NetApp Backup and Recovery -Dokumentation

NetApp Backup and Recovery

NetApp
February 13, 2026

Inhalt

NetApp Backup and Recovery -Dokumentation

Versionshinweise

Was ist neu bei NetApp Backup and Recovery?

Erfahren Sie, was es Neues bei NetApp Backup and Recovery gibt.

09. Februar 2026

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates.

Microsoft Hyper-V-Workloads, die in General Availability (GA) unterstützt werden

Die Unterstützung für Microsoft Hyper-V-Workloads ist jetzt allgemein verfügbar (GA) in NetApp Backup and Recovery.

Unterstützte VMware-Workloads in der allgemeinen Verfügbarkeit (GA)

Die Unterstützung für VMware-Workloads ist jetzt allgemein verfügbar (GA) in NetApp Backup and Recovery.

Kubernetes-Workloads-Erweiterungen

Diese Version von Kubernetes-Workloads bietet die folgenden erweiterten Funktionen:

- **CR-Workflow-Unterstützung**: Sie können jetzt gängige Schutzaufgaben sowohl mit CRs als auch über die Backup and Recovery-Weboberfläche durchführen.
- **Clustermigration**: Sie können jetzt bestehende Kubernetes-Cluster, die mit Trident Protect geschützt sind, zu Backup and Recovery hinzufügen.
- **Unterstützung des Alerting-Frameworks**: Sie können jetzt E-Mail- und UI-Benachrichtigungen für bestimmte Kubernetes-Workload-Ereignisse erhalten.
- **Integration der Registerkarte "Wiederherstellen"**: Sie können jetzt über das Menü "Wiederherstellen" auf die Aktionen zur Wiederherstellung von Kubernetes-Workloads zugreifen.
- **Unterstützung für die 3-2-1-Fanout-Backup-Architektur**: Sie können jetzt eine 3-2-1-Fanout-Architektur in Ihrer Datensicherungsstrategie verwenden, wenn Sie Kubernetes-Workloads schützen.

Weitere Informationen zum Schutz von Kubernetes-Workloads finden Sie unter "Übersicht zum Schützen von Kubernetes-Workloads" .

Verbesserungen der Oracle Database Workloads

Diese Version der Oracle Database Workloads bietet die folgenden erweiterten Funktionen:

- **Unterstützung für Nicht-Root-Benutzer**: Nicht-Root-Benutzer können nun Sicherungs-, Wiederherstellungs- und Klonvorgänge durchführen, was die Sicherheit und Compliance verbessert.
- **Klonunterstützung**: Klonfunktionen werden jetzt in primären und sekundären NAS-, SAN- und ASM-Umgebungen mithilfe der ASM library v2 unterstützt, wodurch koordinierte Schutz-Workflows ermöglicht werden.
- **Unterstützung für das Aufteilen von Klonen**: Sie können jetzt beschreibbare Snapshots (Klone) von ihren übergeordneten Volumes trennen, Speicherplatz freigeben und unabhängige Operationen ermöglichen.

- **Sicherung und Wiederherstellung für Objektspeicher**: Native Sicherungs- und Wiederherstellungsfunktionen werden jetzt für objektbasierte S3-kompatible Speicherziele unterstützt.
- **Clone Lifecycle Management (CLM)**: Klonaktualisierungsvorgänge werden auf dem primären Speicher unterstützt.
- **Auf alternativen Host klonen**: Sie können jetzt Datenbanken zu Test- oder Analysezwecken sowohl vom primären als auch vom sekundären Speicher auf einen anderen Host klonen.
- **ONTAP Konsistenzgruppen-Support**: ONTAP Konsistenzgruppen werden jetzt unterstützt, wodurch applikationskonsistente Snapshots über mehrere Volumes hinweg gewährleistet werden.
- Backup and Recovery unterstützt jetzt die folgenden Datensicherungsstrategie-Architekturen für Oracle Database-Workloads:
  - 3-2-1 Fanout
  - Festplatte zu Festplatte
  - Festplatte zu Objektspeicher
  - Kaskadierend
  - Lokaler Schnappschuss

Weitere Informationen zum Schutz von Oracle Database-Workloads finden Sie unter "Übersicht über den Schutz von Oracle Database-Workloads".

19. Januar 2026

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates.

ONTAP Volume-Workload-Erweiterungen

Diese Version der ONTAP Volume-Workloads führt die folgenden erweiterten Funktionen ein:

Unterstützung für mehrere Buckets: (Private Vorschau) Ab ONTAP 9.17.1 und neueren Versionen können Sie nun die Volumes innerhalb eines Systems mit bis zu 6 Buckets pro System über verschiedene Cloud-Anbieter hinweg schützen.

"Erfahren Sie mehr über die Sicherung von ONTAP Volume-Daten mit NetApp Backup and Recovery.".

VMware-Workload-Verbesserungen

Diese Version von VMware-Workloads bietet die folgenden erweiterten Funktionen:

- Die Unterstützung für VMware-Workloads ist jetzt allgemein verfügbar (GA) in NetApp Backup and Recovery.
- Sie können jetzt Gastbetriebssystemdateien und -ordner wiederherstellen.

"Erfahren Sie mehr über das Wiederherstellen von Gastdateien und -ordnern."Die

Vorschau der Verbesserungen für Hyper-V-Workloads

Diese Version von Hyper-V-Workloads bietet die folgenden erweiterten Funktionen:

- Sie können jetzt Hyper-V-VM-Backups und -Snapshots an einem alternativen Speicherort wiederherstellen. Nutzen Sie diese Funktion, um VM-Versionen auf verschiedenen Hyper-V-Hosts zu verwalten.

- NetApp Backup und Recovery unterstützt jetzt Hyper-V-VMs, die von System Center Virtual Machine Manager (SCVMM) bereitgestellt und auf einer CIFS-Freigabe gehostet werden.
- Sie können nun Schutzgruppen bearbeiten.

> Nur in dieser Version ist es nicht möglich, die NetApp -Plugins für Hyper-V oder Windows über die Option **Upgrade** im Menü Aktionen zu aktualisieren. Entfernen Sie stattdessen jeden Hyper-V-Host und fügen Sie ihn anschließend wieder hinzu, um die Plugins zu aktualisieren.

"Erfahren Sie mehr über die Wiederherstellung von Hyper-V-VMs mit NetApp Backup and Recovery."Die

Vorschau der Verbesserungen für KVM-Workloads

Die KVM-Workload-Vorschau schützt jetzt KVM-Hosts und virtuelle Maschinen, die von Apache CloudStack verwaltet werden.

Weitere Informationen zum Schutz von KVM-Workloads finden Sie unter "Übersicht über den Schutz von KVM-Workloads" .

8. Dezember 2025

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates.

VMware Workloads Vorschau-Verbesserungen

Die Vorschauversion von VMware-Workloads führt die folgenden erweiterten Funktionen ein:

- Sie können Backups und Snapshots jetzt an einem alternativen Speicherort wiederherstellen. Dies ist nützlich, wenn Sie Versionen einer VM auf verschiedenen VMware vCenter-Bereitstellungen, VMware ESXi-Hosts oder VMware-Datenspeichern verwalten möchten.

"Erfahren Sie mehr über die Wiederherstellung von VMware-VMs mit NetApp Backup and Recovery.".

- Sie können nun bestimmte virtuelle VMware-Festplatten (VMDK-Images) entweder von einem primären oder einem sekundären Speicherort wiederherstellen, was eine feinere Kontrolle über die Wiederherstellung von VM-Daten ermöglicht.

"Erfahren Sie mehr über die Wiederherstellung virtueller VMware-Festplatten mit NetApp Backup and Recovery.".

06. Oktober 2025

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates.

BlueXP backup and recovery heißt jetzt NetApp Backup and Recovery

BlueXP backup and recovery wurde in NetApp Backup and Recovery umbenannt.

BlueXP heißt jetzt NetApp Console

Die NetApp Console basiert auf der verbesserten und neu strukturierten BlueXP -Grundlage und ermöglicht die zentrale Verwaltung von NetApp Storage und NetApp Data Services in On-Premises- und Cloud-Umgebungen auf Unternehmensniveau. Sie liefert Einblicke in Echtzeit, schnellere Workflows und eine vereinfachte Administration, die äußerst sicher und konform ist.

Einzelheiten zu den Änderungen finden Sie im"Versionshinweise zur NetApp Console ."

Hyper-V-Workload-Unterstützung als private Vorschau

Diese Version von NetApp Backup and Recovery bietet Unterstützung für die Erkennung und Verwaltung von Hyper-V-Workloads:

- Sichern und Wiederherstellen von VMs auf eigenständigen Instanzen sowie Failover-Cluster-Instanzen (FCI)
- Schützen Sie auf SMB3-Freigaben gespeicherte VMs
- Massenschutz auf virtueller Maschinenebene
- VM- und absturzkonsistente Backups
- Stellen Sie VMs aus dem primären, sekundären und Objektspeicher wieder her
- Suchen und Wiederherstellen von VM-Backups

Weitere Informationen zum Schutz von Hyper-V-Workloads finden Sie unter "Übersicht zum Schützen von Hyper-V-Workloads" .

KVM-Workload-Unterstützung als private Vorschau

Diese Version von NetApp Backup and Recovery bietet Unterstützung für die Erkennung und Verwaltung von KVM-Workloads:

- Sichern und Wiederherstellen von auf NFS-Freigaben gespeicherten qcow2-VM-Images
- Sichern von Speicherpools
- Massenschutz von VMs und Speicherpools mithilfe von Schutzgruppen
- VM-konsistente und absturzkonsistente VM-Backups
- Suchen und Wiederherstellen von VM-Backups aus Primär-, Sekundär- und Objektspeicher
- Geführter Prozess zum Sichern und Wiederherstellen von KVM-basierten VMs und VM-Daten

Weitere Informationen zum Schutz von KVM-Workloads finden Sie unter "Übersicht über den Schutz von KVM-Workloads" .

Verbesserungen der Kubernetes-Vorschau

Die Vorschauversion der Kubernetes-Workloads führt die folgenden erweiterten Funktionen ein:

- Unterstützung der 3-2-1 Fan-Out-Backup-Architektur
- Unterstützung für ONTAP S3 als Backup-Ziel
- Neues Kubernetes-Dashboard für einfachere Verwaltung
- Die erweiterte rollenbasierte Zugriffssteuerungskonfiguration (RBAC) umfasst Unterstützung für die folgenden Rollen:
  - Superadministrator für Backup und Wiederherstellung
  - Backup- und Wiederherstellungs-Backup-Administrator
  - Administrator für die Wiederherstellung von Backup und Wiederherstellung
  - Backup- und Wiederherstellungs-Viewer

- Unterstützung für die SUSE Rancher Kubernetes-Distribution
- Multi-Bucket-Unterstützung: Sie können jetzt die Volumes innerhalb eines Systems mit mehreren Buckets pro System über verschiedene Cloud-Anbieter hinweg schützen

Weitere Informationen zum Schutz von Kubernetes-Workloads finden Sie unter "Übersicht zum Schützen von Kubernetes-Workloads" .

Verbesserungen der VMware-Vorschau

Die Vorschauversion von VMware-Workloads führt die folgenden erweiterten Funktionen ein:

- Unterstützung für die Wiederherstellung aus dem Objektspeicher
- Das Dashboard der NetApp Console zeigt jetzt Informationen zum VMware-Workload-Status an
- Unterstützung der rollenbasierten Zugriffskontrolle (RBAC)
- E-Mail-Warnung und Benachrichtigungsunterstützung für Jobereignisse
- Unterstützung für die Sicherung und Wiederherstellung auf NVMe-basiertem Speicher
- Schutzgruppen bearbeiten
- Schutzrichtlinien bearbeiten

Weitere Informationen zum Schutz von VMware-Workloads finden Sie unter "Übersicht zum Schützen von VMware-Workloads" .

Oracle Database-Workload-Unterstützung als private Vorschau

Diese Version von NetApp Backup and Recovery bietet Unterstützung für die Erkennung und Verwaltung von Oracle Database-Workloads:

- Entdecken Sie eigenständige Oracle-Datenbanken
- Erstellen Sie Schutzrichtlinien nur für Daten oder Daten- und Protokollsicherungen
- Schützen Sie Oracle-Datenbanken mit einem 3-2-1-Backup-Schema
- Konfigurieren der Sicherungsaufbewahrung
- Mounten und Unmounten von ARCHIVELOG-Backups
- Virtualisierte Datenbanken
- Suchen und Wiederherstellen von Datenbanksicherungen
- Oracle-Dashboard-Unterstützung

Weitere Informationen zum Schutz von Oracle Database-Workloads finden Sie unter "Übersicht über den Schutz von Oracle Database-Workloads".

Verbesserungen der ONTAP Volume-Workload

Diese Version der ONTAP Volume-Workloads führt die folgenden erweiterten Funktionen ein:

Ab ONTAP 9.17.1 und neuer wird DataLock jetzt mit der Google Cloud Platform unterstützt. Dies ergänzt die bestehende DataLock-Unterstützung mit Amazon AWS, Microsoft Azure und NetApp StorageGRID.

25. August 2025

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates.

Unterstützung für den Schutz von VMware-Workloads in der Vorschau

Diese Version fügt Vorschauunterstützung zum Schutz von VMware-Workloads hinzu. Sichern Sie VMware-VMs und Datenspeicher von lokalen ONTAP -Systemen auf Amazon Web Services und StorageGRID.

> Dokumentation zum Schutz von VMware-Workloads wird als Technologievorschau bereitgestellt. Bei diesem Vorschauangebot behält sich NetApp das Recht vor, Angebotsdetails, Inhalte und Zeitplan vor der allgemeinen Verfügbarkeit zu ändern.

"Erfahren Sie mehr über den Schutz von VMware-Workloads mit NetApp Backup and Recovery".

Hochleistungsindizierung für AWS, Azure und GCP ist allgemein verfügbar

Im Februar 2025 haben wir die Vorschau der Hochleistungsindizierung (Indexed Catalog v2) für AWS, Azure und GCP angekündigt. Diese Funktion ist jetzt allgemein verfügbar (GA). Im Juni 2025 haben wir es allen *neuen* Kunden standardmäßig zur Verfügung gestellt. Mit dieser Version steht der Support *allen* Kunden zur Verfügung. Durch die Hochleistungsindizierung wird die Leistung von Sicherungs- und Wiederherstellungsvorgängen für Workloads verbessert, die im Objektspeicher geschützt sind.

Standardmäßig aktiviert:

- Wenn Sie ein neuer Kunde sind, ist die Hochleistungsindizierung standardmäßig aktiviert.
- Wenn Sie bereits Kunde sind, können Sie die Neuindizierung aktivieren, indem Sie zum Abschnitt „Wiederherstellen“ der Benutzeroberfläche gehen.

12. August 2025

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates.

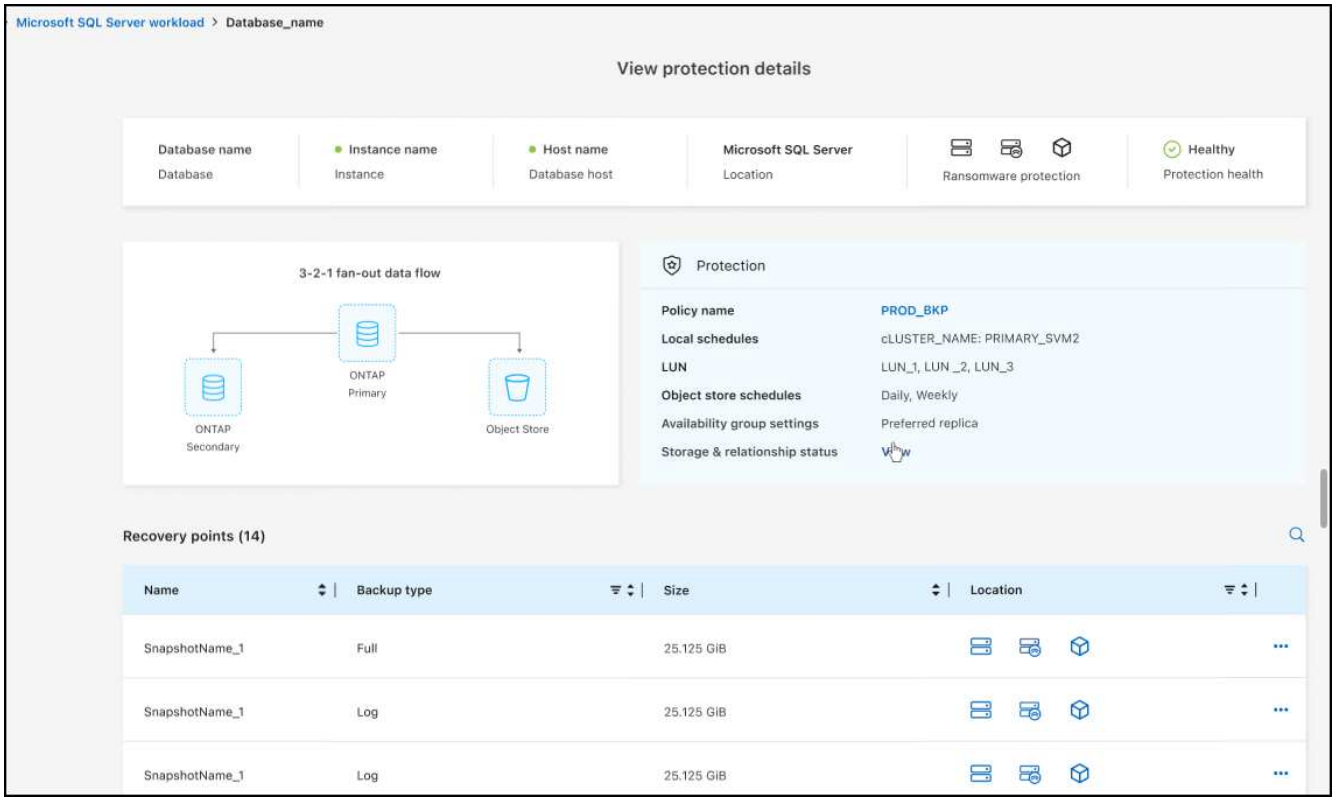
Microsoft SQL Server-Workload wird in der allgemeinen Verfügbarkeit (GA) unterstützt

Die Workload-Unterstützung für Microsoft SQL Server ist jetzt in NetApp Backup and Recovery allgemein verfügbar (GA). Organisationen, die eine MSSQL-Umgebung auf ONTAP, Cloud Volumes ONTAP und Amazon FSx for NetApp ONTAP -Speicher verwenden, können jetzt diesen neuen Backup- und Wiederherstellungsdienst zum Schutz ihrer Daten nutzen.

Diese Version enthält die folgenden Verbesserungen der Microsoft SQL Server-Workload-Unterstützung gegenüber der vorherigen Vorschauversion:

- * SnapMirror Active Sync*: Diese Version unterstützt jetzt SnapMirror Active Sync (auch als SnapMirror Business Continuity [SM-BC] bezeichnet), wodurch Geschäftsdienste auch bei einem vollständigen Site-Ausfall weiter ausgeführt werden können und Anwendungen mithilfe einer sekundären Kopie ein transparentes Failover durchführen können. NetApp Backup and Recovery unterstützt jetzt den Schutz von Microsoft SQL Server-Datenbanken in einer SnapMirror Active Sync- und Metrocluster-Konfiguration. Die Informationen werden im Abschnitt **Speicher- und Beziehungsstatus** der Seite mit den Schutzdetails angezeigt. Die Beziehungsinformationen werden im aktualisierten Abschnitt **Sekundäre Einstellungen** der Richtlinienseite angezeigt.

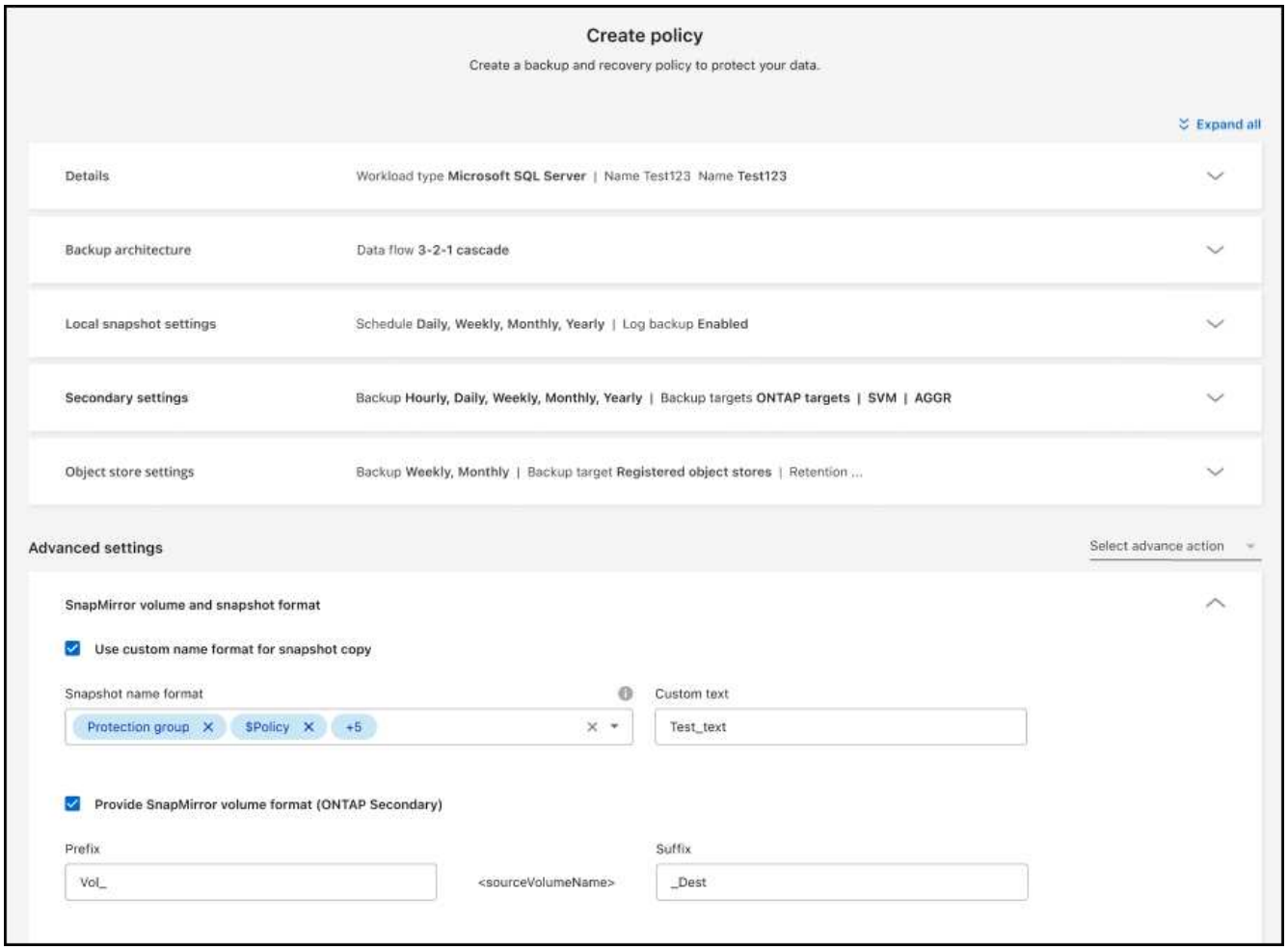
  Siehe "Verwenden Sie Richtlinien zum Schutz Ihrer Workloads" .



- **Multi-Bucket-Unterstützung**: Sie können jetzt die Volumes innerhalb einer Arbeitsumgebung mit bis zu 6 Buckets pro Arbeitsumgebung über verschiedene Cloud-Anbieter hinweg schützen.
- **Lizenzierung und kostenlose Testupdates** für SQL Server-Workloads: Sie können jetzt das vorhandene NetApp Backup and Recovery -Lizenzmodell zum Schutz von SQL Server-Workloads verwenden. Für SQL Server-Workloads besteht keine separate Lizenzanforderung.

  Weitere Einzelheiten finden Sie unter "Einrichten der Lizenzierung für NetApp Backup and Recovery" .

- **Benutzerdefinierter Snapshot-Name**: Sie können jetzt Ihren eigenen Snapshot-Namen in einer Richtlinie verwenden, die die Sicherungen für Microsoft SQL Server-Workloads regelt. Geben Sie diese Informationen im Abschnitt **Erweiterte Einstellungen** der Richtlinienseite ein.

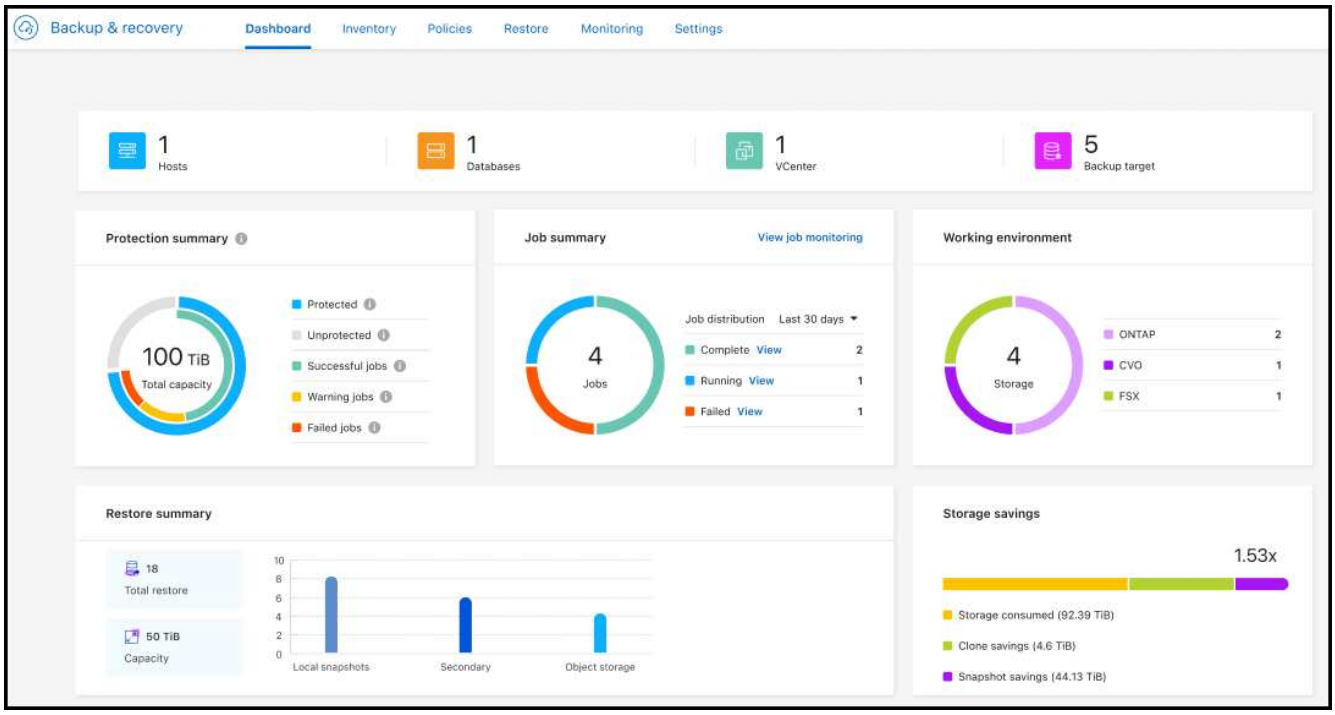


Siehe "Verwenden Sie Richtlinien zum Schutz Ihrer Workloads" .

- **Präfix und Suffix des sekundären Volumes**: Sie können im Abschnitt **Erweiterte Einstellungen** der Richtlinienseite ein benutzerdefiniertes Präfix und Suffix eingeben.
- **Identität und Zugriff**: Sie können jetzt den Zugriff der Benutzer auf Funktionen steuern.

  Siehe "Melden Sie sich bei NetApp Backup and Recovery an" Und "Zugriff auf NetApp Backup and Recovery -Funktionen" .

- **Wiederherstellung vom Objektspeicher auf einem alternativen Host**: Sie können jetzt vom Objektspeicher auf einem alternativen Host wiederherstellen, selbst wenn der primäre Speicher ausgefallen ist.
- **Protokollsicherungsdaten**: Auf der Seite mit den Datenbankschutzdetails werden jetzt Protokollsicherungen angezeigt. In der Spalte „Sicherungstyp“ wird angezeigt, ob es sich bei der Sicherung um eine vollständige Sicherung oder eine Protokollsicherung handelt.
- **Verbessertes Dashboard**: Das Dashboard zeigt jetzt Speicher- und Klon-Einsparungen an.



Verbesserungen der ONTAP Volume-Workload

- **Wiederherstellung mehrerer Ordner für ONTAP -Volumes**: Bisher konnten Sie mit der Funktion „Durchsuchen und Wiederherstellen“ entweder einen Ordner oder mehrere Dateien gleichzeitig wiederherstellen. NetApp Backup and Recovery bietet jetzt die Möglichkeit, mithilfe der Funktion „Durchsuchen und Wiederherstellen“ mehrere Ordner gleichzeitig auszuwählen.
- **Backups gelöschter Volumes anzeigen und verwalten**: Das NetApp Backup and Recovery Dashboard bietet jetzt eine Option zum Anzeigen und Verwalten von Volumes, die aus ONTAP gelöscht wurden. Damit können Sie Backups von Volumes anzeigen und löschen, die in ONTAP nicht mehr vorhanden sind.
- **Löschen von Backups erzwingen**: In einigen extremen Fällen möchten Sie möglicherweise, dass NetApp Backup and Recovery keinen Zugriff mehr auf Backups hat. Dies kann beispielsweise passieren, wenn der Dienst keinen Zugriff mehr auf den Backup-Bucket hat oder Backups durch DataLock geschützt sind, Sie diese aber nicht mehr möchten. Bisher konnten Sie diese nicht selbst löschen und mussten den NetApp -Support anrufen. Mit dieser Version können Sie die Option zum erzwungenen Löschen von Sicherungen (auf Volume- und Arbeitsumgebungsebene) verwenden.

> Verwenden Sie diese Option mit Vorsicht und nur bei extremem Reinigungsbedarf. NetApp Backup and Recovery hat keinen Zugriff mehr auf diese Backups, auch wenn sie nicht im Objektspeicher gelöscht werden. Sie müssen zu Ihrem Cloud-Anbieter gehen und die Backups manuell löschen.

Siehe "Schützen Sie ONTAP -Workloads" .

28. Juli 2025

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates.

Kubernetes-Workload-Unterstützung als Vorschau

Diese Version von NetApp Backup and Recovery bietet Unterstützung für die Erkennung und Verwaltung von Kubernetes-Workloads:

- Entdecken Sie Red Hat OpenShift und Open-Source-Kubernetes-Cluster, unterstützt von NetApp ONTAP, ohne Kubeconfig-Dateien freizugeben.
- Entdecken, verwalten und schützen Sie Anwendungen über mehrere Kubernetes-Cluster hinweg mithilfe einer einheitlichen Steuerungsebene.
- Lagern Sie Datenverschiebungsvorgänge zur Sicherung und Wiederherstellung von Kubernetes-Anwendungen auf NetApp ONTAP aus.
- Orchestrieren Sie lokale und objektspeicherbasierte Anwendungssicherungen.
- Sichern und stellen Sie ganze Anwendungen und einzelne Ressourcen in beliebigen Kubernetes-Clustern wieder her.
- Arbeiten Sie mit Containern und virtuellen Maschinen, die auf Kubernetes laufen.
- Erstellen Sie anwendungskonsistente Backups mithilfe von Ausführungs-Hooks und Vorlagen.

Weitere Informationen zum Schutz von Kubernetes-Workloads finden Sie unter "Übersicht zum Schützen von Kubernetes-Workloads" .

14. Juli 2025

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates.

Verbessertes ONTAP Volume Dashboard

Im April 2025 haben wir eine Vorschau eines verbesserten ONTAP Volume Dashboards veröffentlicht, das viel schneller und effizienter ist.

Dieses Dashboard wurde entwickelt, um Unternehmenskunden mit einer hohen Anzahl an Workloads zu helfen. Selbst für Kunden mit 20.000 Bänden wird das neue Dashboard in <10 Sekunden geladen.

Nach einer erfolgreichen Vorschau und großartigem Feedback von Vorschaukunden machen wir es jetzt zum Standarderlebnis für alle unsere Kunden. Machen Sie sich bereit für ein blitzschnelles Dashboard.

Weitere Einzelheiten finden Sie unter"Anzeigen des Schutzstatus im Dashboard" .

Microsoft SQL Server-Workload-Unterstützung als Public Technology Preview

Diese Version von NetApp Backup and Recovery bietet eine aktualisierte Benutzeroberfläche, mit der Sie Microsoft SQL Server-Workloads mithilfe einer 3-2-1-Schutzstrategie verwalten können, die Sie von NetApp Backup and Recovery kennen. Mit dieser neuen Version können Sie diese Workloads im Primärspeicher sichern, sie im Sekundärspeicher replizieren und sie im Cloud-Objektspeicher sichern.

Sie können sich für die Vorschau anmelden, indem Sie dieses Formular ausfüllen. "Vorschau des Anmeldeformulars" .

> Diese Dokumentation zum Schutz von Microsoft SQL Server-Workloads wird als Technologievorschau bereitgestellt. NetApp behält sich das Recht vor, Details, Inhalte und Zeitplan dieses Vorschauangebots vor der allgemeinen Verfügbarkeit zu ändern.

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates:

- **3-2-1-Backup-Funktion**: Diese Version integriert SnapCenter -Funktionen und ermöglicht Ihnen die Verwaltung und den Schutz Ihrer SnapCenter -Ressourcen mit einer 3-2-1-Datensicherungsstrategie über die NetApp Backup and Recovery Benutzeroberfläche.

- **Import aus SnapCenter**: Sie können SnapCenter -Sicherungsdaten und -Richtlinien in NetApp Backup and Recovery importieren.
- **Eine neu gestaltete Benutzeroberfläche** ermöglicht eine intuitivere Verwaltung Ihrer Sicherungs- und Wiederherstellungsaufgaben.
- **Sicherungsziele**: Sie können Buckets in Amazon Web Services (AWS), Microsoft Azure Blob Storage, StorageGRID und ONTAP S3-Umgebungen hinzufügen, um sie als Sicherungsziele für Ihre Microsoft SQL Server-Workloads zu verwenden.
- **Workload-Unterstützung**: Mit dieser Version können Sie Microsoft SQL Server-Datenbanken und Verfügbarkeitsgruppen sichern, wiederherstellen, überprüfen und klonen. (Unterstützung für andere Workloads wird in zukünftigen Versionen hinzugefügt.)
- **Flexible Wiederherstellungsoptionen**: Mit dieser Version können Sie Datenbanken im Falle einer Beschädigung oder eines versehentlichen Datenverlusts sowohl am ursprünglichen als auch an alternativen Speicherorten wiederherstellen.
- **Sofortige Produktionskopien**: Erstellen Sie platzsparende Produktionskopien für Entwicklung, Tests oder Analysen in Minuten statt in Stunden oder Tagen.
- Diese Version beinhaltet die Möglichkeit, detaillierte Berichte zu erstellen.

Weitere Informationen zum Schutz von Microsoft SQL Server-Workloads finden Sie unter"Übersicht zum Schützen von Microsoft SQL Server-Workloads" .

09. Juni 2025

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates.

Aktualisierungen der Unterstützung für indizierte Kataloge

Im Februar 2025 haben wir die aktualisierte Indizierungsfunktion (Indexed Catalog v2) eingeführt, die Sie während der Such- und Wiederherstellungsmethode zum Wiederherstellen von Daten verwenden. Die vorherige Version hat die Leistung der Datenindizierung in lokalen Umgebungen erheblich verbessert. Mit dieser Version ist der Indexierungskatalog jetzt in den Umgebungen Amazon Web Services, Microsoft Azure und Google Cloud Platform (GCP) verfügbar.

Wenn Sie ein neuer Kunde sind, ist der indizierte Katalog v2 standardmäßig für alle neuen Umgebungen aktiviert. Wenn Sie bereits Kunde sind, können Sie Ihre Umgebung neu indizieren, um den Indexed Catalog v2 zu nutzen.

Wie aktivieren Sie die Indizierung?

Bevor Sie die Methode „Suchen und Wiederherstellen“ zum Wiederherstellen von Daten verwenden können, müssen Sie die „Indizierung“ in jeder Quellarbeitsumgebung aktivieren, aus der Sie Volumes oder Dateien wiederherstellen möchten. Wählen Sie die Option **Indizierung aktivieren**, wenn Sie eine Suche und Wiederherstellung durchführen.

Der indizierte Katalog kann dann jedes Volume und jede Sicherungsdatei verfolgen, sodass Ihre Suche schnell und effizient erfolgt.

Weitere Informationen finden Sie unter "Indizierung für Suchen und Wiederherstellen aktivieren" .

Azure Private Link-Endpunkte und Dienstendpunkte

Normalerweise richtet NetApp Backup and Recovery einen privaten Endpunkt beim Cloud-Anbieter ein, um Schutzaufgaben zu übernehmen. Diese Version führt eine optionale Einstellung ein, mit der Sie die

automatische Erstellung eines privaten Endpunkts durch NetApp Backup and Recovery aktivieren oder deaktivieren können. Dies kann für Sie nützlich sein, wenn Sie mehr Kontrolle über den Prozess der Erstellung privater Endpunkte wünschen.

Sie können diese Option aktivieren oder deaktivieren, wenn Sie den Schutz aktivieren oder den Wiederherstellungsprozess starten.

Wenn Sie diese Einstellung deaktivieren, müssen Sie den privaten Endpunkt manuell erstellen, damit NetApp Backup and Recovery ordnungsgemäß funktioniert. Ohne ordnungsgemäße Konnektivität können Sie Sicherungs- und Wiederherstellungsaufgaben möglicherweise nicht erfolgreich durchführen.

Unterstützung für SnapMirror to Cloud Resync auf ONTAP S3

In der vorherigen Version wurde die Unterstützung für SnapMirror to Cloud Resync (SM-C Resync) eingeführt. Die Funktion optimiert den Datenschutz während der Volumemigration in NetApp -Umgebungen. Diese Version fügt Unterstützung für SM-C Resync auf ONTAP S3 sowie anderen S3-kompatiblen Anbietern wie Wasabi und MinIO hinzu.

Bringen Sie Ihren eigenen Bucket für StorageGRID mit

Wenn Sie Sicherungsdateien im Objektspeicher für eine Arbeitsumgebung erstellen, erstellt NetApp Backup and Recovery standardmäßig den Container (Bucket oder Speicherkonto) für die Sicherungsdateien im von Ihnen konfigurierten Objektspeicherkonto. Bisher konnten Sie dies überschreiben und Ihren eigenen Container für Amazon S3, Azure Blob Storage und Google Cloud Storage angeben. Mit dieser Version können Sie jetzt Ihren eigenen StorageGRID Objektspeichercontainer mitbringen.

Sehen "Erstellen Sie Ihren eigenen Objektspeichercontainer" .

13. Mai 2025

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates.

SnapMirror to Cloud Resync für Volumemigrationen

Die SnapMirror to Cloud Resync-Funktion optimiert den Datenschutz und die Kontinuität während Volumemigrationen in NetApp -Umgebungen. Wenn ein Volume mithilfe von SnapMirror Logical Replication (LRSE) von einer lokalen NetApp Bereitstellung zu einer anderen oder zu einer Cloud-basierten Lösung wie Cloud Volumes ONTAP migriert wird, stellt SnapMirror to Cloud Resync sicher, dass bestehende Cloud-Backups intakt und betriebsbereit bleiben.

Durch diese Funktion entfällt die Notwendigkeit einer zeit- und ressourcenintensiven Neufestlegung der Basislinie, sodass die Sicherungsvorgänge nach der Migration fortgesetzt werden können. Diese Funktion ist in Workload-Migrationsszenarien wertvoll, unterstützt sowohl FlexVols als auch FlexGroups und ist ab ONTAP Version 9.16.1 verfügbar.

Durch die Aufrechterhaltung der Backup-Kontinuität in allen Umgebungen steigert SnapMirror to Cloud Resync die Betriebseffizienz und reduziert die Komplexität der Hybrid- und Multi-Cloud-Datenverwaltung.

Einzelheiten zur Durchführung des Resynchronisierungsvorgangs finden Sie unter "Migrieren Sie Volumes mit SnapMirror zu Cloud Resync" .

Unterstützung für MinIO-Objektspeicher von Drittanbietern (Vorschau)

NetApp Backup and Recovery erweitert jetzt seine Unterstützung auf Objektspeicher von Drittanbietern mit einem Schwerpunkt auf MinIO. Mit dieser neuen Vorschaufunktion können Sie jeden S3-kompatiblen

Objektspeicher für Ihre Sicherungs- und Wiederherstellungsanforderungen nutzen.

Mit dieser Vorschauversion hoffen wir, eine robuste Integration mit Objektspeichern von Drittanbietern sicherzustellen, bevor die vollständige Funktionalität eingeführt wird. Wir möchten Sie ermutigen, diese neue Funktion zu erkunden und Feedback zu geben, um zur Verbesserung des Dienstes beizutragen.

Diese Funktion sollte nicht in der Produktion verwendet werden.

Einschränkungen des Vorschaumodus

Obwohl sich diese Funktion in der Vorschauphase befindet, gelten bestimmte Einschränkungen:

- Bring Your Own Bucket (BYOB) wird nicht unterstützt.
- Das Aktivieren von DataLock in der Richtlinie wird nicht unterstützt.
- Das Aktivieren des Archivierungsmodus in der Richtlinie wird nicht unterstützt.
- Es werden nur lokale ONTAP Umgebungen unterstützt.
- MetroCluster wird nicht unterstützt.
- Optionen zum Aktivieren der Verschlüsselung auf Bucket-Ebene werden nicht unterstützt.

Erste Schritte

Um diese Vorschaufunktion zu verwenden, müssen Sie ein Flag auf dem Konsolenagenten aktivieren. Sie können dann die Verbindungsdetails Ihres MinIO-Objektspeichers von Drittanbietern in den Schutz-Workflow eingeben, indem Sie im Abschnitt „Backup“ die Option „**Drittanbieterkompatibler** Objektspeicher“ auswählen.

16. April 2025

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates.

Verbesserungen der Benutzeroberfläche

Diese Version verbessert Ihr Erlebnis durch Vereinfachung der Benutzeroberfläche:

- Das Entfernen der Spalte „Aggregat“ aus den Volume-Tabellen sowie der Spalten „Snapshot-Richtlinie“, „Sicherungsrichtlinie“ und „Replikationsrichtlinie“ aus der Volume-Tabelle im V2-Dashboard führt zu einem optimierteren Layout.
- Durch das Ausschließen nicht aktivierter Arbeitsumgebungen aus der Dropdown-Liste wird die Benutzeroberfläche übersichtlicher, die Navigation effizienter und das Laden beschleunigt.
- Während die Sortierung nach der Spalte „Tags“ deaktiviert ist, können Sie die Tags weiterhin anzeigen und so sicherstellen, dass wichtige Informationen weiterhin leicht zugänglich sind.
- Das Entfernen von Beschriftungen auf Schutzsymbolen trägt zu einem übersichtlicheren Erscheinungsbild bei und verkürzt die Ladezeit.
- Während des Aktivierungsprozesses der Arbeitsumgebung wird in einem Dialogfeld ein Ladesymbol angezeigt, um Feedback zu geben, bis der Erkennungsprozess abgeschlossen ist. Dies erhöht die Transparenz und das Vertrauen in die Funktionsweise des Systems.

Verbessertes Volume-Dashboard (Vorschau)

Das Volume Dashboard wird jetzt in weniger als 10 Sekunden geladen und bietet eine viel schnellere und effizientere Benutzeroberfläche. Diese Vorschauversion steht ausgewählten Kunden zur Verfügung und bietet

ihnen einen ersten Einblick in diese Verbesserungen.

Unterstützung für Wasabi-Objektspeicher von Drittanbietern (Vorschau)

NetApp Backup and Recovery erweitert jetzt seine Unterstützung auf Objektspeicher von Drittanbietern mit einem Schwerpunkt auf Wasabi. Mit dieser neuen Vorschaufunktion können Sie jeden S3-kompatiblen Objektspeicher für Ihre Sicherungs- und Wiederherstellungsanforderungen nutzen.

Erste Schritte mit Wasabi

Um Speicher von Drittanbietern als Objektspeicher zu verwenden, müssen Sie im Konsolenagenten ein Flag aktivieren. Anschließend können Sie die Verbindungsdetails für Ihren Objektspeicher eines Drittanbieters eingeben und ihn in Ihre Sicherungs- und Wiederherstellungs-Workflows integrieren.

Schritte

1. Melden Sie sich per SSH bei Ihrem Connector an.
2. Gehen Sie in den NetApp Backup and Recovery CBS-Servercontainer:

```
docker exec -it cloudmanager_cbs sh
```

3. Öffnen Sie die `default.json` Datei innerhalb der `config` Ordner über VIM oder einen anderen Editor:

```
vi default.json
```

4. Ändern `allow-s3-compatible` : false bis `allow-s3-compatible` : WAHR.
5. Speichern Sie die Änderungen.
6. Verlassen Sie den Container.
7. Starten Sie den CBS-Servercontainer von NetApp Backup and Recovery neu.

Ergebnis

Nachdem der Container wieder eingeschaltet ist, öffnen Sie die NetApp Backup and Recovery -Benutzeroberfläche. Wenn Sie eine Sicherung initiieren oder eine Sicherungsstrategie bearbeiten, wird der neue Anbieter „S3-kompatibel“ zusammen mit anderen Sicherungsanbietern von AWS, Microsoft Azure, Google Cloud, StorageGRID und ONTAP S3 aufgeführt.

Einschränkungen des Vorschaumodus

Während sich diese Funktion in der Vorschauphase befindet, beachten Sie bitte die folgenden Einschränkungen:

- Bring Your Own Bucket (BYOB) wird nicht unterstützt.
- Das Aktivieren von DataLock in einer Richtlinie wird nicht unterstützt.
- Das Aktivieren des Archivierungsmodus in einer Richtlinie wird nicht unterstützt.
- Es werden nur lokale ONTAP Umgebungen unterstützt.
- MetroCluster wird nicht unterstützt.
- Optionen zum Aktivieren der Verschlüsselung auf Bucket-Ebene werden nicht unterstützt.

Wir empfehlen Ihnen, während dieser Vorschau diese neue Funktion zu erkunden und Feedback zur Integration mit Objektspeichern von Drittanbietern zu geben, bevor die vollständige Funktionalität eingeführt wird.

17. März 2025

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates.

Durchsuchen von SMB-Snapshots

Dieses Update für NetApp Backup and Recovery behebt ein Problem, das Kunden daran hinderte, lokale Snapshots in einer SMB-Umgebung zu durchsuchen.

AWS GovCloud-Umgebungsupdate

Dieses Update für NetApp Backup and Recovery behebt ein Problem, das aufgrund von TLS-Zertifikatfehlern die Verbindung der Benutzeroberfläche mit einer AWS GovCloud-Umgebung verhinderte. Das Problem wurde behoben, indem anstelle der IP-Adresse der Hostname des Konsolenagenten verwendet wurde.

Aufbewahrungsgrenzen für Sicherungsrichtlinien

Zuvor beschränkte die NetApp Backup and Recovery Benutzeroberfläche die Anzahl der Backups auf 999 Kopien, während die CLI mehr zuließ. Jetzt können Sie bis zu 4.000 Volumes an eine Sicherungsrichtlinie anhängen und 1.018 Volumes einschließen, die keiner Sicherungsrichtlinie angehängt sind. Dieses Update enthält zusätzliche Validierungen, die ein Überschreiten dieser Grenzwerte verhindern.

SnapMirror Cloud-Neusynchronisierung

Dieses Update stellt sicher, dass die SnapMirror Cloud-Neusynchronisierung nicht von NetApp Backup and Recovery für nicht unterstützte ONTAP Versionen gestartet werden kann, nachdem eine SnapMirror Beziehung gelöscht wurde.

21. Februar 2025

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates.

Leistungsstarke Indizierung

NetApp Backup and Recovery führt eine aktualisierte Indizierungsfunktion ein, die die Indizierung von Daten auf dem Quellsystem effizienter macht. Die neue Indexierungsfunktion umfasst Aktualisierungen der Benutzeroberfläche, eine verbesserte Leistung der Such- und Wiederherstellungsmethode zum Wiederherstellen von Daten, Upgrades der globalen Suchfunktionen und eine bessere Skalierbarkeit.

Hier ist eine Aufschlüsselung der Verbesserungen:

- **Ordnerkonsolidierung**: Die aktualisierte Version gruppiert Ordner anhand von Namen, die bestimmte Kennungen enthalten, wodurch der Indizierungsprozess reibungsloser verläuft.
- **Parquet-Dateikomprimierung**: Die aktualisierte Version reduziert die Anzahl der Dateien, die zum Indizieren jedes Volumes verwendet werden, vereinfacht den Prozess und macht eine zusätzliche Datenbank überflüssig.
- **Skalierung mit mehr Sitzungen**: Die neue Version fügt mehr Sitzungen hinzu, um Indizierungsaufgaben zu bewältigen und so den Prozess zu beschleunigen.

- **Unterstützung für mehrere Indexcontainer**: Die neue Version verwendet mehrere Container, um Indizierungsaufgaben besser zu verwalten und zu verteilen.
- **Geteilter Index-Workflow**: Die neue Version teilt den Indexierungsprozess in zwei Teile und steigert so die Effizienz.
- **Verbesserte Parallelität**: Die neue Version ermöglicht das gleichzeitige Löschen oder Verschieben von Verzeichnissen, wodurch der Indizierungsprozess beschleunigt wird.

Wer profitiert von dieser Funktion?

Die neue Indexierungsfunktion steht allen Neukunden zur Verfügung.

Wie aktivieren Sie die Indizierung?

Bevor Sie die Methode „Suchen und Wiederherstellen“ zum Wiederherstellen von Daten verwenden können, müssen Sie die „Indizierung“ auf jedem Quellsystem aktivieren, von dem Sie Volumes oder Dateien wiederherstellen möchten. Dadurch kann der indizierte Katalog jedes Volume und jede Sicherungsdatei verfolgen, sodass Ihre Suchvorgänge schnell und effizient erfolgen.

Aktivieren Sie die Indizierung in der Quellarbeitsumgebung, indem Sie beim Durchführen einer Suche und Wiederherstellung die Option „Indizierung aktivieren“ auswählen.

Weitere Informationen finden Sie in der Dokumentation "So stellen Sie ONTAP -Daten mit Search Restore wieder her" .

Unterstützte Skala

Die neue Indizierungsfunktion unterstützt Folgendes:

- Globale Sucheffizienz in weniger als 3 Minuten
- Bis zu 5 Milliarden Dateien
- Bis zu 5000 Volumes pro Cluster
- Bis zu 100.000 Snapshots pro Volume
- Die maximale Zeit für die Basisindexierung beträgt weniger als 7 Tage. Die tatsächliche Zeit hängt von Ihrer Umgebung ab.

Leistungsverbesserungen bei der globalen Suche

Diese Version enthält auch Verbesserungen der globalen Suchleistung. Sie sehen jetzt Fortschrittsanzeigen und detailliertere Suchergebnisse, einschließlich der Anzahl der Dateien und der für die Suche benötigten Zeit. Spezielle Container für Suche und Indizierung stellen sicher, dass globale Suchvorgänge in weniger als fünf Minuten abgeschlossen sind.

Beachten Sie die folgenden Überlegungen zur globalen Suche:

- Der neue Index wird nicht für Snapshots ausgeführt, die als stündlich gekennzeichnet sind.
- Die neue Indizierungsfunktion funktioniert nur bei Snapshots auf FlexVols und nicht bei Snapshots auf FlexGroups.

13. Februar 2025

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates.

Vorschauversion von NetApp Backup and Recovery

Diese Vorschauversion von NetApp Backup and Recovery bietet eine aktualisierte Benutzeroberfläche, mit der Sie Microsoft SQL Server-Workloads mithilfe einer 3-2-1-Schutzstrategie verwalten können, die Sie von NetApp Backup and Recovery kennen. Mit dieser neuen Version können Sie diese Workloads im Primärspeicher sichern, sie im Sekundärspeicher replizieren und sie im Cloud-Objektspeicher sichern.

> Diese Dokumentation wird als Technologievorschau bereitgestellt. Bei diesem Vorschauangebot behält sich NetApp das Recht vor, Angebotsdetails, Inhalte und Zeitplan vor der allgemeinen Verfügbarkeit zu ändern.

Diese Version von NetApp Backup and Recovery Preview 2025 enthält die folgenden Updates.

- Eine neu gestaltete Benutzeroberfläche, die eine intuitivere Erfahrung bei der Verwaltung Ihrer Sicherungs- und Wiederherstellungsaufgaben bietet.
- Mit der Vorschauversion können Sie Microsoft SQL Server-Datenbanken sichern und wiederherstellen. (Unterstützung für andere Workloads wird in zukünftigen Versionen hinzugefügt.)
- Diese Version integriert SnapCenter -Funktionen und ermöglicht Ihnen die Verwaltung und den Schutz Ihrer SnapCenter -Ressourcen mit einer 3-2-1-Datensicherungsstrategie über die NetApp Backup and Recovery -Benutzeroberfläche.
- Mit dieser Version können Sie SnapCenter -Workloads in NetApp Backup and Recovery importieren.

22. November 2024

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates.

SnapLock Compliance und SnapLock Enterprise Schutzmodi

NetApp Backup and Recovery kann jetzt sowohl FlexVol als auch FlexGroup -Volumes vor Ort sichern, die entweder mit den Schutzmodi SnapLock Compliance oder SnapLock Enterprise konfiguriert sind. Für diese Unterstützung müssen Ihre Cluster ONTAP 9.14 oder höher ausführen. Das Sichern von FlexVol -Volumes im SnapLock Enterprise Modus wird seit ONTAP Version 9.11.1 unterstützt. Frühere ONTAP Versionen bieten keine Unterstützung für die Sicherung von SnapLock Schutzvolumes.

Die vollständige Liste der unterstützten Volumes finden Sie im "Erfahren Sie mehr über NetApp Backup and Recovery" .

Indizierung für den Such- und Wiederherstellungsprozess auf der Volumes-Seite

Bevor Sie „Suchen und Wiederherstellen“ verwenden können, müssen Sie die „Indizierung“ auf jedem Quellsystem aktivieren, von dem Sie Volumedaten wiederherstellen möchten. Dadurch kann der indizierte Katalog die Sicherungsdateien für jedes Volume verfolgen. Auf der Seite „Volumes“ wird jetzt der Indizierungsstatus angezeigt:

- Indiziert: Bände wurden indiziert.
- Im Gange
- Nicht indiziert
- Indizierung pausiert
- Fehler
- Nicht aktiviert

27. September 2024

Diese Version von NetApp Backup and Recovery enthält die folgenden Updates.

Podman-Unterstützung auf RHEL 8 oder 9 mit Durchsuchen und Wiederherstellen

NetApp Backup and Recovery unterstützt jetzt die Wiederherstellung von Dateien und Ordnern unter Red Hat Enterprise Linux (RHEL) Version 8 und 9 mithilfe der Podman-Engine. Dies gilt für die Durchsuchen- und Wiederherstellungsmethode von NetApp Backup and Recovery .

Der Konsolenagent Version 3.9.40 unterstützt bestimmte Versionen von Red Hat Enterprise Linux Version 8 und 9 für jede manuelle Installation der Konsolenagent-Software auf einem RHEL 8- oder 9-Host, unabhängig vom Standort zusätzlich zu den im "Hostanforderungen" . Diese neueren RHEL-Versionen erfordern die Podman-Engine anstelle der Docker-Engine. Bisher gab es bei NetApp Backup and Recovery zwei Einschränkungen bei der Verwendung der Podman-Engine. Diese Einschränkungen wurden aufgehoben.

"Erfahren Sie mehr über die Wiederherstellung von ONTAP -Daten aus Sicherungsdateien".

Schnellere Katalogindizierung verbessert Suche und Wiederherstellung

Diese Version enthält einen verbesserten Katalogindex, der die Basisindizierung viel schneller abschließt. Durch die schnellere Indizierung können Sie die Such- und Wiederherstellungsfunktion schneller nutzen.

"Erfahren Sie mehr über die Wiederherstellung von ONTAP -Daten aus Sicherungsdateien".

Bekannte Einschränkungen bei NetApp Backup and Recovery für ONTAP -Volumes

Plattformen, Geräte oder Funktionen, die mit dieser Version nicht oder nicht gut funktionieren, sind hier aufgelistet. Lesen Sie diese Einschränkungen sorgfältig durch.

- NetApp Backup and Recovery kann Cloud Volumes ONTAP in einem Objektspeicher in den AWS-Regionen China (einschließlich Peking und Ningxia) sichern. Möglicherweise müssen Sie jedoch zunächst die Identitäts- und Zugriffsrichtlinien manuell ändern.

  Weitere Informationen zum Erstellen eines Konsolenagenten in AWS finden Sie unter "Installieren eines Konsolenagenten in AWS" .

  Weitere Einzelheiten finden Sie im Blogbeitrag "NetApp Backup and Recovery Feature-Blog Mai 2023" .

- NetApp Backup and Recovery unterstützt keine Microsoft Azure China-Regionen.

  Weitere Informationen zum Erstellen eines Konsolen-Agenten in Azure finden Sie unter "Installieren eines Konsolen-Agenten in Azure" .

- NetApp Backup and Recovery unterstützt keine Sicherungen von FlexCache -Volumes.

Replikationsbeschränkungen für ONTAP -Volumes

- Sie können jeweils nur ein FlexGroup Volume zur Replikation auswählen. Sie müssen Backups für jedes FlexGroup Volume separat aktivieren.

  Für FlexVol -Volumes gibt es keine Einschränkung – Sie können alle FlexVol Volumes in Ihrem System

auswählen und dieselben Sicherungsrichtlinien zuweisen.

- Die folgenden Funktionen werden unterstützt in "NetApp Replication" , jedoch nicht bei Verwendung der Replikationsfunktion von NetApp Backup and Recovery:
  - Eine Kaskadenkonfiguration, bei der die Replikation von Volume A zu Volume B und von Volume B zu Volume C erfolgt, wird nicht unterstützt. Die Replikation von Volume A zu Volume B wird unterstützt.
  - Es gibt keine Unterstützung für die Replikation von Daten zu und von FSx für ONTAP -Systeme.
  - Das Erstellen einer einmaligen Replikation eines Volumes wird nicht unterstützt.
- Wenn beim Erstellen von Replikationen von lokalen ONTAP -Systemen die ONTAP Version auf dem Cloud Volumes ONTAP Zielsystem 9.8, 9.9 oder 9.11 ist, sind nur Mirror-Vault-Richtlinien zulässig.
- NetApp Backup & Recovery unterstützt nicht die Konvertierung eines FlexVol volume mit einer aktiven Cloud-Backup-Beziehung in ein FlexGroup -Volume unter Beibehaltung der Cloud-Backup-Funktionalität.

Einschränkungen bei der Sicherung auf Objekte für ONTAP -Volumes

- Beim Sichern von Daten behält NetApp Backup and Recovery die NetApp Volume Encryption (NVE) nicht bei. Dies bedeutet, dass verschlüsselte Daten auf dem NVE-Volume während der Datenübertragung zum Ziel entschlüsselt werden und die Verschlüsselung nicht aufrechterhalten wird.

  Eine Erklärung zu diesen Verschlüsselungsarten finden Sie unterhttps://docs.netapp.com/us-en/ontap/encryption-at-rest/configure-netapp-volume-encryption-concept.html["Übersicht über die Konfiguration der NetApp Volume-Verschlüsselung"^] .

- Wenn Snapshots mit langfristiger Aufbewahrung auf einem SnapMirror Zielvolume mithilfe des Zeitplans in der SnapMirror -Richtlinie aktiviert sind, werden Snapshots direkt auf dem Zielvolume erstellt. In diesem Fall sollten Sie diese Volumes nicht mit NetApp Backup and Recovery sichern, da diese Snapshots nicht in den Objektspeicher verschoben werden.
- Beim Sichern von Daten behält NetApp Backup and Recovery die NetApp Volume Encryption (NVE) nicht bei. Dies bedeutet, dass verschlüsselte Daten auf dem NVE-Volume während der Datenübertragung zum Ziel entschlüsselt werden und die Verschlüsselung nicht aufrechterhalten wird.

  Eine Erklärung zu diesen Verschlüsselungsarten finden Sie unterhttps://docs.netapp.com/us-en/ontap/encryption-at-rest/configure-netapp-volume-encryption-concept.html["Übersicht über die Konfiguration der NetApp Volume-Verschlüsselung"^] .

- Wenn Snapshots mit langfristiger Aufbewahrung auf einem SnapMirror Zielvolume mithilfe des Zeitplans in der SnapMirror -Richtlinie aktiviert sind, werden Snapshots direkt auf dem Zielvolume erstellt. In diesem Fall sollten Sie diese Volumes nicht mit NetApp Backup and Recovery sichern, da diese Snapshots nicht in den Objektspeicher verschoben werden.
- Wenn Sie eine Sicherungsrichtlinie erstellen oder bearbeiten und der Richtlinie keine Volumes zugewiesen sind, kann die Anzahl der aufbewahrten Sicherungen maximal 1018 betragen. Nachdem Sie der Richtlinie Volumes zugewiesen haben, können Sie die Richtlinie bearbeiten, um bis zu 4.000 Sicherungen zu erstellen.
- Beim Sichern von Datensicherungsvolumes (DP):
  - Beziehungen zu den SnapMirror -Labels `app_consistent` Und `all_source_snapshot` wird nicht in der Cloud gesichert.
  - Wenn Sie lokale Kopien von Snapshots auf dem SnapMirror Zielvolume erstellen (unabhängig von den verwendeten SnapMirror -Labels), werden diese Snapshots nicht als Backups in die Cloud verschoben. Zu diesem Zeitpunkt müssen Sie eine Snapshot-Richtlinie mit den gewünschten Bezeichnungen für das Quell-DP-Volume erstellen, damit NetApp Backup and Recovery diese sichern kann.

