Schützen von Applikationen

Astra Control Center

NetApp
November 27, 2023

Inhalt

Schützen von Applikationen

Sicherungsübersicht

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

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

Workflow für Applikationssicherung

Anhand des folgenden Beispielworkflows können Sie Ihre Apps schützen.

[Eins] Sicherung aller Applikationen

Um sicherzustellen, dass Ihre Apps sofort geschützt sind, "Erstellen Sie ein manuelles Backup aller Apps".

[Zwei] Konfigurieren Sie für jede Applikation eine Sicherungsrichtlinie

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

[Drittens] Passen Sie die Sicherungsrichtlinien an

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

[Vier] Replizieren von Applikationen in einem Remote-Cluster

"Replizierung von Applikationen" Erstellen eines Remote-Clusters mithilfe von NetApp SnapMirror. Astra Control repliziert Snapshots in einen Remote-Cluster und bietet damit asynchrone Disaster Recovery-Funktion.

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

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

Sichern von Applikationen durch Snapshots und Backups

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

Über diese Aufgabe

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

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

Sie können die folgenden Aufgaben zum Schutz Ihrer Applikationsdaten ausführen:

- Konfigurieren einer Sicherungsrichtlinie
- Erstellen Sie einen Snapshot
- Erstellen Sie ein Backup
- Anzeigen von Snapshots und Backups
- Snapshots löschen
- Abbrechen von Backups
- Backups löschen

Konfigurieren einer Sicherungsrichtlinie

Eine Sicherungsrichtlinie sichert eine Applikation, indem Snapshots, Backups oder beides nach einem definierten Zeitplan erstellt werden. Sie können Snapshots und Backups stündlich, täglich, wöchentlich und monatlich erstellen. Außerdem können Sie die Anzahl der beizubehaltenden Kopien festlegen.

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

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.

Wenn Ihre App eine von der unterstützte Storage-Klasse verwendet `ontap-nas-economy` Treiber, Schutzrichtlinien können nicht verwendet werden. Migrieren Sie zu einer von Astra Control unterstützten Storage-Klasse, um Backups und Snapshots zu planen.

