Schützen von Applikationen

Astra Control Center

NetApp
November 21, 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" Zu einem Remote-Cluster mit NetApp SnapMirror Technologie 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 UI oder verwenden "Die Astra Control API" Um Anwendungen zu schützen.

Wenn Sie Helm zur Implementierung von Apps verwenden, erfordert Astra Control Center Helm Version 3. Das Management und Klonen von mit Helm 3 bereitgestellten Apps (oder ein Upgrade von Helm 2 auf Helm 3) werden vollständig unterstützt. Mit Helm 2 implementierte Apps werden nicht unterstützt.

Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder dem Kubernetes-Namespace) eine SecurityContext-UID zugewiesen. Um Astra Control Center zum Schutz Ihrer App zu aktivieren und die App in ein anderes Cluster oder Projekt in OpenShift zu verschieben, müssen Sie Richtlinien hinzufügen, mit denen die App als beliebige UID ausgeführt werden kann. Als Beispiel erteilen die folgenden OpenShift-CLI-Befehle der WordPress-App die entsprechenden Richtlinien.

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

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

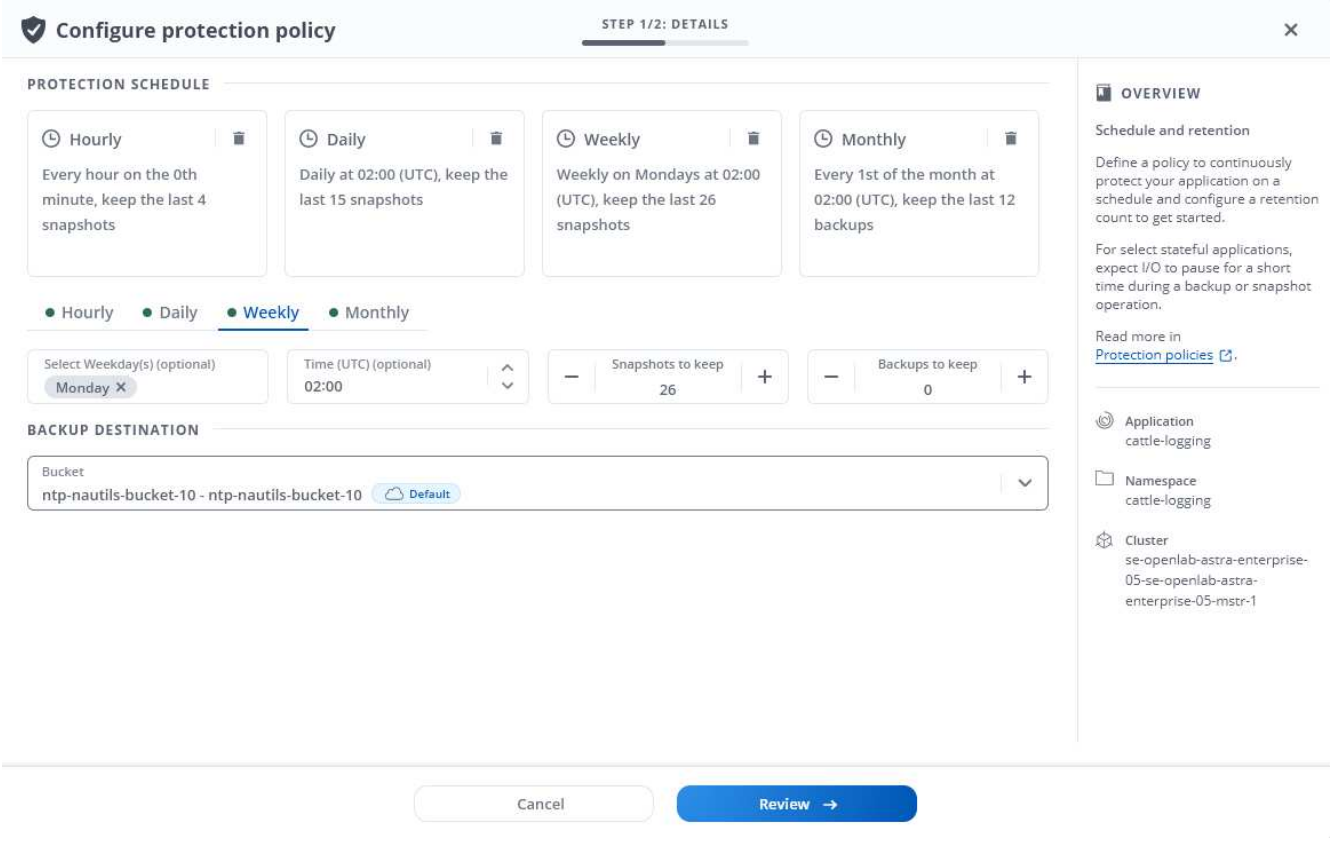
Eine Sicherungsrichtlinie sichert eine Applikation, indem Snapshots, Backups oder beides nach einem definierten Zeitplan erstellt werden. Sie können Snapshots und Backups stündlich, täglich, wöchentlich und monatlich erstellen. Außerdem können Sie die Anzahl der beizubehaltenden Kopien festlegen. Eine Sicherungsrichtlinie kann beispielsweise wöchentliche Backups und tägliche Snapshots erstellen und die Backups und Snapshots einen Monat lang aufbewahren. Wie oft Sie Snapshots und Backups erstellen und wie lange Sie sie behalten, hängt von den Anforderungen Ihres Unternehmens ab.