- FlexGroup Volume-Backups können nicht in den Archivspeicher verschoben werden.
- FlexGroup -Volume-Backups können DataLock- und Ransomware-Schutz verwenden, wenn auf dem Cluster ONTAP 9.13.1 oder höher ausgeführt wird.
- Die SVM-DR-Volume-Sicherung wird mit den folgenden Einschränkungen unterstützt:
  - Backups werden nur vom sekundären ONTAP unterstützt.
  - Die auf das Volume angewendete Snapshot-Richtlinie muss eine der von NetApp Backup and Recovery erkannten Richtlinien sein, einschließlich täglich, wöchentlich, monatlich usw. Die Standardrichtlinie „sm_created“ (verwendet für **Alle Snapshots spiegeln**) wird nicht erkannt und das DP-Volume wird nicht in der Liste der Volumes angezeigt, die gesichert werden können.
  - SVM-DR und Volume-Backup und -Wiederherstellung funktionieren völlig unabhängig, wenn das Backup entweder von der Quelle oder vom Ziel erstellt wird. Die einzige Einschränkung besteht darin, dass SVM-DR die SnapMirror -Cloud-Beziehung nicht repliziert. Im DR-Szenario müssen Sie die SnapMirror Cloud-Beziehung manuell aktualisieren, wenn die SVM am sekundären Standort online geht.
- MetroCluster -Unterstützung:
  - Wenn Sie ONTAP 9.12.1 GA oder höher verwenden, wird die Sicherung unterstützt, wenn eine Verbindung zum primären System besteht. Die gesamte Backup-Konfiguration wird auf das sekundäre System übertragen, sodass die Backups in die Cloud nach der Umstellung automatisch fortgesetzt werden. Sie müssen auf dem sekundären System kein Backup einrichten (tatsächlich ist dies nicht möglich).
  - Wenn Sie ONTAP 9.12.0 und früher verwenden, wird die Sicherung nur vom sekundären ONTAP System unterstützt.
  - Ab ONTAP 9.18.1 werden FlexGroup-Volume-Backups in MetroCluster-Konfigurationen unterstützt.
- Die Ad-hoc-Volume-Sicherung mit der Schaltfläche „Jetzt sichern“ wird auf Datensicherungsvolumes nicht unterstützt.
- SM-BC-Konfigurationen werden nicht unterstützt.
- ONTAP unterstützt kein Fan-Out von SnapMirror -Beziehungen von einem einzelnen Volume auf mehrere Objektspeicher. Daher wird diese Konfiguration von NetApp Backup and Recovery nicht unterstützt.
- Der WORM/Compliance-Modus in einem Objektspeicher wird derzeit auf Amazon S3, Azure und StorageGRID unterstützt. Dies wird als DataLock-Funktion bezeichnet und muss mithilfe der NetApp Backup and Recovery -Einstellungen verwaltet werden, nicht über die Cloud-Provider-Schnittstelle.

Wiederherstellungsbeschränkungen für ONTAP -Volumes

Diese Einschränkungen gelten sowohl für die Methoden „Suchen und Wiederherstellen“ als auch „Durchsuchen und Wiederherstellen“ zum Wiederherstellen von Dateien und Ordnern, sofern nicht ausdrücklich darauf hingewiesen wird.

- Mit „Durchsuchen und Wiederherstellen“ können bis zu 100 einzelne Dateien gleichzeitig wiederhergestellt werden.
- Mit „Suchen und Wiederherstellen“ kann jeweils eine Datei wiederhergestellt werden.
- Bei Verwendung von ONTAP 9.13.0 oder höher können „Browse & Restore“ und „Search & Restore“ einen Ordner zusammen mit allen darin enthaltenen Dateien und Unterordnern wiederherstellen.

  Wenn Sie eine ONTAP -Version höher als 9.11.1, aber vor 9.13.0 verwenden, kann der Wiederherstellungsvorgang nur den ausgewählten Ordner und die Dateien in diesem Ordner wiederherstellen. Unterordner oder Dateien in Unterordnern werden nicht wiederhergestellt.

Bei Verwendung einer ONTAP -Version vor 9.11.1 wird die Ordnerwiederherstellung nicht unterstützt.

- Die Wiederherstellung von Verzeichnissen/Ordnern wird für Daten im Archivspeicher nur unterstützt, wenn auf dem Cluster ONTAP 9.13.1 oder höher ausgeführt wird.
- Die Wiederherstellung von Verzeichnissen/Ordnern wird für mit DataLock geschützte Daten nur unterstützt, wenn auf dem Cluster ONTAP 9.13.1 oder höher ausgeführt wird.
- Die Wiederherstellung von Verzeichnissen/Ordnern wird derzeit nicht aus Replikationen und/oder lokalen Snapshots unterstützt.
- Die Wiederherstellung von FlexGroup Volumes auf FlexVol -Volumes oder von FlexVol Volumes auf FlexGroup -Volumes wird nicht unterstützt.
- Die wiederherzustellende Datei muss dieselbe Sprache verwenden wie die Sprache auf dem Zielvolume. Wenn die Sprachen nicht übereinstimmen, erhalten Sie eine Fehlermeldung.
- Die Wiederherstellungspriorität „Hohe“ wird beim Wiederherstellen von Daten aus dem Azure-Archivspeicher auf StorageGRID -Systemen nicht unterstützt.
- Wenn Sie ein DP-Volume sichern und dann beschließen, die SnapMirror -Beziehung zu diesem Volume aufzuheben, können Sie keine Dateien auf diesem Volume wiederherstellen, es sei denn, Sie löschen auch die SnapMirror -Beziehung oder kehren die SnapMirror Richtung um.
- Einschränkungen der Schnellwiederherstellung:
  - Der Zielspeicherort muss ein Cloud Volumes ONTAP -System mit ONTAP 9.13.0 oder höher sein.
  - Es wird nicht für Sicherungen unterstützt, die sich im Archivspeicher befinden.
  - FlexGroup -Volumes werden nur unterstützt, wenn auf dem Quellsystem, von dem das Cloud-Backup erstellt wurde, ONTAP 9.12.1 oder höher ausgeführt wurde.
  - SnapLock -Volumes werden nur unterstützt, wenn auf dem Quellsystem, von dem das Cloud-Backup erstellt wurde, ONTAP 9.11.0 oder höher ausgeführt wurde.

Bekannte Einschränkungen bei NetApp Backup and Recovery für Microsoft SQL Server-Workloads

Plattformen, Geräte oder Funktionen, die mit dieser Version nicht oder nicht gut funktionieren, sind hier aufgelistet. Lesen Sie diese Einschränkungen sorgfältig durch.

Unterstützung des Klon-Lebenszyklus

- Das Klonen aus dem Objektspeicher wird nicht unterstützt.
- Massenklonvorgänge werden für On-Demand-Klone nicht unterstützt.
- Die Auswahl von I-Gruppen wird nicht unterstützt.
- Die Auswahl von QOS-Optionen (maximaler Durchsatz) wird nicht unterstützt.

Nur Standardbereitstellungsmodus

Diese NetApp Backup and Recovery Version funktioniert nur im Standardbereitstellungsmodus, nicht im eingeschränkten oder privaten Modus.

Einschränkung des Windows-Clusternamens

Der Windows-Clustername darf keinen Unterstrich (_) enthalten.

Probleme bei der SnapCenter -Migration

Die Migration von Ressourcen von SnapCenter in NetApp Backup and Recovery unterliegt den folgenden Einschränkungen.

Weitere Informationen zur Migration von SnapCenter -Richtlinien zu NetApp Backup and Recovery -Richtlinien finden Sie unter"Richtlinien in SnapCenter im Vergleich zu denen in NetApp Backup and Recovery" .

Einschränkungen der Ressourcengruppe

Wenn alle Ressourcen in einer Ressourcengruppe geschützt sind und eine dieser Ressourcen auch außerhalb der Ressourcengruppe geschützt ist, wird die Migration von SnapCenter blockiert.

Problemumgehung: Schützen Sie die Ressource entweder in einer Ressourcengruppe oder einzeln, aber nicht in beiden.

Ressourcen mit mehreren Richtlinien, die dieselbe Zeitplanebene verwenden, werden nicht unterstützt

Sie können einer Ressource nicht mehrere Richtlinien zuweisen, die dieselbe Zeitplanebene verwenden (z. B. stündlich, täglich, wöchentlich usw.). NetApp Backup and Recovery importiert diese Ressourcen nicht aus SnapCenter.

Problemumgehung: Fügen Sie einer Ressource nur eine Richtlinie mit derselben Zeitplanebene hinzu.

Stundenrichtlinien müssen zu Beginn der Stunde beginnen

Wenn Sie über eine SnapCenter -Richtlinie verfügen, die sich stündlich wiederholt, aber zu Beginn der Stunde keine Intervalle verwendet, importiert NetApp Backup and Recovery die Ressource nicht. Beispielsweise werden Richtlinien mit Zeitplänen von 1:30, 2:30, 3:30 usw. nicht unterstützt, während Richtlinien mit Zeitplänen von 1:00, 2:00, 3:00 usw. unterstützt werden.

Problemumgehung: Verwenden Sie eine Richtlinie, die sich ab der vollen Stunde in 1-Stunden-Intervallen wiederholt.

Sowohl tägliche als auch monatliche Richtlinien, die an eine Ressource angehängt sind, werden nicht unterstützt

Wenn sich eine SnapCenter -Richtlinie sowohl in Tages- als auch in Monatsintervallen wiederholt, importiert NetApp Backup and Recovery die Richtlinie nicht.

Sie können beispielsweise einer Ressource keine tägliche Richtlinie (mit weniger als oder gleich 7 Tagen oder mehr als 7 Tagen) und derselben Ressource auch eine monatliche Richtlinie zuordnen.

Problemumgehung: Verwenden Sie eine Richtlinie, die ein tägliches oder ein monatliches Intervall verwendet, aber nicht beides.

On-Demand-Backup-Richtlinien nicht migriert

NetApp Backup and Recovery importiert keine On-Demand-Sicherungsrichtlinien aus SnapCenter.

Nur-Protokoll-Sicherungsrichtlinien werden nicht migriert

NetApp Backup and Recovery importiert keine Nur-Protokoll-Sicherungsrichtlinien aus SnapCenter. Wenn eine SnapCenter -Richtlinie Nur-Protokoll-Backups umfasst, importiert NetApp Backup and Recovery die Ressource nicht.

Problemumgehung: Verwenden Sie in SnapCenter eine Richtlinie, die mehr als nur reine Protokollsicherungen verwendet.

Host-Zuordnung

SnapCenter verfügt nicht über die Möglichkeit, Speichercluster oder SVMs für die Ressourcen den Hosts zuzuordnen, NetApp Backup and Recovery hingegen schon. Der lokale ONTAP Cluster oder SVM wird in den Vorschauversionen von NetApp Backup and Recovery keinem Host zugeordnet. Darüber hinaus unterstützt die NetApp Console keine SVMs.

Problemumgehung: Erstellen Sie vor dem Importieren von Ressourcen aus SnapCenter ein System in NetApp Backup and Recovery für alle lokalen ONTAP Speichersysteme, die im lokalen SnapCenter registriert sind. Importieren Sie dann die Ressourcen für diesen Cluster von SnapCenter in NetApp Backup and Recovery.

Fahrpläne nicht im 15-Minuten-Takt

Wenn Sie über einen SnapCenter -Richtlinienzeitplan verfügen, der zu einer bestimmten Zeit beginnt und in anderen Intervallen als 15 Minuten wiederholt wird, importiert NetApp Backup and Recovery den Zeitplan nicht.

Problemumgehung: Passen Sie die Richtlinie mithilfe von SnapCenter so an, dass sie in 15-Minuten-Intervallen wiederholt wird.

Eingeschränkter Support für Virtualisierungsverwaltungssoftware

Wenn Sie KVM-Workloads schützen, unterstützt NetApp Backup and Recovery die Erkennung von KVM-Workloads nicht, wenn Virtualisierungsverwaltungssoftware wie Apache CloudStack oder Red Hat OpenShift Virtualization verwendet wird.

Bekannte Einschränkungen bei NetApp Backup and Recovery für VMware-Workloads

Plattformen, Geräte oder Funktionen, die mit dieser Version nicht oder nicht gut funktionieren, sind hier aufgelistet. Lesen Sie diese Einschränkungen sorgfältig durch.

Die folgenden Aktionen werden in der Vorschauversion von VMware-Workloads in NetApp Backup and Recovery nicht unterstützt:

- Montieren
- Aushängen
- VMDK anhängen
- VMDK trennen
- vVol-Unterstützung

- NVMe-Unterstützung
- E-Mail-Integration
- Richtlinie bearbeiten
- Schutzgruppe bearbeiten
- Unterstützung der rollenbasierten Zugriffskontrolle (RBAC)

Bekannte Einschränkungen bei NetApp Backup and Recovery für Hyper-V-Workloads

Plattformen, Geräte oder Funktionen, die mit dieser Version nicht oder nicht gut funktionieren, sind hier aufgelistet. Lesen Sie diese Einschränkungen sorgfältig durch.

Nicht unterstützte Aktionen

Die folgenden Aktionen werden in der privaten Vorschauversion von Hyper-V-Workloads in NetApp Backup and Recovery nicht unterstützt:

- Erstellen Sie Ressourcengruppen mithilfe von VMs von mehreren Hyper-V-Hosts.
- Wiederherstellen von VMs an einem anderen Standort
- Spanning-Disks (über mehrere CIFS-Freigaben hinweg)
- Schützen Sie VMs über SAN
- Unabhängig von der Einstellung „Prozessorkompatibilität“ in Hyper-V können Sie keine VMs oder VM-Daten zwischen Systemen mit unterschiedlichen CPU-Herstellern (Intel zu AMD oder umgekehrt) wiederherstellen. Diese Einstellung unterstützt nur die Kompatibilität zwischen verschiedenen Generationen desselben Herstellers (z. B. Intel zu Intel oder AMD zu AMD).

In der Version vom 19. Januar 2026 ist ein Upgrade der NetApp -Plugins für Hyper-V oder Windows über die Option **Upgrade** im Menü Aktionen nicht möglich. Entfernen Sie stattdessen jeden Hyper-V-Host und fügen Sie ihn anschließend wieder hinzu, um die Plugins zu aktualisieren.

Bekannte Einschränkungen bei NetApp Backup and Recovery für KVM-Workloads

Plattformen, Geräte oder Funktionen, die mit dieser Version nicht oder nicht gut funktionieren, sind hier aufgelistet. Lesen Sie diese Einschränkungen sorgfältig durch.

Die folgenden Aktionen und Konfigurationen werden in der privaten Vorschauversion von KVM-Workloads in NetApp Backup and Recovery nicht unterstützt:

Nicht unterstützte Aktionen

Die folgenden Aktionen werden in der privaten Vorschauversion nicht unterstützt:

- Klonen, Mounten oder Unmounten von VMs
- Wiederherstellen von VMs an einem anderen Standort

- Schützen Sie im SAN gespeicherte VMs
- Anwendungen schützen
- Schutzgruppen bearbeiten
- Erstellen Sie Schutzgruppen mithilfe von VMs von mehreren KVM-Hosts
- Erstellen Sie benutzerdefinierte Backups (es werden nur Backups unterstützt, die von der NetApp Console aus initiiert werden).

Nicht unterstützte Konfigurationen

Die folgenden Konfigurationen werden nicht unterstützt:

- Rollenbasierte Zugriffskontrolle (RBAC)
- Direkt an den KVM-Host angeschlossene Festplatten
- Datenträger, die sich über mehrere NFS-Mount-Punkte oder Freigaben erstrecken
- RAW-Festplattenformat
- Andere Speicherpooltypen als NetFS (nur NetFS wird unterstützt)

Hinweise zur Fehlerbehebung

Beachten Sie Folgendes bei der Verwendung der privaten Vorschau von KVM-Workloads mit NetApp Backup and Recovery:

- Um sicherzustellen, dass die Wiederherstellung von KVM-Workloads vollständig und erfolgreich verläuft, vergewissern Sie sich, dass die Einstellung **VM-konsistenten Snapshot aktivieren** in der Schutzrichtlinie, die Sie für KVM-Backups verwenden, aktiv ist.
- Ein Speicherpool mit KVM-Hosts, die von Apache CloudStack verwaltet werden, kann nur gesichert werden, wenn alle verwalteten Hosts zu NetApp Backup and Recovery hinzugefügt werden. Als Ausweichlösung fügen Sie jeden von CloudStack verwalteten KVM-Host zu NetApp Backup and Recovery hinzu.
- Eine gestoppte VM, die zu einer Schutzgruppe gehört, kann nicht gesichert werden. Als Ausweichlösung sollte die gestoppte VM vor dem Start der Sicherung aus der Schutzgruppe entfernt werden.

Bekannte Einschränkungen mit NetApp Backup and Recovery für Oracle Database-Workloads

Plattformen, Geräte oder Funktionen, die mit dieser Version nicht oder nicht gut funktionieren, sind hier aufgelistet. Lesen Sie diese Einschränkungen sorgfältig durch.

Die folgende Aktion wird in der privaten Vorschauversion von Oracle Database-Workloads in NetApp Backup and Recovery nicht unterstützt:

- Offline-Backup

Oracle Database wird nur als eigenständige Bereitstellung mit NFS, SAN oder ASM SAN in der privaten Vorschauversion von Oracle Database-Workloads unterstützt.

Erste Schritte

Erfahren Sie mehr über NetApp Backup and Recovery

NetApp Backup and Recovery ist ein Datenservice, der effizienten, sicheren und kostengünstigen Datenschutz für alle Ihre ONTAP Workloads bietet, einschließlich Volumes, Datenbanken, virtuellen Maschinen und Kubernetes-Workloads.

Die Unterstützung für Backup und Recovery ist bereits in alle ONTAP -Systeme integriert, sodass keine zusätzliche Hardware, Softwarelizenzen oder Medien-Gateways erforderlich sind. Dadurch werden Sicherungsvorgänge einfach und kostengünstig. Die NetApp Console vereinfacht die Implementierung jeder Backup-Strategie, einschließlich des gesamten Spektrums an 3-2-1-Backup-Varianten, ohne dass mehrere Ressourcenmanager oder spezialisiertes Personal erforderlich sind.

Dokumentation zum Schutz von VMware-, KVM-, Hyper-V- und Kubernetes-Workloads wird als Technologievorschau bereitgestellt. Bei diesem Vorschauangebot behält sich NetApp das Recht vor, Angebotsdetails, Inhalte und Zeitplan vor der allgemeinen Verfügbarkeit zu ändern.

Was Sie mit NetApp Backup and Recovery tun können

Verwenden Sie NetApp Backup and Recovery, um die folgenden Ziele zu erreichen:

- * ONTAP -Volumen-Workloads*:
  - Erstellen Sie lokale Snapshots, replizieren Sie auf sekundären Speicher und sichern Sie ONTAP -Volumes von lokalen ONTAP oder Cloud Volumes ONTAP Systemen auf Objektspeicher in Ihrem öffentlichen oder privaten Cloud-Konto.
  - Erstellen Sie inkrementelle Backups auf Blockebene, die dauerhaft auf einem anderen ONTAP Cluster und im Objektspeicher in der Cloud gespeichert werden.
  - Verwenden Sie NetApp Backup and Recovery zusammen mit SnapCenter.
  - Siehe"Schützen Sie ONTAP Volumes" .
- **Microsoft SQL Server-Arbeitslasten**:
  - Sichern Sie Microsoft SQL Server-Instanzen und -Datenbanken von On-Premises ONTAP, Cloud Volumes ONTAP oder Amazon FSx for NetApp ONTAP.
  - Stellen Sie Microsoft SQL Server-Datenbanken wieder her.
  - Klonen Sie Microsoft SQL Server-Datenbanken.
  - Verwenden Sie NetApp Backup and Recovery ohne SnapCenter.
  - Siehe"Schützen Sie Microsoft SQL Server-Workloads" .
- **VMware-Workloads (Vorschau mit neuer Benutzeroberfläche ohne SnapCenter Plug-in for VMware vSphere)**:
  - Schützen Sie Ihre VMware-VMs und Datenspeicher mit NetApp Backup and Recovery.
  - Sichern Sie VMware-Workloads auf Amazon Web Services S3 oder StorageGRID (für die Vorschau).
  - Stellen Sie VMware-Daten aus der Cloud wieder im lokalen vCenter wieder her.
  - Sie können die VM an genau demselben Speicherort wiederherstellen, von dem die Sicherung erstellt wurde, oder an einem anderen Speicherort.

- Verwenden Sie NetApp Backup and Recovery ohne SnapCenter Plug-in for VMware vSphere.
- Siehe"Schutz von VMware-Workloads" .

- **VMware-Workloads (mit SnapCenter Plug-in for VMware vSphere)**:
  - Sichern Sie VMs und Datenspeicher auf Amazon Web Services S3, Microsoft Azure Blob, Google Cloud Platform und StorageGRID und stellen Sie VMs auf dem lokalen SnapCenter Plug-in for VMware vSphere Host wieder her.
  - Stellen Sie mit NetApp Backup and Recovery VM-Daten aus der Cloud zurück in das lokale vCenter wieder her. Sie können die VM an genau demselben Speicherort wiederherstellen, von dem die Sicherung erstellt wurde, oder an einem anderen Speicherort.
  - Verwenden Sie NetApp Backup and Recovery zusammen mit dem SnapCenter Plug-in for VMware vSphere.
  - Siehe"Schutz von VMware-Workloads" .
- **KVM-Workloads (Vorschau)**:
  - Sichern und Wiederherstellen virtueller Maschinen
  - KVM-Speicherpools sichern
  - Verwenden Sie Schutzgruppen, um Sicherungsaufgaben zu verwalten
  - Siehe"Schützen Sie KVM -Workloads" .
- **Hyper-V-Workloads (Vorschau)**:
  - Sichern und Wiederherstellen virtueller Maschinen
  - Verwenden Sie Schutzgruppen, um Sicherungsaufgaben zu verwalten
  - Siehe"Schützen Sie Hyper-V-Workloads" .
- **Oracle Database workloads (Vorschau)**:
  - Sichern und Wiederherstellen von Datenbanken und Protokollen
  - Verwenden Sie Schutzgruppen, um Sicherungsaufgaben zu verwalten
  - Erstellen Sie Richtlinien zum Verwalten von Datenbank- und Protokollsicherungen
  - Schutz einer Datenbank mit einer 3-2-1-Backup-Architektur
  - Konfigurieren der Sicherungsaufbewahrung
  - Mounten und Unmounten von ARCHIVELOG-Backups
  - Siehe "Oracle Database-Workloads schützen".
- **Kubernetes-Workloads (Vorschau)**:
  - Verwalten und schützen Sie Ihre Kubernetes-Anwendungen und -Ressourcen an einem Ort.
  - Verwenden Sie Schutzrichtlinien, um Ihre inkrementellen Backups zu strukturieren.
  - Stellen Sie Anwendungen und Ressourcen in denselben oder in anderen Clustern und Namespaces wieder her.
  - Verwenden Sie NetApp Backup and Recovery ohne SnapCenter.
  - Siehe"Schützen Sie Kubernetes-Workloads" .

Vorteile der Verwendung von NetApp Backup and Recovery

NetApp Backup and Recovery bietet die folgenden Vorteile:

- **Effizient**: NetApp Backup and Recovery führt eine inkrementelle Replikation auf Blockebene durch, wodurch die Menge der replizierten und gespeicherten Daten erheblich reduziert wird. Dies trägt dazu bei, den Netzwerkverkehr und die Speicherkosten zu minimieren.
- **Sicher**: NetApp Backup and Recovery verschlüsselt Daten während der Übertragung und im Ruhezustand und verwendet sichere Kommunikationsprotokolle zum Schutz Ihrer Daten.
- **Kostengünstig**: NetApp Backup and Recovery verwendet die kostengünstigsten verfügbaren Speicherebenen in Ihrem Cloud-Konto und trägt so zur Kostensenkung bei.
- **Automatisiert**: NetApp Backup and Recovery erstellt automatisch Backups basierend auf einem vordefinierten Zeitplan, wodurch sichergestellt wird, dass Ihre Daten geschützt sind.
- **Flexibel**: NetApp Backup and Recovery ermöglicht Ihnen die Wiederherstellung von Daten auf demselben oder einem anderen System, was für Flexibilität bei der Datenwiederherstellung sorgt.

Kosten

NetApp berechnet Ihnen für die Nutzung der Testversion keine Gebühren. Sie sind jedoch für die Kosten verantwortlich, die mit den von Ihnen genutzten Cloud-Ressourcen verbunden sind, beispielsweise für Speicher- und Datenübertragungskosten.

Mit der Verwendung der Backup-to-Object-Funktion von NetApp Backup and Recovery mit ONTAP Systemen sind zwei Arten von Kosten verbunden:

- Ressourcengebühren
- Servicegebühren

Für die Erstellung von Snapshots oder replizierten Volumes fallen keine Gebühren an – außer dem Speicherplatz, der zum Speichern der Snapshots und replizierten Volumes benötigt wird.

Ressourcenkosten

Für die Objektspeicherkapazität und für das Schreiben und Lesen von Sicherungsdateien in der Cloud werden Ressourcengebühren an den Cloud-Anbieter gezahlt.

- Für die Sicherung auf Objektspeicher zahlen Sie Ihrem Cloud-Anbieter die Kosten für den Objektspeicher.

  Da NetApp Backup and Recovery die Speichereffizienz des Quellvolumes beibehält, zahlen Sie dem Cloud-Anbieter die Objektspeicherkosten für die Daten *nach* der ONTAP Effizienz (für die geringere Datenmenge nach Anwendung von Deduplizierung und Komprimierung).

- Für die Wiederherstellung von Daten mit Search & Restore werden bestimmte Ressourcen von Ihrem Cloud-Anbieter bereitgestellt. Außerdem fallen Kosten pro TiB an, die sich nach der Datenmenge richten, die von Ihren Suchanfragen gescannt wird. (Diese Ressourcen werden für Browse & Restore nicht benötigt.)
  - In AWS, "Amazon Athena" Und "AWS Glue" Ressourcen werden in einem neuen S3-Bucket bereitgestellt.
  - In Azure "Azure Synapse-Arbeitsbereich" Und "Azure Data Lake-Speicher" werden in Ihrem Speicherkonto bereitgestellt, um Ihre Daten zu speichern und zu analysieren.
  - Bei Google wird ein neuer Bucket bereitgestellt und der "Google Cloud BigQuery-Dienste" werden auf Konto-/Projektebene bereitgestellt.
- Wenn Sie Volumedaten aus einer Sicherungsdatei wiederherstellen möchten, die in einen Archivobjektspeicher verschoben wurde, fällt beim Cloud-Anbieter eine zusätzliche Abrufgebühr pro GiB und pro Anforderung an.

- Wenn Sie während der Wiederherstellung von Volumedaten eine Sicherungsdatei auf Ransomware scannen möchten (wenn Sie DataLock und Ransomware Resilience für Ihre Cloud-Sicherungen aktiviert haben), entstehen Ihnen auch bei Ihrem Cloud-Anbieter zusätzliche Kosten für den ausgehenden Datenverkehr.

Servicegebühren

Bei ONTAP Volume-Workloads werden Ihnen nur die Volumes in Rechnung gestellt, die durch Objektspeicher geschützt sind. Die Gebühren basieren auf der logischen Nutzkapazität der Quell ONTAP -Volumes vor Anwendung von Effizienzmaßnahmen, auch bekannt als Front-End-Terabytes (FETB).

Für Kubernetes-Workloads werden die Gebühren basierend auf der kombinierten Größe aller persistenten Volumes berechnet.

Für alle anderen Workloads werden Ihnen Ressourcen in Rechnung gestellt, die auf mindestens einem sekundären Speicherziel oder Objektspeicherziel geschützt sind. Die Gebühren werden anhand der logischen Größe der Quell-Workload berechnet. Bei Datenbanken bedeutet dies die Datenbankgröße; bei VMs die VM-Größe.

Es gibt drei Möglichkeiten, für Backup und Wiederherstellung zu bezahlen:

- Die erste Möglichkeit besteht darin, ein Abonnement bei Ihrem Cloud-Anbieter abzuschließen, bei dem Sie monatlich zahlen können.
- Die zweite Möglichkeit besteht im Kauf eines Jahresvertrags.
- Die dritte Möglichkeit besteht darin, Lizenzen direkt von NetApp zu erwerben. Siehe die Lizenzierung Im Abschnitt finden Sie weitere Details.

Lizenzierung

NetApp Backup and Recovery bietet eine kostenlose Testversion an, mit der Sie es für eine begrenzte Zeit ohne Lizenzschlüssel nutzen können.

Eine Backup-Lizenz ist nur für Sicherungs- und Wiederherstellungsvorgänge im Zusammenhang mit Objektspeichern erforderlich. Für das Erstellen von Snapshots und replizierten Volumes ist keine Lizenz erforderlich.

Sie können zwischen drei Lizenzoptionen wählen:

- **Bring Your Own License (BYOL)**: Erwerben Sie eine laufzeitbasierte (1, 2 oder 3 Jahre) und kapazitätsbasierte (in 1-TiB-Schritten) Lizenz von NetApp. Geben Sie die angegebene Seriennummer in der NetApp Console ein, um das Gerät zu aktivieren. Die Lizenz deckt alle Quellsysteme in Ihrer Organisation ab. Eine Verlängerung ist erforderlich, wenn die Laufzeit oder die Kapazitätsgrenze erreicht ist.
- **Pay As You Go (PAYGO)**: Abonnieren Sie über den Marktplatz Ihres Cloud-Anbieters und zahlen Sie pro GiB an gesicherten Daten, die monatlich abgerechnet werden. Es ist keine Vorauszahlung erforderlich. Bei Ihrer ersten Anmeldung steht Ihnen eine 30-tägige kostenlose Testphase zur Verfügung. Weitere Informationen finden Sie unter "Nutzen Sie ein NetApp Backup and Recovery -PAYGO-Abonnement" .
- **Jahresvertrag**: Verfügbar über die AWS- und Azure-Marktplätze für 1, 2 oder 3 Jahre. Es stehen zwei Jahresverträge zur Verfügung:
  - **Cloud-Backup**: Sichert Cloud Volumes ONTAP und lokale ONTAP Daten.
  - **CVO Professional**: Bündelt Cloud Volumes ONTAP und NetApp Backup and Recovery mit unbegrenzten Backups für Cloud Volumes ONTAP -Volumes (die Backup-Kapazität wird nicht auf die

Lizenz angerechnet).

- Beim CVO Professional-Tarif gibt es zwei Arten von Gebühren:
  - **Ressourcenkosten**: Basierend auf der Speichernutzung. Weitere Informationen finden Sie unter "Lizenzierung für Cloud Volumes ONTAP" .
  - **Servicegebühren**: Gebühren für NetApp Backup and Recovery. Befindet sich das Quellvolume jedoch in einem Speichersystem, das den CVO Professional-Plan nutzt, wird NetApp Backup and Recovery kostenlos bereitgestellt.

Wenn Sie die Google Cloud Platform nutzen, fordern Sie ein individuelles Angebot von NetApp an und wählen Sie Ihren Tarif während der Aktivierung im Google Cloud Marketplace aus.

"Erfahren Sie, wie Sie Lizenzen einrichten".

Unterstützte Workloads, Systeme und Sicherungsziele

Unterstützte Arbeitslasten

NetApp Backup and Recovery schützt die folgenden Arten von Workloads:

- ONTAP -Volumes
- Microsoft SQL Server-Instanzen und -Datenbanken werden auf physischen Festplatten und VMware Virtual Machine Disks (VMDK) über VMFS oder NFS gespeichert.
- VMware-VMs und -Datenspeicher
- KVM-Workloads (Vorschau)
- Hyper-V-Workloads (Vorschau)
- Oracle Database-Workloads (Vorschau)
- Kubernetes-Workloads (Vorschau)

Unterstützte Systeme

- Lokales ONTAP SAN (iSCSI-Protokoll) und NAS (über NFS- und CIFS-Protokolle) mit ONTAP Version 9.8 oder höher
- Cloud Volumes ONTAP 9.8 oder höher für AWS (mit SAN und NAS)
- Cloud Volumes ONTAP 9.8 oder höher für Google Cloud Platform (unter Verwendung der NFS- und CIFS-Protokolle)
- Cloud Volumes ONTAP 9.8 oder höher für Microsoft Azure (mit SAN und NAS)
- Amazon FSx for NetApp ONTAP (nur Microsoft SQL Server-Workloads)

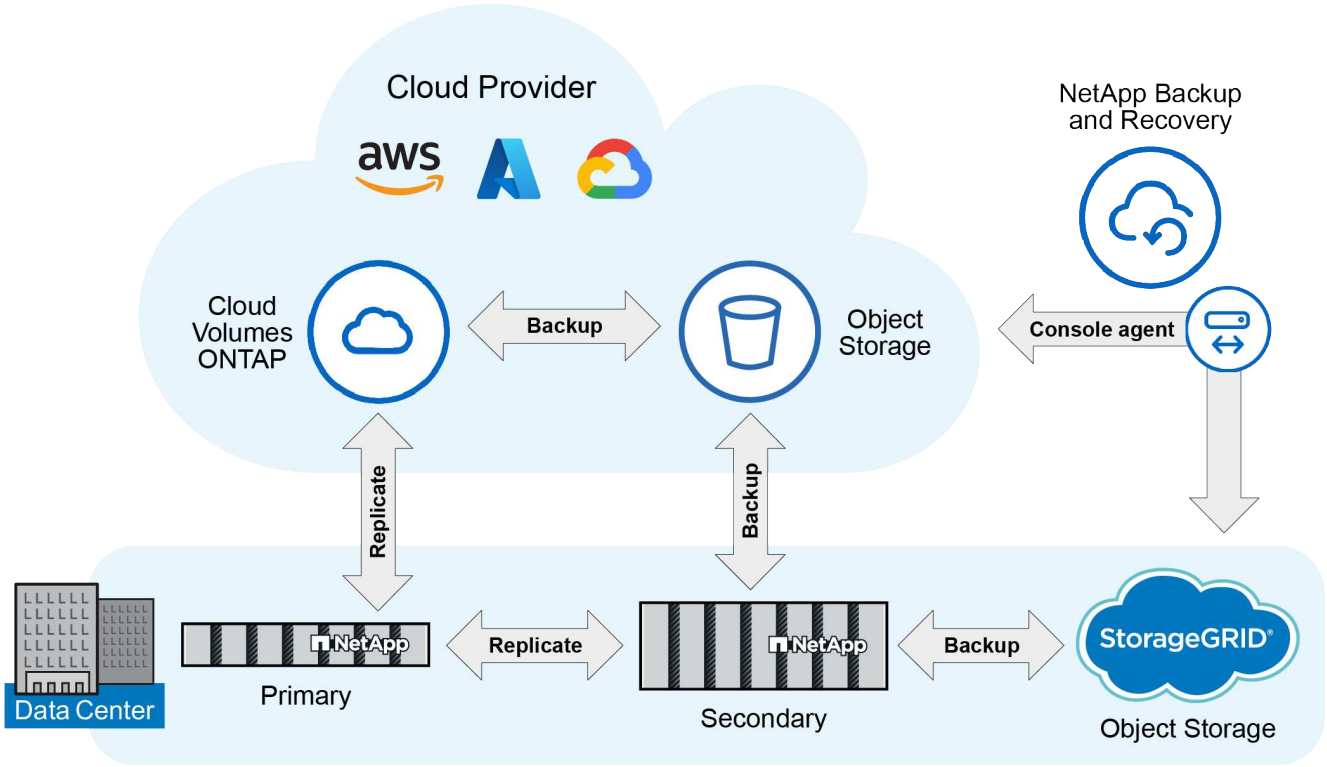
Unterstützte Sicherungsziele

- Amazon Web Services (AWS) S3
- Google Cloud-Speicher
- Microsoft Azure Blob (nicht verfügbar für VMware-Workloads in der Vorschau)
- StorageGRID
- ONTAP S3 (Nicht verfügbar für VMware-Workloads in der Vorschau)

So funktioniert NetApp Backup and Recovery

Wenn Sie NetApp Backup and Recovery aktivieren, führt der Dienst eine vollständige Sicherung Ihrer Daten durch. Nach der ersten Sicherung sind alle weiteren Sicherungen inkrementell. Dadurch wird der Netzwerkverkehr auf ein Minimum reduziert.

Das folgende Bild zeigt die Beziehung zwischen den Komponenten.



Auch die Übertragung vom Primär- zum Objektspeicher wird unterstützt, nicht nur die Übertragung vom Sekundärspeicher zum Objektspeicher.

Wo sich Backups in Objektspeicherorten befinden

Sicherungskopien werden in einem Objektspeicher gespeichert, den die NetApp Console in Ihrem Cloud-Konto erstellt. Es gibt einen Objektspeicher pro Cluster oder System und die Konsole benennt den Objektspeicher wie folgt: `netapp-backup-clusteruuid` . Denken Sie daran, diesen Objektspeicher nicht zu löschen.

- In AWS ermöglicht die NetApp Console die "Amazon S3-Funktion „Öffentlichen Zugriff blockieren“" auf dem S3-Bucket.
- In Azure verwendet die NetApp Console eine neue oder vorhandene Ressourcengruppe mit einem Speicherkonto für den Blob-Container. "blockiert den öffentlichen Zugriff auf Ihre Blob-Daten" standardmäßig.
- In StorageGRID verwendet die Konsole ein vorhandenes Speicherkonto für den Objektspeicher-Bucket.
- In ONTAP S3 verwendet die Konsole ein vorhandenes Benutzerkonto für den S3-Bucket.

Sicherungskopien sind mit Ihrer NetApp Console verknüpft

Sicherungskopien sind mit der NetApp Console verknüpft, in der sich der Konsolenagent befindet. "Erfahren Sie mehr über Identität und Zugriff auf die NetApp Console" .

Wenn Sie mehrere Konsolenagenten in derselben NetApp Console haben, zeigt jeder Konsolenagent dieselbe Liste mit Sicherungen an.

Begriffe, die Ihnen bei NetApp Backup and Recovery helfen könnten

Es kann für Sie von Vorteil sein, einige Begriffe im Zusammenhang mit dem Schutz zu verstehen.

- **Schutz**: Schutz in NetApp Backup and Recovery bedeutet, sicherzustellen, dass Snapshots und unveränderliche Backups regelmäßig mithilfe von Schutzrichtlinien in einer anderen Sicherheitsdomäne erfolgen.
- **Workload**: Ein Workload in NetApp Backup and Recovery kann ONTAP -Volumes, Microsoft SQL Server-Instanzen und -Datenbanken, VMware-VMs und -Datenspeicher oder Kubernetes-Cluster und -Anwendungen umfassen.

Voraussetzungen für NetApp Backup and Recovery

Beginnen Sie mit NetApp Backup and Recovery, indem Sie die Bereitschaft Ihrer Betriebsumgebung, NetApp Console Agenten und NetApp Console -Kontos überprüfen. Um NetApp Backup and Recovery verwenden zu können, benötigen Sie diese Voraussetzungen.

Voraussetzung für ONTAP 9.8 und höher

Auf der lokalen ONTAP Instanz muss eine ONTAP One-Lizenz aktiviert sein.

Voraussetzungen für Backups im Objektspeicher

Um Objektspeicher als Sicherungsziele zu verwenden, benötigen Sie ein Konto bei AWS S3, Microsoft Azure Blob, StorageGRID oder ONTAP und die entsprechenden Zugriffsberechtigungen.

- "Schützen Sie Ihre ONTAP Volume-Daten"

Anforderungen zum Schutz von Microsoft SQL Server-Workloads

Um NetApp Backup and Recovery für Microsoft SQL Server-Workloads zu verwenden, benötigen Sie die folgenden Voraussetzungen hinsichtlich Hostsystem, Speicherplatz und Größe.

Artikel	Anforderungen
Betriebssysteme	Microsoft Windows: Aktuelle Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .
Microsoft SQL Server-Versionen	Version 2012 und höher werden für VMware Virtual Machine File System (VMFS) und VMware Virtual Machine Disk (VMDK) NFS unterstützt.

Artikel	Anforderungen
SnapCenter Server-Version	Wenn Sie Ihre vorhandenen Daten aus SnapCenter in NetApp Backup and Recovery importieren möchten, ist SnapCenter Server Version 5.0 oder höher erforderlich. Wenn Sie bereits über SnapCenter verfügen, überprüfen Sie zunächst, ob Sie die Voraussetzungen erfüllt haben, bevor Sie aus SnapCenter importieren. Sehen"Voraussetzungen für den Import von Ressourcen aus SnapCenter" .
Mindest-RAM für das Plug-In auf dem SQL Server-Host	1 GB
Minimaler Installations- und Protokollspeicherplatz für das Plug-In auf dem SQL Server-Host	5 GB Weisen Sie ausreichend Speicherplatz zu und überwachen Sie den Speicherverbrauch des Protokollordners. Der erforderliche Protokollspeicherplatz variiert je nach Anzahl der durchgeführten Sicherungen und der Häufigkeit der Datenschutzvorgänge. Wenn nicht genügend Speicherplatz vorhanden ist, werden die Protokolle für die Vorgänge nicht erstellt.
Erforderliche Softwarepakete	• ASP.NET Core Runtime 8.0.12 Hosting Bundle (und alle nachfolgenden 8.0.x-Patches) • PowerShell 7.4.2 Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Anforderungen zum Schutz von VMware-Workloads

Sie benötigen bestimmte Anforderungen, um Ihre VMware-Workloads zu erkennen und zu schützen.

Softwareunterstützung

- NFS und VMFS-Datenspeicher werden unterstützt.
- Unterstützte NFS-Versionen: NFS 3 und NFS 4.1
- Unterstützte VMware ESXi Server-Versionen: 7.0U1 und höher
- Unterstützte VMware vCenter vSphere-Versionen: 7.0U1 und höher
- IP-Adressen: IPv4 und IPv6
- VMware TLS: 1.2, 1.3
- Unterstützter verbundener Speicher: ONTAP 9.13 oder höher

Verbindungs- und Portanforderungen zum Schutz von VMware-Workloads

Art des Anschlusses	Vorkonfigurierter Port
VMware ESXi-Server-Port	443 (HTTPS), bidirektional. Die Funktion „Gastdateiwiederherstellung“ verwendet diesen Port.
Speichercluster oder Speicher-VM-Port	443 (HTTPS), bidirektional. 80 (HTTP), bidirektional. Dieser Port wird für die Kommunikation zwischen der virtuellen Appliance und der Speicher-VM oder dem Cluster verwendet, der die Speicher-VM enthält.

Anforderungen an die rollenbasierte Zugriffskontrolle (RBAC) zum Schutz von VMware-Workloads

Das vCenter-Administratorkonto muss über die erforderlichen vCenter-Berechtigungen verfügen.

Eine Liste der erforderlichen vCenter-Berechtigungen finden Sie unter "SnapCenter Plug-in for VMware vSphere vCenter-Berechtigungen erforderlich" .

Anforderungen zum Schutz von KVM-Workloads

Sie benötigen bestimmte Anforderungen, um virtuelle KVM-Maschinen zu erkennen und zu schützen.

- Eine moderne Linux-Distribution mit Kernelversion 5.14.0-503.22.1.el9_5.x86_64 (longterm) oder höher
- Ihre KVM-Hosts und VMs müssen über eine Managementplattform verwaltet werden. NetApp Backup and Recovery unterstützt die folgenden Managementplattformen:
  - Apache CloudStack 4.22.0.0
- Stellen Sie sicher, dass eingehender Netzwerkverkehr von der Konsolenagentur zum KVM-Host an Port 22 zugelassen ist.
- QEMU-Gastagent Version 9.0.0 oder höher
- libvirt Version 10.5.0 oder höher

Um sicherzustellen, dass die Wiederherstellung von KVM-Workloads vollständig und erfolgreich verläuft, vergewissern Sie sich, dass die Einstellung **VM-konsistenten Snapshot aktivieren** in der Schutzrichtlinie, die Sie für KVM-Backups verwenden, aktiv ist.

Um den Schutz von KVM-VMs zu aktivieren, die von Benutzern ohne Root-Rechte verwaltet werden, führen Sie die folgenden Schritte aus:

1. Binden Sie das Volume als NFS3 ein, um die Verwendung von `nobody` Benutzer und Gruppe.
2. Verwenden Sie den folgenden Befehl, um einen Nicht-Root-Benutzer hinzuzufügen `qemu` Gruppen bilden und gleichzeitig ihre bestehenden Gruppen erhalten:

```
usermod -aG qemu <non-root-user>
```

3. Verwenden Sie den folgenden Befehl, um die Besitzrechte am Mount-Pfad zu übertragen. `qemu` Benutzer- und Gruppenberechtigungen für den Mount-Pfad ändern:

```
chown -R qemu:qemu <kvm_vm_mount_path> & chmod 771
<kvm_vm_mount_path>
```

4. Löschen Sie gegebenenfalls das vorhandene Verzeichnis NetApp_SnapCenter_Backups.

Anforderungen für den Schutz von Oracle Database Workloads

Stellen Sie sicher, dass Ihre Umgebung bestimmte Anforderungen zum Erkennen und Schützen von Oracle-Ressourcen erfüllt.

- Oracle-Datenbank:
  - Oracle 19C und 21C werden in einer eigenständigen Bereitstellung unterstützt.
  - Oracle Database muss im primären oder sekundären NetApp ONTAP Speicher bereitgestellt werden.
  - Host-OS-Unterstützung: Red Hat Enterprise Linux 8 und 9
- Objektspeicherunterstützung:
  - Azure-Objektspeicher
  - Amazon AWS
  - NetApp StorageGRID
  - ONTAP S3

Anforderungen zum Schutz von Kubernetes-Anwendungen

Sie benötigen spezifische Anforderungen, um Kubernetes-Ressourcen zu erkennen und Ihre Kubernetes-Anwendungen zu schützen.

Informationen zu den NetApp Console finden Sie unterIn der NetApp Console .

- Ein primäres ONTAP System (ONTAP 9.16.1 oder höher)
- Ein Kubernetes-Cluster – Zu den unterstützten Kubernetes-Distributionen und -Versionen gehören:
  - Anthos On-Prem (VMware) und Anthos auf Bare Metal 1.16
  - Kubernetes 1.27 – 1.33

- OpenShift 4.10 – 4.18
- Rancher Kubernetes Engine 2 (RKE2) v1.26.7+rke2r1, v1.28.5+rke2r1
- Suse Rancher

- NetApp Trident 24.10 oder höher
- NetApp Trident Protect 25.07 oder später (installiert während der Kubernetes-Workload-Erkennung)
- NetApp Trident Protect Connector 25.07 or later (wird während der Kubernetes-Workload-Erkennung installiert)
  - Stellen Sie sicher, dass TCP-Port 443 in ausgehender Richtung zwischen dem Kubernetes-Cluster, dem Trident Protect Connector und dem Trident Protect Proxy ungefiltert ist.

Anforderungen zum Schutz von Hyper-V-Workloads

Stellen Sie sicher, dass Ihre Hyper-V-Instanz bestimmte Anforderungen zum Erkennen und Schützen virtueller Maschinen erfüllt.

- Softwareanforderungen für den Hyper-V Windows Server-Host:
  - Microsoft Hyper-V 2019, 2022 und 2025 Editionen
  - ASP.NET Core Runtime 8.0.12 Hosting Bundle (und alle nachfolgenden 8.0.x-Patches)
  - PowerShell 7.4.2 oder höher
  - Wenn Benutzer, die nicht Teil einer Administratordomäne sind, Hyper-V-VMs schützen sollen, stellen Sie sicher, dass der Benutzer über die folgenden Berechtigungen verfügt:
    - Stellen Sie sicher, dass der Benutzer Mitglied der lokalen Administratorgruppe ist.
    - Stellen Sie sicher, dass der Benutzer Teil der lokalen Sicherheitsrichtlinie „Anmelden als Dienst“ ist.
  - Stellen Sie sicher, dass in den Windows-Firewall-Einstellungen bidirektionaler HTTPS-Verkehr für die folgenden Ports zugelassen ist:
    - 8144 (NetApp -Plugin für Hyper-V)
    - 8145 (NetApp -Plugin für Windows)
- Hardwareanforderungen für den Hyper-V-Host:
  - Standalone- und FCI-Cluster-Hosts werden unterstützt
  - Mindestens 1 GB RAM für das NetApp Hyper-V-Plug-In auf dem Hyper-V-Host
  - Mindestens 5 GB Installations- und Protokollspeicherplatz für das Plug-In auf dem Hyper-V-Host

> Stellen Sie sicher, dass Sie auf dem Hyper-V-Host genügend Speicherplatz für den Protokollordner zuweisen und dessen Nutzung regelmäßig überwachen. Der erforderliche Speicherplatz hängt davon ab, wie oft Backups und Datenschutzvorgänge durchgeführt werden. Wenn nicht genügend Speicherplatz vorhanden ist, werden keine Protokolle erstellt.

- NetApp ONTAP Konfigurationsanforderungen:
  - Ein primäres ONTAP System (ONTAP 9.14.1 oder höher)
  - Stellen Sie bei Hyper-V-Bereitstellungen, die CIFS-Freigaben zum Speichern von Daten virtueller Maschinen verwenden, sicher, dass die Eigenschaft „Continuous Availability Share“ auf dem ONTAP System aktiviert ist. Weitere Informationen finden Sie im "ONTAP-Dokumentation" Anweisungen hierzu finden Sie unter.

In der NetApp Console

Stellen Sie sicher, dass die NetApp Console die folgenden Anforderungen erfüllt.

- Ein Konsolenbenutzer sollte über die erforderliche Rolle und die erforderlichen Berechtigungen verfügen, um Vorgänge an Microsoft SQL Server- und Kubernetes-Workloads auszuführen. Um die Ressourcen zu erkennen, müssen Sie über die NetApp Backup and Recovery -Rolle des Superadministrators verfügen. Sehen"Rollenbasierter Zugriff auf Funktionen von NetApp Backup and Recovery" Weitere Informationen zu den Rollen und Berechtigungen, die zum Ausführen von Vorgängen in NetApp Backup and Recovery erforderlich sind.
- Eine Konsolenorganisation mit mindestens einem aktiven Konsolenagenten, der eine Verbindung zu lokalen ONTAP Clustern oder Cloud Volumes ONTAP.
- Mindestens ein Konsolensystem mit einem lokalen NetApp ONTAP oder Cloud Volumes ONTAP Cluster.
- Ein Konsolenagent

  Siehe "Erfahren Sie, wie Sie einen Konsolenagenten konfigurieren" Und "Standardanforderungen für die NetApp Console" .

  - Die Vorschauversion erfordert das Betriebssystem Ubuntu 22.04 LTS für den Konsolenagenten.

Einrichten der NetApp Console

Der nächste Schritt besteht darin, die Konsole und NetApp Backup and Recovery einzurichten.

Rezension "Standardanforderungen für die NetApp Console" .

Erstellen eines Konsolenagenten

Sie sollten sich an Ihr NetApp -Produktteam wenden, um Backup und Recovery auszuprobieren. Wenn Sie dann den Konsolenagenten verwenden, enthält dieser die entsprechenden Funktionen für den Dienst.

Informationen zum Erstellen eines Konsolenagenten in der NetApp Console vor der Verwendung des Dienstes finden Sie in der Konsolendokumentation. Dort wird beschrieben, "So erstellen Sie einen Konsolenagenten" .

Wo soll der Konsolenagent installiert werden?

Um einen Wiederherstellungsvorgang abzuschließen, kann der Konsolenagent an den folgenden Speicherorten installiert werden:

- Für Amazon S3 kann der Konsolenagent bei Ihnen vor Ort bereitgestellt werden.
- Für Azure Blob kann der Konsolen-Agent vor Ort bereitgestellt werden.
- Für StorageGRID muss der Konsolenagent in Ihren Räumlichkeiten bereitgestellt werden, mit oder ohne Internetzugang.
- Für ONTAP S3 kann der Konsolenagent in Ihren Räumlichkeiten (mit oder ohne Internetzugang) oder in einer Cloud-Provider-Umgebung bereitgestellt werden

Verweise auf „On-Premises ONTAP -Systeme“ umfassen FAS und AFF Systeme.

Einrichten der Lizenzierung für NetApp Backup and Recovery

Sie können NetApp Backup and Recovery lizenzieren, indem Sie bei Ihrem Cloud-Anbieter ein Pay-as-you-go-Abonnement (PAYGO) oder ein jährliches Marktplatz-Abonnement für * NetApp Intelligent Services* erwerben oder eine Bring-Your-Own-License (BYOL) von NetApp erwerben. Um NetApp Backup and Recovery auf einem System zu aktivieren, Backups Ihrer Produktionsdaten zu erstellen und Backup-Daten auf einem Produktionssystem wiederherzustellen, ist eine gültige Lizenz erforderlich.

Ein paar Anmerkungen, bevor Sie weiterlesen:

- Wenn Sie im Marktplatz Ihres Cloud-Anbieters bereits das Pay-as-you-go-Abonnement (PAYGO) für ein Cloud Volumes ONTAP System abonniert haben, sind Sie automatisch auch für NetApp Backup and Recovery angemeldet. Sie müssen sich nicht erneut anmelden.
- Die Bring-Your-Own-License (BYOL) von NetApp Backup and Recovery ist eine Floating-Lizenz, die Sie auf allen Systemen verwenden können, die mit Ihrer NetApp Console -Organisation oder Ihrem NetApp Console-Konto verknüpft sind. Wenn Ihnen also durch eine vorhandene BYOL-Lizenz ausreichend Sicherungskapazität zur Verfügung steht, müssen Sie keine weitere BYOL-Lizenz erwerben.
- Wenn Sie eine BYOL-Lizenz verwenden, wird empfohlen, dass Sie auch ein PAYGO-Abonnement abschließen. Wenn Sie mehr Daten sichern, als Ihre BYOL-Lizenz zulässt, oder wenn die Laufzeit Ihrer Lizenz abläuft, wird die Sicherung über Ihr Pay-as-you-go-Abonnement fortgesetzt – es kommt zu keiner Dienstunterbrechung.
- Wenn Sie lokale ONTAP Daten auf StorageGRID sichern, benötigen Sie eine BYOL-Lizenz, für den Speicherplatz des Cloud-Anbieters fallen jedoch keine Kosten an.

"Erfahren Sie mehr über die Kosten im Zusammenhang mit der Verwendung von NetApp Backup and Recovery."

30 Tage kostenlos testen

Eine kostenlose 30-Tage-Testversion von NetApp Backup and Recovery ist verfügbar, wenn Sie sich im Marktplatz Ihres Cloud-Anbieters für ein Pay-as-you-go-Abonnement für * NetApp Intelligent Services* anmelden. Die kostenlose Testversion beginnt mit der Anmeldung zum Marktplatzeintrag. Beachten Sie: Wenn Sie beim Bereitstellen eines Cloud Volumes ONTAP -Systems für das Marktplatzabonnement bezahlen und dann 10 Tage später Ihre kostenlose Testversion von NetApp Backup and Recovery starten, haben Sie noch 20 Tage Zeit, die kostenlose Testversion zu nutzen.

Nach Ablauf der kostenlosen Testphase erfolgt die Umstellung automatisch und ohne Unterbrechung auf das PAYGO-Abo. Wenn Sie sich entscheiden, NetApp Backup and Recovery nicht weiter zu verwenden,"Aufheben der Registrierung von NetApp Backup and Recovery vom System" bevor die Testphase endet, und es entstehen Ihnen keine Kosten.

Kostenlose Testversion beenden

Wenn Sie NetApp Backup and Recovery nach Ablauf der kostenlosen Testversion weiterhin verwenden möchten, müssen Sie ein kostenpflichtiges Abonnement einrichten. Sie können dies über die NetApp Console tun, indem Sie zum Abschnitt „Abrechnung“ navigieren und einen Abonnementplan auswählen, der Ihren Anforderungen entspricht. Wenn Sie NetApp Backup and Recovery nicht weiter verwenden möchten, können Sie die kostenlose Testversion beenden.

Wenn Sie die kostenlose Testversion beenden, ohne einen kostenpflichtigen Plan zu abonnieren, werden Ihre Daten 60 Tage nach Ablauf der kostenlosen Testversion automatisch gelöscht. Optional können Sie Ihre Daten auch sofort vom System löschen lassen.

Schritte

1. Wählen Sie auf der Zielseite von NetApp Backup and Recovery **Kostenlose Testversion anzeigen** aus.
2. Wählen Sie **Kostenlose Testversion beenden**.
3. Wählen Sie **Daten sofort nach Beendigung meiner kostenlosen Testversion löschen**, um Ihre Daten sofort zu löschen.
4. Geben Sie **Testversion beenden** in das Feld ein.
5. Wählen Sie zur Bestätigung **Ende**.

Verwenden Sie ein NetApp Backup and Recovery PAYGO-Abonnement

Beim Pay-as-you-go-Modell zahlen Sie Ihrem Cloud-Anbieter die Kosten für die Objektspeicherung und die Lizenzkosten für das NetApp -Backup auf Stundenbasis in einem einzigen Abonnement. Sie sollten * NetApp Intelligent Services* im Marketplace abonnieren, auch wenn Sie über eine kostenlose Testversion verfügen oder Ihre eigene Lizenz mitbringen (BYOL):

- Durch das Abonnement wird sichergestellt, dass es nach Ablauf Ihrer kostenlosen Testversion zu keiner Dienstunterbrechung kommt. Nach Ablauf der Testphase werden Ihnen stündlich Gebühren entsprechend der Menge der von Ihnen gesicherten Daten berechnet.
- Wenn Sie mehr Daten sichern, als Ihre BYOL-Lizenz zulässt, werden die Datensicherungs- und Wiederherstellungsvorgänge über Ihr Pay-as-you-go-Abonnement fortgesetzt. Wenn Sie beispielsweise über eine BYOL-Lizenz mit 10 TiB verfügen, wird die gesamte Kapazität über 10 TiB hinaus über das PAYGO-Abonnement abgerechnet.

Während Ihrer kostenlosen Testphase oder wenn Sie Ihre BYOL-Lizenz nicht überschritten haben, werden Ihnen keine Kosten für Ihr Pay-as-you-go-Abonnement in Rechnung gestellt.

Es gibt einige PAYGO-Pläne für NetApp Backup and Recovery:

- Ein „Cloud Backup“-Paket, mit dem Sie Cloud Volumes ONTAP Daten und lokale ONTAP -Daten sichern können.
- Ein „CVO Professional“-Paket, mit dem Sie Cloud Volumes ONTAP und NetApp Backup and Recovery bündeln können. Dies beinhaltet unbegrenzte Backups für das Cloud Volumes ONTAP System unter Verwendung der Lizenz (die Backup-Kapazität wird nicht auf die lizenzierte Kapazität angerechnet). Mit dieser Option können Sie keine lokalen ONTAP -Daten sichern.

  Beachten Sie, dass für diese Option auch ein PAYGO-Abonnement für Backup und Wiederherstellung erforderlich ist, für berechtigte Cloud Volumes ONTAP Systeme jedoch keine Gebühren anfallen.

"Erfahren Sie mehr über diese kapazitätsbasierten Lizenzpakete".

Verwenden Sie diese Links, um NetApp Backup and Recovery über den Marktplatz Ihres Cloud-Anbieters zu abonnieren:

- AWS: "Preisdetails finden Sie im Marketplace-Angebot für NetApp Intelligent Services." Die
- Azurblau: "Preisdetails finden Sie im Marketplace-Angebot für NetApp Intelligent Services." Die
- Google Cloud: "Preisdetails finden Sie im Marketplace-Angebot für NetApp Intelligent Services." Die

Verwenden Sie einen Jahresvertrag

Bezahlen Sie jährlich für NetApp Backup and Recovery , indem Sie einen Jahresvertrag abschließen. Sie sind mit einer Laufzeit von 1, 2 oder 3 Jahren erhältlich.

Wenn Sie einen Jahresvertrag von einem Marktplatz haben, wird der gesamte Verbrauch von NetApp Backup and Recovery über diesen Vertrag abgerechnet. Sie können einen jährlichen Marktplatzvertrag nicht mit einem BYOL kombinieren.

Wenn Sie AWS verwenden, stehen Ihnen zwei Jahresverträge zur Verfügung: "AWS Marketplace-Seite" für Cloud Volumes ONTAP und lokale ONTAP Systeme:

- Ein „Cloud Backup“-Plan, mit dem Sie Cloud Volumes ONTAP -Daten und lokale ONTAP -Daten sichern können.

  Wenn Sie diese Option nutzen möchten, richten Sie Ihr Abonnement auf der Marketplace-Seite ein und dann "Verknüpfen Sie das Abonnement mit Ihren AWS-Anmeldeinformationen" . Beachten Sie, dass Sie mit diesem Jahresvertragsabonnement auch für Ihre Cloud Volumes ONTAP -Systeme bezahlen müssen, da Sie Ihren AWS-Anmeldeinformationen in der Konsole nur ein aktives Abonnement zuweisen können.

- Ein „CVO Professional“-Plan, der es Ihnen ermöglicht, Cloud Volumes ONTAP und NetApp Backup and Recovery zu bündeln. Dies beinhaltet unbegrenzte Backups für das Cloud Volumes ONTAP System unter Verwendung der Lizenz (die Backup-Kapazität wird nicht auf die lizenzierte Kapazität angerechnet). Mit dieser Option können Sie keine lokalen ONTAP -Daten sichern.

  Siehe die "Thema zur Lizenzierung von Cloud Volumes ONTAP" um mehr über diese Lizenzierungsoption zu erfahren.

  Wenn Sie diese Option nutzen möchten, können Sie den Jahresvertrag einrichten, wenn Sie ein Cloud Volumes ONTAP -System erstellen. Die Konsole fordert Sie dann auf, den AWS Marketplace zu abonnieren.