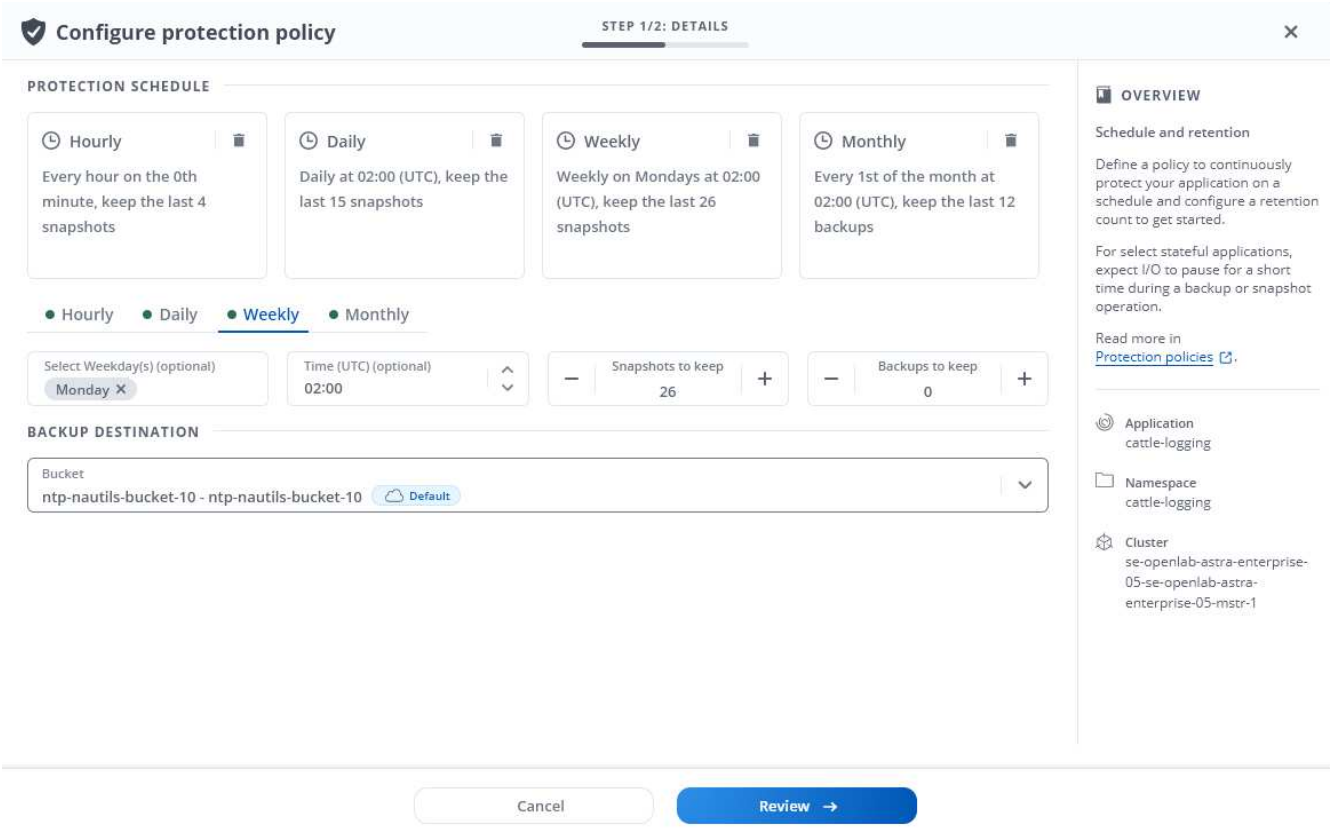
Schritte

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

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

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

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



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

Ergebnis

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

Erstellen Sie einen Snapshot

Sie können jederzeit einen On-Demand-Snapshot erstellen.

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

Schritte

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

Ergebnis

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

Erstellen Sie ein Backup

Sie können eine App auch jederzeit sichern.

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

> 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. Backups für Applikationen, die von der gesichert werden `ontap-nas-economy` Die App ist nicht verfügbar, bis der Backup-Vorgang abgeschlossen ist.

Schritte

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

Ergebnis

Astra Control erstellt ein Backup der App.

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

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

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

Anzeigen von Snapshots und Backups

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

Schritte

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

   Die Snapshots werden standardmäßig angezeigt.
3. Wählen Sie **Backups**, um die Liste der Backups anzuzeigen.

Snapshots löschen

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

Sie können keinen Snapshot löschen, der derzeit repliziert wird.

Schritte

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

Ergebnis

Astra Control löscht den Snapshot.

Abbrechen von Backups

Sie können ein gerade einlaufenden Backup abbrechen.

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

Schritte

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

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

Backups löschen

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

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

Schritte

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

Ergebnis

Astra Control löscht das Backup.

Wiederherstellung von Applikationen

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

Über diese Aufgabe

- **Schützen Sie Ihre Anwendungen zuerst**: Es wird dringend empfohlen, dass Sie einen Snapshot oder ein Backup Ihrer Anwendung vor der Wiederherstellung machen. Dadurch können Sie den Snapshot oder die Datensicherung klonen, wenn die Wiederherstellung nicht erfolgreich war.
- **Zieldatenträger prüfen**: Wenn Sie eine andere Speicherklasse wiederherstellen, stellen Sie sicher, dass die Speicherklasse den gleichen persistenten Zugriffsmodus für Volumes verwendet (z. B. ReadWriteMany). Der Wiederherstellungsvorgang schlägt fehl, wenn der Zugriffsmodus des Ziel-persistenten Volumes anders ist. Wenn das persistente Quell-Volume beispielsweise den RWX-Zugriffsmodus verwendet, wählen Sie eine Ziel-Storage-Klasse aus, die RWX nicht bereitstellen kann, wie z. B. Azure Managed Disks, AWS EBS, Google Persistent Disk oder `ontap-san`Wird dazu führen, dass der Wiederherstellungsvorgang fehlschlägt. Weitere Informationen zu den Zugriffsmodi für persistente Volumes finden Sie im "Kubernetes" Dokumentation.

- **Planung des Platzbedarfs**: Wenn Sie eine in-Place-Wiederherstellung einer Applikation durchführen, die NetApp ONTAP Storage nutzt, kann sich der von der wiederhergestellten Applikation genutzte Speicherplatz verdoppeln. Nachdem Sie eine in-Place-Wiederherstellung durchgeführt haben, entfernen Sie alle unerwünschten Snapshots aus der wiederhergestellten Applikation, um Speicherplatz freizugeben.
- **(nur OpenShift-Cluster) Richtlinien hinzufügen**: Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder Kubernetes-Namespace) eine SecurityContext-UID zugewiesen. Um Astra Control Center zum Schutz Ihrer App zu aktivieren und die App in ein anderes Cluster oder Projekt in OpenShift zu verschieben, müssen Sie Richtlinien hinzufügen, mit denen die App als beliebige UID ausgeführt werden kann. Als Beispiel erteilen die folgenden OpenShift-CLI-Befehle der WordPress-App die entsprechenden Richtlinien.

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

- **Helm bereitgestellte Apps**: Apps, die mit Helm 3 (oder von Helm 2 auf Helm 3 aktualisiert) bereitgestellt werden, werden vollständig unterstützt. Mit Helm 2 implementierte Apps werden nicht unterstützt.

