Schützen Sie Kubernetes-Workloads

NetApp Backup and Recovery

NetApp
June 24, 2026

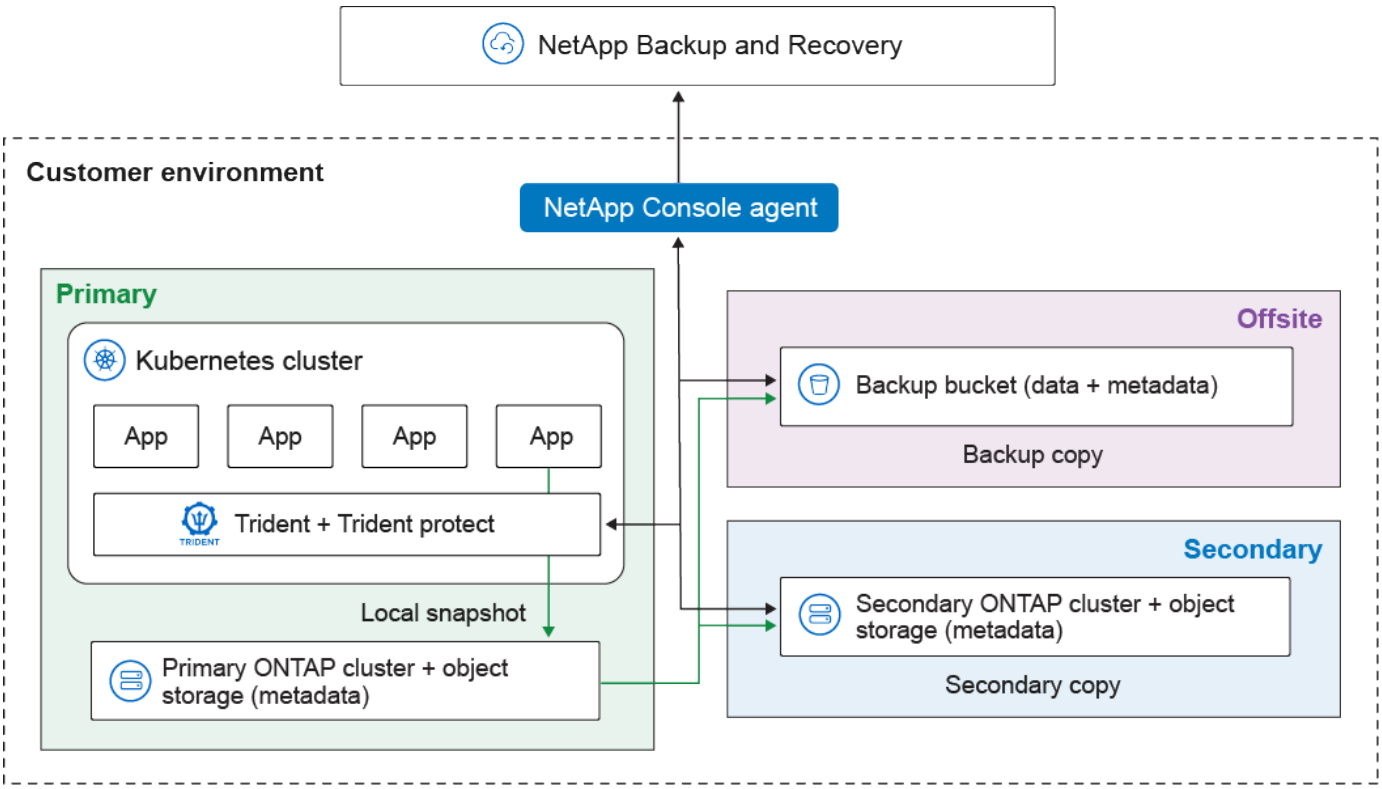
Inhalt

Schützen Sie Kubernetes-Workloads

Übersicht über die Verwaltung von Kubernetes-Workloads

Die Verwaltung von Kubernetes-Workloads in NetApp Backup and Recovery ermöglicht es Ihnen, Ihre Kubernetes-Cluster und Anwendungen zentral zu erkennen, zu verwalten und zu schützen. Sie können Ressourcen und Anwendungen verwalten, die auf Ihren Kubernetes-Clustern gehostet werden. Sie können außerdem Schutzrichtlinien erstellen und Ihren Kubernetes-Anwendungen zuordnen, und das alles über eine einzige Benutzeroberfläche.

Das folgende Diagramm zeigt die Komponenten und die grundlegende Architektur der Sicherung und Wiederherstellung für Kubernetes-Workloads und wie verschiedene Kopien Ihrer Daten an unterschiedlichen Orten gespeichert werden können:



NetApp Backup and Recovery bietet die folgenden Vorteile für die Verwaltung von Kubernetes-Workloads:

- Eine zentrale Steuerungsebene zum Schutz von Anwendungen, die über mehrere Kubernetes-Cluster hinweg ausgeführt werden. Diese Anwendungen können Container oder virtuelle Maschinen umfassen, die auf Ihren Kubernetes-Clustern ausgeführt werden.
- Native Integration mit NetApp SnapMirror, die Speicher-Offloading-Funktionen für alle Backup- und Wiederherstellungs-Workflows ermöglicht.
- Inkrementelle Dauersicherungen für Kubernetes-Anwendungen, was zu niedrigeren Recovery Point Objectives (RPOs) und Recovery Time Objectives (RTOs) führt.

Sie können die folgenden Aufgaben im Zusammenhang mit der Verwaltung von Kubernetes-Workloads ausführen:

- "Entdecken Sie Kubernetes-Workloads".
- "Verwalten von Kubernetes-Clustern".
- "Kubernetes-Anwendungen hinzufügen und schützen".
- "Verwalten von Kubernetes-Anwendungen".
- "Wiederherstellen von Kubernetes-Anwendungen".

Entdecken Sie Kubernetes-Workloads in NetApp Backup and Recovery

NetApp Backup and Recovery muss Kubernetes-Workloads erkennen, bevor sie geschützt werden können.

*Erforderliche NetApp Console * Superadministrator für Backup und Wiederherstellung. Erfahren Sie mehr über"Rollen und Berechtigungen für Backup und Wiederherstellung" . "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Entdecken Sie Kubernetes-Workloads

Ermitteln Sie im Sicherungs- und Wiederherstellungsinventar die Kubernetes-Workloads in Ihrer Umgebung. Durch das Hinzufügen einer Workload wird NetApp Backup and Recovery ein Kubernetes-Cluster hinzugefügt. Anschließend können Sie Anwendungen hinzufügen und Clusterressourcen schützen.

> Wenn Sie einen Cluster entdecken, der aktuell mit Trident Protect geschützt ist, werden alle mit Trident Protect verwendeten Sicherungszeitpläne während des Erkennungsprozesses deaktiviert (Trident Protect-Sicherungszeitpläne sind nicht mit Backup and Recovery kompatibel). Um die Anwendungen des Clusters zu schützen, "eine neue Datensicherungsstrategie erstellen" oder ordnen Sie die Anwendungen einer bestehenden Richtlinie zu. Sie können dann die Trident Protect-Sicherungszeitpläne bei Bedarf entfernen.

Schritte

1. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie Kubernetes-Workloads zum ersten Mal entdecken, wählen Sie in NetApp Backup and Recovery unter **Workloads** die Kachel **Kubernetes** aus.
   - Wenn Sie Kubernetes-Workloads bereits erkannt haben, wählen Sie in NetApp Backup and Recovery*Inventar* > **Workloads** und dann **Ressourcen erkennen**.
2. Wählen Sie den Workloadtyp **Kubernetes** aus.
3. Geben Sie einen Clusternamen ein und wählen Sie einen Connector zur Verwendung mit dem Cluster aus.
4. Befolgen Sie die angezeigten Befehlszeilenanweisungen:
   - Erstellen Sie einen Trident Protect-Namespace
   - Erstellen eines Kubernetes-Geheimnisses
   - Hinzufügen eines Helm-Repositorys
   - Installieren oder aktualisieren Sie Trident Protect und den Trident Protect connector

     Diese Schritte stellen sicher, dass NetApp Backup and Recovery mit dem Cluster interagieren kann.
5. Nachdem Sie die Schritte abgeschlossen haben, wählen Sie **Entdecken**.

Der Cluster wird zum Inventar hinzugefügt.

6. Wählen Sie in der zugehörigen Kubernetes-Workload „Anzeigen“ aus, um die Liste der Anwendungen, Cluster und Namespaces für diese Workload anzuzeigen.

Weiter zum NetApp Backup and Recovery Dashboard

Führen Sie die folgenden Schritte aus, um das NetApp Backup and Recovery Dashboard anzuzeigen.

1. Wählen Sie im NetApp Console **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie eine Workload-Kachel aus (z. B. Microsoft SQL Server).
3. Wählen Sie im Menü „Sichern und Wiederherstellen“ die Option „Dashboard“ aus.
4. Überprüfen Sie den Zustand des Datenschutzes. Die Anzahl der gefährdeten oder geschützten Workloads steigt basierend auf den neu entdeckten, geschützten und gesicherten Workloads.

   "Erfahren Sie, was Ihnen das Dashboard anzeigt".

Kubernetes-Anwendungen hinzufügen und schützen

Kubernetes-Anwendungen hinzufügen und schützen

NetApp Backup and Recovery ermöglicht das Hinzufügen von Kubernetes-Anwendungen über die Web-Oberfläche oder durch Anwenden benutzerdefinierter Ressourcendateien. Anwendungen können Namespace-basiert sein, aus Standard-Kubernetes-Ressourcen bestehen, oder VM-basiert sein und aus einer oder mehreren virtuellen Maschinen bestehen.

Erforderliche NetApp Console

Organisationsadministrator oder SnapCenter Administrator. "Erfahren Sie mehr über die Zugriffsrollen für NetApp Backup and Recovery" . "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Hinzufügen und Schützen einer neuen Kubernetes-Anwendung

Der erste Schritt zum Schutz von Kubernetes-Anwendungen besteht darin, eine Anwendung innerhalb von NetApp Backup and Recovery zu erstellen. Wenn Sie eine Anwendung erstellen, machen Sie Backup and Recovery auf die auf dem Kubernetes-Cluster laufende Anwendung aufmerksam.

Bevor Sie beginnen

Bevor Sie eine Kubernetes-Anwendung hinzufügen und schützen können, müssen Sie"Kubernetes-Workloads entdecken" .

Eine Namespace-basierte App (Web-UI) hinzufügen

Schritte

1. Wählen Sie in NetApp Backup and Recovery*Inventar* aus.
2. Oben rechts auf der Seite muss **Kubernetes** in der Liste der Workloads ausgewählt sein.
3. Für den Workload-Eintrag kann **Ansicht** ausgewählt werden, um die Kubernetes-Ressourcen anzuzeigen.
4. Wählen Sie die Registerkarte **Anwendungen**.
5. Wählen Sie **Anwendung erstellen**.
6. Geben Sie einen Namen für die Anwendung ein.
7. Wählen Sie in der **Cluster**-Liste den Cluster aus, der die Anwendung hostet.
8. Unter **Filter** wählen Sie **Namespace** aus, um Anwendungen nach Namespace zu filtern.
9. Wählen Sie optional eines der folgenden Felder aus, um nach den Ressourcen zu suchen, die Sie schützen möchten:
   - Zugehörige Namespaces
   - Ressourcentypen
   - Beschriftungsselektoren
     i. Wählen Sie **Clusterbezogene Ressourcen hinzufügen**, um Ressourcen hinzuzufügen, die auf Clusterebene gelten. Wenn Sie diese einschließen, werden sie der Anwendung beim Erstellen hinzugefügt.
     ii. Wählen Sie optional **Suchen** aus, um die Ressourcen basierend auf Ihren Suchkriterien zu finden.

   > ⓘ Backup and Recovery speichert weder die Suchparameter noch die Ergebnisse; die Parameter werden verwendet, um den ausgewählten Kubernetes-Cluster nach Ressourcen zu durchsuchen, die in die Anwendung aufgenommen werden können.

10. Backup and Recovery zeigt eine Liste der Ressourcen an, die Ihren Suchkriterien entsprechen.
11. Wenn die Liste die Ressourcen enthält, die Sie schützen möchten, wählen Sie **Weiter**.
12. Optional können Sie im Bereich **Richtlinie** eine vorhandene Datensicherungsstrategie auswählen, um die Anwendung zu schützen, oder eine neue Strategie erstellen. Wenn Sie keine Strategie auswählen, wird die Anwendung ohne Datensicherungsstrategie erstellt. Sie können "Fügen Sie eine Schutzrichtlinie hinzu" dies später nachholen.
13. Aktivieren und konfigurieren Sie im Bereich **Prescripts und Postscripts** alle Prescript- oder Postscript-Ausführungs-Hooks, die Sie vor oder nach Sicherungsvorgängen ausführen möchten. Um Präskripte oder Postskripte zu aktivieren, müssen Sie bereits mindestens ein"Ausführungs-Hook-Vorlage" .
14. Wählen Sie **Erstellen**.

Ergebnis

Die Anwendung wurde erstellt und erscheint in der Liste der Anwendungen auf der Registerkarte **Applications** des Kubernetes-Inventars. Backup and Recovery ermöglicht den Schutz der Anwendung gemäß Ihren Einstellungen, und Sie können den Fortschritt im Bereich **Monitoring** überwachen.

VM-basierte App hinzufügen (Web-UI)

Schritte

1. Wählen Sie in NetApp Backup and Recovery*Inventar* aus.
2. Oben rechts auf der Seite muss **Kubernetes** in der Liste der Workloads ausgewählt sein.
3. Für den Workload-Eintrag kann **Ansicht** ausgewählt werden, um die Kubernetes-Ressourcen anzuzeigen.
4. Wählen Sie die Registerkarte **Anwendungen**.
5. Wählen Sie **Anwendung erstellen**.
6. Geben Sie einen Namen für die Anwendung ein.
7. Wählen Sie in der **Cluster**-Liste den Cluster aus, der die Anwendung hostet.
8. Wählen Sie unter **Filter** die Option **Virtuelle Maschinen**, um eine VM-basierte Anwendung zu erstellen.
9. Suchen Sie nach virtuellen Maschinen, die Sie der Anwendung hinzufügen möchten, indem Sie einen Namespace auswählen und optional Label-Selektoren angeben.

   > Wenn Sie VMs aus der Liste auswählen, ist die Anwendungsdefinition statisch — neue VMs werden der Anwendung nicht nachträglich hinzugefügt (Sie müssen die Anwendung bearbeiten, um sie hinzuzufügen und zu schützen). Wenn Sie Label-Selektoren verwenden, können Sie keine einzelnen VMs auswählen oder die generierte Liste bearbeiten, aber jede VM, die später dem Selektor entspricht, wird automatisch hinzugefügt und geschützt.