Wenn Sie Azure verwenden, stehen Ihnen zwei Jahresverträge zur Verfügung von "Azure Marketplace-Seite" für Cloud Volumes ONTAP und lokale ONTAP Systeme:

- Ein „Cloud Backup“-Plan, mit dem Sie Cloud Volumes ONTAP -Daten und lokale ONTAP -Daten sichern können.

  Wenn Sie diese Option nutzen möchten, richten Sie Ihr Abonnement auf der Marketplace-Seite ein und dann "Verknüpfen Sie das Abonnement mit Ihren Azure-Anmeldeinformationen" . Beachten Sie, dass Sie mit diesem Jahresvertragsabonnement auch für Ihre Cloud Volumes ONTAP -Systeme bezahlen müssen, da Sie Ihren Azure-Anmeldeinformationen in der Konsole nur ein aktives Abonnement zuweisen können.

- Ein „CVO Professional“-Plan, der es Ihnen ermöglicht, Cloud Volumes ONTAP und NetApp Backup and Recovery zu bündeln. Dies beinhaltet unbegrenzte Backups für das Cloud Volumes ONTAP System unter Verwendung der Lizenz (die Backup-Kapazität wird nicht auf die lizenzierte Kapazität angerechnet). Mit dieser Option können Sie keine lokalen ONTAP -Daten sichern.

  Siehe die "Thema zur Lizenzierung von Cloud Volumes ONTAP" um mehr über diese Lizenzierungsoption zu erfahren.

  Wenn Sie diese Option nutzen möchten, können Sie den Jahresvertrag einrichten, wenn Sie ein Cloud Volumes ONTAP -System erstellen und die Konsole Sie auffordert, den Azure Marketplace zu abonnieren.

Wenn Sie GCP verwenden, wenden Sie sich an Ihren NetApp Vertriebsmitarbeiter, um einen Jahresvertrag abzuschließen. Der Vertrag ist als privates Angebot im Google Cloud Marketplace verfügbar.

Nachdem NetApp Ihnen das private Angebot mitgeteilt hat, können Sie den Jahresplan auswählen, wenn Sie sich während der Aktivierung von NetApp Backup and Recovery über den Google Cloud Marketplace anmelden.

Verwenden Sie eine NetApp Backup and Recovery BYOL-Lizenz

Bring-Your-Own-Lizenzen von NetApp haben eine Laufzeit von 1, 2 oder 3 Jahren. Sie zahlen nur für die Daten, die Sie schützen, berechnet anhand der logisch genutzten Kapazität (*vor* jeglicher Effizienz) der Quell-ONTAP -Volumes, die gesichert werden. Diese Kapazität wird auch als Front-End-Terabyte (FETB) bezeichnet.

Bei der BYOL NetApp Backup and Recovery -Lizenz handelt es sich um eine Floating-Lizenz, bei der die Gesamtkapazität auf alle Systeme aufgeteilt wird, die mit Ihrer NetApp Console -Organisation oder Ihrem NetApp Console-Konto verknüpft sind. Für ONTAP -Systeme können Sie eine grobe Schätzung der benötigten Kapazität erhalten, indem Sie den CLI-Befehl ausführen `volume show -fields logical-used-by-afs` für die Volumes, die Sie sichern möchten.

Wenn Sie keine NetApp Backup and Recovery BYOL-Lizenz haben, klicken Sie auf das Chat-Symbol unten rechts in der Konsole, um eine zu erwerben.

Wenn Sie über eine nicht zugewiesene knotenbasierte Lizenz für Cloud Volumes ONTAP verfügen, die Sie nicht verwenden, können Sie diese optional in eine NetApp Backup and Recovery -Lizenz mit demselben Dollaräquivalent und demselben Ablaufdatum umwandeln. "Hier finden Sie weitere Einzelheiten" .

Sie verwenden die NetApp Console , um BYOL-Lizenzen zu verwalten. Sie können neue Lizenzen hinzufügen, vorhandene Lizenzen aktualisieren und den Lizenzstatus über die Konsole anzeigen.

"Informationen zum Hinzufügen von Lizenzen".

Überschreitung der Lizenzkapazität

Wenn Sie Ihr lizenziertes Speicherkontingent überschreiten, fallen PAYGO-Gebühren an; ohne ein PAYGO-Abonnement können Sie keine neuen Backups erstellen, bestehende Backups bleiben jedoch ohne Servicegarantie wiederherstellbar. Erneuern Sie Ihre Lizenz unbedingt, bevor sie abläuft; eine abgelaufene Lizenz verhindert neue Backups und unterbricht den Service.

Einrichten von Sicherheitszertifikaten für StorageGRID und ONTAP in NetApp Backup and Recovery

Erstellen Sie ein Sicherheitszertifikat, um die Kommunikation zwischen NetApp Backup and Recovery und StorageGRID oder ONTAP zu ermöglichen.

Erstellen Sie ein Sicherheitszertifikat für StorageGRID

Wenn die Kommunikation zwischen NetApp Backup and Recovery Containern und StorageGRID das StorageGRID -Zertifikat überprüfen soll, führen Sie die folgenden Schritte aus.

Das generierte Zertifikat sollte CN und Subject Alternative Name als den Namen enthalten, der in NetApp Backup and Recovery angegeben wurde, als Sie die Sicherung aktiviert haben.

Schritte

1. Befolgen Sie die Schritte in der StorageGRID -Dokumentation, um das StorageGRID -Zertifikat zu erstellen.

   "StorageGRID Informationen zum Konfigurieren von Zertifikaten"

2. Aktualisieren Sie StorageGRID mit dem Zertifikat, falls Sie dies noch nicht getan haben.
3. Melden Sie sich als Root-Benutzer beim Konsolenagenten an. Laufen:

   ```
   sudo su
   ```

4. Holen Sie sich das Docker-Volume von NetApp Backup and Recovery (Cloud Backup Service). Laufen:

   ```
   docker volume ls | grep cbs
   ```

   Ausgabebeispiel:

   ```
   local service-manager-2_cloudmanager_cbs_volume"
   ```

   Der Volumename ist in den Bereitstellungsmodi „Standard“, „Privat“ und „Eingeschränkt“ unterschiedlich. In diesem Beispiel wird der Standardmodus verwendet. Siehe "Bereitstellungsmodi der NetApp Console" .

5. Suchen Sie den Einhängepunkt des NetApp Backup and Recovery -Volumes. Laufen:

   ```
   docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep
   Mountpoint
   ```

   Ausgabebeispiel:

   ```
   "Mountpoint": "/var/lib/docker/volumes/service-manager-
   2_cloudmanager_cbs_volume/_data"
   ```

   Der Einhängepunkt ist in den Bereitstellungsmodi „Standard“, „Privat“ und „Eingeschränkt“ unterschiedlich. Dieses Beispiel zeigt eine Standard-Cloud-Bereitstellung. Siehe "Bereitstellungsmodi der NetApp Console" .

6. Wechseln Sie in das MountPoint-Verzeichnis. Laufen:

   ```
   cd /var/lib/docker/volumes/service-manager-
   2_cloudmanager_cbs_volume/_data
   ```

7. Wenn das Zertifikat von StorageGRID von der Stammzertifizierungsstelle und einer

Zwischenzertifizierungsstelle signiert ist, fügen Sie die `pem` Dateien von beiden in eine Datei mit dem Namen `sgws.crt` am aktuellen Standort. Fügen Sie das Blattzertifikat nicht zu dieser Datei hinzu.

Schritte für den Cloudmanager_CBS-Container

Sie müssen die StorageGRID -Server-Zertifikatsüberprüfung in NetApp Backup and Recovery (Cloud Backup Service) aktivieren.

1. Wechseln Sie zum Verzeichnis des Docker-Volumes, das Sie in den vorherigen Schritten erhalten haben.

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Wechseln Sie in das Konfigurationsverzeichnis.

```
cd cbs_config
```

3. Erstellen und speichern Sie eine Konfigurationsdatei wie unten gezeigt mit einem der folgenden Namen, basierend auf Ihrer Bereitstellungsumgebung:

   - `production-customer.json`Wird für Bereitstellungen im Standardmodus und eingeschränkten Modus verwendet.
   - `darksite-customer.json`Wird für Bereitstellungen im privaten Modus verwendet.

   Siehe "Bereitstellungsmodi der NetApp Console" .

   Konfigurationsdatei

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  }
}
```

4. Verlassen Sie den Container. Laufen:

```
exit
```

5. Neustart `cloudmanager_cbs` . Laufen:

```
docker restart cloudmanager_cbs
```

Schritte für den Container „cloudmanager_cbs_catalog“

Als Nächstes müssen Sie die StorageGRID -Server-Zertifikatsüberprüfung für den Katalogisierungsdienst aktivieren.

1. Wechseln Sie zum Docker-Volume:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Konfigurieren Sie den Katalog. Laufen:

```
cd cbs_catalog_config
```

3. Erstellen Sie eine Konfigurationsdatei wie unten gezeigt mit einem der folgenden Namen, basierend auf Ihrer Bereitstellungsumgebung:

   - `production-customer.json`Wird für Bereitstellungen im Standardmodus und eingeschränkten Modus verwendet.
   - `darksite-customer.json`Wird für Bereitstellungen im privaten Modus verwendet.

   Siehe "Bereitstellungsmodi der NetApp Console" .

   Katalogkonfigurationsdatei

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  }
}
```

4. Starten Sie den Katalog neu. Laufen:

```
docker restart cloudmanager_cbs_catalog
```

Aktualisieren Sie das Konsolen-Agent-Zertifikat mit dem StorageGRID -Zertifikat basierend auf dem Agent-Betriebssystem

Ubuntu

1. Kopieren Sie das SGWS-Zertifikat nach `/usr/local/share/ca-certificates` . Hier ist ein Beispiel:

```
cp /config/sgws.crt /usr/local/share/ca-certificates/
```

   Wo `sgws.crt` ist das Stamm-CA-Zertifikat.

2. Aktualisieren Sie die Hostzertifikate mit dem StorageGRID -Zertifikat. Laufen

```
sudo update-ca-certificates
```

Red Hat Enterprise Linux

1. Kopieren Sie das SGWS-Zertifikat nach `/etc/pki/ca-trust/source/anchors/` .

```
cp /config/sgws.crt /etc/pki/ca-trust/source/anchors/
```

   Wo `sgws.crt` ist das Stamm-CA-Zertifikat.

2. Aktualisieren Sie die Hostzertifikate mit dem StorageGRID -Zertifikat.

```
update-ca-trust extract
```

3. Aktualisieren Sie die `ca-bundle.crt`

```
cd /etc/pki/tls/certs/
openssl x509 -in ca-bundle.crt -text -noout
```

4. Um zu überprüfen, ob die Zertifikate vorhanden sind, führen Sie den folgenden Befehl aus:

```
openssl crl2pkcs7 -nocrl -certfile /etc/pki/tls/certs/ca-bundle.crt |
openssl pkcs7 -print_certs | grep subject | head
```

Erstellen Sie ein Sicherheitszertifikat für ONTAP

Wenn die Kommunikation zwischen den NetApp Backup and Recovery -Containern und ONTAP das ONTAP -Zertifikat validieren soll, führen Sie die folgenden Schritte aus.

NetApp Backup and Recovery verwendet die Cluster Management IP, um eine Verbindung mit ONTAP herzustellen. Geben Sie die IP-Adresse des Clusters in die alternativen Betreffnamen des Zertifikats ein. Geben Sie diesen Schritt an, wenn Sie die CSR mithilfe der System Manager-Benutzeroberfläche generieren.

Verwenden Sie die System Manager-Dokumentation, um ein neues CA-Zertifikat für ONTAP zu erstellen.

- "Zertifikate mit System Manager verwalten"
- "So verwalten Sie ONTAP SSL-Zertifikate mit System Manager"

Schritte

1. Melden Sie sich als Root beim Konsolenagenten an. Laufen:

```
sudo su
```

2. Holen Sie sich das Docker-Volume für NetApp Backup and Recovery . Laufen:

```
docker volume ls | grep cbs
```

Ausgabebeispiel:

```
local service-manager-2_cloudmanager_cbs_volume
```

Der Volumename ist in den Bereitstellungsmodi „Standard“, „Privat“ und „Eingeschränkt“ unterschiedlich. Dieses Beispiel zeigt eine Standard-Cloud-Bereitstellung. Siehe "Bereitstellungsmodi der NetApp Console" .

3. Besorgen Sie sich die Halterung für das Volume. Laufen:

```
docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep
Mountpoint
```

Ausgabebeispiel:

```
"Mountpoint": "/var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

Der Einhängepunkt ist in den Bereitstellungsmodi „Standard“, „Privat“ und „Eingeschränkt“ unterschiedlich. Dieses Beispiel zeigt eine Standard-Cloud-Bereitstellung. Siehe "Bereitstellungsmodi der NetApp Console" .

4. Wechseln Sie in das Mountpoint-Verzeichnis. Laufen:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

5. Führen Sie einen der folgenden Schritte aus:
   - Wenn das ONTAP -Zertifikat von der Stammzertifizierungsstelle und einer Zwischenzertifizierungsstelle signiert ist, fügen Sie die `pem` Dateien von beiden in eine Datei mit dem Namen `ontap.crt` am aktuellen Standort.
   - Wenn das ONTAP -Zertifikat von einer einzigen Zertifizierungsstelle signiert ist, benennen Sie das `pem` Datei als `ontap.crt` und kopieren Sie es an den aktuellen Speicherort. Fügen Sie das Blattzertifikat nicht zu dieser Datei hinzu.

Schritte für den Cloudmanager_CBS-Container

Aktivieren Sie als Nächstes die ONTAP -Server-Zertifikatsüberprüfung in NetApp Backup and Recovery (Cloud Backup Service).

1. Wechseln Sie zum Verzeichnis des Docker-Volumes, das Sie in den vorherigen Schritten erhalten haben.

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Wechseln Sie in das Konfigurationsverzeichnis. Laufen:

```
cd cbs_config
```

3. Erstellen Sie eine Konfigurationsdatei wie unten gezeigt mit einem der folgenden Namen, basierend auf Ihrer Bereitstellungsumgebung:
   - `production-customer.json`Wird für Bereitstellungen im Standardmodus und eingeschränkten Modus verwendet.
   - `darksite-customer.json`Wird für Bereitstellungen im privaten Modus verwendet.

     Siehe "Bereitstellungsmodi der NetApp Console" .

     Konfigurationsdatei

```
{
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

4. Verlassen Sie den Container. Laufen:

```
exit
```

5. Starten Sie NetApp Backup and Recovery neu. Laufen:

```
docker restart cloudmanager_cbs
```

Schritte für den Container „cloudmanager_cbs_catalog“

Aktivieren Sie die ONTAP -Server-Zertifikatsüberprüfung für den Katalogisierungsdienst.

1. Wechseln Sie zum Docker-Volume. Laufen:

```
cd /var/lib/docker/volumes/service-manager-
2_cloudmanager_cbs_volume/_data
```

2. Laufen:

```
cd cbs_catalog_config
```

3. Erstellen Sie eine Konfigurationsdatei wie unten gezeigt mit einem der folgenden Namen, basierend auf Ihrer Bereitstellungsumgebung:

   - `production-customer.json`Wird für Bereitstellungen im Standardmodus und eingeschränkten Modus verwendet.
   - `darksite-customer.json`Wird für Bereitstellungen im privaten Modus verwendet.

   Siehe "Bereitstellungsmodi der NetApp Console" .

   Konfigurationsdatei

```
{
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

4. Starten Sie NetApp Backup and Recovery neu. Laufen:

```
docker restart cloudmanager_cbs_catalog
```

Erstellen Sie ein Zertifikat für ONTAP und StorageGRID

Wenn Sie das Zertifikat sowohl für ONTAP als auch für StorageGRID aktivieren müssen, sieht die Konfigurationsdatei folgendermaßen aus:

Konfigurationsdatei für ONTAP und StorageGRID

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  },
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

Richten Sie Sicherungsziele ein, bevor Sie NetApp Backup and Recovery verwenden

Bevor Sie NetApp Backup and Recovery verwenden, führen Sie einige Schritte zum Einrichten von Sicherungszielen aus.

Bevor Sie beginnen, überprüfen Sie"Voraussetzungen" um sicherzustellen, dass Ihre Umgebung bereit ist.

Vorbereiten des Sicherungsziels

Bereiten Sie eines oder mehrere der folgenden Sicherungsziele vor:

- NetApp StorageGRID.

  Siehe "Entdecken Sie StorageGRID" .

  Siehe "StorageGRID -Dokumentation" für Details zu StorageGRID.

- Amazon Web Services. Siehe "Amazon S3-Dokumentation" .

Gehen Sie wie folgt vor, um AWS als Sicherungsziel vorzubereiten:

  - Richten Sie ein Konto in AWS ein.
  - Konfigurieren Sie die S3-Berechtigungen in AWS, die im nächsten Abschnitt aufgeführt sind.
  - Weitere Informationen zur Verwaltung Ihres AWS-Speichers in der Konsole finden Sie unter "Verwalten Sie Ihre Amazon S3-Buckets" .

- Microsoft Azure.
  - Siehe "Azure NetApp Files Dokumentation" .
  - Richten Sie ein Konto in Azure ein.
  - Konfigurieren "Azure-Berechtigungen" in Azure.
  - Weitere Informationen zur Verwaltung Ihres Azure-Speichers in der Konsole finden Sie unter "Verwalten Ihrer Azure-Speicherkonten" .

Nachdem Sie Optionen im Sicherungsziel selbst konfiguriert haben, konfigurieren Sie es später als Sicherungsziel in NetApp Backup and Recovery. Einzelheiten zum Konfigurieren des Sicherungsziels in NetApp Backup and Recovery finden Sie unter"Ermitteln von Sicherungszielen" .

S3-Berechtigungen einrichten

Sie müssen zwei Sätze von AWS S3-Berechtigungen konfigurieren:

- Berechtigungen für den Konsolenagenten zum Erstellen und Verwalten des S3-Buckets.
- Berechtigungen für den lokalen ONTAP Cluster, damit dieser Daten aus dem S3-Bucket lesen und schreiben kann.

Schritte

1. Stellen Sie sicher, dass der Konsolenagent über die erforderlichen Berechtigungen verfügt. Weitere Einzelheiten finden Sie unter "Richtlinienberechtigungen für die NetApp Console" .

   Wenn Sie Backups in AWS China-Regionen erstellen, müssen Sie den AWS-Ressourcennamen „arn“ unter allen *Resource*-Abschnitten in den IAM-Richtlinien von „aws“ in „aws-cn“ ändern. Beispiel: `arn:aws-cn:s3:::netapp-backup-*` .

2. Wenn Sie den Dienst aktivieren, werden Sie vom Backup-Assistenten aufgefordert, einen Zugriffsschlüssel und einen geheimen Schlüssel einzugeben. Diese Anmeldeinformationen werden an den ONTAP Cluster weitergegeben, damit ONTAP Daten im S3-Bucket sichern und wiederherstellen kann. Dazu müssen Sie einen IAM-Benutzer mit den folgenden Berechtigungen erstellen.

   Weitere Informationen finden Sie im "AWS-Dokumentation: Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer" .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "arn:aws:s3:::netapp-backup-*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/*",
      "Effect": "Allow"
    }
  ]
}
```

Melden Sie sich bei NetApp Backup and Recovery an

Sie verwenden die NetApp Console , um sich bei NetApp Backup and Recovery anzumelden.

NetApp Backup and Recovery verwendet Identitäts- und Zugriffsverwaltung, um zu steuern, was jeder Benutzer tun kann.

Einzelheiten zu den Aktionen, die jede Rolle ausführen kann, finden Sie unter"NetApp Backup and Recovery -Benutzerrollen" .

Um sich bei der NetApp Console anzumelden, können Sie Ihre Anmeldeinformationen für die NetApp -Support -Site verwenden oder sich mit Ihrer E-Mail-Adresse und einem Kennwort für die Anmeldung bei der NetApp Console registrieren. "Erfahren Sie mehr über die Anmeldung" .

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

Um einen Konsolenagenten hinzuzufügen, müssen Sie über die Superadministratorrolle „Backup und Wiederherstellung“ verfügen.

Schritte

1. Öffnen Sie einen Webbrowser und gehen Sie zu "NetApp Console" .

   Die Anmeldeseite der NetApp Console wird angezeigt.

2. Melden Sie sich bei der Konsole an.
3. Wählen Sie in der linken Navigation der Konsole **Schutz** > **Sicherung und Wiederherstellung**.
   - Wenn Sie sich zum ersten Mal bei Backup and Recovery anmelden und noch kein System zur Seite **Systeme** hinzugefügt haben, zeigt Backup and Recovery die Startseite "Willkommen bei der neuen NetApp Backup and Recovery" mit der Option zum Hinzufügen eines Systems an. Einzelheiten zum Hinzufügen eines Systems zur Seite **Systeme** finden Sie unter "Erste Schritte mit dem Standardmodus der NetApp Console"Die
   - Wenn Sie sich zum ersten Mal bei Backup and Recovery anmelden und zwar ein System in der Konsole haben, aber keine Ressourcen erkannt wurden, wird die Seite *Willkommen bei der neuen NetApp Backup and Recovery* mit einer Option zum **Erkennen von Ressourcen** angezeigt.
4. Falls noch nicht geschehen, wählen Sie die Option **Erkennen und verwalten**.
   - Informationen zu Microsoft SQL Server-Workloads finden Sie unter"Entdecken Sie Microsoft SQL Server-Workloads" .
   - Informationen zu VMware-Workloads finden Sie unter"Entdecken Sie VMware-Workloads" .
   - Informationen zu KVM-Workloads finden Sie unter"Entdecken Sie KVM-Workloads" .
   - Für Oracle Database-Workloads siehe "Oracle Database-Workloads entdecken".
   - Informationen zu Hyper-V-Workloads finden Sie unter"Entdecken Sie Hyper-V-Workloads" .
   - Informationen zu Kubernetes-Workloads finden Sie unter"Entdecken Sie Kubernetes-Workloads" .

Ermitteln Sie externe Sicherungsziele in NetApp Backup and Recovery

Führen Sie einige Schritte aus, um externe Sicherungsziele in NetApp Backup and Recovery zu ermitteln oder manuell hinzuzufügen.

Ermitteln eines Sicherungsziels

Konfigurieren Sie Ihre Sicherungsziele (Amazon Web Services (AWS) S3, Microsoft Azure Blob Storage, Google Cloud Storage oder StorageGRID), bevor Sie NetApp Backup and Recovery verwenden.

Sie können diese Ziele automatisch ermitteln oder manuell hinzufügen.

Geben Sie Anmeldeinformationen für den Zugriff auf das Speicherkonto ein. NetApp Backup and Recovery verwendet diese Anmeldeinformationen, um die Workloads zu ermitteln, die Sie sichern möchten.

Bevor Sie beginnen

Sie müssen mindestens eine Arbeitslast ermitteln, bevor Sie ein externes Sicherungsziel hinzufügen können.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie die Registerkarte **Offsite-Sicherungsziele**.
3. Wählen Sie **Sicherungsziel ermitteln**.
4. Wählen Sie einen der Sicherungszieltypen: **Amazon Web Services (AWS) S3**, **Microsoft Azure Blob Storage**, * StorageGRID* oder * ONTAP S3*.
5. Wählen Sie im Abschnitt **Speicherort der Anmeldeinformationen auswählen** den Speicherort aus, an dem sich die Anmeldeinformationen befinden, und wählen Sie dann aus, wie die Anmeldeinformationen verknüpft werden sollen.
6. Wählen Sie **Weiter**.
7. Geben Sie die Anmeldeinformationen ein. Die Informationen variieren je nach Art des ausgewählten Sicherungsziels und dem von Ihnen gewählten Speicherort der Anmeldeinformationen.
   - Für AWS:
     - **Anmeldeinformationsname**: Geben Sie den AWS-Anmeldeinformationsnamen ein.
     - **Zugriffsschlüssel**: Geben Sie das AWS-Geheimnis ein.
     - **Geheimschlüssel**: Geben Sie den geheimen AWS-Schlüssel ein.
   - Für Azure:
     - **Anmeldeinformationsname**: Geben Sie den Anmeldeinformationsnamen für Azure Blob Storage ein.
     - **Clientgeheimnis**: Geben Sie das Clientgeheimnis von Azure Blob Storage ein.
     - **Anwendungs-ID (Client-ID)**: Wählen Sie die Azure Blob Storage-Anwendungs-ID aus.
     - **Verzeichnis-Mandanten-ID**: Geben Sie die Azure Blob Storage-Mandanten-ID ein.
   - Für StorageGRID:
     - **Anmeldeinformationsname**: Geben Sie den Anmeldeinformationsnamen von StorageGRID ein.
     - **Gateway-Knoten-FQDN**: Geben Sie einen FQDN-Namen für StorageGRID ein.

- **Port**: Geben Sie die Portnummer für StorageGRID ein.
- **Zugriffsschlüssel**: Geben Sie den StorageGRID S3-Zugriffsschlüssel ein.
- **Geheimschlüssel**: Geben Sie den geheimen Schlüssel von StorageGRID S3 ein.

◦ Für ONTAP S3:

- **Anmeldeinformationsname**: Geben Sie den Anmeldeinformationsnamen für ONTAP S3 ein.
- **Gateway-Knoten-FQDN**: Geben Sie einen FQDN-Namen für ONTAP S3 ein.
- **Port**: Geben Sie die Portnummer für ONTAP S3 ein.
- **Zugriffsschlüssel**: Geben Sie den ONTAP S3-Zugriffsschlüssel ein.
- **Geheimschlüssel**: Geben Sie den geheimen Schlüssel von ONTAP S3 ein.

8. Wählen Sie **Entdecken**.

Einen Bucket für ein Sicherungsziel hinzufügen

Anstatt Buckets automatisch von NetApp Backup and Recovery erkennen zu lassen, können Sie einem externen Sicherungsziel manuell einen Bucket hinzufügen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie **Offsite-Sicherungsziele**.
3. Wählen Sie das Ziel aus und wählen Sie rechts die **Aktionen*** **Symbol und wählen Sie *Bucket hinzufügen**.
4. Geben Sie die Bucket-Informationen ein. Die Informationen unterscheiden sich je nach Art des ausgewählten Sicherungsziels.

◦ Für AWS:

- **Bucketname**: Geben Sie den Namen des S3-Buckets ein. Das Präfix „netapp-backup“ ist ein erforderliches Präfix und wird automatisch zu dem von Ihnen angegebenen Namen hinzugefügt.
- **AWS-Konto**: Geben Sie den AWS-Kontonamen ein.
- **Bucket-Region**: Geben Sie die AWS-Region für den Bucket ein.
- **S3-Objektsperre aktivieren**: Wählen Sie diese Option, um die S3-Objektsperre für den Bucket zu aktivieren. S3 Object Lock verhindert, dass Objekte für einen bestimmten Aufbewahrungszeitraum gelöscht oder überschrieben werden, und bietet so eine zusätzliche Ebene des Datenschutzes. Sie können dies nur aktivieren, wenn Sie einen Bucket erstellen, und Sie können es später nicht mehr deaktivieren.
  - **Governance-Modus**: Wählen Sie diese Option, um den Governance-Modus für den S3 Object Lock-Bucket zu aktivieren. Im Governance-Modus können Sie Objekte vor dem Löschen oder Überschreiben durch die meisten Benutzer schützen, bestimmten Benutzern ist jedoch das Ändern der Aufbewahrungseinstellungen gestattet.
  - **Compliance-Modus**: Wählen Sie diese Option, um den Compliance-Modus für den S3 Object Lock-Bucket zu aktivieren. Der Compliance-Modus verhindert, dass Benutzer, einschließlich des Root-Benutzers, die Aufbewahrungseinstellungen ändern oder Objekte löschen, bis die Aufbewahrungsfrist abgelaufen ist.
- **Versionierung**: Wählen Sie diese Option, um die Versionierung für den S3-Bucket zu aktivieren. Durch die Versionierung können Sie mehrere Versionen von Objekten im Bucket behalten, was für Sicherungs- und Wiederherstellungszwecke nützlich sein kann.

- **Tags**: Wählen Sie Tags für den S3-Bucket aus. Tags sind Schlüssel-Wert-Paare, die zum Organisieren und Verwalten Ihrer S3-Ressourcen verwendet werden können.
- **Verschlüsselung**: Wählen Sie die Art der Verschlüsselung für den S3-Bucket aus. Zur Auswahl stehen entweder von AWS S3 verwaltete Schlüssel oder AWS Key Management Service-Schlüssel. Wenn Sie AWS Key Management Service-Schlüssel auswählen, müssen Sie die Schlüssel-ID angeben.

◦ Für Azure:

- **Abonnement**: Wählen Sie den Namen des Azure Blob Storage-Containers aus.
- **Ressourcengruppe**: Wählen Sie den Namen der Azure-Ressourcengruppe aus.
- **Instanzdetails**:
  - **Speicherkontoname**: Geben Sie den Namen des Azure Blob Storage-Containers ein.
  - **Azure-Region**: Geben Sie die Azure-Region für den Container ein.
  - **Leistungstyp**: Wählen Sie den Leistungstyp „Standard“ oder „Premium“ für den Azure Blob Storage-Container aus, der das erforderliche Leistungsniveau angibt.
  - **Verschlüsselung**: Wählen Sie den Verschlüsselungstyp für den Azure Blob Storage-Container aus. Zur Auswahl stehen entweder von Microsoft verwaltete Schlüssel oder vom Kunden verwaltete Schlüssel. Wenn Sie vom Kunden verwaltete Schlüssel auswählen, müssen Sie den Namen des Schlüsseltresors und den Schlüsselnamen angeben.

◦ Für StorageGRID:

- **Name des Sicherungsziels**: Wählen Sie den Namen des StorageGRID Buckets aus.
- **Bucket-Name**: Geben Sie den Namen des StorageGRID Buckets ein.
- **Region**: Geben Sie die StorageGRID -Region für den Bucket ein.
- **Versionierung aktivieren**: Wählen Sie diese Option, um die Versionierung für den StorageGRID Bucket zu aktivieren. Durch die Versionierung können Sie mehrere Versionen von Objekten im Bucket behalten, was für Sicherungs- und Wiederherstellungszwecke nützlich sein kann.
- **Objektsperre**: Wählen Sie diese Option, um die Objektsperre für den StorageGRID Bucket zu aktivieren. Durch die Objektsperre wird verhindert, dass Objekte für einen bestimmten Aufbewahrungszeitraum gelöscht oder überschrieben werden, und so eine zusätzliche Ebene des Datenschutzes geschaffen. Sie können dies nur aktivieren, wenn Sie einen Bucket erstellen, und Sie können es später nicht mehr deaktivieren.
- **Kapazität**: Geben Sie die Kapazität für den StorageGRID Bucket ein. Dies ist die maximale Datenmenge, die im Bucket gespeichert werden kann.

◦ Für ONTAP S3:

- **Name des Sicherungsziels**: Wählen Sie den Namen des ONTAP S3-Buckets aus.
- **Bucket-Zielname**: Geben Sie den Namen des ONTAP S3-Buckets ein.
- **Kapazität**: Geben Sie die Kapazität für den ONTAP S3-Bucket ein. Dies ist die maximale Datenmenge, die im Bucket gespeichert werden kann.
- **Versionierung aktivieren**: Wählen Sie diese Option, um die Versionierung für den ONTAP S3-Bucket zu aktivieren. Durch die Versionierung können Sie mehrere Versionen von Objekten im Bucket behalten, was für Sicherungs- und Wiederherstellungszwecke nützlich sein kann.
- **Objektsperre**: Wählen Sie diese Option, um die Objektsperre für den ONTAP S3-Bucket zu aktivieren. Durch die Objektsperre wird verhindert, dass Objekte für einen bestimmten Aufbewahrungszeitraum gelöscht oder überschrieben werden, und so eine zusätzliche Ebene des Datenschutzes geschaffen. Sie können dies nur aktivieren, wenn Sie einen Bucket erstellen, und

Sie können es später nicht mehr deaktivieren.

5. Wählen Sie **Hinzufügen**.

Anmeldeinformationen für ein Sicherungsziel ändern

Geben Sie die für den Zugriff auf das Sicherungsziel erforderlichen Anmeldeinformationen ein.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie **Offsite-Sicherungsziele**.
3. Wählen Sie das Ziel aus und wählen Sie rechts die **Aktionen*** **Symbol und wählen Sie *Anmeldeinformationen ändern**.
4. Geben Sie die neuen Anmeldeinformationen für das Sicherungsziel ein. Die Informationen unterscheiden sich je nach Art des ausgewählten Sicherungsziels.
5. Wählen Sie **Fertig**.

Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads

Sie können zwischen den verschiedenen NetApp Backup and Recovery -Workloads wechseln.

Wechseln Sie zu einer anderen Arbeitslast

Sie können in der NetApp Backup and Recovery -Benutzeroberfläche zu einer anderen Arbeitslast wechseln.

Schritte

1. Wählen Sie in der linken Navigation der Konsole **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie in der oberen rechten Ecke der Seite die Dropdown-Liste **Workload wechseln** aus.
3. Wählen Sie die Arbeitslast aus, zu der Sie wechseln möchten.

   Die Seite wird aktualisiert und zeigt die ausgewählte Arbeitslast an.

Konfigurieren der NetApp Backup and Recovery -Einstellungen

Nachdem Sie die NetApp Console eingerichtet haben, konfigurieren Sie die Sicherungs- und Wiederherstellungseinstellungen. Fügen Sie Anmeldeinformationen für Hostressourcen hinzu, importieren Sie SnapCenter -Ressourcen, konfigurieren Sie Protokollverzeichnisse und legen Sie VMware vCenter-Einstellungen fest. Führen Sie diese Schritte aus, bevor Sie Daten sichern oder wiederherstellen.

- Anmeldeinformationen für Hostressourcen hinzufügen für alle Windows-, Microsoft SQL Server-, Oracle Database- oder Linux-Hosts, bei denen NetApp Backup and Recovery eine Authentifizierung durchführen muss. Dies umfasst die Anmeldeinformationen des Windows-Gastbetriebssystems, die beim Wiederherstellen von Gastdateien oder -ordnern verwendet werden.

- Verwalten der VMware vCenter-Einstellungen.
- Importieren und Verwalten von SnapCenter -Hostressourcen. (Nur Microsoft SQL Server-Workloads)
- Fügen Sie eine KVM-Managementplattform hinzu.Die (Nur KVM-Workloads)
- Konfigurieren von Protokollverzeichnissen in Snapshots für Windows-Hosts.
- Erstellen einer Ausführungs-Hook-Vorlage zum Ausführen von Skripten vor und nach Backup-Jobs. (Nur Kubernetes-Workloads)

*Erforderliche NetApp Console * Superadministrator für Backup und Wiederherstellung, Backup-Administrator für Backup und Wiederherstellung, Wiederherstellungsadministrator 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" .

Anmeldeinformationen für Hostressourcen hinzufügen

Fügen Sie Anmeldeinformationen für Hostressourcen hinzu. NetApp Backup and Recovery verwendet diese Anmeldeinformationen, um Workloads zu erkennen und Backup-Richtlinien anzuwenden.

Wenn Sie keine Anmeldeinformationen haben, erstellen Sie diese mit Berechtigungen für den Zugriff auf und die Verwaltung von Host-Workloads.

Sie müssen die folgenden Arten von Anmeldeinformationen konfigurieren:

- Microsoft SQL Server-Anmeldeinformationen
- SnapCenter Windows-Host-Anmeldeinformationen
- Anmeldeinformationen des Windows-Gastbetriebssystems, die beim Wiederherstellen von Gastdateien oder -ordnern verwendet werden
- Oracle-Datenbank-Zugangsdaten
- Anmeldeinformationen für den Linux-Host

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Einstellungen** aus.
2. Wählen Sie den Abwärtspfeil für **Anmeldeinformationen**.
3. Wählen Sie **Neue Anmeldeinformationen hinzufügen**.
4. Geben Sie die Zugangsdaten ein. Je nach gewähltem Authentifizierungsmodus werden unterschiedliche Felder angezeigt. Bewegen Sie den Mauszeiger über das Informationssymbol **i**, um weitere Informationen zu den Feldern zu erhalten.
    - **Name der Anmeldeinformationen**: Geben Sie einen Namen für die Anmeldeinformationen ein.
    - **Authentifizierungsmodus**: Wählen Sie **Windows**, **Microsoft SQL**, **Oracle Database** oder **Linux**.

Für Microsoft SQL Server-Workloads müssen Sie Anmeldeinformationen sowohl für Windows als auch für Microsoft SQL Server eingeben, daher müssen Sie zwei Sätze von Anmeldeinformationen hinzufügen.

Windows

i. Wenn Sie **Windows** ausgewählt haben:

- **Agenten**: Wählen Sie einen Konsolenagenten aus der Liste aus.
- **Domänen- und Benutzername**: Geben Sie den NetBIOS- oder Domänen-FQDN und den Benutzernamen für die Anmeldeinformationen ein.
- **Passwort**: Geben Sie das Passwort für die Anmeldeinformationen ein.

Microsoft SQL Server

i. Wenn Sie **Microsoft SQL Server** ausgewählt haben:

- **Domänen- und Benutzername**: Geben Sie den NetBIOS- oder Domänen-FQDN und den Benutzernamen für die Anmeldeinformationen ein.
- **Passwort**: Geben Sie das Passwort für die Anmeldeinformationen ein.
- **Hosts**: Wählen Sie eine ermittelte SQL Server-Hostadresse aus.
- **SQL Server-Instanz**: Wählen Sie eine erkannte SQL Server-Instanz aus.

Oracle-Datenbank

i. Wenn Sie **Oracle Database** ausgewählt haben:

- **Agenten**: Wählen Sie einen Konsolenagenten aus der Liste aus.
- **Benutzername**: Geben Sie den Benutzernamen für die Anmeldeinformationen ein.
- **Passwort**: Geben Sie das Passwort für die Anmeldeinformationen ein.

Linux

i. Wenn Sie **Linux** ausgewählt haben:

- **Agenten**: Wählen Sie einen Konsolenagenten aus der Liste aus.
- **Benutzername**: Geben Sie den Benutzernamen für die Anmeldeinformationen ein.
- **Passwort**: Geben Sie das Passwort für die Anmeldeinformationen ein.

5. Wählen Sie **Hinzufügen**.

Anmeldeinformationen für Hostressourcen bearbeiten

Sie können das Passwort für alle von Ihnen erstellten Zugangsdaten später bearbeiten.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Einstellungen** aus.
2. Wählen Sie den Abwärtspfeil aus, um den Abschnitt **Anmeldeinformationen** zu erweitern.
3. Wählen Sie das Symbol Aktionen ••• > **Anmeldeinformationen bearbeiten**.
   - **Passwort**: Geben Sie das Passwort für die Anmeldeinformationen ein.
4. Wählen Sie **Speichern**.

Verwalten der VMware vCenter-Einstellungen

Geben Sie VMware vCenter-Anmeldeinformationen ein, um Workloads für die Sicherung zu ermitteln. Wenn

Sie keine Anmeldeinformationen haben, erstellen Sie diese mit Berechtigungen für den Zugriff auf und die Verwaltung der VMware vCenter Server-Workloads.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Einstellungen** aus.
2. Wählen Sie den Abwärtspfeil aus, um den Abschnitt **VMware vCenter** zu erweitern.
3. Wählen Sie **vCenter hinzufügen**.
4. Geben Sie die VMware vCenter Server-Informationen ein.
   - **vCenter FQDN oder IP-Adresse**: Geben Sie einen FQDN-Namen oder die IP-Adresse für den VMware vCenter Server ein.
   - **Benutzername** und **Passwort**: Geben Sie den Benutzernamen und das Passwort für den VMware vCenter Server ein.
   - **Port**: Geben Sie die Portnummer für den VMware vCenter Server ein.
   - **Protokoll**: Wählen Sie **HTTP** oder **HTTPS**.
5. Wählen Sie **Hinzufügen**.

Importieren und Verwalten von SnapCenter -Hostressourcen

Wenn Sie zuvor SnapCenter zum Sichern Ihrer Ressourcen verwendet haben, können Sie diese Ressourcen in NetApp Backup and Recovery importieren und verwalten. Mit dieser Option können Sie SnapCenter -Serverinformationen importieren, um mehrere SnapCenter -Server zu registrieren und Datenbank-Workloads zu ermitteln.

Dies ist ein zweiteiliger Prozess:

- Importieren Sie SnapCenter Server-Anwendungs- und Hostressourcen
- Verwalten ausgewählter SnapCenter -Hostressourcen

Importieren Sie SnapCenter Server-Anwendungs- und Hostressourcen

Dieser erste Schritt importiert Hostressourcen aus SnapCenter und zeigt diese Ressourcen auf der Inventarseite von NetApp Backup and Recovery an. Zu diesem Zeitpunkt werden die Ressourcen noch nicht von NetApp Backup and Recovery verwaltet.

Nachdem Sie SnapCenter -Hostressourcen importiert haben, übernimmt NetApp Backup and Recovery nicht die Schutzverwaltung. Dazu müssen Sie die Verwaltung dieser Ressourcen in NetApp Backup and Recovery ausdrücklich auswählen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Einstellungen** aus.
2. Wählen Sie den Abwärtspfeil aus, um den Abschnitt **Aus SnapCenter importieren** zu erweitern.
3. Wählen Sie **Aus SnapCenter importieren**, um die SnapCenter -Ressourcen zu importieren.
4. Geben Sie * Anmeldeinformationen für die SnapCenter -Anwendung* ein:
   a. * SnapCenter FQDN oder IP-Adresse*: Geben Sie den FQDN oder die IP-Adresse der SnapCenter -Anwendung selbst ein.
   b. **Port**: Geben Sie die Portnummer für den SnapCenter -Server ein.

c. **Benutzername** und **Passwort**: Geben Sie den Benutzernamen und das Passwort für den SnapCenter -Server ein.

d. **Konsolenagent**: Wählen Sie den Konsolenagenten für SnapCenter aus.

5. Geben Sie * SnapCenter -Server-Host-Anmeldeinformationen* ein:

a. **Vorhandene Anmeldeinformationen**: Wenn Sie diese Option auswählen, können Sie die vorhandenen Anmeldeinformationen verwenden, die Sie bereits hinzugefügt haben. Geben Sie den Anmeldenamen ein.

b. **Neue Anmeldeinformationen hinzufügen**: Wenn Sie keine vorhandenen SnapCenter -Host -Anmeldeinformationen haben, können Sie neue Anmeldeinformationen hinzufügen. Geben Sie den Anmeldenamen, den Authentifizierungsmodus, den Benutzernamen und das Kennwort ein.

6. Wählen Sie **Importieren**, um Ihre Eingaben zu bestätigen und den SnapCenter -Server zu registrieren.

Wenn der SnapCenter -Server bereits registriert ist, können Sie die vorhandenen Registrierungsdetails aktualisieren.

Ergebnis

Auf der Inventarseite werden die importierten SnapCenter -Ressourcen angezeigt.

Verwalten von SnapCenter -Hostressourcen

Nachdem Sie die SnapCenter -Ressourcen importiert haben, verwalten Sie diese Hostressourcen in NetApp Backup and Recovery. Nachdem Sie die Verwaltung dieser importierten Ressourcen ausgewählt haben, kann NetApp Backup and Recovery die Ressourcen, die Sie aus SnapCenter importieren, sichern und wiederherstellen. Sie müssen diese Ressourcen nicht mehr im SnapCenter Server verwalten.

Schritte

1. Nachdem Sie die SnapCenter -Ressourcen importiert haben, wählen Sie auf der angezeigten Inventarseite die importierten SnapCenter -Ressourcen aus, die von nun an von NetApp Backup and Recovery verwaltet werden sollen.
2. Wählen Sie das Symbol Aktionen ••• > **Verwalten**, um die Ressourcen zu verwalten.
3. Wählen Sie **In NetApp Console verwalten**.

   Auf der Inventarseite wird unter dem Hostnamen **Verwaltet** angezeigt, um anzuzeigen, dass die ausgewählten Hostressourcen jetzt von NetApp Backup and Recovery verwaltet werden.

Importierte SnapCenter -Ressourcen bearbeiten

Sie können SnapCenter -Ressourcen später erneut importieren oder die importierten SnapCenter -Ressourcen bearbeiten, um die Registrierungsdetails zu aktualisieren.

Sie können nur die Port- und Kennwortdetails für den SnapCenter -Server ändern.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Einstellungen** aus.
2. Wählen Sie den Abwärtspfeil für **Aus SnapCenter importieren**.

   Auf der Seite „Aus SnapCenter importieren“ werden alle vorherigen Importe angezeigt.

3. Wählen Sie das Symbol Aktionen ••• > **Bearbeiten**, um die Ressourcen zu aktualisieren.

4. Aktualisieren Sie bei Bedarf das SnapCenter -Passwort und die Portdetails.
5. Wählen Sie **Importieren**.

Fügen Sie eine KVM-Managementplattform hinzu.

Wenn Sie die Apache CloudStack-Managementplattform zur Verwaltung von KVM-Ressourcen verwenden, müssen Sie diese mit NetApp Backup and Recovery integrieren, damit Backup and Recovery die verwalteten KVM-Hosts und VMs erkennen und schützen kann.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Einstellungen** aus.
2. Klicken Sie auf den Abwärtspfeil, um den Abschnitt **Managementplattform** zu erweitern.
3. Wählen Sie **Verwaltungsplattform-Anmeldeinformationen hinzufügen**.
4. Geben Sie die folgenden Informationen ein:
   - **IP-Adresse oder FQDN der Managementplattform**: Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen der Managementplattform ein.
   - **API-Schlüssel**: Geben Sie den API-Schlüssel ein, der zur Authentifizierung von API-Anfragen verwendet werden soll.
   - **Geheimer Schlüssel**: Geben Sie den geheimen Schlüssel ein, der zur Authentifizierung von API-Anfragen verwendet werden soll.
   - **Port**: Geben Sie den Port ein, der für die Kommunikation zwischen Backup und Recovery und der Managementplattform verwendet werden soll.
   - **Agenten**: Wählen Sie einen Konsolenagenten aus, der die Kommunikation zwischen Backup und Recovery und der Managementplattform erleichtern soll.
5. Wenn Sie fertig sind, wählen Sie **Hinzufügen**.

Konfigurieren von Protokollverzeichnissen in Snapshots für Windows-Hosts

Bevor Sie Richtlinien für Windows-Hosts erstellen, sollten Sie Protokollverzeichnisse in Snapshots für Windows-Hosts konfigurieren. Protokollverzeichnisse werden zum Speichern der Protokolle verwendet, die während des Sicherungsvorgangs generiert werden.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie auf der Inventarseite eine Arbeitslast aus und wählen Sie dann das Symbol Aktionen ••• > **Details anzeigen**, um die Arbeitslastdetails anzuzeigen.
3. Wählen Sie auf der Seite mit den Inventardetails, auf der Microsoft SQL Server angezeigt wird, die Registerkarte „Hosts“ aus.
4. Wählen Sie auf der Seite „Inventardetails“ einen Host aus und wählen Sie das Symbol „Aktionen“ ••• > **Protokollverzeichnis konfigurieren**.
5. Durchsuchen Sie das Protokollverzeichnis oder geben Sie den Pfad ein.
6. Wählen Sie **Speichern**.

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.

Richten Sie rollenbasierte Zugriffssteuerung in NetApp Backup and Recovery ein

Um die Sicherheit zu erhöhen und den Ressourcenzugriff zu kontrollieren, konfigurieren Sie rollenbasierte Zugriffssteuerung für NetApp Backup and Recovery. Die NetApp Console unterstützt rollenbasierte Zugriffssteuerung (RBAC) für einige Backup and Recovery Workloads. Sie können diesen Workloads spezifische Administrator- oder Betrachterrollen zuweisen. Andere Workloads, die noch keine rollenbasierte Zugriffssteuerung unterstützen, bleiben für alle Benutzer mit Backup and Recovery Rollen zugänglich, bis die Zuordnung auf Projektebene unterstützt wird.

Führen Sie diese Schritte aus, um den Zugriff auf Ressourcen in Ihrer Organisation zu steuern. Nehmen Sie Änderungen auf der Seite **Administration > Identität und Zugriff** im NetApp Console-Menü vor.

Diese Schritte setzen voraus, dass Ihnen in der Console die Rolle „Organization Admin“ zugewiesen ist.

Schritte

1. Erstellen Sie die Identitäts- und Zugriffsprojektstruktur.

   Als Organisationsadministrator richten Sie den Ordner für Identität und Zugriff sowie die Projektstruktur ein, in der die Workloads gespeichert werden.

2. Benutzerrollen zuweisen.
   a. Primäre Option:

Fügen Sie jedem für Arbeitslasten vorgesehenen Projekt Benutzer hinzu und weisen Sie ihnen die entsprechende Rolle zu. Beispiel:

- **Organisationsadministrator** und **Backup and Recovery Superadministrator**: Ein Benutzer mit diesen Rollen kann alle Ressourcen in allen Organisationen sehen, und Backup and Recovery Workloads erkennen und diese Projekten zuordnen (zum Beispiel US East oder US West).
- **Ordner- oder Projektadministrator** und **Backup and Recovery Superadmin**: Ein Benutzer mit diesen Rollen kann nur die Ressourcen in dem Ordner oder Projekt sehen, für das er Berechtigungen hat, kann aber Backup and Recovery Workloads erkennen und sie diesem Projekt zuweisen.

b. Alternative Option:

Anstatt einem Benutzer vollen Backup and Recovery-Administratorzugriff zu gewähren, können Sie sich selbst die Backup and Recovery-Superadmin-Rolle zuweisen und die Workloads direkt entdecken.

3. Workloads in NetApp Backup and Recovery ermitteln.

Organisation-Admins oder Ordner- oder Projekt-Admins entdecken die verfügbaren Workloads und wählen das entsprechende Projekt aus (wie US East oder US West). Jeder Workload wird automatisch dem ausgewählten Projekt zugeordnet.

4. Fügen Sie Benutzer zu Projekten hinzu.

Organisation-Admins oder Ordner-/Projekt-Admins fügen Console-Benutzer zu Projekten mit Workloads hinzu. Weisen Sie Benutzern die Rolle Organization viewer und eine Backup and Recovery-Rolle entsprechend ihren Zugriffsanforderungen zu. Benutzer mit der richtigen Backup and Recovery-Rolle erhalten automatisch Zugriff auf neue Workloads in diesen Projekten.

Verwandte Informationen

- "Erfahren Sie mehr über das NetApp Console-Identitäts- und Zugriffsmanagement".
- "NetApp Backup and Recovery -Rollen in der NetApp Console".

Verwenden Sie NetApp Backup and Recovery

Anzeigen des Schutzstatus im NetApp Backup and Recovery Dashboard

Durch die Überwachung des Zustands Ihrer Workloads wird sichergestellt, dass Sie über Probleme beim Workload-Schutz informiert sind und Schritte zu deren Lösung unternehmen können. Zeigen Sie den Status Ihrer Backups und Wiederherstellungen im NetApp Backup and Recovery Dashboard an. Sie können die Systemübersicht, die Schutzübersicht, die Jobübersicht, die Wiederherstellungsübersicht und mehr überprüfen.

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

Schritte

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.

   Sie können die folgenden Arten von Informationen überprüfen:

   - Anzahl der erkannten Hosts oder VMs
   - Anzahl der erkannten Kubernetes-Cluster
   - Anzahl der Sicherungsziele im Objektspeicher
   - Anzahl der vCenter
   - Anzahl der Speichercluster in ONTAP

Schutzübersicht anzeigen

Überprüfen Sie die folgenden Informationen in der Schutzzusammenfassung:

- Die Gesamtzahl der geschützten und ungeschützten Datenbanken, VMs und Datenspeicher.

  Eine geschützte Datenbank ist eine Datenbank, der eine Sicherungsrichtlinie zugewiesen ist. Eine ungeschützte Datenbank ist eine Datenbank, der keine Sicherungsrichtlinie zugewiesen ist.

- Die Anzahl der Sicherungen, die erfolgreich waren, eine Warnung aufweisen oder fehlgeschlagen sind.
- Die vom Sicherungsdienst ermittelte Gesamtkapazität und die geschützte bzw. ungeschützte Kapazität. Bewegen Sie den Mauszeiger über das Symbol „**i**“, um die Details anzuzeigen.

Jobzusammenfassung anzeigen

Überprüfen Sie in der Auftragszusammenfassung die Gesamtzahl der abgeschlossenen, laufenden oder

fehlgeschlagenen Aufträge.

Schritte

1. Ändern Sie für jede Jobverteilung einen Filter, um die Zusammenfassung der fehlgeschlagenen, laufenden und abgeschlossenen Jobs basierend auf der Anzahl der Tage anzuzeigen, z. B. die letzten 30 Tage, die letzten 7 Tage, die letzten 24 Stunden oder das letzte Jahr.
2. Zeigen Sie Details zu fehlgeschlagenen, laufenden und abgeschlossenen Jobs an, indem Sie **Jobüberwachung anzeigen** auswählen.

Wiederherstellungszusammenfassung anzeigen

Überprüfen Sie die folgenden Informationen in der Wiederherstellungszusammenfassung:

- Die Gesamtzahl der durchgeführten Wiederherstellungsaufträge
- Die Gesamtmenge der wiederhergestellten Kapazität
- Die Anzahl der Wiederherstellungsaufträge, die auf lokalem, sekundärem und Objektspeicher ausgeführt wurden. Bewegen Sie den Mauszeiger über das Diagramm, um die Details anzuzeigen.

Erstellen und verwalten Sie Richtlinien zur Steuerung von Backups in NetApp Backup and Recovery

Erstellen Sie in NetApp Backup and Recovery Ihre eigenen Richtlinien, die die Sicherungshäufigkeit, den Zeitpunkt der Sicherung und die Anzahl der aufbewahrten Sicherungsdateien 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 (nicht verfügbar für VMware-Vorschau-Workloads)
- Richtlinien löschen

Richtlinien anzeigen

1. Wählen Sie im NetApp Backup and Recovery -Menü **Richtlinien** aus.
2. Überprüfen Sie diese Richtliniendetails.
    - **Workload**: Beispiele sind Microsoft SQL Server, 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.
3. Geben Sie auf der Seite „Richtlinien“ die folgenden Informationen ein.
   - Abschnitt **Details**:
     - Workload-Typ: Wählen Sie den Workload aus, der die Richtlinie verwenden soll.
     - Geben Sie einen Richtliniennamen ein.

       Eine Liste der zu vermeidenden Zeichen finden Sie im Hover-Tipp.

     - Wählen Sie einen Konsolenagenten aus der Liste **Agent** aus.
   - Abschnitt **Sicherungsarchitektur**: Wählen Sie den Abwärtspfeil und wählen Sie den Datenfluss für die Sicherung, z. B. 3-2-1-Fan-Out, 3-2-1-Kaskade oder Festplatte zu Festplatte.
     - **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. Diese Konfigurationen helfen dabei, optimalen Datenschutz und Notfallwiederherstellung zu erreichen.

Diese Option ist für Amazon FSx for NetApp ONTAP nicht verfügbar.

Bei VMware-Workloads wird dadurch der lokale Snapshot auf den Datenspeichern oder VMs auf dem primären Speicher konfiguriert und vom primären Festplattenspeicher auf den sekundären Festplattenspeicher sowie vom primären auf den Cloud-Objektspeicher repliziert.

- **3-2-1-Kaskade**: (Nicht verfügbar für Kubernetes-Workloads) Primärspeicher (Festplatte) zu Sekundärspeicher (Festplatte) und Primärspeicher (Festplatte) zu Cloud-Speicher (Objektspeicher). Dies kann ein Cloud-Hyperscaler-Objektspeicher oder ein privater Objektspeicher sein – StorageGRID. Dadurch wird eine Kette der Datenreplikation über mehrere Systeme hinweg erstellt, um Redundanz und Zuverlässigkeit zu gewährleisten.

  Diese Option ist für Amazon FSx for NetApp ONTAP nicht verfügbar.

Für VMware-Workloads wird dadurch der lokale Snapshot auf den Datenspeichern oder VMs auf dem primären Speicher und eine Kaskade vom primären Festplattenspeicher zum sekundären Festplattenspeicher und dann zum Cloud-Objektspeicher konfiguriert.

- **Disk to Disk**: (Nicht verfügbar für Kubernetes-Workloads) Primärspeicher (Disk) zu sekundärem Speicher (Disk). Die ONTAP -zu- ONTAP Datensicherungsstrategie repliziert Daten zwischen zwei ONTAP Systemen, um hohe Verfügbarkeit und Notfallwiederherstellung sicherzustellen. Dies wird normalerweise mit SnapMirror erreicht, das sowohl synchrone als auch asynchrone Replikation unterstützt. Diese Methode stellt sicher, dass Ihre Daten kontinuierlich aktualisiert werden und an mehreren Standorten verfügbar sind, und bietet einen robusten Schutz vor Datenverlust.

  Bei VMware-Workloads wird dadurch der lokale Snapshot auf den Datenspeichern oder VMwares auf dem primären Speichersystem konfiguriert und anschließend werden die Daten vom primären Festplattenspeichersystem auf das sekundäre Festplattenspeichersystem repliziert.

- **Disk-to-Object-Store**: Primärspeicher (Disk) zur Cloud (Objektspeicher). Dadurch werden Daten von einem ONTAP -System auf ein Objektspeichersystem wie AWS S3, Azure Blob Storage oder StorageGRID repliziert. Dies wird normalerweise durch die Verwendung von SnapMirror Cloud erreicht, das inkrementelle Backups für immer bereitstellt, indem nach der anfänglichen Basisübertragung nur geänderte Datenblöcke übertragen werden. Dies kann ein Cloud-Hyperscaler-Objektspeicher oder ein privater Objektspeicher sein – StorageGRID. Diese Methode eignet sich ideal für die langfristige Datenaufbewahrung und -archivierung und bietet eine kostengünstige und skalierbare Lösung für den Datenschutz.

  Für VMWare-Workloads wird hierdurch der lokale Snapshot auf den Datenspeichern oder VMs auf dem primären Server und die Replikation vom primären Festplattenspeicher zum Cloud-Objektspeicher konfiguriert.

- **Disk-to-Disk-Fanout**: (Nicht verfügbar für Kubernetes-Workloads) Primärspeicher (Disk) zu Sekundärspeicher (Disk) und Primärspeicher (Disk) zu Sekundärspeicher (Disk).

  Sie können mehrere sekundäre Einstellungen für die Disk-to-Disk-Fanout-Option konfigurieren.

Bei VMware-Workloads wird dadurch der primäre Festplattenspeicher auf den sekundären Festplattenspeicher konfiguriert und der primäre Festplattenspeicher auf den sekundären Festplattenspeicher repliziert.

  - **Lokale Snapshots**: Lokaler Snapshot auf dem ausgewählten Volume (Microsoft SQL Server). Lokale

Snapshots sind eine Schlüsselkomponente von Datenschutzstrategien, da sie den Zustand Ihrer Daten zu bestimmten Zeitpunkten erfassen. Dadurch werden schreibgeschützte Point-in-Time-Kopien der Produktionsvolumes erstellt, auf denen Ihre Workloads ausgeführt werden. Der Snapshot verbraucht nur minimalen Speicherplatz und verursacht nur einen vernachlässigbaren Leistungsaufwand, da er nur die Änderungen an Dateien seit dem letzten Snapshot aufzeichnet. Sie können lokale Snapshots verwenden, um Datenverlust oder -beschädigung zu beheben und um Backups für die Notfallwiederherstellung zu erstellen.

Für VMware-Workloads wird hierdurch der lokale Snapshot auf den Datenspeichern oder VMs auf dem primären Speichersystem konfiguriert.

Erstellen einer lokalen Snapshot-Richtlinie

Geben Sie Informationen zum lokalen Snapshot 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.
- **Protokollsicherung aktivieren**: (Gilt nur für Microsoft SQL Server-Workloads und Oracle Database-Workloads.) Aktivieren Sie diese Option, um Protokolle zu sichern und die Häufigkeit und Aufbewahrung der Protokollsicherungen festzulegen. Dazu müssen Sie bereits eine Protokollsicherung konfiguriert haben. Sehen"Konfigurieren von Protokollverzeichnissen" .
  - **Archivprotokolle nach der Sicherung bereinigen**: (Nur Oracle-Datenbank-Workloads) Wenn Protokollsicherungen aktiviert sind, können Sie diese Funktion optional aktivieren, um zu begrenzen, wie lange Backup and Recovery Oracle-Archivprotokolle aufbewahrt. Sie können den Aufbewahrungszeitraum sowie den Ort auswählen, an dem Backup and Recovery die Archivprotokolle löschen soll.
- **Anbieter**: (Nur Kubernetes-Workloads) Wählen Sie den Speicheranbieter aus, der die Kubernetes-Anwendungsressourcen hostet.

Erstellen Sie eine Richtlinie für sekundäre Einstellungen (Replikation auf sekundären Speicher).

Geben Sie Informationen zur Replikation auf den Sekundärspeicher an. Zeitplaninformationen aus den lokalen Snapshot-Einstellungen werden Ihnen in den sekundären Einstellungen angezeigt. Diese Einstellungen sind für Kubernetes-Workloads nicht verfügbar.

- **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.
- **Snapshot-Sperre aktivieren**: Wählen Sie aus, ob Sie manipulationssichere Snapshots aktivieren möchten.
- **Sperrzeitraum für Snapshots**: Geben Sie die Anzahl der Tage, Monate oder Jahre ein, für die Sie den Snapshot sperren möchten.
- **Wechsel zur weiterführenden Schule**:
  - Die Option * ONTAP Übertragungsplan – Inline* ist standardmäßig ausgewählt und gibt an, dass Snapshots sofort auf das sekundäre Speichersystem übertragen werden. Sie müssen die Sicherung nicht planen.

    - Weitere Optionen: Wenn Sie eine aufgeschobene Überweisung wählen, erfolgen die Überweisungen nicht sofort und Sie können einen Zeitplan festlegen.
- * Sekundäre Beziehung zwischen SnapMirror und SnapVault SMAS*: Verwenden Sie sekundäre Beziehungen zwischen SnapMirror und SnapVault SMAS für SQL Server-Workloads.