> Die Durchführung einer in-Place-Wiederherstellung in einer Anwendung, in der Ressourcen mit einer anderen Anwendung geteilt werden, kann unbeabsichtigte Ergebnisse haben. Alle Ressourcen, die von den Applikationen gemeinsam genutzt werden, werden ersetzt, wenn eine in-Place-Wiederherstellung für eine der Applikationen durchgeführt wird. Weitere Informationen finden Sie unter bei der Ressourcen mit einer anderen App geteilt werden,Dieses Beispiel.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie im Menü Optionen in der Spalte Aktionen die Option **Wiederherstellen** aus.
3. Wählen Sie den Wiederherstellungstyp aus:
   - **Wiederherstellen auf ursprünglichen Namespaces**: Verwenden Sie dieses Verfahren, um die App an Ort und Stelle auf dem ursprünglichen Cluster wiederherzustellen.

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

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

     ii. Wählen Sie **Weiter**.

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

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

Mit diesem Verfahren können Sie eine der beiden Optionen verwenden Zu einer Storage-Klasse, die von unterstützt wird `ontap-nas` Auf demselben Cluster **ODER** kopieren Sie die App auf ein anderes Cluster mit einer Storage-Klasse, die vom unterstützt wird `ontap-nas-economy` Treiber.

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

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

iii. Geben Sie für jeden mit der App verknüpften Quell-Namespace einen Ziel-Namespace ein.

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

iv. Wählen Sie **Weiter**.

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

vi. Wählen Sie **Weiter**.

vii. Folgenden Optionen wählbar:

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

viii. Wählen Sie **Weiter**.

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

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

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

Ergebnis

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

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

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

Filtern Sie Ressourcen während einer Anwendungswiederherstellung

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

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

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

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

Schritte

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

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

2. Konfigurieren Sie die Filterregel:

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

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

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

   b. (Optional) Geben Sie einen Ressourcennamen ein.

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

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

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

      i. (Optional) **Gruppe**: Wählen Sie aus der Dropdown-Liste die Kubernetes API-Gruppe aus.

      ii. **Kind**: Wählen Sie aus der Dropdown-Liste das Objektschema für den Kubernetes-Ressourcentyp aus, der im Filter verwendet werden soll.

      iii. **Version**: Wählen Sie die Kubernetes API Version.

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

4. Wählen Sie **Hinzufügen**.

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

Migrieren Sie von ontap-nas-Storage der Wirtschaftlichkeit auf ontap-nas-Storage

Sie können eine Astra Managementkonsole verwenden "Applikations-Restore" Oder "Anwendungsklon" Operation zum Migrieren von Applikations-Volumes von einer Storage-Klasse, die von unterstützt wird `ontap-nas-economy`, Die begrenzte Anwendungsschutzoptionen erlaubt, auf eine von unterstützte Storage-Klasse `ontap-nas` Mit der gesamten Palette der Astra Control Schutzoptionen. Der Klon- oder Wiederherstellungsvorgang migriert Qtree-basierte Volumes, die einen verwenden `ontap-nas-economy`

Back-End zu Standard-Volumes, die von gesichert werden `ontap-nas`. Volumes erstellen, unabhängig davon, ob sie sich befinden `ontap-nas-economy` Nur gesichert oder gemischt, wird in die Ziel-Storage-Klasse migriert. Nach Abschluss der Migration sind die Schutzoptionen nicht mehr begrenzt.

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

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

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

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

Replizierung von Applikationen zwischen Storage Back-Ends mithilfe von SnapMirror Technologie

Mithilfe von Astra Control können Sie mit den asynchronen Replizierungsfunktionen der NetApp SnapMirror Technologie Business Continuity für Ihre Applikationen erzielen: Mit Low-RPO (Recovery Point Objective) und Low-RTO (Recovery Time Objective). Nach der Konfiguration können Ihre Applikationen auf diese Weise Daten und Applikationsänderungen von einem Storage-Back-End auf ein anderes replizieren, sowohl im selben Cluster als auch zwischen verschiedenen Clustern.

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

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

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

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

replizieren.

> Sie können gleichzeitig eine andere App in die entgegengesetzte Richtung replizieren. So können beispielsweise Applikationen A, B und C von Datacenter 1 nach Datacenter 2 repliziert werden. Applikationen X, Y und Z können von Datacenter 2 zu Datacenter 1 repliziert werden.

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

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

Replikationsvoraussetzungen

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

- **ONTAP-Cluster**:
  - **Astra Trident**: Astra Trident Version 22.10 oder höher muss sowohl auf den Quell- als auch auf den Ziel-Kubernetes-Clustern vorhanden sein, die ONTAP als Backend nutzen.
  - **Lizenzen**: Asynchrone Lizenzen von ONTAP SnapMirror, die das Datensicherungspaket verwenden, müssen sowohl auf den Quell- als auch auf den Ziel-ONTAP-Clustern aktiviert sein. Siehe "Übersicht über die SnapMirror Lizenzierung in ONTAP" Finden Sie weitere Informationen.
- **Peering**:
  - **Cluster und SVM**: Die ONTAP Speicher-Back-Ends müssen aktiviert werden. Siehe "Übersicht über Cluster- und SVM-Peering" Finden Sie weitere Informationen.

