



Schützen Sie Kubernetes-Workloads (Vorschau)

NetApp Backup and Recovery

NetApp
February 23, 2026

Inhalt

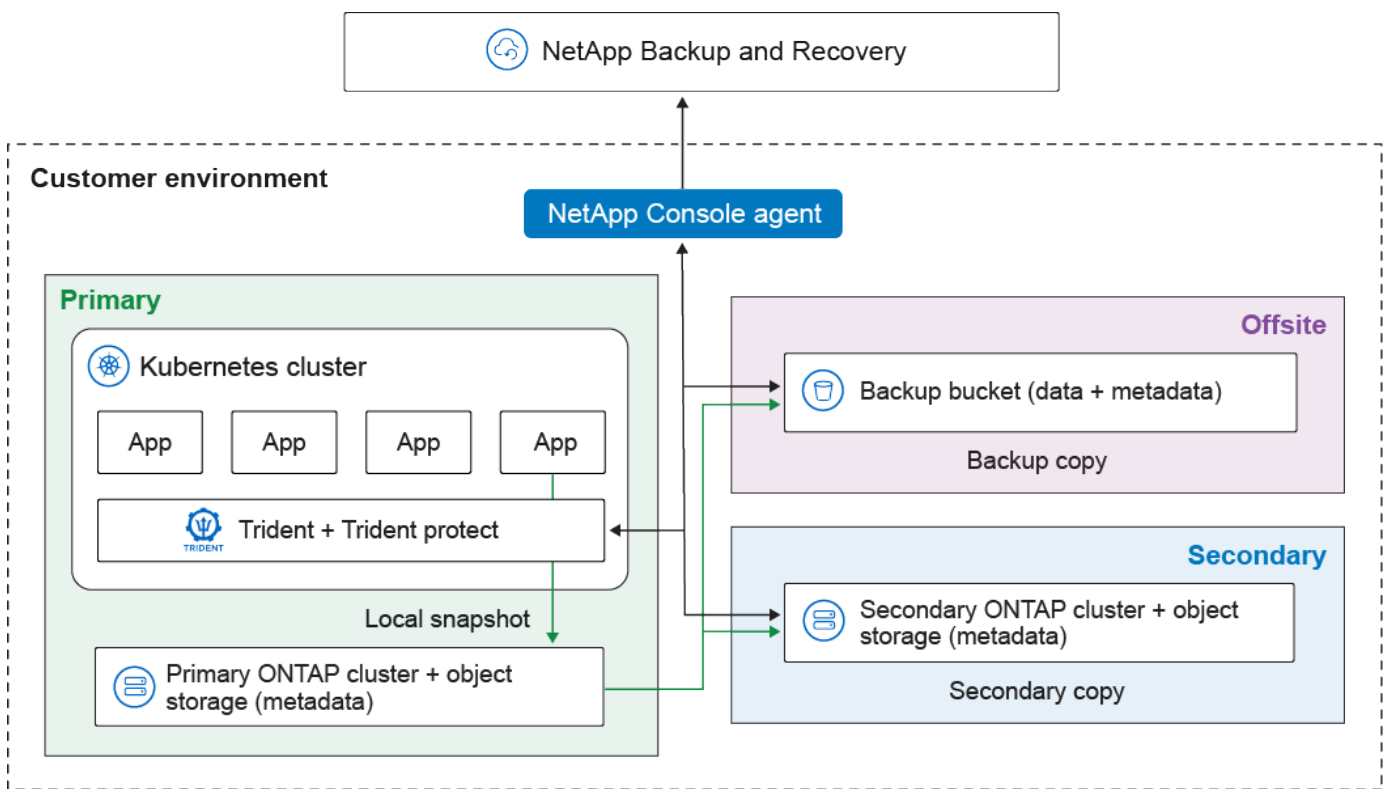
Schützen Sie Kubernetes-Workloads (Vorschau)	1
Übersicht über die Verwaltung von Kubernetes-Workloads	1
Entdecken Sie Kubernetes-Workloads in NetApp Backup and Recovery	2
Entdecken Sie Kubernetes-Workloads	2
Weiter zum NetApp Backup and Recovery Dashboard	3
Kubernetes-Anwendungen hinzufügen und schützen	3
Kubernetes-Anwendungen hinzufügen und schützen	3
Sichern Sie jetzt Kubernetes-Anwendungen mit der Backup and Recovery-Weboberfläche	7
Sichern Sie jetzt Kubernetes-Anwendungen mithilfe benutzerdefinierter Ressourcen in Backup and Recovery	8
Wiederherstellen von Kubernetes-Anwendungen	13
Kubernetes-Anwendungen mithilfe der Web-Benutzeroberfläche wiederherstellen	13
Kubernetes-Anwendungen mithilfe einer benutzerdefinierten Ressource wiederherstellen	15
Erweiterte benutzerdefinierte Ressourcenwiederherstellungseinstellungen verwenden	26
Verwalten von Kubernetes-Clustern	29
Kubernetes-Clusterinformationen bearbeiten	29
Entfernen eines Kubernetes-Clusters	30
Verwalten von Kubernetes-Anwendungen	30
Aufheben des Schutzes einer Kubernetes-Anwendung	30
Löschen einer Kubernetes-Anwendung	30
Einen Wiederherstellungspunkt für eine Kubernetes-Anwendung entfernen	31
Verwalten Sie NetApp Backup and Recovery -Ausführungs-Hook-Vorlagen für Kubernetes-Workloads	31
Arten von Ausführungs-Hooks	32
Wichtige Hinweise zu benutzerdefinierten Ausführungs-Hooks	33
Ausführungs-Hook-Filter	33
Beispiele für Ausführungs-Hooks	34
Erstellen einer Ausführungs-Hook-Vorlage	34
Erstellen und Verwalten von Schutzberichten für Kubernetes-Workloads in NetApp Backup and Recovery	34
Erstellen Sie einen Schutzbericht	34
Laden Sie einen Schutzbericht herunter	35
Einen Schutzbericht anzeigen	35
Einen Schutzbericht löschen	36

