und `spec.dayOfWeek`)
    - `monthly` (Erfordert, dass Sie angeben `spec.minute`, `spec.hour`, und

```
spec.dayOfMonth)
```

- <DAY\_OF\_MONTH>: (*Optional*) der Tag des Monats (1 - 31), an dem der Zeitplan ausgeführt werden soll. Dieses Feld ist erforderlich, wenn die Granularität auf festgelegt ist `monthly`.
- <DAY\_OF\_WEEK>: (*Optional*) der Wochentag (0 - 7), an dem der Zeitplan ausgeführt werden soll. Werte von 0 oder 7 zeigen Sonntag an. Dieses Feld ist erforderlich, wenn die Granularität auf festgelegt ist `weekly`.
- <HOUR\_OF\_DAY>: (*Optional*) die Stunde des Tages (0 - 23), die der Zeitplan ausführen soll. Dieses Feld ist erforderlich, wenn die Granularität auf festgelegt ist `daily`, `weekly`, Oder `monthly`.
- <MINUTE\_OF\_HOUR>: (*Optional*) die Minute der Stunde (0 - 59), die der Zeitplan ausführen soll. Dieses Feld ist erforderlich, wenn die Granularität auf festgelegt ist `hourly`, `daily`, `weekly`, Oder `monthly`.

```
apiVersion: astra.netapp.io/v1
kind: Schedule
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  backupRetention: "<BACKUPS_RETAINED>"
  snapshotRetention: "<SNAPSHOTS_RETAINED>"
  granularity: <GRANULARITY>
  dayOfMonth: "<DAY_OF_MONTH>"
  dayOfWeek: "<DAY_OF_WEEK>"
  hour: "<HOUR_OF_DAY>"
  minute: "<MINUTE_OF_HOUR>"
```

2. Nachdem Sie das ausgefüllt haben `astra-control-schedule-cr.yaml` Datei mit den richtigen Werten, CR anwenden:

```
kubectl apply -f astra-control-schedule-cr.yaml
```

## Ergebnis

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

## Erstellen Sie einen Snapshot

Sie können jederzeit einen On-Demand-Snapshot erstellen.

### Über diese Aufgabe

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

unterstützt werden:

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



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

## Erstellen Sie mithilfe der Web-Benutzeroberfläche einen Snapshot

### 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. **[Tech Preview]** Wählen Sie einen Ziel-Bucket für den Snapshot aus der Liste der Speicher-Buckets.
5. Überprüfen Sie die Snapshot-Zusammenfassung und wählen Sie **Snapshot**.

## **[Tech Preview]** Erstellen Sie einen Snapshot mit einem CR

### Schritte

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie `astra-control-snapshot-cr.yaml`. Aktualisieren Sie die Werte in Klammern `<>`, um sie an die Astra Control-Umgebung und die Cluster-Konfiguration anzupassen:
  - `<CR_NAME>`: Der Name dieser benutzerdefinierten Ressource; wählen Sie einen eindeutigen und vernünftigen Namen für Ihre Umgebung.
  - `<APPLICATION_NAME>`: Der Kubernetes-Name der Applikation, für die ein Snapshot erstellt werden soll.
  - `<APPVAULT_NAME>`: Der Name des AppVault, in dem der Snapshot-Inhalt gespeichert werden soll.
  - `<RECLAIM_POLICY>`: (*Optional*) definiert, was mit einem Snapshot passiert, wenn der Snapshot CR gelöscht wird. Gültige Optionen:
    - Retain
    - Delete (Standard)

```
apiVersion: astra.netapp.io/v1
kind: Snapshot
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  reclaimPolicy: <RECLAIM_POLICY>
```

2. Nachdem Sie das ausgefüllt haben `astra-control-snapshot-cr.yaml` Datei mit den richtigen Werten, CR anwenden:

```
kubectl apply -f astra-control-snapshot-cr.yaml
```

## 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.



Achten Sie darauf, wie Speicherplatz verarbeitet wird, wenn Sie eine Applikation sichern, die auf Azure NetApp Files Storage gehostet wird. Siehe "[Applikations-Backups](#)" Finden Sie weitere Informationen.



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

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

### Über diese Aufgabe

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

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

## Erstellen Sie mithilfe der Web-Benutzeroberfläche ein Backup

### 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. **[Tech Preview]** Wählen Sie einen Ziel-Bucket für das Backup aus der Liste der Speicher-Buckets.
6. Wählen Sie **Weiter**.
7. Überprüfen Sie die Backup-Zusammenfassung und wählen Sie **Backup**.

### [Tech Preview] Erstellen Sie ein Backup mit einem CR

#### Schritte

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie `astra-control-backup-cr.yaml`. Aktualisieren Sie die Werte in Klammern `<>`, um sie an die Astra Control-Umgebung und die Cluster-Konfiguration anzupassen:
  - `<CR_NAME>`: Der Name dieser benutzerdefinierten Ressource; wählen Sie einen eindeutigen und vernünftigen Namen für Ihre Umgebung.
  - `<APPLICATION_NAME>`: Der Kubernetes-Name der zu Back-up-Applikation.
  - `<APPVAULT_NAME>`: Der Name des AppVault, in dem der Backup-Inhalt gespeichert werden soll.

```
apiVersion: astra.netapp.io/v1
kind: Backup
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
```

2. Nachdem Sie das ausgefüllt haben `astra-control-backup-cr.yaml` Datei mit den richtigen Werten, CR anwenden:

```
kubectl apply -f astra-control-backup-cr.yaml
```

## Ergebnis

Astra Control erstellt ein Backup der App.