   Die ausgewählten virtuellen Maschinen werden in der Liste auf der rechten Seite angezeigt.
10. Wenn die Liste die VMs enthält, die Sie schützen möchten, wählen Sie **Weiter**.
11. Optional können Sie im Bereich **Richtlinie** eine vorhandene Datensicherungsstrategie auswählen, um die Anwendung zu schützen, oder eine neue Strategie erstellen. Wenn Sie keine Strategie auswählen, wird die Anwendung ohne Datensicherungsstrategie erstellt. Sie können "Fügen Sie eine Schutzrichtlinie hinzu" dies später nachholen.
12. Aktivieren und konfigurieren Sie im Bereich **Prescripts und Postscripts** alle Prescript- oder Postscript-Ausführungs-Hooks, die Sie vor oder nach Sicherungsvorgängen ausführen möchten. Um Präskripte oder Postskripte zu aktivieren, müssen Sie bereits mindestens ein"Ausführungs-Hook-Vorlage" .
13. Wählen Sie **Erstellen**.

Ergebnis

Die Anwendung wird erstellt und in der Liste der Anwendungen auf der Registerkarte **Anwendungen** des Kubernetes-Inventars angezeigt. Die NetApp Console ermöglicht den Schutz der Anwendung basierend auf Ihren Einstellungen und Sie können den Fortschritt im Bereich **Überwachung** der Sicherung und Wiederherstellung überwachen.

Fügen Sie eine Namespace-basierte App (CR) hinzu

Schritte

1. Erstellen Sie die CR-Datei der Zielanwendung:
   a. Erstellen Sie die benutzerdefinierte Ressourcendatei (CR) und benennen Sie sie (zum Beispiel `my-app-name.yaml`).
   b. Konfigurieren Sie die folgenden Attribute:

- **metadata.name**: (*Erforderlich*) Der Name der benutzerdefinierten Anwendungsressource. Merken Sie sich den Namen, den Sie wählen, da andere für Schutzvorgänge benötigte CR-Dateien auf diesen Wert verweisen.
- **spec.includedNamespaces**: (*Erforderlich*) Verwenden Sie Namespace und Label-Selektor, um die Namespaces und Ressourcen anzugeben, die die Anwendung verwendet. Der Anwendungsnamespace muss Teil dieser Liste sein. Der Label-Selektor ist optional und kann verwendet werden, um Ressourcen innerhalb jedes angegebenen Namespace zu filtern.
- **spec.includedClusterScopedResources**: (*Optional*) Verwenden Sie dieses Attribut, um Cluster-Scoped-Ressourcen anzugeben, die in die Anwendungsdefinition aufgenommen werden sollen. Mit diesem Attribut können Sie diese Ressourcen anhand ihrer Gruppe, Version, Art und Bezeichnungen auswählen.
  - **groupVersionKind**: (*Erforderlich*) Gibt die API-Gruppe, die Version und die Art der clusterweiten Ressource an.
  - **labelSelector**: (*Optional*) Filtert die clusterweiten Ressourcen anhand ihrer Labels.

c. Konfigurieren Sie die folgenden Annotationen, falls erforderlich:

- **metadata.annotations.protect.trident.netapp.io/skip-vm-freeze**: (*Optional*) Diese Annotation ist nur für Anwendungen relevant, die von virtuellen Maschinen aus definiert werden, z. B. in KubeVirt-Umgebungen, in denen das Dateisystem vor Snapshots eingefroren wird. Legen Sie fest, ob diese Anwendung während eines Snapshots auf das Dateisystem schreiben darf. Ist die Option auf true gesetzt, ignoriert die Anwendung die globale Einstellung und kann während eines Snapshots auf das Dateisystem schreiben. Ist die Option auf false gesetzt, ignoriert die Anwendung die globale Einstellung und das Dateisystem wird während eines Snapshots eingefroren. Wird die Option angegeben, die Anwendung aber keine virtuellen Maschinen in der Anwendungsdefinition hat, wird die Annotation ignoriert. Wird sie nicht angegeben, folgt die Anwendung der "Einstellung für das globale Dateisystem-Freeze".
- **protect.trident.netapp.io/protection-command**: (*Optional*) Verwenden Sie diese Annotation, um Backup and Recovery anzuweisen, die Anwendung zu schützen oder den Schutz zu beenden. Die möglichen Werte sind `protect` oder `unprotect`.
- **protect.trident.netapp.io/protection-policy-name**: (*Optional*) Verwenden Sie diese Annotation, um den Namen der Backup und Recovery Datensicherungsstrategie anzugeben, die Sie zum Schutz dieser Anwendung verwenden möchten. Diese Datensicherungsstrategie muss bereits in Backup und Recovery vorhanden sein.

Falls Sie diese Annotation nachträglich anwenden müssen, nachdem eine Anwendung bereits erstellt wurde, können Sie den folgenden Befehl verwenden:

```
kubectl annotate application -n <application CR namespace> <application CR name> protect.trident.netapp.io/skip-vm-freeze="true"
```

+
Beispiel YAML:

+

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  annotations:
    protect.trident.netapp.io/skip-vm-freeze: "false"
    protect.trident.netapp.io/protection-command: "protect"
    protect.trident.netapp.io/protection-policy-name: "policy-name"
  name: my-app-name
  namespace: my-app-namespace
spec:
  includedNamespaces:
    - namespace: namespace-1
      labelSelector:
        matchLabels:
          app: example-app
    - namespace: namespace-2
      labelSelector:
        matchLabels:
          app: another-example-app
  includedClusterScopedResources:
    - groupVersionKind:
        group: rbac.authorization.k8s.io
        kind: ClusterRole
        version: v1
      labelSelector:
        matchLabels:
          mylabel: test
```

1. (*Optional*) Fügen Sie eine Filterung hinzu, die Ressourcen mit bestimmten Labels ein- oder ausschließt:

   - **resourceFilter.resourceSelectionCriteria**: (Für die Filterung erforderlich) Verwenden Sie `Include` oder `Exclude`, um eine in resourceMatchers definierte Ressource ein- oder auszuschließen. Fügen Sie die folgenden resourceMatchers Parameter hinzu, um die Ressourcen zu definieren, die ein- oder auszuschließen sind:

     - **resourceFilter.resourceMatchers**: Ein Array von resourceMatcher-Objekten. Wenn Sie mehrere Elemente in diesem Array definieren, werden diese mit einer ODER-Verknüpfung verglichen und die Felder innerhalb jedes Elements (group, kind, version) werden mit einer UND-Verknüpfung verglichen.
       - **resourceMatchers[].group**: (*Optional*) Gruppe der zu filternden Ressource.

- **resourceMatchers[].kind**: (*Optional*) Art der zu filternden Ressource.
- **resourceMatchers[].version**: (*Optional*) Version der zu filternden Ressource.
- **resourceMatchers[].names**: (*Optional*) Namen im Kubernetes metadata.name-Feld der Ressource, die gefiltert werden soll.
- **resourceMatchers[].namespaces**: (*Optional*) Namespaces im Kubernetes metadata.name-Feld der Ressource, die gefiltert werden soll.
- **resourceMatchers[].labelSelectors**: (*Optional*) Label-Selektorzeichenfolge im Kubernetes-Metadatenfeld name der Ressource, wie definiert in der "Kubernetes-Dokumentation". Zum Beispiel: `"trident.netapp.io/os=linux"`.

> Wenn sowohl `resourceFilter` als auch `labelSelector` verwendet werden, wird `resourceFilter` zuerst ausgeführt und anschließend `labelSelector` auf die resultierenden Ressourcen angewendet.

Beispiel:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

2. Nachdem Sie die Anwendungs-CR erstellt haben, die zu Ihrer Umgebung passt, wenden Sie die CR an. Zum Beispiel:

```
kubectl apply -f my-app-name.yaml
```

Erstellen und Verwalten von Kubernetes-Backup-Richtlinien in NetApp Backup und Recovery

In NetApp Backup und Recovery können Sie eigene Kubernetes-Backup-Richtlinien erstellen, die die Backup-Häufigkeit, den Zeitpunkt der Backup-Erstellung und die Anzahl

der aufbewahrten Backup-Dateien regeln.

Einige dieser Optionen und Konfigurationsabschnitte sind nicht für alle Workloads verfügbar.

Wenn Sie Ressourcen aus SnapCenter importieren, können Sie auf Unterschiede zwischen den in SnapCenter und den in NetApp Backup and Recovery verwendeten Richtlinien stoßen. Sehen"Richtlinienunterschiede zwischen SnapCenter und NetApp Backup and Recovery" .

Sie können die folgenden Ziele im Zusammenhang mit Richtlinien erreichen:

- Erstellen einer lokalen Snapshot-Richtlinie
- Erstellen einer Richtlinie für die Replikation auf sekundären Speicher
- Erstellen einer Richtlinie für Objektspeichereinstellungen
- Konfigurieren erweiterter Richtlinieneinstellungen
- Richtlinien bearbeiten
- Richtlinien löschen

Richtlinien anzeigen

1. Wählen Sie im NetApp Backup and Recovery -Menü **Richtlinien** aus.
2. Überprüfen Sie die Richtliniendetails. Zum Beispiel:
    - **Workload**: Beispiele sind Microsoft SQL Server, ONTAP Volumes, VMware, KVM, Hyper-V, Oracle Database oder Kubernetes.
    - **Sicherungstyp**: Beispiele sind vollständige Sicherung und Protokollsicherung.
    - **Architektur**: Beispiele hierfür sind lokaler Snapshot, Fan-Out, Kaskadierung, Disk-to-Disk und Disk-to-Object-Store.
    - **Geschützte Ressourcen**: Zeigt an, wie viele Ressourcen der Gesamtressourcen dieser Arbeitslast geschützt sind.
    - **Ransomware-Schutz**: Zeigt an, ob die Richtlinie eine Snapshot-Sperre für den lokalen Snapshot, eine Snapshot-Sperre für den sekundären Speicher oder eine DataLock-Sperre für den Objektspeicher umfasst.

Erstellen einer Richtlinie

Sie können Richtlinien erstellen, die Ihre lokalen Snapshots, Replikationen auf sekundären Speicher und Backups auf Objektspeicher regeln. Ein Teil Ihrer 3-2-1-Strategie besteht darin, einen Snapshot der Instanzen, Datenbanken, Anwendungen oder VMs auf dem **primären** Speichersystem zu erstellen.

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Wiederherstellung, Backupadministrator für Backup und Wiederherstellung. Erfahren Sie mehr über"Rollen und Berechtigungen für Backup und Wiederherstellung" . "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Bevor Sie beginnen

Wenn Sie eine Replikation auf einen sekundären Speicher planen und die Snapshot-Sperre auf lokalen Snapshots oder auf einem Remote ONTAP Sekundärspeicher verwenden möchten, müssen Sie zunächst die ONTAP Compliance-Uhr auf Clusterebene initialisieren. Dies ist eine Voraussetzung zum Aktivieren der Snapshot-Sperre in der Richtlinie.

Anweisungen hierzu finden Sie unter "Initialisieren Sie die Compliance-Uhr in ONTAP" .

Allgemeine Informationen zum Sperren von Snapshots finden Sie unter "Snapshot-Sperre in ONTAP" .

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Richtlinien** aus.
2. Wählen Sie auf der Seite „Richtlinien“ die Option „Neue Richtlinie erstellen“ aus.

   Die Seite „Richtlinien“ wird angezeigt.

3. Geben Sie im Abschnitt **Details** Informationen ein:
   - Workload-Typ: Wählen Sie **Kubernetes**.
   - Geben Sie einen Richtliniennamen ein.
   - Wählen Sie einen Konsolenagenten aus der Liste **Agent** aus.
4. Geben Sie im Abschnitt **Backup-Architektur** Informationen ein. Wählen Sie den Datenfluss für das Backup aus der Liste aus:
   - **3-2-1-Fanout**: Primärspeicher (Festplatte) zu Sekundärspeicher (Festplatte) zu Cloud (Objektspeicher). Erstellt mehrere Kopien von Daten auf verschiedenen Speichersystemen, wie ONTAP zu ONTAP und ONTAP zu Objektspeicher-Konfigurationen. Dies kann ein Cloud-Hyperscaler-Objektspeicher oder ein privater Objektspeicher sein. Am besten geeignet für optimale Datensicherung und Disaster Recovery. Diese Option ist für Amazon FSx for NetApp ONTAP nicht verfügbar.
   - **Festplatte zu Festplatte**: Primärspeicher (Festplatte) zu Sekundärspeicher (Festplatte). Die ONTAP zu ONTAP Datensicherungsstrategie repliziert Daten zwischen zwei ONTAP Systemen, um hohe Verfügbarkeit und Disaster Recovery zu gewährleisten. Dies wird typischerweise mithilfe von SnapMirror erreicht, das sowohl synchron als auch asynchrone Replizierung unterstützt. Diese Methode hält Ihre Daten standortübergreifend aktuell und verfügbar für eine starke Datensicherung.
   - **Disk-to-object storage**: Primärspeicher (Festplatte) zu Cloud (Objektspeicher). Dabei werden Daten von einem ONTAP System zu einem Objektspeichersystem repliziert. Dies kann ein Cloud-Hyperscaler-Objektspeicher oder ein privater Objektspeicher wie StorageGRID sein. Diese Methode ist ideal für die langfristige Datenaufbewahrung und Archivierung. Diese Option ist für Amazon FSx for NetApp ONTAP nicht verfügbar.
   - **Lokale Snapshots**: Lokaler Snapshot des ausgewählten Volumes. Dadurch werden schreibgeschützte, zeitpunktgenaue Kopien der Produktionsvolumes erstellt, auf denen Ihre Workloads ausgeführt werden. Sie können lokale Snapshots verwenden, um Datenverlust oder -beschädigung zu beheben sowie um Backups für die Notfallwiederherstellung zu erstellen.
5. Geben Sie Informationen für den Abschnitt **Lokale Snapshot-Einstellungen** an:
   - Wählen Sie die Option **Zeitplan hinzufügen**, um den oder die Snapshot-Zeitpläne auszuwählen. Sie können maximal 5 Zeitpläne haben.
   - **Schnappschusshäufigkeit**: Wählen Sie die Häufigkeit stündlich, täglich, wöchentlich, monatlich oder jährlich. Die jährliche Häufigkeit ist für Kubernetes-Workloads nicht verfügbar.
   - **Aufbewahrung von Snapshots**: Geben Sie die Anzahl der aufzubewahrenden Snapshots ein.
   - **Anbieter**: Wählen Sie den Speicheranbieter aus, der die Kubernetes-Anwendungsressourcen hostet, und geben Sie die Anmeldeinformationen zur Authentifizierung beim Anbieter ein.
6. Geben Sie Informationen für den Abschnitt **Sekundäre Einstellungen** (Replikation auf Sekundärspeicher) an:
   - **Sicherung**: Wählen Sie die Häufigkeit stündlich, täglich, wöchentlich, monatlich oder jährlich.

- **Sicherungsziel**: Wählen Sie das Zielsystem auf dem Sekundärspeicher für die Sicherung aus.
- **Aufbewahrung**: Geben Sie die Anzahl der aufzubewahrenden Snapshots ein.
- **Anbieter**: Wählen Sie den Speicheranbieter aus, der die Kubernetes-Anwendungsressourcen hostet, und geben Sie die Anmeldeinformationen zur Authentifizierung beim Anbieter ein.

7. Geben Sie Informationen für den Abschnitt **Objektspeichereinstellungen** (Sicherung im Objektspeicher) an:

   Die angezeigten Felder unterscheiden sich je nach ausgewähltem Anbieter und Architektur.

   - **Anbieter**: Wählen Sie den Anbieter für Ihren Objektspeicher und geben Sie die Anmeldeinformationen in die entsprechenden Felder ein (die Felder für die Anmeldeinformationen unterscheiden sich je nach Anbieter).
   - **Sicherungsziel**: Wählen Sie ein registriertes Objektspeicherziel aus. Stellen Sie sicher, dass das Ziel in Ihrer Sicherungsumgebung zugänglich ist.
   - **IPspace**: Wählen Sie den IPspace aus, der für die Sicherungsvorgänge verwendet werden soll. Dies ist nützlich, wenn Sie über mehrere IP-Bereiche verfügen und steuern möchten, welcher für Sicherungen verwendet wird.
   - **Zeitplaneinstellungen**: Wählen Sie den Zeitplan aus, der für die lokalen Snapshots festgelegt wurde. Sie können einen Zeitplan entfernen, aber keinen hinzufügen, da die Zeitpläne entsprechend den lokalen Snapshot-Zeitplänen festgelegt werden.
   - **Aufbewahrungskopien**: Geben Sie die Anzahl der aufzubewahrenden Snapshots ein.
   - **Ausführen um**: Wählen Sie den ONTAP Übertragungszeitplan zum Sichern von Daten im Objektspeicher.
   - **Stufen Sie Ihre Backups vom Objektspeicher in den Archivspeicher auf**: Wenn Sie Backups in den Archivspeicher (z. B. AWS Glacier) aufstufen möchten, wählen Sie die Stufenoption und die Anzahl der Tage für die Archivierung aus.

Bearbeiten einer Richtlinie

Sie können die Backup-Architektur, die Backup-Frequenz, die Aufbewahrungsrichtlinie und weitere Einstellungen einer Richtlinie bearbeiten. Für Kubernetes-Workload-Richtlinien können Sie nur die Zeitplan- und Aufbewahrungseinstellungen bearbeiten.

Sie können beim Bearbeiten einer Richtlinie eine weitere Schutzebene hinzufügen, aber keine Schutzebene entfernen. Wenn die Richtlinie beispielsweise nur lokale Snapshots schützt, können Sie die Replikation zum sekundären Speicher oder die Backups zum Objektspeicher hinzufügen. Wenn Sie über lokale Snapshots und Replikation verfügen, können Sie Objektspeicher hinzufügen. Wenn Sie jedoch über lokale Snapshots, Replikation und Objektspeicher verfügen, können Sie keine dieser Ebenen entfernen.

Wenn Sie eine Richtlinie bearbeiten, die eine Sicherung im Objektspeicher vornimmt, können Sie die Archivierung aktivieren.

Wenn Sie Ressourcen aus SnapCenter importiert haben, stoßen Sie möglicherweise auf einige Unterschiede zwischen den in SnapCenter und NetApp Backup and Recovery verwendeten Richtlinien. Sehen"Richtlinienunterschiede zwischen SnapCenter und NetApp Backup and Recovery" .

Erforderliche NetApp Console

Superadministrator für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Gehen Sie in der NetApp Console zu **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie die Option **Richtlinien**.
3. Wählen Sie die Richtlinie aus, die Sie bearbeiten möchten.
4. Wählen Sie die **Aktionen*** **Symbol und wählen Sie *Bearbeiten**.

Löschen einer Richtlinie

Sie können eine Richtlinie löschen, wenn Sie sie nicht mehr benötigen.

Sie können keine Richtlinie löschen, die einer Arbeitslast zugeordnet ist.

Schritte

1. Gehen Sie in der Konsole zu **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie die Option **Richtlinien**.
3. Wählen Sie die Richtlinie aus, die Sie löschen möchten.
4. Wählen Sie die **Aktionen*** **Symbol und wählen Sie *Löschen**.
5. Bestätigen Sie die Aktion und wählen Sie **Löschen**.

Sichern Sie jetzt Kubernetes-Anwendungen mit der Backup and Recovery-Weboberfläche.

NetApp Backup and Recovery ermöglicht es Ihnen, Kubernetes-Anwendungen manuell über die Weboberfläche zu sichern.

Erforderliche NetApp Console

Organisationsadministrator oder SnapCenter Administrator. "Erfahren Sie mehr über die Zugriffsrollen für NetApp Backup and Recovery" . "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Sichern Sie jetzt eine Kubernetes-Anwendung über die Web-Oberfläche

Erstellen Sie manuell ein Backup einer Kubernetes-Anwendung, um eine Basis für zukünftige Backups und Snapshots zu schaffen oder um sicherzustellen, dass die aktuellsten Daten geschützt sind.

Schritte

1. Wählen Sie in NetApp Backup and Recovery*Inventar* aus.
2. Wählen Sie eine Kubernetes-Instanz und wählen Sie **Anzeigen**, um die mit dieser Instanz verknüpften Ressourcen anzuzeigen.
3. Wählen Sie die Registerkarte **Anwendungen**.
4. Wählen Sie in der Anwendungsliste eine Anwendung aus, die Sie sichern möchten, und wählen Sie das zugehörige Aktionsmenü.
5. Wählen Sie **Jetzt sichern**.
6. Stellen Sie sicher, dass der richtige Anwendungsname ausgewählt ist.
7. Wählen Sie **Sichern**.

Ergebnis

Die Konsole erstellt eine Sicherungskopie der Anwendung und zeigt den Fortschritt im Bereich **Überwachung** von Sicherung und Wiederherstellung an. Das Backup wird basierend auf der mit der Anwendung verknüpften Schutzrichtlinie erstellt.

Sichern Sie jetzt Kubernetes-Anwendungen mithilfe benutzerdefinierter Ressourcen in Backup and Recovery

NetApp Backup and Recovery ermöglicht es Ihnen, Kubernetes-Anwendungen mithilfe von benutzerdefinierten Ressourcen (CRs) manuell zu sichern.

Sichern Sie jetzt eine Kubernetes-Anwendung mithilfe benutzerdefinierter Ressourcen

Erstellen Sie manuell ein Backup einer Kubernetes-Anwendung, um eine Basis für zukünftige Backups und Snapshots zu schaffen oder um sicherzustellen, dass die aktuellsten Daten geschützt sind.

> Clusterbezogene Ressourcen werden in eine Sicherung, einen Snapshot oder einen Klon aufgenommen, wenn sie in der Anwendungsdefinition explizit referenziert werden oder wenn sie Verweise auf einen der Anwendungs-Namespaces enthalten.

Bevor Sie beginnen

Stellen Sie sicher, dass die Gültigkeitsdauer des AWS-Sitzungstokens für alle länger laufenden s3-Backup-Vorgänge ausreichend ist. Wenn das Token während des Backup-Vorgangs abläuft, kann der Vorgang fehlschlagen.

- Weitere Informationen zum Prüfen des Ablaufs des aktuellen Sitzungstokens finden Sie in der "AWS API-Dokumentation".
- Weitere Informationen zu Anmeldeinformationen für AWS-Ressourcen finden Sie im "AWS IAM-Dokumentation".

Erstellen Sie einen lokalen Snapshot mithilfe einer benutzerdefinierten Ressource

Um einen Snapshot Ihrer Kubernetes-Anwendung zu erstellen und lokal zu speichern, verwenden Sie die benutzerdefinierte Ressource Snapshot mit spezifischen Attributen.

Schritte

1. Erstellen Sie die benutzerdefinierte Ressourcendatei (CR) und benennen Sie sie `local-snapshot-cr.yaml`.
2. Konfigurieren Sie in der von Ihnen erstellten Datei die folgenden Attribute:
   - **metadata.name**: (*Erforderlich*) Der Name dieser benutzerdefinierten Ressource; wählen Sie einen eindeutigen und sinnvollen Namen für Ihre Umgebung.
   - **spec.applicationRef**: Der Kubernetes-Name der Anwendung, für die ein Snapshot erstellt werden soll.
   - **spec.appVaultRef**: (*Erforderlich*) Der Name des AppVault, wo die Snapshot-Inhalte (Metadaten) gespeichert werden sollen.
   - **spec.reclaimPolicy**: (*Optional*) Definiert, was mit dem AppArchive eines Snapshots geschieht, wenn die Snapshot-CR gelöscht wird. Das bedeutet, dass selbst wenn auf `Retain` gesetzt, der Snapshot gelöscht wird. Gültige Optionen:
     - `Retain` (Standard)

- `Delete`

```
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  namespace: my-app-namespace
  name: local-snapshot-cr
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  reclaimPolicy: Retain
```

3. Nachdem Sie die `local-snapshot-cr.yaml` Datei mit den korrekten Werten gefüllt haben, wenden Sie die CR an:

```
kubectl apply -f local-snapshot-cr.yaml
```

Sichern Sie eine Anwendung in einem Objektspeicher mithilfe einer benutzerdefinierten Ressource

Erstellen Sie eine Backup-CR mit spezifischen Attributen, um Ihre Anwendung in einem Objektspeicher zu sichern.

Schritte

1. Erstellen Sie die benutzerdefinierte Ressourcendatei (CR) und benennen Sie sie `object-store-backup-cr.yaml`.
2. Konfigurieren Sie in der von Ihnen erstellten Datei die folgenden Attribute:
   - **metadata.name**: (*Erforderlich*) Der Name dieser benutzerdefinierten Ressource; wählen Sie einen eindeutigen und sinnvollen Namen für Ihre Umgebung.
   - **spec.applicationRef**: (*Erforderlich*) Der Kubernetes-Name der zu sichernden Anwendung.
   - **spec.appVaultRef**: (*Erforderlich, schließt sich gegenseitig mit spec.appVaultTargetsRef aus*) Wenn Sie denselben Bucket zum Speichern des Snapshots und des Backups verwenden, ist dies der Name des AppVault, in dem die Backup-Inhalte gespeichert werden sollen.
   - **spec.appVaultTargetsRef**: (*Erforderlich, schließt sich gegenseitig mit spec.appVaultRef aus*) Wenn Sie unterschiedliche Buckets zum Speichern des Snapshots und des Backups verwenden, ist dies der Name des AppVault, in dem die Backup-Inhalte gespeichert werden sollen.
   - **spec.dataMover**: (Optional, erforderlich für Cluster, die von Trident Protect migriert wurden) Eine Zeichenkette, die angibt, welches Backup-Tool für den Backup-Vorgang verwendet werden soll. Wenn dieser Cluster von Trident Protect zu NetApp Backup and Recovery migriert wurde, ist der Wert Groß-/Kleinschreibung und muss `CBS` sein.
   - **spec.reclaimPolicy**: (*Optional*) Definiert, was mit den Sicherungsinhalten (Metadaten/Volume-Daten) geschieht, wenn die Backup-CR gelöscht wird. Mögliche Werte:
     - `Delete`
     - `Retain` (Standard)

- **spec.cleanupSnapshot**: (*Erforderlich*) Stellt sicher, dass der vom Backup CR erstellte temporäre Snapshot nach Abschluss des Sicherungsvorgangs nicht gelöscht wird. Empfohlener Wert: `false`.

  Beispiel-YAML bei Verwendung desselben Buckets zum Speichern des Snapshots und des Backups:

```
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: my-cr-name
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
```

  Beispiel-YAML bei Verwendung unterschiedlicher Buckets zum Speichern des Snapshots und des Backups:

```
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: object-store-backup-cr
spec:
  applicationRef: my-application
  appVaultTargetsRef: appvault-targets-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
```

3. Nachdem Sie die `object-store-backup-cr.yaml` Datei mit den korrekten Werten gefüllt haben, wenden Sie die CR an:

```
kubectl apply -f object-store-backup-cr.yaml
```

Erstellen Sie ein 3-2-1-Fanout-Backup mithilfe einer benutzerdefinierten Ressource

Bei der Datensicherung mit einer 3-2-1-Fanout-Architektur wird eine Sicherung sowohl auf einem Sekundärspeicher als auch in einem Objektspeicher erstellt. Um eine 3-2-1-Fanout-Sicherung zu erstellen, erstellen Sie ein Backup CR mit bestimmten Attributen.

Schritte

1. Erstellen Sie die benutzerdefinierte Ressourcendatei (CR) und benennen Sie sie `3-2-1-fanout-`

`backup-cr.yaml`.

2. Konfigurieren Sie in der von Ihnen erstellten Datei die folgenden Attribute:

   - **metadata.name**: (*Erforderlich*) Der Name dieser benutzerdefinierten Ressource; wählen Sie einen eindeutigen und sinnvollen Namen für Ihre Umgebung.
   - **spec.applicationRef**: (*Erforderlich*) Der Kubernetes-Name der zu sichernden Anwendung.
   - **spec.appVaultTargetsRef**: (*Erforderlich*) Der Name des AppVault, wo die Sicherungsinhalte gespeichert werden sollen.
   - **spec.dataMover**: (*Optional*) Eine Zeichenkette, die angibt, welches Sicherungstool für den Sicherungsvorgang verwendet werden soll. Der Wert ist Groß-/Kleinschreibung und muss `CBS` sein.
   - **spec.reclaimPolicy**: (*Optional*) Definiert, was mit den Sicherungsinhalten (Metadaten/Volume-Daten) geschieht, wenn die Backup-CR gelöscht wird. Mögliche Werte:
     - `Delete`
     - `Retain` (Standard)
   - **spec.cleanupSnapshot**: (*Erforderlich*) Stellt sicher, dass der vom Backup CR erstellte temporäre Snapshot nach Abschluss des Sicherungsvorgangs nicht gelöscht wird. Empfohlener Wert: `false`.
   - **spec.replicateSnapshot**: (*Erforderlich*) Weist Backup and Recovery an, den Snapshot auf den Sekundärspeicher zu replizieren. Erforderlicher Wert: `true`.
   - **spec.replicateSnapshotReclaimPolicy**: (*Optional*) Definiert, was mit dem replizierten Snapshot geschieht, wenn er gelöscht wird. Mögliche Werte:
     - `Delete`
     - `Retain` (Standard)

     Beispiel YAML:

```yaml
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: 3-2-1-fanout-backup-cr
spec:
  applicationRef: my-application
  appVaultTargetsRef: appvault-targets-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
  replicateSnapshot: true
  replicateSnapshotReclaimPolicy: Retain
```

3. Nachdem Sie die `3-2-1-fanout-backup-cr.yaml` Datei mit den korrekten Werten gefüllt haben, wenden Sie die CR an:

```
kubectl apply -f 3-2-1-fanout-backup-cr.yaml
```

Unterstützte Sicherungsanmerkungen

Die folgende Tabelle beschreibt die Anmerkungen, die Sie beim Erstellen eines Backup-CR verwenden können.

Anmerkung	Typ	Beschreibung	Standardwert
protect.trident.netapp.io/full-backup	Zeichenkette	Legt fest, ob eine Sicherung nicht inkrementell sein soll. Setzen Sie auf `true`, um eine nicht inkrementelle Sicherung zu erstellen. Es ist bewährte Praxis, regelmäßig eine vollständige Sicherung durchzuführen und dazwischen inkrementelle Sicherungen zu erstellen, um das mit Wiederherstellungen verbundene Risiko zu minimieren.	"false"
protect.trident.netapp.io/snapshot-completion-timeout	Zeichenkette	Die maximal zulässige Zeit für den Abschluss des gesamten Snapshot-Vorgangs.	"60m"
protect.trident.netapp.io/volume-snapshots-ready-to-use-timeout	Zeichenkette	Die maximal zulässige Zeitspanne, bis Volume-Snapshots den einsatzbereiten Zustand erreichen.	"30m"
protect.trident.netapp.io/volume-snapshots-created-timeout	Zeichenkette	Die maximal zulässige Zeit für die Erstellung von Volume-Snapshots.	"5m"
protect.trident.netapp.io/pvc-bind-timeout-sec	Zeichenkette	Maximale Zeit (in Sekunden), die gewartet wird, bis neu erstellte PersistentVolumeClaims (PVCs) die `Bound` Phase erreichen, bevor die Operation fehlschlägt.	"1200" (20 Minuten)

Wiederherstellen von Kubernetes-Anwendungen

Kubernetes-Anwendungen mithilfe der Web-Benutzeroberfläche wiederherstellen

Mit NetApp Backup and Recovery können Sie Anwendungen wiederherstellen, die Sie mit einer Schutzrichtlinie geschützt haben. Zur Wiederherstellung einer Anwendung muss mindestens ein Wiederherstellungspunkt verfügbar sein. Ein Wiederherstellungspunkt besteht entweder aus dem lokalen Snapshot oder der Sicherung im Objektspeicher (oder beidem). Sie können eine Anwendung mithilfe des lokalen, sekundären oder Objektspeicherarchivs wiederherstellen.

Geschützte Ressourcen für einen Anwendungswiederherstellungspunkt anzeigen

Für jede Anwendung, die Sie mit Backup and Recovery schützen, können Sie die Ressourcen anzeigen, die für einen bestimmten Wiederherstellungspunkt gesichert wurden.

Erforderliche NetApp Console

Backup- und Wiederherstellungsanzeige. "Erfahren Sie mehr über die Zugriffsrollen für NetApp Backup and

Recovery". "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste".

Schritte

1. In NetApp Backup and Recovery wählen Sie **Inventar** > **Anwendungen**.
2. Wählen Sie in der Anwendungsliste eine Anwendung aus und klicken Sie auf das Symbol „Aktionen“ ••• > **Anzeigen und Wiederherstellen**.
3. Wählen Sie in der Liste der Wiederherstellungspunkte einen Wiederherstellungspunkt aus und klicken Sie auf das Symbol „Aktionen“ ••• > **Ressourcen anzeigen**.

   Es wird eine Liste der Ressourcen und ihrer Details angezeigt. Sie können die Ressourcen nach Namensraum oder Clusterbereich anzeigen und die Liste als JSON-Datei für zukünftige Audits herunterladen.

4. Wenn Sie fertig sind, wählen Sie **Schließen**.

Wiederherstellen von Kubernetes-Anwendungen

Sie können Namespace-basierte oder VM-basierte Anwendungen von einem Wiederherstellungspunkt wiederherstellen, indem Sie entweder alle Ressourcen wiederherstellen oder eine Teilmenge der wiederherzustellenden Ressourcen auswählen.

Bevor Sie beginnen

Wenn Sie eine Anwendung wiederherstellen, die mit Trident Protect gesichert wurde, stellen Sie sicher, dass Trident Protect sowohl auf dem Quell-Cluster als auch auf dem Ziel-Cluster installiert ist.

Erforderliche NetApp Console

Superadministrator für Backup und Recovery oder Restore-Administrator für Backup und Recovery. "Erfahren Sie mehr über die Zugriffsrollen für NetApp Backup and Recovery". "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste".

Schritte

1. Wählen Sie im NetApp Backup und Recovery-Menü **Wiederherstellen** aus.
2. Wählen Sie eine Kubernetes-Anwendung aus der Liste und wählen Sie **Anzeigen und Wiederherstellen** für diese Anwendung.

   Die Liste der Wiederherstellungspunkte wird angezeigt.

3. Wählen Sie die Schaltfläche **Restore** für den Wiederherstellungspunkt aus, den Sie verwenden möchten.

   Der Assistent zum Wiederherstellen von Daten wird gestartet und die Seite *Allgemeine Einstellungen* wird angezeigt.

4. Wählen Sie den Quellspeicherort aus, von dem wiederhergestellt werden soll.
5. Wählen Sie den Zielcluster aus der Liste **Cluster** aus.
6. Wählen Sie, ob Sie in die ursprünglichen Namensräume oder in neue Namensräume wiederherstellen möchten.
7. Wenn Sie die Wiederherstellung in neuen Namensräumen gewählt haben, sind folgende Schritte erforderlich:
   a. Geben Sie den oder die Ziel-Namespaces ein, die verwendet werden.
   b. Den Namen der Zielanwendung eingeben.

c. Optional kann die Option **Keine Anwendung für wiederhergestellte Ressourcen erstellen** ausgewählt werden, um Ressourcen wiederherzustellen, ohne ein benutzerdefiniertes Anwendungsressourcenobjekt zu erstellen. Dies reduziert unnötige Einträge im Anwendungsinventar.

8. Wählen Sie **Weiter**.

   Die Seite „Ressourcenauswahl“ wird angezeigt.

9. Wählen Sie aus, ob Sie alle mit der Anwendung verknüpften Ressourcen wiederherstellen möchten, oder verwenden Sie einen Filter, um bestimmte wiederherzustellende Ressourcen auszuwählen:

Alle Ressourcen

a. Wählen Sie **Alle Ressourcen wiederherstellen**.

   Bei der Wiederherstellung einer VM-basierten Anwendung listet Backup and Recovery alle virtuellen Maschinen im Wiederherstellungspunkt auf.

b. Wählen Sie **Weiter**.

Spezifische namensraumbasierte App-Ressourcen

a. Wählen Sie **Selektive Ressourcen** aus und entscheiden Sie, ob Sie die Ressourcen, die Sie auswählen, anhand von Regeln oder anhand des Namensraums filtern möchten.

Methode zur Ressourcenauswahl	Schritte
Ressourcen mithilfe von Regeln filtern	i. Wählen Sie die Registerkarte **Regeln** aus. ii. Wählen Sie das Verhalten des Ressourcenfilters. Wenn Sie **Einschließen** wählen, werden die von Ihnen ausgewählten Ressourcen wiederhergestellt. Wenn Sie **Ausschließen** wählen, werden die ausgewählten Ressourcen nicht wiederhergestellt. iii. Wählen Sie **Regeln hinzufügen** aus, um Regeln hinzuzufügen, die Filter für die Auswahl von Ressourcen definieren. Sie benötigen mindestens eine Regel zum Filtern von Ressourcen. Jede Regel kann nach Kriterien wie Ressourcennamespace, Bezeichnungen, Gruppe, Version und Art filtern. iv. Wählen Sie **Speichern**, um jede Regel zu speichern. v. Wenn Sie alle benötigten Regeln hinzugefügt haben, wählen Sie **Ressourcen anzeigen**, um die im Sicherungsarchiv verfügbaren Ressourcen anzuzeigen, die Ihren Filterkriterien entsprechen.

Methode zur Ressourcenauswahl	Schritte
Ressourcen manuell aus einer Liste auswählen	i. Wählen Sie die Registerkarte **Benutzerdefiniert** aus. ii. Wählen Sie **Namespace-bezogen** oder **Cluster-bezogen**, um die entsprechenden Ressourcen anzuzeigen. Backup and Recovery listet alle Ressourcen im Wiederherstellungspunkt auf. iii. Wählen Sie die Ressourcen aus, die in den Wiederherstellungsvorgang einbezogen werden sollen.

Bei den angezeigten Ressourcen handelt es sich um die Ressourcen, die derzeit im Cluster vorhanden sind.

b. Wenn Sie fertig sind, wählen Sie **Weiter**.

Spezifische VM-basierte Anwendungsressourcen

a. Wählen Sie **Selektive Ressourcen** aus.

b. Führen Sie einen der folgenden Schritte aus:

- Zur Wiederherstellung ganzer virtueller Maschinen die Registerkarte **Virtuelle Maschinen** auswählen.

  Backup and Recovery listet alle virtuellen Maschinen im Wiederherstellungspunkt auf. Sie können auswählen, welche VMs in den Wiederherstellungsvorgang einbezogen werden sollen.

- Zum Wiederherstellen einzelner persistenter Volume-Ansprüche die Registerkarte **Persistente Volume-Ansprüche** auswählen.

  Backup and Recovery listet alle Persistent Volume Claims im Wiederherstellungspunkt auf. Es kann ausgewählt werden, welche Persistent Volume Claims in die Wiederherstellungsoperation einbezogen werden.

c. Wenn Sie fertig sind, wählen Sie **Weiter**.

Die Seite „Zieleinstellungen“ wird angezeigt.

10. Erweitern Sie den Abschnitt **Destination settings** und wählen Sie aus, ob Sie entweder in der Standard-Speicherklasse, in einer anderen Speicherklasse wiederherstellen möchten oder, wenn Sie in einem anderen Cluster wiederherstellen, die Speicherklassen dem Ziel-Cluster zuordnen möchten.
11. Wenn Sie die Wiederherstellung in einer anderen Speicherklasse gewählt haben, wählen Sie eine Zielspeicherklasse aus, die zu jeder Quellspeicherklasse passt.
12. Optional können Sie, wenn Sie eine mit Trident Protect erstellte Sicherung oder einen Snapshot wiederherstellen, die Details des AppVault, der als Speicher-Bucket für die Wiederherstellungsoperation verwendet wurde, anzeigen. Wenn es eine Änderung in Ihrer Umgebung oder im AppVault-Status gibt,

wählen Sie **Sync App Vault**, um die Details zu aktualisieren.

> Wenn Sie einen AppVault auf einem Kubernetes-Cluster erstellen müssen, um die Wiederherstellung eines mit Trident Protect erstellten Backups oder Snapshots zu erleichtern, lesen Sie "Verwenden Sie Trident Protect AppVault-Objekte, um Buckets zu verwalten".

13. Optional können Sie den Abschnitt **Wiederherstellungsskripte** erweitern und die Option **Postscript** aktivieren, um eine Ausführungs-Hook-Vorlage auszuwählen, die nach Abschluss des Wiederherstellungsvorgangs ausgeführt wird. Geben Sie bei Bedarf alle Argumente ein, die das Skript benötigt, und fügen Sie Label-Selektoren hinzu, um Ressourcen anhand von Ressourcen-Labels zu filtern.
14. Optional können Sie den Abschnitt **Ressourcentransformationen** erweitern, um während des Wiederherstellungsprozesses Ressourcenattribute hinzuzufügen, zu entfernen oder zu ändern. Gehen Sie dann wie folgt vor:

    > Die Modifizierung von PersistentVolumeClaims und Namespaces wird derzeit nicht unterstützt.

    a. Aktivieren Sie die Option **Ressourcentransformation**, um Änderungen am Modifikator vorzunehmen.
    b. Wählen Sie eine Vorlage aus der **Vorlagen**-Liste, um häufig verwendete Modifikatoreinstellungen schnell anzuwenden. Diese Liste enthält vordefinierte Vorlagen für gängige Anwendungsfälle sowie von Ihnen erstellte benutzerdefinierte Vorlagen.

        > Erstellen Sie Ressourcentransformationsvorlagen im globalen "Einstellungen" Bereich.

    c. Geben Sie an, welche Ressource Sie ändern möchten, indem Sie die Ressourcengruppe, die Version, den Kind und den Namen eingeben.
    d. Geben Sie die Operation an, die Sie an der Ressource ausführen möchten, indem Sie eine Operation aus der Liste **Operation** auswählen.
    e. Geben Sie einen JSON-Pfad für den spezifischen Schlüssel ein, den Sie ändern möchten.
    f. Geben Sie gegebenenfalls einen neuen Wert ein. Das Feld **Wert** wird nur bei bestimmten Operationen angezeigt (z. B. **Hinzufügen** oder **Ersetzen**).
    g. Optional können bei Bedarf weitere Ressourcentransformationen hinzugefügt werden.
15. Wenn Sie fertig sind, wählen Sie **Wiederherstellen**.

Kubernetes-Anwendungen mithilfe einer benutzerdefinierten Ressource wiederherstellen

Sie können benutzerdefinierte Ressourcen verwenden, um Ihre Anwendungen aus einem Snapshot oder einem Backup wiederherzustellen. Die Wiederherstellung aus einem vorhandenen Snapshot ist schneller, wenn die Anwendung im selben Cluster wiederhergestellt wird.

- Wenn Sie eine Anwendung wiederherstellen, werden alle für die Anwendung konfigurierten Ausführungs-Hooks mit der Anwendung wiederhergestellt. Wenn ein Ausführungs-Hook nach der Wiederherstellung vorhanden ist, wird er automatisch als Teil des Wiederherstellungsvorgangs ausgeführt.
- Die Wiederherstellung aus einem Backup in einen anderen Namespace oder in den ursprünglichen Namespace wird für qtree Volumes unterstützt. Die Wiederherstellung aus einem Snapshot in einen anderen Namespace oder in den ursprünglichen Namespace wird für qtree Volumes jedoch nicht unterstützt.
- Sie können die Wiederherstellungsvorgänge mithilfe erweiterter Einstellungen anpassen. Weitere Informationen finden Sie unter "Erweiterte benutzerdefinierte Ressourcenwiederherstellungseinstellungen verwenden".

Eine Sicherung in einen anderen Namensraum wiederherstellen

Wenn Sie eine Sicherung mithilfe einer BackupRestore CR in einem anderen Namespace wiederherstellen, stellt Backup und Recovery die Anwendung in einem neuen Namespace wieder her und erstellt eine Anwendungs-CR für die wiederhergestellte Anwendung. Um die wiederhergestellte Anwendung zu schützen, erstellen Sie bedarfsgesteuerte Backups oder Snapshots oder legen Sie eine Datensicherungsstrategie fest.

- Die Wiederherstellung einer Sicherung in einem anderen Namensraum mit vorhandenen Ressourcen ändert keine Ressourcen, die denselben Namen wie die in der Sicherung haben. Um alle Ressourcen in der Sicherung wiederherzustellen, löschen und erstellen Sie entweder den Zielnamensraum neu oder stellen Sie die Sicherung in einem neuen Namensraum wieder her.
- Wenn Sie eine CR zur Wiederherstellung in einem neuen Namespace verwenden, müssen Sie den Ziel-Namespace manuell erstellen, bevor Sie die CR anwenden. Backup und Recovery erstellt Namespaces automatisch nur bei Verwendung der CLI.

Bevor Sie beginnen

Stellen Sie sicher, dass die Gültigkeitsdauer des AWS-Sitzungstokens für alle länger dauernden s3-Wiederherstellungsvorgänge ausreichend ist. Wenn das Token während des Wiederherstellungsvorgangs abläuft, kann der Vorgang fehlschlagen.

- Weitere Informationen zum Prüfen des Ablaufs des aktuellen Sitzungstokens finden Sie in der "AWS API-Dokumentation".
- Weitere Informationen zu Anmeldeinformationen für AWS-Ressourcen finden Sie im "AWS IAM-Dokumentation".

Wenn Sie Backups mit Kopia als Datenmover wiederherstellen, können Sie optional Anmerkungen in der CR angeben, um das Verhalten des von Kopia verwendeten temporären Speichers zu steuern. Weitere Informationen zu den Optionen, die Sie konfigurieren können, finden Sie in der "Kopia-Dokumentation".

Schritte

1. Erstellen Sie die benutzerdefinierte Ressourcendatei (CR) und benennen Sie sie `trident-protect-backup-restore-cr.yaml`.
2. Konfigurieren Sie in der von Ihnen erstellten Datei die folgenden Attribute:
   - **metadata.name**: (*Erforderlich*) Der Name dieser benutzerdefinierten Ressource; wählen Sie einen eindeutigen und sinnvollen Namen für Ihre Umgebung.

- **spec.appArchivePath**: Der Pfad innerhalb von AppVault, in dem die Sicherungsinhalte gespeichert sind. Sie können den folgenden Befehl verwenden, um diesen Pfad zu finden:

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
='{.status.appArchivePath}'
```