Erstellen einer Richtlinie für Objektspeichereinstellungen

Geben Sie Informationen für die Sicherung im Objektspeicher an. Diese Einstellungen werden als „Sicherungseinstellungen“ für Kubernetes-Workloads bezeichnet.

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

Erstellen einer Richtlinie für AWS-Objektspeicher

Geben Sie Informationen in die folgenden Felder ein:

- **Anbieter**: Wählen Sie **AWS**.
- **AWS-Konto**: Wählen Sie das AWS-Konto aus.
- **Sicherungsziel**: Wählen Sie ein registriertes S3-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.
- **Integritätsscan aktivieren**: (Nicht verfügbar für Kubernetes-Workloads) Wählen Sie aus, ob Sie Integritätsscans (Snapshot-Sperre) im Objektspeicher aktivieren möchten. Dadurch wird sichergestellt, dass die Sicherungen gültig sind und erfolgreich wiederhergestellt werden können. Die Häufigkeit des Integritätsscans ist standardmäßig auf 7 Tage eingestellt. Um Ihre Backups vor Änderungen oder Löschungen zu schützen, wählen Sie die Option **Integritätsscan**. Der Scan erfolgt nur für den neuesten Snapshot. Sie können Integritätsscans für den neuesten Snapshot aktivieren oder deaktivieren.

Erstellen einer Richtlinie für Microsoft Azure-Objektspeicher

Geben Sie Informationen in die folgenden Felder ein:

- **Anbieter**: Wählen Sie **Azure**.
- **Azure-Abonnement**: Wählen Sie das erkannte Azure-Abonnement aus.
- **Azure-Ressourcengruppe**: Wählen Sie die Azure-Ressourcengruppe aus den erkannten aus.
- **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 aufstufen möchten, wählen Sie die Stufenoption und die Anzahl der Tage für die Archivierung aus.
- **Integritätsscan aktivieren**: (Nicht verfügbar für Kubernetes-Workloads) Wählen Sie aus, ob Sie Integritätsscans (Snapshot-Sperre) im Objektspeicher aktivieren möchten. Dadurch wird sichergestellt, dass die Sicherungen gültig sind und erfolgreich wiederhergestellt werden können. Die Häufigkeit des Integritätsscans ist standardmäßig auf 7 Tage eingestellt. Um Ihre Backups vor Änderungen oder Löschungen zu schützen, wählen Sie die Option **Integritätsscan**. Der Scan erfolgt nur für den neuesten Snapshot. Sie können Integritätsscans für den neuesten Snapshot aktivieren oder deaktivieren.

Erstellen einer Richtlinie für den StorageGRID Objektspeicher

Geben Sie Informationen in die folgenden Felder ein:

- **Anbieter**: Wählen Sie * StorageGRID*.
- * StorageGRID -Anmeldeinformationen*: Wählen Sie die StorageGRID -Anmeldeinformationen aus den erkannten aus. Diese Anmeldeinformationen werden für den Zugriff auf das StorageGRID Objektspeichersystem verwendet und wurden in der Option „Einstellungen“ eingegeben.
- **Sicherungsziel**: Wählen Sie ein registriertes S3-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 Snapshots ein, die für jede Frequenz aufbewahrt werden sollen.
- **Übertragungsplan für Objektspeicher**: (Nicht verfügbar für Kubernetes-Workloads) Wählen Sie den ONTAP Übertragungsplan, um Daten im Objektspeicher zu sichern.
- **Integritätsscan aktivieren**: (Nicht verfügbar für Kubernetes-Workloads) Wählen Sie aus, ob Sie Integritätsscans (Snapshot-Sperre) im Objektspeicher aktivieren möchten. Dadurch wird sichergestellt, dass die Sicherungen gültig sind und erfolgreich wiederhergestellt werden können. Die Häufigkeit des Integritätsscans ist standardmäßig auf 7 Tage eingestellt. Um Ihre Backups vor Änderungen oder Löschungen zu schützen, wählen Sie die Option **Integritätsscan**. Der Scan erfolgt nur für den neuesten Snapshot. Sie können Integritätsscans für den neuesten Snapshot aktivieren oder deaktivieren.
- **Stufen Sie Ihre Backups vom Objektspeicher in den Archivspeicher auf**: (Nicht verfügbar für Kubernetes-Workloads) Wenn Sie Backups in den Archivspeicher aufstufen möchten, wählen Sie die Stufenoption und die Anzahl der Tage für die Archivierung aus.

Konfigurieren Sie erweiterte Einstellungen in der Richtlinie

Optional können Sie erweiterte Einstellungen in der Richtlinie konfigurieren. Diese Einstellungen sind für alle Backup-Architekturen verfügbar, einschließlich lokaler Snapshots, Replikation auf sekundären Speicher und Backups auf Objektspeicher. Diese Einstellungen sind für Kubernetes-Workloads nicht verfügbar. Die verfügbaren erweiterten Einstellungen unterscheiden sich je nach der oben auf der Seite ausgewählten Arbeitslast. Daher gelten die hier beschriebenen erweiterten Einstellungen möglicherweise nicht für alle Arbeitslasten. Beim Konfigurieren einer Richtlinie für Kubernetes-Workloads sind erweiterte Einstellungen nicht verfügbar.

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.
3. Wählen Sie im Abschnitt „Richtlinie > Erweitert*-Einstellungen“ das Menü „Erweiterte Aktion auswählen*, um aus einer Liste erweiterter Einstellungen auszuwählen.
4. Aktivieren Sie alle Einstellungen, die Sie anzeigen oder ändern möchten, und wählen Sie dann **Akzeptieren**.
5. Geben Sie die folgenden Informationen an:
   - **Nur Kopie-Backup**: (Gilt nur für Microsoft SQL Server-Workloads) Wählen Sie „Nur Kopie-Backup“ (eine Art Microsoft SQL Server-Backup), wenn Sie Ihre Ressourcen mithilfe einer anderen Backup-Anwendung sichern müssen.
   - **Einstellungen der Verfügbarkeitsgruppe**: (Gilt nur für Microsoft SQL Server-Workloads) Wählen Sie bevorzugte Sicherungsreplikate aus oder geben Sie ein bestimmtes Replikat an. Diese Einstellung ist nützlich, wenn Sie über eine SQL Server-Verfügbarkeitsgruppe verfügen und steuern möchten, welches Replikat für Sicherungen verwendet wird.
   - **Maximale Übertragungsrate**: Um keine Begrenzung der Bandbreitennutzung festzulegen, wählen Sie **Unbegrenzt**. Wenn Sie die Übertragungsrate begrenzen möchten, wählen Sie **Begrenzt** und wählen Sie die Netzwerkbandbreite zwischen 1 und 1.000 Mbit/s aus, die zum Hochladen von Backups in den Objektspeicher zugewiesen ist. Standardmäßig kann ONTAP eine unbegrenzte Bandbreite nutzen, um die Sicherungsdaten von Volumes im System in den Objektspeicher zu übertragen. Wenn Sie feststellen, dass der Sicherungsverkehr die normale Arbeitslast der Benutzer beeinträchtigt, sollten Sie die während der Übertragung verwendete Netzwerkbandbreite verringern.
   - **Sicherungswiederholungen**: (Gilt nicht für VMware-Workloads) Um den Job im Falle eines Fehlers oder einer Unterbrechung zu wiederholen, wählen Sie **Jobwiederholungen bei Fehler aktivieren**. Geben Sie die maximale Anzahl der Wiederholungsversuche für Snapshot- und Sicherungsaufträge sowie das Wiederholungszeitintervall ein. Die Nachzählung muss weniger als 10 ergeben. Diese Einstellung ist nützlich, wenn Sie sicherstellen möchten, dass der Sicherungsauftrag im Falle eines Fehlers oder einer Unterbrechung wiederholt wird.

     Wenn die Snapshot-Frequenz auf 1 Stunde eingestellt ist, sollte die maximale Verzögerung zusammen mit der Anzahl der Wiederholungsversuche 45 Minuten nicht überschreiten.

   - **VM-konsistente Snapshots aktivieren**: Wählen Sie aus, ob Sie VM-konsistente Snapshots aktivieren möchten. Dadurch wird sichergestellt, dass die neu erstellten Snapshots mit dem Zustand der virtuellen Maschine zum Zeitpunkt des Snapshots übereinstimmen. Dies ist nützlich, um sicherzustellen, dass die Backups erfolgreich wiederhergestellt werden können und dass sich die Daten in einem konsistenten Zustand befinden. Dies gilt nicht für bereits existierende Snapshots.
   - **Ransomware-Scan**: Wählen Sie aus, ob Sie den Ransomware-Scan für jeden Bucket aktivieren möchten. Dies erfordert eine DataLock-Sperre auf dem Objektspeicher. Geben Sie die Häufigkeit des

Scans in Tagen ein. Diese Option gilt für AWS- und Microsoft Azure-Objektspeicher. Beachten Sie, dass für diese Option je nach Cloud-Anbieter zusätzliche Kosten anfallen können.

- **Sicherungsüberprüfung**: (Gilt nicht für VMware-Workloads) Wählen Sie aus, ob Sie die Sicherungsüberprüfung aktivieren möchten und ob Sie diese sofort oder später durchführen möchten. Diese Funktion stellt sicher, dass die Sicherungen gültig sind und erfolgreich wiederhergestellt werden können. Wir empfehlen Ihnen, diese Option zu aktivieren, um die Integrität Ihrer Backups zu gewährleisten. Standardmäßig wird die Sicherungsüberprüfung vom Sekundärspeicher ausgeführt, wenn ein Sekundärspeicher konfiguriert ist. Wenn kein sekundärer Speicher konfiguriert ist, wird die Sicherungsüberprüfung vom primären Speicher aus ausgeführt.

  Konfigurieren Sie zusätzlich die folgenden Optionen:

  - **Tägliche**, **Wöchentliche**, **Monatliche** oder **Jährliche** Überprüfung: Wenn Sie **Später** als Sicherungsüberprüfung gewählt haben, wählen Sie die Häufigkeit der Sicherungsüberprüfung aus. Dadurch wird sichergestellt, dass Backups regelmäßig auf Integrität geprüft werden und erfolgreich wiederhergestellt werden können.
  - **Sicherungsbezeichnungen**: Geben Sie eine Bezeichnung für die Sicherung ein. Dieses Label dient zur Identifizierung des Backups im System und kann für die Verfolgung und Verwaltung von Backups nützlich sein.
  - **Datenbankkonsistenzprüfung**: (Gilt nicht für VMware-Workloads) Wählen Sie aus, ob Sie Datenbankkonsistenzprüfungen aktivieren möchten. Diese Option stellt sicher, dass sich die Datenbanken vor der Sicherung in einem konsistenten Zustand befinden, was für die Gewährleistung der Datenintegrität von entscheidender Bedeutung ist.
  - **Protokollsicherungen überprüfen**: (Gilt nicht für VMware-Workloads) Wählen Sie aus, ob Sie Protokollsicherungen überprüfen möchten. Wählen Sie den Verifizierungsserver aus. Wenn Sie Disk-to-Disk oder 3-2-1 gewählt haben, wählen Sie auch den Speicherort für die Überprüfung aus. Diese Option stellt sicher, dass die Protokollsicherungen gültig sind und erfolgreich wiederhergestellt werden können, was für die Aufrechterhaltung der Integrität Ihrer Datenbanken wichtig ist.
- **Netzwerk**: Wählen Sie die Netzwerkschnittstelle aus, die für die Sicherungsvorgänge verwendet werden soll. Dies ist nützlich, wenn Sie über mehrere Netzwerkschnittstellen verfügen und steuern möchten, welche für Sicherungen verwendet wird.
  - **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.
  - **Konfiguration des privaten Endpunkts**: Wenn Sie einen privaten Endpunkt für Ihren Objektspeicher verwenden, wählen Sie die private Endpunktkonfiguration aus, die für die Sicherungsvorgänge verwendet werden soll. Dies ist nützlich, wenn Sie sicherstellen möchten, dass die Sicherungen sicher über eine private Netzwerkverbindung übertragen werden.
- **Benachrichtigung**: Wählen Sie aus, ob Sie E-Mail-Benachrichtigungen für Sicherungsvorgänge aktivieren möchten. Dies ist nützlich, wenn Sie benachrichtigt werden möchten, wenn ein Sicherungsvorgang beginnt, abgeschlossen wird oder fehlschlägt.
- **Unabhängige Datenträger**: (Gilt nur für VMware-Workloads) Aktivieren Sie diese Option, um alle Datenspeicher mit unabhängigen Datenträgern, die temporäre Daten enthalten, in die Sicherung einzuschließen. Eine unabhängige Festplatte ist eine VM-Festplatte, die nicht in VMware-Snapshots enthalten ist.
- * SnapMirror -Volume und Snapshot-Format*: Geben Sie optional Ihren eigenen Snapshot-Namen in eine Richtlinie ein, die die Backups für Microsoft SQL Server-Workloads regelt. Geben Sie das Format und den benutzerdefinierten Text ein. Wenn Sie sich für die Sicherung auf einem sekundären Speicher entschieden haben, können Sie auch ein SnapMirror -Volume-Präfix und -Suffix hinzufügen.

Bearbeiten einer Richtlinie

Sie können die Sicherungsarchitektur, die Sicherungshäufigkeit, die Aufbewahrungsrichtlinie und andere Einstellungen für eine Richtlinie 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**.

Schützen Sie ONTAP Volume-Workloads

Schützen Sie Ihre ONTAP Volume-Daten mit NetApp Backup and Recovery

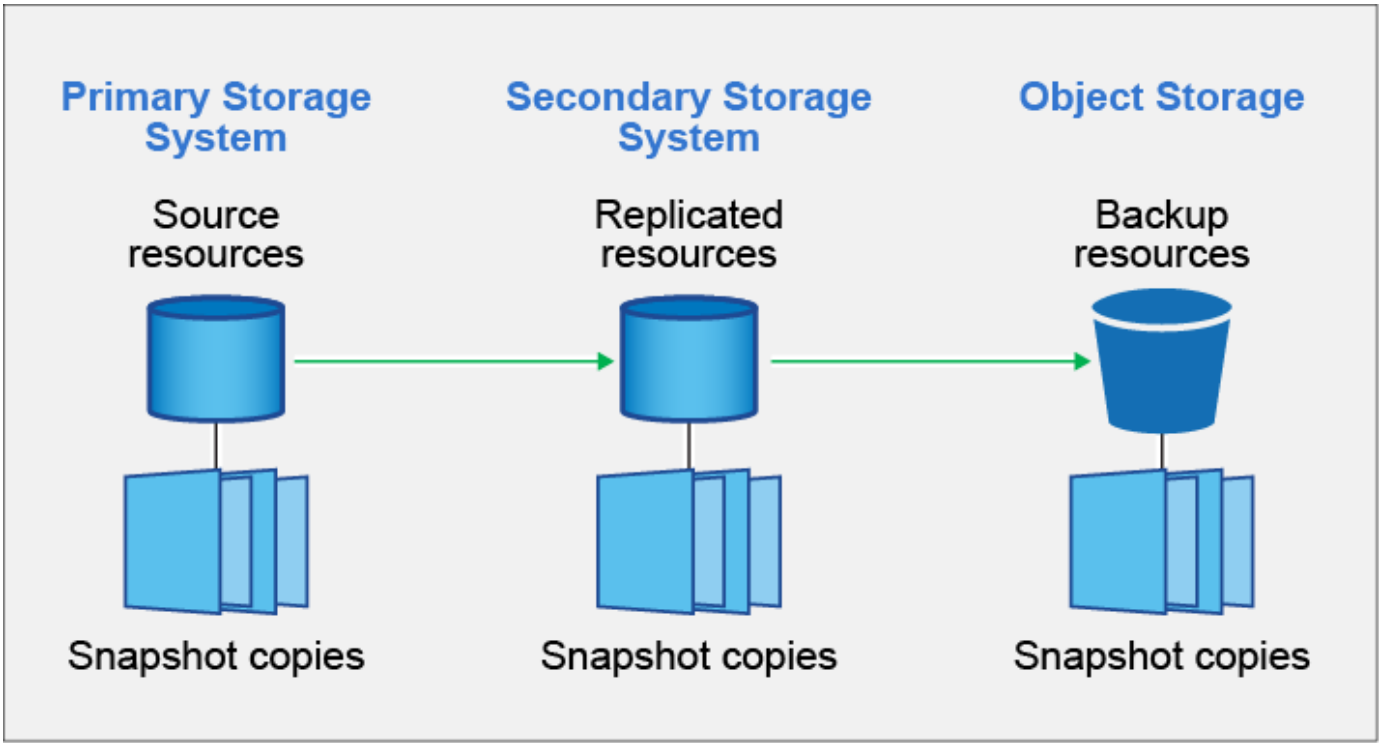
NetApp Backup and Recovery bietet Sicherungs- und Wiederherstellungsfunktionen zum Schutz und zur langfristigen Archivierung Ihrer ONTAP Volume-Daten. Sie können eine 3-2-1-Strategie implementieren, bei der Sie 3 Kopien Ihrer Quelldaten auf 2 verschiedenen

Speichersystemen und 1 Kopie in der Cloud haben.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

Nach der Aktivierung erstellt Backup und Recovery inkrementelle Backups auf Blockebene, die dauerhaft auf einem anderen ONTAP Cluster und im Objektspeicher in der Cloud gespeichert werden. Zusätzlich zu Ihrem Quellvolumen verfügen Sie über:

- Momentaufnahme des Volumens auf dem Quellsystem
- Repliziertes Volume auf einem anderen Speichersystem
- Sicherung des Volumes im Objektspeicher



NetApp Backup and Recovery nutzt die SnapMirror -Datenreplikationstechnologie von NetApp, um sicherzustellen, dass alle Backups vollständig synchronisiert werden, indem Snapshots erstellt und an die Backup-Speicherorte übertragen werden.

Zu den Vorteilen des 3-2-1-Ansatzes gehören:

- Mehrere Datenkopien schützen vor internen und externen Cybersicherheitsbedrohungen.
- Die Verwendung unterschiedlicher Medientypen erleichtert Ihnen die Wiederherstellung, wenn ein Typ ausfällt.
- Sie können die Wiederherstellung schnell von der Vor-Ort-Kopie durchführen und die Offsite-Kopien verwenden, wenn die Vor-Ort-Kopie kompromittiert ist.

Bei Bedarf können Sie ein ganzes *Volume*, einen *Ordner* oder eine oder mehrere *Dateien* aus einer der Sicherungskopien auf demselben oder einem anderen System wiederherstellen.

Features

Replikationsfunktionen:

- Replizieren Sie Daten zwischen ONTAP -Speichersystemen, um Backup und Disaster Recovery zu unterstützen.
- Stellen Sie die Zuverlässigkeit Ihrer DR-Umgebung mit hoher Verfügbarkeit sicher.
- Native ONTAP -In-Flight-Verschlüsselung über Pre-Shared Key (PSK) zwischen den beiden Systemen eingerichtet.
- Kopierte Daten sind unveränderlich, bis Sie sie beschreibbar und einsatzbereit machen.
- Bei einem Übertragungsfehler ist die Replikation selbstheilend.
- Im Vergleich zu "NetApp Replication" Die Replikation in NetApp Backup and Recovery umfasst die folgenden Funktionen:
  - Replizieren Sie mehrere FlexVol -Volumes gleichzeitig auf ein sekundäres System.
  - Stellen Sie ein repliziertes Volume mithilfe der Benutzeroberfläche auf dem Quellsystem oder einem anderen System wieder her.

Sehen"Replikationsbeschränkungen für ONTAP -Volumes" für eine Liste der Replikationsfunktionen, die bei NetApp Backup and Recovery für ONTAP -Volumes nicht verfügbar sind.

Backup-to-Object-Funktionen:

- Sichern Sie unabhängige Kopien Ihrer Datenmengen auf kostengünstigem Objektspeicher.
- Wenden Sie eine einzige Sicherungsrichtlinie auf alle Volumes in einem Cluster an oder weisen Sie Volumes mit eindeutigen Wiederherstellungspunktzielen unterschiedliche Sicherungsrichtlinien zu.
- Erstellen Sie eine Sicherungsrichtlinie, die auf alle zukünftigen im Cluster erstellten Volumes angewendet werden soll.
- Erstellen Sie unveränderliche Sicherungsdateien, damit diese für die Dauer der Aufbewahrungsfrist gesperrt und geschützt sind.
- Scannen Sie Sicherungsdateien auf mögliche Ransomware-Angriffe – und entfernen/ersetzen Sie infizierte Sicherungen automatisch.
- Um Kosten zu sparen, verschieben Sie ältere Sicherungsdateien in den Archivspeicher.
- Löschen Sie die Sicherungsbeziehung, damit Sie nicht benötigte Quellvolumes archivieren und gleichzeitig Volumesicherungen beibehalten können.
- Sichern Sie von Cloud zu Cloud und von lokalen Systemen in die öffentliche oder private Cloud.
- Sicherungsdaten werden im Ruhezustand mit AES-256-Bit-Verschlüsselung und während der Übertragung mit TLS 1.2 HTTPS-Verbindungen gesichert.
- Verwenden Sie zur Datenverschlüsselung Ihre eigenen, vom Kunden verwalteten Schlüssel, anstatt die Standardverschlüsselungsschlüssel Ihres Cloud-Anbieters zu verwenden.
- Unterstützung für bis zu 4.000 Backups eines einzelnen Volumes.

Funktionen wiederherstellen:

- Daten von einem bestimmten Zeitpunkt aus lokalen Snapshots, replizierten Volumes oder gesicherten Volumes im Objektspeicher wiederherstellen.
- Stellen Sie ein Volume, einen Ordner oder einzelne Dateien auf dem Quellsystem oder einem anderen System wieder her.

- Stellen Sie Daten auf einem System wieder her, das ein anderes Abonnement/Konto verwendet oder sich in einer anderen Region befindet.
- Führen Sie eine *schnelle Wiederherstellung* eines Volumes aus dem Cloud-Speicher auf ein Cloud Volumes ONTAP -System oder auf ein lokales System durch. Ideal für Disaster-Recovery-Situationen, in denen Sie schnellstmöglich Zugriff auf ein Volume bereitstellen müssen.
- Stellen Sie Daten auf Blockebene wieder her und platzieren Sie die Daten direkt an dem von Ihnen angegebenen Speicherort, wobei die ursprünglichen ACLs erhalten bleiben.
- Durchsuchen Sie Dateikataloge, um einzelne Ordner und Dateien für die Wiederherstellung einzelner Dateien einfach auszuwählen.

Unterstützte Systeme für Sicherungs- und Wiederherstellungsvorgänge

NetApp Backup and Recovery unterstützt ONTAP -Systeme sowie öffentliche und private Cloud-Anbieter.

Unterstützte Regionen

NetApp Backup and Recovery wird mit Cloud Volumes ONTAP in vielen Amazon Web Services-, Microsoft Azure- und Google Cloud-Regionen unterstützt.

"Erfahren Sie mehr mit der globalen Regionskarte"

Unterstützte Sicherungsziele

NetApp Backup and Recovery ermöglicht die Sicherung von ONTAP Volumes von den folgenden Quellsystemen auf die folgenden Sekundärsysteme und Objektspeicher bei öffentlichen und privaten Cloud-Anbietern. Die Snapshots werden auf dem Quellsystem gespeichert.

Quellsystem	Sekundärsystem (Replikation)	Zielobjektspeicher (Backup)
Cloud Volumes ONTAP in AWS	Cloud Volumes ONTAP in AWS On-Premises- ONTAP -System	Amazon S3
Cloud Volumes ONTAP in Azure	Cloud Volumes ONTAP in Azure On-Premises- ONTAP -System	Azure-Blob
Cloud Volumes ONTAP in Google	Cloud Volumes ONTAP im lokalen ONTAP -System von Google	Google Cloud-Speicher
On-Premises- ONTAP -System	Cloud Volumes ONTAP On-Premises ONTAP -System	Amazon S3, Azure Blob, Google Cloud Storage, NetApp StorageGRID ONTAP S3

Unterstützte Wiederherstellungsziele

ONTAP Daten können aus einer Sicherungsdatei, die sich auf einem sekundären System (einem replizierten Volume) oder im Objektspeicher (einer Sicherungsdatei) befindet, auf den folgenden Systemen wiederhergestellt werden. Snapshots befinden sich auf dem Quellsystem und können nur auf demselben System wiederhergestellt werden.

Speicherort der Sicherungsdatei		Zielsystem
Objektspeicher (Backup)	**Sekundäres System (Replikation)**	
Amazon S3	Cloud Volumes ONTAP in AWS On-Premises- ONTAP -System	Cloud Volumes ONTAP in AWS On-Premises- ONTAP -System

Speicherort der Sicherungsdatei		Zielsystem
Azure-Blob	Cloud Volumes ONTAP in Azure On-Premises- ONTAP -System	Cloud Volumes ONTAP in Azure On-Premises- ONTAP -System
Google Cloud-Speicher	Cloud Volumes ONTAP im lokalen ONTAP -System von Google	Cloud Volumes ONTAP im lokalen ONTAP -System von Google
NetApp StorageGRID	On-Premises- ONTAP -System Cloud Volumes ONTAP	On-Premises- ONTAP -System
ONTAP S3	On-Premises- ONTAP -System Cloud Volumes ONTAP	On-Premises- ONTAP -System

Beachten Sie, dass Verweise auf „On-Premises ONTAP Systeme“ FAS, AFF und ONTAP Select Systeme umfassen.

Unterstützte Volumes

NetApp Backup and Recovery unterstützt die folgenden Volumetypen:

- FlexVol Lese-/Schreib-Volumes
- FlexGroup Volumes (erfordert ONTAP 9.12.1 oder höher)
- SnapLock Enterprise Volumes (erfordert ONTAP 9.11.1 oder höher)
- SnapLock Compliance für lokale Volumes (erfordert ONTAP 9.14 oder höher)
- SnapMirror -Datenschutzzielvolumes (DP)

NetApp Backup and Recovery unterstützt keine Sicherungen von FlexCache -Volumes.

Siehe die Abschnitte zu"Einschränkungen bei der Sicherung und Wiederherstellung von ONTAP -Volumes" für zusätzliche Anforderungen und Einschränkungen.

Kosten

Mit der Verwendung von NetApp Backup and Recovery mit ONTAP -Systemen sind zwei Arten von Kosten verbunden: Ressourcengebühren und Servicegebühren. Beide Gebühren gelten für den Objekt-Backup-Teil des Dienstes.

Für die Erstellung von Snapshots oder replizierten Volumes fallen keine Gebühren an – außer dem Speicherplatz, der zum Speichern der Snapshots und replizierten Volumes benötigt wird.

Ressourcenkosten

Für die Objektspeicherkapazität und für das Schreiben und Lesen von Sicherungsdateien in der Cloud werden Ressourcengebühren an den Cloud-Anbieter gezahlt.

- Für die Sicherung auf Objektspeicher zahlen Sie Ihrem Cloud-Anbieter die Kosten für den Objektspeicher.

  Da NetApp Backup and Recovery die Speichereffizienz des Quellvolumes beibehält, zahlen Sie dem Cloud-Anbieter die Objektspeicherkosten für die Daten *nach* der ONTAP Effizienz (für die geringere Datenmenge nach Anwendung von Deduplizierung und Komprimierung).

- Für die Wiederherstellung von Daten mit Search & Restore werden bestimmte Ressourcen von Ihrem Cloud-Anbieter bereitgestellt. Außerdem fallen Kosten pro TiB an, die sich nach der Datenmenge richten,

die von Ihren Suchanfragen gescannt wird. (Diese Ressourcen werden für Browse & Restore nicht benötigt.)

  - In AWS, "Amazon Athena" Und "AWS Glue" Ressourcen werden in einem neuen S3-Bucket bereitgestellt.
  - In Azure "Azure Synapse-Arbeitsbereich" Und "Azure Data Lake-Speicher" werden in Ihrem Speicherkonto bereitgestellt, um Ihre Daten zu speichern und zu analysieren.
  - Bei Google wird ein neuer Bucket bereitgestellt und der "Google Cloud BigQuery-Dienste" werden auf Konto-/Projektebene bereitgestellt.

- Wenn Sie Volumedaten aus einer Sicherungsdatei wiederherstellen möchten, die in einen Archivobjektspeicher verschoben wurde, fällt beim Cloud-Anbieter eine zusätzliche Abrufgebühr pro GiB und pro Anforderung an.
- Wenn Sie während der Wiederherstellung von Volumedaten eine Sicherungsdatei auf Ransomware scannen möchten (sofern Sie DataLock und Ransomware Resilience für Ihre Cloud-Sicherungen aktiviert haben), entstehen Ihnen auch bei Ihrem Cloud-Anbieter zusätzliche Kosten für den Datenverkehr.

Servicegebühren

Servicegebühren werden an NetApp gezahlt und decken sowohl die Kosten für das Erstellen von Backups im Objektspeicher als auch für das Wiederherstellen von Volumes oder Dateien aus diesen Backups ab. Sie zahlen nur für die Daten, die Sie im Objektspeicher schützen. Die Berechnung erfolgt anhand der logisch genutzten Quellkapazität (*vor* ONTAP -Effizienz) der ONTAP -Volumes, die im Objektspeicher gesichert werden. Diese Kapazität wird auch als Front-End-Terabyte (FETB) bezeichnet.

Es gibt drei Möglichkeiten, für den Backup-Dienst zu bezahlen. Die erste Möglichkeit besteht darin, ein Abonnement bei Ihrem Cloud-Anbieter abzuschließen, bei dem Sie monatlich zahlen können. Die zweite Möglichkeit besteht darin, einen Jahresvertrag abzuschließen. Die dritte Möglichkeit besteht darin, Lizenzen direkt von NetApp zu erwerben.

Lizenzierung

NetApp Backup and Recovery ist mit den folgenden Verbrauchsmodellen verfügbar:

- **BYOL**: Eine von NetApp erworbene Lizenz, die bei jedem Cloud-Anbieter verwendet werden kann.
- **PAYGO**: Ein stündliches Abonnement vom Marktplatz Ihres Cloud-Anbieters.
- **Jährlich**: Ein Jahresvertrag vom Marktplatz Ihres Cloud-Anbieters.

Eine Backup-Lizenz ist nur für die Sicherung und Wiederherstellung aus dem Objektspeicher erforderlich. Für die Erstellung von Snapshots und replizierten Volumes ist keine Lizenz erforderlich.

Bringen Sie Ihre eigene Lizenz mit

BYOL ist laufzeitbasiert (1, 2 oder 3 Jahre) und kapazitätsbasiert in 1-TiB-Schritten. Sie zahlen NetApp für die Nutzung des Dienstes für einen bestimmten Zeitraum, beispielsweise 1 Jahr, und für eine maximale Kapazität, beispielsweise 10 TiB.

Sie erhalten eine Seriennummer, die Sie in der NetApp Console eingeben, um den Dienst zu aktivieren. Wenn eines der Limits erreicht ist, müssen Sie die Lizenz erneuern. Die Backup-BYOL-Lizenz gilt für alle Quellsysteme, die mit Ihrer NetApp Console -Organisation oder Ihrem NetApp Console-Konto verknüpft sind.

"Erfahren Sie, wie Sie Ihre BYOL-Lizenzen verwalten".

Pay-as-you-go-Abonnement

NetApp Backup and Recovery bietet verbrauchsbasierte Lizenzierung in einem Pay-as-you-go-Modell. Nachdem Sie das Abonnement über den Marktplatz Ihres Cloud-Anbieters abgeschlossen haben, zahlen Sie pro GiB für die gesicherten Daten – es ist keine Vorauszahlung erforderlich. Die Abrechnung erfolgt durch Ihren Cloud-Anbieter über Ihre monatliche Rechnung.

"Erfahren Sie, wie Sie ein Pay-as-you-go-Abonnement einrichten".

Beachten Sie, dass bei der ersten Anmeldung mit einem PAYGO-Abonnement eine 30-tägige kostenlose Testversion verfügbar ist.

Jahresvertrag

Wenn Sie AWS verwenden, stehen Ihnen zwei Jahresverträge mit einer Laufzeit von 1, 2 oder 3 Jahren zur Verfügung:

- Ein „Cloud Backup“-Plan, mit dem Sie Cloud Volumes ONTAP -Daten und lokale ONTAP -Daten sichern können.
- Ein „CVO Professional“-Plan, der es Ihnen ermöglicht, Cloud Volumes ONTAP und NetApp Backup and Recovery zu bündeln. Dies umfasst unbegrenzte Backups für Cloud Volumes ONTAP Volumes, die dieser Lizenz in Rechnung gestellt werden (die Backup-Kapazität wird nicht auf die Lizenz angerechnet).

Wenn Sie Azure verwenden, stehen Ihnen zwei Jahresverträge mit einer Laufzeit von 1, 2 oder 3 Jahren zur Verfügung:

- Ein „Cloud Backup“-Plan, mit dem Sie Cloud Volumes ONTAP -Daten und lokale ONTAP -Daten sichern können.
- Ein „CVO Professional“-Plan, der es Ihnen ermöglicht, Cloud Volumes ONTAP und NetApp Backup and Recovery zu bündeln. Dies umfasst unbegrenzte Backups für Cloud Volumes ONTAP Volumes, die dieser Lizenz in Rechnung gestellt werden (die Backup-Kapazität wird nicht auf die Lizenz angerechnet).

Wenn Sie GCP verwenden, können Sie ein privates Angebot von NetApp anfordern und dann den Plan auswählen, wenn Sie während der Aktivierung von NetApp Backup and Recovery ein Abonnement im Google Cloud Marketplace abschließen.

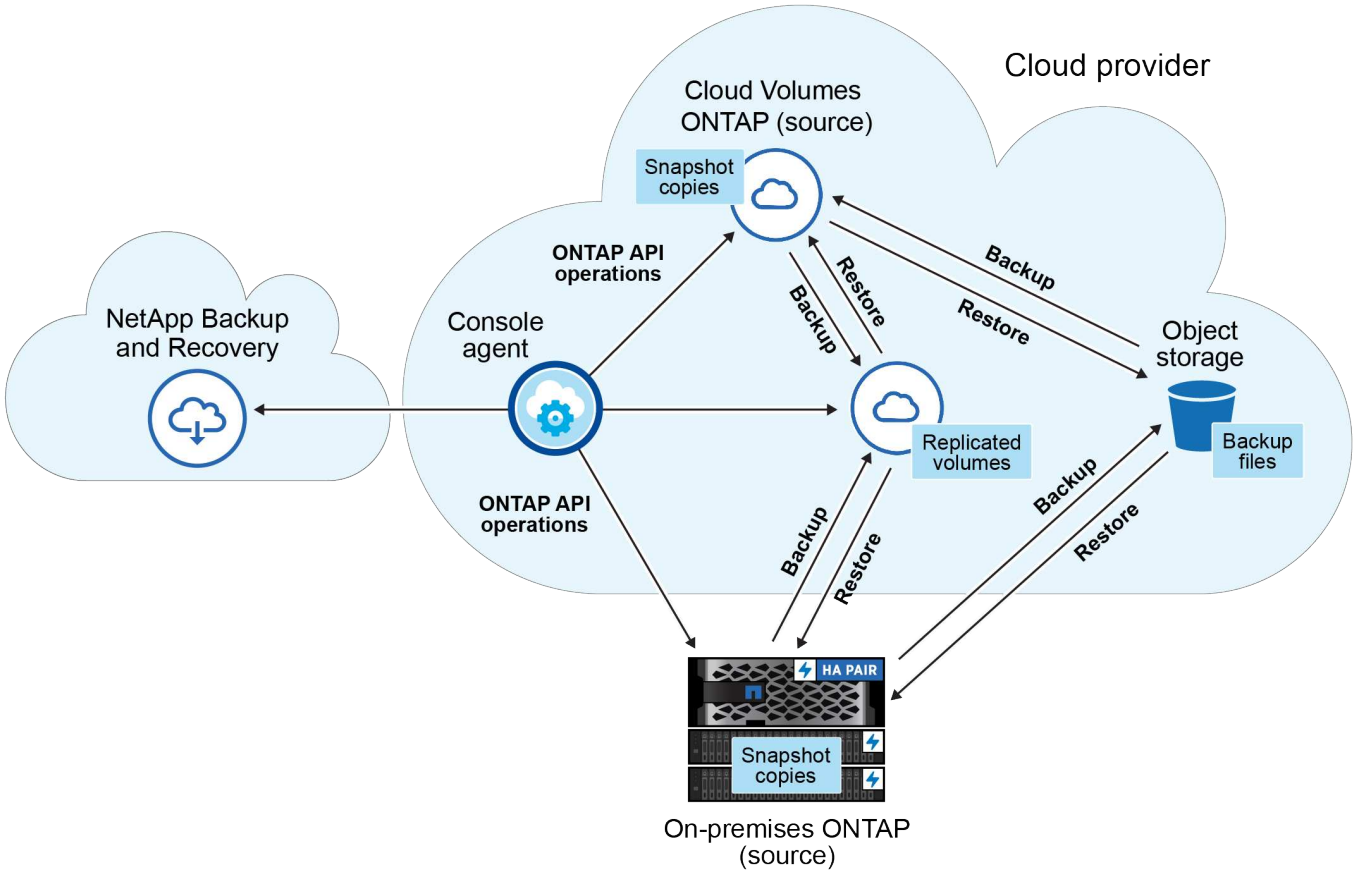
"Erfahren Sie, wie Sie Jahresverträge abschließen".

So funktioniert NetApp Backup and Recovery

Wenn Sie NetApp Backup and Recovery auf einem Cloud Volumes ONTAP oder On-Premises ONTAP -System aktivieren, führt der Dienst eine vollständige Sicherung Ihrer Daten durch. Nach der ersten Sicherung sind alle weiteren Sicherungen inkrementell, d. h. es werden nur geänderte und neue Blöcke gesichert. Dadurch wird der Netzwerkverkehr auf ein Minimum reduziert. Die Sicherung auf Objektspeicher basiert auf "NetApp SnapMirror Cloud-Technologie" .

> Alle Aktionen, die Sie direkt aus der Umgebung Ihres Cloud-Anbieters ausführen, um Cloud-Sicherungsdateien zu verwalten oder zu ändern, können die Dateien beschädigen und zu einer nicht unterstützten Konfiguration führen.

Das folgende Bild zeigt die Beziehung zwischen den einzelnen Komponenten:



Dieses Diagramm zeigt, wie Volumes auf ein Cloud Volumes ONTAP -System repliziert werden. Volumes könnten jedoch auch auf ein lokales ONTAP System repliziert werden.

Wo sich die Backups befinden

Je nach Sicherungstyp befinden sich die Sicherungen an unterschiedlichen Speicherorten:

- *Snapshots* befinden sich auf dem Quellvolume im Quellsystem.
- *Replizierte Volumes* befinden sich auf dem sekundären Speichersystem – einem Cloud Volumes ONTAP oder On-Premises ONTAP -System.
- *Sicherungskopien* werden in einem Objektspeicher gespeichert, den die Konsole in Ihrem Cloud-Konto erstellt. Es gibt einen Objektspeicher pro Cluster/System und die Konsole benennt den Objektspeicher wie folgt: „netapp-backup-clusteruuid“. Denken Sie daran, diesen Objektspeicher nicht zu löschen.
  - In AWS ermöglicht die Konsole Folgendes: "Amazon S3-Funktion „Öffentlichen Zugriff blockieren“" auf dem S3-Bucket.
  - In Azure verwendet die Konsole eine neue oder vorhandene Ressourcengruppe mit einem Speicherkonto für den Blob-Container. Die Konsole "blockiert den öffentlichen Zugriff auf Ihre Blob-Daten" standardmäßig.
  - In GCP verwendet die Konsole ein neues oder bestehendes Projekt mit einem Speicherkonto für den Google Cloud Storage-Bucket.
  - In StorageGRID verwendet die Konsole ein bestehendes Mandantenkonto für den S3-Bucket.
  - In ONTAP S3 verwendet die Konsole ein vorhandenes Benutzerkonto für den S3-Bucket.

Wenn Sie den Zielobjektspeicher für einen Cluster in Zukunft ändern möchten, müssen Sie"Aufheben der Registrierung von NetApp Backup and Recovery für das System" und aktivieren Sie dann NetApp Backup and

Recovery mit den neuen Cloud-Anbieterinformationen.

Anpassbarer Sicherungszeitplan und Aufbewahrungseinstellungen

Wenn Sie NetApp Backup and Recovery für ein System aktivieren, werden alle ursprünglich ausgewählten Volumes unter Verwendung der von Ihnen ausgewählten Richtlinien gesichert. Sie können separate Richtlinien für Snapshots, replizierte Volumes und Sicherungsdateien auswählen. Wenn Sie bestimmten Volumes mit unterschiedlichen Recovery Point Objectives (RPO) unterschiedliche Sicherungsrichtlinien zuweisen möchten, können Sie zusätzliche Richtlinien für diesen Cluster erstellen und diese Richtlinien den anderen Volumes zuweisen, nachdem NetApp Backup and Recovery aktiviert wurde.

Sie können eine Kombination aus stündlichen, täglichen, wöchentlichen, monatlichen und jährlichen Backups aller Volumes auswählen. Für die Sicherung auf Objekt können Sie auch eine der systemdefinierten Richtlinien auswählen, die Sicherungen und Aufbewahrung für 3 Monate, 1 Jahr und 7 Jahre vorsehen. Richtlinien zum Sicherungsschutz, die Sie mit ONTAP System Manager oder der ONTAP CLI auf dem Cluster erstellt haben, werden ebenfalls als Auswahlmöglichkeiten angezeigt. Dazu gehören Richtlinien, die mit benutzerdefinierten SnapMirror -Labels erstellt wurden.

> Die auf das Volume angewendete Snapshot-Richtlinie muss eine der Bezeichnungen aufweisen, die Sie in Ihrer Replikationsrichtlinie und Ihrer Richtlinie zur Sicherung auf Objekt verwenden. Wenn keine passenden Labels gefunden werden, werden keine Sicherungsdateien erstellt. Wenn Sie beispielsweise wöchentlich replizierte Volumes und Sicherungsdateien erstellen möchten, müssen Sie eine Snapshot-Richtlinie verwenden, die wöchentliche Snapshots erstellt.

Sobald Sie die maximale Anzahl an Backups für eine Kategorie oder ein Intervall erreicht haben, werden ältere Backups entfernt, sodass Sie immer über die aktuellsten Backups verfügen (und veraltete Backups nicht weiterhin Speicherplatz belegen).

> Die Aufbewahrungsdauer für Sicherungen von Datensicherungsvolumes ist dieselbe wie in der SnapMirror Quellbeziehung definiert. Sie können dies bei Bedarf mithilfe der API ändern.

Einstellungen für den Sicherungsdateischutz

Wenn Ihr Cluster ONTAP 9.11.1 oder höher verwendet, können Sie Ihre Backups im Objektspeicher vor Löschung und Ransomware-Angriffen schützen. Jede Sicherungsrichtlinie enthält einen Abschnitt für *DataLock und Ransomware-Resilienz*, der für einen bestimmten Zeitraum – den *Aufbewahrungszeitraum* – auf Ihre Sicherungsdateien angewendet werden kann.

- *DataLock* schützt Ihre Sicherungsdateien vor Änderungen oder Löschungen.
- Der Ransomware-Schutz durchsucht Ihre Sicherungsdateien nach Hinweisen auf einen Ransomware-Angriff, wenn eine Sicherungsdatei erstellt wird und wenn Daten aus einer Sicherungsdatei wiederhergestellt werden.

Geplante Ransomware-Schutzscans sind standardmäßig aktiviert. Die Standardeinstellung für die Scanhäufigkeit beträgt 7 Tage. Der Scan erfolgt nur für den neuesten Snapshot. Um Ihre Kosten zu senken, können die geplanten Scans deaktiviert werden. Sie können geplante Ransomware-Scans für den neuesten Snapshot über die entsprechende Option auf der Seite „Erweiterte Einstellungen“ aktivieren oder deaktivieren. Wenn Sie es aktivieren, werden Scans standardmäßig wöchentlich durchgeführt. Sie können diesen Zeitplan auf Tage oder Wochen ändern oder ihn deaktivieren, um Kosten zu sparen.

Der Aufbewahrungszeitraum für die Sicherung entspricht dem Aufbewahrungszeitraum des Sicherungsplans zuzüglich eines Puffers von maximal 31 Tagen. Beispielsweise wird bei *wöchentlichen* Sicherungen mit *5* aufbewahrten Kopien jede Sicherungsdatei für 5 Wochen gesperrt. Bei *monatlichen* Backups mit *6* aufbewahrten Kopien wird jede Backup-Datei für 6 Monate gesperrt.

Support ist derzeit verfügbar, wenn Ihr Sicherungsziel Amazon S3, Azure Blob oder NetApp StorageGRID ist. In zukünftigen Versionen werden weitere Speicheranbieterziele hinzugefügt.

Weitere Einzelheiten finden Sie in diesen Informationen:

- "So funktionieren DataLock und Ransomware-Schutz".
- "So aktualisieren Sie die Ransomware-Schutzoptionen auf der Seite „Erweiterte Einstellungen“".

DataLock kann nicht aktiviert werden, wenn Sie Sicherungen in Archivspeicher einstufen.

Archivspeicher für ältere Sicherungsdateien

Bei der Verwendung bestimmter Cloud-Speicher können Sie ältere Sicherungsdateien nach einer bestimmten Anzahl von Tagen in eine weniger teure Speicherklasse/Zugriffsebene verschieben. Sie können Ihre Sicherungsdateien auch sofort in den Archivspeicher senden, ohne sie in den Standard-Cloud-Speicher zu schreiben. Beachten Sie, dass der Archivspeicher nicht verwendet werden kann, wenn Sie DataLock aktiviert haben.

- In AWS beginnen Backups in der Speicherklasse *Standard* und wechseln nach 30 Tagen zur Speicherklasse *Standard – seltener Zugriff*.

  Wenn Ihr Cluster ONTAP 9.10.1 oder höher verwendet, können Sie zur weiteren Kostenoptimierung ältere Backups nach einer bestimmten Anzahl von Tagen in der NetApp Backup and Recovery Benutzeroberfläche entweder auf *S3 Glacier*- oder *S3 Glacier Deep Archive*-Speicher verschieben. "Erfahren Sie mehr über AWS-Archivspeicher".

- In Azure sind Sicherungen mit der Zugriffsebene „Cool“ verknüpft.

  Wenn Ihr Cluster ONTAP 9.10.1 oder höher verwendet, können Sie zur weiteren Kostenoptimierung ältere Backups nach einer bestimmten Anzahl von Tagen in der NetApp Backup and Recovery Benutzeroberfläche in den Azure Archive-Speicher verschieben. "Erfahren Sie mehr über Azure-Archivspeicher".

- In GCP sind Backups mit der Speicherklasse *Standard* verknüpft.

  Wenn Ihr Cluster ONTAP 9.12.1 oder höher verwendet, können Sie zur weiteren Kostenoptimierung ältere Backups nach einer bestimmten Anzahl von Tagen in der NetApp Backup and Recovery Benutzeroberfläche in den Archivspeicher verschieben. "Erfahren Sie mehr über den Archivspeicher von Google".

- In StorageGRID sind Backups mit der Speicherklasse *Standard* verknüpft.

  Wenn Ihr On-Prem-Cluster ONTAP 9.12.1 oder höher verwendet und Ihr StorageGRID System 11.4 oder höher verwendet, können Sie ältere Sicherungsdateien nach einer bestimmten Anzahl von Tagen im öffentlichen Cloud-Archivspeicher archivieren. Derzeit wird die Speicherebene AWS S3 Glacier/S3 Glacier Deep Archive oder Azure Archive unterstützt. "Erfahren Sie mehr über das Archivieren von Backup-Dateien von StorageGRID".

Weitere Informationen zum Archivieren älterer Sicherungsdateien finden Sie unter [link:prev-ontap-policy-object-options.html].

Überlegungen zur FabricPool Tiering-Richtlinie

Es gibt bestimmte Dinge, die Sie beachten müssen, wenn sich das Volume, das Sie sichern, auf einem FabricPool Aggregat befindet und ihm eine andere Tiering-Richtlinie zugewiesen ist als `none` :

- Für die erste Sicherung eines FabricPool-Tiered-Volumes müssen alle lokalen und alle Tiered-Daten (aus dem Objektspeicher) gelesen werden. Bei einem Sicherungsvorgang werden die kalten, im Objektspeicher abgelegten Daten nicht „wieder aufgewärmt“.

  Dieser Vorgang kann zu einer einmaligen Kostenerhöhung beim Lesen der Daten von Ihrem Cloud-Anbieter führen.

  - Nachfolgende Sicherungen sind inkrementell und haben diesen Effekt nicht.
  - Wenn die Tiering-Richtlinie dem Volume bei seiner Ersterstellung zugewiesen wird, tritt dieses Problem nicht auf.
- Berücksichtigen Sie die Auswirkungen von Backups, bevor Sie die `all` Tiering-Richtlinie für Volumes. Da die Daten sofort in Tiers aufgeteilt werden, liest NetApp Backup and Recovery die Daten aus der Cloud-Tier-Ebene und nicht aus der lokalen Ebene. Da bei gleichzeitigen Sicherungsvorgängen die Netzwerkverbindung zum Cloud-Objektspeicher gemeinsam genutzt wird, kann es zu Leistungseinbußen kommen, wenn die Netzwerkressourcen überlastet sind. In diesem Fall möchten Sie möglicherweise proaktiv mehrere Netzwerkschnittstellen (LIFs) konfigurieren, um diese Art der Netzwerksättigung zu verringern.

Planen Sie Ihren Schutz mit NetApp Backup and Recovery

Mit NetApp Backup and Recovery können Sie zum Schutz Ihrer Daten bis zu drei Kopien Ihrer Quellvolumes erstellen. Beim Aktivieren der Sicherung und Wiederherstellung auf Ihren Volumes stehen Ihnen zahlreiche Optionen zur Auswahl. Überprüfen Sie daher Ihre Auswahl, damit Sie vorbereitet sind.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

Wir gehen die folgenden Optionen durch:

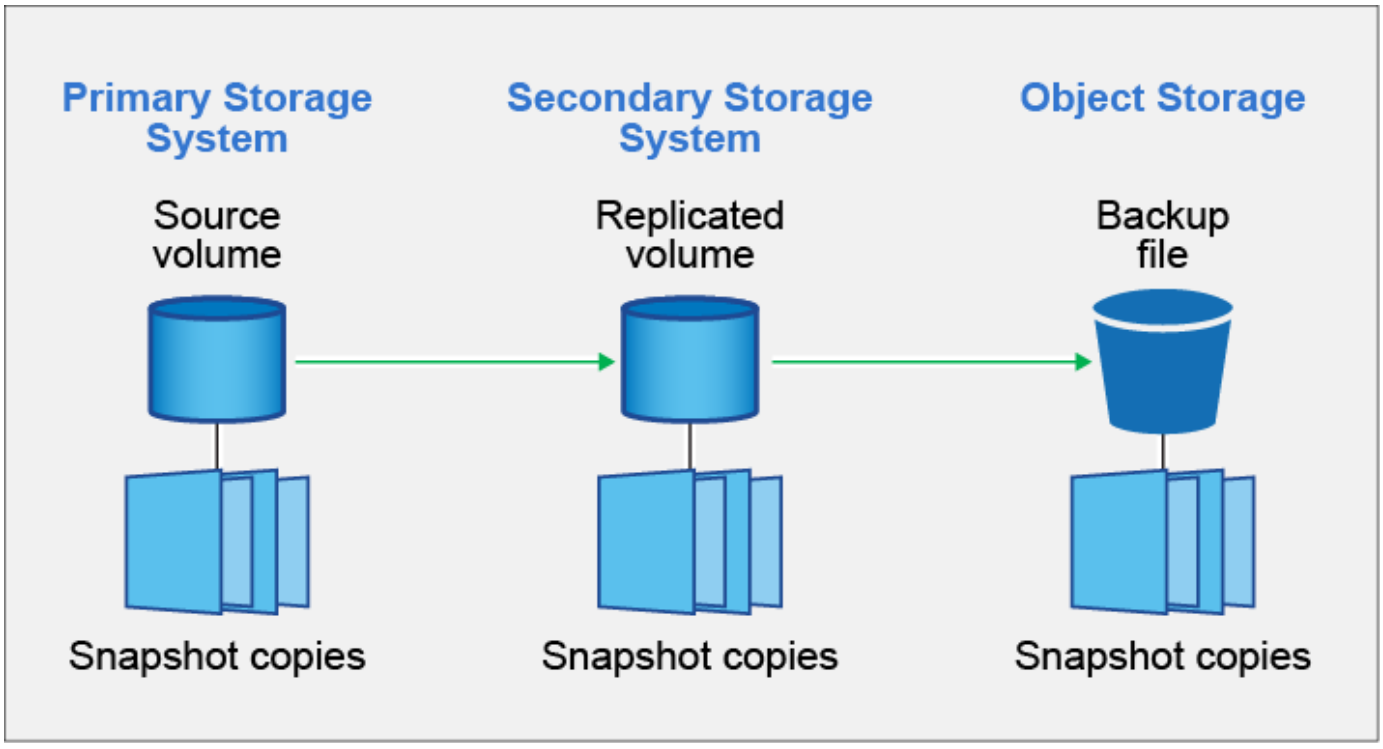
- Welche Schutzfunktionen werden Sie verwenden: Snapshots, replizierte Volumes und/oder Backup in der Cloud?
- Welche Backup-Architektur werden Sie verwenden: ein Kaskaden- oder Fan-Out-Backup Ihrer Volumes
- Werden Sie die Standard-Backup-Richtlinien verwenden oder müssen Sie benutzerdefinierte Richtlinien erstellen?
- Möchten Sie, dass der Dienst die Cloud-Buckets für Sie erstellt, oder möchten Sie Ihre Objektspeichercontainer erstellen, bevor Sie beginnen?
- Welchen Bereitstellungsmodus des Konsolenagenten verwenden Sie (Standard-, eingeschränkter oder privater Modus)?

Welche Schutzfunktionen werden Sie nutzen?

Bevor Sie die Funktionen auswählen, die Sie verwenden möchten, finden Sie hier eine kurze Erklärung, was die einzelnen Funktionen bewirken und welche Art von Schutz sie bieten.

Sicherungstyp	Beschreibung
Schnappschuss	Erstellt ein schreibgeschütztes Momentaufnahme-Image eines Volumes innerhalb des Quellvolumes. Sie können den Snapshot verwenden, um einzelne Dateien wiederherzustellen oder um den gesamten Inhalt eines Volumes wiederherzustellen.
Replikation	Erstellt eine sekundäre Kopie Ihrer Daten auf einem anderen ONTAP Speichersystem und aktualisiert die sekundären Daten kontinuierlich. Ihre Daten bleiben aktuell und stehen Ihnen jederzeit zur Verfügung.
Cloud-Backup	Erstellt zum Schutz und zur langfristigen Archivierung Backups Ihrer Daten in der Cloud. Bei Bedarf können Sie ein Volume, einen Ordner oder einzelne Dateien aus der Sicherung auf demselben oder einem anderen System wiederherstellen.

Snapshots sind die Grundlage aller Sicherungsmethoden und werden für die Verwendung des Sicherungs- und Wiederherstellungsdienstes benötigt. Ein Snapshot ist ein schreibgeschütztes, zeitpunktbezogenes Abbild eines Datenträgers. Das Image benötigt nur minimalen Speicherplatz und verursacht einen vernachlässigbaren Leistungsmehraufwand, da es lediglich die Änderungen an den Dateien seit der Erstellung des letzten Snapshots aufzeichnet. Der auf Ihrem Volume erstellte Snapshot dient dazu, das replizierte Volume und die Sicherungsdatei mit den am Quellvolume vorgenommenen Änderungen zu synchronisieren – wie in der Abbildung dargestellt.



Sie können sowohl replizierte Volumes auf einem anderen ONTAP Speichersystem erstellen als auch Dateien in der Cloud sichern. Oder Sie können sich dafür entscheiden, nur replizierte Volumes oder Sicherungsdateien zu erstellen – Sie haben die Wahl.

Zusammenfassend sind dies die gültigen Schutzflüsse, die Sie für Volumes in Ihrem ONTAP System erstellen können:

- Quellvolume → Snapshot → Repliziertes Volume → Sicherungsdatei
- Quellvolume → Snapshot → Sicherungsdatei
- Quellvolume → Snapshot → Repliziertes Volume

Die erstmalige Erstellung eines replizierten Volumes oder einer Sicherungsdatei umfasst eine vollständige Kopie der Quelldaten – dies wird als *Baseline-Übertragung* bezeichnet. Nachfolgende Übertragungen enthalten nur differenzielle Kopien der Quelldaten (den Snapshot).

Vergleich der verschiedenen Backup-Methoden

Die folgende Tabelle zeigt einen allgemeinen Vergleich der drei Sicherungsmethoden. Obwohl Objektspeicherplatz in der Regel günstiger ist als Ihr lokaler Festplattenspeicher, können die Austrittsgebühren der Cloud-Anbieter Ihre Ersparnisse teilweise schmälern, wenn Sie davon ausgehen, dass Sie Daten häufig aus der Cloud wiederherstellen. Sie müssen ermitteln, wie oft Sie Daten aus den Sicherungsdateien in der Cloud wiederherstellen müssen.

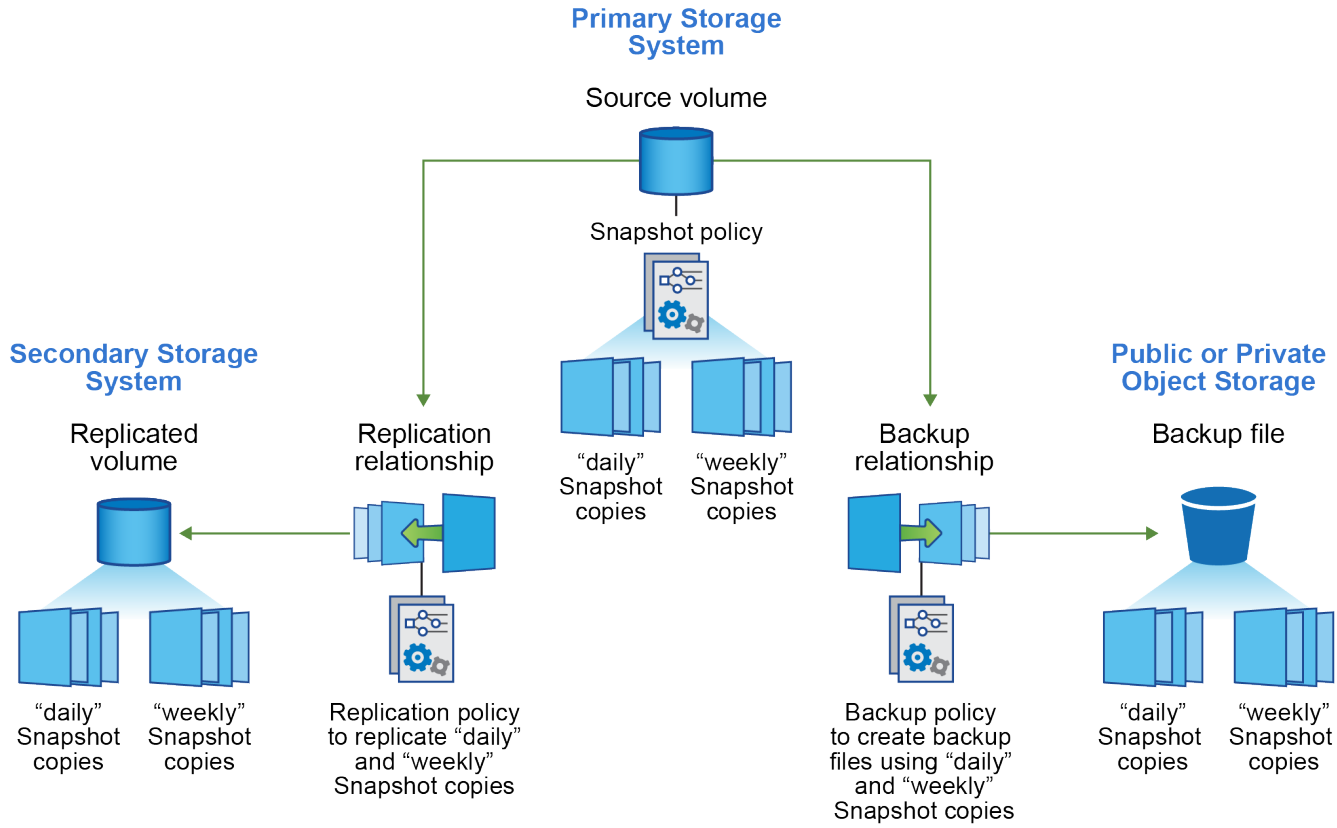
Zusätzlich zu diesen Kriterien bietet der Cloud-Speicher zusätzliche Sicherheitsoptionen, wenn Sie die Funktionen DataLock und Ransomware Resilience verwenden, und zusätzliche Kosteneinsparungen durch die Auswahl von Archivspeicherklassen für ältere Sicherungsdateien. "Erfahren Sie mehr über DataLock und Ransomware-Schutz sowie Archivspeichereinstellungen".