- Wenn Ihr Netzwerk ausfällt oder ungewöhnlich langsam ist, kann es zu einer Zeit für einen Backup-Vorgang kommen. Dies führt zum Fehlschlagen der Datensicherung.
- Wenn Sie eine laufende Sicherung abbrechen müssen, befolgen Sie die Anweisungen unter [Abbrechen von Backups](#). Um das Backup zu löschen, warten Sie, bis es abgeschlossen ist, und befolgen Sie die Anweisungen unter [Backups löschen](#).
- Nach einer Datensicherungsoperation (Klonen, Backup, Restore) und einer anschließenden Anpassung des persistenten Volumens beträgt die Verzögerung bis zu zwanzig Minuten, bevor die neue Volume-Größe in der UI angezeigt wird. Der Datensicherungsvorgang ist innerhalb von Minuten erfolgreich und Sie können mit der Management Software für das Storage-Backend die Änderung der Volume-Größe bestätigen.

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

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

### Bevor Sie beginnen

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

## Erweitern Sie für Konfigurationsschritte

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

- Finden Sie die SVM, die den hostet `ontap-nas-economy`-Basierte Volumen der Anwendung.
- Melden Sie sich bei einem Terminal an, das mit ONTAP verbunden ist, wo die Volumes erstellt werden.
- Snapshot-Verzeichnis für SVM ausblenden:



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

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

+



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

2. Gehen Sie in Astra Control Provisioner oder Astra Trident wie folgt vor:

- Aktivieren Sie das Snapshot-Verzeichnis für jedes PV, das auf `ontap-nas-Economy` basiert und der Applikation zugeordnet ist:

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

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

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

Antwort:

```
snapshotDirectory: "true"
```

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

### Ergebnis

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

## Unveränderliches Backup erstellen

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

### Bevor Sie beginnen

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

- **Amazon Web Services:** "[Aktivieren Sie S3 Object Lock beim Erstellen des Buckets und legen Sie den Standardaufbewahrungsmodus „Governance“ mit einer Standardaufbewahrungszeit fest](#)".
- **Google Cloud:** "[Konfigurieren Sie einen Bucket mit einer Aufbewahrungsrichtlinie und geben Sie einen Aufbewahrungszeitraum an](#)".
- **Microsoft Azure:** "[Konfigurieren Sie einen Blob-Storage-Bucket mit einer zeitbasierten Aufbewahrungsrichtlinie im Umfang von Containern](#)".
- **NetApp StorageGRID:** "[Aktivieren Sie S3 Object Lock beim Erstellen des Buckets und legen Sie den Standardaufbewahrungsmodus „Compliance“ mit einer Standardaufbewahrungsdauer fest](#)".



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



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

### Schritte

1. Wählen Sie **Anwendungen**.
2. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für die gewünschte App die Option **Sichern** aus.
3. Passen Sie den Namen des Backups an.
4. Wählen Sie aus, ob die Anwendung aus einem vorhandenen Snapshot gesichert werden soll. Wenn Sie diese Option auswählen, können Sie aus einer Liste vorhandener Snapshots auswählen.
5. Wählen Sie aus der Liste der Storage-Buckets einen Ziel-Bucket für das Backup aus. Ein WORM-Bucket (Write Once Read Many) wird neben dem Bucket-Namen mit dem Status „gesperrt“ angezeigt.



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

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

### Ergebnis

Astra Control erstellt eine unveränderliche Sicherung der App.



- Wenn Ihr Netzwerk ausfällt oder ungewöhnlich langsam ist, kann es zu einer Zeit für einen Backup-Vorgang kommen. Dies führt zum Fehlschlagen der Datensicherung.
- Wenn Sie versuchen, zwei unveränderliche Backups derselben App gleichzeitig im selben Bucket zu erstellen, verhindert Astra Control, dass das zweite Backup gestartet wird. Warten Sie, bis die erste Sicherung abgeschlossen ist, bevor Sie eine andere starten.
- Sie können ein auslaufendes unveränderliches Backup nicht abbrechen.
- Nach einer Datensicherungsoperation (Klonen, Backup, Restore) und einer anschließenden Anpassung des persistenten Volumes beträgt die Verzögerung bis zu zwanzig Minuten, bevor die neue Volume-Größe in der UI angezeigt wird. Der Datensicherungsvorgang ist innerhalb von Minuten erfolgreich und Sie können mit der Management Software für das Storage-Backend die Änderung der Volume-Größe bestätigen.

## Anzeigen von Snapshots und Backups

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



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

### Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer 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 befindet, nicht abbrechen **Pending Bundesland**.