Schritte

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

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

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



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

Ergebnis

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

Erstellen Sie einen Snapshot

Sie können jederzeit einen On-Demand-Snapshot erstellen.

Schritte

1. Wählen Sie **Anwendungen**.
2. Wählen Sie 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 **Review**.
4. Überprüfen Sie die Snapshot-Zusammenfassung und wählen Sie **Snapshot**.

Ergebnis

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

Erstellen Sie ein Backup

Sie können eine App auch jederzeit sichern.

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

Schritte

1. Wählen Sie **Anwendungen**.
2. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für die gewünschte App die Option **Backup** 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 ein Ziel für das Backup aus der Liste der Speicher-Buckets aus.
6. Wählen Sie **Bewertung**.
7. Überprüfen Sie die Backup-Zusammenfassung und wählen Sie **Backup**.

Ergebnis

Astra Control Center erstellt ein Backup der App.

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

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

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

Anzeigen von Snapshots und Backups

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

Schritte

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

   Die Snapshots werden standardmäßig angezeigt.

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

Snapshots löschen

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

Eine Snapshot Kopie, die derzeit repliziert wird, kann nicht gelöscht werden.

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer 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 Center löscht den Snapshot.

Abbrechen von Backups

Sie können ein gerade einlaufenden Backup abbrechen.

Um ein Backup abzubrechen, muss sich das Backup im laufenden Zustand befinden. Sie können ein Backup, das sich im Status „Ausstehend“ befindet, nicht abbrechen.

Schritte

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

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

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 Center löscht das Backup.

Wiederherstellung von Applikationen

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

Über diese Aufgabe

- Es wird dringend empfohlen, einen Snapshot von Ihrer Anwendung zu erstellen oder zu sichern, bevor Sie sie wiederherstellen. Dadurch können Sie den Snapshot oder die Datensicherung klonen, wenn die Wiederherstellung nicht erfolgreich war.
- Wenn Sie Helm zur Implementierung von Apps verwenden, erfordert Astra Control Center Helm Version 3. Das Management und Klonen von mit Helm 3 bereitgestellten Apps (oder ein Upgrade von Helm 2 auf Helm 3) werden vollständig unterstützt. Mit Helm 2 implementierte Apps werden nicht unterstützt.
- Wenn Sie ein anderes Cluster wiederherstellen, stellen Sie sicher, dass das Cluster denselben Zugriffsmodus für persistente Volumes verwendet (z. B. ReadWriteManche). Der Wiederherstellungsvorgang schlägt fehl, wenn der Zugriffsmodus des Ziel-persistenten Volumes anders ist.
- Jeder Mitgliedsbenutzer mit Namespace-Einschränkungen nach Namespace-Name/ID oder durch Namespace-Bezeichnungen kann eine App in einem neuen Namespace auf demselben 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.
- Wenn Sie ein Projekt zum Hosten einer App auf einem OpenShift-Cluster erstellen, wird dem Projekt (oder dem Kubernetes-Namespace) eine SecurityContext-UID zugewiesen. Um Astra Control Center zum Schutz Ihrer App zu aktivieren und die App in ein anderes Cluster oder Projekt in OpenShift zu verschieben, müssen Sie Richtlinien hinzufügen, mit denen die App als beliebige UID ausgeführt werden kann. Als Beispiel erteilen die folgenden OpenShift-CLI-Befehle der WordPress-App die entsprechenden Richtlinien.