Sicherungstyp	Sicherungsgeschwindigkeit	Backup-Kosten	Geschwindigkeit wiederherstellen	Wiederherstellungskosten
Schnappschuss	Hoch	Niedrig (Speicherplatz)	Hoch	Niedrig
Replikation	Medium	Medium (Speicherplatz)	Medium	Medium (Netzwerk)
Cloud-Backup	Niedrig	Niedrig (Objektraum)	Niedrig	Hoch (Anbietergebühren)

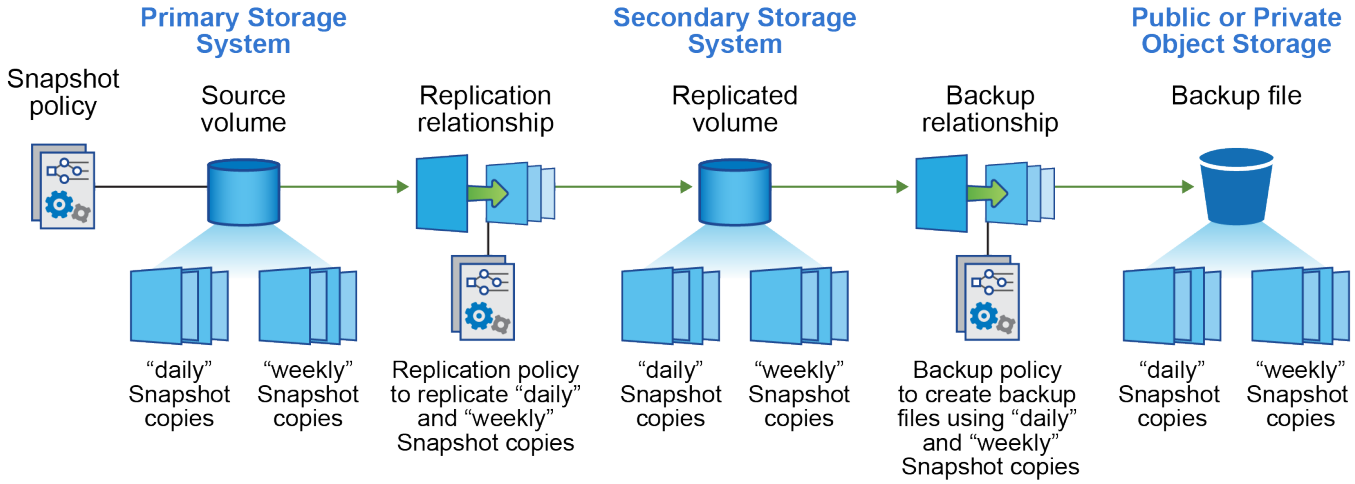
Welche Backup-Architektur werden Sie verwenden?

Wenn Sie sowohl replizierte Volumes als auch Sicherungsdateien erstellen, können Sie zum Sichern Ihrer Volumes eine Fan-Out- oder Kaskadenarchitektur wählen.

Eine **Fan-Out**-Architektur überträgt den Snapshot unabhängig sowohl an das Zielspeichersystem als auch an das Backup-Objekt in der Cloud.



Eine **kaskadierte** Architektur überträgt den Snapshot zuerst an das Zielspeichersystem, und dieses System überträgt dann die Kopie an das Backup-Objekt in der Cloud.



Vergleich der verschiedenen Architekturoptionen

Diese Tabelle bietet einen Vergleich der Fan-Out- und Kaskadenarchitekturen.

Fan-Out	Kaskade
Geringe Auswirkungen auf die Leistung des Quellsystems, da Snapshots an zwei verschiedene Systeme gesendet werden.	Geringere Auswirkungen auf die Leistung des Quellspeichersystems, da der Snapshot nur einmal gesendet wird.

Fan-Out	Kaskade
Einfachere Einrichtung, da alle Richtlinien, Netzwerke und ONTAP -Konfigurationen auf dem Quellsystem vorgenommen werden	Erfordert einige Netzwerk- und ONTAP -Konfigurationen, die auch vom sekundären System aus durchgeführt werden müssen.

Werden Sie die Standardrichtlinien für Snapshots, Replikationen und Backups verwenden?

Sie können zum Erstellen Ihrer Backups die von NetApp bereitgestellten Standardrichtlinien verwenden oder benutzerdefinierte Richtlinien erstellen. Wenn Sie den Aktivierungsassistenten verwenden, um den Sicherungs- und Wiederherstellungsdienst für Ihre Volumes zu aktivieren, können Sie aus den Standardrichtlinien und allen anderen Richtlinien auswählen, die bereits im System vorhanden sind (Cloud Volumes ONTAP oder lokales ONTAP System). Wenn Sie eine andere Richtlinie als die vorhandenen Richtlinien verwenden möchten, können Sie die Richtlinie vor dem Start oder während der Verwendung des Aktivierungsassistenten erstellen.

- Die Standard-Snapshot-Richtlinie erstellt stündliche, tägliche und wöchentliche Snapshots, wobei 6 stündliche, 2 tägliche und 2 wöchentliche Snapshots gespeichert werden.
- Die Standardreplikationsrichtlinie repliziert tägliche und wöchentliche Snapshots und speichert 7 tägliche und 52 wöchentliche Snapshots.
- Die Standard-Backup-Richtlinie repliziert tägliche und wöchentliche Snapshots und speichert 7 tägliche und 52 wöchentliche Snapshots.

Wenn Sie benutzerdefinierte Richtlinien für die Replikation oder Sicherung erstellen, müssen die Richtlinienbezeichnungen (z. B. „täglich“ oder „wöchentlich“) mit den Bezeichnungen in Ihren Snapshot-Richtlinien übereinstimmen. Andernfalls werden keine replizierten Volumes und Sicherungsdateien erstellt.

Sie können Snapshot-, Replikations- und Backup-to-Object-Storage-Richtlinien in der NetApp Backup and Recovery Benutzeroberfläche erstellen. Weitere Informationen finden Sie im Abschnitt"Hinzufügen einer neuen Sicherungsrichtlinie" für Details.

Zusätzlich zur Verwendung von NetApp Backup and Recovery zum Erstellen benutzerdefinierter Richtlinien können Sie System Manager oder die ONTAP Befehlszeilenschnittstelle (CLI) verwenden:

- "Erstellen Sie eine Snapshot-Richtlinie mit System Manager oder der ONTAP CLI"
- "Erstellen Sie eine Replikationsrichtlinie mit System Manager oder der ONTAP CLI"

Hinweis: Wählen Sie bei Verwendung des System Managers **Asynchron** als Richtlinientyp für Replikationsrichtlinien und **Asynchron** und **In Cloud sichern** für Richtlinien zur Sicherung auf Objekt.

Hier sind einige Beispiele für ONTAP CLI-Befehle, die beim Erstellen benutzerdefinierter Richtlinien hilfreich sein können. Beachten Sie, dass Sie den *admin* vserver (Speicher-VM) als `<vserver_name>` in diesen Befehlen.

Richtlinienbeschreibung	Befehl
Einfache Snapshot-Richtlinie	`snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly`

Richtlinienbeschreibung	Befehl
Einfaches Backup in die Cloud	`snapmirror policy create -policy <policy_name> -transfer -priority normal -vserver <vserver_name> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`
Backup in die Cloud mit DataLock und Ransomware-Schutz	`snapmirror policy create -policy CloudBackupService-Enterprise -snapshot-lock-mode enterprise -vserver <vserver_name>` `snapmirror policy add-rule -policy CloudBackupService-Enterprise -retention-period 30days`
Backup in die Cloud mit Archivspeicherklasse	`snapmirror policy create -vserver <vserver_name> -policy <policy_name> -archive-after-days <days> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`
Einfache Replikation auf ein anderes Speichersystem	`snapmirror policy create -policy <policy_name> -type async-mirror -vserver <vserver_name>` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

Für Backup-to-Cloud-Beziehungen können nur Tresorrichtlinien verwendet werden.

Wo befinden sich meine Policen?

Sicherungsrichtlinien befinden sich an unterschiedlichen Orten, abhängig von der Sicherungsarchitektur, die Sie verwenden möchten: Fan-Out oder Kaskadierung. Replikationsrichtlinien und Sicherungsrichtlinien sind nicht auf die gleiche Weise konzipiert, da Replikationen zwei ONTAP Speichersysteme koppeln und die Sicherung auf ein Objekt einen Speicheranbieter als Ziel verwendet.

- Snapshot-Richtlinien befinden sich immer auf dem primären Speichersystem.
- Replikationsrichtlinien befinden sich immer auf dem sekundären Speichersystem.
- Backup-to-Object-Richtlinien werden auf dem System erstellt, auf dem sich das Quellvolume befindet. Dies ist der primäre Cluster für Fan-Out-Konfigurationen und der sekundäre Cluster für kaskadierende Konfigurationen.

Diese Unterschiede sind in der Tabelle dargestellt.

Architektur	Snapshot-Richtlinie	Replikationsrichtlinie	Sicherungsrichtlinie
Auffächern	Primär	Sekundär	Primär
Kaskade	Primär	Sekundär	Sekundär

Wenn Sie also bei Verwendung der kaskadierenden Architektur benutzerdefinierte Richtlinien erstellen möchten, müssen Sie die Replikations- und Backup-to-Object-Richtlinien auf dem sekundären System erstellen, auf dem die replizierten Volumes erstellt werden. Wenn Sie bei Verwendung der Fan-Out-Architektur

benutzerdefinierte Richtlinien erstellen möchten, müssen Sie die Replikationsrichtlinien auf dem sekundären System erstellen, auf dem die replizierten Volumes erstellt werden, und Richtlinien für die Sicherung auf Objekten auf dem primären System.

Wenn Sie die Standardrichtlinien verwenden, die auf allen ONTAP -Systemen vorhanden sind, sind Sie startklar.

Möchten Sie Ihren eigenen Objektspeichercontainer erstellen

Wenn Sie Sicherungsdateien im Objektspeicher für ein System erstellen, erstellt der Sicherungs- und Wiederherstellungsdienst standardmäßig den Container (Bucket oder Speicherkonto) für die Sicherungsdateien im von Ihnen konfigurierten Objektspeicherkonto. Der AWS- oder GCP-Bucket heißt standardmäßig „netapp-backup-<uuid>“. Das Azure Blob-Speicherkonto hat den Namen „netappbackup<uuid>“.

Sie können den Container im Objektanbieterkonto selbst erstellen, wenn Sie ein bestimmtes Präfix verwenden oder spezielle Eigenschaften zuweisen möchten. Wenn Sie einen eigenen Container erstellen möchten, müssen Sie dies vor dem Starten des Aktivierungsassistenten tun. NetApp Backup and Recovery kann jeden Bucket verwenden und Buckets freigeben. Der Assistent zur Sicherungsaktivierung erkennt automatisch Ihre bereitgestellten Container für das ausgewählte Konto und die Anmeldeinformationen, sodass Sie den gewünschten Container auswählen können.

Sie können den Bucket über die Konsole oder Ihren Cloud-Anbieter erstellen.

- "Erstellen Sie Amazon S3-Buckets über die Konsole"
- "Erstellen Sie Azure Blob Storage-Konten über die Konsole"
- "Erstellen Sie Google Cloud Storage-Buckets über die Konsole"

Wenn Sie ein anderes Bucket-Präfix als „netapp-backup-xxxxxx“ verwenden möchten, müssen Sie die S3-Berechtigungen für die IAM-Rolle des Konsolenagenten ändern.

Erweiterte Bucket-Einstellungen

Wenn Sie ältere Sicherungsdateien in einen Archivspeicher verschieben oder DataLock und Ransomware-Schutz aktivieren möchten, um Ihre Sicherungsdateien zu sperren und auf mögliche Ransomware zu scannen, müssen Sie den Container mit bestimmten Konfigurationseinstellungen erstellen:

- Archivspeicherung in Ihren eigenen Buckets wird derzeit im AWS S3-Speicher unterstützt, wenn Sie auf Ihren Clustern die Software ONTAP 9.10.1 oder höher verwenden. Standardmäßig beginnen Sicherungen in der Speicherklasse S3 *Standard*. Stellen Sie sicher, dass Sie den Bucket mit den entsprechenden Lebenszyklusregeln erstellen:
  - Verschieben Sie die Objekte im gesamten Umfang des Buckets nach 30 Tagen nach S3 *Standard-IA*.
  - Verschieben Sie die Objekte mit dem Tag "smc_push_to_archive: true" nach *Glacier Flexible Retrieval* (früher S3 Glacier).
- DataLock- und Ransomware-Schutz werden im AWS-Speicher unterstützt, wenn Sie auf Ihren Clustern die Software ONTAP 9.11.1 oder höher verwenden, und im Azure-Speicher, wenn Sie die Software ONTAP 9.12.1 oder höher verwenden.
  - Für AWS müssen Sie die Objektsperre für den Bucket mit einer Aufbewahrungsfrist von 30 Tagen aktivieren.
  - Für Azure müssen Sie die Speicherklasse mit Unterstützung für Unveränderlichkeit auf Versionsebene erstellen.

Welchen Bereitstellungsmodus des Konsolenagenten verwenden Sie?

Wenn Sie die Konsole bereits zur Verwaltung Ihres Speichers verwenden, wurde bereits ein Konsolenagent installiert. Wenn Sie denselben Konsolenagenten mit NetApp Backup and Recovery verwenden möchten, sind Sie startklar. Wenn Sie einen anderen Konsolenagenten verwenden müssen, müssen Sie ihn installieren, bevor Sie mit der Implementierung Ihrer Sicherung und Wiederherstellung beginnen.

Die NetApp Console bietet mehrere Bereitstellungsmodi, mit denen Sie die Konsole so verwenden können, dass sie Ihren Geschäfts- und Sicherheitsanforderungen entspricht. Der *Standardmodus* nutzt die SaaS-Ebene der Konsole, um die volle Funktionalität bereitzustellen, während der *eingeschränkte Modus* und der *private Modus* für Organisationen mit Verbindungsbeschränkungen verfügbar sind.

"Erfahren Sie mehr über die Bereitstellungsmodi der NetApp Console".

Unterstützung für Sites mit vollständiger Internetkonnektivität

Wenn NetApp Backup and Recovery an einem Standort mit vollständiger Internetkonnektivität (auch als *Standardmodus* oder *SaaS-Modus* bezeichnet) verwendet wird, können Sie replizierte Volumes auf allen lokalen ONTAP oder Cloud Volumes ONTAP Systemen erstellen, die von der Konsole verwaltet werden, und Sie können Sicherungsdateien auf Objektspeichern bei jedem der unterstützten Cloud-Anbieter erstellen. "Vollständige Liste der unterstützten Sicherungsziele anzeigen".

Eine Liste der gültigen Konsolenagent-Speicherorte finden Sie in einem der folgenden Sicherungsverfahren für den Cloud-Anbieter, bei dem Sie Sicherungsdateien erstellen möchten. Es gibt einige Einschränkungen, bei denen der Konsolenagent manuell auf einem Linux-Computer installiert oder bei einem bestimmten Cloud-Anbieter bereitgestellt werden muss.

- "Sichern Sie Cloud Volumes ONTAP Daten auf Amazon S3"
- "Sichern Sie Cloud Volumes ONTAP Daten in Azure Blob"
- "Sichern Sie Cloud Volumes ONTAP Daten in Google Cloud"
- "Sichern Sie lokale ONTAP -Daten auf Amazon S3"
- "Sichern Sie lokale ONTAP Daten in Azure Blob"
- "Sichern Sie lokale ONTAP -Daten in der Google Cloud"
- "Sichern Sie lokale ONTAP Daten auf StorageGRID"
- "Sichern Sie lokales ONTAP auf ONTAP S3"

Unterstützung für Websites mit eingeschränkter Internetverbindung

NetApp Backup and Recovery kann an einem Standort mit eingeschränkter Internetverbindung (auch als *eingeschränkter Modus* bezeichnet) zum Sichern von Volumedaten verwendet werden. In diesem Fall müssen Sie den Konsolenagenten in der Ziel-Cloudregion bereitstellen.

- Sie können Daten von lokalen ONTAP -Systemen oder Cloud Volumes ONTAP -Systemen, die in kommerziellen AWS-Regionen installiert sind, auf Amazon S3 sichern. "Sichern Sie Cloud Volumes ONTAP Daten auf Amazon S3".
- Sie können Daten von lokalen ONTAP -Systemen oder Cloud Volumes ONTAP -Systemen, die in kommerziellen Azure-Regionen installiert sind, in Azure Blob sichern. "Sichern Sie Cloud Volumes ONTAP Daten in Azure Blob".

Unterstützung für Websites ohne Internetverbindung

NetApp Backup and Recovery kann an einem Standort ohne Internetverbindung (auch als *privater Modus* oder *dark* Sites bezeichnet) zum Sichern von Volumedaten verwendet werden. In diesem Fall müssen Sie den Konsolen-Agenten auf einem Linux-Host am selben Standort bereitstellen.

> Der private BlueXP Modus (alte BlueXP -Schnittstelle) wird normalerweise in lokalen Umgebungen ohne Internetverbindung und mit sicheren Cloud-Regionen verwendet, darunter AWS Secret Cloud, AWS Top Secret Cloud und Azure IL6. NetApp unterstützt diese Umgebungen weiterhin mit der alten BlueXP Schnittstelle. Die Dokumentation zum privaten Modus in der alten BlueXP Schnittstelle finden Sie im "PDF-Dokumentation für den privaten Modus von BlueXP" .

- Sie können Daten von lokalen ONTAP -Systemen vor Ort auf lokalen NetApp StorageGRID -Systemen sichern. "Sichern Sie lokale ONTAP Daten auf StorageGRID".
- Sie können Daten von lokalen ONTAP -Systemen vor Ort auf lokalen ONTAP Systemen vor Ort oder auf für S3-Objektspeicher konfigurierten Cloud Volumes ONTAP -Systemen sichern. "Sichern Sie lokale ONTAP -Daten auf ONTAP S3"Die

Verwalten Sie Backup-Richtlinien für ONTAP -Volumes mit NetApp Backup and Recovery

Verwenden Sie mit NetApp Backup and Recovery die von NetApp bereitgestellten Standard-Backup-Richtlinien zum Erstellen Ihrer Backups oder erstellen Sie benutzerdefinierte Richtlinien. Richtlinien regeln die Sicherungshäufigkeit, den Zeitpunkt der Sicherung und die Anzahl der aufbewahrten Sicherungsdateien.

> Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

Wenn Sie den Aktivierungsassistenten verwenden, um den Sicherungs- und Wiederherstellungsdienst für Ihre Volumes zu aktivieren, können Sie aus den Standardrichtlinien und allen anderen Richtlinien auswählen, die bereits im System vorhanden sind (Cloud Volumes ONTAP oder lokales ONTAP System). Wenn Sie eine andere Richtlinie als die vorhandenen Richtlinien verwenden möchten, können Sie die Richtlinie vor oder während der Verwendung des Aktivierungsassistenten erstellen.

Weitere Informationen zu den bereitgestellten Standard-Sicherungsrichtlinien finden Sie unter"Planen Sie Ihren Schutzweg" .

NetApp Backup and Recovery bietet drei Arten von Backups von ONTAP -Daten: Snapshots, Replikationen und Backups auf Objektspeicher. Ihre Richtlinien befinden sich je nach verwendeter Architektur und Sicherungstyp an unterschiedlichen Orten:

Architektur	Speicherort der Snapshot-Richtlinie	Speicherort der Replikationsrichtlinie	Sicherung am Speicherort der Objektrichtlinie
Auffächern	Primär	Sekundär	Primär
Kaskade	Primär	Sekundär	Sekundär

Erstellen Sie Sicherungsrichtlinien mit den folgenden Tools, abhängig von Ihrer Umgebung, Ihren Präferenzen und dem Schutztyp:

- NetApp Console -UI
- System Manager-Benutzeroberfläche
- ONTAP CLI

Wählen Sie bei Verwendung des System Managers **Asynchron** als Richtlinientyp für Replikationsrichtlinien und **Asynchron** und **In Cloud sichern** für Richtlinien zur Sicherung auf Objekt.

Richtlinien für ein System anzeigen

1. Wählen Sie in der Konsolen-Benutzeroberfläche **Volumes** > **Sicherungseinstellungen**.
2. Wählen Sie auf der Seite „Backup-Einstellungen“ das System aus und wählen Sie die **Aktionen*** **Symbol und wählen Sie *Richtlinienverwaltung**.

   Die Seite „Richtlinienverwaltung“ wird angezeigt. Snapshot-Richtlinien werden standardmäßig angezeigt.

3. Um andere im System vorhandene Richtlinien anzuzeigen, wählen Sie entweder **Replikationsrichtlinien** oder **Sicherungsrichtlinien**. Wenn die vorhandenen Richtlinien für Ihre Sicherungspläne verwendet werden können, sind Sie startklar. Wenn Sie eine Richtlinie mit anderen Merkmalen benötigen, können Sie auf dieser Seite neue Richtlinien erstellen.

Erstellen von Richtlinien

Sie können Richtlinien erstellen, die Ihre Snapshots, Replikationen und Backups im Objektspeicher steuern:

- bevor Sie den Snapshot starten
- bevor Sie die Replikation starten
- bevor Sie das Backup starten

Erstellen Sie eine Snapshot-Richtlinie, bevor Sie den Snapshot starten

Ein Teil Ihrer 3-2-1-Strategie besteht darin, einen Snapshot des Volumes auf dem **primären** Speichersystem zu erstellen.

Ein Teil des Richtlinienerstellungsprozesses umfasst die Identifizierung von Snapshot- und SnapMirror -Bezeichnungen, die den Zeitplan und die Aufbewahrung angeben. Sie können vordefinierte Beschriftungen verwenden oder eigene erstellen.

Schritte

1. Wählen Sie in der Konsolen-Benutzeroberfläche **Volumes** > **Sicherungseinstellungen**.
2. Wählen Sie auf der Seite „Backup-Einstellungen“ das System aus und wählen Sie die **Aktionen*** **Symbol und wählen Sie *Richtlinienverwaltung**.

   Die Seite „Richtlinienverwaltung“ wird angezeigt.

3. Wählen Sie auf der Seite „Richtlinien“ **Richtlinie erstellen** > **Snapshot-Richtlinie erstellen**.
4. Geben Sie den Richtliniennamen an.
5. Wählen Sie den oder die Snapshot-Zeitpläne aus. Sie können maximal 5 Etiketten haben. Oder erstellen Sie einen Zeitplan.
6. Wenn Sie einen Zeitplan erstellen möchten:

a. Wählen Sie die Häufigkeit stündlich, täglich, wöchentlich, monatlich oder jährlich.
b. Geben Sie die Snapshot-Beschriftungen an, die den Zeitplan und die Aufbewahrung kennzeichnen.
c. Geben Sie ein, wann und wie oft der Schnappschuss erstellt werden soll.
d. Aufbewahrung: Geben Sie die Anzahl der aufzubewahrenden Snapshots ein.

7. Wählen Sie **Erstellen**.

Beispiel für eine Snapshot-Richtlinie mit kaskadierender Architektur

In diesem Beispiel wird eine Snapshot-Richtlinie mit zwei Clustern erstellt:

1. Cluster 1:
   a. Wählen Sie Cluster 1 auf der Richtlinienseite aus.
   b. Ignorieren Sie die Richtlinienabschnitte „Replikation“ und „Sicherung auf Objekt“.
   c. Erstellen Sie die Snapshot-Richtlinie.
2. Cluster 2:
   a. Wählen Sie Cluster 2 auf der Richtlinienseite aus.
   b. Ignorieren Sie den Abschnitt zur Snapshot-Richtlinie.
   c. Konfigurieren Sie die Replikations- und Sicherungsrichtlinien für Objekte.

Erstellen Sie eine Replikationsrichtlinie, bevor Sie die Replikation starten

Ihre 3-2-1-Strategie könnte die Replikation eines Volumes auf einem anderen Speichersystem umfassen. Die Replikationsrichtlinie befindet sich auf dem **sekundären** Speichersystem.

Schritte

1. Wählen Sie auf der Seite „Richtlinien“ die Optionen **Richtlinie erstellen** > **Replikationsrichtlinie erstellen**.
2. Geben Sie im Abschnitt „Richtliniendetails“ den Richtliniennamen an.
3. Geben Sie die SnapMirror -Beschriftungen (maximal 5) an, die die Aufbewahrungsdauer für jede Beschriftung angeben.
4. Geben Sie den Übertragungsplan an.
5. Wählen Sie **Erstellen**.

Erstellen Sie eine Backup-to-Object-Storage-Richtlinie, bevor Sie das Backup starten

Ihre 3-2-1-Strategie könnte die Sicherung eines Volumes im Objektspeicher umfassen.

Diese Speicherrichtlinie befindet sich je nach Sicherungsarchitektur an verschiedenen Speicherorten des Speichersystems:

- Fan-Out: Primäres Speichersystem
- Kaskadierung: Sekundärspeichersystem

Schritte

1. Wählen Sie auf der Seite „Richtlinienverwaltung“ **Richtlinie erstellen** > **Sicherungsrichtlinie erstellen**.
2. Geben Sie im Abschnitt „Richtliniendetails“ den Richtliniennamen an.

3. Geben Sie die SnapMirror -Beschriftungen (maximal 5) an, die die Aufbewahrungsdauer für jede Beschriftung angeben.
4. Geben Sie die Einstellungen an, einschließlich des Übertragungszeitplans und des Zeitpunkts, zu dem die Sicherungen archiviert werden sollen.
5. (Optional) Um ältere Sicherungsdateien nach einer bestimmten Anzahl von Tagen in eine weniger teure Speicherklasse oder Zugriffsebene zu verschieben, wählen Sie die Option **Archivieren** und geben Sie die Anzahl der Tage an, die vergehen sollen, bevor die Daten archiviert werden. Geben Sie **0** als „Archiv nach Tagen“ ein, um Ihre Sicherungsdatei direkt an den Archivspeicher zu senden.

   "Weitere Informationen zu den Einstellungen für die Archivspeicherung".
6. (Optional) Um Ihre Backups vor Änderungen oder Löschungen zu schützen, wählen Sie die Option **DataLock & Ransomware-Schutz**.

   Wenn Ihr Cluster ONTAP 9.11.1 oder höher verwendet, können Sie Ihre Backups vor dem Löschen schützen, indem Sie *DataLock* und *Ransomware-Schutz* konfigurieren.

   "Erfahren Sie mehr über die verfügbaren DataLock-Einstellungen".
7. Wählen Sie **Erstellen**.

Bearbeiten einer Richtlinie

Sie können eine benutzerdefinierte Snapshot-, Replikations- oder Sicherungsrichtlinie bearbeiten.

Das Ändern der Sicherungsrichtlinie wirkt sich auf alle Volumes aus, die diese Richtlinie verwenden.

Schritte

1. Wählen Sie auf der Seite „Richtlinienverwaltung“ die Richtlinie aus und wählen Sie die Option „Aktionen“ ••• Symbol und wählen Sie **Richtlinie bearbeiten**.

   Der Prozess ist für Replikations- und Sicherungsrichtlinien derselbe.
2. Nehmen Sie auf der Seite „Richtlinie bearbeiten“ die Änderungen vor.
3. Wählen Sie **Speichern**.

Löschen einer Richtlinie

Sie können Richtlinien löschen, die keinem Volume zugeordnet sind.

Wenn eine Richtlinie mit einem Volume verknüpft ist und Sie die Richtlinie löschen möchten, müssen Sie die Richtlinie zuerst vom Volume entfernen.

Schritte

1. Wählen Sie auf der Seite „Richtlinienverwaltung“ die Richtlinie aus und wählen Sie die Option „Aktionen“ ••• Symbol und wählen Sie **Snapshot-Richtlinie löschen**.
2. Wählen Sie **Löschen**.

Weitere Informationen

Anweisungen zum Erstellen von Richtlinien mit System Manager oder ONTAP CLI finden Sie hier:

"Erstellen einer Snapshot-Richtlinie mit System Manager" "Erstellen einer Snapshot-Richtlinie mit der ONTAP CLI" "Erstellen einer Replikationsrichtlinie mit System Manager" "Erstellen einer Replikationsrichtlinie mit der ONTAP CLI" "Erstellen einer Richtlinie für die Sicherung in einem Objektspeicher mit System Manager" "Erstellen einer Richtlinie für das Backup in einem Objektspeicher mithilfe der ONTAP CLI"

Optionen für die Backup-to-Object-Richtlinie in NetApp Backup and Recovery

Mit NetApp Backup and Recovery können Sie Sicherungsrichtlinien mit einer Vielzahl von Einstellungen für Ihre lokalen ONTAP und Cloud Volumes ONTAP Systeme erstellen.

Diese Richtlinieneinstellungen sind nur für die Sicherung auf Objektspeicher relevant. Keine dieser Einstellungen wirkt sich auf Ihre Snapshot- oder Replikationsrichtlinien aus.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

Optionen für den Sicherungszeitplan

Mit NetApp Backup and Recovery können Sie mehrere Sicherungsrichtlinien mit individuellen Zeitplänen für jedes System (Cluster) erstellen. Sie können Volumes mit unterschiedlichen Recovery Point Objectives (RPO) unterschiedliche Sicherungsrichtlinien zuweisen.

Jede Sicherungsrichtlinie enthält einen Abschnitt für *Labels und Aufbewahrung*, den Sie auf Ihre Sicherungsdateien anwenden können. Beachten Sie, dass die auf das Volume angewendete Snapshot-Richtlinie eine der von NetApp Backup and Recovery erkannten Richtlinien sein muss, da sonst keine Sicherungsdateien erstellt werden.

Der Zeitplan besteht aus zwei Teilen: dem Label und dem Aufbewahrungswert:

- Das **Label** definiert, wie oft eine Sicherungsdatei vom Volume erstellt (oder aktualisiert) wird. Sie können zwischen folgenden Etikettentypen wählen:
  - Sie können einen oder eine Kombination aus **stündlichen**, **täglichen**, **wöchentlichen**, **monatlichen** und **jährlichen** Zeitrahmen auswählen.
  - Sie können eine der systemdefinierten Richtlinien auswählen, die eine Sicherung und Aufbewahrung für 3 Monate, 1 Jahr oder 7 Jahre ermöglichen.
  - Wenn Sie mit ONTAP System Manager oder der ONTAP CLI benutzerdefinierte Richtlinien zum Sicherungsschutz auf dem Cluster erstellt haben, können Sie eine dieser Richtlinien auswählen.
- Der **Aufbewahrungswert** definiert, wie viele Sicherungsdateien für jedes Label (Zeitraum) aufbewahrt werden. Sobald die maximale Anzahl an Backups in einer Kategorie oder einem Intervall erreicht ist, werden ältere Backups entfernt, sodass Sie immer über die aktuellsten Backups verfügen. Dadurch sparen Sie auch Speicherkosten, da veraltete Backups keinen weiteren Speicherplatz in der Cloud belegen.

Angenommen, Sie erstellen eine Sicherungsrichtlinie, die 7 **wöchentliche** und 12 **monatliche** Sicherungen erstellt:

- jede Woche und jeden Monat wird eine Sicherungsdatei für das Volume erstellt
- In der 8. Woche wird das erste wöchentliche Backup entfernt und das neue wöchentliche Backup für die 8. Woche hinzugefügt (maximal 7 wöchentliche Backups bleiben erhalten).
- Im 13. Monat wird das erste monatliche Backup entfernt und das neue monatliche Backup für den 13. Monat hinzugefügt (maximal 12 monatliche Backups bleiben erhalten).

Jährliche Backups werden nach der Übertragung in den Objektspeicher automatisch aus dem Quellsystem gelöscht. Dieses Standardverhalten kann auf der Seite „Erweiterte Einstellungen“ für das System geändert werden.

DataLock- und Ransomware-Schutzoptionen

NetApp Backup and Recovery bietet Unterstützung für DataLock- und Ransomware-Schutz für Ihre Volume-Backups. Mit diesen Funktionen können Sie Ihre Sicherungsdateien sperren und scannen, um mögliche Ransomware in den Sicherungsdateien zu erkennen. Dies ist eine optionale Einstellung, die Sie in Ihren Sicherungsrichtlinien definieren können, wenn Sie zusätzlichen Schutz für Ihre Volumesicherungen für einen Cluster wünschen.

Beide Funktionen schützen Ihre Sicherungsdateien, sodass Sie im Falle eines Ransomware-Angriffs auf Ihre Sicherungen immer über eine gültige Sicherungsdatei verfügen, aus der Sie Daten wiederherstellen können. Es ist auch hilfreich, bestimmte gesetzliche Anforderungen zu erfüllen, wenn Backups gesperrt und für einen bestimmten Zeitraum aufbewahrt werden müssen. Wenn die Option „DataLock und Ransomware-Resilienz“ aktiviert ist, sind für den Cloud-Bucket, der im Rahmen der Aktivierung von NetApp Backup and Recovery bereitgestellt wird, die Objektsperre und die Objektversionierung aktiviert.

Diese Funktion bietet keinen Schutz für Ihre Quellvolumes, sondern nur für die Sicherungen dieser Quellvolumes. Verwenden Sie einige der "Anti-Ransomware-Schutz von ONTAP" um Ihre Quellvolumes zu schützen.

- Wenn Sie DataLock und Ransomware-Schutz verwenden möchten, können Sie diese aktivieren, wenn Sie Ihre erste Sicherungsrichtlinie erstellen und NetApp Backup and Recovery für diesen Cluster aktivieren. Sie können das Scannen auf Ransomware später mithilfe der erweiterten Einstellungen für NetApp Backup and Recovery aktivieren oder deaktivieren.
- Wenn die Konsole beim Wiederherstellen von Volumedaten eine Sicherungsdatei auf Ransomware scannt, entstehen Ihnen bei Ihrem Cloud-Anbieter zusätzliche Kosten für den Zugriff auf den Inhalt der Sicherungsdatei.

Was ist DataLock

Mit dieser Funktion können Sie die über SnapMirror in die Cloud replizierten Cloud-Snapshots sperren und außerdem die Funktion aktivieren, einen Ransomware-Angriff zu erkennen und eine konsistente Kopie des Snapshots im Objektspeicher wiederherzustellen. Diese Funktion wird auf AWS, Azure, Google Cloud Platform und StorageGRID unterstützt.

DataLock schützt Ihre Sicherungsdateien für einen bestimmten Zeitraum vor Änderungen oder Löschungen – auch als *unveränderlicher Speicher* bezeichnet. Diese Funktion nutzt die Technologie des Objektspeicheranbieters zur „Objektsperre“.

Cloud-Anbieter verwenden ein Retention Until Date (RUD), das auf Grundlage der Snapshot-Aufbewahrungsdauer berechnet wird. Der Aufbewahrungszeitraum für Snapshots wird anhand der Bezeichnung und der in der Sicherungsrichtlinie definierten Aufbewahrungsanzahl berechnet.

Die Mindestaufbewahrungsdauer für Snapshots beträgt 30 Tage. Sehen wir uns einige Beispiele an, wie das funktioniert:

- Wenn Sie die Bezeichnung **Täglich** mit der Aufbewahrungsanzahl 20 wählen, beträgt die Aufbewahrungsdauer des Snapshots 20 Tage, standardmäßig also mindestens 30 Tage.
- Wenn Sie die Bezeichnung **Wöchentlich** mit der Aufbewahrungsanzahl 4 wählen, beträgt die

Aufbewahrungsdauer des Snapshots 28 Tage, standardmäßig ist das Minimum 30 Tage.

- Wenn Sie die Bezeichnung **Monatlich** mit der Aufbewahrungsanzahl 3 wählen, beträgt die Aufbewahrungsdauer des Snapshots 90 Tage.
- Wenn Sie die Bezeichnung **Jährlich** mit der Aufbewahrungsanzahl 1 wählen, beträgt die Aufbewahrungsdauer des Snapshots 365 Tage.

Was ist das Retention Until Date (RUD) und wie wird es berechnet?

Das Aufbewahrungsdatum (RUD) wird basierend auf der Snapshot-Aufbewahrungsdauer bestimmt. Das Aufbewahrungsdatum wird durch die Summe der Snapshot-Aufbewahrungsdauer und eines Puffers berechnet.

- Der Puffer ist der Puffer für die Übertragungszeit (3 Tage) + Puffer für die Kostenoptimierung (28 Tage), was insgesamt 31 Tage ergibt.
- Das Mindestaufbewahrungsdatum beträgt 30 Tage + 31 Tage Puffer = 61 Tage.

Hier sind einige Beispiele:

- Wenn Sie einen monatlichen Sicherungszeitplan mit 12 Aufbewahrungszeiten erstellen, werden Ihre Sicherungen 12 Monate (plus 31 Tage) gesperrt, bevor sie gelöscht (durch die nächste Sicherungsdatei ersetzt) werden.
- Wenn Sie eine Sicherungsrichtlinie erstellen, die 30 tägliche, 7 wöchentliche und 12 monatliche Sicherungen erstellt, gibt es drei gesperrte Aufbewahrungszeiträume:
  - Die „30 täglichen“ Backups werden 61 Tage lang aufbewahrt (30 Tage plus 31 Tage Puffer),
  - Die "7 wöchentlichen" Backups werden 11 Wochen (7 Wochen plus 31 Tage) aufbewahrt und
  - Die „12 monatlichen“ Backups werden 12 Monate (plus 31 Tage) aufbewahrt.
- Wenn Sie einen stündlichen Sicherungsplan mit 24 Aufbewahrungszeiten erstellen, denken Sie möglicherweise, dass die Sicherungen 24 Stunden lang gesperrt sind. Da dies jedoch weniger als das Minimum von 30 Tagen ist, wird jede Sicherung gesperrt und 61 Tage lang aufbewahrt (30 Tage plus 31 Tage Puffer).

> Alte Sicherungen werden nach Ablauf der DataLock-Aufbewahrungsfrist gelöscht, nicht nach Ablauf der Aufbewahrungsfrist der Sicherungsrichtlinie.

Die DataLock-Aufbewahrungseinstellung überschreibt die Richtlinienaufbewahrungseinstellung Ihrer Sicherungsrichtlinie. Dies kann sich auf Ihre Speicherkosten auswirken, da Ihre Sicherungsdateien für einen längeren Zeitraum im Objektspeicher gespeichert werden.

Aktivieren Sie DataLock und Ransomware-Schutz

Sie können DataLock und Ransomware-Schutz aktivieren, wenn Sie eine Richtlinie erstellen. Sie können dies nach der Erstellung der Richtlinie nicht mehr aktivieren, ändern oder deaktivieren.

1. Erweitern Sie beim Erstellen einer Richtlinie den Abschnitt **DataLock and Ransomware Resilience**.
2. Wählen Sie eine der folgenden Optionen:
   - **Keine**: DataLock-Schutz und Ransomware-Resilienz sind deaktiviert.
   - **Entsperrt**: DataLock-Schutz und Ransomware-Resilienz sind aktiviert. Benutzer mit bestimmten Berechtigungen können geschützte Sicherungsdateien während der Aufbewahrungsfrist überschreiben oder löschen.
   - **Gesperrt**: DataLock-Schutz und Ransomware-Resilienz sind aktiviert. Während der

Aufbewahrungsfrist können keine Benutzer geschützte Sicherungsdateien überschreiben oder löschen. Damit wird die Einhaltung aller gesetzlichen Vorschriften gewährleistet.

Siehe"So aktualisieren Sie die Ransomware-Schutzoptionen auf der Seite „Erweiterte Einstellungen“" .

Was ist Ransomware-Schutz?

Der Ransomware-Schutz durchsucht Ihre Sicherungsdateien nach Hinweisen auf einen Ransomware-Angriff. Die Erkennung von Ransomware-Angriffen erfolgt über einen Prüfsummenvergleich. Wenn in einer neuen Sicherungsdatei im Vergleich zur vorherigen Sicherungsdatei potenzielle Ransomware identifiziert wird, wird diese neuere Sicherungsdatei durch die neueste Sicherungsdatei ersetzt, die keine Anzeichen eines Ransomware-Angriffs aufweist. (Die Datei, bei der ein Ransomware-Angriff festgestellt wurde, wird 1 Tag nach ihrer Ersetzung gelöscht.)

Scans werden in folgenden Situationen durchgeführt:

- Scans von Cloud-Backup-Objekten werden kurz nach der Übertragung in den Cloud-Objektspeicher eingeleitet. Der Scan wird nicht beim ersten Schreiben der Sicherungsdatei in den Cloud-Speicher durchgeführt, sondern beim Schreiben der nächsten Sicherungsdatei.
- Ransomware-Scans können gestartet werden, wenn das Backup für den Wiederherstellungsprozess ausgewählt wird.
- Scans können jederzeit auf Anfrage durchgeführt werden.

Wie funktioniert der Wiederherstellungsprozess?

Wenn ein Ransomware-Angriff erkannt wird, verwendet der Dienst die Integrity Checker REST-API des Active Data Console-Agenten, um den Wiederherstellungsprozess zu starten. Die älteste Version der Datenobjekte ist die Quelle der Wahrheit und wird im Rahmen des Wiederherstellungsprozesses zur aktuellen Version gemacht.

Sehen wir uns an, wie das funktioniert:

- Im Falle eines Ransomware-Angriffs versucht der Dienst, das Objekt im Bucket zu überschreiben oder zu löschen.
- Da der Cloud-Speicher versionierungsfähig ist, erstellt er automatisch eine neue Version des Sicherungsobjekts. Wenn ein Objekt bei aktivierter Versionierung gelöscht wird, wird es als gelöscht markiert, kann aber weiterhin abgerufen werden. Beim Überschreiben eines Objekts werden vorherige Versionen gespeichert und gekennzeichnet.
- Wenn ein Ransomware-Scan gestartet wird, werden die Prüfsummen für beide Objektversionen validiert und verglichen. Wenn die Prüfsummen inkonsistent sind, wurde potenzielle Ransomware erkannt.
- Der Wiederherstellungsprozess umfasst die Rückkehr zur letzten bekannten funktionierenden Kopie.

Unterstützte Systeme und Objektspeicheranbieter

Sie können DataLock- und Ransomware-Schutz auf ONTAP -Volumes der folgenden Systeme aktivieren, wenn Sie Objektspeicher bei den folgenden öffentlichen und privaten Cloud-Anbietern verwenden.

Quellsystem	Ziel der Sicherungsdatei
Cloud Volumes ONTAP in AWS	Amazon S3
Cloud Volumes ONTAP in Azure	Azure-Blob
Cloud Volumes ONTAP in Google Cloud	Google Cloud

Quellsystem	Ziel der Sicherungsdatei
On-Premises- ONTAP -System	Amazon S3, Azure Blob, Google Cloud , NetApp StorageGRID

Anforderungen

- Für AWS:
  - Ihre Cluster müssen ONTAP 9.11.1 oder höher ausführen
  - Der Konsolenagent kann in der Cloud oder vor Ort eingesetzt werden
  - Die folgenden S3-Berechtigungen müssen Teil der IAM-Rolle sein, die dem Konsolenagenten Berechtigungen erteilt. Sie befinden sich im Abschnitt „backupS3Policy“ für die Ressource „arn:aws:s3:::netapp-backup-*“:

AWS S3-Berechtigungen

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:Objekt löschen
- s3:DeleteObjectTagging
- s3:GetObjectRetention
- s3:DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBucketVersions
- s3:ListBucket
- s3:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketVersioning
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BypassGovernanceRetention
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

"Zeigen Sie das vollständige JSON-Format für die Richtlinie an, in dem Sie erforderliche Berechtigungen kopieren und einfügen können.".

- Für Azure:
  - Ihre Cluster müssen ONTAP 9.12.1 oder höher ausführen
  - Der Konsolenagent kann in der Cloud oder vor Ort eingesetzt werden
- Für Google Cloud:
  - Ihre Cluster müssen ONTAP 9.17.1 oder höher ausführen
  - Der Konsolenagent kann in der Cloud oder vor Ort eingesetzt werden
- Für StorageGRID:

- Ihre Cluster müssen ONTAP 9.11.1 oder höher ausführen
- Auf Ihren StorageGRID -Systemen muss die Version 11.6.0.3 oder höher ausgeführt werden.
- Der Konsolenagent muss bei Ihnen vor Ort bereitgestellt werden (er kann an einem Standort mit oder ohne Internetzugang installiert werden).
- Die folgenden S3-Berechtigungen müssen Teil der IAM-Rolle sein, die dem Konsolenagenten Berechtigungen erteilt:

StorageGRID S3-Berechtigungen

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:Objekt löschen
- s3:DeleteObjectTagging
- s3:GetObjectRetention
- s3:DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBucketVersions
- s3:ListBucket
- s3:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketVersioning
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

Einschränkungen

- Die DataLock- und Ransomware-Schutzfunktion ist nicht verfügbar, wenn Sie in der Sicherungsrichtlinie Archivspeicher konfiguriert haben.
- Die DataLock-Option, die Sie beim Aktivieren von NetApp Backup and Recovery auswählen, muss für alle

Sicherungsrichtlinien für diesen Cluster verwendet werden.

- Sie können nicht mehrere DataLock-Modi auf einem einzelnen Cluster verwenden.
- Wenn Sie DataLock aktivieren, werden alle Volume-Backups gesperrt. Sie können gesperrte und nicht gesperrte Volume-Backups für einen einzelnen Cluster nicht mischen.
- DataLock- und Ransomware-Schutz ist für neue Volume-Backups anwendbar, bei denen eine Backup-Richtlinie mit aktiviertem DataLock- und Ransomware-Schutz verwendet wird. Sie können diese Funktionen später mithilfe der Option „Erweiterte Einstellungen“ aktivieren oder deaktivieren.
- FlexGroup -Volumes können DataLock- und Ransomware-Schutz nur verwenden, wenn ONTAP 9.13.1 oder höher verwendet wird.

Tipps zur Minimierung der DataLock-Kosten

Sie können die Ransomware-Scan-Funktion aktivieren oder deaktivieren, während die DataLock-Funktion aktiv bleibt. Um zusätzliche Kosten zu vermeiden, können Sie geplante Ransomware-Scans deaktivieren. So können Sie Ihre Sicherheitseinstellungen individuell anpassen und Kosten beim Cloud-Anbieter vermeiden.

Auch wenn geplante Ransomware-Scans deaktiviert sind, können Sie bei Bedarf weiterhin On-Demand-Scans durchführen.

Sie können zwischen verschiedenen Schutzstufen wählen:

- **DataLock *ohne* Ransomware-Scans**: Bietet Schutz für Sicherungsdaten im Zielspeicher, der sich entweder im Governance- oder Compliance-Modus befinden kann.
  - **Governance-Modus**: Bietet Administratoren die Flexibilität, geschützte Daten zu überschreiben oder zu löschen.
  - **Compliance-Modus**: Bietet vollständige Unlöschbarkeit bis zum Ablauf der Aufbewahrungsfrist. Dies trägt dazu bei, die strengsten Datensicherheitsanforderungen in stark regulierten Umgebungen zu erfüllen. Die Daten können während ihres Lebenszyklus weder überschrieben noch geändert werden, was den größtmöglichen Schutz für Ihre Sicherungskopien bietet.

    Microsoft Azure verwendet stattdessen einen Sperr- und Entsperrmodus.

- **DataLock *mit* Ransomware-Scans**: Bietet eine zusätzliche Sicherheitsebene für Ihre Daten. Diese Funktion hilft dabei, alle Versuche zu erkennen, Sicherungskopien zu ändern. Bei einem Versuch wird diskret eine neue Version der Daten erstellt. Die Scanhäufigkeit kann auf 1, 2, 3, 4, 5, 6 oder 7 Tage geändert werden. Wenn die Scans auf alle 7 Tage eingestellt werden, verringern sich die Kosten erheblich.

Weitere Tipps zur Reduzierung der DataLock-Kosten finden Sie unterhttps://community.netapp.com/t5/Tech-ONTAP-Blogs/Understanding-NetApp-Backup-and-Recovery-DataLock-and-Ransomware-Feature-TCO/ba-p/453475[]

Darüber hinaus können Sie Schätzungen für die mit DataLock verbundenen Kosten erhalten, indem Sie die "Rechner für die Gesamtbetriebskosten (TCO) von NetApp Backup and Recovery" .

Archivspeicheroptionen

Wenn Sie AWS-, Azure- oder Google-Cloud-Speicher verwenden, können Sie ältere Sicherungsdateien nach einer bestimmten Anzahl von Tagen in eine weniger teure Archivspeicherklasse oder Zugriffsebene verschieben. Sie können Ihre Sicherungsdateien auch sofort in den Archivspeicher senden, ohne sie in den Standard-Cloud-Speicher zu schreiben. Geben Sie einfach **0** als „Archiv nach Tagen“ ein, um Ihre Sicherungsdatei direkt in den Archivspeicher zu senden. Dies kann besonders für Benutzer hilfreich sein, die selten auf Daten aus Cloud-Backups zugreifen müssen, oder für Benutzer, die eine Backup-to-Tape-Lösung

ersetzen.

Auf Daten in Archivebenen kann bei Bedarf nicht sofort zugegriffen werden und der Abruf ist mit höheren Kosten verbunden. Sie müssen daher überlegen, wie oft Sie Daten aus Sicherungsdateien wiederherstellen müssen, bevor Sie sich für die Archivierung Ihrer Sicherungsdateien entscheiden.

- Auch wenn Sie „0“ auswählen, um alle Datenblöcke an den Archiv-Cloud-Speicher zu senden, werden Metadatenblöcke immer in den Standard-Cloud-Speicher geschrieben.
- Wenn Sie DataLock aktiviert haben, kann der Archivspeicher nicht verwendet werden.
- Sie können die Archivierungsrichtlinie nicht mehr ändern, nachdem Sie **0** Tage ausgewählt haben (sofort archivieren).

Jede Sicherungsrichtlinie enthält einen Abschnitt für *Archivierungsrichtlinien*, den Sie auf Ihre Sicherungsdateien anwenden können.

- In AWS beginnen Backups in der Speicherklasse *Standard* und wechseln nach 30 Tagen zur Speicherklasse *Standard – seltener Zugriff*.

  Wenn Ihr Cluster ONTAP 9.10.1 oder höher verwendet, können Sie ältere Backups entweder in den Speicher *S3 Glacier* oder *S3 Glacier Deep Archive* verschieben. "Erfahren Sie mehr über AWS-Archivspeicher".

  - Wenn Sie bei der Aktivierung von NetApp Backup and Recovery in Ihrer ersten Sicherungsrichtlinie keine Archivebene auswählen, ist *S3 Glacier* Ihre einzige Archivierungsoption für zukünftige Richtlinien.
  - Wenn Sie in Ihrer ersten Sicherungsrichtlinie *S3 Glacier* auswählen, können Sie für zukünftige Sicherungsrichtlinien für diesen Cluster zur Ebene *S3 Glacier Deep Archive* wechseln.
  - Wenn Sie in Ihrer ersten Sicherungsrichtlinie *S3 Glacier Deep Archive* auswählen, ist diese Ebene die einzige Archivebene, die für zukünftige Sicherungsrichtlinien für diesen Cluster verfügbar ist.
- In Azure sind Sicherungen mit der Zugriffsebene „Cool“ verknüpft.

  Wenn Ihr Cluster ONTAP 9.10.1 oder höher verwendet, können Sie ältere Sicherungen in den Azure Archive-Speicher verschieben. "Erfahren Sie mehr über Azure-Archivspeicher".

- In GCP sind Backups mit der Speicherklasse *Standard* verknüpft.

  Wenn Ihr Cluster vor Ort ONTAP 9.12.1 oder höher verwendet, können Sie zur weiteren Kostenoptimierung ältere Backups nach einer bestimmten Anzahl von Tagen in der NetApp Backup and Recovery -Benutzeroberfläche in den Archivspeicher verschieben. "Erfahren Sie mehr über den Archivspeicher von Google".

- In StorageGRID sind Backups mit der Speicherklasse *Standard* verknüpft.

  Wenn Ihr lokaler Cluster ONTAP 9.12.1 oder höher verwendet und Ihr StorageGRID System 11.4 oder höher verwendet, können Sie ältere Sicherungsdateien im öffentlichen Cloud-Archivspeicher archivieren.

  - Bei AWS können Sie Backups auf AWS *S3 Glacier* oder *S3 Glacier Deep Archive*-Speicher auslagern. "Erfahren Sie mehr über AWS-Archivspeicher"Die
  - Bei Azure können Sie ältere Backups im Azure-Archivspeicher auslagern. "Erfahren Sie mehr über Azure-Archivspeicher"Die

Verwalten Sie die Optionen für die Sicherung auf Objektspeicher in den erweiterten Einstellungen von NetApp Backup and Recovery

Sie können die Backup-to-Object-Storage-Einstellungen auf Clusterebene ändern, die Sie beim Aktivieren von NetApp Backup and Recovery für jedes ONTAP System festlegen, indem Sie die Seite „Erweiterte Einstellungen“ verwenden. Sie können auch einige Einstellungen ändern, die als „Standard“-Sicherungseinstellungen angewendet werden. Dies umfasst die Änderung der Übertragungsrate von Backups auf Objektspeicher, die Frage, ob historische Snapshots als Backup-Dateien exportiert werden, und die Aktivierung oder Deaktivierung von Ransomware-Scans für ein System.

Diese Einstellungen sind nur für die Sicherung im Objektspeicher verfügbar. Keine dieser Einstellungen wirkt sich auf Ihre Snapshot- oder Replikationseinstellungen aus.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

Auf der Seite „Erweiterte Einstellungen“ können Sie die folgenden Optionen ändern:

- Ändern der Speicherschlüssel, die Ihrem ONTAP System die Berechtigung zum Zugriff auf den Objektspeicher erteilen.
- Ändern des ONTAP IP-Bereichs, der mit dem Objektspeicher verbunden ist
- Ändern der für das Hochladen von Backups in den Objektspeicher zugewiesenen Netzwerkbandbreite mithilfe der Option „Maximale Übertragungsrate“
- Ändern der Option, ob historische Snapshots als Sicherungsdateien exportiert und in die anfänglichen Basissicherungsdateien für zukünftige Volumes aufgenommen werden.
- Ändern, ob „jährliche“ Snapshots aus dem Quellsystem entfernt werden
- Aktivieren oder Deaktivieren von Ransomware-Scans für ein System, einschließlich geplanter Scans

Anzeigen der Sicherungseinstellungen auf Clusterebene

Sie können die Systemeinstellungen auf Clusterebene und die Provider-Einstellungen für jedes System anzeigen.

Schritte

1. Wählen Sie im Konsolenmenü **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.
3. Wählen Sie auf der Seite „Sicherungseinstellungen“ die Option „…“ aus. ••• Wählen Sie für das System **Erweiterte Einstellungen konfigurieren > Systemeinstellungen**, um die Systemeinstellungen anzuzeigen, und **Erweiterte Einstellungen konfigurieren > Anbietereinstellungen**, um die Anbietereinstellungen anzuzeigen.

   Auf der daraufhin angezeigten Seite werden die aktuellen Einstellungen für dieses System angezeigt. Die angezeigten Provider-Einstellungen beziehen sich auf den Bucket, den Sie oben auf der Seite auswählen.

Beachten Sie, dass einige Optionen je nach ONTAP -Version auf dem Quellcluster und dem Cloud-Anbieter, bei dem die Backups gespeichert sind, nicht verfügbar sind.

Ändern Sie die zum Hochladen von Backups in den Objektspeicher verfügbare Netzwerkbandbreite

Wenn Sie NetApp Backup and Recovery für ein System aktivieren, kann ONTAP standardmäßig eine unbegrenzte Bandbreite nutzen, um die Sicherungsdaten von Volumes im System in den Objektspeicher zu übertragen. Wenn Sie feststellen, dass der Sicherungsverkehr die normale Arbeitslast der Benutzer beeinträchtigt, können Sie die während der Übertragung verwendete Netzwerkbandbreite mithilfe der Option „Maximale Übertragungsrate“ auf der Seite „Erweiterte Einstellungen“ drosseln.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.
2. Klicken Sie auf der Seite „Sicherungseinstellungen“ auf ••• für das System und wählen Sie **Erweiterte Einstellungen konfigurieren > Systemeinstellungen**.
3. Erweitern Sie auf der Seite „Erweiterte Einstellungen“ den Abschnitt „Maximale Übertragungsrate“.
4. Wählen Sie als maximale Übertragungsrate einen Wert zwischen 1 und 1.000 Mbit/s.
5. Wählen Sie das Optionsfeld **Begrenzt** und geben Sie die maximal nutzbare Bandbreite ein, oder wählen Sie **Unbegrenzt**, um anzugeben, dass keine Begrenzung besteht.
6. Wählen Sie **Übernehmen**.

Diese Einstellung hat keine Auswirkungen auf die Bandbreite, die anderen Replikationsbeziehungen zugewiesen wird, die möglicherweise für Volumes im System konfiguriert sind.

Ändern Sie, ob historische Snapshots als Sicherungsdateien exportiert werden.

Falls lokale Snapshots für Volumes existieren, die mit der in diesem System verwendeten Backup-Zeitplanbezeichnung übereinstimmen (z. B. täglich, wöchentlich usw.), können Sie diese historischen Snapshots als Sicherungsdateien in den Objektspeicher exportieren. Dies ermöglicht es Ihnen, Ihre Backups in der Cloud zu initialisieren, indem ältere Snapshots in die Basis-Backup-Kopie verschoben werden.

Beachten Sie, dass diese Option nur für neue Sicherungsdateien für neue Lese-/Schreibvolumes gilt und bei Datensicherungsvolumes (DP) nicht unterstützt wird.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.
2. Klicken Sie auf der Seite „Sicherungseinstellungen“ auf ••• für das System und wählen Sie **Erweiterte Einstellungen konfigurieren > Systemeinstellungen**.
3. Erweitern Sie auf der Seite „Erweiterte Einstellungen“ den Abschnitt **Vorhandene Snapshot-Kopien exportieren**.
4. Wählen Sie aus, ob vorhandene Snapshots exportiert werden sollen.
5. Wählen Sie **Übernehmen**.

Ändern, ob „jährliche“ Snapshots aus dem Quellsystem entfernt werden

Wenn Sie für eine Sicherungsrichtlinie eines Ihrer Volumes die Bezeichnung „jährlich“ auswählen, wird ein sehr großer Snapshot erstellt. Standardmäßig werden diese jährlichen Snapshots nach der Übertragung in den Objektspeicher automatisch aus dem Quellsystem gelöscht. Sie können dieses Standardverhalten im Abschnitt „Jährliche Löschung von Snapshots“ ändern.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.

2. Klicken Sie auf der Seite „Sicherungseinstellungen“ auf ••• für das System und wählen Sie **Erweiterte Einstellungen konfigurieren > Systemeinstellungen**.
3. Erweitern Sie auf der Seite „Erweiterte Einstellungen“ den Abschnitt „Jährliche Snapshot-Löschung“*.
4. Wählen Sie **Deaktiviert**, um die jährlichen Snapshots auf dem Quellsystem beizubehalten.
5. Wählen Sie **Übernehmen**.

Aktivieren oder Deaktivieren von Ransomware-Scans

Ransomware-Schutzscans sind standardmäßig aktiviert. Die Standardeinstellung für die Scanhäufigkeit beträgt 7 Tage. Der Scan erfolgt nur für den neuesten Snapshot.

Weitere Informationen zu den Optionen DataLock und Ransomware Resilience finden Sie unter"DataLock- und Ransomware-Resilienzoptionen" .

Sie können diesen Zeitplan auf Tage oder Wochen ändern oder ihn deaktivieren, um Kosten zu sparen.

Für die Aktivierung von Ransomware-Scans fallen je nach Cloud-Anbieter zusätzliche Gebühren an.

Wenn die geplanten Ransomware-Scans deaktiviert sind, können Sie weiterhin On-Demand-Scans durchführen und der Scan während eines Wiederherstellungsvorgangs wird weiterhin ausgeführt.

Siehe"Richtlinien verwalten" Weitere Informationen zum Verwalten von Richtlinien zur Implementierung der Ransomware-Erkennung.

Aktivieren oder deaktivieren Sie Ransomware-Scans für ein System

Sie können Ransomware-Scans für einen Cluster aktivieren oder deaktivieren.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.
2. Klicken Sie auf der Seite „Sicherungseinstellungen“ auf ••• für das System und wählen Sie **Erweiterte Einstellungen konfigurieren > Systemeinstellungen**.
3. Erweitern Sie auf der folgenden Seite den Abschnitt **Ransomware-Scan**.
4. Aktivieren oder deaktivieren Sie den **Ransomware-Scan**.
5. Wählen Sie **Geplanter Ransomware-Scan**.
6. Ändern Sie optional den wöchentlichen Standardscan auf Tage oder Wochen.
7. Legen Sie fest, wie oft (in Tagen oder Wochen) der Scan ausgeführt werden soll.
8. Wählen Sie **Übernehmen**.

Aktivieren oder deaktivieren Sie Ransomware-Scans für einen Anbieter.

Sie können Ransomware-Scans auf Anbieterebene über die Anbietereinstellungsseite aktivieren oder deaktivieren. Die Einstellungen auf dieser Seite beziehen sich auf den Bucket, den Sie oben auf der Seite auswählen.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.
2. Klicken Sie auf der Seite „Sicherungseinstellungen“ auf ••• für das System und wählen Sie **Erweiterte**

Einstellungen konfigurieren > Anbietereinstellungen.

3. Wählen Sie oben auf der angezeigten Seite den Bucket aus, dessen Einstellungen Sie ändern möchten.
4. Erweitern Sie den Abschnitt **Ransomware-Scan**.
5. Aktivieren oder deaktivieren Sie den **Ransomware-Scan**.
6. Wählen Sie **Geplanter Ransomware-Scan**.
7. Ändern Sie optional den wöchentlichen Standardscan auf Tage oder Wochen.
8. Legen Sie fest, wie oft (in Tagen oder Wochen) der Scan ausgeführt werden soll.
9. Wählen Sie **Übernehmen**.

Sichern Sie Cloud Volumes ONTAP -Daten mit NetApp Backup and Recovery auf Amazon S3

Führen Sie einige Schritte in NetApp Backup and Recovery aus, um mit der Sicherung von Volume-Daten von Ihren Cloud Volumes ONTAP Systemen auf Amazon S3 zu beginnen.