Sie können ein auslaufendes unveränderliches Backup nicht abbrechen.

### Schritte

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

## Backups löschen

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



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.



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

### 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.

## [Tech Preview] Schützen Sie einen gesamten Cluster

Sie können ein geplantes, automatisches Backup von beliebigen oder allen nicht gemanagten Namespaces in einem Cluster erstellen. Diese Workflows werden von NetApp als Kubernetes-Servicekonto, als Rollenbindung und als cron-Job bereitgestellt, orchestriert mit einem Python Skript.

### So funktioniert es

Wenn Sie den vollständigen Cluster-Backup-Workflow konfigurieren und installieren, wird ein Cron-Job regelmäßig ausgeführt und schützt alle noch nicht verwalteten Namespaces. Dabei werden automatisch Schutzrichtlinien basierend auf Zeitplänen erstellt, die Sie während der Installation auswählen.

Wenn Sie nicht jeden nicht verwalteten Namespace auf dem Cluster mit dem vollständigen Cluster-Backup-Workflow schützen möchten, können Sie stattdessen den labelbasierten Backup-Workflow verwenden. Der labelbasierte Backup-Workflow verwendet auch eine Cron-Aufgabe, aber anstatt alle nicht verwalteten Namespaces zu schützen, identifiziert er Namespaces durch von Ihnen zur Verfügung gestellt Labels, um optional die Namespaces auf Basis von Bronze-, Silber- oder Gold-Backup-Richtlinien zu schützen.

Wenn ein neuer Namespace erstellt wird, der in den Umfang des von Ihnen gewählten Workflows fällt, wird er automatisch und ohne Administratoraktionen geschützt. Diese Workflows werden auf Cluster-Basis implementiert. Je nach Cluster-Bedeutung können unterschiedliche Cluster einen der beiden Workflows mit individuellen Sicherungsstufen nutzen.

### **Beispiel: Vollständige Cluster-Sicherung**

Wenn Sie beispielsweise den vollständigen Cluster-Backup-Workflow konfigurieren und installieren, werden alle Applikationen in einem Namespace regelmäßig und ohne weiteren Aufwand durch den Administrator gemanagt und geschützt. Der Namespace muss bei der Installation des Workflows nicht vorhanden sein; wenn ein Namespace in der Zukunft hinzugefügt wird, wird er geschützt.

### **Beispiel: Label-basierter Schutz**

Für eine größere Granularität können Sie den labelbasierten Workflow verwenden. Sie können beispielsweise diesen Workflow installieren und Ihren Benutzern mitteilen, je nach Schutzstufe eine von mehreren Labels auf alle Namespaces anzuwenden, die sie schützen möchten. Auf diese Weise können Benutzer den Namespace mit einem dieser Labels erstellen, ohne dass sie einen Administrator benachrichtigen müssen. Der neue Namespace und alle darin Apps werden automatisch geschützt.

## **Erstellen Sie ein geplantes Backup aller Namespaces**

Sie können mithilfe des vollständigen Cluster-Backup-Workflows ein geplantes Backup aller Namespaces auf einem Cluster erstellen.

### **Schritte**

1. Laden Sie die folgenden Dateien auf einen Computer herunter, der über Netzwerkzugriff auf den Cluster verfügt:
  - ["Components.yaml CRD-Datei"](#)
  - ["protectCluster.py Python-Skript"](#)
2. So konfigurieren und installieren Sie das Toolkit: ["Befolgen Sie die im Lieferumfang enthaltenen Anweisungen"](#).

## **Erstellen Sie ein geplantes Backup bestimmter Namespaces**

Sie können mithilfe des labelbasierten Backup-Workflows ein geplantes Backup bestimmter Namespaces anhand ihrer Labels erstellen.

### **Schritte**

1. Laden Sie die folgenden Dateien auf einen Computer herunter, der über Netzwerkzugriff auf den Cluster verfügt:
  - ["Components.yaml CRD-Datei"](#)
  - ["protectCluster.py Python-Skript"](#)
2. So konfigurieren und installieren Sie das Toolkit: ["Befolgen Sie die im Lieferumfang enthaltenen Anweisungen"](#).