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

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

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

  - **Verwaltete Cluster**: Folgende Cluster müssen von Astra Control hinzugefügt und verwaltet werden, idealerweise an verschiedenen Ausfalldomänen oder Standorten:
    - Quell-Kubernetes-Cluster
    - Kubernetes Ziel-Cluster
    - Zugeordnete ONTAP-Cluster
  - **Benutzerkonten**: Wenn Sie ein ONTAP-Speicher-Backend zu Astra Control Center hinzufügen, wenden Sie die Anmeldeinformationen des Benutzers mit der Rolle "admin" an. Diese Rolle verfügt

über Zugriffsmethoden `http` Und `ontapi` Sowohl auf ONTAP Quell- als auch auf Ziel-Clustern aktiviert. Siehe "Managen von Benutzerkonten in der ONTAP Dokumentation" Finden Sie weitere Informationen.

- **Astra Trident / ONTAP Konfiguration**: Astra Control Center erfordert, dass Sie mindestens ein Storage-Backend konfigurieren, das sowohl die Replikation für die Quell- als auch für Ziel-Cluster unterstützt. Wenn die Quell- und Ziel-Cluster identisch sind, sollte die Zielanwendung ein anderes Speicher-Back-End als die Quellanwendung verwenden, um die beste Ausfallsicherheit zu erreichen.

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

Richten Sie eine Replikationsbeziehung ein

Die Einrichtung einer Replikationsbeziehung umfasst Folgendes:

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

Schritte

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

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

5. Wählen Sie **Weiter**, lesen Sie die Zusammenfassung und wählen Sie **Speichern**.

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

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

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

   Der Snapshot-Name verwendet das Format von `replication-schedule-<string>`. Astra Control behält den letzten Snapshot bei, der für die Replizierung verwendet wurde. Alle älteren Replikations-Snapshots werden nach erfolgreichem Abschluss der Replikation gelöscht.

Ergebnis

Dadurch wird die Replikationsbeziehung erstellt.

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

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

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

Beispiel:
Normal

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

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

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

Schritte

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

Ergebnis

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

- Die Zielanwendung wird basierend auf dem zuletzt replizierten Snapshot gestartet.
- Das Quellcluster und die App (falls betriebsbereit) werden nicht angehalten und werden weiterhin ausgeführt.
- Der Replikationsstatus ändert sich zu „Failover“ und dann zu „Failover“, wenn er abgeschlossen ist.
- Die Schutzrichtlinie der Quell-App wird auf Basis der zum Zeitpunkt des Failovers auf der Quell-App vorhandenen Zeitpläne in die Ziel-App kopiert.
- Wenn in der Quell-App mindestens eine Ausführungshaken nach der Wiederherstellung aktiviert ist, werden diese Ausführungshaken für die Ziel-App ausgeführt.
- Astra Control zeigt die App sowohl auf den Quell- und Ziel-Clustern und deren jeweiligen Zustand.

Resynchronisierung einer fehlgeschlagenen Überreplikation

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

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

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

Schritte

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

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

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

Ergebnis

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

Replizierung der Applikation wird rückgängig gemacht

Dies ist der geplante Vorgang, mit dem die Applikation auf das Ziel-Storage Back-End verschoben und gleichzeitig weiterhin zurück auf das ursprüngliche Quell-Storage Back-End repliziert werden soll. Astra Control stoppt die Quellapplikation und repliziert die Daten zum Ziel, bevor ein Failover zur Ziel-App durchgeführt wird.

In dieser Situation tauschen Sie Quelle und Ziel aus.

Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie die Registerkarte **Data Protection** > **Replication** aus.
3. Wählen Sie im Menü Aktionen die Option **Reverse Replication**.
4. Überprüfen Sie auf der Seite „Replikation umkehren“ die Informationen und wählen Sie zum Fortfahren **Replikation umkehren** aus.

Ergebnis

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

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

Führen Sie ein Failback von Anwendungen auf das ursprüngliche Quellcluster durch

Mit Astra Control können Sie nach einem Failover-Vorgang mithilfe der folgenden Sequenz von Vorgängen „Failback“ erreichen. In diesem Workflow zur Wiederherstellung der ursprünglichen Replikationsrichtung repliziert (synchronisiert) Astra Control alle Anwendungsänderungen zurück zur ursprünglichen Quellanwendung, bevor die Replikationsrichtung umkehrt.

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

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

Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie die Registerkarte **Data Protection** > **Replication** aus.

3. Wählen Sie im Menü Aktionen die Option **Resync**.
4. Wählen Sie für einen Failback-Vorgang die Failoveranwendung als Quelle für den Resync-Vorgang aus (unter Beibehaltung der nach dem Failover geschriebenen Daten).
5. Geben Sie zur Bestätigung „Resynchronisieren“ ein.
6. Wählen Sie **Ja, Resynchronisierung**, um den Vorgang abzuschließen.
7. Nach Abschluss der Resynchronisierung wählen Sie im Menü Aktionen auf der Registerkarte Data Protection > Replication die Option **Replikation umkehren** aus.
8. Überprüfen Sie auf der Seite „Replikation umkehren“ die Informationen und wählen Sie **Replikation umkehren**.