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

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer App aus.
2. Wählen Sie **Datenschutz**.
3. Wenn Sie von einem Snapshot wiederherstellen möchten, lassen Sie das **Snapshots** -Symbol ausgewählt. Andernfalls wählen Sie das Symbol **Backups** aus, um aus einem Backup wiederherzustellen.
4. Wählen Sie im Menü Optionen in der Spalte **Aktionen** für den Snapshot oder die Datensicherung, aus der Sie wiederherstellen möchten, **Anwendung wiederherstellen** aus.
5. **Restore Details**: Geben Sie Details für die wiederhergestellte App an. Standardmäßig werden das aktuelle Cluster und der aktuelle Namespace angezeigt. Lassen Sie diese Werte intakt, um eine App an Ort und

Stelle wiederherzustellen, die die App auf eine frühere Version von selbst zurücksetzt. Ändern Sie diese Werte, wenn Sie die Daten in einem anderen Cluster oder Namespace wiederherstellen möchten.

- Geben Sie einen Namen und einen Namespace für die App ein.
- Wählen Sie das Ziel-Cluster für die App aus.
- Wählen Sie **Bewertung**.

> 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.

6. **Zusammenfassung wiederherstellen**: Überprüfen Sie die Details über die Wiederherstellungsaktion, geben Sie "wiederherstellen" ein und wählen Sie **Wiederherstellen**.

Ergebnis

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

> Nach einer Datensicherungsoperation (Klonen, Backup, Restore) und einer anschließenden Anpassung des persistenten Volumes beträgt die Verzögerung bis zu zwanzig Minuten, bevor die neue Volume-Größe in der 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.

Replizieren von Applikationen auf einem Remote-System mit 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). Sobald Ihre Applikationen konfiguriert sind, können sie Daten und Applikationsänderungen von einem Cluster auf ein anderes replizieren.

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

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

- 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 Applikation (auf dem anderen Cluster oder Standort ausgeführt) 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-Betrieb einer replizierten App 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

Siehe "Replikationsvoraussetzungen" Bevor Sie beginnen.

Richten Sie eine Replikationsbeziehung ein

Die Einrichtung einer Replikationsbeziehung umfasst Folgendes, die die Replikationsrichtlinie enthält;

- Wählen Sie, wie häufig Astra Control einen App Snapshot erstellen soll (einschließlich der Kubernetes-Ressourcen der Applikation und der Volume-Snapshots für die einzelnen Applikations-Volumes).
- Auswahl des Replizierungszeitplans (einschließlich Kubernetes-Ressourcen und persistente Volume-Daten)
- Einstellen der Zeit, die für die Erstellung des Snapshots verwendet werden soll

Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie auf der Seite Anwendung die Registerkarte **Datenschutz** > **Replikation** aus.
3. Wählen Sie auf der Registerkarte Data Protection > Replication die Option **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
   - **Zielspeicherklasse**: Wählen Sie die Speicherklasse aus, die die gekoppelte SVM auf dem Ziel-ONTAP-Cluster verwendet.
   - **Replikationstyp**: "Asynchron" ist derzeit der einzige verfügbare Replikationstyp.
   - **Ziel-Namespace**: Geben Sie einen neuen oder bestehenden Ziel-Namespace für das Ziel-Cluster ein.

     > Alle in Konflikt stehenden Ressourcen im ausgewählten Namespace werden überschrieben.

- **Frequenz der Replikation**: Legen Sie fest, wie oft Astra Control einen Snapshot machen und ihn an sein Ziel replizieren soll.
- **Offset**: Stellen Sie die Anzahl der Minuten von der Stunde her, die Sie möchten, dass Astra Control einen Schnappschuss machen soll. Möglicherweise möchten Sie einen Offset verwenden, sodass er nicht mit anderen geplanten Vorgängen übereinstimmt. Wenn Sie beispielsweise den Snapshot alle 5 Minuten ab 10:02 Uhr aufnehmen möchten, geben Sie als Offset-Minuten „02“ ein. Das Ergebnis sind 10:02, 10:07, 10:12 usw.

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**.