# 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 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.

## Bevor Sie beginnen

- **Schützen Sie Ihre Anwendungen zuerst:** Es wird dringend empfohlen, dass Sie einen Snapshot oder ein Backup Ihrer Anwendung vor der Wiederherstellung machen. Auf diese Weise können Sie aus dem Snapshot oder Backup klonen, wenn die Wiederherstellung nicht erfolgreich war.
- **Zieldatenträger prüfen:** Wenn Sie eine andere Speicherklasse wiederherstellen, stellen Sie sicher, dass die Speicherklasse den gleichen persistenten Zugriffsmodus für Volumes verwendet (z. B. ReadWriteMany). Der Wiederherstellungsvorgang schlägt fehl, wenn der Zugriffsmodus des Ziel-persistenten Volumes anders ist. Wenn das persistente Quell-Volume beispielsweise den RWX-Zugriffsmodus verwendet, wählen Sie eine Ziel-Storage-Klasse aus, die RWX nicht bereitstellen kann, wie z. B. Azure Managed Disks, AWS EBS, Google Persistent Disk oder `ontap-san` Wird dazu führen, dass der Wiederherstellungsvorgang fehlschlägt. Weitere Informationen zu den Zugriffsmodi für persistente Volumes finden Sie im ["Kubernetes"](#) Dokumentation.
- **Planung des Platzbedarfs:** Wenn Sie eine in-Place-Wiederherstellung einer Applikation durchführen, die NetApp ONTAP Storage nutzt, kann sich der von der wiederhergestellten Applikation genutzte Speicherplatz verdoppeln. Nachdem Sie eine in-Place-Wiederherstellung durchgeführt haben, entfernen Sie alle unerwünschten Snapshots aus der wiederhergestellten Applikation, um Speicherplatz freizugeben.
- **Unterstützte Storage Class Treiber:** Astra Control unterstützt die Wiederherstellung von Backups mit Speicherklassen, die von den folgenden Treibern unterstützt werden:
  - `ontap-nas`
  - `ontap-nas-economy`
  - `ontap-san`
  - `ontap-san-economy`
- **(nur ontap-nas-Economy-Treiber) Backups und Wiederherstellungen:** Vor dem Backup oder der Wiederherstellung einer App, die eine von der unterstützte Storage-Klasse verwendet `ontap-nas-economy` Überprüfen Sie, ob der ["Das snapshot Verzeichnis auf dem ONTAP Storage-Backend ist verborgen"](#). Das Ausblenden dieses Verzeichnisses kann zu einem Verlust des Zugriffs auf Ihre Anwendung führen, insbesondere wenn es NFSv3 verwendet.



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.

## Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie im Menü Optionen in der Spalte Aktionen die Option **Wiederherstellen** aus.
3. Wählen Sie den Wiederherstellungstyp aus:
  - **Wiederherstellen auf ursprünglichen Namespaces:** Verwenden Sie dieses Verfahren, um die App an Ort und Stelle auf dem ursprünglichen Cluster wiederherzustellen.
    - i. Wählen Sie den Snapshot oder das Backup aus, mit dem die App direkt wiederhergestellt werden soll. Dadurch wird die App auf eine frühere Version von selbst zurückgesetzt.
    - ii. Wählen Sie **Weiter**.



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

- **Wiederherstellen auf neuen Namespaces:** Verwenden Sie dieses Verfahren, um die App auf einem anderen Cluster oder mit verschiedenen Namespaces von der Quelle wiederherzustellen. Mit diesem Verfahren können Sie auch eine App zu einer anderen Storage-Klasse migrieren.
  - i. Geben Sie den Namen für die wiederhergestellte App an.
  - ii. Wählen Sie das Ziel-Cluster für die Anwendung aus, die Sie wiederherstellen möchten.
  - iii. Geben Sie für jeden mit der App verknüpften Quell-namespace einen Ziel-namespace ein.



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

- iv. Wählen Sie **Weiter**.
- v. Wählen Sie den Snapshot oder das Backup aus, mit dem die App wiederhergestellt werden soll.
- vi. Wählen Sie **Weiter**.
- vii. Folgenden Optionen wählbar:
  - **Wiederherstellung unter Verwendung der ursprünglichen Speicherklassen:** Die Anwendung verwendet die ursprünglich zugeordnete Speicherkategorie, es sei denn, sie existiert nicht auf dem Zielcluster. In diesem Fall wird die Standard-Storage-Kategorie für das Cluster verwendet.
  - **Wiederherstellen mit einer anderen Storage-Kategorie:** Wählen Sie eine Storage-Kategorie aus, die auf dem Ziel-Cluster vorhanden ist. Alle Applikations-Volumes, unabhängig von den ursprünglich zugewiesenen Storage-Kategorien, werden im Rahmen der Wiederherstellung in diese andere Storage-Kategorie migriert.
- viii. Wählen Sie **Weiter**.

4. Wählen Sie die Ressourcen aus, die gefiltert werden sollen:
  - **Alle Ressourcen wiederherstellen:** Alle mit der ursprünglichen App verknüpften Ressourcen wiederherstellen.
  - **Ressourcen filtern:** Geben Sie Regeln an, um einen Gegensatz der ursprünglichen Anwendungsressourcen wiederherzustellen:
    - i. Wählen Sie diese Option, um Ressourcen aus der wiederhergestellten Anwendung einzuschließen

oder auszuschließen.

- ii. Wählen Sie entweder **Include rule** oder **Add exclude rule** aus und konfigurieren Sie die Regel, um die richtigen Ressourcen während der Anwendungswiederherstellung zu filtern. Sie können eine Regel bearbeiten oder entfernen und eine Regel erneut erstellen, bis die Konfiguration korrekt ist.



Weitere Informationen zum Konfigurieren von Einschließen- und Ausschlussregeln finden Sie unter [Filtern Sie Ressourcen während einer Anwendungswiederherstellung](#).