Ergebnis

Dies kombiniert die Ergebnisse aus den „Resync“- und „umgekehrten Beziehungs“-Vorgängen, um die Applikation auf dem ursprünglichen Quell-Cluster online zu schalten und die Replizierung wieder auf das ursprüngliche Ziel-Cluster zu übertragen.

Löschen einer Replikationsbeziehung für Anwendungen

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

Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie die Registerkarte **Data Protection** > **Replication** aus.
3. Wählen Sie im Feld Anwendungsschutz oder im Beziehungsdiagramm **Replikationsbeziehung löschen** aus.

Ergebnis

Die folgenden Aktionen treten beim Löschen einer Replikationsbeziehung auf:

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

Status des Integritätsstatus der Replikationsbeziehung und Lebenszyklusstatus der Beziehungen

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

Integritätsstatus von Replikationsbeziehungen

Die folgenden Status geben den Zustand der Replikationsbeziehung an:

- **Normal**: Die Beziehung wird entweder aufgebaut oder hat sich etabliert, und der letzte Snapshot wurde erfolgreich übertragen.
- **Warnung**: Die Beziehung wird entweder überschlagen oder ist gescheitert (und somit schützt die Quell-

App nicht mehr).

- * Kritisch*
  - Die Beziehung wird erstellt oder fehlgeschlagen, und der letzte Versuch der Abstimmung ist fehlgeschlagen.
  - Die Beziehung wird hergestellt, und der letzte Versuch, die Hinzufügung eines neuen PVC zu vereinbaren, ist gescheitert.
  - Die Beziehung wird hergestellt (so dass ein erfolgreicher Snapshot repliziert wurde und Failover möglich ist), aber der aktuelle Snapshot ist fehlgeschlagen oder konnte nicht repliziert werden.

Lebenszyklusstatus der Replikation

Die folgenden Zustände spiegeln die verschiedenen Phasen des Replikationslebenszyklus wider:

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

Klonen und Migrieren von Applikationen

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

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

Bevor Sie beginnen

- **Zieldatenträger prüfen**: Wenn Sie in eine andere Speicherklasse klonen, stellen Sie sicher, dass die Speicherklasse den gleichen persistenten Zugriffsmodus für Volumes verwendet (z. B. ReadWriteMany). Der Klonvorgang schlägt fehl, wenn der Zugriffsmodus des persistenten Volume-Ziels anders ist. Wenn das persistente Quell-Volume beispielsweise den RWX-Zugriffsmodus verwendet, wählen Sie eine Ziel-Storage-Klasse aus, die RWX nicht bereitstellen kann, wie z. B. Azure Managed Disks, AWS EBS, Google Persistent Disk oder `ontap-san`, Führt dazu, dass der Klonvorgang fehlschlägt. Weitere Informationen zu den Zugriffsmodi für persistente Volumes finden Sie im "Kubernetes" Dokumentation.
- Um Applikationen in einem anderen Cluster zu klonen, müssen Sie sicherstellen, dass die Cloud-Instanzen, die die Quell- und Ziel-Cluster enthalten (wenn sie nicht identisch sind), einen Standard-Bucket haben. Für jede Cloud-Instanz müssen Sie einen Standard-Bucket zuweisen.
- Während Klonvorgängen müssen Applikationen, die eine Ressource oder Webhooks der ProgresClass benötigen, nicht über die Ressourcen verfügen, die bereits auf dem Ziel-Cluster definiert sind.

> Beim Klonen von Applikationen in OpenShift-Umgebungen muss das Astra Control Center OpenShift erlauben, Volumes anzuhängen und die Eigentümerschaft von Dateien zu ändern. Daher müssen Sie eine ONTAP Volume Export-Richtlinie konfigurieren, damit diese Vorgänge möglich sind. Sie können dies mit folgenden Befehlen tun:
>
> 1. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sys`
> 2. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -anon 65534`