   Der Snapshot-Name verwendet das Format „Replication-Schedule-<string>“. Astra Control behält den letzten Snapshot, der für die Replizierung verwendet wurde. Alle älteren Replizierungs-Snapshots werden nach 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.
- Ersten applikationskonsistenten Snapshot
- Legt mithilfe des ersten Snapshots die SnapMirror Beziehung für persistente Volumes fest

Auf der Seite Datensicherung werden der Status und der Status der Replikationsbeziehung angezeigt: <Status> <Lebenszyklus der Beziehung>

Zum Beispiel: Normal

Weitere Informationen zu Replikationsstatus und -Status finden Sie unten.

Online-Betrieb einer replizierten App auf dem Ziel-Cluster (Failover)

Mit Astra Control können Sie ein „Failover“ Ihrer replizierten Applikationen auf ein Ziel-Cluster ausführen. 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 auf der Seite Anwendung die Registerkarte **Datenschutz** > **Replikation** aus.
3. Wählen Sie auf der Registerkarte Datenschutz > Replikation im Menü Aktionen die Option **Failover** aus.
4. Überprüfen Sie auf der Seite Failover die Informationen, und wählen Sie **Failover**.

Ergebnis

Die folgenden Aktionen ergeben sich aus dem Failover-Verfahren:

- Auf dem Ziel-Cluster wird die Applikation 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 basierend auf den Zeitplänen in der Quell-App zum Zeitpunkt des Failover in die Ziel-App kopiert.
- 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 auf der Seite Anwendung die Registerkarte **Datenschutz** > **Replikation** aus.
3. Wählen Sie auf der Registerkarte Datenschutz > Replikation im Menü Aktionen die Option **Resync** aus.
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 ein geplanter Vorgang, bei dem die Applikation zum Ziel-Cluster verschoben und anschließend wieder zurück auf das ursprüngliche Quell-Cluster repliziert wird. Astra Control stoppt die Applikation auf dem Quell-

Cluster und repliziert die Daten zum Ziel, bevor ein Failover der App zum Ziel-Cluster erfolgt.

In dieser Situation tauschen Sie Quelle und Ziel aus. Der ursprüngliche Quellcluster wird zum neuen Ziel-Cluster, und das ursprüngliche Ziel-Cluster wird zum neuen Quellcluster.

Schritte

1. Wählen Sie in der linken Navigation von Astra Control die Option **Anwendungen**.
2. Wählen Sie auf der Seite Anwendung die Registerkarte **Datenschutz** > **Replikation** aus.
3. Wählen Sie auf der Registerkarte Datenschutz > Replikation im Menü Aktionen die Option **Replikation umkehren** aus.
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:

- Es wird ein Snapshot der Kubernetes-Ressourcen der ursprünglichen Quell-Applikation 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 Applikation erstellt und repliziert.
- Die SnapMirror Beziehungen sind beschädigt, wodurch die Zieldatenträger für Lese-/Schreibvorgänge bereit sind.
- Die Kubernetes-Ressourcen der Applikation werden aus dem vor dem Herunterfahren-Snapshot wiederhergestellt. Dabei werden die Volume-Daten repliziert, nachdem die ursprüngliche Quell-App heruntergefahren wurde.
- 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 „Failback“ erreichen, indem Sie die folgende Reihenfolge der Vorgänge verwenden. In diesem Workflow repliziert (neu synchronisiert) Astra Control alle Anwendungen, die in die ursprüngliche Replikationsrichtung geändert werden, zurück zum ursprünglichen Quell-Cluster, bevor die Replikationsrichtung umkehrt.

Dieser Prozess beginnt mit einer Beziehung, die ein Failover zu einem Ziel abgeschlossen hat und die folgenden Schritte umfasst:

- 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 auf der Seite Anwendung die Registerkarte **Datenschutz** > **Replikation** aus.
3. Wählen Sie auf der Registerkarte Datenschutz > Replikation im Menü Aktionen die Option **Resync** aus.
4. Für einen Fail-Back-Vorgang wählen Sie die Failover-App als Quelle für den Resynchronisierungsvorgang aus (wobei Daten nach dem Failover beim Schreiben beibehalten werden).

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 auf der Seite Anwendung die Registerkarte **Datenschutz** > **Replikation** aus.
3. Wählen Sie auf der Registerkarte Datenschutz > Replikation im Feld Anwendungsschutz oder im Beziehungsdiagramm die Option **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 hergestellt oder hat sich etabliert, und der jüngste 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 steht fest (also, ein erfolgreicher Snapshot wurde repliziert, und ein Failover ist möglich), aber der neueste Snapshot ist ausgefallen oder zur Replizierung fehlgeschlagen.