5. Wählen Sie **Weiter**.

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

## **[Tech Preview] Wiederherstellen von Backups mithilfe einer benutzerdefinierten Ressource (CR)**

Sie können Daten aus einem Backup mithilfe einer benutzerdefinierten Ressourcendatei (CR) entweder in einem anderen Namespace oder im ursprünglichen QuellNamespace wiederherstellen.

## Mit einem CR-System aus der Sicherung wiederherstellen

### Schritte

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie `astra-control-backup-restore-cr.yaml`. Aktualisieren Sie die Werte in Klammern `<>`, um sie an die Astra Control-Umgebung und die Cluster-Konfiguration anzupassen:
  - `<CR_NAME>`: Der Name dieser CR-Operation; wählen Sie einen vernünftigen Namen für Ihre Umgebung.
  - `<APPVAULT_NAME>`: Der Name des AppVault, in dem der Backup-Inhalt gespeichert ist.
  - `<BACKUP_PATH>`: Der Pfad innerhalb von AppVault, wo die Backup-Inhalte gespeichert werden. Beispiel:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-20231213023800_94347756-9d9b-401d-a0c3
```

- `<SOURCE_NAMESPACE>`: Der Quell-Namespace des Wiederherstellungsvorgangs.
- `<DESTINATION_NAMESPACE>`: Der Ziel-Namespace des Wiederherstellungsvorgangs.

```
apiVersion: astra.netapp.io/v1
kind: BackupRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appVaultRef: <APPVAULT_NAME>
  appArchivePath: <BACKUP_PATH>
  namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
"destination": "<DESTINATION_NAMESPACE>"}]
```

Ungelöste Direktive in `<stdin>` - `include:../_include/selective-Restore-cr.adoc[]`

1. Nachdem Sie das ausgefüllt haben `astra-control-backup-restore-cr.yaml` Datei mit den richtigen Werten, CR anwenden:

```
kubectl apply -f astra-control-backup-restore-cr.yaml
```

## Wiederherstellung aus dem Backup in den ursprünglichen Namespace mit einem CR

### Schritte

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie `astra-control-backup-ipr-cr.yaml`. Aktualisieren Sie die Werte in Klammern `<>`, um sie an die Astra Control-Umgebung und die Cluster-Konfiguration anzupassen:
  - `<CR_NAME>`: Der Name dieser CR-Operation; wählen Sie einen vernünftigen Namen für Ihre Umgebung.

- <APPVAULT\_NAME>: Der Name des AppVault, in dem der Backup-Inhalt gespeichert ist.
- <BACKUP\_PATH>: Der Pfad innerhalb von AppVault, wo die Backup-Inhalte gespeichert werden.  
Beispiel:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-  
20231213023800_94347756-9d9b-401d-a0c3
```

```
apiVersion: astra.netapp.io/v1  
kind: BackupInplaceRestore  
metadata:  
  name: <CR_NAME>  
  namespace: astra-connector  
spec:  
  appVaultRef: <APPVAULT_NAME>  
  appArchivePath: <BACKUP_PATH>
```

Ungelöste Direktive in <stdin> - include:../\_include/selective-Restore-cr.adoc[]

1. Nachdem Sie das ausgefüllt haben astra-control-backup-ipr-cr.yaml Datei mit den richtigen Werten, CR anwenden:

```
kubectl apply -f astra-control-backup-ipr-cr.yaml
```

## [Tech Preview] Wiederherstellen von Snapshots mithilfe einer benutzerdefinierten Ressource (CR)

Sie können Daten aus einem Snapshot mithilfe einer benutzerdefinierten Ressourcendatei (CR) entweder in einem anderen Namespace oder im ursprünglichen QuellNamespace wiederherstellen.

## Mit einem CR-System aus Snapshot wiederherstellen

### Schritte

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie `astra-control-snapshot-restore-cr.yaml`. Aktualisieren Sie die Werte in Klammern `<>`, um sie an die Astra Control-Umgebung und die Cluster-Konfiguration anzupassen:
  - `<CR_NAME>`: Der Name dieser CR-Operation; wählen Sie einen vernünftigen Namen für Ihre Umgebung.
  - `<APPVAULT_NAME>`: Der Name des AppVault, in dem der Backup-Inhalt gespeichert ist.
  - `<BACKUP_PATH>`: Der Pfad innerhalb von AppVault, wo die Backup-Inhalte gespeichert werden. Beispiel:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-20231213023800_94347756-9d9b-401d-a0c3
```

- `<SOURCE_NAMESPACE>`: Der Quell-Namespace des Wiederherstellungsvorgangs.
- `<DESTINATION_NAMESPACE>`: Der Ziel-Namespace des Wiederherstellungsvorgangs.