Einschränkungen beim Klonen

- **Explicit Storage class**: Wenn Sie eine App mit einer explizit eingestellten Speicherklasse bereitstellen und die App klonen müssen, muss das Ziel-Cluster über die ursprünglich angegebene Speicherklasse verfügen. Das Klonen einer Applikation mit einer explizit festgelegten Storage-Klasse auf ein Cluster ohne dieselbe Storage-Klasse schlägt fehl.
- **storage-Klasse mit unterstützung der ontap-nas-Wirtschaft**: Wenn Ihre Applikation eine Storage-Klasse verwendet, die von der unterstützt wird `ontap-nas-economy` Treiber, der Backup-Teil eines Klonvorgangs ist störend. Die Quellanwendung ist erst nach Abschluss der Sicherung verfügbar. Der Wiederherstellungsteil des Klonvorgangs ist unterbrechungsfrei.
- **Klone und Benutzerbeschränkungen**: Jeder Mitgliedsbenutzer mit Namespace-Beschränkungen durch Namespace-Name/ID oder durch Namespace-Labels kann eine Anwendung in einem neuen Namespace im selben Cluster oder einem anderen Cluster im Konto ihres Unternehmens klonen oder wiederherstellen. Derselbe Benutzer kann jedoch nicht auf die geklonte oder wiederhergestellte Anwendung im neuen Namespace zugreifen. Nachdem ein neuer Namespace durch einen Klon- oder Wiederherstellungsvorgang erstellt wurde, kann der Account-Administrator/-Eigentümer das Mitglied-Benutzerkonto bearbeiten und Rolleneinschränkungen für den betroffenen Benutzer aktualisieren, um dem neuen Namespace Zugriff zu gewähren.
- **Klone verwenden Standard-Buckets**: Während einer App-Sicherung oder App-Wiederherstellung können Sie optional eine Bucket-ID angeben. Ein Applikationsklonvorgang verwendet jedoch immer den definierten Standard-Bucket. Es besteht keine Möglichkeit, die Buckets für einen Klon zu ändern. Wenn Sie die Kontrolle darüber haben möchten, welcher Bucket verwendet wird, können Sie entweder "Ändern Sie

den Bucket-Standard" Oder machen Sie ein "Backup" Gefolgt von A "Wiederherstellen" Separat.

- **Mit Jenkins CI**: Wenn Sie eine vom Betreiber implementierte Instanz von Jenkins CI klonen, müssen Sie die persistenten Daten manuell wiederherstellen. Dies ist eine Einschränkung des Bereitstellungsmodells der Applikation.
- **Mit S3 Buckets**: S3 Buckets im Astra Control Center melden keine verfügbare Kapazität. Bevor Sie Backups oder Klonanwendungen durchführen, die von Astra Control Center gemanagt werden, sollten Sie die Bucket-Informationen im ONTAP oder StorageGRID Managementsystem prüfen.
- **Mit einer bestimmten Version von PostgreSQL**: App-Klone innerhalb desselben Clusters schlagen mit dem Bitnami PostgreSQL 11.5.0-Chart konsequent fehl. Um erfolgreich zu klonen, verwenden Sie eine frühere oder höhere Version des Diagramms.

OpenShift-Überlegungen

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

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

Schritte

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

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

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

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

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

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

Ergebnis

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

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

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

Anwendungsausführungshaken verwalten

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

Arten von Ausführungshaken

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

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

Filter für Testausführungshaken

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

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

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

Wichtige Hinweise zu benutzerdefinierten Testausführungshaken

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

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

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

- Für Ad-hoc-Datenschutzvorgänge werden alle Hook-Ereignisse generiert und im Ereignisprotokoll der Seite **Aktivität** gespeichert. Bei geplanten Datenschutzvorgängen werden jedoch nur Hook-Failure-Ereignisse im Ereignisprotokoll aufgezeichnet (Ereignisse, die von den geplanten Datenschutzvorgängen selbst generiert werden, werden noch aufgezeichnet).
- Wenn Astra Control Center einen Failover über eine replizierte Quell-App an die Ziel-App ausführt, werden nach dem Failover alle für die Quell-App aktivierten Ausführungs-Hooks für die Ziel-App ausgeführt.

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

Ausführungsreihenfolge

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

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

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

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

Ein Beispiel für diese Konfiguration finden Sie in Szenario 2 aus der Tabelle in ob ein Haken läuft.

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

Bestimmen Sie, ob ein Haken läuft

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

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

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

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

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

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

Szenario	Betrieb	Vorhandener Snapshot	Vorhandenes Backup	Namespace	Cluster	Snapshot Hooks laufen	Backup Hooks laufen	Hooks Run wiederherstellen	Failover Hooks werden ausgeführt
8	Wiederherstellen	N	Y	Vorhanden	Gleich	N	N	Y	N
9	Snapshot	K. A.	K. A.	K. A.	K. A.	Y	K. A.	K. A.	N
10	Backup	N	K. A.	K. A.	K. A.	Y	Y	K. A.	N
11	Backup	Y	K. A.	K. A.	K. A.	N	N	K. A.	N
12	Failover	Y	K. A.	Durch Replikation erstellt	Anders	N	N	N	Y
13	Failover	Y	K. A.	Durch Replikation erstellt	Gleich	N	N	N	Y

Beispiele für Testausführungshaken

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

Vorhandene Testsuiten anzeigen

Sie können vorhandene benutzerdefinierte Testsuiten für eine App anzeigen.