Schützen Sie Kubernetes-Workloads (Vorschau)

Übersicht über die Verwaltung von Kubernetes-Workloads

Durch die Verwaltung von Kubernetes-Workloads in NetApp Backup and Recovery können Sie Ihre Kubernetes-Cluster und -Anwendungen an einem Ort erkennen, verwalten und schützen. Sie können die auf Ihren Kubernetes-Clustern gehosteten Ressourcen und Anwendungen verwalten. Außerdem können Sie Schutzrichtlinien erstellen und Ihren Kubernetes-Workloads zuordnen – alles über eine einzige Oberfläche.

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.



Diese Dokumentation wird als Technologievorschau bereitgestellt. Während der Vorschau wird die Kubernetes-Funktionalität für Produktions-Workloads nicht empfohlen. Bei diesem Vorschauangebot behält sich NetApp das Recht vor, Angebotsdetails, Inhalte und Zeitplan vor der allgemeinen Verfügbarkeit zu ändern.

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

Mit NetApp Backup and Recovery können Sie Ihre Kubernetes-Cluster einfach erkennen, ohne Kubeconfig-Dateien generieren und hochladen zu müssen. Sie können Kubernetes-Cluster verbinden und die erforderliche Software mithilfe einfacher Befehle installieren, die Sie aus der Benutzeroberfläche der NetApp Console kopiert haben.

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 die Konsole auf die laufende Anwendung im Kubernetes-Cluster aufmerksam.

Bevor Sie beginnen

Bevor Sie eine Kubernetes-Anwendung hinzufügen und schützen können, müssen Sie ["Kubernetes-Workloads entdecken"](#) .

Fügen Sie eine Anwendung über die Web-Benutzeroberfläche hinzu

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 **Anwendung erstellen**.
5. Geben Sie einen Namen für die Anwendung ein.
6. Wählen Sie optional eines der folgenden Felder aus, um nach den Ressourcen zu suchen, die Sie schützen möchten:
 - Zugehöriger Cluster
 - Zugehörige Namespaces
 - Ressourcentypen
 - Beschriftungsselektoren
7. Wählen Sie optional **Cluster Scoped Resources** aus, um Ressourcen auszuwählen, die auf Clusterebene liegen. Wenn Sie diese einschließen, werden sie der Anwendung beim Erstellen hinzugefügt.
8. Wählen Sie optional **Suchen** aus, um die Ressourcen basierend auf Ihren Suchkriterien zu finden.



Die Konsole speichert die Suchparameter oder Ergebnisse nicht. Die Parameter werden verwendet, um im ausgewählten Kubernetes-Cluster nach Ressourcen zu suchen, die in die Anwendung integriert werden können.