```
apiVersion: astra.netapp.io/v1
kind: SnapshotRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appArchivePath: <BACKUP_PATH>
  appVaultRef: <APPVAULT_NAME>
  namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
"destination": "<DESTINATION_NAMESPACE>"}]
```

Ungelöste Direktive in `<stdin>` - `include:../_include/selective-Restore-cr.adoc[]`

1. Nachdem Sie das ausgefüllt haben `astra-control-snapshot-restore-cr.yaml` Datei mit den richtigen Werten, CR anwenden:

```
kubectl apply -f astra-control-snapshot-restore-cr.yaml
```

## Wiederherstellen von Snapshots in den ursprünglichen Namespace mit einem CR

### Schritte

1. Erstellen Sie die CR-Datei (Custom Resource) und benennen Sie sie `astra-control-snapshot-ipc-cr.yaml`. Aktualisieren Sie die Werte in Klammern `<>`, um sie an die Astra Control-Umgebung und die Cluster-Konfiguration anzupassen:
  - `<CR_NAME>`: Der Name dieser CR-Operation; wählen Sie einen vernünftigen Namen für Ihre Umgebung.

- <APPVAULT\_NAME>: Der Name des AppVault, in dem der Backup-Inhalt gespeichert ist.
- <BACKUP\_PATH>: Der Pfad innerhalb von AppVault, wo die Backup-Inhalte gespeichert werden.  
Beispiel:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
20231213023800_94347756-9d9b-401d-a0c3
```

```
apiVersion: astra.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appArchivePath: <BACKUP_PATH>
  appVaultRef: <APPVAULT_NAME>
```

Ungelöste Direktive in <stdin> - include:../\_include/selective-Restore-cr.adoc[]

1. Nachdem Sie das ausgefüllt haben astra-control-snapshot-ipr-cr.yaml Datei mit den richtigen Werten, CR anwenden:

```
kubectl apply -f astra-control-snapshot-ipr-cr.yaml
```

## Ergebnis

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



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



Jeder Mitgliedsbenutzer mit Namespace-Einschränkungen nach Namespace-Name/ID oder anhand von Namespace-Bezeichnungen kann eine Applikation in einem neuen Namespace im selben Cluster oder einem anderen Cluster in seinem Unternehmenskonto klonen oder wiederherstellen. Derselbe Benutzer kann jedoch nicht auf die geklonte oder wiederhergestellte Anwendung im neuen Namespace zugreifen. Nachdem durch einen Klon- oder Wiederherstellungsvorgang ein neuer Namespace erstellt wurde, kann der Kontoadministrator/Kontoinhaber das Mitgliedskonto bearbeiten und Rolleneinschränkungen aktualisieren, damit der betroffene Benutzer Zugriff auf den neuen Namespace gewährt.

## Filtern Sie Ressourcen während einer Anwendungswiederherstellung

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

### Lesen Sie mehr über ein- und Ausschlusszenarien

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

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

### Schritte

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



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

2. Konfigurieren Sie die Filterregel:



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

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



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



- b. (Optional) Geben Sie einen Ressourcennamen ein.
- c. (Optional) **Etikettenauswahl**: A einschließen "Etikettenauswahl" Um der Regel hinzuzufügen. Mit der Etikettenauswahl werden nur die Ressourcen gefiltert, die der ausgewählten Bezeichnung entsprechen.
- d. (Optional) Wählen Sie **Use GVK (GroupVersionKind) Set, um Ressourcen zu filtern**, um weitere Filteroptionen zu erhalten.



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

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

3. Überprüfen Sie die Regel, die auf Ihren Einträgen erstellt wird.

4. Wählen Sie **Hinzufügen**.



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

## 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.

### Bevor Sie beginnen

- **Zieldatenträger prüfen**: Wenn Sie in eine andere Speicherklasse klonen, stellen Sie sicher, dass die Speicherklasse den gleichen persistenten Zugriffsmodus für Volumes verwendet (z. B. ReadWriteMany). Der Klonvorgang schlägt fehl, wenn der Zugriffsmodus des persistenten Volume-Ziels anders ist. Wenn das persistente Quell-Volume beispielsweise den RWX-Zugriffsmodus verwendet, wählen Sie eine Ziel-Storage-Klasse aus, die RWX nicht bereitstellen kann, wie z. B. Azure Managed Disks, AWS EBS, Google Persistent Disk oder `ontap-san`, Führt dazu, dass der Klonvorgang fehlschlägt. Weitere Informationen zu den Zugriffsmodi für persistente Volumes finden Sie im "[Kubernetes](#)" Dokumentation.
- Um 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 class:** Wenn Sie eine App mit einer explizit eingestellten Speicherklasse bereitstellen und die App klonen müssen, muss das Ziel-Cluster über die ursprünglich angegebene Speicherklasse verfügen. Das Klonen einer Applikation mit einer explizit festgelegten Storage-Klasse auf ein Cluster ohne dieselbe Storage-Klasse schlägt fehl.
- **Anwendungen mit Unterstützung der ontap-nas-Wirtschaft:** Klonvorgänge können nicht verwendet werden, wenn die Storage-Klasse Ihrer Applikation von unterstützt wird `ontap-nas-economy` Treiber. Sie können es jedoch ["Backup und Restore für den wirtschaftlichen Betrieb von ontap-nas"](#).
- **Klone und Benutzerbeschränkungen:** Jeder Mitgliedsbenutzer mit Namespace-Beschränkungen durch Namespace-Name/ID oder durch Namespace-Labels kann eine Anwendung in einem neuen Namespace im selben Cluster oder einem anderen Cluster im Konto ihres Unternehmens klonen oder wiederherstellen. Derselbe Benutzer kann jedoch nicht auf die geklonte oder wiederhergestellte Anwendung im neuen Namespace zugreifen. Nachdem durch einen Klon- oder Wiederherstellungsvorgang ein neuer Namespace erstellt wurde, kann der Kontoadministrator/Kontoinhaber das Mitgliedskonto bearbeiten und Rolleneinschränkungen aktualisieren, damit der betroffene Benutzer Zugriff auf den neuen Namespace gewährt.
- **Klone verwenden 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-Namespaces. Die angegebenen Ziel-Namespaces dürfen nicht bereits im Ziel-Cluster vorhanden sein.