Schritte

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

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

Vorhandene Skripte anzeigen

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

Schritte

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

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

Fügen Sie ein Skript hinzu

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

Schritte

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

Ergebnis

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

Ein Skript löschen

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

Schritte

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

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

Erstellen Sie einen benutzerdefinierten Testsuite-Haken

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

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

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

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

6. Wählen Sie anschließend **Weiter** aus.
7. Führen Sie im Bereich **Script** einen der folgenden Schritte aus:
   - Fügen Sie ein neues Skript hinzu.
     i. Wählen Sie **Hinzufügen**.
     ii. Führen Sie einen der folgenden Schritte aus:

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

◦ Wählen Sie ein vorhandenes Skript aus der Liste aus.

Hiermit wird der Testsuitelink angewiesen, dieses Skript zu verwenden.

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

Überprüfen Sie den Status eines Testablaufanhängees

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

Schritte

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

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

Skriptverwendung anzeigen

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

Schritte

1. Wählen Sie **Konto**.

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

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

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

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

Bearbeiten Sie einen Testsuite-Haken

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

Schritte

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

Deaktivieren Sie einen Testsuite-Haken

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

Schritte

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

Löschen Sie einen Testsuite-Haken

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

Schritte

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

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

Finden Sie weitere Informationen

- "NetApp Verda GitHub Projekt"

Astra Control Center kann über Astra Control Center geschützt werden

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

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

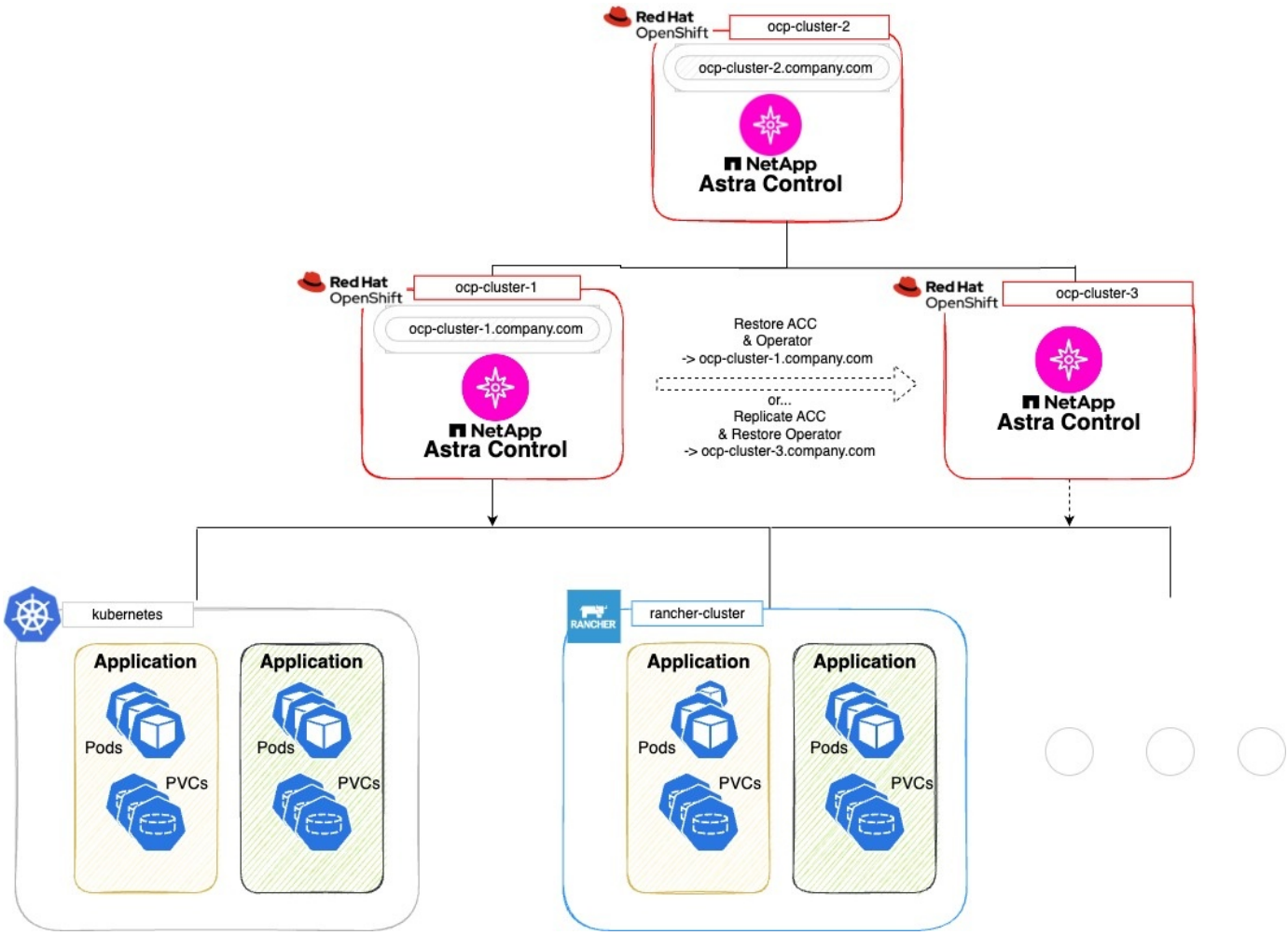
Bevor Sie beginnen

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

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

Über diese Aufgabe

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



In dieser Beispielkonfiguration wird Folgendes angezeigt:

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

verwendet.