- **spec.appVaultRef**: (*Erforderlich*) Der Name des AppVault, in dem die Sicherungsinhalte gespeichert sind.
- **spec.namespaceMapping**: Die Zuordnung des Quell-Namespace des Wiederherstellungsvorgangs zum Ziel-Namespace. Ersetzen Sie `my-source-namespace` und `my-destination-namespace` durch Informationen aus Ihrer Umgebung.

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appArchivePath: my-backup-path
  appVaultRef: appvault-name
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

3. (*Optional*) Falls Sie nur bestimmte Ressourcen der Anwendung für die Wiederherstellung auswählen möchten, fügen Sie Filter hinzu, die Ressourcen mit bestimmten Bezeichnungen ein- oder ausschließen:

> Trident Protect wählt bestimmte Ressourcen automatisch aus, weil sie mit den von Ihnen ausgewählten Ressourcen in Beziehung stehen. Wenn Sie beispielsweise eine Ressource für einen persistenten Volume-Claim auswählen und diese einen zugehörigen Pod hat, wird Trident Protect auch den zugehörigen Pod wiederherstellen.

- **resourceFilter.resourceSelectionCriteria**: (Für die Filterung erforderlich) Verwenden Sie `Include` oder `Exclude`, um eine in resourceMatchers definierte Ressource ein- oder auszuschließen. Fügen Sie die folgenden resourceMatchers Parameter hinzu, um die Ressourcen zu definieren, die ein- oder auszuschließen sind:
  - **resourceFilter.resourceMatchers**: Ein Array von resourceMatcher-Objekten. Wenn Sie mehrere Elemente in diesem Array definieren, werden diese mit einer ODER-Verknüpfung verglichen und die Felder innerhalb jedes Elements (group, kind, version) werden mit einer UND-Verknüpfung verglichen.
    - **resourceMatchers[].group**: (*Optional*) Gruppe der zu filternden Ressource.
    - **resourceMatchers[].kind**: (*Optional*) Art der zu filternden Ressource.
    - **resourceMatchers[].version**: (*Optional*) Version der zu filternden Ressource.
    - **resourceMatchers[].names**: (*Optional*) Namen im Kubernetes metadata.name-Feld der Ressource, die gefiltert werden soll.
    - **resourceMatchers[].namespaces**: (*Optional*) Namespaces im Kubernetes metadata.name-

Feld der Ressource, die gefiltert werden soll.

- **resourceMatchers[].labelSelectors**: (*Optional*) Label-Selektorzeichenfolge im Kubernetes-Metadatenfeld name der Ressource, wie definiert in der "Kubernetes-Dokumentation". Zum Beispiel: `"trident.netapp.io/os=linux"`.

  Beispiel:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Nachdem Sie die `trident-protect-backup-restore-cr.yaml` Datei mit den korrekten Werten gefüllt haben, wenden Sie die CR an:

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

Stellen Sie ein Backup im ursprünglichen Namespace wieder her

Sie können ein Backup jederzeit im ursprünglichen Namespace wiederherstellen.

Bevor Sie beginnen

Stellen Sie sicher, dass die Gültigkeitsdauer des AWS-Sitzungstokens für alle länger dauernden s3-Wiederherstellungsvorgänge ausreichend ist. Wenn das Token während des Wiederherstellungsvorgangs abläuft, kann der Vorgang fehlschlagen.

- Weitere Informationen zum Prüfen des Ablaufs des aktuellen Sitzungstokens finden Sie in der "AWS API-Dokumentation".
- Weitere Informationen zu Anmeldeinformationen für AWS-Ressourcen finden Sie im "AWS IAM-Dokumentation".

Wenn Sie Backups mit Kopia als Datenmover wiederherstellen, können Sie optional Anmerkungen in der CR angeben, um das Verhalten des von Kopia verwendeten temporären Speichers zu steuern. Weitere Informationen zu den Optionen, die Sie konfigurieren können, finden Sie in der "Kopia-Dokumentation".

Schritte

1. Erstellen Sie die benutzerdefinierte Ressourcendatei (CR) und benennen Sie sie `trident-protect-backup-ipr-cr.yaml`.
2. Konfigurieren Sie in der von Ihnen erstellten Datei die folgenden Attribute:
   - **metadata.name**: (*Erforderlich*) Der Name dieser benutzerdefinierten Ressource; wählen Sie einen eindeutigen und sinnvollen Namen für Ihre Umgebung.
   - **spec.appArchivePath**: Der Pfad innerhalb von AppVault, in dem die Sicherungsinhalte gespeichert sind. Sie können den folgenden Befehl verwenden, um diesen Pfad zu finden:

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
     ='{.status.appArchivePath}'
     ```

   - **spec.appVaultRef**: (*Erforderlich*) Der Name des AppVault, in dem die Sicherungsinhalte gespeichert sind.

     Beispiel:

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appArchivePath: my-backup-path
  appVaultRef: appvault-name
```

3. (*Optional*) Falls Sie nur bestimmte Ressourcen der Anwendung für die Wiederherstellung auswählen möchten, fügen Sie Filter hinzu, die Ressourcen mit bestimmten Bezeichnungen ein- oder ausschließen:

   Trident Protect wählt bestimmte Ressourcen automatisch aus, weil sie mit den von Ihnen ausgewählten Ressourcen in Beziehung stehen. Wenn Sie beispielsweise eine Ressource für einen persistenten Volume-Claim auswählen und diese einen zugehörigen Pod hat, wird Trident Protect auch den zugehörigen Pod wiederherstellen.

   - **resourceFilter.resourceSelectionCriteria**: (Für die Filterung erforderlich) Verwenden Sie `Include` oder `Exclude`, um eine in resourceMatchers definierte Ressource ein- oder auszuschließen. Fügen Sie die folgenden resourceMatchers Parameter hinzu, um die Ressourcen zu definieren, die ein- oder auszuschließen sind:
     - **resourceFilter.resourceMatchers**: Ein Array von resourceMatcher-Objekten. Wenn Sie mehrere Elemente in diesem Array definieren, werden diese mit einer ODER-Verknüpfung verglichen und die Felder innerhalb jedes Elements (group, kind, version) werden mit einer UND-Verknüpfung

verglichen.

- **resourceMatchers[].group**: (*Optional*) Gruppe der zu filternden Ressource.
- **resourceMatchers[].kind**: (*Optional*) Art der zu filternden Ressource.
- **resourceMatchers[].version**: (*Optional*) Version der zu filternden Ressource.
- **resourceMatchers[].names**: (*Optional*) Namen im Kubernetes metadata.name-Feld der Ressource, die gefiltert werden soll.
- **resourceMatchers[].namespaces**: (*Optional*) Namespaces im Kubernetes metadata.name-Feld der Ressource, die gefiltert werden soll.
- **resourceMatchers[].labelSelectors**: (*Optional*) Label-Selektorzeichenfolge im Kubernetes-Metadatenfeld name der Ressource, wie definiert in der "Kubernetes-Dokumentation". Zum Beispiel: `"trident.netapp.io/os=linux"`.

  Beispiel:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Nachdem Sie die `trident-protect-backup-ipr-cr.yaml` Datei mit den korrekten Werten gefüllt haben, wenden Sie die CR an:

```
kubectl apply -f trident-protect-backup-ipr-cr.yaml
```

Stellen Sie ein Backup auf einem anderen Cluster wieder her

Sie können ein Backup auf einem anderen Cluster wiederherstellen, wenn es ein Problem mit dem ursprünglichen Cluster gibt.

- Wenn Sie Backups mit Kopia als Datenmover wiederherstellen, können Sie optional Anmerkungen in der CR angeben, um das Verhalten des von Kopia verwendeten temporären Speichers zu steuern. Weitere Informationen zu den Optionen, die Sie konfigurieren können, finden Sie in der "Kopia-Dokumentation".
- Wenn Sie eine CR verwenden, um in einem neuen Namespace wiederherzustellen, müssen Sie den Ziel-Namespace manuell erstellen, bevor Sie die CR anwenden.

Bevor Sie beginnen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Auf dem Ziel-Cluster ist Trident Protect installiert.
- Der Ziel-Cluster hat Zugriff auf den Bucket-Pfad desselben AppVault wie der Quell-Cluster, in dem die Sicherung gespeichert ist.
- Stellen Sie sicher, dass die Gültigkeitsdauer des AWS-Sitzungstokens für alle länger dauernden Wiederherstellungsvorgänge ausreichend ist. Wenn das Token während des Wiederherstellungsvorgangs abläuft, kann der Vorgang fehlschlagen.
  - Weitere Informationen zum Prüfen des Ablaufs des aktuellen Sitzungstokens finden Sie in der "AWS API-Dokumentation".
  - Weitere Informationen zu Anmeldeinformationen für AWS-Ressourcen finden Sie in der "AWS-Dokumentation".

Schritte

1. Überprüfen Sie die Verfügbarkeit des AppVault CR auf dem Ziel-Cluster mithilfe des Trident Protect CLI-Plugins:

   ```
   tridentctl-protect get appvault --context <destination_cluster_name>
   ```

   Stellen Sie sicher, dass der für die Anwendungswiederherstellung vorgesehene Namespace auf dem Ziel-Cluster vorhanden ist.

2. Zeigen Sie die Sicherungsinhalte des verfügbaren AppVault vom Ziel-Cluster an:

   ```
   tridentctl-protect get appvaultcontent <appvault_name> \
   --show-resources backup \
   --show-paths \
   --context <destination_cluster_name>
   ```

   Durch Ausführen dieses Befehls werden die verfügbaren Backups im AppVault angezeigt, einschließlich ihrer Ursprungscluster, entsprechenden Anwendungsnamen, Zeitstempel und Archivpfade.

   Beispielausgabe:

```
+------------+----------+--------+-----------------
+-------------------------+-------------+
|   CLUSTER   |    APP    |  TYPE  |      NAME       |        TIMESTAMP
|    PATH     |
+------------+----------+--------+-----------------
+-------------------------+-------------+
| production1 | wordpress | backup | wordpress-bkup-1| 2024-10-30
08:37:40 (UTC)| backuppath1 |
| production1 | wordpress | backup | wordpress-bkup-2| 2024-10-30
08:37:40 (UTC)| backuppath2 |
+------------+----------+--------+-----------------
+-------------------------+-------------+
```

3. Stellen Sie die Anwendung im Ziel-Cluster mithilfe des AppVault-Namens und des Archivpfads wieder her:
4. Erstellen Sie die benutzerdefinierte Ressourcendatei (CR) und benennen Sie sie `trident-protect-backup-restore-cr.yaml`.
5. Konfigurieren Sie in der von Ihnen erstellten Datei die folgenden Attribute:
   - **metadata.name**: (*Erforderlich*) Der Name dieser benutzerdefinierten Ressource; wählen Sie einen eindeutigen und sinnvollen Namen für Ihre Umgebung.
   - **spec.appVaultRef**: (*Erforderlich*) Der Name des AppVault, in dem die Sicherungsinhalte gespeichert sind.
   - **spec.appArchivePath**: Der Pfad innerhalb von AppVault, in dem die Sicherungsinhalte gespeichert sind. Sie können den folgenden Befehl verwenden, um diesen Pfad zu finden:

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
     ='{.status.appArchivePath}'
     ```

     Falls BackupRestore CR nicht verfügbar ist, können Sie den in Schritt 2 genannten Befehl verwenden, um den Sicherungsinhalt anzuzeigen.

   - **spec.namespaceMapping**: Die Zuordnung des Quell-Namespace des Wiederherstellungsvorgangs zum Ziel-Namespace. Ersetzen Sie `my-source-namespace` und `my-destination-namespace` durch Informationen aus Ihrer Umgebung.

     Beispiel:

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-backup-path
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

6. Nachdem Sie die `trident-protect-backup-restore-cr.yaml` Datei mit den korrekten Werten gefüllt haben, wenden Sie die CR an:

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

Einen Snapshot in einen anderen Namespace wiederherstellen

Sie können Daten aus einem Snapshot mithilfe einer benutzerdefinierten Ressourcendatei (CR) entweder in einem anderen Namespace oder im ursprünglichen Quell-Namespace wiederherstellen. Wenn Sie einen Snapshot mithilfe einer SnapshotRestore CR in einem anderen Namespace wiederherstellen, stellt Backup und Recovery die Anwendung in einem neuen Namespace wieder her und erstellt eine Anwendungs-CR für die wiederhergestellte Anwendung. Um die wiederhergestellte Anwendung zu schützen, erstellen Sie On-Demand-Backups oder Snapshots, oder legen Sie einen Datensicherungszeitplan fest.

- SnapshotRestore unterstützt das `spec.storageClassMapping` Attribut, jedoch nur, wenn die Quell- und Ziel-Speicherklassen dasselbe Speicher-Backend verwenden. Wenn Sie versuchen, auf eine `StorageClass` wiederherzustellen, die ein anderes Speicher-Backend verwendet, schlägt der Wiederherstellungsvorgang fehl.
- Wenn Sie eine CR verwenden, um in einem neuen Namespace wiederherzustellen, müssen Sie den Ziel-Namespace manuell erstellen, bevor Sie die CR anwenden.

Bevor Sie beginnen

Stellen Sie sicher, dass die Gültigkeitsdauer des AWS-Sitzungstokens für alle länger dauernden s3-Wiederherstellungsvorgänge ausreichend ist. Wenn das Token während des Wiederherstellungsvorgangs abläuft, kann der Vorgang fehlschlagen.

- Weitere Informationen zum Prüfen des Ablaufs des aktuellen Sitzungstokens finden Sie in der "AWS API-Dokumentation".
- Weitere Informationen zu Anmeldeinformationen für AWS-Ressourcen finden Sie im "AWS IAM-Dokumentation".

Schritte

1. Erstellen Sie die benutzerdefinierte Ressourcendatei (CR) und benennen Sie sie `trident-protect-snapshot-restore-cr.yaml`.
2. Konfigurieren Sie in der von Ihnen erstellten Datei die folgenden Attribute:

- **metadata.name**: (*Erforderlich*) Der Name dieser benutzerdefinierten Ressource; wählen Sie einen eindeutigen und sinnvollen Namen für Ihre Umgebung.
- **spec.appVaultRef**: (*Erforderlich*) Der Name des AppVault, in dem die Snapshot-Inhalte gespeichert sind.
- **spec.appArchivePath**: Der Pfad innerhalb von AppVault, in dem die Snapshot-Inhalte gespeichert sind. Sie können den folgenden Befehl verwenden, um diesen Pfad zu finden:

```
kubectl get snapshots <SNAPHOT_NAME> -n my-app-namespace -o jsonpath
='{.status.appArchivePath}'
```

- **spec.namespaceMapping**: Die Zuordnung des Quell-Namespace des Wiederherstellungsvorgangs zum Ziel-Namespace. Ersetzen Sie `my-source-namespace` und `my-destination-namespace` durch Informationen aus Ihrer Umgebung.

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-snapshot-path
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

3. (*Optional*) Falls Sie nur bestimmte Ressourcen der Anwendung für die Wiederherstellung auswählen möchten, fügen Sie Filter hinzu, die Ressourcen mit bestimmten Bezeichnungen ein- oder ausschließen:

> Trident Protect wählt bestimmte Ressourcen automatisch aus, weil sie mit den von Ihnen ausgewählten Ressourcen in Beziehung stehen. Wenn Sie beispielsweise eine Ressource für einen persistenten Volume-Claim auswählen und diese einen zugehörigen Pod hat, wird Trident Protect auch den zugehörigen Pod wiederherstellen.

- **resourceFilter.resourceSelectionCriteria**: (Für die Filterung erforderlich) Verwenden Sie `Include` oder `Exclude`, um eine in resourceMatchers definierte Ressource ein- oder auszuschließen. Fügen Sie die folgenden resourceMatchers Parameter hinzu, um die Ressourcen zu definieren, die ein- oder auszuschließen sind:
  - **resourceFilter.resourceMatchers**: Ein Array von resourceMatcher-Objekten. Wenn Sie mehrere Elemente in diesem Array definieren, werden diese mit einer ODER-Verknüpfung verglichen und die Felder innerhalb jedes Elements (group, kind, version) werden mit einer UND-Verknüpfung verglichen.
    - **resourceMatchers[].group**: (*Optional*) Gruppe der zu filternden Ressource.
    - **resourceMatchers[].kind**: (*Optional*) Art der zu filternden Ressource.
    - **resourceMatchers[].version**: (*Optional*) Version der zu filternden Ressource.
    - **resourceMatchers[].names**: (*Optional*) Namen im Kubernetes metadata.name-Feld der

Ressource, die gefiltert werden soll.

- **resourceMatchers[].namespaces**: (*Optional*) Namespaces im Kubernetes metadata.name-Feld der Ressource, die gefiltert werden soll.
- **resourceMatchers[].labelSelectors**: (*Optional*) Label-Selektorzeichenfolge im Kubernetes-Metadatenfeld name der Ressource, wie definiert in der "Kubernetes-Dokumentation". Zum Beispiel: `"trident.netapp.io/os=linux"`.

  Beispiel:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Nachdem Sie die `trident-protect-snapshot-restore-cr.yaml` Datei mit den korrekten Werten gefüllt haben, wenden Sie die CR an:

```
kubectl apply -f trident-protect-snapshot-restore-cr.yaml
```

Einen Snapshot im ursprünglichen Namensraum wiederherstellen

Sie können einen Snapshot jederzeit im ursprünglichen Namensraum wiederherstellen.

> Die In-Place-Wiederherstellung (Wiederherstellung im ursprünglichen Namespace und ursprünglichen Cluster) von VM-basierten Anwendungen aus lokalen Snapshots wird derzeit nicht unterstützt.

Bevor Sie beginnen

Stellen Sie sicher, dass die Gültigkeitsdauer des AWS-Sitzungstokens für alle länger dauernden s3-Wiederherstellungsvorgänge ausreichend ist. Wenn das Token während des Wiederherstellungsvorgangs abläuft, kann der Vorgang fehlschlagen.

- Weitere Informationen zum Prüfen des Ablaufs des aktuellen Sitzungstokens finden Sie in der "AWS API-Dokumentation".

- Weitere Informationen zu Anmeldeinformationen für AWS-Ressourcen finden Sie im "AWS IAM-Dokumentation".

Schritte

1. Erstellen Sie die benutzerdefinierte Ressourcendatei (CR) und benennen Sie sie `trident-protect-snapshot-ipr-cr.yaml`.
2. Konfigurieren Sie in der von Ihnen erstellten Datei die folgenden Attribute:
   - **metadata.name**: (*Erforderlich*) Der Name dieser benutzerdefinierten Ressource; wählen Sie einen eindeutigen und sinnvollen Namen für Ihre Umgebung.
   - **spec.appVaultRef**: (*Erforderlich*) Der Name des AppVault, in dem die Snapshot-Inhalte gespeichert sind.
   - **spec.appArchivePath**: Der Pfad innerhalb von AppVault, in dem die Snapshot-Inhalte gespeichert sind. Sie können den folgenden Befehl verwenden, um diesen Pfad zu finden:

     ```
     kubectl get snapshots <SNAPSHOT_NAME> -n my-app-namespace -o jsonpath='{.status.appArchivePath}'
     ```

     ```
     apiVersion: protect.trident.netapp.io/v1
     kind: SnapshotInplaceRestore
     metadata:
       name: my-cr-name
       namespace: my-app-namespace
     spec:
       appVaultRef: appvault-name
       appArchivePath: my-snapshot-path
     ```

3. (*Optional*) Falls Sie nur bestimmte Ressourcen der Anwendung für die Wiederherstellung auswählen möchten, fügen Sie Filter hinzu, die Ressourcen mit bestimmten Bezeichnungen ein- oder ausschließen:

   Trident Protect wählt bestimmte Ressourcen automatisch aus, weil sie mit den von Ihnen ausgewählten Ressourcen in Beziehung stehen. Wenn Sie beispielsweise eine Ressource für einen persistenten Volume-Claim auswählen und diese einen zugehörigen Pod hat, wird Trident Protect auch den zugehörigen Pod wiederherstellen.

   - **resourceFilter.resourceSelectionCriteria**: (Für die Filterung erforderlich) Verwenden Sie `Include` oder `Exclude`, um eine in resourceMatchers definierte Ressource ein- oder auszuschließen. Fügen Sie die folgenden resourceMatchers Parameter hinzu, um die Ressourcen zu definieren, die ein- oder auszuschließen sind:
     - **resourceFilter.resourceMatchers**: Ein Array von resourceMatcher-Objekten. Wenn Sie mehrere Elemente in diesem Array definieren, werden diese mit einer ODER-Verknüpfung verglichen und die Felder innerhalb jedes Elements (group, kind, version) werden mit einer UND-Verknüpfung verglichen.
       - **resourceMatchers[].group**: (*Optional*) Gruppe der zu filternden Ressource.
       - **resourceMatchers[].kind**: (*Optional*) Art der zu filternden Ressource.

- **resourceMatchers[].version**: (*Optional*) Version der zu filternden Ressource.
- **resourceMatchers[].names**: (*Optional*) Namen im Kubernetes metadata.name-Feld der Ressource, die gefiltert werden soll.
- **resourceMatchers[].namespaces**: (*Optional*) Namespaces im Kubernetes metadata.name-Feld der Ressource, die gefiltert werden soll.
- **resourceMatchers[].labelSelectors**: (*Optional*) Label-Selektorzeichenfolge im Kubernetes-Metadatenfeld name der Ressource, wie definiert in der "Kubernetes-Dokumentation". Zum Beispiel: `"trident.netapp.io/os=linux"`.

  Beispiel:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Nachdem Sie die `trident-protect-snapshot-ipr-cr.yaml` Datei mit den korrekten Werten gefüllt haben, wenden Sie die CR an:

```
kubectl apply -f trident-protect-snapshot-ipr-cr.yaml
```

Erweiterte benutzerdefinierte Ressourcenwiederherstellungseinstellungen verwenden

Sie können Wiederherstellungsvorgänge mithilfe erweiterter Einstellungen wie Annotationen, Namespace-Einstellungen und Speicheroptionen an Ihre spezifischen Anforderungen anpassen.

Namespace-Annotationen und -Labels während Wiederherstellungs- und Failover-Operationen

Bei Wiederherstellung und Failover werden die Namespace-Bezeichnungen und -Annotationen des Ziels aktualisiert, um mit denen der Quelle übereinzustimmen: Schlüssel aus der Quelle werden zu den Zielschlüsseln hinzugefügt oder überschrieben, während Schlüssel, die nur im Ziel existieren, unverändert

bleiben.

> In Red Hat OpenShift sind Namespace-Annotationen wichtig, da sie sicherstellen, dass wiederhergestellte Pods die korrekten Sicherheitskontextbeschränkungen und Berechtigungen erhalten, sodass sie auf Volumes zugreifen und ohne Berechtigungsfehler ausgeführt werden können. Weitere Informationen finden Sie unter "OpenShift security context constraints Dokumentation".

Setzen Sie die Kubernetes-Umgebungsvariable

```
RESTORE_SKIP_NAMESPACE_ANNOTATIONS
```

Vor der Wiederherstellung oder dem Failover sollte verhindert werden, dass bestimmte Ziel-Namespace-Annotationen überschrieben werden. Zum Beispiel:

```
helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect \
  --set-string
restoreSkipNamespaceAnnotations="{<annotation_key_to_skip_1>,<annotation_k
ey_to_skip_2>}" \
  --reuse-values
```

> Während der Wiederherstellung oder des Failovers werden alle in `restoreSkipNamespaceAnnotations` und `restoreSkipNamespaceLabels` angegebenen Namespace-Annotationen und -Labels von der Wiederherstellungs- oder Failover-Operation ausgeschlossen. Stellen Sie sicher, dass diese Einstellungen während der initialen Helm-Installation konfiguriert sind. Weitere Informationen finden Sie unter "Konfigurieren Sie zusätzliche Trident Protect Helm-Chart-Einstellungen".

Wenn Sie Helm mit dem `--create-namespace` Flag zur Installation der Quellanwendung verwendet haben, kopiert Trident Protect die Namensbezeichnung in den Ziel-Namespace. Stimmt der Wert der Bezeichnung mit dem Namen des Quell-Namespace überein, wird er durch den Namen des Ziel-Namespace ersetzt; andernfalls bleibt er unverändert.

Beispiel

Das folgende Beispiel zeigt Quell- und Ziel-Namensräume mit unterschiedlichen Bezeichnungen und Annotationen und zeigt den Ziel-Namensraum vor und nach der Operation, um zu veranschaulichen, wie Schlüssel hinzugefügt, zusammengeführt oder überschrieben werden.

Vor dem Wiederherstellungs- oder Failover-Vorgang

Die folgende Tabelle veranschaulicht den Zustand der Beispiel-Quell- und Ziel-Namespaces vor der Wiederherstellungs- oder Failover-Operation:

Namensraum	Anmerkungen	Etiketten
Namespace ns-1 (Quelle)	• annotation.one/key: "updatedvalue" • annotation.two/key: "true"	• environment=production • compliance=hipaa • name=ns-1
Namespace ns-2 (Ziel)	• annotation.one/key: "true" • annotation.three/key: "false"	• role=database

Nach dem Wiederherstellungsvorgang

Die folgende Tabelle veranschaulicht den Zustand des Beispiel-Ziel-Namespace nach der Wiederherstellung oder dem Failover. Einige Schlüssel wurden hinzugefügt, einige wurden überschrieben, und das `name` Label wurde aktualisiert, um dem Ziel-Namespace zu entsprechen:

Namensraum	Anmerkungen	Etiketten
Namespace ns-2 (Ziel)	• annotation.one/key: "updatedvalue" • annotation.two/key: "true" • annotation.three/key: "false"	• name=ns-2 • compliance=hipaa • environment=production • role=database

Unterstützte Felder

In diesem Abschnitt werden zusätzliche Felder beschrieben, die für Wiederherstellungsvorgänge zur Verfügung stehen.

Speicherklassenzuordnung

Das `spec.storageClassMapping` Attribut definiert eine Zuordnung von einer Speicherklasse in der Quellanwendung zu einer neuen Speicherklasse im Zielcluster. Sie können dies verwenden, wenn Sie Anwendungen zwischen Clustern mit unterschiedlichen Speicherklassen migrieren oder das Speicher-Backend für BackupRestore-Operationen ändern.

Beispiel:

```
storageClassMapping:
  - destination: "destinationStorageClass1"
    source: "sourceStorageClass1"
  - destination: "destinationStorageClass2"
    source: "sourceStorageClass2"
```

Unterstützte Annotationen

Dieser Abschnitt listet die unterstützten Annotationen zur Konfiguration verschiedener Verhaltensweisen im System auf. Wenn eine Annotation nicht explizit vom Benutzer festgelegt wird, verwendet das System den Standardwert.

Anmerkung	Typ	Beschreibung	Standardwert
protect.trident.netapp.io/data-mover-timeout-sec	Zeichenkette	Die maximal zulässige Zeit (in Sekunden), in der der Datenübertragungsvorgang angehalten werden darf.	"300"
protect.trident.netapp.io/kopia-content-cache-size-limit-mb	Zeichenkette	Die maximale Größenbeschränkung (in Megabytes) für den Kopia-Inhaltscache.	"1000"
protect.trident.netapp.io/pvc-bind-timeout-sec	Zeichenkette	Maximale Zeit (in Sekunden), die auf neu erstellte PersistentVolumeClaims (PVCs) gewartet wird, um die `Bound` Phase zu erreichen, bevor der Vorgang fehlschlägt. Gilt für alle Restore-CR-Typen (BackupRestore, BackupInplaceRestore, SnapshotRestore, SnapshotInplaceRestore). Verwenden Sie einen höheren Wert, wenn Ihr Storage-Backend oder Cluster häufig mehr Zeit benötigt.	"1200" (20 Minuten)

Ändern Sie Ressourcen während der Wiederherstellung mithilfe benutzerdefinierter Ressourcen

Ressourcentransformationen ermöglichen es Ihnen, eine Ressource während der Wiederherstellung zu modifizieren. Dies ist nützlich, wenn die wiederhergestellte Version von der ursprünglichen Version abweichen soll – beispielsweise die Änderung der IP-Adresse einer virtuellen Maschine bei der Wiederherstellung in einem anderen Netzwerk. Sie können auch "Modifizieren Sie Ressourcen während der Wiederherstellung mithilfe der Web-Benutzeroberfläche".

Erforderliche NetApp Console-Rolle Backup and Recovery Superadministrator oder Backup and Recovery Wiederherstellungsadministrator. "Erfahren Sie mehr über die Zugriffsrollen für NetApp Backup and Recovery". "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste".

Wie Ressourcenmodifikation funktioniert

Das `transformations` Feld in `SnapshotRestore`, `BackupRestore`, `AppMirrorRelationship` und anderen Wiederherstellungsressourcen ermöglicht es Ihnen, Kubernetes-Ressourcen während des Wiederherstellungsprozesses zu ändern. Dies ist nützlich, um Anwendungen oder virtuelle Maschinen an einen neuen Cluster anzupassen, indem Sie Hostnamen, Registry-URLs, Ressourcenlimits oder Umgebungsvariablen ändern.

Ressourcentransformationen verwenden "RFC 6902" JSON-Patch-Operationen und "RFC 6901" JSON-Pointer-Pfade, um bestimmte Felder innerhalb von Kubernetes-Ressourcen anzusprechen und zu modifizieren.

Hier ist die grundlegende Struktur eines Wiederherstellungsobjekts, das Ressourcentransformationen enthält:

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  name: my-restore
  namespace: target-namespace
spec:
  appVaultRef: my-vault
  appArchivePath: /path/to/snapshot
  namespaceMapping:
    - source: source-ns
      destination: target-ns
  transformations:
    - resource:
        kind: ConfigMap       # Required: resource kind
        group: ""             # Optional: API group (empty for core
resources)
        version: ""           # Optional: API version
        name: ""              # Optional: specific resource name
      operations:
        - op: replace         # Operation type
          path: "/data/key"   # JSON Pointer path
          value: "new-value"  # New value (for add/replace/test)
```

Unterstützte Ressourcen

Sie können Ressourcentransformationen mit Ressourcen verwenden, die den folgenden Kriterien entsprechen:

- `kind` (erforderlich): Der Kubernetes-Ressourcentyp (zum Beispiel, `ConfigMap`, `Deployment`, `Pod`)
- `group` (optional): Die API-Gruppe (zum Beispiel, `apps`, `route.openshift.io`) - für Kernressourcen weglassen
- `version` (optional): Die API-Version (z. B. `v1`, `v1beta1`)
- `name` (optional): Nur auf eine bestimmte Ressource anhand des Namens anwenden

Die Modifizierung von PersistentVolumeClaims und Namespaces wird derzeit nicht unterstützt.

Unterstützte Operationen

Sie können die folgenden Operationen verwenden, um Ressourcen zu ändern:

- `add`: Füge einer Ressource einen Wert hinzu.
- `copy`: Einen Wert von einem Pfad in einen anderen kopieren.
- `move`: Einen Wert innerhalb einer Ressource verschieben.
- `remove`: Einen Wert aus einer Ressource entfernen.
- `replace`: Ersetzen Sie einen Wert innerhalb einer Ressource.

- `test`: Testen Sie eine Operation, bevor Sie sie ausführen.

Einer Ressource einen Wert hinzufügen

Verwenden Sie die `add`-Operation, um ein neues Feld oder einen neuen Wert am angegebenen Pfad hinzuzufügen. Sie können Daten zu Objekten oder Arrays hinzufügen. Das folgende Beispiel fügt einer Deployment-Ressource einen Knotenselektor hinzu:

```
transformations:
  - resource:
      kind: Deployment
    operations:
      - op: add
        path: "/spec/template/spec/nodeSelector"
        value:
          "topology.kubernetes.io/zone": "us-east-1a"
          disktype: "ssd"
```

Verwenden Sie den folgenden Befehl, um diese Transformation über die Befehlszeile auszuführen:

```
tridentctl-protect --transformation
'apps,v1,Deployment:add{"path":"/spec/template/spec/nodeSelector","value":
{"topology.kubernetes.io/zone":"us-east-1a","disktype":"ssd"}}'
```

Einen Wert innerhalb einer Ressource kopieren

Verwenden Sie die `copy`Operation, um einen Wert innerhalb derselben Ressource von einem Pfad in einen anderen zu kopieren. Die Quelle bleibt unverändert. Das folgende Beispiel dupliziert einen Datenschlüssel für ein ConfigMap-Objekt:

```
transformations:
  - resource:
      kind: ConfigMap
    operations:
      - op: copy
        from: "/data/source-key"
        path: "/data/backup-key"
```

Verwenden Sie den folgenden Befehl, um diese Transformation über die Befehlszeile auszuführen:

```
tridentctl-protect --transformation
',v1,ConfigMap:copy{"from":"/data/source-key","path":"/data/backup-key"}'
```

Verschieben Sie einen Wert innerhalb einer Ressource

Verwenden Sie die `move`-Operation, um einen Wert innerhalb derselben Ressource von einem Pfad zu einem anderen zu verschieben. Die Quelle wird entfernt und der Wert am Zielort eingefügt. Das folgende Beispiel benennt einen Datenschlüssel für ein ConfigMap-Objekt um:

```
transformations:
  - resource:
      kind: ConfigMap
    operations:
      - op: move
        from: "/data/OLD_KEY"
        path: "/data/NEW_KEY"
```

Verwenden Sie den folgenden Befehl, um diese Transformation über die Befehlszeile auszuführen:

```
tridentctl-protect --transformation
',v1,ConfigMap:move{"from":"/data/OLD_KEY","path":"/data/NEW_KEY"}'
```

Einen Wert aus einer Ressource entfernen

Verwenden Sie die `remove` Operation, um ein Feld oder einen Wert am angegebenen Pfad zu entfernen. Das folgende Beispiel entfernt eine Annotation aus einer ConfigMap-Ressource:

```
transformations:
  - resource:
      kind: ConfigMap
    operations:
      - op: remove
        path: "/metadata/annotations/kubectl.kubernetes.io~1last-applied-
configuration"
```

Im Pfad des obigen Beispiels `~1` ist die JSON Pointer Escape-Sequenz für `/`.

Verwenden Sie den folgenden Befehl, um diese Transformation über die Befehlszeile auszuführen:

```
tridentctl-protect --transformation
',v1,ConfigMap:remove{"path":"/metadata/annotations/kubectl.kubernetes.io~
1last-applied-configuration"}'
```

Ersetzen Sie einen Wert innerhalb einer Ressource

Verwenden Sie die `replace` Operation, um einen vorhandenen Wert innerhalb einer Ressource am angegebenen Pfad zu ersetzen. Der JSON-Pfad muss bereits existieren. Das folgende Beispiel ändert einen

Hostnamen für ein Route-Objekt:

```
transformations:
  - resource:
      kind: Route
      group: route.openshift.io
    operations:
      - op: replace
        path: "/spec/host"
        value: "prod.example.com"
```

Verwenden Sie den folgenden Befehl, um diese Transformation über die Befehlszeile auszuführen:

```
tridentctl-protect --transformation
'route.openshift.io,v1,Route:replace{"path":"/spec/host","value":"prod.exa
mple.com"}'
```

Testen Sie die Ressourcenänderung

Verwenden Sie die `test`Operation, um zu testen, ob der Wert an einem Pfad dem erwarteten Wert entspricht. Wenn der Test fehlschlägt, wird die gesamte Änderung zurückgesetzt. Im folgenden Beispiel wird `database-host`nur aktualisiert, wenn `environment staging` entspricht:

```
transformations:
  - resource:
      kind: ConfigMap
    operations:
      - op: test
        path: "/data/environment"
        value: "staging"
      - op: replace
        path: "/data/database-host"
        value: "prod-db.example.com"
```

Verwenden Sie den folgenden Befehl, um diese Transformation über die Befehlszeile auszuführen:

```
tridentctl-protect --transformation
',v1,ConfigMap:test{"path":"/data/environment","value":"staging"},replace{
"path":"/data/database-host","value":"prod-db.example.com"}'
```

Verwalten von Kubernetes-Clustern

Mit NetApp Backup and Recovery können Sie Ihre Kubernetes-Cluster erkennen und verwalten, sodass Sie die von den Clustern gehosteten Ressourcen schützen können.

Erforderliche NetApp Console

Organisationsadministrator oder SnapCenter Administrator. "Erfahren Sie mehr über die Zugriffsrollen für NetApp Backup and Recovery" . "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Informationen zum Erkennen von Kubernetes-Clustern finden Sie unter"Entdecken Sie Kubernetes-Workloads" .

Kubernetes-Clusterinformationen bearbeiten

Sie können einen Cluster bearbeiten, wenn Sie seinen Namen ändern müssen.

Schritte

1. Wählen Sie in NetApp Backup and Recovery*Inventar* > **Cluster**.
2. Wählen Sie in der Liste der Cluster einen Cluster aus, den Sie bearbeiten möchten, und wählen Sie das zugehörige Aktionsmenü aus.
3. Wählen Sie **Cluster bearbeiten**.
4. Nehmen Sie alle erforderlichen Änderungen am Clusternamen vor. Der Clustername muss mit dem Namen übereinstimmen, den Sie während des Erkennungsprozesses mit dem Helm-Befehl verwendet haben.
5. Wählen Sie **Fertig**.

Entfernen eines Kubernetes-Clusters

Um den Schutz eines Kubernetes-Clusters zu beenden, deaktivieren Sie den Schutz und löschen Sie die zugehörigen Anwendungen. Entfernen Sie anschließend den Cluster aus NetApp Backup and Recovery. NetApp Backup and Recovery löscht weder den Cluster noch seine Ressourcen, sondern entfernt den Cluster lediglich aus dem Inventar der NetApp Console .

Schritte

1. Wählen Sie in NetApp Backup and Recovery*Inventar* > **Cluster**.
2. Wählen Sie in der Liste der Cluster einen Cluster aus, den Sie bearbeiten möchten, und wählen Sie das zugehörige Aktionsmenü aus.
3. Wählen Sie **Cluster entfernen**.
4. Überprüfen Sie die Informationen im Bestätigungsdialogfeld und wählen Sie **Entfernen**.

Trident Protect aktualisieren

Für Kubernetes-Cluster mit Trident Protect 26.05 oder höher können Sie Trident Protect direkt aus NetApp Backup and Recovery aktualisieren. Die Aktualisierungsoption wird nur angezeigt, wenn eine neuere Version verfügbar ist.

Schritte

1. Wählen Sie in NetApp Backup and Recovery*Inventar* > **Cluster**.

2. Wählen Sie einen Kubernetes-Cluster für das Upgrade aus und klicken Sie auf das Symbol ••• > **Cluster aktualisieren**.
3. Führen Sie im Upgrade-Dialog folgende Schritte aus:
   a. Wählen Sie aus der Liste die Version aus, auf die Sie aktualisieren möchten.
   b. Wählen Sie **Upgrade**.

Verwalten von Kubernetes-Anwendungen

Mit NetApp Backup and Recovery können Sie den Schutz Ihrer Kubernetes-Anwendungen und der zugehörigen Ressourcen aufheben und diese löschen.

Erforderliche NetApp Console

Organisationsadministrator oder SnapCenter Administrator. "Erfahren Sie mehr über die Zugriffsrollen für NetApp Backup and Recovery" . "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Aufheben des Schutzes einer Kubernetes-Anwendung

Sie können den Schutz einer Anwendung aufheben, wenn Sie sie nicht mehr schützen möchten. Wenn Sie den Schutz einer Anwendung aufheben, beendet NetApp Backup and Recovery den Schutz der Anwendung, behält jedoch alle zugehörigen Backups und Snapshots bei.

Sie können den Schutz einer Anwendung nicht aufheben, solange noch Schutzvorgänge für sie ausgeführt werden. Warten Sie entweder, bis der Vorgang abgeschlossen ist, oder als Workaround den Wiederherstellungspunkt entfernen den laufenden Schutzvorgang verwendet. Anschließend können Sie den Schutz der Anwendung aufheben.

Schritte

1. Wählen Sie in NetApp Backup and Recovery*Inventar* aus.
2. Wählen Sie eine Kubernetes-Instanz und wählen Sie **Anzeigen**, um die mit dieser Instanz verknüpften Ressourcen anzuzeigen.
3. Wählen Sie die Registerkarte **Anwendungen**.
4. Wählen Sie in der Anwendungsliste eine Anwendung aus, deren Schutz Sie aufheben möchten, und wählen Sie das zugehörige Aktionsmenü.
5. Wählen Sie **Schutz aufheben**.
6. Lesen Sie den Hinweis und wählen Sie anschließend „Schutz aufheben“ aus.

Löschen einer Kubernetes-Anwendung

Löschen Sie eine Anwendung, die Sie nicht mehr benötigen. NetApp Backup and Recovery beendet den Schutz und entfernt alle Backups und Snapshots für gelöschte Anwendungen.

Schritte

1. Wählen Sie in NetApp Backup and Recovery*Inventar* aus.
2. Wählen Sie eine Kubernetes-Instanz und wählen Sie **Anzeigen**, um die mit dieser Instanz verknüpften Ressourcen anzuzeigen.
3. Wählen Sie die Registerkarte **Anwendungen**.

4. Wählen Sie in der Anwendungsliste eine Anwendung aus, die Sie löschen möchten, und wählen Sie das zugehörige Aktionsmenü.
5. Wählen Sie **Löschen**.
6. Aktivieren Sie **Snapshots und Backups löschen**, um alle Snapshots und Backups der Anwendung zu entfernen.

   Sie können die Anwendung mithilfe dieser Snapshots und Backups nicht mehr wiederherstellen.