- Wählen Sie **Weiter**.
- Wählen Sie aus, ob die der App zugeordnete ursprüngliche Storage-Klasse beibehalten oder eine andere Storage-Klasse ausgewählt werden soll.



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



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

5. Wählen Sie **Weiter**.

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

### Ergebnis

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

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

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



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

## Wichtige Hinweise zu benutzerdefinierten Testausführungshaken

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



Da Testsuitehaken 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 benötigen.

Wenn Sie eine Backup- oder Snapshot-Operation mit zugeordneten Testsuiten starten, diese aber dann abbrechen, können die Haken trotzdem ausgeführt werden, wenn der Backup- oder Snapshot-Vorgang bereits gestartet wurde. Das bedeutet, dass die in einem Testsuite nach dem Backup verwendete Logik nicht davon ausgehen kann, dass das Backup abgeschlossen wurde.

- Die Ausführungshaken-Funktion ist bei neuen Astra Control-Bereitstellungen standardmäßig deaktiviert.
  - Sie müssen die Funktion „Ausführungshaken“ aktivieren, bevor Sie Ausführungshaken verwenden können.
  - Benutzer von Eigentümer oder Administrator können die Funktion „Ausführungshaken“ für alle Benutzer aktivieren oder deaktivieren, die im aktuellen Astra Control-Konto definiert sind. Siehe [Aktivieren Sie die Funktion „Ausführungshaken“](#) Und [Deaktivieren Sie die Funktion Ausführungshaken](#) Weitere Anweisungen.
  - Der Status der Funktionsunterstützung bleibt bei Astra Control Upgrades erhalten.
- Ein Testsuite muss ein Skript verwenden, um Aktionen durchzuführen. Viele Testsuitehooks können auf dasselbe Skript verweisen.
- Astra Control erfordert, dass die Skripte, mit denen Ausführungshaken ausgeführt werden, im Format ausführbarer Shell-Skripte geschrieben werden.
- Die Skriptgröße ist auf 96 KB begrenzt.

- Astra Control verwendet Hook-Einstellungen für die Ausführung und alle übereinstimmenden Kriterien, um festzustellen, welche Haken für einen Snapshot-, Backup- oder Wiederherstellungsvorgang gelten.
- Alle Fehler bei den Testausführungshaken sind weiche Ausfälle, andere Haken und der Datenschutzvorgang werden immer noch versucht, auch wenn ein Haken ausfällt. Wenn ein Haken jedoch ausfällt, wird ein Warnereignis im Ereignisprotokoll der Seite \* aufgezeichnet.
- Um Testsuiten zu erstellen, zu bearbeiten oder zu löschen, müssen Sie Benutzer mit den Berechtigungen Eigentümer, Administrator oder Mitglied sein.
- Wenn ein Execution Hook länger als 25 Minuten dauert, schlägt der Hook fehl und erstellt einen Ereignisprotokolleintrag mit einem Rückgabecode von „N/A“. Jeder betroffene Snapshot wird als fehlgeschlagen markiert, und ein resultierender Eintrag im Ereignisprotokoll weist auf das Timeout hin.
- Für Ad-hoc-Datenschutzvorgänge werden alle Hook-Ereignisse generiert und im Ereignisprotokoll der Seite **Aktivität** gespeichert. Bei geplanten Datenschutzvorgängen werden jedoch nur Hook-Failure-Ereignisse im Ereignisprotokoll aufgezeichnet (Ereignisse, die von den geplanten Datenschutzvorgängen selbst generiert werden, werden noch aufgezeichnet).

## Ausführungsreihenfolge

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

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

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

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

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



Sie sollten Ihre Hook-Skripte immer testen, bevor Sie sie in einer Produktionsumgebung aktivieren. Mit dem Befehl '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	N	Y
6	Klonen oder Wiederherstellen	N	Y	Neu	Anders	N	N	Y
7	Wiederherstellen	Y	N	Vorhanden	Gleich	N	N	Y

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

## Aktivieren Sie die Funktion „Ausführungshaken“

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

### Schritte

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

Die Registerkarte **Account > feature settings** wird angezeigt.

4. Wählen Sie im Bereich **Ausführungshaken** das Einstellungsmenü aus.
5. Wählen Sie **Enable**.
6. Beachten Sie die Sicherheitswarnung, die angezeigt wird.
7. Wählen Sie **Ja, Ausführungshaken aktivieren**.