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

Nicht im Diagramm dargestellt:

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

Schritt 1 Option: Backup und Wiederherstellung von Astra Control Center

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

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

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

Bevor Sie beginnen

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

Schritte

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

g. Wählen Sie diese Einträge aus, und wählen Sie **Hinzufügen**:
   - Etikettenauswahl: ACC-crds
   - Gruppe: Apiextensions.k8s.io
   - Stand: v1
   - Art: CustomResourceDefinition

h. Bestätigen Sie die Anwendungsinformationen.

i. Wählen Sie **Definieren**.

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

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

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

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

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

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

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

Antwort:

```
NAME  UUID                                   VERSION    ADDRESS
READY
astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.07.0-24 ocp-cluster-
1.company.com           True
```

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

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

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

ii. Speichern Sie die Konfiguration.

iii. Bestätigen Sie, dass die Adresse aktualisiert wurde:

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

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

Schritt 1: Astra Control Center mit Replizierung schützen

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

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

Bevor Sie beginnen

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

Schritte

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

Astra Control Center-Instanz:

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

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

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

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

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

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

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

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

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

3. Back-Ends für Replikation konfigurieren:

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

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

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

4. Replikation konfigurieren:

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

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

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

d. Wählen Sie die Storage-Klasse aus.

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

f. Ändern Sie bei Bedarf die Replizierungshäufigkeit.

g. Wählen Sie **Weiter**.

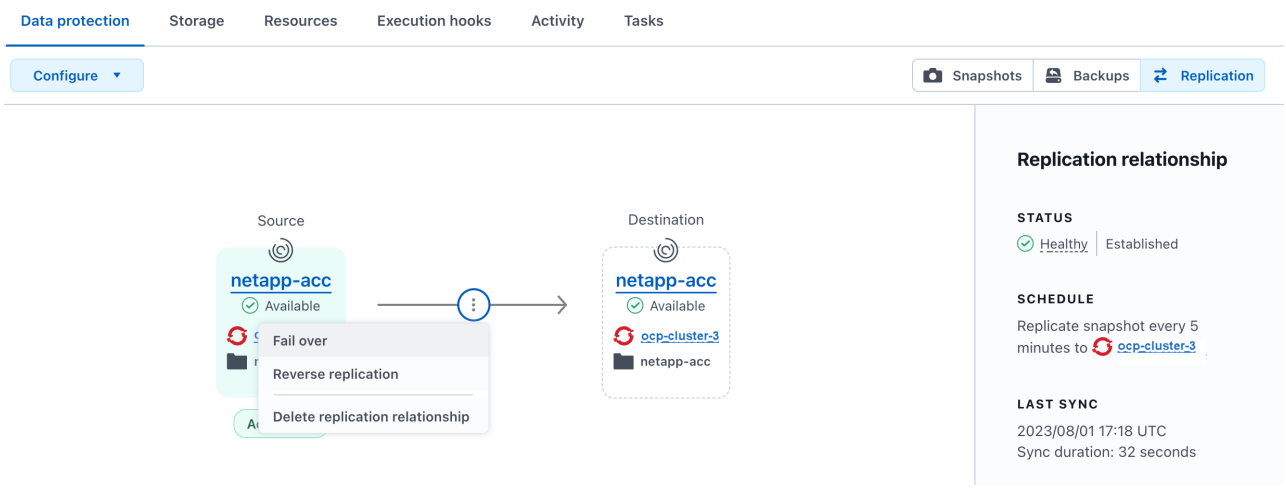
h. Bestätigen Sie, dass die Konfiguration korrekt ist, und wählen Sie **Speichern**.

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

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

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

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



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

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

6. Schließen Sie die Failover-Konfiguration ab:

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

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

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

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

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

      ii. Speichern Sie die Konfiguration.

      iii. Bestätigen Sie, dass die Adresse aktualisiert wurde:

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

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

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

   Erforderliche Traefik CRDS:

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

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

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

   iv. Traefik neu starten:

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

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

Schritt 2: Wiederherstellen des Bedieners des Astra Control Centers

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

Schritte

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

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

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

Ergebnis

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

Fehlerbehebung

Bestimmen Sie den Systemzustand und ob die Schutzprozesse erfolgreich waren.

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

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

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

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

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

  Antwort:

  ```
  NAME  UUID                                   VERSION    ADDRESS
  READY
  astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.07.0-24 ocp-cluster-
  1.company.com           True
  ```

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

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

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