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 PVCs verfügbar sind, überprüft die Replikationsbeziehung, erstellt regelmäßig Snapshots der App und identifiziert alle neuen Quell-VES in der App. Wenn ja, erstellt Astra Control die Ressourcen, die sie in die Replikation aufnehmen.
- **Failover**: Astra Control durchbricht die SnapMirror Beziehungen und stellt die Kubernetes-Ressourcen der App aus dem letzten erfolgreich replizierten App-Snapshot wieder her.
- **Failover**: Astra Control stoppt die Replizierung vom Quell-Cluster, 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 klonen, um eine doppelte Applikation auf demselben Kubernetes-Cluster oder einem anderen Cluster zu erstellen. Wenn Astra Control Center eine Applikation geklont, 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 UI oder verwenden "Die Astra Control API" Zum Klonen und Migrieren von Applikationen

Was Sie benötigen

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

Über diese Aufgabe

- Wenn Sie eine App implementieren, die explizit auf StorageClass gesetzt ist und Sie die Applikation klonen müssen, muss das Ziel-Cluster über die ursprünglich angegebene StorageClass verfügen. Das Klonen einer Applikation, deren StorageClass explizit auf ein Cluster festgelegt ist, das nicht über dieselbe StorageClass verfügt, schlägt fehl.
- Wenn Sie eine vom Betreiber implementierte Instanz von Jenkins CI klonen, müssen Sie die persistenten Daten manuell wiederherstellen. Dies ist eine Einschränkung des Bereitstellungsmodells der Applikation.
- 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.
- Während eines Applikations-Backups oder Applikations-Restores 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.
- Jeder Mitgliedsbenutzer mit Namespace-Einschränkungen nach Namespace-Name/ID oder durch Namespace-Bezeichnungen kann eine App in einem neuen Namespace auf demselben 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.

OpenShift-Überlegungen

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

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

Schritte

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

Ergebnis

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

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

Anwendungsausführungshaken verwalten

Ein Execution Hook ist 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 mithilfe von Testsuiten alle Datenbanktransaktionen vor dem Snapshot anhalten und die Transaktionen nach Abschluss des Snapshots fortsetzen. 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

Wichtige Hinweise zu benutzerdefinierten Testausführungshaken

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

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

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

Ausführungsreihenfolge

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

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

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

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

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

> Sie sollten Ihre Hook-Skripte immer testen, bevor Sie sie in einer Produktionsumgebung aktivieren. Mit dem Befehl '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
1	Klon	N	N	Neu	Gleich	Y	N	Y
2	Klon	N	N	Neu	Anders	Y	Y	Y

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

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, die Quelle und den Ablauf eines Hakens (vor oder nach dem Betrieb). Um Ereignisprotokolle zu den Testausführungshaken anzuzeigen, gehen Sie zur Seite **Aktivität** im linken Navigationsbereich.

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

Sie können einen oder mehrere Skripte hinzufügen, auf die Testausführungshaken verweisen können. Viele Testsuitehaoks können auf dasselbe Skript verweisen. So können Sie viele Testsuiten aktualisieren, indem Sie nur ein Skript ändern.