## Deaktivieren Sie die Funktion Ausführungshaken

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

### Schritte

1. Gehen Sie zu **Account** und wählen Sie dann die Registerkarte **Feature settings**.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie im Bereich **Ausführungshaken** das Einstellungsmenü aus.
4. Wählen Sie **Deaktivieren**.



5. Beachten Sie die Warnmeldung, die angezeigt wird.
6. Typ `disable` Um zu bestätigen, dass Sie die Funktion für alle Benutzer deaktivieren möchten.
7. Wählen Sie **Ja, deaktivieren**.

## Vorhandene Testsuiten anzeigen

Sie können vorhandene benutzerdefinierte Testsuiten für eine App anzeigen.

### Schritte

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

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

## Vorhandene Skripte anzeigen

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

### Schritte

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

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

## Fügen Sie ein Skript hinzu

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

### Schritte

1. Stellen Sie sicher, dass die Funktion Ausführungshaken aktiviert ist [Aktiviert](#).
2. Gehen Sie zu **Konto**.
3. Wählen Sie die Registerkarte **Skripts** aus.
4. Wählen Sie **Hinzufügen**.
5. Führen Sie einen der folgenden Schritte aus:
  - Laden Sie ein benutzerdefiniertes Skript hoch.
    - i. Wählen Sie die Option **Datei hochladen**.
    - ii. Navigieren Sie zu einer Datei, und laden Sie sie hoch.



- iii. Geben Sie dem Skript einen eindeutigen Namen.
  - iv. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.
  - v. Wählen Sie **Skript speichern**.
- Fügen Sie in ein benutzerdefiniertes Skript aus der Zwischenablage ein.
    - i. Wählen Sie die Option **Einfügen oder Typ** aus.
    - ii. Wählen Sie das Textfeld aus, und fügen Sie den Skripttext in das Feld ein.
    - iii. Geben Sie dem Skript einen eindeutigen Namen.
    - iv. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.
6. Wählen Sie **Skript speichern**.

## Ergebnis

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

## Ein Skript löschen

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

### Schritte

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



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

## Erstellen Sie einen benutzerdefinierten Testsuite-Haken

Sie können einen benutzerdefinierten Ausführungshaken für eine App erstellen und ihn zu Astra Control hinzufügen. Siehe [Beispiele für Testausführungshaken](#) Beispiele für Haken. Sie müssen über die Berechtigungen Eigentümer, Administrator oder Mitglied verfügen, um Testausführungshaken zu erstellen.



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

### Schritte

1. Stellen Sie sicher, dass die Funktion Ausführungshaken aktiviert ist [Aktiviert](#).
2. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
3. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
4. Wählen Sie **Hinzufügen**.

5. Im Bereich **Klettdetails**:

- a. Bestimmen Sie, wann der Haken ausgeführt werden soll, indem Sie im Dropdown-Menü \* Operation\* einen Operationstyp auswählen.
- b. Geben Sie einen eindeutigen Namen für den Haken ein.
- c. (Optional) Geben Sie alle Argumente ein, um während der Ausführung an den Haken weiterzuleiten. Drücken Sie nach jedem eingegebenen Argument die Eingabetaste, um jedes Argument aufzuzeichnen.

6. (Optional) im Bereich **Hook Filter Details** können Sie Filter hinzufügen, um zu steuern, auf welchen Behältern der Execution Hook läuft:

- a. Wählen Sie **Filter hinzufügen**.
- b. Wählen Sie in der Spalte **Hook Filtertyp** ein Attribut aus, nach dem Sie im Dropdown-Menü filtern möchten.
- c. Geben Sie in der Spalte **Regex** einen regulären Ausdruck ein, der als Filter verwendet werden soll. Astra Control verwendet den "[Regex-Syntax für regulären Ausdruck 2 \(RE2\)](#)".



Wenn Sie 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.

7. Wählen Sie anschließend **Weiter** aus.

8. Führen Sie im Bereich **Skript** einen der folgenden Schritte aus:

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

- Wählen Sie ein vorhandenes Skript aus der Liste aus.

Hiermit wird der Testsuitelink angewiesen, dieses Skript zu verwenden.

9. Wählen Sie **Weiter**.
10. Überprüfen Sie die Konfiguration der Testsuite.
11. Wählen Sie **Hinzufügen**.

## Überprüfen Sie den Status eines Testablaufanhänges

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

### Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Datenschutz** aus.
3. Wählen Sie **Snapshots** aus, um die laufenden Snapshots zu sehen, oder **Backups**, um die laufenden Backups zu sehen.

Der **Hook-Status** zeigt den Status der Ausführung Hakenlauf nach Abschluss des Vorgangs an. Sie können den Mauszeiger auf den Status bewegen, um weitere Details zu erhalten. Wenn z. B. beim Snapshot Fehler beim Ausführen von Hakenabfällen auftreten, wird beim Mauszeiger über den Hakenzustand für diesen Snapshot eine Liste mit fehlgeschlagenen Testsuitelinken 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 © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

## Markeninformationen

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