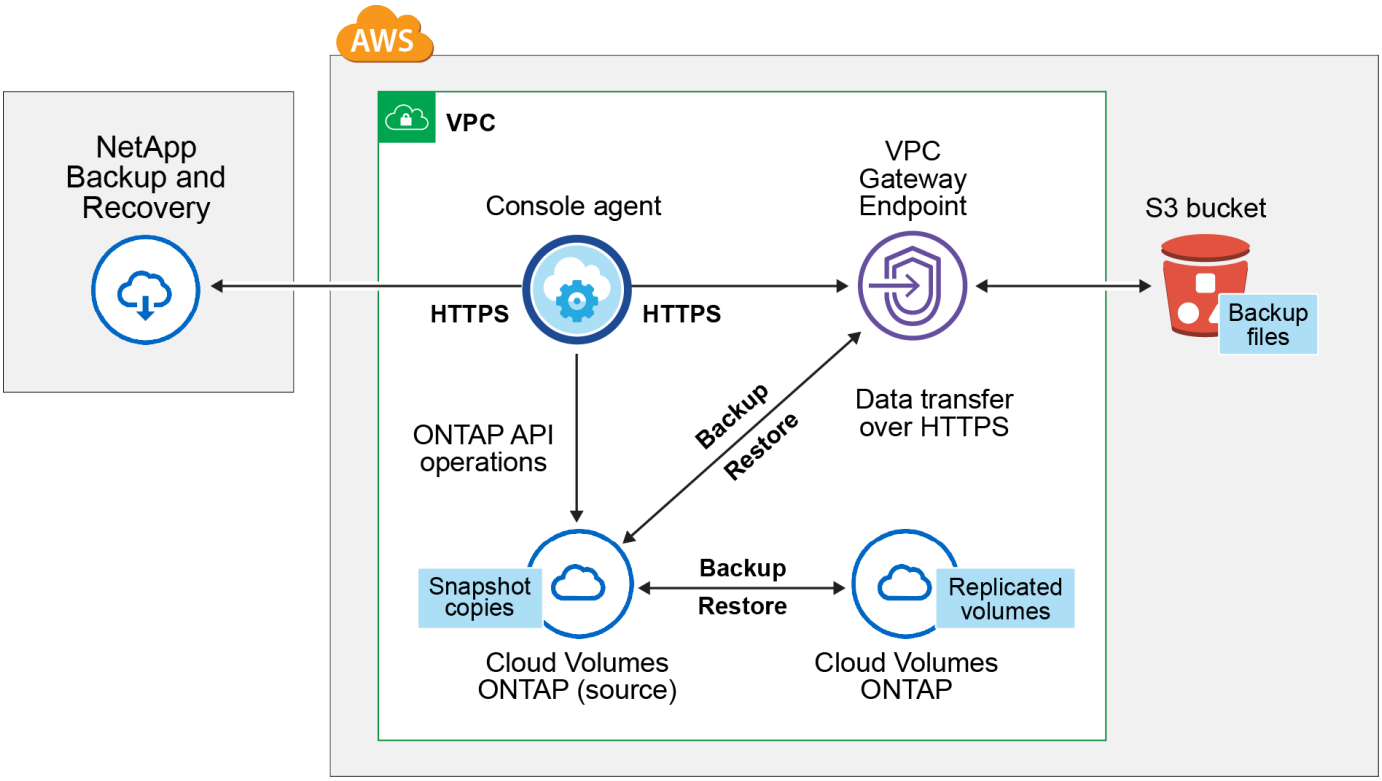
Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

Überprüfen der Unterstützung für Ihre Konfiguration

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie mit der Sicherung von Volumes auf S3 beginnen.

Das folgende Bild zeigt jede Komponente und die Verbindungen, die Sie zwischen ihnen vorbereiten müssen.

Optional können Sie auch über die öffentliche oder private Verbindung eine Verbindung zu einem sekundären ONTAP System für replizierte Volumes herstellen.



Der VPC-Gateway-Endpunkt muss bereits in Ihrer VPC vorhanden sein. "Erfahren Sie mehr über Gateway-Endpunkte" .

Unterstützte ONTAP-Versionen

Mindestens ONTAP 9.8; ONTAP 9.8P13 und höher wird empfohlen.

Erforderliche Informationen zur Verwendung von kundenverwalteten Schlüsseln zur Datenverschlüsselung

Sie können im Aktivierungsassistenten Ihre eigenen, vom Kunden verwalteten Schlüssel für die Datenverschlüsselung auswählen, anstatt die standardmäßigen Amazon S3-Verschlüsselungsschlüssel zu verwenden. In diesem Fall müssen Sie die verwalteten Verschlüsselungsschlüssel bereits eingerichtet haben. "Erfahren Sie, wie Sie Ihre eigenen Schlüssel verwenden" .

Überprüfen der Lizenzanforderungen

Für die NetApp Backup and Recovery PAYGO-Lizenzierung ist im AWS Marketplace ein Konsolenabonnement verfügbar, das die Bereitstellung von Cloud Volumes ONTAP und NetApp Backup and Recovery ermöglicht. Sie müssen "dieses NetApp Console Abonnement abonnieren" bevor Sie NetApp Backup and Recovery aktivieren. Die Abrechnung für NetApp Backup and Recovery erfolgt über dieses Abonnement.

Für einen Jahresvertrag, der Ihnen die Sicherung von Cloud Volumes ONTAP -Daten und On-Premises-ONTAP -Daten ermöglicht, müssen Sie sich über die "AWS Marketplace-Seite" und dann "Verknüpfen Sie das Abonnement mit Ihren AWS-Anmeldeinformationen" .

Für einen Jahresvertrag, der Ihnen die Bündelung von Cloud Volumes ONTAP und NetApp Backup and Recovery ermöglicht, müssen Sie den Jahresvertrag beim Erstellen eines Cloud Volumes ONTAP Systems einrichten. Mit dieser Option können Sie keine lokalen Daten sichern.

Für die NetApp Backup and Recovery BYOL-Lizenzierung benötigen Sie die Seriennummer von NetApp , die Ihnen die Nutzung des Dienstes für die Dauer und Kapazität der Lizenz ermöglicht. "Erfahren Sie, wie Sie Ihre BYOL-Lizenzen verwalten". Sie müssen eine BYOL-Lizenz verwenden, wenn der Konsolenagent und das

Cloud Volumes ONTAP -System an einem Dark Site bereitgestellt werden.

Und Sie benötigen ein AWS-Konto für den Speicherplatz, auf dem Ihre Backups gespeichert werden.

Vorbereiten Ihres Konsolenagenten

Der Konsolenagent muss in einer AWS-Region mit vollständigem oder eingeschränktem Internetzugang („Standard“- oder „eingeschränkter“ Modus) installiert werden. "Weitere Informationen finden Sie unter Bereitstellungsmodi der NetApp Console." .

- "Erfahren Sie mehr über Konsolenagenten"
- "Stellen Sie einen Konsolenagenten in AWS im Standardmodus bereit (vollständiger Internetzugang)."
- "Installieren Sie den Konsolenagenten im eingeschränkten Modus (eingeschränkter ausgehender Zugriff)."

Überprüfen oder Hinzufügen von Berechtigungen für den Konsolenagenten

Die IAM-Rolle, die der Konsole Berechtigungen erteilt, muss S3-Berechtigungen der neuesten Version enthalten. "Konsolenrichtlinie" . Wenn die Richtlinie nicht alle diese Berechtigungen enthält, lesen Sie die "AWS-Dokumentation: Bearbeiten von IAM-Richtlinien" .

Hier sind die spezifischen Berechtigungen aus der Richtlinie:

```
{
  "Sid": "backupPolicy",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteBucket",
    "s3:GetLifecycleConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:PutBucketTagging",
    "s3:ListBucketVersions",
    "s3:GetObject",
    "s3:DeleteObject",
    "s3:PutObject",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicy",
    "s3:PutBucketPolicy",
    "s3:PutBucketOwnershipControls",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutEncryptionConfiguration",
    "s3:GetObjectVersionTagging",
    "s3:GetBucketObjectLockConfiguration",
    "s3:GetObjectVersionAcl",
    "s3:PutObjectTagging",
    "s3:DeleteObjectTagging",
    "s3:GetObjectRetention",
    "s3:DeleteObjectVersionTagging",
    "s3:PutBucketObjectLockConfiguration",
    "s3:DeleteObjectVersion",
    "s3:GetObjectTagging",
    "s3:PutBucketVersioning",
    "s3:PutObjectVersionTagging",
    "s3:GetBucketVersioning",
    "s3:BypassGovernanceRetention",
    "s3:PutObjectRetention",
    "s3:GetObjectVersion",
    "athena:StartQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryExecution",
    "glue:GetDatabase",
    "glue:GetTable",
```

```
            "glue:CreateTable",
            "glue:CreateDatabase",
            "glue:GetPartitions",
            "glue:BatchCreatePartition",
            "glue:BatchDeletePartition"
        ],
        "Resource": [
            "arn:aws:s3:::netapp-backup-*"
        ]
    }
```

Wenn Sie Backups in AWS China-Regionen erstellen, müssen Sie den AWS-Ressourcennamen „arn“ unter allen *Resource*-Abschnitten in den IAM-Richtlinien von „aws“ in „aws-cn“ ändern. Beispiel: `arn:aws-cn:s3:::netapp-backup-*` .

Erforderliche AWS Cloud Volumes ONTAP Berechtigungen

Wenn auf Ihrem Cloud Volumes ONTAP -System ONTAP 9.12.1 oder eine höhere Software ausgeführt wird, muss die IAM-Rolle, die diesem System Berechtigungen erteilt, einen neuen Satz von S3-Berechtigungen speziell für NetApp Backup and Recovery ab der neuesten Version enthalten. "Cloud Volumes ONTAP -Richtlinie" .

Wenn Sie das Cloud Volumes ONTAP -System mit der Konsolenversion 3.9.23 oder höher erstellt haben, sollten diese Berechtigungen bereits Teil der IAM-Rolle sein. Andernfalls müssen Sie die fehlenden Berechtigungen hinzufügen.

Unterstützte AWS-Regionen

NetApp Backup and Recovery wird in allen AWS-Regionen unterstützt, einschließlich der AWS GovCloud-Regionen.

Erforderliche Einrichtung zum Erstellen von Backups in einem anderen AWS-Konto

Standardmäßig werden Backups mit demselben Konto erstellt, das auch für Ihr Cloud Volumes ONTAP -System verwendet wird. Wenn Sie für Ihre Sicherungen ein anderes AWS-Konto verwenden möchten, müssen Sie:

- Stellen Sie sicher, dass die Berechtigungen „s3:PutBucketPolicy“ und „s3:PutBucketOwnershipControls“ Teil der IAM-Rolle sind, die dem Konsolenagenten Berechtigungen erteilt.
- Fügen Sie die Anmeldeinformationen des AWS-Zielkontos in der Konsole hinzu. "So geht’s" .
- Fügen Sie den Benutzeranmeldeinformationen im zweiten Konto die folgenden Berechtigungen hinzu:

```
"athena:StartQueryExecution",
"athena:GetQueryResults",
"athena:GetQueryExecution",
"glue:GetDatabase",
"glue:GetTable",
"glue:CreateTable",
"glue:CreateDatabase",
"glue:GetPartitions",
"glue:BatchCreatePartition",
"glue:BatchDeletePartition"
```

Erstellen Sie Ihre eigenen Eimer

Standardmäßig erstellt der Dienst Buckets für Sie. Wenn Sie Ihre eigenen Buckets verwenden möchten, können Sie diese vor dem Starten des Backup-Aktivierungsassistenten erstellen und diese Buckets dann im Assistenten auswählen.

"Erfahren Sie mehr über das Erstellen eigener Buckets".

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replikation von Volumes

Wenn Sie mit NetApp Backup and Recovery replizierte Volumes auf einem sekundären ONTAP System erstellen möchten, stellen Sie sicher, dass die Quell- und Zielsysteme die folgenden Netzwerkanforderungen erfüllen.

On-Premises ONTAP Netzwerkanforderungen

- Wenn sich der Cluster vor Ort befindet, sollten Sie über eine Verbindung von Ihrem Unternehmensnetzwerk zu Ihrem virtuellen Netzwerk beim Cloud-Anbieter verfügen. Dies ist normalerweise eine VPN-Verbindung.
- ONTAP -Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Clusteranforderungen erfüllen.

  Da Sie auf Cloud Volumes ONTAP oder lokale Systeme replizieren können, überprüfen Sie die Peering-Anforderungen für lokale ONTAP -Systeme. "Voraussetzungen für Cluster-Peering in der ONTAP Dokumentation anzeigen" .

Netzwerkanforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen Regeln für eingehenden und ausgehenden Datenverkehr enthalten, insbesondere Regeln für ICMP und die Ports 11104 und 11105. Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.
- Um Daten zwischen zwei Cloud Volumes ONTAP Systemen in unterschiedlichen Subnetzen zu replizieren, müssen die Subnetze zusammen geroutet werden (dies ist die Standardeinstellung).

Aktivieren Sie NetApp Backup and Recovery auf Cloud Volumes ONTAP

Die Aktivierung von NetApp Backup and Recovery ist einfach. Die Schritte unterscheiden sich geringfügig, je nachdem, ob Sie über ein vorhandenes oder ein neues Cloud Volumes ONTAP System verfügen.

- NetApp Backup and Recovery auf einem neuen System aktivieren*

NetApp Backup and Recovery ist im Systemassistenten standardmäßig aktiviert. Stellen Sie sicher, dass die Option aktiviert bleibt.

Sehen "Starten von Cloud Volumes ONTAP in AWS" für Anforderungen und Details zum Erstellen Ihres Cloud Volumes ONTAP Systems.

Schritte

1. Wählen Sie auf der Konsolenseite **Systeme** die Option **System hinzufügen**, wählen Sie den Cloud-Anbieter und wählen Sie **Neu hinzufügen**. Wählen Sie * Cloud Volumes ONTAP erstellen*.
2. Wählen Sie **Amazon Web Services** als Cloud-Anbieter und wählen Sie dann einen Einzelknoten oder ein HA-System.
3. Füllen Sie die Seite „Details und Anmeldeinformationen“ aus.
4. Lassen Sie den Dienst auf der Seite „Dienste“ aktiviert und wählen Sie **Weiter**.
5. Füllen Sie die Seiten im Assistenten aus, um das System bereitzustellen.

Ergebnis

NetApp Backup and Recovery ist auf dem System aktiviert. Nachdem Sie Volumes auf diesen Cloud Volumes ONTAP -Systemen erstellt haben, starten Sie NetApp Backup and Recovery und"Aktivieren Sie die Sicherung auf jedem Volume, das Sie schützen möchten" .

- NetApp Backup and Recovery auf einem bestehenden System aktivieren*

Aktivieren Sie NetApp Backup and Recovery auf einem vorhandenen System jederzeit direkt von der Konsole aus.

Schritte

1. Wählen Sie auf der Konsolenseite **Systeme** den Cluster aus und wählen Sie im rechten Bereich neben „Sicherung und Wiederherstellung“ die Option „Aktivieren“ aus.

   Wenn das Amazon S3-Ziel für Ihre Backups als Cluster auf der Seite **Systeme** vorhanden ist, können Sie den Cluster auf das Amazon S3-System ziehen, um den Setup-Assistenten zu starten.

Aktivieren Sie Backups auf Ihren ONTAP -Volumes

Aktivieren Sie Backups jederzeit direkt von Ihrem lokalen System aus.

Ein Assistent führt Sie durch die folgenden Hauptschritte:

- die Sie sichern möchten
- Definieren Sie die Sicherungsstrategie
- Überprüfen Sie Ihre Auswahl

Sie können auchAPI-Befehle anzeigen im Überprüfungsschritt, damit Sie den Code kopieren können, um die Sicherungsaktivierung für zukünftige Systeme zu automatisieren.

Starten des Assistenten

Schritte

1. Greifen Sie auf eine der folgenden Arten auf den Assistenten „Sicherung und Wiederherstellung aktivieren“ zu:

- Wählen Sie auf der Konsolenseite **Systeme** das System aus und wählen Sie im rechten Bereich neben „Sicherung und Wiederherstellung“ die Option „Aktivieren > Sicherungsvolumes“ aus.

  Wenn das AWS-Ziel für Ihre Backups als System auf der Konsolenseite **Systeme** vorhanden ist, können Sie den ONTAP Cluster auf den AWS-Objektspeicher ziehen.

- Wählen Sie in der Sicherungs- und Wiederherstellungsleiste **Volumes** aus. Wählen Sie auf der Registerkarte „Volumes“ die Option „Aktionen“. ••• Wählen Sie die Option „Symbol“ und aktivieren Sie **3-2-1-Schutz** für ein einzelnes Volume (bei dem die Replikation oder Sicherung auf Objektspeicher noch nicht aktiviert ist).

Auf der Einführungsseite des Assistenten werden die Schutzoptionen angezeigt, darunter lokale Snapshots, Replikation und Backups. Wenn Sie in diesem Schritt die zweite Option gewählt haben, wird die Seite „Sicherungsstrategie definieren“ mit einem ausgewählten Volume angezeigt.

2. Fahren Sie mit den folgenden Optionen fort:
   - Wenn Sie bereits über einen Konsolenagenten verfügen, sind Sie startklar. Wählen Sie einfach **Weiter**.
   - Wenn Sie noch keinen Konsolenagenten haben, wird die Option **Konsolenagenten hinzufügen** angezeigt. SieheVorbereiten Ihres Konsolenagenten .

Wählen Sie die Volumes aus, die Sie sichern möchten

Wählen Sie die Volumes aus, die Sie schützen möchten. Ein geschütztes Volume verfügt über eine oder mehrere der folgenden Optionen: Snapshot-Richtlinie, Replikationsrichtlinie, Backup-to-Object-Richtlinie.

Sie können FlexVol oder FlexGroup -Volumes schützen. Sie können jedoch keine Mischung dieser Volumes auswählen, wenn Sie die Sicherung für ein System aktivieren. Erfahren Sie, wie Sie"Aktivieren Sie die Sicherung für zusätzliche Volumes im System" (FlexVol oder FlexGroup), nachdem Sie die Sicherung für die ersten Volumes konfiguriert haben.

- Sie können eine Sicherung jeweils nur auf einem einzigen FlexGroup -Volume aktivieren.
- Die von Ihnen ausgewählten Volumes müssen über dieselbe SnapLock Einstellung verfügen. Auf allen Volumes muss SnapLock Enterprise aktiviert oder SnapLock sein.

Schritte

Wenn auf die von Ihnen ausgewählten Volumes bereits Snapshot- oder Replikationsrichtlinien angewendet wurden, werden diese vorhandenen Richtlinien durch die später ausgewählten Richtlinien überschrieben.

1. Wählen Sie auf der Seite „Volumes auswählen“ das oder die Volumes aus, die Sie schützen möchten.
   - Filtern Sie die Zeilen optional, um nur Datenträger mit bestimmten Datenträgertypen, Stilen usw. anzuzeigen und so die Auswahl zu vereinfachen.
   - Nachdem Sie das erste Volume ausgewählt haben, können Sie alle FlexVol Volumes auswählen (FlexGroup Volumes können jeweils nur einzeln ausgewählt werden). Um alle vorhandenen FlexVol Volumes zu sichern, markieren Sie zuerst ein Volume und aktivieren Sie dann das Kontrollkästchen in der Titelzeile.
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume.
2. Wählen Sie **Weiter**.

Definieren Sie die Sicherungsstrategie

Zum Definieren der Sicherungsstrategie müssen die folgenden Optionen festgelegt werden:

- Ob Sie eine oder alle Backup-Optionen wünschen: lokale Snapshots, Replikation und Backup auf Objektspeicher
- Architektur
- Lokale Snapshot-Richtlinie
- Replikationsziel und -richtlinie

> Wenn die von Ihnen ausgewählten Volumes andere Snapshot- und Replikationsrichtlinien haben als die Richtlinien, die Sie in diesem Schritt auswählen, werden die vorhandenen Richtlinien überschrieben.

- Informationen zur Sicherung in Objektspeichern (Anbieter, Verschlüsselung, Netzwerk, Sicherungsrichtlinie und Exportoptionen).

Schritte

1. Wählen Sie auf der Seite „Sicherungsstrategie definieren“ eine oder alle der folgenden Optionen aus. Alle drei sind standardmäßig ausgewählt:
   - **Lokale Snapshots**: Wenn Sie eine Replikation oder Sicherung im Objektspeicher durchführen, müssen lokale Snapshots erstellt werden.
   - **Replikation**: Erstellt replizierte Volumes auf einem anderen ONTAP Speichersystem.
   - **Backup**: Sichert Volumes im Objektspeicher. Beim Auswählen vorhandener Buckets oder Konfigurieren neuer Buckets können Sie Volumes in bis zu sechs Buckets pro Cluster sichern.
2. **Architektur**: Wenn Sie Replikation und Sicherung gewählt haben, wählen Sie einen der folgenden Informationsflüsse:
   - **Kaskadierung**: Informationen fließen vom primären Speichersystem zum sekundären und vom sekundären zum Objektspeicher.
   - **Fan-out**: Informationen fließen vom primären Speichersystem zum sekundären *und* vom primären zum Objektspeicher.

     Weitere Informationen zu diesen Architekturen finden Sie unter"Planen Sie Ihren Schutzweg" .
3. **Lokaler Snapshot**: Wählen Sie eine vorhandene Snapshot-Richtlinie oder erstellen Sie eine neue.

   > Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung des Snapshots finden Sie unter"Erstellen einer Richtlinie" .

   Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:

   a. Geben Sie den Namen der Richtlinie ein.
   b. Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
   c. Wählen Sie **Erstellen**.
4. **Replikation**: Legen Sie die folgenden Optionen fest:
   - **Replikationsziel**: Wählen Sie das Zielsystem und die Speicher-VM aus. Optional können Sie das oder die Zielaggregate sowie ein Präfix oder Suffix auswählen, das dem Namen des replizierten Datenträgers hinzugefügt werden soll.
   - **Replikationsrichtlinie**: Wählen Sie eine vorhandene Replikationsrichtlinie aus oder erstellen Sie eine.

Informationen zum Erstellen einer benutzerdefinierten Richtlinie finden Sie unter"Erstellen einer Richtlinie" .

Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:

i. Geben Sie den Namen der Richtlinie ein.

ii. Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.

iii. Wählen Sie **Erstellen**.

5. **Sicherung**: Legen Sie die folgenden Optionen fest:

   - **Anbieter**: Wählen Sie **Amazon Web Services**.
   - **Anbietereinstellungen**: Geben Sie die Anbieterdetails und die Region ein, in der die Backups gespeichert werden.

     Geben Sie das AWS-Konto ein, das zum Speichern der Sicherungen verwendet wird. Dies kann ein anderes Konto sein als das, auf dem sich das Cloud Volumes ONTAP -System befindet.

     Wenn Sie für Ihre Sicherungen ein anderes AWS-Konto verwenden möchten, müssen Sie die Anmeldeinformationen des AWS-Zielkontos in der Konsole hinzufügen und der IAM-Rolle, die der Konsole Berechtigungen erteilt, die Berechtigungen „s3:PutBucketPolicy“ und „s3:PutBucketOwnershipControls“ hinzufügen.

     Wählen Sie die Region aus, in der die Sicherungen gespeichert werden sollen. Dies kann eine andere Region sein als die, in der sich das Cloud Volumes ONTAP -System befindet.

     Erstellen Sie entweder einen neuen Bucket oder wählen Sie einen vorhandenen aus.

   - **Verschlüsselung**: Wenn Sie einen neuen Bucket erstellt haben, geben Sie die Ihnen vom Anbieter mitgeteilten Verschlüsselungsschlüsselinformationen ein. Entscheiden Sie, ob Sie die standardmäßigen AWS-Verschlüsselungsschlüssel verwenden oder Ihre eigenen, vom Kunden verwalteten Schlüssel aus Ihrem AWS-Konto auswählen möchten, um die Verschlüsselung Ihrer Daten zu verwalten. ("Erfahren Sie, wie Sie Ihre eigenen Verschlüsselungsschlüssel verwenden").

     Wenn Sie Ihre eigenen, vom Kunden verwalteten Schlüssel verwenden möchten, geben Sie den Schlüsseltresor und die Schlüsselinformationen ein.

     Wenn Sie einen vorhandenen Bucket ausgewählt haben, sind die Verschlüsselungsinformationen bereits verfügbar, sodass Sie sie jetzt nicht eingeben müssen.

   - **Netzwerk**: Konfigurieren Sie die Netzwerkoptionen für diesen Anbieter.
   - **Sicherungsrichtlinie**: Wählen Sie eine vorhandene Richtlinie für die Sicherung in Objektspeicher aus oder erstellen Sie eine.

     Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Sicherung finden Sie unter"Erstellen einer Richtlinie" .

     Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:

     i. Geben Sie den Namen der Richtlinie ein.

     ii. Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.

iii. Legen Sie für Backup-to-Object-Richtlinien die Einstellungen „DataLock“ und „Ransomware Resilience“ fest. Weitere Informationen zu DataLock und Ransomware Resilience finden Sie unter"Einstellungen der Backup-to-Object-Richtlinie" .

iv. Wählen Sie **Erstellen**.

- **Vorhandenen Snapshot exportieren**: Wenn es lokale Snapshots für Volumes in diesem System gibt, die mit der von Ihnen soeben für dieses System ausgewählten Sicherungszeitplanbezeichnung übereinstimmen (z. B. täglich, wöchentlich usw.), wird diese zusätzliche Aufforderung angezeigt. Aktivieren Sie dieses Kontrollkästchen, um alle historischen Snapshots als Sicherungsdateien im Objektspeicher zu speichern und so einen umfassenden Schutz Ihrer Volumes zu gewährleisten.

6. Wählen Sie **Weiter**.

Überprüfen Sie Ihre Auswahl

Dies ist die Gelegenheit, Ihre Auswahl zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

Schritte

1. Überprüfen Sie Ihre Auswahl auf der Überprüfungsseite.
2. Optional können Sie das Kontrollkästchen aktivieren, um **nicht übereinstimmende Bezeichnungen bei lokalen Snapshots, Replikationen und Backups automatisch zu korrigieren**. Dadurch werden Snapshots mit einer Bezeichnung erstellt, die mit den Bezeichnungen in den Snapshot-, Replikations- und Sicherungsrichtlinien übereinstimmt.
3. Wählen Sie **Backup aktivieren**.

Ergebnis

NetApp Backup and Recovery beginnt mit der Durchführung der ersten Sicherungen Ihrer Volumes. Die Basisübertragung des replizierten Volumes und der Sicherungsdatei umfasst eine vollständige Kopie der Daten des primären Speichersystems. Nachfolgende Übertragungen enthalten differentielle Kopien der Daten des primären Speichersystems, die in Snapshots enthalten sind.

Im Zielcluster wird ein repliziertes Volume erstellt, das mit dem primären Speichervolume synchronisiert wird.

Im durch den von Ihnen eingegebenen S3-Zugriffsschlüssel und geheimen Schlüssel angegebenen Dienstkonto wird ein S3-Bucket erstellt und die Sicherungsdateien werden dort gespeichert.

Das Volume-Backup-Dashboard wird angezeigt, damit Sie den Status der Backups überwachen können.

Sie können den Status von Sicherungs- und Wiederherstellungsaufträgen auch mithilfe der"Seite „Jobüberwachung“" .

API-Befehle anzeigen

Möglicherweise möchten Sie die im Assistenten „Sicherung und Wiederherstellung aktivieren“ verwendeten API-Befehle anzeigen und optional kopieren. Möglicherweise möchten Sie dies tun, um die Sicherungsaktivierung in zukünftigen Systemen zu automatisieren.

Schritte

1. Wählen Sie im Assistenten „Sicherung und Wiederherstellung aktivieren“ die Option „API-Anforderung anzeigen“ aus.
2. Um die Befehle in die Zwischenablage zu kopieren, wählen Sie das Symbol **Kopieren**.

Sichern Sie Cloud Volumes ONTAP -Daten mit NetApp Backup and Recovery auf Azure Blob Storage

Führen Sie einige Schritte in NetApp Backup and Recovery aus, um mit der Sicherung von Volumedaten von Ihren Cloud Volumes ONTAP -Systemen in Azure Blob Storage zu beginnen.

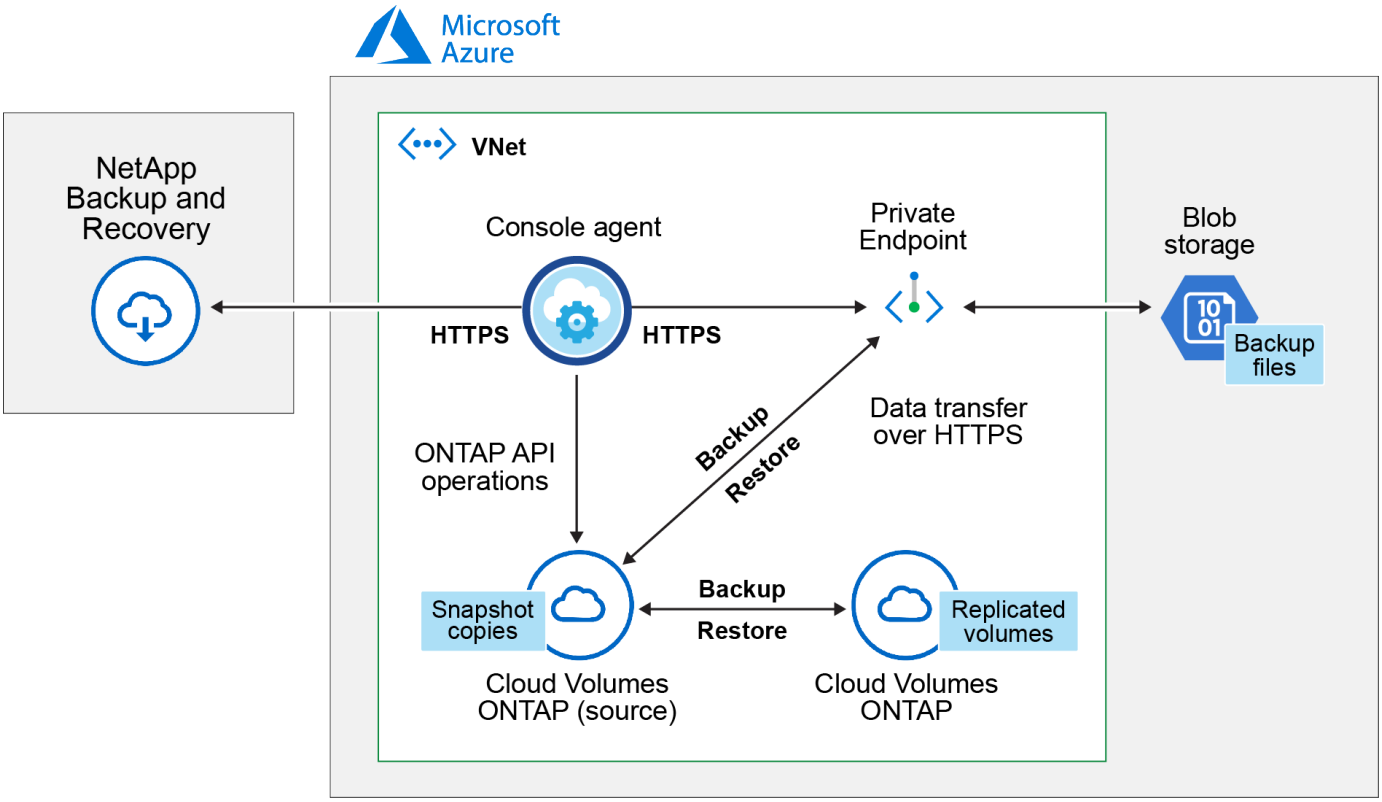
Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

Überprüfen der Unterstützung für Ihre Konfiguration

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie mit der Sicherung von Volumes im Azure Blob-Speicher beginnen.

Das folgende Bild zeigt jede Komponente und die Verbindungen, die Sie zwischen ihnen vorbereiten müssen.

Optional können Sie auch über die öffentliche oder private Verbindung eine Verbindung zu einem sekundären ONTAP System für replizierte Volumes herstellen.



Unterstützte ONTAP-Versionen

Mindestens ONTAP 9.8; ONTAP 9.8P13 und höher wird empfohlen.

Unterstützte Azure-Regionen

NetApp Backup and Recovery wird in allen Azure-Regionen unterstützt, einschließlich der Azure Government-Regionen.

Standardmäßig stellt NetApp Backup and Recovery den Blob-Container zur Kostenoptimierung mit lokaler Redundanz (LRS) bereit. Sie können diese Einstellung nach der Aktivierung von NetApp Backup and

Recovery in Zonenredundanz (ZRS) ändern, wenn Sie sicherstellen möchten, dass Ihre Daten zwischen verschiedenen Zonen repliziert werden. Siehe die Microsoft-Anweisungen für "Ändern der Replikation Ihres Speicherkontos" .

Erforderliche Einrichtung zum Erstellen von Sicherungen in einem anderen Azure-Abonnement

Standardmäßig werden Backups mit demselben Abonnement erstellt, das auch für Ihr Cloud Volumes ONTAP -System verwendet wird.

Überprüfen der Lizenzanforderungen

Für die NetApp Backup and Recovery PAYGO-Lizenzierung ist ein Abonnement über den Azure Marketplace erforderlich, bevor Sie NetApp Backup and Recovery aktivieren. Die Abrechnung für NetApp Backup and Recovery erfolgt über dieses Abonnement. "Sie können sich über die Seite „Details und Anmeldeinformationen“ des Systemassistenten anmelden." .

Für die NetApp Backup and Recovery BYOL-Lizenzierung benötigen Sie die Seriennummer von NetApp , die Ihnen die Nutzung des Dienstes für die Dauer und Kapazität der Lizenz ermöglicht. "Erfahren Sie, wie Sie Ihre BYOL-Lizenzen verwalten". Sie müssen eine BYOL-Lizenz verwenden, wenn der Konsolenagent und das Cloud Volumes ONTAP -System an einem dunklen Standort („privater Modus“) bereitgestellt werden.

Und Sie benötigen ein Microsoft Azure-Abonnement für den Speicherplatz, auf dem Ihre Backups gespeichert werden.

Vorbereiten Ihres Konsolenagenten

Der Konsolen-Agent kann in einer Azure-Region mit vollständigem oder eingeschränktem Internetzugang („Standard“- oder „eingeschränkter“ Modus) installiert werden. "Weitere Informationen finden Sie unter Bereitstellungsmodi der NetApp Console." .

- "Erfahren Sie mehr über Konsolenagenten"
- "Bereitstellen eines Konsolen-Agenten in Azure im Standardmodus (vollständiger Internetzugang)"
- "Installieren Sie den Konsolenagenten im eingeschränkten Modus (eingeschränkter ausgehender Zugriff)."

Überprüfen oder Hinzufügen von Berechtigungen für den Konsolenagenten

Um die Such- und Wiederherstellungsfunktion von NetApp Backup and Recovery verwenden zu können, benötigen Sie bestimmte Berechtigungen in der Rolle für den Konsolenagenten, damit dieser auf den Azure Synapse-Arbeitsbereich und das Data Lake-Speicherkonto zugreifen kann. Sehen Sie sich die Berechtigungen unten an und befolgen Sie die Schritte, wenn Sie die Richtlinie ändern müssen.

Bevor Sie beginnen

- Sie müssen den Azure Synapse Analytics-Ressourcenanbieter (genannt „Microsoft.Synapse“) mit Ihrem Abonnement registrieren. "Erfahren Sie, wie Sie diesen Ressourcenanbieter für Ihr Abonnement registrieren." . Sie müssen der **Eigentümer** oder **Mitwirkende** des Abonnements sein, um den Ressourcenanbieter zu registrieren.
- Port 1433 muss für die Kommunikation zwischen dem Konsolen-Agent und den Azure Synapse SQL-Diensten geöffnet sein.

Schritte

1. Identifizieren Sie die der virtuellen Maschine des Konsolenagenten zugewiesene Rolle:
   a. Öffnen Sie im Azure-Portal den Dienst für virtuelle Computer.
   b. Wählen Sie die virtuelle Maschine des Konsolenagenten aus.

c. Wählen Sie unter „Einstellungen“ die Option „Identität“ aus.

d. Wählen Sie **Azure-Rollenzuweisungen** aus.

e. Notieren Sie sich die benutzerdefinierte Rolle, die der virtuellen Maschine des Konsolenagenten zugewiesen ist.

2. Aktualisieren Sie die benutzerdefinierte Rolle:

a. Öffnen Sie im Azure-Portal Ihr Azure-Abonnement.

b. Wählen Sie **Zugriffskontrolle (IAM) > Rollen**.

c. Wählen Sie die Auslassungspunkte (**…**) für die benutzerdefinierte Rolle und wählen Sie dann **Bearbeiten**.

d. Wählen Sie **JSON** aus und fügen Sie die folgenden Berechtigungen hinzu:

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"Vollständiges JSON-Format für die Richtlinie anzeigen"

e. Wählen Sie **Überprüfen + Aktualisieren** und dann **Aktualisieren**.

Erforderliche Informationen zur Verwendung von kundenverwalteten Schlüsseln zur Datenverschlüsselung

Sie können im Aktivierungsassistenten Ihre eigenen, vom Kunden verwalteten Schlüssel zur Datenverschlüsselung verwenden, anstatt die standardmäßigen, von Microsoft verwalteten Verschlüsselungsschlüssel zu verwenden. In diesem Fall benötigen Sie das Azure-Abonnement, den Key Vault-Namen und den Schlüssel. "Erfahren Sie, wie Sie Ihre eigenen Schlüssel verwenden" .

NetApp Backup and Recovery unterstützt *Azure-Zugriffsrichtlinien*, das *Azure-rollenbasierte Zugriffssteuerungsmodell* (Azure RBAC) und das *Managed Hardware Security Model* (HSM) (siehe "Was ist Azure Key Vault Managed HSM?").

Erstellen Ihres Azure Blob-Speicherkontos

Standardmäßig erstellt der Dienst Speicherkonten für Sie. Wenn Sie Ihre eigenen Speicherkonten verwenden möchten, können Sie diese vor dem Starten des Sicherungsaktivierungsassistenten erstellen und diese Speicherkonten dann im Assistenten auswählen.

"Erfahren Sie mehr über das Erstellen eigener Speicherkonten".

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replikation von Volumes

Wenn Sie mit NetApp Backup and Recovery replizierte Volumes auf einem sekundären ONTAP System erstellen möchten, stellen Sie sicher, dass die Quell- und Zielsysteme die folgenden Netzwerkanforderungen erfüllen.

On-Premises ONTAP Netzwerkanforderungen

- Wenn sich der Cluster vor Ort befindet, sollten Sie über eine Verbindung von Ihrem Unternehmensnetzwerk zu Ihrem virtuellen Netzwerk beim Cloud-Anbieter verfügen. Dies ist normalerweise eine VPN-Verbindung.
- ONTAP -Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Clusteranforderungen erfüllen.

  Da Sie auf Cloud Volumes ONTAP oder lokale Systeme replizieren können, überprüfen Sie die Peering-Anforderungen für lokale ONTAP -Systeme. "Voraussetzungen für Cluster-Peering in der ONTAP Dokumentation anzeigen" .

Netzwerkanforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen Regeln für eingehenden und ausgehenden Datenverkehr enthalten, insbesondere Regeln für ICMP und die Ports 11104 und 11105. Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.
- Um Daten zwischen zwei Cloud Volumes ONTAP Systemen in unterschiedlichen Subnetzen zu replizieren, müssen die Subnetze zusammen geroutet werden (dies ist die Standardeinstellung).

Aktivieren Sie NetApp Backup and Recovery auf Cloud Volumes ONTAP

Die Aktivierung von NetApp Backup and Recovery ist einfach. Die Schritte unterscheiden sich geringfügig, je nachdem, ob Sie über ein vorhandenes oder ein neues Cloud Volumes ONTAP System verfügen.

- NetApp Backup and Recovery auf einem neuen System aktivieren*

NetApp Backup and Recovery ist im Systemassistenten standardmäßig aktiviert. Stellen Sie sicher, dass die Option aktiviert bleibt.

Sehen "Starten von Cloud Volumes ONTAP in Azure" für Anforderungen und Details zum Erstellen Ihres Cloud Volumes ONTAP Systems.

> Wenn Sie den Namen der Ressourcengruppe auswählen möchten, **deaktivieren** Sie NetApp Backup and Recovery, wenn Sie Cloud Volumes ONTAP bereitstellen.

Schritte

1. Wählen Sie auf der Konsolenseite **Systeme** die Option **System hinzufügen**, wählen Sie den Cloud-Anbieter und wählen Sie **Neu hinzufügen**. Wählen Sie * Cloud Volumes ONTAP erstellen*.
2. Wählen Sie **Microsoft Azure** als Cloud-Anbieter und wählen Sie dann einen Einzelknoten oder ein HA-System.
3. Geben Sie auf der Seite „Azure-Anmeldeinformationen definieren“ den Anmeldeinformationsnamen, die Client-ID, das Clientgeheimnis und die Verzeichnis-ID ein und wählen Sie **Weiter** aus.
4. Füllen Sie die Seite „Details und Anmeldeinformationen“ aus, stellen Sie sicher, dass ein Azure Marketplace-Abonnement vorhanden ist, und wählen Sie **Weiter** aus.
5. Lassen Sie den Dienst auf der Seite „Dienste“ aktiviert und wählen Sie **Weiter**.
6. Füllen Sie die Seiten im Assistenten aus, um das System bereitzustellen.

Ergebnis

NetApp Backup and Recovery ist auf dem System aktiviert. Nachdem Sie Volumes auf diesen Cloud Volumes ONTAP -Systemen erstellt haben, starten Sie NetApp Backup and Recovery und"Aktivieren Sie die Sicherung auf jedem Volume, das Sie schützen möchten" .

- NetApp Backup and Recovery auf einem bestehenden System aktivieren*

Aktivieren Sie NetApp Backup and Recovery jederzeit direkt vom System aus.

Schritte

1. Wählen Sie auf der Konsolenseite **Systeme** das System aus und wählen Sie im rechten Bereich neben „Sicherung und Wiederherstellung“ die Option „Aktivieren“ aus.

   Wenn das Azure Blob-Ziel für Ihre Sicherungen als System auf der Konsolenseite **Systeme** vorhanden ist, können Sie den Cluster auf das Azure Blob-System ziehen, um den Setup-Assistenten zu starten.

2. Füllen Sie die Seiten im Assistenten aus, um NetApp Backup and Recovery bereitzustellen.
3. Wenn Sie Backups starten möchten, fahren Sie fort mitAktivieren Sie Backups auf Ihren ONTAP -Volumes .

Aktivieren Sie Backups auf Ihren ONTAP -Volumes

Aktivieren Sie Backups jederzeit direkt von Ihrem lokalen System aus.

Ein Assistent führt Sie durch die folgenden Hauptschritte:

- die Sie sichern möchten
- Definieren Sie die Sicherungsstrategie
- Überprüfen Sie Ihre Auswahl

Sie können auchAPI-Befehle anzeigen im Überprüfungsschritt, damit Sie den Code kopieren können, um die Sicherungsaktivierung für zukünftige Systeme zu automatisieren.

Starten des Assistenten

Schritte

1. Greifen Sie auf eine der folgenden Arten auf den Assistenten „Sicherung und Wiederherstellung aktivieren“ zu:

   - Wählen Sie auf der Konsolenseite **Systeme** das System aus und wählen Sie im rechten Bereich neben „Sicherung und Wiederherstellung“ die Option „Aktivieren > Sicherungsvolumes“ aus.

     Wenn das Azure-Ziel für Ihre Sicherungen als System auf der Seite **Systeme** vorhanden ist, können Sie den ONTAP Cluster auf den Azure Blob-Objektspeicher ziehen.

   - Wählen Sie in der Leiste „Sichern und Wiederherstellen“ **Volumes** aus. Wählen Sie auf der Registerkarte „Volumes“ die Option „Aktionen“ aus. ••• und wählen Sie **Sicherung aktivieren** für ein einzelnes Volume (für das die Replikation oder Sicherung in den Objektspeicher noch nicht aktiviert ist).

   Auf der Einführungsseite des Assistenten werden die Schutzoptionen angezeigt, darunter lokale Snapshots, Replikation und Backups. Wenn Sie in diesem Schritt die zweite Option gewählt haben, wird die Seite „Sicherungsstrategie definieren“ mit einem ausgewählten Volume angezeigt.

2. Fahren Sie mit den folgenden Optionen fort:

   - Wenn Sie bereits über einen Konsolenagenten verfügen, sind Sie startklar. Wählen Sie einfach **Weiter**.
   - Wenn Sie noch keinen Konsolenagenten haben, wird die Option **Konsolenagenten hinzufügen** angezeigt. SieheVorbereiten Ihres Konsolenagenten .

Wählen Sie die Volumes aus, die Sie sichern möchten

Wählen Sie die Volumes aus, die Sie schützen möchten. Ein geschütztes Volume verfügt über eine oder mehrere der folgenden Eigenschaften: Snapshot-Richtlinie, Replikationsrichtlinie, Backup-to-Object-Richtlinie.

Sie können FlexVol oder FlexGroup -Volumes schützen. Sie können jedoch keine Mischung dieser Volumes auswählen, wenn Sie die Sicherung für ein System aktivieren. Erfahren Sie, wie Sie"Aktivieren Sie die Sicherung für zusätzliche Volumes im System" (FlexVol oder FlexGroup), nachdem Sie die Sicherung für die ersten Volumes konfiguriert haben.

- Sie können eine Sicherung jeweils nur auf einem einzigen FlexGroup -Volume aktivieren.
- Die von Ihnen ausgewählten Volumes müssen über dieselbe SnapLock Einstellung verfügen. Auf allen Volumes muss SnapLock Enterprise aktiviert oder SnapLock sein.

Schritte

Wenn auf die von Ihnen ausgewählten Volumes bereits Snapshot- oder Replikationsrichtlinien angewendet wurden, werden diese vorhandenen Richtlinien durch die später ausgewählten Richtlinien überschrieben.

1. Wählen Sie auf der Seite „Volumes auswählen“ das oder die Volumes aus, die Sie schützen möchten.

   - Filtern Sie die Zeilen optional, um nur Datenträger mit bestimmten Datenträgertypen, Stilen usw. anzuzeigen und so die Auswahl zu vereinfachen.
   - Nachdem Sie das erste Volume ausgewählt haben, können Sie alle FlexVol -Volumes auswählen. (FlexGroup -Volumes können jeweils nur einzeln ausgewählt werden.) Um alle vorhandenen FlexVol Volumes zu sichern, markieren Sie zuerst ein Volume und aktivieren Sie dann das Kontrollkästchen in der Titelzeile.
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume.

2. Wählen Sie **Weiter**.

Definieren Sie die Sicherungsstrategie

Zum Definieren der Sicherungsstrategie müssen die folgenden Optionen festgelegt werden:

- Ob Sie eine oder alle der Backup-Optionen wünschen: lokale Snapshots, Replikation und Backup auf Objektspeicher
- Architektur
- Lokale Snapshot-Richtlinie
- Replikationsziel und -richtlinie

> Wenn die von Ihnen ausgewählten Volumes andere Snapshot- und Replikationsrichtlinien haben als die Richtlinien, die Sie in diesem Schritt auswählen, werden die vorhandenen Richtlinien überschrieben.

- Informationen zur Sicherung in Objektspeichern (Anbieter, Verschlüsselung, Netzwerk, Sicherungsrichtlinie und Exportoptionen).

Schritte

1. Wählen Sie auf der Seite „Sicherungsstrategie definieren“ eine oder alle der folgenden Optionen aus. Alle drei sind standardmäßig ausgewählt:
   - **Lokale Snapshots**: Wenn Sie eine Replikation oder Sicherung im Objektspeicher durchführen, müssen lokale Snapshots erstellt werden.
   - **Replikation**: Erstellt replizierte Volumes auf einem anderen ONTAP Speichersystem.
   - **Backup**: Sichert Volumes im Objektspeicher.
2. **Architektur**: Wenn Sie Replikation und Sicherung gewählt haben, wählen Sie einen der folgenden Informationsflüsse:
   - **Kaskadierung**: Informationen fließen vom primären Speichersystem zum sekundären und vom sekundären zum Objektspeicher.
   - **Fan-out**: Informationen fließen vom primären Speichersystem zum sekundären *und* vom primären zum Objektspeicher.

     Weitere Informationen zu diesen Architekturen finden Sie unter"Planen Sie Ihren Schutzweg" .
3. **Lokaler Snapshot**: Wählen Sie eine vorhandene Snapshot-Richtlinie aus oder erstellen Sie eine.

   > Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung des Snapshots finden Sie unter"Erstellen einer Richtlinie" .

   Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:
   - Geben Sie den Namen der Richtlinie ein.
   - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
   - Wählen Sie **Erstellen**.
4. **Replikation**: Legen Sie die folgenden Optionen fest:
   - **Replikationsziel**: Wählen Sie das Zielsystem und die SVM aus. Wählen Sie optional das oder die Zielaggregate sowie das Präfix oder Suffix aus, das dem Namen des replizierten Volumes hinzugefügt

wird.

- **Replikationsrichtlinie**: Wählen Sie eine vorhandene Replikationsrichtlinie aus oder erstellen Sie eine.

  Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Replikation finden Sie unter"Erstellen einer Richtlinie" .

  Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:

  - Geben Sie den Namen der Richtlinie ein.
  - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
  - Wählen Sie **Erstellen**.

5. **Sichern auf Objekt**: Wenn Sie **Sichern** ausgewählt haben, legen Sie die folgenden Optionen fest:
   - **Anbieter**: Wählen Sie **Microsoft Azure**.
   - **Anbietereinstellungen**: Geben Sie die Anbieterdetails ein.

     Geben Sie die Region ein, in der die Sicherungen gespeichert werden. Dies kann eine andere Region sein als die, in der sich das Cloud Volumes ONTAP -System befindet.

     Erstellen Sie entweder ein neues Speicherkonto oder wählen Sie ein vorhandenes aus.

     Geben Sie das Azure-Abonnement ein, das zum Speichern der Sicherungen verwendet wird. Dies kann ein anderes Abonnement sein als das, in dem sich das Cloud Volumes ONTAP -System befindet.

     Erstellen Sie entweder Ihre eigene Ressourcengruppe, die den Blob-Container verwaltet, oder wählen Sie den Ressourcengruppentyp und die Gruppe aus.

     Wenn Sie Ihre Sicherungsdateien vor Änderungen oder Löschungen schützen möchten, stellen Sie sicher, dass das Speicherkonto mit aktiviertem unveränderlichem Speicher und einer Aufbewahrungsfrist von 30 Tagen erstellt wurde.

   - **Verschlüsselungsschlüssel**: Wenn Sie ein neues Azure-Speicherkonto erstellt haben, geben Sie die Informationen zum Verschlüsselungsschlüssel ein, die Sie vom Anbieter erhalten haben. Wählen Sie, ob Sie die standardmäßigen Azure-Verschlüsselungsschlüssel verwenden oder Ihre eigenen, vom Kunden verwalteten Schlüssel aus Ihrem Azure-Konto auswählen möchten, um die Verschlüsselung Ihrer Daten zu verwalten.

     Wenn Sie Ihre eigenen, vom Kunden verwalteten Schlüssel verwenden möchten, geben Sie den Schlüsseltresor und die Schlüsselinformationen ein. "Erfahren Sie, wie Sie Ihre eigenen Schlüssel verwenden" .

     Wenn Sie ein vorhandenes Microsoft-Speicherkonto ausgewählt haben, sind die Verschlüsselungsinformationen bereits verfügbar, sodass Sie sie jetzt nicht eingeben müssen.

   - **Netzwerk**: Wählen Sie den IP-Bereich und geben Sie an, ob Sie einen privaten Endpunkt verwenden möchten. Privater Endpunkt ist standardmäßig deaktiviert.
     i. Der IP-Bereich im ONTAP -Cluster, in dem sich die Volumes befinden, die Sie sichern möchten. Die Intercluster-LIFs für diesen IPspace müssen über ausgehenden Internetzugang verfügen.
     ii. Wählen Sie optional aus, ob Sie einen zuvor konfigurierten privaten Azure-Endpunkt verwenden möchten. "Erfahren Sie mehr über die Verwendung eines privaten Azure-Endpunkts" .

- **Sicherungsrichtlinie**: Wählen Sie eine vorhandene Richtlinie für die Sicherung in Objektspeichern aus.

  Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Sicherung finden Sie unter"Erstellen einer Richtlinie" .

  Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:

  - Geben Sie den Namen der Richtlinie ein.
  - Legen Sie für Backup-to-Object-Richtlinien die Einstellungen „DataLock“ und „Ransomware Resilience“ fest. Weitere Informationen zu DataLock und Ransomware Resilience finden Sie unter"Einstellungen der Backup-to-Object-Richtlinie" .
  - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
  - Wählen Sie **Erstellen**.

- **Vorhandene Snapshots als Sicherungskopien in den Objektspeicher exportieren**: Wenn es lokale Snapshots für Volumes in diesem System gibt, die mit der von Ihnen soeben für dieses System ausgewählten Sicherungszeitplanbezeichnung übereinstimmen (z. B. täglich, wöchentlich usw.), wird diese zusätzliche Aufforderung angezeigt. Aktivieren Sie dieses Kontrollkästchen, um alle historischen Snapshots als Sicherungsdateien in den Objektspeicher zu kopieren und so den umfassendsten Schutz für Ihre Volumes zu gewährleisten.

6. Wählen Sie **Weiter**.

Überprüfen Sie Ihre Auswahl

Dies ist die Gelegenheit, Ihre Auswahl zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

Schritte

1. Überprüfen Sie Ihre Auswahl auf der Überprüfungsseite.
2. Aktivieren Sie optional das Kontrollkästchen, um **die Snapshot-Richtlinienbezeichnungen automatisch mit den Replikations- und Sicherungsrichtlinienbezeichnungen zu synchronisieren**. Dadurch werden Snapshots mit einer Bezeichnung erstellt, die mit den Bezeichnungen in den Replikations- und Sicherungsrichtlinien übereinstimmt.
3. Wählen Sie **Backup aktivieren**.

Ergebnis

NetApp Backup and Recovery beginnt mit der Durchführung der ersten Sicherungen Ihrer Volumes. Die Basisübertragung des replizierten Volumes und der Sicherungsdatei umfasst eine vollständige Kopie der Daten des primären Speichersystems. Nachfolgende Übertragungen enthalten differentielle Kopien der im Primärspeicher enthaltenen Daten, die in Snapshots gespeichert sind.

Im Zielcluster wird ein repliziertes Volume erstellt, das mit dem primären Volume synchronisiert wird.

In der von Ihnen eingegebenen Ressourcengruppe wird ein Blob-Speichercontainer erstellt und die Sicherungsdateien werden dort gespeichert.

Standardmäßig stellt NetApp Backup and Recovery den Blob-Container zur Kostenoptimierung mit lokaler Redundanz (LRS) bereit. Sie können diese Einstellung in Zonenredundanz (ZRS) ändern, wenn Sie sicherstellen möchten, dass Ihre Daten zwischen verschiedenen Zonen repliziert werden. Siehe die Microsoft-Anweisungen für "Ändern der Replikation Ihres Speicherkontos" .

Das Volume-Backup-Dashboard wird angezeigt, damit Sie den Status der Backups überwachen können.

Sie können den Status von Sicherungs- und Wiederherstellungsaufträgen auch mithilfe der"Seite „Jobüberwachung“" .

API-Befehle anzeigen

Möglicherweise möchten Sie die im Assistenten „Sicherung und Wiederherstellung aktivieren“ verwendeten API-Befehle anzeigen und optional kopieren. Möglicherweise möchten Sie dies tun, um die Sicherungsaktivierung in zukünftigen Systemen zu automatisieren.

Schritte

1. Wählen Sie im Assistenten „Sicherung und Wiederherstellung aktivieren“ die Option „API-Anforderung anzeigen“ aus.
2. Um die Befehle in die Zwischenablage zu kopieren, wählen Sie das Symbol **Kopieren**.

Wie geht es weiter?

- Du kannst"Verwalten Sie Ihre Sicherungsdateien und Sicherungsrichtlinien" . Dazu gehören das Starten und Stoppen von Sicherungen, das Löschen von Sicherungen, das Hinzufügen und Ändern des Sicherungszeitplans und mehr.
- Du kannst"Verwalten von Backup-Einstellungen auf Clusterebene" . Dazu gehört das Ändern der Speicherschlüssel, die ONTAP für den Zugriff auf den Cloud-Speicher verwendet, das Ändern der verfügbaren Netzwerkbandbreite zum Hochladen von Backups in den Objektspeicher, das Ändern der automatischen Backup-Einstellung für zukünftige Volumes und mehr.
- Sie können auch"Wiederherstellen von Volumes, Ordnern oder einzelnen Dateien aus einer Sicherungsdatei" zu einem Cloud Volumes ONTAP -System in AWS oder zu einem lokalen ONTAP System.

Sichern Sie Cloud Volumes ONTAP -Daten mit NetApp Backup and Recovery in Google Cloud Storage

Führen Sie einige Schritte in NetApp Backup and Recovery aus, um mit der Sicherung von Volume-Daten von Ihren Cloud Volumes ONTAP Systemen in Google Cloud Storage zu beginnen.

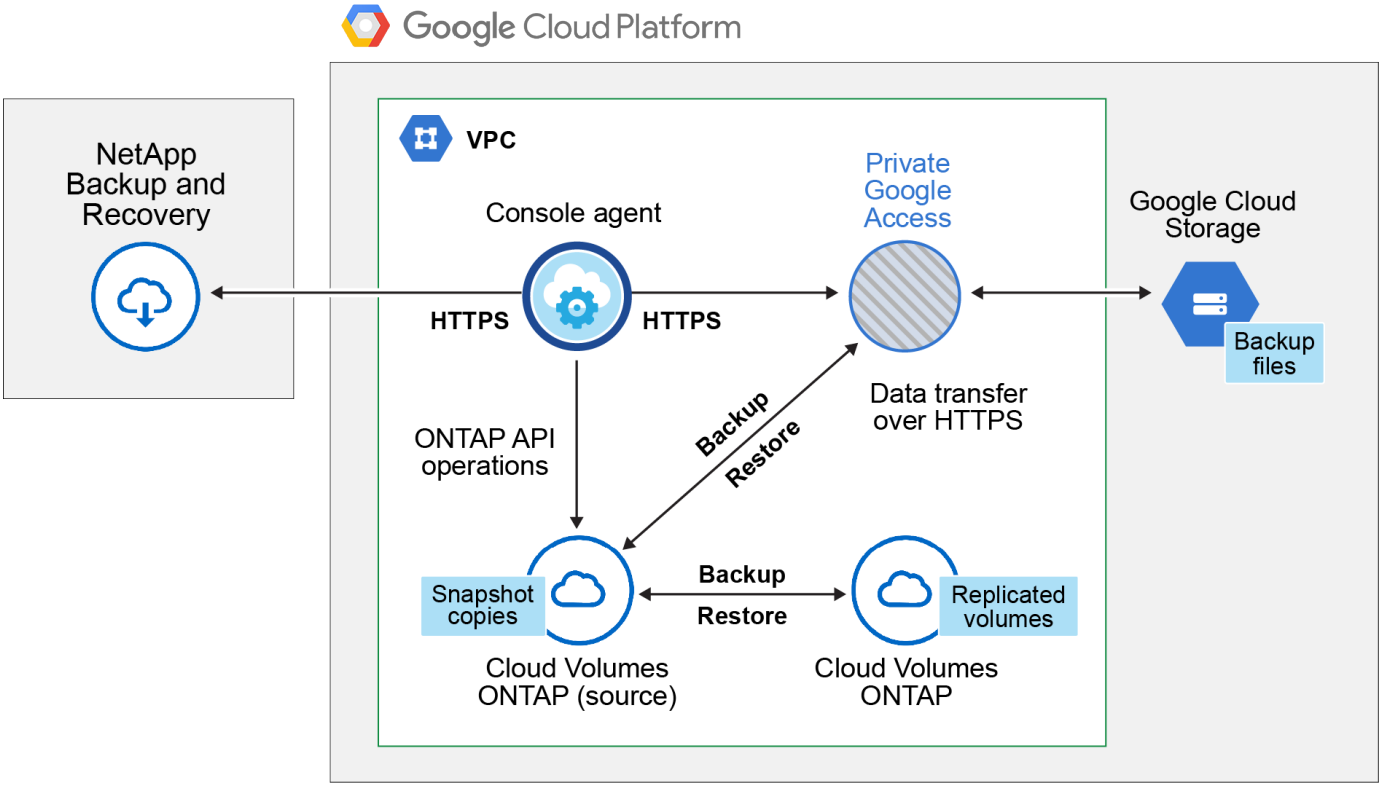
Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

Überprüfen der Unterstützung für Ihre Konfiguration

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie mit der Sicherung von Volumes in Google Cloud Storage beginnen.

Das folgende Bild zeigt jede Komponente und die Verbindungen, die Sie zwischen ihnen vorbereiten müssen.

Optional können Sie auch über die öffentliche oder private Verbindung eine Verbindung zu einem sekundären ONTAP System für replizierte Volumes herstellen.



Unterstützte ONTAP-Versionen

Mindestens ONTAP 9.8; ONTAP 9.8P13 und höher wird empfohlen.

Unterstützte GCP-Regionen

NetApp Backup and Recovery wird in allen GCP-Regionen unterstützt.

GCP-Dienstkonto

Sie benötigen in Ihrem Google Cloud-Projekt ein Dienstkonto mit der benutzerdefinierten Rolle. "Erfahren Sie, wie Sie ein Dienstkonto erstellen" .

Die Rolle „Storage Admin“ ist für das Dienstkonto, das NetApp Backup and Recovery den Zugriff auf Google Cloud Storage-Buckets ermöglicht, nicht mehr erforderlich.

Überprüfen der Lizenzanforderungen

Für die NetApp Backup and Recovery PAYGO-Lizenzierung ist im Google Marketplace ein Konsolenabonnement verfügbar, das die Bereitstellung von Cloud Volumes ONTAP und NetApp Backup and Recovery ermöglicht. Sie müssen "dieses Konsolenabonnement abonnieren" bevor Sie NetApp Backup and Recovery aktivieren. Die Abrechnung für NetApp Backup and Recovery erfolgt über dieses Abonnement. "Sie können sich über die Seite „Details und Anmeldeinformationen“ des Systemassistenten anmelden." .

Für die NetApp Backup and Recovery BYOL-Lizenzierung benötigen Sie die Seriennummer von NetApp , die Ihnen die Nutzung des Dienstes für die Dauer und Kapazität der Lizenz ermöglicht. "Erfahren Sie, wie Sie Ihre BYOL-Lizenzen verwalten".

Und Sie benötigen ein Google-Abonnement für den Speicherplatz, auf dem Ihre Backups gespeichert werden.