Schritte

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

Ergebnis

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

Ein Skript löschen

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

Schritte

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

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

Erstellen Sie einen benutzerdefinierten Testsuite-Haken

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

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

Schritte

1. Wählen Sie **Anwendungen** und dann den Namen einer verwalteten App aus.
2. Wählen Sie die Registerkarte **Testsuitehaschen** aus.
3. Wählen Sie **Hinzufügen**.
4. Legen Sie im Bereich **Hook Details** fest, wann der Haken ausgeführt werden soll, indem Sie im Dropdown-Menü **Operation** einen Operationstyp auswählen.
5. Geben Sie einen eindeutigen Namen für den Haken ein.
6. (Optional) Geben Sie alle Argumente ein, um während der Ausführung an den Haken weiterzuleiten. Drücken Sie nach jedem eingegebenen Argument die Eingabetaste, um jedes Argument aufzuzeichnen.
7. Wenn der Haken im Bereich **Container Images** auf alle Container-Bilder in der Anwendung laufen soll, aktivieren Sie das Kontrollkästchen **auf alle Container-Bilder** anwenden. Sollte der Haken stattdessen nur auf ein oder mehrere angegebene Container-Images wirken, geben Sie die Container-Bildnamen in das Feld **Container-Bildnamen ein, die mit** übereinstimmen.
8. Führen Sie im Bereich **Script** einen der folgenden Schritte aus:
   - Fügen Sie ein neues Skript hinzu.
     i. Wählen Sie **Hinzufügen**.
     ii. Führen Sie einen der folgenden Schritte aus:
       - Laden Sie ein benutzerdefiniertes Skript hoch.
         I. Wählen Sie die Option **Datei hochladen**.
         II. Navigieren Sie zu einer Datei, und laden Sie sie hoch.
         III. Geben Sie dem Skript einen eindeutigen Namen.
         IV. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.
         V. Wählen Sie **Skript speichern**.
       - Fügen Sie in ein benutzerdefiniertes Skript aus der Zwischenablage ein.
         I. Wählen Sie die Option **Einfügen oder Typ** aus.
         II. Wählen Sie das Textfeld aus, und fügen Sie den Skripttext in das Feld ein.
         III. Geben Sie dem Skript einen eindeutigen Namen.

IV. (Optional) Geben Sie alle Notizen ein, die andere Administratoren über das Skript wissen sollten.

- Wählen Sie ein vorhandenes Skript aus der Liste aus.

  Hiermit wird der Testsuitelink angewiesen, dieses Skript zu verwenden.

9. Wählen Sie **Haken 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.

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**.

Beispiele für Testausführungshaken

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

Einfaches Erfolgsbeispiel

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

```
#!/bin/sh

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



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

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

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


#
# main
#

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

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

Einfaches Erfolgsbeispiel (Bash-Version)

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

```
#!/bin/bash

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


#
```

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


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

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


#
# main
#

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

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

Einfaches Erfolgsbeispiel (zsh-Version)

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

```
#!/bin/zsh
```

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



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



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

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

#
# main
#

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

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

Erfolg mit Argumenten Beispiel

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

```
#!/bin/sh

# success_sample_args.sh
#
# A simple success hook script with args for testing purposes.
#
# args: Up to two optional args that are echoed to stdout

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


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

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


#
# main
#

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

```
# collect args
arg1=$1
arg2=$2

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

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

Beispiel für Haken vor dem Snapshot/nach dem Snapshot

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

```
#!/bin/sh

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

# unique error codes for every error case
ebase=100
eusage=$((ebase+1))
ebadstage=$((ebase+2))
epre=$((ebase+3))
epost=$((ebase+4))


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

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

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


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

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


#
# main
#

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

```
    exit ${eusage}
fi

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

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

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

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

exit ${rc}
```

Fehlerbeispiel

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

```
#!/bin/sh

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



#
# Writes the given message to standard output
#
```

```
# $* - The message to write
#
msg() {
    echo "$*"
}


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

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


#
# main
#

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

argexitcode=$1

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

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

Beispiel für ausführlichen Fehler

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

```
#!/bin/sh

# failure_sample_verbose.sh
#
# A simple failure hook script with args for testing purposes.
#
# args: [The number of lines to output to stdout]


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


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

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


#
# main
#

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


# output arg value to stdout
```

```
linecount=$1
info "line count ${linecount}"

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

error "exiting with error code 8"
exit 8
```

Fehler bei einem Beispiel für den Exit-Code

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

```
#!/bin/sh

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



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



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

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


#
# main
#

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

argexitcode=$1

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

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

Beispiel Erfolg nach Ausfall

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

```
#!/bin/sh

# failure_then_success_sample.sh
#
# A hook script that fails on initial run but succeeds on second run for
testing purposes.
#
# Helpful for testing retry logic for post hooks.
#
# args: None
#

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

```
#
msg() {
    echo "$*"
}


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

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


#
# main
#

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


if [ -e /tmp/hook-test.junk ] ; then
    info "File does exist.  Removing /tmp/hook-test.junk"
    rm /tmp/hook-test.junk
    info "Second run so returning exit code 0"
    exit 0
else
    info "File does not exist.  Creating /tmp/hook-test.junk"
    echo "test" > /tmp/hook-test.junk
    error "Failed first run, returning exit code 5"
    exit 5
fi
```