Kubernetes-Anwendungen hinzufügen und schützen

NetApp Backup and Recovery

NetApp
June 24, 2026

Inhalt

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:

```
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)