Vorbereiten Ihres Konsolenagenten

Der Konsolenagent muss in einer Google-Region mit Internetzugang installiert werden.

- "Erfahren Sie mehr über Konsolenagenten"
- "Bereitstellen eines Konsolenagenten in Google Cloud"

Überprüfen oder Hinzufügen von Berechtigungen für den Konsolenagenten

Um die Funktion „Suchen und Wiederherstellen“ von NetApp Backup and Recovery verwenden zu können, benötigen Sie bestimmte Berechtigungen in der Rolle für den Konsolenagenten, damit dieser auf den Google Cloud BigQuery-Dienst zugreifen kann. Sehen Sie sich die Berechtigungen unten an und befolgen Sie die Schritte, wenn Sie die Richtlinie ändern müssen.

Schritte

1. Im "Google Cloud Console" , gehen Sie zur Seite **Rollen**.
2. Wählen Sie mithilfe der Dropdownliste oben auf der Seite das Projekt oder die Organisation aus, das/die die Rolle enthält, die Sie bearbeiten möchten.
3. Wählen Sie eine benutzerdefinierte Rolle aus.
4. Wählen Sie **Rolle bearbeiten**, um die Berechtigungen der Rolle zu aktualisieren.
5. Wählen Sie **Berechtigungen hinzufügen** aus, um der Rolle die folgenden neuen Berechtigungen hinzuzufügen.

```
bigquery.jobs.get
bigquery.jobs.list
bigquery.jobs.listAll
bigquery.datasets.create
bigquery.datasets.get
bigquery.jobs.create
bigquery.tables.get
bigquery.tables.getData
bigquery.tables.list
bigquery.tables.create
```

6. Wählen Sie **Aktualisieren**, um die bearbeitete Rolle zu speichern.

Erforderliche Informationen zur Verwendung von kundenverwalteten Verschlüsselungsschlüsseln (CMEK)

Sie können Ihre eigenen, vom Kunden verwalteten Schlüssel zur Datenverschlüsselung verwenden, anstatt die standardmäßig von Google verwalteten Verschlüsselungsschlüssel zu verwenden. Es werden sowohl regions- als auch projektübergreifende Schlüssel unterstützt, sodass Sie für einen Bucket ein Projekt auswählen können, das sich vom Projekt des CMEK-Schlüssels unterscheidet. Wenn Sie Ihre eigenen, vom Kunden verwalteten Schlüssel verwenden möchten:

- Sie benötigen den Schlüsselbund und den Schlüsselnamen, damit Sie diese Informationen im Aktivierungsassistenten hinzufügen können. "Erfahren Sie mehr über vom Kunden verwaltete Verschlüsselungsschlüssel" .
- Sie müssen überprüfen, ob die folgenden erforderlichen Berechtigungen in der Rolle für den Konsolenagenten enthalten sind:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Sie müssen überprüfen, ob die Google-API „Cloud Key Management Service (KMS)“ in Ihrem Projekt aktiviert ist. Siehe die "Google Cloud-Dokumentation: APIs aktivieren" für Details.

CMEK-Überlegungen:

- Es werden sowohl HSM-Schlüssel (hardwaregestützt) als auch softwaregenerierte Schlüssel unterstützt.
- Es werden sowohl neu erstellte als auch importierte Cloud KMS-Schlüssel unterstützt.
- Es werden nur regionale Schlüssel unterstützt; globale Schlüssel werden nicht unterstützt.
- Derzeit wird nur der Zweck „Symmetrische Verschlüsselung/Entschlüsselung“ unterstützt.
- Dem mit dem Speicherkonto verknüpften Service-Agent wird von NetApp Backup and Recovery die IAM-Rolle „CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)“ zugewiesen.

Erstellen Sie Ihre eigenen Eimer

Standardmäßig erstellt der Dienst Buckets für Sie. Wenn Sie Ihre eigenen Buckets verwenden möchten, können Sie diese vor dem Starten des Backup-Aktivierungsassistenten erstellen und diese Buckets dann im Assistenten auswählen.

"Erfahren Sie mehr über das Erstellen eigener Buckets".

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replikation von Volumes

Wenn Sie mit NetApp Backup and Recovery replizierte Volumes auf einem sekundären ONTAP System erstellen möchten, stellen Sie sicher, dass die Quell- und Zielsysteme die folgenden Netzwerkanforderungen erfüllen.

On-Premises ONTAP Netzwerkanforderungen

- Wenn sich der Cluster vor Ort befindet, sollten Sie über eine Verbindung von Ihrem Unternehmensnetzwerk zu Ihrem virtuellen Netzwerk beim Cloud-Anbieter verfügen. Dies ist normalerweise eine VPN-Verbindung.
- ONTAP -Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Clusteranforderungen erfüllen.

  Da Sie auf Cloud Volumes ONTAP oder lokale Systeme replizieren können, überprüfen Sie die Peering-Anforderungen für lokale ONTAP -Systeme. "Voraussetzungen für Cluster-Peering in der ONTAP Dokumentation anzeigen" .

Netzwerkanforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen Regeln für eingehenden und ausgehenden Datenverkehr enthalten, insbesondere Regeln für ICMP und die Ports 11104 und 11105. Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.
- Um Daten zwischen zwei Cloud Volumes ONTAP Systemen in unterschiedlichen Subnetzen zu replizieren, müssen die Subnetze zusammen geroutet werden (dies ist die Standardeinstellung).

Aktivieren Sie NetApp Backup and Recovery auf Cloud Volumes ONTAP

Die Schritte zum Aktivieren von NetApp Backup and Recovery unterscheiden sich geringfügig, je nachdem, ob Sie über ein vorhandenes oder ein neues Cloud Volumes ONTAP -System verfügen.

- NetApp Backup and Recovery auf einem neuen System aktivieren*

NetApp Backup and Recovery kann aktiviert werden, wenn Sie den Systemassistenten zum Erstellen eines neuen Cloud Volumes ONTAP Systems abschließen.

Sie müssen bereits ein Dienstkonto konfiguriert haben. Wenn Sie beim Erstellen des Cloud Volumes ONTAP -Systems kein Dienstkonto auswählen, müssen Sie das System ausschalten und das Dienstkonto über die GCP-Konsole zu Cloud Volumes ONTAP hinzufügen.

Sehen "Starten von Cloud Volumes ONTAP in GCP" für Anforderungen und Details zum Erstellen Ihres Cloud Volumes ONTAP Systems.

Schritte

1. Wählen Sie auf der Konsolenseite **Systeme** die Option **System hinzufügen**, wählen Sie den Cloud-Anbieter und wählen Sie **Neu hinzufügen**. Wählen Sie * Cloud Volumes ONTAP erstellen*.
2. **Wählen Sie einen Standort**: Wählen Sie **Google Cloud Platform**.
3. **Typ auswählen**: Wählen Sie * Cloud Volumes ONTAP* (entweder Einzelknoten oder Hochverfügbarkeit).
4. **Details und Anmeldeinformationen**: Geben Sie die folgenden Informationen ein:
    a. Klicken Sie auf **Projekt bearbeiten** und wählen Sie ein neues Projekt aus, wenn das von Ihnen gewünschte Projekt sich vom Standardprojekt (in dem sich der Konsolenagent befindet) unterscheidet.
    b. Geben Sie den Clusternamen an.
    c. Aktivieren Sie den Schalter **Dienstkonto** und wählen Sie das Dienstkonto aus, das über die vordefinierte Rolle „Speicheradministrator“ verfügt. Dies ist erforderlich, um Backups und Tiering zu aktivieren.
    d. Geben Sie die Anmeldeinformationen an.

    Stellen Sie sicher, dass ein GCP Marketplace-Abonnement vorhanden ist.
5. **Dienste**: Lassen Sie NetApp Backup and Recovery aktiviert und klicken Sie auf **Weiter**.
6. Füllen Sie die Seiten im Assistenten aus, um das System wie in beschrieben bereitzustellen "Starten von Cloud Volumes ONTAP in GCP" .

Ergebnis

NetApp Backup and Recovery ist auf dem System aktiviert. Nachdem Sie Volumes auf diesen Cloud Volumes ONTAP -Systemen erstellt haben, starten Sie NetApp Backup and Recovery und"Aktivieren Sie die Sicherung auf jedem Volume, das Sie schützen möchten" .

- NetApp Backup and Recovery auf einem bestehenden System aktivieren*

Sie können NetApp Backup and Recovery jederzeit direkt vom System aus aktivieren.

Schritte

1. Wählen Sie auf der Konsolenseite **Systeme** das System aus und wählen Sie im rechten Bereich neben „Sicherung und Wiederherstellung“ die Option „Aktivieren“ aus.

   Wenn das Google Cloud Storage-Ziel für Ihre Sicherungen als System auf der Konsolenseite **Systeme** vorhanden ist, können Sie den Cluster auf das Google Cloud Storage-System ziehen, um den Setup-Assistenten zu starten.

Bereiten Sie Google Cloud Storage als Sicherungsziel vor

Die Vorbereitung von Google Cloud Storage als Sicherungsziel umfasst die folgenden Schritte:

- Richten Sie Berechtigungen ein.
- (Optional) Erstellen Sie Ihre eigenen Buckets. (Der Dienst erstellt auf Wunsch Buckets für Sie.)
- (Optional) Einrichten von kundenverwalteten Schlüsseln für die Datenverschlüsselung

Einrichten von Berechtigungen

Sie müssen Speicherzugriffsschlüssel für ein Dienstkonto bereitstellen, das über bestimmte Berechtigungen mithilfe einer benutzerdefinierten Rolle verfügt. Ein Dienstkonto ermöglicht NetApp Backup and Recovery die Authentifizierung und den Zugriff auf Cloud Storage-Buckets, die zum Speichern von Backups verwendet werden. Die Schlüssel werden benötigt, damit Google Cloud Storage weiß, wer die Anfrage stellt.

Schritte

1. Im "Google Cloud Console" , gehen Sie zur Seite **Rollen**.
2. "Erstellen einer neuen Rolle"mit den folgenden Berechtigungen:

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. In der Google Cloud-Konsole "Gehen Sie zur Seite „Dienstkonten“" .
4. Wählen Sie Ihr Cloud-Projekt aus.
5. Wählen Sie **Dienstkonto erstellen** und geben Sie die erforderlichen Informationen ein:

a. **Servicekontodetails**: Geben Sie einen Namen und eine Beschreibung ein.

b. **Diesem Dienstkonto Zugriff auf das Projekt gewähren**: Wählen Sie die benutzerdefinierte Rolle aus, die Sie gerade erstellt haben.

c. Wählen Sie **Fertig**.

6. Gehe zu "GCP-Speichereinstellungen" und erstellen Sie Zugriffsschlüssel für das Dienstkonto:

a. Wählen Sie ein Projekt und dann **Interoperabilität** aus. Falls Sie dies noch nicht getan haben, wählen Sie **Interoperabilitätszugriff aktivieren**.

b. Wählen Sie unter **Zugriffsschlüssel für Dienstkonten** die Option **Schlüssel für ein Dienstkonto erstellen** aus, wählen Sie das gerade erstellte Dienstkonto aus und klicken Sie auf **Schlüssel erstellen**.

Sie müssen die Schlüssel später in NetApp Backup and Recovery eingeben, wenn Sie den Sicherungsdienst konfigurieren.

Erstellen Sie Ihre eigenen Eimer

Standardmäßig erstellt der Dienst Buckets für Sie. Wenn Sie Ihre eigenen Buckets verwenden möchten, können Sie diese auch erstellen, bevor Sie den Backup-Aktivierungsassistenten starten, und diese Buckets dann im Assistenten auswählen.

"Erfahren Sie mehr über das Erstellen eigener Buckets".

Einrichten von kundenverwalteten Verschlüsselungsschlüsseln (CMEK) zur Datenverschlüsselung

Sie können Ihre eigenen, vom Kunden verwalteten Schlüssel zur Datenverschlüsselung verwenden, anstatt die standardmäßig von Google verwalteten Verschlüsselungsschlüssel zu verwenden. Es werden sowohl regions- als auch projektübergreifende Schlüssel unterstützt, sodass Sie für einen Bucket ein Projekt auswählen können, das sich vom Projekt des CMEK-Schlüssels unterscheidet.

Wenn Sie Ihre eigenen, vom Kunden verwalteten Schlüssel verwenden möchten:

- Sie benötigen den Schlüsselbund und den Schlüsselnamen, damit Sie diese Informationen im Aktivierungsassistenten hinzufügen können. "Erfahren Sie mehr über vom Kunden verwaltete Verschlüsselungsschlüssel" .
- Sie müssen überprüfen, ob die folgenden erforderlichen Berechtigungen in der Rolle für den Konsolenagenten enthalten sind:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Sie müssen überprüfen, ob die Google-API „Cloud Key Management Service (KMS)“ in Ihrem Projekt aktiviert ist. Siehe die "Google Cloud-Dokumentation: APIs aktivieren" für Details.

CMEK-Überlegungen:

- Es werden sowohl HSM-Schlüssel (Hardware-gestützt) als auch softwaregenerierte Schlüssel unterstützt.
- Es werden sowohl neu erstellte als auch importierte Cloud KMS-Schlüssel unterstützt.
- Es werden nur regionale Schlüssel unterstützt, globale Schlüssel werden nicht unterstützt.
- Derzeit wird nur der Zweck „Symmetrische Verschlüsselung/Entschlüsselung“ unterstützt.
- Dem mit dem Speicherkonto verknüpften Service-Agent wird von NetApp Backup and Recovery die IAM-Rolle „CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)“ zugewiesen.

Aktivieren Sie Backups auf Ihren ONTAP -Volumes

Aktivieren Sie Backups jederzeit direkt von Ihrem lokalen System aus.

Ein Assistent führt Sie durch die folgenden Hauptschritte:

- die Sie sichern möchten
- Definieren Sie die Sicherungsstrategie
- Überprüfen Sie Ihre Auswahl

Sie können auchAPI-Befehle anzeigen im Überprüfungsschritt, damit Sie den Code kopieren können, um die Sicherungsaktivierung für zukünftige Systeme zu automatisieren.

Starten des Assistenten

Schritte

1. Greifen Sie auf eine der folgenden Arten auf den Assistenten „Sicherung und Wiederherstellung aktivieren“ zu:

   - Wählen Sie auf der Konsolenseite **Systeme** das System aus und wählen Sie im rechten Bereich neben „Sicherung und Wiederherstellung“ die Option „Aktivieren > Sicherungsvolumes“ aus.

     Wenn das GCP-Ziel für Ihre Backups als System auf der Konsolenseite **Systeme** vorhanden ist, können Sie den ONTAP Cluster auf den GCP-Objektspeicher ziehen.

   - Wählen Sie in der Leiste „Sichern und Wiederherstellen“ **Volumes** aus. Wählen Sie auf der Registerkarte „Volumes“ die Option „Aktionen“ aus. ••• und wählen Sie **Sicherung aktivieren** für ein einzelnes Volume (für das die Replikation oder Sicherung in den Objektspeicher noch nicht aktiviert ist).

   Auf der Einführungsseite des Assistenten werden die Schutzoptionen angezeigt, darunter lokale Snapshots, Replikation und Backups. Wenn Sie in diesem Schritt die zweite Option gewählt haben, wird die Seite „Sicherungsstrategie definieren“ mit einem ausgewählten Volume angezeigt.

2. Fahren Sie mit den folgenden Optionen fort:

   - Wenn Sie bereits über einen Konsolenagenten verfügen, sind Sie startklar. Wählen Sie einfach **Weiter**.
   - Wenn Sie noch keinen Konsolenagenten haben, wird die Option **Konsolenagenten hinzufügen** angezeigt. SieheVorbereiten Ihres Konsolenagenten .

Wählen Sie die Volumes aus, die Sie sichern möchten

Wählen Sie die Volumes aus, die Sie schützen möchten. Ein geschütztes Volume verfügt über eine oder mehrere der folgenden Optionen: Snapshot-Richtlinie, Replikationsrichtlinie, Backup-to-Object-Richtlinie.

Sie können FlexVol oder FlexGroup -Volumes schützen. Sie können jedoch keine Mischung dieser Volumes auswählen, wenn Sie die Sicherung für ein System aktivieren. Erfahren Sie, wie Sie"Aktivieren Sie die Sicherung für zusätzliche Volumes im System" (FlexVol oder FlexGroup), nachdem Sie die Sicherung für die ersten Volumes konfiguriert haben.

- Sie können eine Sicherung jeweils nur auf einem einzigen FlexGroup -Volume aktivieren.
- Die von Ihnen ausgewählten Volumes müssen über dieselbe SnapLock Einstellung verfügen. Auf allen Volumes muss SnapLock Enterprise aktiviert oder SnapLock sein.

Schritte

Beachten Sie: Wenn auf die von Ihnen ausgewählten Volumes bereits Snapshot- oder Replikationsrichtlinien angewendet wurden, werden diese vorhandenen Richtlinien durch die später ausgewählten Richtlinien überschrieben.

1. Wählen Sie auf der Seite „Volumes auswählen“ das oder die Volumes aus, die Sie schützen möchten.
   - Filtern Sie die Zeilen optional, um nur Datenträger mit bestimmten Datenträgertypen, Stilen usw. anzuzeigen und so die Auswahl zu vereinfachen.
   - Nachdem Sie das erste Volume ausgewählt haben, können Sie alle FlexVol Volumes auswählen (FlexGroup Volumes können jeweils nur einzeln ausgewählt werden). Um alle vorhandenen FlexVol Volumes zu sichern, markieren Sie zuerst ein Volume und aktivieren Sie dann das Kontrollkästchen in der Titelzeile.
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume.
2. Wählen Sie **Weiter**.

Definieren Sie die Sicherungsstrategie

Zum Definieren der Sicherungsstrategie müssen die folgenden Optionen festgelegt werden:

- Ob Sie eine oder alle Backup-Optionen wünschen: lokale Snapshots, Replikation und Backup auf Objektspeicher
- Architektur
- Lokale Snapshot-Richtlinie
- Replikationsziel und -richtlinie

Wenn die von Ihnen ausgewählten Volumes andere Snapshot- und Replikationsrichtlinien haben als die Richtlinien, die Sie in diesem Schritt auswählen, werden die vorhandenen Richtlinien überschrieben.

- Informationen zur Sicherung in Objektspeichern (Anbieter, Verschlüsselung, Netzwerk, Sicherungsrichtlinie und Exportoptionen).

Schritte

1. Wählen Sie auf der Seite „Sicherungsstrategie definieren“ eine oder alle der folgenden Optionen aus. Alle drei sind standardmäßig ausgewählt:
   - **Lokale Snapshots**: Wenn Sie eine Replikation oder Sicherung im Objektspeicher durchführen, müssen lokale Snapshots erstellt werden.
   - **Replikation**: Erstellt replizierte Volumes auf einem anderen ONTAP Speichersystem.
   - **Backup**: Sichert Volumes im Objektspeicher.

2. **Architektur**: Wenn Sie Replikation und Sicherung gewählt haben, wählen Sie einen der folgenden Informationsflüsse:
   - **Kaskadierung**: Informationen fließen vom primären Speichersystem zum sekundären und vom sekundären zum Objektspeicher.
   - **Fan-out**: Informationen fließen vom primären Speichersystem zum sekundären *und* vom primären zum Objektspeicher.

     Weitere Informationen zu diesen Architekturen finden Sie unter"Planen Sie Ihren Schutzweg" .
3. **Lokaler Snapshot**: Wählen Sie eine vorhandene Snapshot-Richtlinie aus oder erstellen Sie eine.

   Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Sicherung finden Sie unter"Erstellen einer Richtlinie" .

   Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:
   - Geben Sie den Namen der Richtlinie ein.
   - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
   - Konfigurieren Sie für Backup-to-Object-Richtlinien Datalock und Ransomware Resilience. Weitere Informationen zu Datalock und Ransomware Resilience finden Sie unter"Einstellungen der Backup-to-Object-Richtlinie" .
   - Wählen Sie **Erstellen**.
4. **Replikation**: Legen Sie die folgenden Optionen fest:
   - **Replikationsziel**: Wählen Sie das Zielsystem und die SVM aus. Wählen Sie optional das oder die Zielaggregate sowie das Präfix oder Suffix aus, das dem Namen des replizierten Volumes hinzugefügt wird.
   - **Replikationsrichtlinie**: Wählen Sie eine vorhandene Replikationsrichtlinie aus oder erstellen Sie eine.

     Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Replikation finden Sie unter"Erstellen einer Richtlinie" .

     Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:
     - Geben Sie den Namen der Richtlinie ein.
     - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
     - Wählen Sie **Erstellen**.
5. **Sichern auf Objekt**: Wenn Sie **Sichern** ausgewählt haben, legen Sie die folgenden Optionen fest:
   - **Anbieter**: Wählen Sie **Google Cloud**.
   - **Anbietereinstellungen**: Geben Sie die Anbieterdetails und die Region ein, in der die Backups gespeichert werden.

     Erstellen Sie entweder einen neuen Bucket oder wählen Sie einen vorhandenen aus.
   - **Verschlüsselungsschlüssel**: Wenn Sie einen neuen Google-Bucket erstellt haben, geben Sie die Informationen zum Verschlüsselungsschlüssel ein, die Sie vom Anbieter erhalten haben. Wählen Sie, ob Sie die standardmäßigen Google Cloud-Verschlüsselungsschlüssel verwenden oder Ihre eigenen, vom Kunden verwalteten Schlüssel aus Ihrem Google-Konto auswählen möchten, um die Verschlüsselung Ihrer Daten zu verwalten.

Wenn Sie Ihre eigenen, vom Kunden verwalteten Schlüssel verwenden möchten, geben Sie den Schlüsseltresor und die Schlüsselinformationen ein.

Wenn Sie einen vorhandenen Google Cloud-Bucket ausgewählt haben, sind die Verschlüsselungsinformationen bereits verfügbar, sodass Sie sie jetzt nicht eingeben müssen.

- **Sicherungsrichtlinie**: Wählen Sie eine vorhandene Richtlinie für die Sicherung in Objektspeicher aus oder erstellen Sie eine.

  Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Sicherung finden Sie unter"Erstellen einer Richtlinie" .

  Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:

  - Geben Sie den Namen der Richtlinie ein.
  - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
  - Wählen Sie **Erstellen**.

- **Vorhandene Snapshots als Sicherungskopien in den Objektspeicher exportieren**: Wenn es lokale Snapshots für Volumes in diesem System gibt, die mit der von Ihnen soeben für dieses System ausgewählten Sicherungszeitplanbezeichnung übereinstimmen (z. B. täglich, wöchentlich usw.), wird diese zusätzliche Aufforderung angezeigt. Aktivieren Sie dieses Kontrollkästchen, um alle historischen Snapshots als Sicherungsdateien in den Objektspeicher zu kopieren und so den umfassendsten Schutz für Ihre Volumes zu gewährleisten.

6. Wählen Sie **Weiter**.

Überprüfen Sie Ihre Auswahl

Dies ist die Gelegenheit, Ihre Auswahl zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

Schritte

1. Überprüfen Sie Ihre Auswahl auf der Überprüfungsseite.
2. Aktivieren Sie optional das Kontrollkästchen, um **die Snapshot-Richtlinienbezeichnungen automatisch mit den Replikations- und Sicherungsrichtlinienbezeichnungen zu synchronisieren**. Dadurch werden Snapshots mit einer Bezeichnung erstellt, die mit den Bezeichnungen in den Replikations- und Sicherungsrichtlinien übereinstimmt.
3. Wählen Sie **Backup aktivieren**.

Ergebnis

NetApp Backup and Recovery beginnt mit der Durchführung der ersten Sicherungen Ihrer Volumes. Die Basisübertragung des replizierten Volumes und der Sicherungsdatei umfasst eine vollständige Kopie der Daten des primären Speichersystems. Nachfolgende Übertragungen enthalten differentielle Kopien der Daten des primären Speichersystems, die in Snapshots enthalten sind.

Im Zielcluster wird ein repliziertes Volume erstellt, das mit dem Volume des primären Speichersystems synchronisiert wird.

Ein Google Cloud Storage-Bucket wird im Dienstkonto erstellt, das durch den von Ihnen eingegebenen Google-Zugriffsschlüssel und geheimen Schlüssel angegeben ist, und die Sicherungsdateien werden dort gespeichert.

Sicherungen werden standardmäßig der Speicherklasse *Standard* zugeordnet. Sie können die kostengünstigeren Speicherklassen *Nearline*, *Coldline* oder *Archive* verwenden. Sie konfigurieren die Speicherklasse jedoch über Google und nicht über die NetApp Backup and Recovery -Benutzeroberfläche. Siehe das Google-Thema "Ändern der Standardspeicherklasse eines Buckets" für Details.

Das Volume-Backup-Dashboard wird angezeigt, damit Sie den Status der Backups überwachen können.

Sie können den Status von Sicherungs- und Wiederherstellungsaufträgen auch mithilfe der"Seite „Jobüberwachung“" .

API-Befehle anzeigen

Möglicherweise möchten Sie die im Assistenten „Sicherung und Wiederherstellung aktivieren“ verwendeten API-Befehle anzeigen und optional kopieren. Möglicherweise möchten Sie dies tun, um die Sicherungsaktivierung in zukünftigen Systemen zu automatisieren.

Schritte

1. Wählen Sie im Assistenten „Sicherung und Wiederherstellung aktivieren“ die Option „API-Anforderung anzeigen“ aus.
2. Um die Befehle in die Zwischenablage zu kopieren, wählen Sie das Symbol **Kopieren**.

Wie geht es weiter?

- Du kannst"Verwalten Sie Ihre Sicherungsdateien und Sicherungsrichtlinien" . Dazu gehören das Starten und Stoppen von Sicherungen, das Löschen von Sicherungen, das Hinzufügen und Ändern des Sicherungszeitplans und mehr.
- Du kannst"Verwalten von Backup-Einstellungen auf Clusterebene" . Dazu gehört das Ändern der Speicherschlüssel, die ONTAP für den Zugriff auf den Cloud-Speicher verwendet, das Ändern der verfügbaren Netzwerkbandbreite zum Hochladen von Backups in den Objektspeicher, das Ändern der automatischen Backup-Einstellung für zukünftige Volumes und mehr.
- Sie können auch"Wiederherstellen von Volumes, Ordnern oder einzelnen Dateien aus einer Sicherungsdatei" zu einem Cloud Volumes ONTAP -System in AWS oder zu einem lokalen ONTAP System.

Sichern Sie lokale ONTAP -Daten mit NetApp Backup and Recovery auf Amazon S3

Führen Sie einige Schritte in NetApp Backup and Recovery aus, um mit der Sicherung von Volume-Daten von Ihren lokalen ONTAP -Systemen auf einem sekundären Speichersystem und im Amazon S3-Cloud-Speicher zu beginnen.

Zu den „On-Premises ONTAP -Systemen“ gehören FAS, AFF und ONTAP Select Systeme.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

Identifizieren Sie die Verbindungsmethode

Wählen Sie aus, welche der beiden Verbindungsmethoden Sie beim Konfigurieren von Backups von lokalen ONTAP -Systemen zu AWS S3 verwenden möchten.

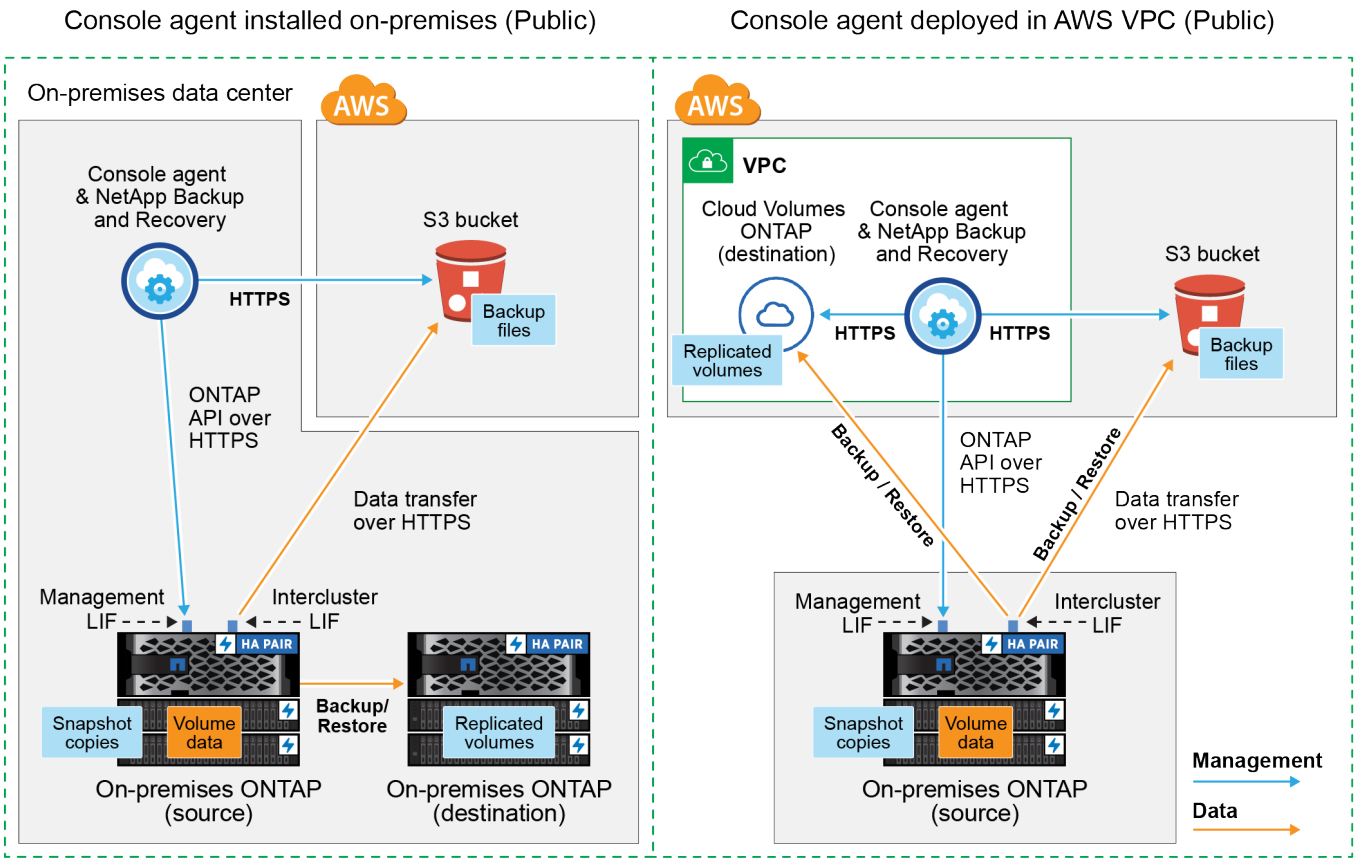
- **Öffentliche Verbindung** – Verbinden Sie das ONTAP -System über einen öffentlichen S3-Endpunkt direkt

mit AWS S3.

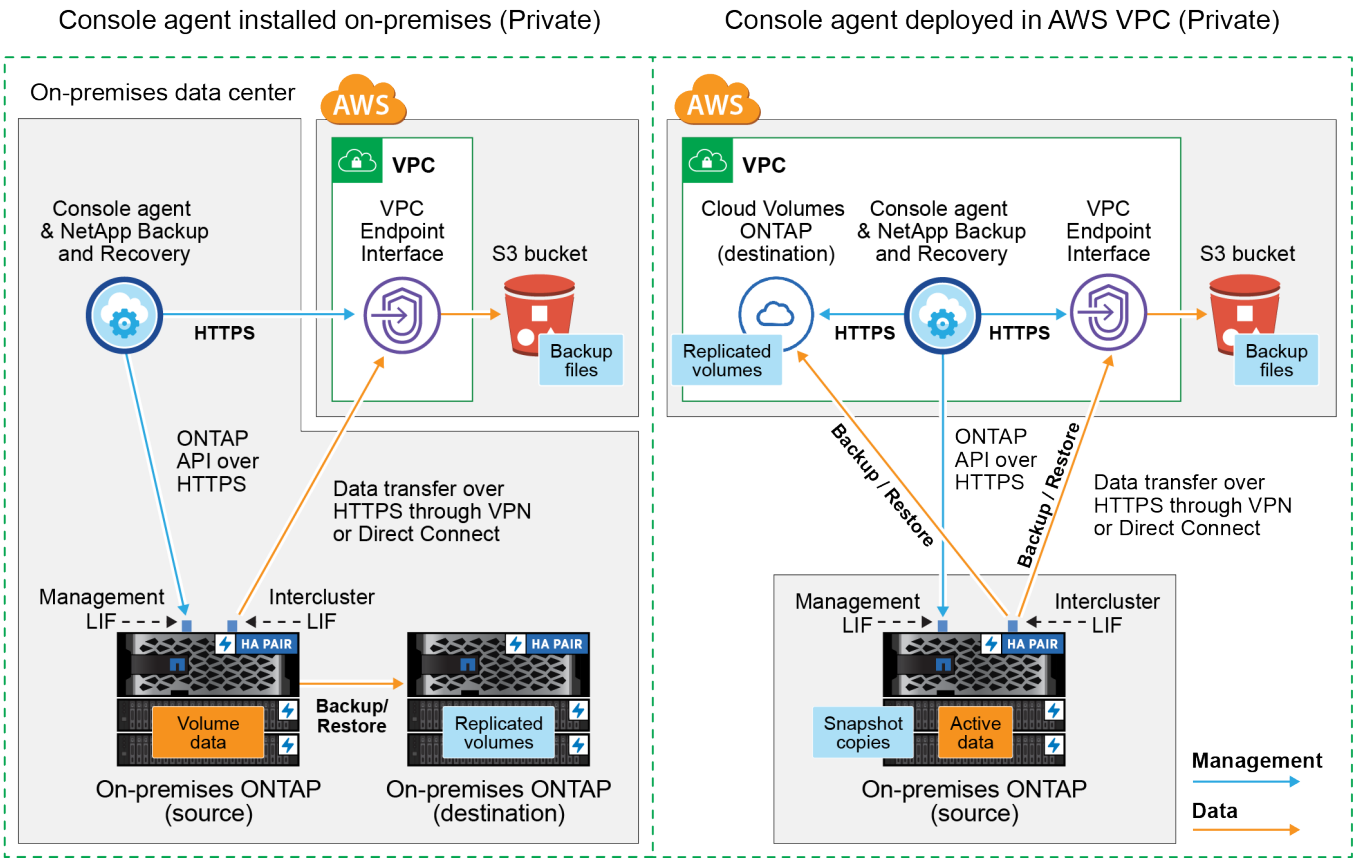
- **Private Verbindung** – Verwenden Sie ein VPN oder AWS Direct Connect und leiten Sie den Datenverkehr über eine VPC-Endpunktschnittstelle, die eine private IP-Adresse verwendet.

Optional können Sie auch über die öffentliche oder private Verbindung eine Verbindung zu einem sekundären ONTAP System für replizierte Volumes herstellen.

Das folgende Diagramm zeigt die Methode **öffentliche Verbindung** und die Verbindungen, die Sie zwischen den Komponenten vorbereiten müssen. Sie können einen Konsolenagenten verwenden, den Sie vor Ort installiert haben, oder einen Konsolenagenten, den Sie im AWS VPC bereitgestellt haben.



Das folgende Diagramm zeigt die Methode **private Verbindung** und die Verbindungen, die Sie zwischen den Komponenten vorbereiten müssen. Sie können einen Konsolenagenten verwenden, den Sie vor Ort installiert haben, oder einen Konsolenagenten, den Sie im AWS VPC bereitgestellt haben.



Vorbereiten Ihres Konsolenagenten

Der Konsolenagent ist die Hauptsoftware für die NetApp Console . Zum Sichern und Wiederherstellen Ihrer ONTAP Daten ist ein Konsolenagent erforderlich.

Erstellen oder Wechseln von Konsolenagenten

Wenn Sie bereits einen Konsolenagenten in Ihrem AWS VPC oder vor Ort bereitgestellt haben, sind Sie startklar.

Wenn nicht, müssen Sie an einem dieser Standorte einen Konsolenagenten erstellen, um ONTAP Daten im AWS S3-Speicher zu sichern. Sie können keinen Konsolenagenten verwenden, der bei einem anderen Cloud-Anbieter bereitgestellt wird.

- "Erfahren Sie mehr über Konsolenagenten"
- "Installieren Sie einen Konsolenagenten in AWS"
- "Installieren Sie einen Konsolenagenten in Ihren Räumlichkeiten"
- "Installieren Sie einen Konsolenagenten in einer AWS GovCloud-Region"

  NetApp Backup and Recovery wird in GovCloud-Regionen unterstützt, wenn der Konsolenagent in der Cloud bereitgestellt wird – nicht, wenn er bei Ihnen vor Ort installiert ist. Darüber hinaus müssen Sie den Konsolenagenten vom AWS Marketplace bereitstellen. Sie können den Konsolenagenten nicht von der NetApp Console SaaS-Website in einer Regierungsregion bereitstellen.

Netzwerkanforderungen für den Konsolenagenten vorbereiten

Stellen Sie sicher, dass die folgenden Netzwerkanforderungen erfüllt sind:

- Stellen Sie sicher, dass das Netzwerk, in dem der Konsolenagent installiert ist, die folgenden Verbindungen ermöglicht:
  - Eine HTTPS-Verbindung über Port 443 zu NetApp Backup and Recovery und zu Ihrem S3-Objektspeicher("siehe Liste der Endpunkte")
  - Eine HTTPS-Verbindung über Port 443 zu Ihrem ONTAP Cluster-Management-LIF
  - Für AWS- und AWS GovCloud-Bereitstellungen sind zusätzliche Sicherheitsgruppenregeln für eingehenden und ausgehenden Datenverkehr erforderlich. Sehen "Regeln für den Konsolenagenten in AWS" für Details.
- Wenn Sie über eine Direct Connect- oder VPN-Verbindung von Ihrem ONTAP Cluster zum VPC verfügen und die Kommunikation zwischen dem Konsolenagenten und S3 in Ihrem internen AWS-Netzwerk bleiben soll (eine **private** Verbindung), müssen Sie eine VPC-Endpunktschnittstelle zu S3 aktivieren. Konfigurieren Sie Ihr System für eine private Verbindung mithilfe einer VPC-Endpunktschnittstelle.

Überprüfen der Lizenzanforderungen

Sie müssen die Lizenzanforderungen sowohl für AWS als auch für die NetApp Console überprüfen:

- Bevor Sie NetApp Backup and Recovery für Ihren Cluster aktivieren können, müssen Sie entweder ein Pay-as-you-go (PAYGO) NetApp Console Marketplace-Angebot von AWS abonnieren oder eine NetApp Backup and Recovery BYOL-Lizenz von NetApp erwerben und aktivieren. Diese Lizenzen gelten für Ihr Konto und können systemübergreifend verwendet werden.
  - Für die NetApp Backup and Recovery PAYGO-Lizenzierung benötigen Sie ein Abonnement für die "NetApp Console -Angebot vom AWS Marketplace" . Die Abrechnung für NetApp Backup and Recovery erfolgt über dieses Abonnement.
  - Für die NetApp Backup and Recovery BYOL-Lizenzierung benötigen Sie die Seriennummer von NetApp , die Ihnen die Nutzung des Dienstes für die Dauer und Kapazität der Lizenz ermöglicht.
- Sie benötigen ein AWS-Abonnement für den Objektspeicherplatz, in dem Ihre Backups gespeichert werden.

Unterstützte Regionen

Sie können in allen Regionen, einschließlich der AWS GovCloud-Regionen, Backups von lokalen Systemen auf Amazon S3 erstellen. Sie geben die Region an, in der die Sicherungen gespeichert werden, wenn Sie den Dienst einrichten.

Bereiten Sie Ihre ONTAP -Cluster vor

Bereiten Sie Ihr lokales ONTAP -Quellsystem und alle sekundären lokalen ONTAP oder Cloud Volumes ONTAP Systeme vor.

Die Vorbereitung Ihrer ONTAP Cluster umfasst die folgenden Schritte:

- Entdecken Sie Ihre ONTAP -Systeme in der NetApp Console
- Überprüfen der ONTAP Systemanforderungen
- Überprüfen Sie die ONTAP Netzwerkanforderungen für die Datensicherung im Objektspeicher
- Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replikation von Volumes

Entdecken Sie Ihre ONTAP -Systeme in der NetApp Console

Sowohl Ihr lokales ONTAP Quellsystem als auch alle sekundären lokalen ONTAP oder Cloud Volumes ONTAP -Systeme müssen auf der Seite **Systeme** der NetApp Console verfügbar sein.

Sie müssen die IP-Adresse der Clusterverwaltung und das Kennwort für das Administratorbenutzerkonto kennen, um den Cluster hinzuzufügen. "Erfahren Sie, wie Sie einen Cluster erkennen".

Überprüfen der ONTAP Systemanforderungen

Stellen Sie sicher, dass Ihr ONTAP -System die folgenden Anforderungen erfüllt:

- Mindestens ONTAP 9.8; ONTAP 9.8P13 und höher wird empfohlen.
- Eine SnapMirror -Lizenz (im Premium-Paket oder Datenschutz-Paket enthalten).

  Hinweis: Das „Hybrid Cloud Bundle“ ist bei der Verwendung von NetApp Backup and Recovery nicht erforderlich.

  Erfahren Sie, wie Sie "Verwalten Sie Ihre Cluster-Lizenzen" .
- Uhrzeit und Zeitzone sind richtig eingestellt. Erfahren Sie, wie Sie "Konfigurieren Sie Ihre Clusterzeit" .
- Wenn Sie Daten replizieren, überprüfen Sie, ob auf den Quell- und Zielsystemen kompatible ONTAP Versionen ausgeführt werden.

  "Kompatible ONTAP -Versionen für SnapMirror -Beziehungen anzeigen".

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Datensicherung im Objektspeicher

Sie müssen die folgenden Anforderungen auf dem System konfigurieren, das eine Verbindung zum Objektspeicher herstellt.

- Konfigurieren Sie für eine Fan-Out-Backup-Architektur die folgenden Einstellungen auf dem *primären* System.
- Konfigurieren Sie für eine kaskadierte Sicherungsarchitektur die folgenden Einstellungen auf dem *sekundären* System.

Die folgenden ONTAP Cluster-Netzwerkanforderungen sind erforderlich:

- Der Cluster erfordert eine eingehende HTTPS-Verbindung vom Konsolenagenten zum Clusterverwaltungs-LIF.
- Auf jedem ONTAP Knoten, der die zu sichernden Volumes hostet, ist ein Intercluster-LIF erforderlich. Diese Cluster-übergreifenden LIFs müssen auf den Objektspeicher zugreifen können.

  Der Cluster initiiert eine ausgehende HTTPS-Verbindung über Port 443 von den LIFs zwischen den Clustern zum Amazon S3-Speicher für Sicherungs- und Wiederherstellungsvorgänge. ONTAP liest und schreibt Daten in den und aus dem Objektspeicher – der Objektspeicher wird nie initiiert, er antwortet nur.
- Die Intercluster-LIFs müssen mit dem *IPspace* verknüpft sein, den ONTAP für die Verbindung mit dem Objektspeicher verwenden soll. "Erfahren Sie mehr über IPspaces" .

  Wenn Sie NetApp Backup and Recovery einrichten, werden Sie nach dem zu verwendenden IPspace gefragt. Sie sollten den IPspace auswählen, mit dem diese LIFs verknüpft sind. Dies kann der „Standard“-IP-Bereich oder ein benutzerdefinierter IP-Bereich sein, den Sie erstellt haben.

Wenn Sie einen anderen IP-Bereich als „Standard“ verwenden, müssen Sie möglicherweise eine statische Route erstellen, um Zugriff auf den Objektspeicher zu erhalten.

Alle Intercluster-LIFs innerhalb des IPspace müssen Zugriff auf den Objektspeicher haben. Wenn Sie dies für den aktuellen IPspace nicht konfigurieren können, müssen Sie einen dedizierten IPspace erstellen, in dem alle LIFs zwischen Clustern Zugriff auf den Objektspeicher haben.

- Für die Speicher-VM, auf der sich die Volumes befinden, müssen DNS-Server konfiguriert worden sein. Erfahren Sie, wie Sie "Konfigurieren Sie DNS-Dienste für die SVM" .
- Aktualisieren Sie bei Bedarf die Firewall-Regeln, um NetApp Backup and Recovery -Verbindungen von ONTAP zum Objektspeicher über Port 443 und Namensauflösungsdatenverkehr von der Speicher-VM zum DNS-Server über Port 53 (TCP/UDP) zuzulassen.
- Wenn Sie für die S3-Verbindung einen privaten VPC-Schnittstellenendpunkt in AWS verwenden, müssen Sie das S3-Endpunktzertifikat in den ONTAP Cluster laden, damit HTTPS/443 verwendet werden kann. Konfigurieren Sie Ihr System für eine private Verbindung mithilfe einer VPC-Endpunktschnittstelle.
- Stellen Sie sicher, dass Ihr ONTAP Cluster über die Berechtigung zum Zugriff auf den S3-Bucket verfügt.

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replikation von Volumes

Wenn Sie mit NetApp Backup and Recovery replizierte Volumes auf einem sekundären ONTAP System erstellen möchten, stellen Sie sicher, dass die Quell- und Zielsysteme die folgenden Netzwerkanforderungen erfüllen.

On-Premises ONTAP Netzwerkanforderungen

- Wenn sich der Cluster vor Ort befindet, sollten Sie über eine Verbindung von Ihrem Unternehmensnetzwerk zu Ihrem virtuellen Netzwerk beim Cloud-Anbieter verfügen. Dies ist normalerweise eine VPN-Verbindung.
- ONTAP -Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Clusteranforderungen erfüllen.

  Da Sie auf Cloud Volumes ONTAP oder lokale Systeme replizieren können, überprüfen Sie die Peering-Anforderungen für lokale ONTAP -Systeme. "Voraussetzungen für Cluster-Peering in der ONTAP Dokumentation anzeigen" .

Netzwerkanforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen Regeln für eingehenden und ausgehenden Datenverkehr enthalten, insbesondere Regeln für ICMP und die Ports 11104 und 11105. Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.

Bereiten Sie Amazon S3 als Ihr Sicherungsziel vor

Die Vorbereitung von Amazon S3 als Sicherungsziel umfasst die folgenden Schritte:

- Richten Sie S3-Berechtigungen ein.
- (Optional) Erstellen Sie Ihre eigenen S3-Buckets. (Der Dienst erstellt auf Wunsch Buckets für Sie.)
- (Optional) Richten Sie vom Kunden verwaltete AWS-Schlüssel für die Datenverschlüsselung ein.
- (Optional) Konfigurieren Sie Ihr System für eine private Verbindung mithilfe einer VPC-Endpunktschnittstelle.

S3-Berechtigungen einrichten

Sie müssen zwei Berechtigungssätze konfigurieren:

- Berechtigungen für den Konsolenagenten zum Erstellen und Verwalten des S3-Buckets.
- Berechtigungen für den lokalen ONTAP Cluster, damit dieser Daten aus dem S3-Bucket lesen und schreiben kann.

Schritte

1. Stellen Sie sicher, dass der Konsolenagent über die erforderlichen Berechtigungen verfügt. Weitere Einzelheiten finden Sie unter "Richtlinienberechtigungen für die NetApp Console" .

   Wenn Sie Backups in AWS China-Regionen erstellen, müssen Sie den AWS-Ressourcennamen „arn“ unter allen *Resource*-Abschnitten in den IAM-Richtlinien von „aws“ in „aws-cn“ ändern. Beispiel: `arn:aws-cn:s3:::netapp-backup-*` .

2. Wenn Sie den Dienst aktivieren, werden Sie vom Backup-Assistenten aufgefordert, einen Zugriffsschlüssel und einen geheimen Schlüssel einzugeben. Diese Anmeldeinformationen werden an den ONTAP Cluster weitergegeben, damit ONTAP Daten im S3-Bucket sichern und wiederherstellen kann. Dazu müssen Sie einen IAM-Benutzer mit den folgenden Berechtigungen erstellen.

   Weitere Informationen finden Sie im "AWS-Dokumentation: Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer" .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "arn:aws:s3:::netapp-backup-*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/*",
      "Effect": "Allow"
    }
  ]
}
```

Erstellen Sie Ihre eigenen Eimer

Standardmäßig erstellt der Dienst Buckets für Sie. Wenn Sie Ihre eigenen Buckets verwenden möchten, können Sie diese auch erstellen, bevor Sie den Backup-Aktivierungsassistenten starten, und diese Buckets dann im Assistenten auswählen.

"Erfahren Sie mehr über das Erstellen eigener Buckets".

Wenn Sie Ihre eigenen Buckets erstellen, sollten Sie den Bucket-Namen „netapp-backup“ verwenden. Falls Sie einen benutzerdefinierten Namen verwenden möchten, bearbeiten Sie die `ontapcloud-instance-policy-netapp-backup` IAMRole für die bestehenden CVOs und fügen Sie den folgenden JSON-Block zu den S3-Berechtigungen hinzu. `Statement` Array. Sie müssen Folgendes einschließen: `"Resource": "arn:aws:s3:::*"` und weisen Sie alle erforderlichen Berechtigungen zu, die mit dem Bucket verknüpft werden müssen.

```
[
  {
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject",
      "s3:ListAllMyBuckets",
      "s3:PutObjectTagging",
      "s3:GetObjectTagging",
      "s3:RestoreObject",
      "s3:GetBucketObjectLockConfiguration",
      "s3:GetObjectRetention",
      "s3:PutBucketObjectLockConfiguration",
      "s3:PutObjectRetention"
    ],
    "Resource": "arn:aws:s3:::*"
  }
]
```

Einrichten von kundenverwalteten AWS-Schlüsseln zur Datenverschlüsselung

Wenn Sie die standardmäßigen Amazon S3-Verschlüsselungsschlüssel zum Verschlüsseln der zwischen Ihrem lokalen Cluster und dem S3-Bucket übertragenen Daten verwenden möchten, sind Sie bestens gerüstet,

da die Standardinstallation diese Art der Verschlüsselung verwendet.

Wenn Sie stattdessen Ihre eigenen, vom Kunden verwalteten Schlüssel zur Datenverschlüsselung verwenden möchten, anstatt die Standardschlüssel zu verwenden, müssen Sie die verwalteten Verschlüsselungsschlüssel bereits eingerichtet haben, bevor Sie den NetApp Backup and Recovery -Assistenten starten.

"Informieren Sie sich, wie Sie Ihre eigenen Amazon-Verschlüsselungsschlüssel mit Cloud Volumes ONTAP verwenden.".

"Informieren Sie sich darüber, wie Sie Ihre eigenen Amazon-Verschlüsselungsschlüssel mit NetApp Backup and Recovery verwenden.".

Konfigurieren Sie Ihr System für eine private Verbindung mithilfe einer VPC-Endpunktschnittstelle

Wenn Sie eine standardmäßige öffentliche Internetverbindung verwenden möchten, werden alle Berechtigungen vom Konsolenagenten festgelegt und Sie müssen nichts weiter tun.

Wenn Sie eine sicherere Verbindung über das Internet von Ihrem lokalen Rechenzentrum zum VPC wünschen, können Sie im Backup-Aktivierungsassistenten eine AWS PrivateLink-Verbindung auswählen. Dies ist erforderlich, wenn Sie ein VPN oder AWS Direct Connect verwenden möchten, um Ihr lokales System über eine VPC-Endpunktschnittstelle zu verbinden, die eine private IP-Adresse verwendet.

Schritte

1. Erstellen Sie mithilfe der Amazon VPC-Konsole oder der Befehlszeile eine Schnittstellenendpunktkonfiguration. "Weitere Informationen zur Verwendung von AWS PrivateLink für Amazon S3 finden Sie hier." .
2. Ändern Sie die Sicherheitsgruppenkonfiguration, die dem Konsolenagenten zugeordnet ist. Sie müssen die Richtlinie von "Vollzugriff" auf "Benutzerdefiniert" ändern undFügen Sie die S3-Berechtigungen aus der Sicherungsrichtlinie hinzu wie bereits gezeigt.

   Wenn Sie Port 80 (HTTP) für die Kommunikation mit dem privaten Endpunkt verwenden, sind Sie fertig. Sie können NetApp Backup and Recovery jetzt auf dem Cluster aktivieren.

   Wenn Sie Port 443 (HTTPS) für die Kommunikation mit dem privaten Endpunkt verwenden, müssen Sie das Zertifikat vom VPC S3-Endpunkt kopieren und es Ihrem ONTAP Cluster hinzufügen, wie in den nächsten 4 Schritten gezeigt.

3. Rufen Sie den DNS-Namen des Endpunkts von der AWS-Konsole ab.
4. Besorgen Sie sich das Zertifikat vom VPC S3-Endpunkt. Sie tun dies, indem Sie "Anmelden bei der VM, die den Konsolenagenten hostet" und führen Sie den folgenden Befehl aus. Wenn Sie den DNS-Namen des Endpunkts eingeben, fügen Sie am Anfang „bucket“ hinzu und ersetzen Sie das „*“:

   ```
   openssl s_client -connect bucket.vpce-0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443 -showcerts
   ```

5. Kopieren Sie aus der Ausgabe dieses Befehls die Daten für das S3-Zertifikat (alle Daten zwischen und einschließlich der Tags BEGIN / END CERTIFICATE):

```
Certificate chain
0 s:/CN=s3.us-west-2.amazonaws.com`
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
-----BEGIN CERTIFICATE-----
MIIM6zCCC9OgAwIBAgIQA7MGJ4FaDBR8uL0KR3oltTANBgkqhkiG9w0BAQsFADBG
…
…
GqvbOz/oO2NWLLFCqI+xmkLcMiPrZy+/6Af+HH2mLCM4EsI2b+IpBmPkriWnnxo=
-----END CERTIFICATE-----
```

6. Melden Sie sich bei der CLI des ONTAP Clusters an und wenden Sie das kopierte Zertifikat mit dem folgenden Befehl an (ersetzen Sie den Namen Ihrer eigenen Speicher-VM):