9. Die Konsole zeigt eine Liste der Ressourcen an, die Ihren Suchkriterien entsprechen.
10. Wenn die Liste die Ressourcen enthält, die Sie schützen möchten, wählen Sie **Weiter**.
11. Wählen Sie im Bereich **Richtlinie** optional eine vorhandene Schutzrichtlinie zum Schutz der Anwendung aus oder erstellen Sie eine neue Richtlinie. Wenn Sie keine Richtlinie auswählen, wird die Anwendung ohne Schutzrichtlinie erstellt. Du kannst "[Fügen Sie eine Schutzrichtlinie hinzu](#)" später.
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 Anwendung mithilfe eines 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 hat jedoch keine virtuellen Maschinen in der Anwendungsdefinition, 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
```

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-](#)

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)* 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`.

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 <code>true</code> , 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-hot-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"

Anmerkung	Typ	Beschreibung	Standardwert
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 <code>Bound</code> 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.

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

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"](#) .

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.

Allgemeine Einstellungen

1. Wählen Sie den Quellspeicherort aus, von dem wiederhergestellt werden soll.
2. Wählen Sie den Zielcluster aus der Liste **Cluster** aus.



Das Wiederherstellen eines von Trident Protect erstellten lokalen Snapshots auf einem anderen Cluster wird derzeit nicht unterstützt.

3. Wählen Sie, ob Sie in die ursprünglichen Namensräume oder in neue Namensräume wiederherstellen möchten.
4. Wenn Sie die Wiederherstellung in neuen Namensräumen gewählt haben, geben Sie den Ziel-Namespace

oder die Ziel-Namensräume an, die verwendet werden sollen.

5. Wählen Sie **Weiter**.

Ressourcenauswahl

1. 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 wiederherstellen

1. Wählen Sie **Alle Ressourcen wiederherstellen**.
2. Wählen Sie **Weiter**.

Wiederherstellen bestimmter Ressourcen

1. Wählen Sie **Selektive Ressourcen** aus.
2. 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.
3. 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.

4. Wählen Sie **Speichern**, um jede Regel zu speichern.
5. Wenn Sie alle benötigten Regeln hinzugefügt haben, wählen Sie **Suchen**, um die im Sicherungsarchiv verfügbaren Ressourcen anzuzeigen, die Ihren Filterkriterien entsprechen.



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

6. Wenn Sie mit den Ergebnissen zufrieden sind, wählen Sie **Weiter**.

Zieleinstellungen

1. 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.
2. Wenn Sie die Wiederherstellung in einer anderen Speicherklasse gewählt haben, wählen Sie eine Zielspeicherklasse aus, die zu jeder Quellspeicherklasse passt.
3. 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"](#).

4. 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.
5. 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 <SNAPSHOT_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.

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

Während Wiederherstellungs- und Failover-Vorgängen werden die Labels und Annotationen im Ziel-Namensraum so angepasst, dass sie den Labels und Annotationen im Quell-Namensraum entsprechen. Labels oder Annotationen aus dem Quell-Namensraum, die im Ziel-Namensraum nicht existieren, werden hinzugefügt, und alle Labels oder Annotationen, die bereits vorhanden sind, werden überschrieben, um dem Wert aus dem Quell-Namensraum zu entsprechen. Labels oder Annotationen, die nur im Ziel-Namensraum existieren, bleiben unverändert.



Wenn Sie Red Hat OpenShift verwenden, ist es wichtig, die entscheidende Rolle von Namespace-Annotationen in OpenShift-Umgebungen zu beachten. Namespace-Annotationen stellen sicher, dass wiederhergestellte Pods die entsprechenden Berechtigungen und Sicherheitskonfigurationen einhalten, die durch OpenShift Security Context Constraints (SCCs) definiert sind, und ohne Berechtigungsprobleme auf Volumes zugreifen können. Weitere Informationen finden Sie unter ["OpenShift security context constraints Dokumentation"](#).

Sie können verhindern, dass bestimmte Annotationen im Ziel-Namespace überschrieben werden, indem Sie die Kubernetes-Umgebungsvariable `RESTORE_SKIP_NAMESPACE_ANNOTATIONS` festlegen, bevor Sie die Wiederherstellungs- oder Failover-Operation durchführen. Zum Beispiel:

```
helm upgrade trident-protect -n trident-protect netapp-trident-protect/trident-protect \
  --set-string
restoreSkipNamespaceAnnotations="{<annotation_key_to_skip_1>,<annotation_key_to_skip_2>}" \
  --reuse-values
```



Bei der Durchführung einer Wiederherstellungs- oder Failover-Operation werden alle Namespace-Annotationen und Labels, die in `restoreSkipNamespaceAnnotations` und `restoreSkipNamespaceLabels` angegeben sind, von der Wiederherstellungs- oder Failover-Operation ausgeschlossen. Stellen Sie sicher, dass diese Einstellungen während der initialen Helm-Installation konfiguriert werden. Weitere Informationen finden Sie unter ["Konfigurieren Sie zusätzliche Trident Protect Helm-Chart-Einstellungen"](#).

Wenn Sie die Quellanwendung mit Helm mit dem `--create-namespace` Flag installiert haben, wird dem `name` Label-Schlüssel eine besondere Behandlung zuteil. Während des Wiederherstellungs- oder Failover-Prozesses kopiert Trident Protect dieses Label in den Ziel-Namespace, aktualisiert jedoch den Wert auf den Wert des Ziel-Namespace, wenn der Wert aus der Quelle mit dem Quell-Namespace übereinstimmt. Wenn dieser Wert nicht mit dem Quell-Namespace übereinstimmt, wird er unverändert in den Ziel-Namespace kopiert.

Beispiel

Das folgende Beispiel zeigt einen Quell- und einen Ziel-Namensraum mit jeweils unterschiedlichen Annotationen und Labels. Sie können den Zustand des Ziel-Namensraums vor und nach der Operation sehen und erkennen, wie die Annotationen und Labels im Ziel-Namensraum kombiniert oder überschrieben werden.

Vor dem Wiederherstellungs- oder Failover-Vorgang

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

Namensraum	Anmerkungen	Etiketten
Namespace ns-1 (Quelle)	• <code>annotation.one/key</code>: "updatedvalue" • <code>annotation.two/key</code>: "true"	• <code>environment</code>=production • <code>compliance</code>=hipaa • <code>name</code>=ns-1

Namensraum	Anmerkungen	Etiketten
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)

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 Bestätigungsdiaologfeld und wählen Sie **Entfernen**.

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.

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.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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