7. Bestätigen Sie die Aktion und wählen Sie **Löschen**.

Einen Wiederherstellungspunkt für eine Kubernetes-Anwendung entfernen

Möglicherweise müssen Sie einen Wiederherstellungspunkt für eine Anwendung entfernen, wenn Sie den Schutz aufheben müssen und derzeit Schutzvorgänge ausgeführt werden.

Schritte

1. Wählen Sie im NetApp Backup und Recovery-Menü **Wiederherstellen** aus.
2. Wählen Sie eine Kubernetes-Anwendung aus der Liste und wählen Sie **Anzeigen und Wiederherstellen** für diese Anwendung.

   Die Liste der Wiederherstellungspunkte wird angezeigt.

3. Wählen Sie den Wiederherstellungspunkt aus, den Sie löschen möchten, und wählen Sie das Aktionssymbol ••• > **Wiederherstellungspunkt löschen**, um ihn zu löschen.

Verwalten Sie NetApp Backup and Recovery -Ausführungs -Hook-Vorlagen für Kubernetes-Workloads

Ein Ausführungs-Hook ist eine benutzerdefinierte Aktion, die mit einem Datenschutzvorgang in einer verwalteten Kubernetes-Anwendung ausgeführt wird. Erstellen Sie beispielsweise anwendungskonsistente Snapshots, indem Sie mithilfe eines Ausführungs-Hooks Datenbanktransaktionen vor einem Snapshot anhalten und danach fortsetzen. Wenn Sie eine Ausführungs-Hook-Vorlage erstellen, geben Sie den Hook-Typ, das auszuführende Skript und Filter für Zielcontainer an. Verwenden Sie die Vorlage, um Ausführungs-Hooks mit Ihren Anwendungen zu verknüpfen.

NetApp Backup and Recovery friert Dateisysteme für Anwendungen wie KubeVirt während der Datensicherung ein und taut sie wieder auf. Sie können dieses Verhalten global oder für bestimmte Anwendungen mithilfe der Trident Protect Dokumentation deaktivieren:

- Um dieses Verhalten für alle Anwendungen zu deaktivieren, lesen Sie "Datenschutz mit KubeVirt-VMs" .
- Informationen zum Deaktivieren dieses Verhaltens für eine bestimmte Anwendung finden Sie unter "Definieren einer Anwendung" .

Erforderliche NetApp Console

Organisationsadministrator oder SnapCenter Administrator. "Erfahren Sie mehr über die Zugriffsrollen für

NetApp Backup and Recovery" . "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Arten von Ausführungs-Hooks

NetApp Backup and Recovery unterstützt die folgenden Typen von Ausführungs-Hooks, je nachdem, wann sie ausgeführt werden können:

- Vorab-Schnappschuss
- Nach dem Snapshot
- Vorsicherung
- Nach der Sicherung
- Nach der Wiederherstellung

Reihenfolge der Ausführung

Wenn ein Datenschutzvorgang ausgeführt wird, finden Ausführungs-Hook-Ereignisse in der folgenden Reihenfolge statt:

1. Alle anwendbaren benutzerdefinierten Ausführungs-Hooks vor der Operation werden auf den entsprechenden Containern ausgeführt. Sie können mehrere benutzerdefinierte Pre-Operation-Hooks erstellen, deren Ausführungsreihenfolge ist jedoch nicht garantiert oder konfigurierbar.
2. Gegebenenfalls kommt es zum Einfrieren des Dateisystems.
3. Der Datenschutzvorgang wird durchgeführt.
4. Eingefrorene Dateisysteme werden gegebenenfalls wieder freigegeben.
5. NetApp Backup and Recovery führt alle anwendbaren benutzerdefinierten Ausführungs-Hooks vor dem Vorgang auf den entsprechenden Containern aus. Sie können mehrere benutzerdefinierte Post-Operation-Hooks erstellen, deren Ausführungsreihenfolge ist jedoch nicht garantiert oder konfigurierbar.

Wenn Sie mehrere Hooks desselben Typs erstellen, ist deren Ausführungsreihenfolge nicht garantiert. Hooks unterschiedlichen Typs werden immer in der angegebenen Reihenfolge ausgeführt. Im Folgenden sehen Sie beispielsweise die Ausführungsreihenfolge einer Konfiguration, die alle verschiedenen Hook-Typen enthält:

1. Vor dem Snapshot ausgeführte Hooks
2. Nach dem Snapshot ausgeführte Hooks
3. Vor der Sicherung ausgeführte Hooks
4. Nach der Sicherung ausgeführte Hooks

Testen Sie Ausführungs-Hook-Skripte, bevor Sie sie in der Produktion aktivieren. Verwenden Sie „kubectl exec“, um Skripte zu testen, und überprüfen Sie dann Snapshots und Backups, indem Sie die App in einen temporären Namespace klonen und wiederherstellen.

Wenn ein Pre-Snapshot-Ausführungs-Hook Kubernetes-Ressourcen hinzufügt, ändert oder entfernt, werden diese Änderungen in den Snapshot oder die Sicherung und in alle nachfolgenden Wiederherstellungsvorgänge einbezogen.

Wichtige Hinweise zu benutzerdefinierten Ausführungs-Hooks

Berücksichtigen Sie Folgendes, wenn Sie Ausführungs-Hooks für Ihre Apps planen.

- Ein Ausführungs-Hook muss ein Skript verwenden, um Aktionen auszuführen. Viele Ausführungs-Hooks können auf dasselbe Skript verweisen.
- Ausführungs-Hooks müssen im Format ausführbarer Shell-Skripte geschrieben werden.
- Die Skriptgröße ist auf 96 KB begrenzt.
- Anhand der Ausführungs-Hook-Einstellungen und aller Übereinstimmungskriterien wird ermittelt, welche Hooks für einen Snapshot-, Sicherungs- oder Wiederherstellungsvorgang anwendbar sind.

> Ausführungs-Hooks können die Anwendungsfunktionalität einschränken oder deaktivieren. Sorgen Sie dafür, dass Ihre benutzerdefinierten Hooks so schnell wie möglich ausgeführt werden. Wenn Sie einen Sicherungs- oder Snapshot-Vorgang mit zugehörigen Ausführungs-Hooks starten, ihn dann aber abbrechen, können die Hooks weiterhin ausgeführt werden, wenn der Sicherungs- oder Snapshot-Vorgang bereits begonnen hat. Dies bedeutet, dass die in einem Ausführungs-Hook nach der Sicherung verwendete Logik nicht davon ausgehen kann, dass die Sicherung abgeschlossen wurde.

Ausführungs-Hook-Filter

Wenn Sie einen Ausführungs-Hook für eine Anwendung hinzufügen oder bearbeiten, können Sie dem Ausführungs-Hook Filter hinzufügen, um zu verwalten, mit welchen Containern der Hook übereinstimmt. Filter sind nützlich für Anwendungen, die auf allen Containern dasselbe Container-Image verwenden, aber jedes Image möglicherweise für einen anderen Zweck verwenden (z. B. Elasticsearch). Mithilfe von Filtern können Sie Szenarien erstellen, in denen Ausführungs-Hooks auf einigen, aber nicht unbedingt allen identischen Containern ausgeführt werden. Wenn Sie mehrere Filter für einen einzelnen Ausführungs-Hook erstellen, werden diese mit einem logischen UND-Operator kombiniert. Sie können bis zu 10 aktive Filter pro Ausführungs-Hook haben.

Jeder Filter, den Sie einem Ausführungs-Hook hinzufügen, verwendet einen regulären Ausdruck, um Container in Ihrem Cluster abzugleichen. Wenn ein Hook mit einem Container übereinstimmt, führt der Hook das zugehörige Skript auf diesem Container aus. Reguläre Ausdrücke für Filter verwenden die Syntax „Regulärer Ausdruck 2“ (RE2), die das Erstellen eines Filters, der Container aus der Liste der Übereinstimmungen ausschließt, nicht unterstützt. Informationen zur Syntax, die NetApp Backup and Recovery für reguläre Ausdrücke in Ausführungs-Hook-Filtern unterstützt, finden Sie unter "Unterstützung der Syntax „Regulärer Ausdruck 2“ (RE2)" .

> Wenn Sie einem Ausführungs-Hook, der nach einem Wiederherstellungs- oder Klonvorgang ausgeführt wird, einen Namespace-Filter hinzufügen und sich die Wiederherstellungs- oder Klonquelle und das Ziel in unterschiedlichen Namespaces befinden, wird der Namespace-Filter nur auf den Ziel-Namespace angewendet.

Beispiele für Ausführungs-Hooks

Besuchen Sie die "NetApp Verda GitHub-Projekt" um echte Ausführungs-Hooks für beliebte Apps wie Apache Cassandra und Elasticsearch herunterzuladen. Sie können sich auch Beispiele ansehen und Ideen für die Strukturierung Ihrer eigenen benutzerdefinierten Ausführungs-Hooks holen.

Die Skripte im Verda GitHub Repository werden wie bereitgestellt und sind nicht offiziell von NetApp unterstützt. Nur das Execution Hooks Framework innerhalb von Trident Protect und Backup and Recovery wird offiziell von NetApp unterstützt.

Erstellen einer Ausführungs-Hook-Vorlage

Sie können eine benutzerdefinierte Ausführungs-Hook-Vorlage erstellen, mit der Sie Aktionen vor oder nach einem Datenschutzvorgang für eine Anwendung ausführen können.

Vorlagen, die Sie hier erstellen, sind nur beim Schutz von Kubernetes-Workloads verwendbar.

Schritte

1. Gehen Sie in der Konsole zu **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie die Registerkarte **Einstellungen**.
3. Erweitern Sie den Abschnitt **Ausführungs-Hook-Vorlage**.
4. Wählen Sie **Ausführungs-Hook-Vorlage erstellen**.
5. Geben Sie einen Namen für den Ausführungs-Hook ein.
6. Wählen Sie optional einen Hook-Typ aus. Beispielsweise wird ein Post-Restore-Hook ausgeführt, nachdem der Wiederherstellungsvorgang abgeschlossen ist.
7. Geben Sie im Textfeld **Skript** das ausführbare Shell-Skript ein, das Sie als Teil der Ausführungs-Hook-Vorlage ausführen möchten. Optional können Sie **Skript hochladen** auswählen, um stattdessen eine Skriptdatei hochzuladen.
8. Wählen Sie **Erstellen**.

   Nachdem Sie die Vorlage erstellt haben, wird sie in der Vorlagenliste im Abschnitt **Ausführungs-Hook-Vorlage** angezeigt.

Erstellen und Verwalten von Schutzberichten für Kubernetes-Workloads in NetApp Backup and Recovery

In NetApp Backup and Recovery können Sie Schutzberichte für Kubernetes-Workloads erstellen, um den Schutzstatus und Details anzuzeigen, einschließlich der Anzahl erfolgreicher und fehlgeschlagener Backups, der Backup-Typen, Informationen zum Cluster-Zustand und mehr.

Erforderliche NetApp Console-Rolle Backup and Recovery Super Admin, Backup and Recovery Backup Admin oder Backup and Recovery Restore Admin. Erfahren Sie mehr über "Rollen und Berechtigungen für Backup und Wiederherstellung". "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste".

Erstellen Sie einen Schutzbericht

Erstellen Sie einen Schutzbericht, um den Schutzstatus Ihrer Cluster anzuzeigen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü die Option **Berichte**.

2. Wählen Sie **Bericht erstellen**.
3. Geben Sie Details zum Berichtsumfang ein:
   - **Berichtsname**: Geben Sie einen eindeutigen Namen für den Bericht ein.
   - **Berichtstyp**: Wählen Sie, ob Sie einen Bericht nach Konto oder nach Workload wünschen (wählen Sie Kubernetes aus der Liste).
   - **Cluster auswählen**: Wenn Sie die Auswahl anhand der Arbeitslast getroffen haben, wählen Sie den Cluster aus der Liste aus, für den Sie den Bericht generieren möchten, und wählen Sie **Akzeptieren**. Wählen Sie **Alle auswählen**, um einen Bericht für alle Cluster zu generieren.
4. Berichtszeitraum eingeben: Wählen Sie, ob der Bericht Daten vom letzten Tag, den letzten 7 Tagen, den letzten 30 Tagen, dem letzten Quartal oder dem letzten Jahr enthalten soll.
5. Geben Sie die Konfigurationsdetails für den Bericht ein: Wählen Sie, ob der Bericht nur einmalig ausgeführt oder eine wiederkehrende Berichtserstellung geplant werden soll. Für geplante Berichte wählen Sie die Häufigkeit der Wiederholung und ein Startdatum.

   a. E-Mail-Zustellungsdetails eingeben: (Nur für geplante Berichte) Wenn der Bericht per E-Mail zugestellt werden soll, geben Sie eine oder mehrere E-Mail-Adressen ein, die den geplanten Bericht erhalten sollen.

   Konfigurieren Sie E-Mail-Benachrichtigungen auf der Seite „Einstellungen“. Einzelheiten zum Konfigurieren von E-Mail-Benachrichtigungen finden Sie unter"Konfigurieren der Einstellungen" .
6. Wählen Sie **Erstellen**.

Laden Sie einen Schutzbericht herunter

Laden Sie einen generierten Schutzbericht entweder als JSON-Datei oder als PDF-Dokument herunter, damit Sie ihn anzeigen und weitergeben können.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü die Option **Berichte**.
2. Auf der Seite **Berichte** wählen Sie das Menü **Berichte** aus, um die Liste der generierten Schutzberichte anzuzeigen.
3. Für den Bericht, den Sie herunterladen möchten, wählen Sie das Aktionen-Symbol ••• > **Download**.
   - Wählen Sie **Download JSON**, um den Bericht im JSON-Format herunterzuladen.
   - Wählen Sie **Download PDF**, um den Bericht als PDF-Dokument herunterzuladen.

Einen Schutzbericht anzeigen

Schnell interaktive Details eines Schutzberichts innerhalb von NetApp Backup and Recovery anzeigen. Sie können Zusammenfassungsinformationen zum Auftrag, den Status der Datensicherung, Konfigurationsdetails und mehr sehen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü die Option **Berichte**.
2. Auf der Seite **Berichte** wählen Sie das Menü **Berichte** aus, um die Liste der generierten Schutzberichte anzuzeigen.
3. Für den Bericht, den Sie anzeigen möchten, wählen Sie das Aktionen-Symbol ••• > **Bericht anzeigen**.

   Die Berichtsdetails werden angezeigt.

Einen Schutzbericht löschen

Löschen Sie einen Datensicherungsbericht, wenn Sie ihn nicht mehr benötigen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü die Option **Berichte**.
2. Auf der Seite **Berichte** wählen Sie das Menü **Berichte** aus, um die Liste der generierten Schutzberichte anzuzeigen.
3. Für den Bericht, den Sie löschen möchten, wählen Sie das Aktionen-Symbol ••• > **Löschen**.
4. Bestätigen Sie die Aktion, indem Sie **Löschen** auswählen.