```
cluster1::> security certificate install -vserver cluster1 -type server-
ca
Please enter Certificate: Press <Enter> when done
```

Aktivieren Sie Backups auf Ihren ONTAP -Volumes

Aktivieren Sie Backups jederzeit direkt von Ihrem lokalen System aus.

Ein Assistent führt Sie durch die folgenden Hauptschritte:

- die Sie sichern möchten
- Definieren Sie die Sicherungsstrategie
- Überprüfen Sie Ihre Auswahl

Sie können auchAPI-Befehle anzeigen im Überprüfungsschritt, damit Sie den Code kopieren können, um die Sicherungsaktivierung für zukünftige Systeme zu automatisieren.

Starten des Assistenten

Schritte

1. Greifen Sie auf eine der folgenden Arten auf den Assistenten „Sicherung und Wiederherstellung aktivieren“ zu:

   - Wählen Sie auf der Konsolenseite **Systeme** das System aus und wählen Sie im rechten Bereich neben „Sicherung und Wiederherstellung“ die Option „Aktivieren > Sicherungsvolumes“ aus.

     Wenn das Amazon S3-Ziel für Ihre Backups als System auf der Konsolenseite **Systeme** vorhanden ist, können Sie den ONTAP Cluster auf den Amazon S3-Objektspeicher ziehen.

   - Wählen Sie in der Leiste „Sichern und Wiederherstellen“ **Volumes** aus. Wählen Sie auf der Registerkarte „Volumes“ die Option „Aktionen“ aus. ••• und wählen Sie **Sicherung aktivieren** für ein einzelnes Volume (für das die Replikation oder Sicherung in den Objektspeicher noch nicht aktiviert ist).

   Auf der Einführungsseite des Assistenten werden die Schutzoptionen angezeigt, darunter lokale

Snapshots, Replikation und Backups. Wenn Sie in diesem Schritt die zweite Option gewählt haben, wird die Seite „Sicherungsstrategie definieren“ mit einem ausgewählten Volume angezeigt.

2. Fahren Sie mit den folgenden Optionen fort:
   - Wenn Sie bereits über einen Konsolenagenten verfügen, sind Sie startklar. Wählen Sie einfach **Weiter**.
   - Wenn Sie noch keinen Konsolenagenten haben, wird die Option **Konsolenagenten hinzufügen** angezeigt. SieheVorbereiten Ihres Konsolenagenten .

Wählen Sie die Volumes aus, die Sie sichern möchten

Wählen Sie die Volumes aus, die Sie schützen möchten. Ein geschütztes Volume verfügt über eine oder mehrere der folgenden Optionen: Snapshot-Richtlinie, Replikationsrichtlinie, Backup-to-Object-Richtlinie.

Sie können FlexVol oder FlexGroup -Volumes schützen. Sie können jedoch keine Mischung dieser Volumes auswählen, wenn Sie die Sicherung für ein System aktivieren. Erfahren Sie, wie Sie"Aktivieren Sie die Sicherung für zusätzliche Volumes im System" (FlexVol oder FlexGroup), nachdem Sie die Sicherung für die ersten Volumes konfiguriert haben.

- Sie können eine Sicherung jeweils nur auf einem einzigen FlexGroup -Volume aktivieren.
- Die von Ihnen ausgewählten Volumes müssen über dieselbe SnapLock Einstellung verfügen. Auf allen Volumes muss SnapLock Enterprise aktiviert oder SnapLock sein.

Schritte

Wenn auf die von Ihnen ausgewählten Volumes bereits Snapshot- oder Replikationsrichtlinien angewendet wurden, werden diese vorhandenen Richtlinien durch die später ausgewählten Richtlinien überschrieben.

1. Wählen Sie auf der Seite „Volumes auswählen“ das oder die Volumes aus, die Sie schützen möchten.
   - Filtern Sie die Zeilen optional, um nur Datenträger mit bestimmten Datenträgertypen, Stilen usw. anzuzeigen und so die Auswahl zu vereinfachen.
   - Nachdem Sie das erste Volume ausgewählt haben, können Sie alle FlexVol Volumes auswählen (FlexGroup Volumes können jeweils nur einzeln ausgewählt werden). Um alle vorhandenen FlexVol Volumes zu sichern, markieren Sie zuerst ein Volume und aktivieren Sie dann das Kontrollkästchen in der Titelzeile.
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume.
2. Wählen Sie **Weiter**.

Definieren Sie die Sicherungsstrategie

Zum Definieren der Sicherungsstrategie müssen die folgenden Optionen festgelegt werden:

- Ob Sie eine oder alle der Backup-Optionen wünschen: lokale Snapshots, Replikation und Backup auf Objektspeicher
- Architektur
- Lokale Snapshot-Richtlinie
- Replikationsziel und -richtlinie

Wenn die von Ihnen ausgewählten Volumes andere Snapshot- und Replikationsrichtlinien haben als die Richtlinien, die Sie in diesem Schritt auswählen, werden die vorhandenen Richtlinien überschrieben.

- Informationen zur Sicherung in Objektspeichern (Anbieter, Verschlüsselung, Netzwerk, Sicherungsrichtlinie und Exportoptionen).

Schritte

1. Wählen Sie auf der Seite „Sicherungsstrategie definieren“ eine oder alle der folgenden Optionen aus. Alle drei sind standardmäßig ausgewählt:
   - **Lokale Snapshots**: Wenn Sie eine Replikation oder Sicherung im Objektspeicher durchführen, müssen lokale Snapshots erstellt werden.
   - **Replikation**: Erstellt replizierte Volumes auf einem anderen ONTAP Speichersystem.
   - **Backup**: Sichert Volumes im Objektspeicher.
2. **Architektur**: Wenn Sie Replikation und Sicherung gewählt haben, wählen Sie einen der folgenden Informationsflüsse:
   - **Kaskadierung**: Informationen fließen vom primären zum sekundären zum Objektspeicher und vom sekundären zum Objektspeicher.
   - **Fan-out**: Informationen fließen vom primären zum sekundären *und* vom primären zum Objektspeicher.

   Weitere Informationen zu diesen Architekturen finden Sie unter"Planen Sie Ihren Schutzweg" .
3. **Lokaler Snapshot**: Wählen Sie eine vorhandene Snapshot-Richtlinie oder erstellen Sie eine Richtlinie.

   Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung des Snapshots finden Sie unter"Erstellen einer Richtlinie" .
4. Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:
   - Geben Sie den Namen der Richtlinie ein.
   - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
     - Legen Sie für Backup-to-Object-Richtlinien die Einstellungen „DataLock“ und „Ransomware Resilience“ fest. Weitere Informationen zu DataLock und Ransomware Resilience finden Sie unter"Einstellungen der Backup-to-Object-Richtlinie" .
   - Wählen Sie **Erstellen**.
5. **Replikation**: Legen Sie die folgenden Optionen fest:
   - **Replikationsziel**: Wählen Sie das Zielsystem und die SVM aus. Wählen Sie optional das oder die Zielaggregate sowie das Präfix oder Suffix aus, das dem Namen des replizierten Volumes hinzugefügt wird.
   - **Replikationsrichtlinie**: Wählen Sie eine vorhandene Replikationsrichtlinie aus oder erstellen Sie eine Richtlinie.

     Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Replikation finden Sie unter"Erstellen einer Richtlinie" .

     Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:
     - Geben Sie den Namen der Richtlinie ein.
     - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
     - Wählen Sie **Erstellen**.
6. **Sichern auf Objekt**: Wenn Sie **Sichern** ausgewählt haben, legen Sie die folgenden Optionen fest:

- **Anbieter**: Wählen Sie **Amazon Web Services**.
- **Anbietereinstellungen**: Geben Sie die Anbieterdetails und die AWS-Region ein, in der die Backups gespeichert werden.

  Der Zugriffsschlüssel und der geheime Schlüssel sind für den IAM-Benutzer, den Sie erstellt haben, um dem ONTAP Cluster Zugriff auf den S3-Bucket zu gewähren.

- **Bucket**: Wählen Sie entweder einen vorhandenen S3-Bucket aus oder erstellen Sie einen neuen. Siehe "S3-Buckets hinzufügen" .
- **Verschlüsselungsschlüssel**: Wenn Sie einen neuen S3-Bucket erstellt haben, geben Sie die Informationen zum Verschlüsselungsschlüssel ein, die Sie vom Anbieter erhalten haben. Wählen Sie, ob Sie die standardmäßigen Amazon S3-Verschlüsselungsschlüssel verwenden oder Ihre eigenen, vom Kunden verwalteten Schlüssel aus Ihrem AWS-Konto auswählen möchten, um die Verschlüsselung Ihrer Daten zu verwalten.

  Wenn Sie einen vorhandenen Bucket ausgewählt haben, sind die Verschlüsselungsinformationen bereits verfügbar, sodass Sie sie jetzt nicht eingeben müssen.

- **Netzwerk**: Wählen Sie den IP-Bereich und geben Sie an, ob Sie einen privaten Endpunkt verwenden möchten. Privater Endpunkt ist standardmäßig deaktiviert.
  i. Der IP-Bereich im ONTAP -Cluster, in dem sich die Volumes befinden, die Sie sichern möchten. Die Intercluster-LIFs für diesen IPspace müssen über ausgehenden Internetzugang verfügen.
  ii. Wählen Sie optional aus, ob Sie einen zuvor konfigurierten AWS PrivateLink verwenden möchten. "Details zur Verwendung von AWS PrivateLink für Amazon S3 anzeigen" .
- **Sicherungsrichtlinie**: Wählen Sie eine vorhandene Sicherungsrichtlinie aus oder erstellen Sie eine Richtlinie.

  Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Sicherung finden Sie unter"Erstellen einer Richtlinie" .

  Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:

  - Geben Sie den Namen der Richtlinie ein.
  - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
  - Wählen Sie **Erstellen**.
- **Vorhandene Snapshots als Sicherungskopien in den Objektspeicher exportieren**: Wenn es lokale Snapshots für Volumes in diesem System gibt, die mit der von Ihnen soeben für dieses System ausgewählten Sicherungszeitplanbezeichnung übereinstimmen (z. B. täglich, wöchentlich usw.), wird diese zusätzliche Aufforderung angezeigt. Aktivieren Sie dieses Kontrollkästchen, um alle historischen Snapshots als Sicherungsdateien in den Objektspeicher zu kopieren und so den umfassendsten Schutz für Ihre Volumes zu gewährleisten.

7. Wählen Sie **Weiter**.

Überprüfen Sie Ihre Auswahl

Dies ist die Gelegenheit, Ihre Auswahl zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

Schritte

1. Überprüfen Sie Ihre Auswahl auf der Überprüfungsseite.
2. Aktivieren Sie optional das Kontrollkästchen, um **die Snapshot-Richtlinienbezeichnungen automatisch mit den Replikations- und Sicherungsrichtlinienbezeichnungen zu synchronisieren**. Dadurch werden Snapshots mit einer Bezeichnung erstellt, die mit den Bezeichnungen in den Replikations- und Sicherungsrichtlinien übereinstimmt.
3. Wählen Sie **Backup aktivieren**.

Ergebnis

NetApp Backup and Recovery beginnt mit der Durchführung der ersten Sicherungen Ihrer Volumes. Die Basisübertragung des replizierten Volumes und der Sicherungsdatei umfasst eine vollständige Kopie der Daten des primären Speichersystems. Nachfolgende Übertragungen enthalten differentielle Kopien der primären Daten, die in Snapshots enthalten sind.

Im Zielcluster wird ein repliziertes Volume erstellt, das mit dem primären Speichervolume synchronisiert wird.

Der S3-Bucket wird in dem Dienstkonto erstellt, das durch den von Ihnen eingegebenen S3-Zugriffsschlüssel und geheimen Schlüssel angegeben ist, und die Sicherungsdateien werden dort gespeichert. Das Volume-Backup-Dashboard wird angezeigt, damit Sie den Status der Backups überwachen können.

Sie können den Status von Sicherungs- und Wiederherstellungsaufträgen auch mithilfe der"Seite „Jobüberwachung“" .

API-Befehle anzeigen

Möglicherweise möchten Sie die im Assistenten „Sicherung und Wiederherstellung aktivieren“ verwendeten API-Befehle anzeigen und optional kopieren. Möglicherweise möchten Sie dies tun, um die Sicherungsaktivierung in zukünftigen Systemen zu automatisieren.

Schritte

1. Wählen Sie im Assistenten „Sicherung und Wiederherstellung aktivieren“ die Option „API-Anforderung anzeigen“ aus.
2. Um die Befehle in die Zwischenablage zu kopieren, wählen Sie das Symbol **Kopieren**.

Sichern Sie lokale ONTAP -Daten mit NetApp Backup and Recovery auf Azure Blob Storage

Führen Sie einige Schritte in NetApp Backup and Recovery aus, um mit der Sicherung von Volumedaten von Ihren lokalen ONTAP -Systemen auf einem sekundären Speichersystem und im Azure Blob-Speicher zu beginnen.

Zu den „On-Premises ONTAP -Systemen“ gehören FAS, AFF und ONTAP Select Systeme.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

Identifizieren Sie die Verbindungsmethode

Wählen Sie aus, welche der beiden Verbindungsmethoden Sie beim Konfigurieren von Sicherungen von lokalen ONTAP -Systemen zu Azure Blob verwenden möchten.

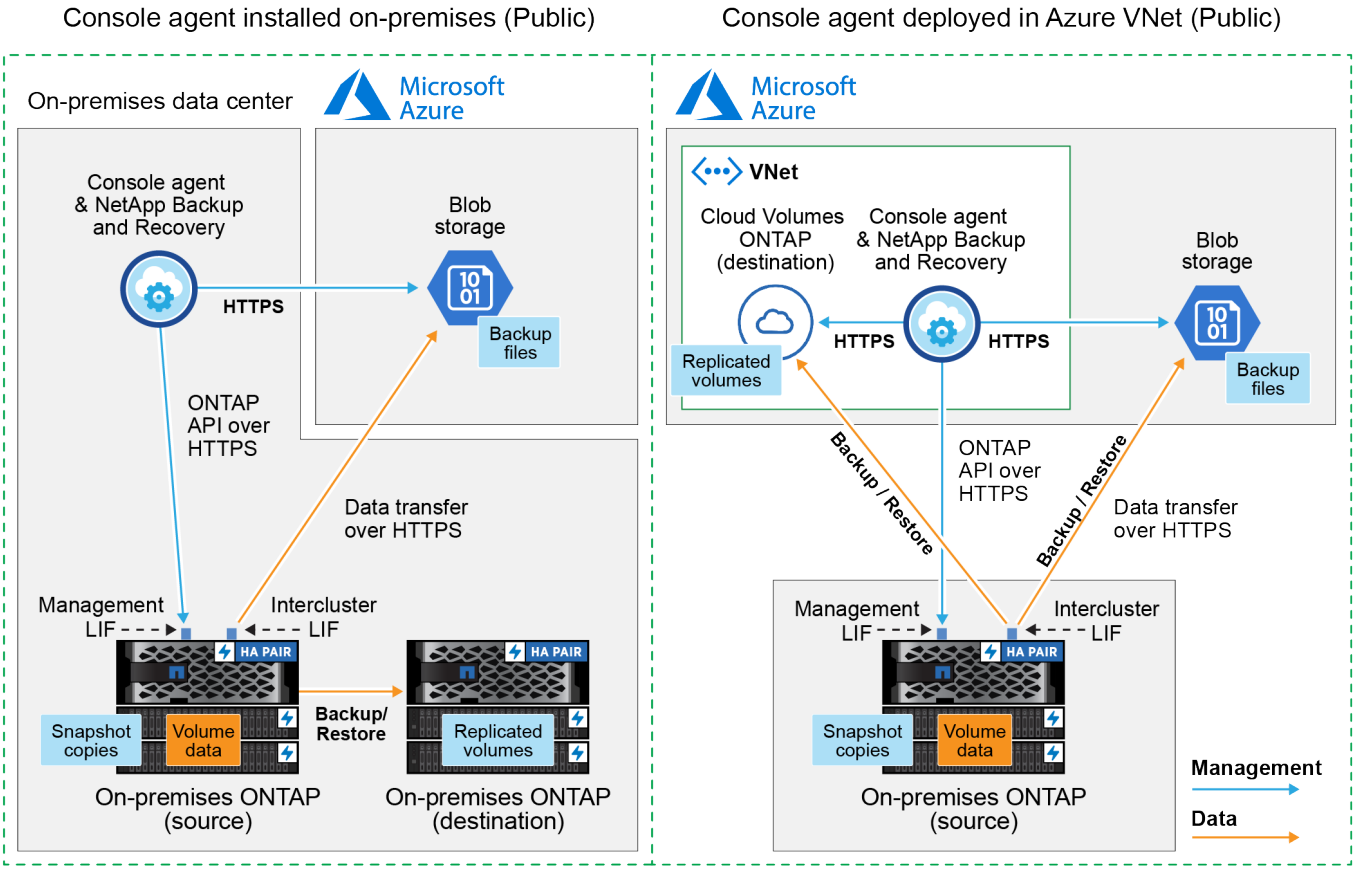
- **Öffentliche Verbindung** – Verbinden Sie das ONTAP -System über einen öffentlichen Azure-Endpunkt

direkt mit dem Azure Blob-Speicher.

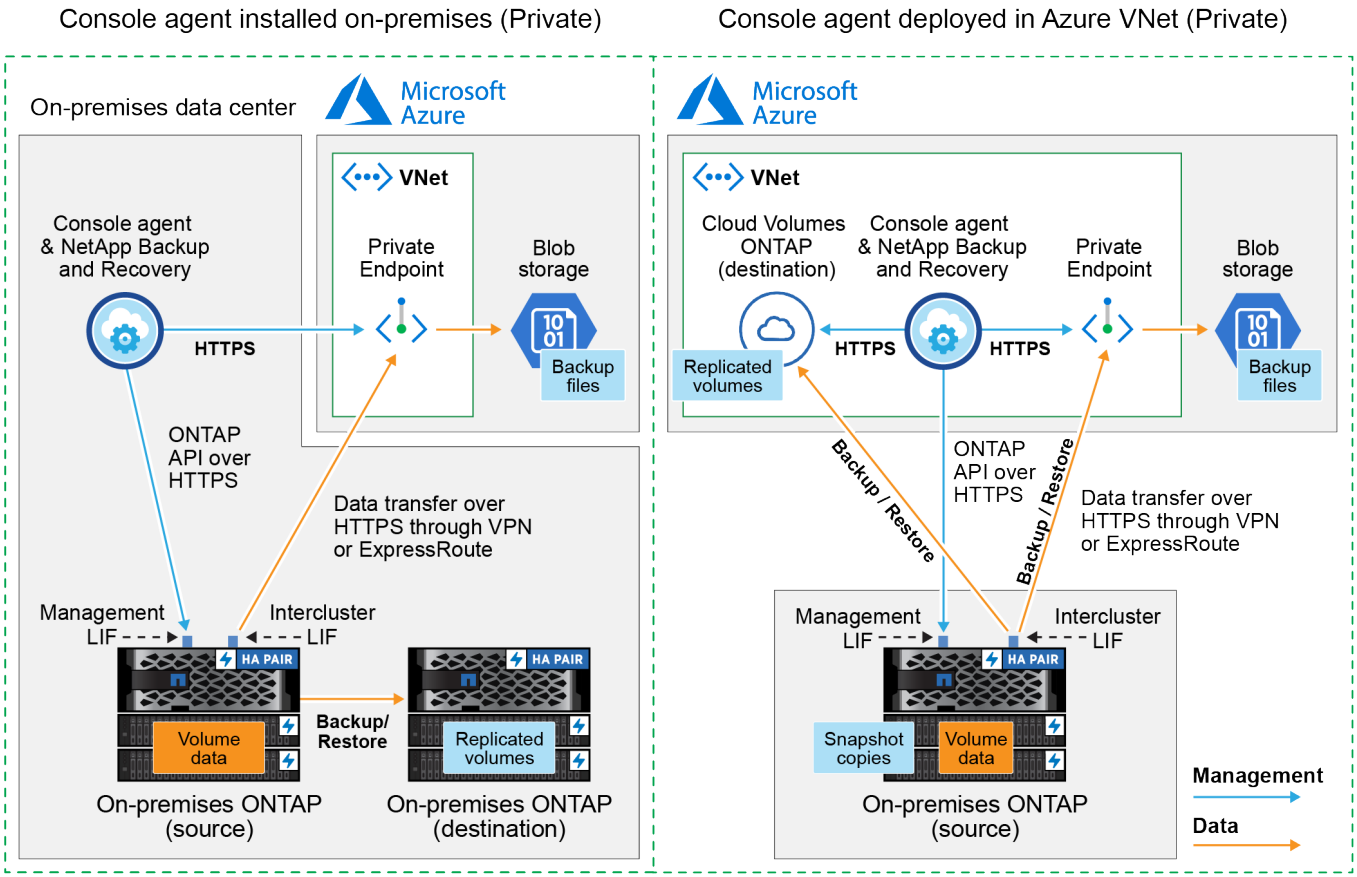
- **Private Verbindung** – Verwenden Sie ein VPN oder ExpressRoute und leiten Sie den Datenverkehr über einen privaten VNet-Endpunkt, der eine private IP-Adresse verwendet.

Optional können Sie auch über die öffentliche oder private Verbindung eine Verbindung zu einem sekundären ONTAP System für replizierte Volumes herstellen.

Das folgende Diagramm zeigt die Methode **öffentliche Verbindung** und die Verbindungen, die Sie zwischen den Komponenten vorbereiten müssen. Sie können einen Konsolen-Agenten verwenden, den Sie vor Ort installiert haben, oder einen Konsolen-Agenten, den Sie im Azure VNet bereitgestellt haben.



Das folgende Diagramm zeigt die Methode **private Verbindung** und die Verbindungen, die Sie zwischen den Komponenten vorbereiten müssen. Sie können einen Konsolen-Agenten verwenden, den Sie vor Ort installiert haben, oder einen Konsolen-Agenten, den Sie im Azure VNet bereitgestellt haben.



Vorbereiten Ihres Konsolenagenten

Der Konsolenagent ist die Hauptsoftware für die NetApp Console . Zum Sichern und Wiederherstellen Ihrer ONTAP Daten ist ein Konsolenagent erforderlich.

Erstellen oder Wechseln von Konsolenagenten

Wenn Sie bereits einen Konsolen-Agenten in Ihrem Azure VNet oder vor Ort bereitgestellt haben, sind Sie startklar.

Wenn nicht, müssen Sie an einem dieser Standorte einen Konsolenagenten erstellen, um ONTAP -Daten im Azure Blob-Speicher zu sichern. Sie können keinen Konsolenagenten verwenden, der bei einem anderen Cloud-Anbieter bereitgestellt wird.

- "Erfahren Sie mehr über Konsolenagenten"
- "Installieren eines Konsolen-Agents in Azure"
- "Installieren Sie einen Konsolenagenten in Ihren Räumlichkeiten"
- "Installieren eines Konsolen-Agenten in einer Azure Government-Region"

  NetApp Backup and Recovery wird in Azure Government-Regionen unterstützt, wenn der Konsolenagent in der Cloud bereitgestellt wird – nicht, wenn er in Ihren Räumlichkeiten installiert ist. Darüber hinaus müssen Sie den Konsolen-Agenten vom Azure Marketplace bereitstellen. Sie können den Konsolenagenten nicht von der SaaS-Website der Konsole in einer Regierungsregion bereitstellen.

Vorbereiten des Netzwerks für den Konsolenagenten

Stellen Sie sicher, dass der Konsolenagent über die erforderlichen Netzwerkverbindungen verfügt.

Schritte

1. Stellen Sie sicher, dass das Netzwerk, in dem der Konsolenagent installiert ist, die folgenden Verbindungen ermöglicht:
   - Eine HTTPS-Verbindung über Port 443 zu NetApp Backup and Recovery und zu Ihrem Blob-Objektspeicher("siehe Liste der Endpunkte")
   - Eine HTTPS-Verbindung über Port 443 zu Ihrem ONTAP Cluster-Management-LIF
   - Damit die Such- und Wiederherstellungsfunktion von NetApp Backup and Recovery funktioniert, muss Port 1433 für die Kommunikation zwischen dem Konsolenagenten und den Azure Synapse SQL-Diensten geöffnet sein.
   - Für Azure- und Azure Government-Bereitstellungen sind zusätzliche Regeln für eingehende Sicherheitsgruppen erforderlich. Sehen "Regeln für den Konsolen-Agent in Azure" für Details.
2. Aktivieren Sie einen privaten VNet-Endpunkt für Azure-Speicher. Dies ist erforderlich, wenn Sie über eine ExpressRoute- oder VPN-Verbindung von Ihrem ONTAP Cluster zum VNet verfügen und die Kommunikation zwischen dem Konsolenagenten und dem Blob-Speicher in Ihrem virtuellen privaten Netzwerk (einer **privaten** Verbindung) bleiben soll.

Überprüfen oder Hinzufügen von Berechtigungen für den Konsolenagenten

Um die Such- und Wiederherstellungsfunktion von NetApp Backup and Recovery verwenden zu können, benötigen Sie bestimmte Berechtigungen in der Rolle für den Konsolenagenten, damit dieser auf den Azure Synapse-Arbeitsbereich und das Data Lake-Speicherkonto zugreifen kann. Sehen Sie sich die Berechtigungen unten an und befolgen Sie die Schritte, wenn Sie die Richtlinie ändern müssen.

Bevor Sie beginnen

Sie müssen den Azure Synapse Analytics-Ressourcenanbieter (genannt „Microsoft.Synapse“) mit Ihrem Abonnement registrieren. "Erfahren Sie, wie Sie diesen Ressourcenanbieter für Ihr Abonnement registrieren." . Sie müssen der **Eigentümer** oder **Mitwirkende** des Abonnements sein, um den Ressourcenanbieter zu registrieren.

Schritte

1. Identifizieren Sie die der virtuellen Maschine des Konsolenagenten zugewiesene Rolle:
   a. Öffnen Sie im Azure-Portal den Dienst „Virtuelle Computer“.
   b. Wählen Sie die virtuelle Maschine des Konsolenagenten aus.
   c. Wählen Sie unter **Einstellungen** die Option **Identität** aus.
   d. Wählen Sie **Azure-Rollenzuweisungen** aus.
   e. Notieren Sie sich die benutzerdefinierte Rolle, die der virtuellen Maschine des Konsolenagenten zugewiesen ist.
2. Aktualisieren Sie die benutzerdefinierte Rolle:
   a. Öffnen Sie im Azure-Portal Ihr Azure-Abonnement.
   b. Wählen Sie **Zugriffskontrolle (IAM) > Rollen**.
   c. Wählen Sie die Auslassungspunkte (**…**) für die benutzerdefinierte Rolle und wählen Sie dann **Bearbeiten**.
   d. Wählen Sie **JSON** aus und fügen Sie die folgenden Berechtigungen hinzu:

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"Vollständiges JSON-Format für die Richtlinie anzeigen"

e. Wählen Sie **Überprüfen + Aktualisieren** und dann **Aktualisieren**.

Überprüfen der Lizenzanforderungen

Sie müssen die Lizenzanforderungen sowohl für Azure als auch für die Konsole überprüfen:

- Bevor Sie NetApp Backup and Recovery für Ihren Cluster aktivieren können, müssen Sie entweder ein Pay-as-you-go (PAYGO) Console Marketplace-Angebot von Azure abonnieren oder eine NetApp Backup and Recovery BYOL-Lizenz von NetApp erwerben und aktivieren. Diese Lizenzen gelten für Ihr Konto und können systemübergreifend verwendet werden.
  - Für die NetApp Backup and Recovery PAYGO-Lizenzierung benötigen Sie ein Abonnement für die "NetApp Console Angebot vom Azure Marketplace" . Die Abrechnung für NetApp Backup and Recovery erfolgt über dieses Abonnement.
  - Für die NetApp Backup and Recovery BYOL-Lizenzierung benötigen Sie die Seriennummer von NetApp , die Ihnen die Nutzung des Dienstes für die Dauer und Kapazität der Lizenz ermöglicht. "Erfahren Sie, wie Sie Ihre BYOL-Lizenzen verwalten".
- Sie benötigen ein Azure-Abonnement für den Objektspeicherplatz, in dem Ihre Sicherungen gespeichert werden.

Unterstützte Regionen

Sie können Sicherungen von lokalen Systemen in Azure Blob in allen Regionen erstellen, einschließlich Azure Government-Regionen. Sie geben die Region an, in der die Sicherungen gespeichert werden, wenn Sie den Dienst einrichten.

Bereiten Sie Ihre ONTAP -Cluster vor

Bereiten Sie Ihr lokales ONTAP -Quellsystem und alle sekundären lokalen ONTAP oder Cloud Volumes ONTAP Systeme vor.

Die Vorbereitung Ihrer ONTAP Cluster umfasst die folgenden Schritte:

- Entdecken Sie Ihre ONTAP -Systeme in der NetApp Console
- Überprüfen der ONTAP Systemanforderungen
- Überprüfen Sie die ONTAP Netzwerkanforderungen für die Datensicherung im Objektspeicher
- Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replikation von Volumes

Entdecken Sie Ihre ONTAP -Systeme in der NetApp Console

Sowohl Ihr lokales ONTAP Quellsystem als auch alle sekundären lokalen ONTAP oder Cloud Volumes ONTAP -Systeme müssen auf der Seite **Systeme** der NetApp Console verfügbar sein.

Sie müssen die IP-Adresse der Clusterverwaltung und das Kennwort für das Administratorbenutzerkonto kennen, um den Cluster hinzuzufügen. "Erfahren Sie, wie Sie einen Cluster erkennen".

Überprüfen der ONTAP Systemanforderungen

Stellen Sie sicher, dass Ihr ONTAP -System die folgenden Anforderungen erfüllt:

- Mindestens ONTAP 9.8; ONTAP 9.8P13 und höher wird empfohlen.
- Eine SnapMirror -Lizenz (im Premium-Paket oder Datenschutz-Paket enthalten).

  Hinweis: Das „Hybrid Cloud Bundle“ ist bei der Verwendung von NetApp Backup and Recovery nicht erforderlich.

Erfahren Sie, wie Sie "Verwalten Sie Ihre Cluster-Lizenzen" .

- Uhrzeit und Zeitzone sind richtig eingestellt. Erfahren Sie, wie Sie "Konfigurieren Sie Ihre Clusterzeit" .
- Wenn Sie Daten replizieren, überprüfen Sie, ob auf den Quell- und Zielsystemen kompatible ONTAP Versionen ausgeführt werden.

  "Kompatible ONTAP -Versionen für SnapMirror -Beziehungen anzeigen".

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Datensicherung im Objektspeicher

Sie müssen die folgenden Anforderungen auf dem System konfigurieren, das eine Verbindung zum Objektspeicher herstellt.

- Konfigurieren Sie für eine Fan-Out-Backup-Architektur die folgenden Einstellungen auf dem *primären* System.
- Konfigurieren Sie für eine kaskadierte Sicherungsarchitektur die folgenden Einstellungen auf dem *sekundären* System.

Die folgenden ONTAP Cluster-Netzwerkanforderungen sind erforderlich:

- Der ONTAP -Cluster initiiert für Sicherungs- und Wiederherstellungsvorgänge eine HTTPS-Verbindung über Port 443 vom Intercluster-LIF zum Azure Blob-Speicher.

  ONTAP liest und schreibt Daten in den und aus dem Objektspeicher. Der Objektspeicher wird nie initiiert, er reagiert nur.

- ONTAP erfordert eine eingehende Verbindung vom Konsolenagenten zum Cluster-Management-LIF. Der Konsolenagent kann sich in einem Azure VNet befinden.
- Auf jedem ONTAP Knoten, der die zu sichernden Volumes hostet, ist ein Intercluster-LIF erforderlich. Das LIF muss mit dem *IPspace* verknüpft sein, den ONTAP für die Verbindung mit dem Objektspeicher verwenden soll. "Erfahren Sie mehr über IPspaces" .

  Wenn Sie NetApp Backup and Recovery einrichten, werden Sie nach dem zu verwendenden IPspace gefragt. Sie sollten den IPspace auswählen, mit dem jedes LIF verknüpft ist. Dies kann der „Standard“-IP-Bereich oder ein benutzerdefinierter IP-Bereich sein, den Sie erstellt haben.

- Die LIFs der Knoten und zwischen Clustern können auf den Objektspeicher zugreifen.
- Für die Speicher-VM, auf der sich die Volumes befinden, wurden DNS-Server konfiguriert. Erfahren Sie, wie Sie "Konfigurieren Sie DNS-Dienste für die SVM" .
- Wenn Sie einen anderen IP-Bereich als den Standard verwenden, müssen Sie möglicherweise eine statische Route erstellen, um Zugriff auf den Objektspeicher zu erhalten.
- Aktualisieren Sie bei Bedarf die Firewall-Regeln, um Verbindungen des NetApp Backup and Recovery -Dienstes von ONTAP zum Objektspeicher über Port 443 und Namensauflösungsdatenverkehr von der Speicher-VM zum DNS-Server über Port 53 (TCP/UDP) zuzulassen.

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replikation von Volumes

Wenn Sie mit NetApp Backup and Recovery replizierte Volumes auf einem sekundären ONTAP System erstellen möchten, stellen Sie sicher, dass die Quell- und Zielsysteme die folgenden Netzwerkanforderungen erfüllen.

On-Premises ONTAP Netzwerkanforderungen

- Wenn sich der Cluster vor Ort befindet, sollten Sie über eine Verbindung von Ihrem Unternehmensnetzwerk zu Ihrem virtuellen Netzwerk beim Cloud-Anbieter verfügen. Dies ist normalerweise eine VPN-Verbindung.
- ONTAP -Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Clusteranforderungen erfüllen.

  Da Sie auf Cloud Volumes ONTAP oder lokale Systeme replizieren können, überprüfen Sie die Peering-Anforderungen für lokale ONTAP -Systeme. "Voraussetzungen für Cluster-Peering in der ONTAP Dokumentation anzeigen" .

Netzwerkanforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen Regeln für eingehenden und ausgehenden Datenverkehr enthalten, insbesondere Regeln für ICMP und die Ports 11104 und 11105. Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.

Bereiten Sie Azure Blob als Sicherungsziel vor

1. Sie können im Aktivierungsassistenten Ihre eigenen benutzerdefinierten verwalteten Schlüssel zur Datenverschlüsselung verwenden, anstatt die standardmäßigen, von Microsoft verwalteten Verschlüsselungsschlüssel zu verwenden. In diesem Fall benötigen Sie das Azure-Abonnement, den Key Vault-Namen und den Schlüssel. "Erfahren Sie, wie Sie Ihre eigenen Schlüssel verwenden" .

   Beachten Sie, dass Backup und Wiederherstellung *Azure-Zugriffsrichtlinien* als Berechtigungsmodell unterstützen. Das Berechtigungsmodell *Azure Role-Based Access Control* (Azure RBAC) wird derzeit nicht unterstützt.

2. Wenn Sie eine sicherere Verbindung über das öffentliche Internet von Ihrem lokalen Rechenzentrum zum VNet wünschen, besteht im Aktivierungsassistenten die Möglichkeit, einen privaten Azure-Endpunkt zu konfigurieren. In diesem Fall müssen Sie das VNet und das Subnetz für diese Verbindung kennen. "Weitere Informationen zur Verwendung eines privaten Endpunkts finden Sie hier." .

Erstellen Ihres Azure Blob-Speicherkontos

Standardmäßig erstellt der Dienst Speicherkonten für Sie. Wenn Sie Ihre eigenen Speicherkonten verwenden möchten, können Sie diese vor dem Starten des Sicherungsaktivierungsassistenten erstellen und diese Speicherkonten dann im Assistenten auswählen.

"Erfahren Sie mehr über das Erstellen eigener Speicherkonten".

Aktivieren Sie Backups auf Ihren ONTAP -Volumes

Aktivieren Sie Backups jederzeit direkt von Ihrem lokalen System aus.

Ein Assistent führt Sie durch die folgenden Hauptschritte:

- die Sie sichern möchten
- Definieren Sie die Sicherungsstrategie
- Überprüfen Sie Ihre Auswahl

Sie können auchAPI-Befehle anzeigen im Überprüfungsschritt, damit Sie den Code kopieren können, um die Sicherungsaktivierung für zukünftige Systeme zu automatisieren.

Starten des Assistenten

Schritte

1. Greifen Sie auf eine der folgenden Arten auf den Assistenten „Sicherung und Wiederherstellung aktivieren“ zu:

   - Wählen Sie auf der Konsolenseite **Systeme** das System aus und wählen Sie im rechten Bereich neben dem Sicherungs- und Wiederherstellungsdienst **Aktivieren > Sicherungsvolumes**.

     Wenn das Azure-Ziel für Ihre Sicherungen auf der Konsolenseite **Systeme** vorhanden ist, können Sie den ONTAP Cluster auf den Azure Blob-Objektspeicher ziehen.

   - Wählen Sie in der Leiste „Sichern und Wiederherstellen“ **Volumes** aus. Wählen Sie auf der Registerkarte „Volumes“ die Option „Aktionen“ aus. ••• und wählen Sie **Sicherung aktivieren** für ein einzelnes Volume (für das die Replikation oder Sicherung in den Objektspeicher noch nicht aktiviert ist).

   Auf der Einführungsseite des Assistenten werden die Schutzoptionen angezeigt, darunter lokale Snapshots, Replikation und Backups. Wenn Sie in diesem Schritt die zweite Option gewählt haben, wird die Seite „Sicherungsstrategie definieren“ mit einem ausgewählten Volume angezeigt.

2. Fahren Sie mit den folgenden Optionen fort:

   - Wenn Sie bereits über einen Konsolenagenten verfügen, sind Sie startklar. Wählen Sie einfach **Weiter**.
   - Wenn Sie noch keinen Konsolenagenten haben, wird die Option **Konsolenagenten hinzufügen** angezeigt. SieheVorbereiten Ihres Konsolenagenten .

Wählen Sie die Volumes aus, die Sie sichern möchten

Wählen Sie die Volumes aus, die Sie schützen möchten. Ein geschütztes Volume verfügt über eine oder mehrere der folgenden Optionen: Snapshot-Richtlinie, Replikationsrichtlinie, Backup-to-Object-Richtlinie.

Sie können FlexVol oder FlexGroup -Volumes schützen. Sie können jedoch keine Mischung dieser Volumes auswählen, wenn Sie die Sicherung für ein System aktivieren. Erfahren Sie, wie Sie"Aktivieren Sie die Sicherung für zusätzliche Volumes im System" (FlexVol oder FlexGroup), nachdem Sie die Sicherung für die ersten Volumes konfiguriert haben.

- Sie können eine Sicherung jeweils nur auf einem einzigen FlexGroup -Volume aktivieren.
- Die von Ihnen ausgewählten Volumes müssen über dieselbe SnapLock Einstellung verfügen. Auf allen Volumes muss SnapLock Enterprise aktiviert oder SnapLock sein.

Schritte

Beachten Sie: Wenn auf die von Ihnen ausgewählten Volumes bereits Snapshot- oder Replikationsrichtlinien angewendet wurden, werden diese vorhandenen Richtlinien durch die später ausgewählten Richtlinien überschrieben.

1. Wählen Sie auf der Seite „Volumes auswählen“ das oder die Volumes aus, die Sie schützen möchten.
   - Filtern Sie die Zeilen optional, um nur Datenträger mit bestimmten Datenträgertypen, Stilen usw. anzuzeigen und so die Auswahl zu vereinfachen.
   - Nachdem Sie das erste Volume ausgewählt haben, können Sie alle FlexVol Volumes auswählen (FlexGroup Volumes können jeweils nur einzeln ausgewählt werden). Um alle vorhandenen FlexVol Volumes zu sichern, markieren Sie zuerst ein Volume und aktivieren Sie dann das Kontrollkästchen in der Titelzeile.

- Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume.

2. Wählen Sie **Weiter**.

Definieren Sie die Sicherungsstrategie

Zum Definieren der Sicherungsstrategie müssen die folgenden Optionen festgelegt werden:

- Ob Sie eine oder alle Backup-Optionen wünschen: lokale Snapshots, Replikation und Backup auf Objektspeicher
- Architektur
- Lokale Snapshot-Richtlinie
- Replikationsziel und -richtlinie

> Wenn die von Ihnen ausgewählten Volumes andere Snapshot- und Replikationsrichtlinien haben als die Richtlinien, die Sie in diesem Schritt auswählen, werden die vorhandenen Richtlinien überschrieben.

- Informationen zur Sicherung in Objektspeichern (Anbieter, Verschlüsselung, Netzwerk, Sicherungsrichtlinie und Exportoptionen).

Schritte

1. Wählen Sie auf der Seite „Sicherungsstrategie definieren“ eine oder alle der folgenden Optionen aus. Alle drei sind standardmäßig ausgewählt:
   - **Lokale Snapshots**: Wenn Sie eine Replikation oder Sicherung im Objektspeicher durchführen, müssen lokale Snapshots erstellt werden.
   - **Replikation**: Erstellt replizierte Volumes auf einem anderen ONTAP Speichersystem.
   - **Backup**: Sichert Volumes im Objektspeicher.
2. **Architektur**: Wenn Sie Replikation und Sicherung gewählt haben, wählen Sie einen der folgenden Informationsflüsse:
   - **Kaskadierung**: Informationen fließen vom Primär- zum Sekundärspeicher und vom Sekundärspeicher zum Objektspeicher.
   - **Fan-out**: Informationen fließen vom primären zum sekundären *und* vom primären zum Objektspeicher.

     Weitere Informationen zu diesen Architekturen finden Sie unter"Planen Sie Ihren Schutzweg" .
3. **Lokaler Snapshot**: Wählen Sie eine vorhandene Snapshot-Richtlinie oder erstellen Sie eine neue.

   > Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung des Snapshots finden Sie unter"Erstellen einer Richtlinie" .

   Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:
   - Geben Sie den Namen der Richtlinie ein.
   - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
   - Wählen Sie **Erstellen**.
4. **Replikation**: Legen Sie die folgenden Optionen fest:
   - **Replikationsziel**: Wählen Sie das Zielsystem und die SVM aus. Wählen Sie optional das oder die

Zielaggregate sowie das Präfix oder Suffix aus, das dem Namen des replizierten Volumes hinzugefügt wird.

- **Replikationsrichtlinie**: Wählen Sie eine vorhandene Replikationsrichtlinie aus oder erstellen Sie eine neue.

  Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Replikation finden Sie unter"Erstellen einer Richtlinie" .

  Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:

  - Geben Sie den Namen der Richtlinie ein.
  - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
  - Wählen Sie **Erstellen**.

5. **Sichern auf Objekt**: Wenn Sie **Sichern** ausgewählt haben, legen Sie die folgenden Optionen fest:
   - **Anbieter**: Wählen Sie **Microsoft Azure**.
   - **Anbietereinstellungen**: Geben Sie die Anbieterdetails und die Region ein, in der die Backups gespeichert werden.

     Erstellen Sie entweder ein neues Speicherkonto oder wählen Sie ein vorhandenes aus.

     Erstellen Sie entweder Ihre eigene Ressourcengruppe, die den Blob-Container verwaltet, oder wählen Sie den Ressourcengruppentyp und die Gruppe aus.

     Wenn Sie Ihre Sicherungsdateien vor Änderungen oder Löschungen schützen möchten, stellen Sie sicher, dass das Speicherkonto mit aktiviertem unveränderlichem Speicher und einer Aufbewahrungsfrist von 30 Tagen erstellt wurde.

     Wenn Sie ältere Sicherungsdateien zur weiteren Kostenoptimierung in Azure Archive Storage auslagern möchten, stellen Sie sicher, dass das Speicherkonto über die entsprechende Lebenszyklusregel verfügt.

   - **Verschlüsselungsschlüssel**: Wenn Sie ein neues Azure-Speicherkonto erstellt haben, geben Sie die Informationen zum Verschlüsselungsschlüssel ein, die Sie vom Anbieter erhalten haben. Wählen Sie, ob Sie die standardmäßigen Azure-Verschlüsselungsschlüssel verwenden oder Ihre eigenen, vom Kunden verwalteten Schlüssel aus Ihrem Azure-Konto auswählen möchten, um die Verschlüsselung Ihrer Daten zu verwalten.

     Wenn Sie Ihre eigenen, vom Kunden verwalteten Schlüssel verwenden möchten, geben Sie den Schlüsseltresor und die Schlüsselinformationen ein.

     Wenn Sie ein vorhandenes Microsoft-Speicherkonto ausgewählt haben, sind die Verschlüsselungsinformationen bereits verfügbar, sodass Sie sie jetzt nicht eingeben müssen.

   - **Netzwerk**: Wählen Sie den IP-Bereich und geben Sie an, ob Sie einen privaten Endpunkt verwenden möchten. Privater Endpunkt ist standardmäßig deaktiviert.
     i. Der IP-Bereich im ONTAP -Cluster, in dem sich die Volumes befinden, die Sie sichern möchten. Die Intercluster-LIFs für diesen IPspace müssen über ausgehenden Internetzugang verfügen.
     ii. Wählen Sie optional aus, ob Sie einen zuvor konfigurierten privaten Azure-Endpunkt verwenden

möchten. "Erfahren Sie mehr über die Verwendung eines privaten Azure-Endpunkts" .

- **Sicherungsrichtlinie**: Wählen Sie eine vorhandene Richtlinie zum Sichern in einem Objektspeicher aus oder erstellen Sie eine neue.

  Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Sicherung finden Sie unter"Erstellen einer Richtlinie" .

  Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:

  - Geben Sie den Namen der Richtlinie ein.
  - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
  - Legen Sie für Backup-to-Object-Richtlinien die Einstellungen „DataLock“ und „Ransomware Resilience“ fest. Weitere Informationen zu DataLock und Ransomware Resilience finden Sie unter"Einstellungen der Backup-to-Object-Richtlinie" .
  - Wählen Sie **Erstellen**.

- **Vorhandene Snapshots als Sicherungskopien in den Objektspeicher exportieren**: Wenn es lokale Snapshots für Volumes in diesem System gibt, die mit der von Ihnen soeben für dieses System ausgewählten Sicherungszeitplanbezeichnung übereinstimmen (z. B. täglich, wöchentlich usw.), wird diese zusätzliche Aufforderung angezeigt. Aktivieren Sie dieses Kontrollkästchen, um alle historischen Snapshots als Sicherungsdateien in den Objektspeicher zu kopieren und so den umfassendsten Schutz für Ihre Volumes zu gewährleisten.

6. Wählen Sie **Weiter**.

Überprüfen Sie Ihre Auswahl

Dies ist die Gelegenheit, Ihre Auswahl zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

Schritte

1. Überprüfen Sie Ihre Auswahl auf der Überprüfungsseite.
2. Aktivieren Sie optional das Kontrollkästchen, um **die Snapshot-Richtlinienbezeichnungen automatisch mit den Replikations- und Sicherungsrichtlinienbezeichnungen zu synchronisieren**. Dadurch werden Snapshots mit einer Bezeichnung erstellt, die mit den Bezeichnungen in den Replikations- und Sicherungsrichtlinien übereinstimmt.
3. Wählen Sie **Backup aktivieren**.

Ergebnis

NetApp Backup and Recovery beginnt mit der Durchführung der ersten Sicherungen Ihrer Volumes. Die Basisübertragung des replizierten Volumes und der Sicherungsdatei umfasst eine vollständige Kopie der Daten des primären Speichersystems. Nachfolgende Übertragungen enthalten differentielle Kopien der Daten des primären Speichersystems, die in Snapshots enthalten sind.

Im Zielcluster wird ein repliziertes Volume erstellt, das mit dem primären Volume synchronisiert wird.

In der von Ihnen eingegebenen Ressourcengruppe wird ein Blob-Speicherkonto erstellt und die Sicherungsdateien werden dort gespeichert. Das Volume-Backup-Dashboard wird angezeigt, damit Sie den Status der Backups überwachen können.

Sie können den Status von Sicherungs- und Wiederherstellungsaufträgen auch mithilfe der"Seite „Jobüberwachung“" .

API-Befehle anzeigen

Möglicherweise möchten Sie die im Assistenten „Sicherung und Wiederherstellung aktivieren“ verwendeten API-Befehle anzeigen und optional kopieren. Möglicherweise möchten Sie dies tun, um die Sicherungsaktivierung in zukünftigen Systemen zu automatisieren.

Schritte

1. Wählen Sie im Assistenten „Sicherung und Wiederherstellung aktivieren“ die Option „API-Anforderung anzeigen“ aus.
2. Um die Befehle in die Zwischenablage zu kopieren, wählen Sie das Symbol **Kopieren**.

Sichern Sie lokale ONTAP -Daten mit NetApp Backup and Recovery in Google Cloud Storage

Führen Sie einige Schritte in NetApp Backup and Recovery aus, um mit der Sicherung von Volume-Daten von Ihren lokalen primären ONTAP Systemen auf ein sekundäres Speichersystem und in Google Cloud Storage zu beginnen.

Zu den „On-Premises ONTAP -Systemen“ gehören FAS, AFF und ONTAP Select Systeme.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

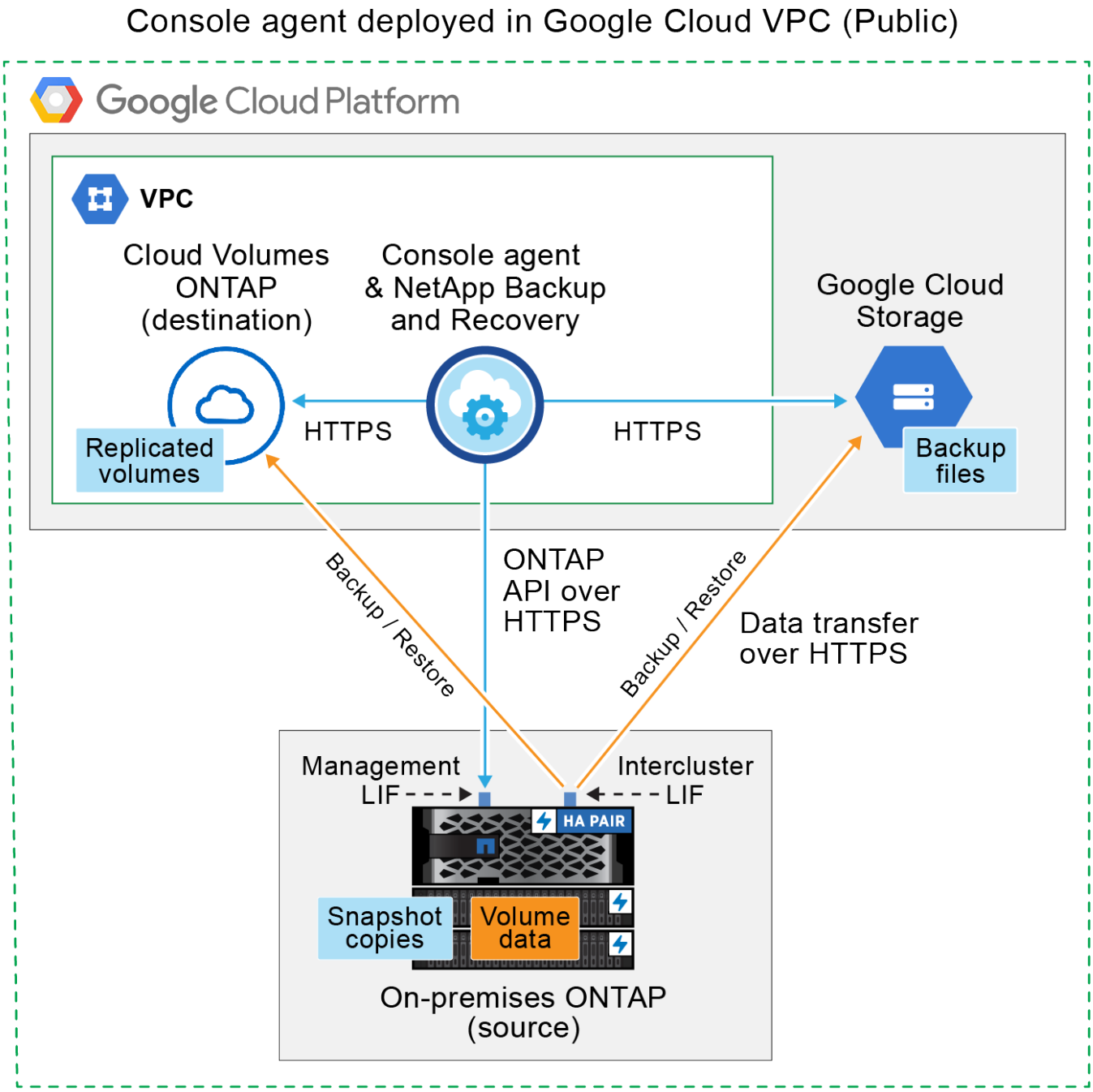
Identifizieren Sie die Verbindungsmethode

Wählen Sie aus, welche der beiden Verbindungsmethoden Sie beim Konfigurieren von Backups von lokalen ONTAP -Systemen zu Google Cloud Storage verwenden möchten.

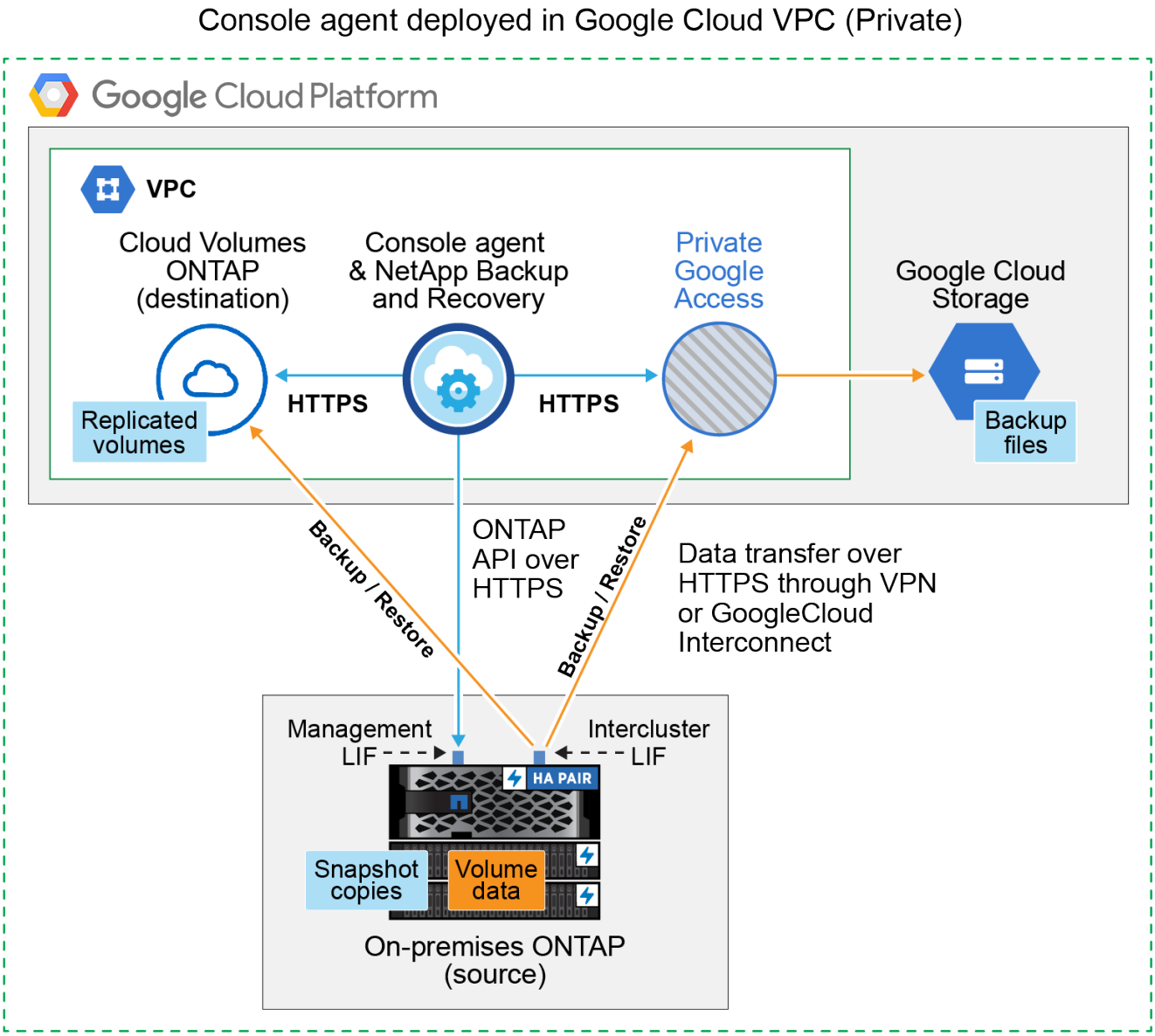
- **Öffentliche Verbindung** – Verbinden Sie das ONTAP -System über einen öffentlichen Google-Endpunkt direkt mit Google Cloud Storage.
- **Private Verbindung** – Verwenden Sie ein VPN oder Google Cloud Interconnect und leiten Sie den Datenverkehr über eine private Google Access-Schnittstelle, die eine private IP-Adresse verwendet.

Optional können Sie auch über die öffentliche oder private Verbindung eine Verbindung zu einem sekundären ONTAP System für replizierte Volumes herstellen.

Das folgende Diagramm zeigt die Methode **öffentliche Verbindung** und die Verbindungen, die Sie zwischen den Komponenten vorbereiten müssen. Der Konsolenagent muss in der Google Cloud Platform VPC bereitgestellt werden.



Das folgende Diagramm zeigt die Methode **private Verbindung** und die Verbindungen, die Sie zwischen den Komponenten vorbereiten müssen. Der Konsolenagent muss in der Google Cloud Platform VPC bereitgestellt werden.



Vorbereiten Ihres Konsolenagenten

Der Konsolenagent ist die Hauptsoftware für die Konsolenfunktionalität. Zum Sichern und Wiederherstellen Ihrer ONTAP Daten ist ein Konsolenagent erforderlich.

Erstellen oder Wechseln von Konsolenagenten

Wenn Sie bereits einen Konsolenagenten in Ihrer Google Cloud Platform VPC bereitgestellt haben, sind Sie startklar.

Wenn nicht, müssen Sie an diesem Speicherort einen Konsolenagenten erstellen, um ONTAP -Daten in Google Cloud Storage zu sichern. Sie können keinen Konsolenagenten verwenden, der bei einem anderen Cloud-Anbieter oder vor Ort bereitgestellt wird.

- "Erfahren Sie mehr über Konsolenagenten"
- "Installieren Sie einen Konsolenagenten in GCP"

Vorbereiten des Netzwerks für den Konsolenagenten

Stellen Sie sicher, dass der Konsolenagent über die erforderlichen Netzwerkverbindungen verfügt.

Schritte

1. Stellen Sie sicher, dass das Netzwerk, in dem der Konsolenagent installiert ist, die folgenden Verbindungen ermöglicht:
   - Eine HTTPS-Verbindung über Port 443 zu NetApp Backup and Recovery und zu Ihrem Google Cloud-Speicher("siehe Liste der Endpunkte")
   - Eine HTTPS-Verbindung über Port 443 zu Ihrem ONTAP Cluster-Management-LIF
2. Aktivieren Sie den privaten Google-Zugriff (oder Private Service Connect) in dem Subnetz, in dem Sie den Konsolen-Agenten bereitstellen möchten. "Privater Google-Zugriff" oder "Private Service Connect" werden benötigt, wenn Sie eine direkte Verbindung von Ihrem ONTAP Cluster zum VPC haben und die Kommunikation zwischen dem Konsolenagenten und Google Cloud Storage in Ihrem virtuellen privaten Netzwerk (einer **privaten** Verbindung) bleiben soll.

   Befolgen Sie die Google-Anweisungen zum Einrichten dieser privaten Zugriffsoptionen. Stellen Sie sicher, dass Ihre DNS-Server so konfiguriert sind, dass sie auf `www.googleapis.com` Und `storage.googleapis.com` an die richtigen internen (privaten) IP-Adressen.

Überprüfen oder Hinzufügen von Berechtigungen für den Konsolenagenten

Um die Funktion „Suchen und Wiederherstellen“ von NetApp Backup and Recovery verwenden zu können, benötigen Sie bestimmte Berechtigungen in der Rolle für den Konsolenagenten, damit dieser auf den Google Cloud BigQuery-Dienst zugreifen kann. Überprüfen Sie die unten aufgeführten Berechtigungen und befolgen Sie die Schritte, wenn Sie die Richtlinie ändern müssen.

Schritte

1. Im "Google Cloud Console" , gehen Sie zur Seite **Rollen**.
2. Wählen Sie mithilfe der Dropdownliste oben auf der Seite das Projekt oder die Organisation aus, das/die die Rolle enthält, die Sie bearbeiten möchten.
3. Wählen Sie eine benutzerdefinierte Rolle aus.
4. Wählen Sie **Rolle bearbeiten**, um die Berechtigungen der Rolle zu aktualisieren.
5. Wählen Sie **Berechtigungen hinzufügen** aus, um der Rolle die folgenden neuen Berechtigungen hinzuzufügen.

```
bigquery.jobs.get
bigquery.jobs.list
bigquery.jobs.listAll
bigquery.datasets.create
bigquery.datasets.get
bigquery.jobs.create
bigquery.tables.get
bigquery.tables.getData
bigquery.tables.list
bigquery.tables.create
```

6. Wählen Sie **Aktualisieren**, um die bearbeitete Rolle zu speichern.

Überprüfen der Lizenzanforderungen

- Bevor Sie NetApp Backup and Recovery für Ihren Cluster aktivieren können, müssen Sie entweder ein Pay-as-you-go (PAYGO) Console Marketplace-Angebot von Google abonnieren oder eine NetApp Backup and Recovery BYOL-Lizenz von NetApp erwerben und aktivieren. Diese Lizenzen gelten für Ihr Konto und können systemübergreifend verwendet werden.
  - Für die NetApp Backup and Recovery PAYGO-Lizenzierung benötigen Sie ein Abonnement für die "NetApp Console -Angebot vom Google Marketplace" . Die Abrechnung für NetApp Backup and Recovery erfolgt über dieses Abonnement.
  - Für die NetApp Backup and Recovery BYOL-Lizenzierung benötigen Sie die Seriennummer von NetApp , die Ihnen die Nutzung des Dienstes für die Dauer und Kapazität der Lizenz ermöglicht. "Erfahren Sie, wie Sie Ihre BYOL-Lizenzen verwalten".
- Sie benötigen ein Google-Abonnement für den Objektspeicherplatz, in dem Ihre Backups gespeichert werden.

Unterstützte Regionen

Sie können in allen Regionen Backups von lokalen Systemen in Google Cloud Storage erstellen. Sie geben die Region an, in der die Sicherungen gespeichert werden, wenn Sie den Dienst einrichten.

Bereiten Sie Ihre ONTAP -Cluster vor

Bereiten Sie Ihr lokales ONTAP -Quellsystem und alle sekundären lokalen ONTAP oder Cloud Volumes ONTAP Systeme vor.

Die Vorbereitung Ihrer ONTAP Cluster umfasst die folgenden Schritte:

- Entdecken Sie Ihre ONTAP -Systeme in der NetApp Console
- Überprüfen der ONTAP Systemanforderungen
- Überprüfen Sie die ONTAP Netzwerkanforderungen für die Datensicherung im Objektspeicher
- Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replikation von Volumes

Entdecken Sie Ihre ONTAP -Systeme in der NetApp Console

Sowohl Ihr lokales ONTAP Quellsystem als auch alle sekundären lokalen ONTAP oder Cloud Volumes ONTAP -Systeme müssen auf der Seite **Systeme** der NetApp Console verfügbar sein.

Sie müssen die IP-Adresse der Clusterverwaltung und das Kennwort für das Administratorbenutzerkonto kennen, um den Cluster hinzuzufügen. "Erfahren Sie, wie Sie einen Cluster erkennen".

Überprüfen der ONTAP Systemanforderungen

Stellen Sie sicher, dass Ihr ONTAP -System die folgenden Anforderungen erfüllt:

- Mindestens ONTAP 9.8; ONTAP 9.8P13 und höher wird empfohlen.
- Eine SnapMirror -Lizenz (im Premium-Paket oder Datenschutz-Paket enthalten).

  Hinweis: Das „Hybrid Cloud Bundle“ ist bei der Verwendung von NetApp Backup and Recovery nicht erforderlich.

Erfahren Sie, wie Sie "Verwalten Sie Ihre Cluster-Lizenzen" .

- Uhrzeit und Zeitzone sind richtig eingestellt. Erfahren Sie, wie Sie "Konfigurieren Sie Ihre Clusterzeit" .
- Wenn Sie Daten replizieren, überprüfen Sie, ob auf den Quell- und Zielsystemen kompatible ONTAP Versionen ausgeführt werden.

  "Kompatible ONTAP -Versionen für SnapMirror -Beziehungen anzeigen".

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Datensicherung im Objektspeicher

Sie müssen die folgenden Anforderungen auf dem System konfigurieren, das eine Verbindung zum Objektspeicher herstellt.

- Konfigurieren Sie für eine Fan-Out-Backup-Architektur die folgenden Einstellungen auf dem *primären* System.
- Konfigurieren Sie für eine kaskadierte Sicherungsarchitektur die folgenden Einstellungen auf dem *sekundären* System.

Die folgenden ONTAP Cluster-Netzwerkanforderungen sind erforderlich:

- Der ONTAP -Cluster initiiert für Sicherungs- und Wiederherstellungsvorgänge eine HTTPS-Verbindung über Port 443 vom Intercluster-LIF zu Google Cloud Storage.

  ONTAP liest und schreibt Daten in den und aus dem Objektspeicher. Der Objektspeicher wird nie initiiert, er reagiert nur.

- ONTAP erfordert eine eingehende Verbindung vom Konsolenagenten zum Cluster-Management-LIF. Der Konsolenagent kann sich in einer Google Cloud Platform VPC befinden.
- Auf jedem ONTAP Knoten, der die zu sichernden Volumes hostet, ist ein Intercluster-LIF erforderlich. Das LIF muss mit dem *IPspace* verknüpft sein, den ONTAP für die Verbindung mit dem Objektspeicher verwenden soll. "Erfahren Sie mehr über IPspaces" .

  Wenn Sie NetApp Backup and Recovery einrichten, werden Sie nach dem zu verwendenden IPspace gefragt. Sie sollten den IPspace auswählen, mit dem jedes LIF verknüpft ist. Dies kann der „Standard“-IP-Bereich oder ein benutzerdefinierter IP-Bereich sein, den Sie erstellt haben.

- Die Intercluster-LIFs der Knoten können auf den Objektspeicher zugreifen.
- Für die Speicher-VM, auf der sich die Volumes befinden, wurden DNS-Server konfiguriert. Erfahren Sie, wie Sie "Konfigurieren Sie DNS-Dienste für die SVM" .

  Wenn Sie Private Google Access oder Private Service Connect verwenden, stellen Sie sicher, dass Ihre DNS-Server so konfiguriert sind, dass sie auf `storage.googleapis.com` an die richtige interne (private) IP-Adresse.

- Beachten Sie, dass Sie möglicherweise eine statische Route erstellen müssen, um Zugriff auf den Objektspeicher zu erhalten, wenn Sie einen anderen IP-Bereich als den Standard verwenden.
- Aktualisieren Sie bei Bedarf die Firewall-Regeln, um NetApp Backup and Recovery -Verbindungen von ONTAP zum Objektspeicher über Port 443 und Namensauflösungsdatenverkehr von der Speicher-VM zum DNS-Server über Port 53 (TCP/UDP) zuzulassen.

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replikation von Volumes

Wenn Sie mit NetApp Backup and Recovery replizierte Volumes auf einem sekundären ONTAP System erstellen möchten, stellen Sie sicher, dass die Quell- und Zielsysteme die folgenden Netzwerkanforderungen erfüllen.

On-Premises ONTAP Netzwerkanforderungen

- Wenn sich der Cluster vor Ort befindet, sollten Sie über eine Verbindung von Ihrem Unternehmensnetzwerk zu Ihrem virtuellen Netzwerk beim Cloud-Anbieter verfügen. Dies ist normalerweise eine VPN-Verbindung.
- ONTAP -Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Clusteranforderungen erfüllen.

  Da Sie auf Cloud Volumes ONTAP oder lokale Systeme replizieren können, überprüfen Sie die Peering-Anforderungen für lokale ONTAP -Systeme. "Voraussetzungen für Cluster-Peering in der ONTAP Dokumentation anzeigen" .

Netzwerkanforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen Regeln für eingehenden und ausgehenden Datenverkehr enthalten, insbesondere Regeln für ICMP und die Ports 11104 und 11105. Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.

Bereiten Sie Google Cloud Storage als Sicherungsziel vor

Die Vorbereitung von Google Cloud Storage als Sicherungsziel umfasst die folgenden Schritte:

- Richten Sie Berechtigungen ein.
- (Optional) Erstellen Sie Ihre eigenen Buckets. (Der Dienst erstellt auf Wunsch Buckets für Sie.)
- (Optional) Einrichten von kundenverwalteten Schlüsseln für die Datenverschlüsselung

Einrichten von Berechtigungen

Sie müssen Speicherzugriffsschlüssel für ein Dienstkonto bereitstellen, das über bestimmte Berechtigungen mithilfe einer benutzerdefinierten Rolle verfügt. Ein Dienstkonto ermöglicht NetApp Backup and Recovery die Authentifizierung und den Zugriff auf Cloud Storage-Buckets, die zum Speichern von Backups verwendet werden. Die Schlüssel werden benötigt, damit Google Cloud Storage weiß, wer die Anfrage stellt.

Schritte

1. Im "Google Cloud Console" , gehen Sie zur Seite **Rollen**.
2. "Erstellen einer neuen Rolle"mit den folgenden Berechtigungen:

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. In der Google Cloud-Konsole "Gehen Sie zur Seite „Dienstkonten“" .
4. Wählen Sie Ihr Cloud-Projekt aus.
5. Wählen Sie **Dienstkonto erstellen** und geben Sie die erforderlichen Informationen ein:
   a. **Servicekontodetails**: Geben Sie einen Namen und eine Beschreibung ein.
   b. **Diesem Dienstkonto Zugriff auf das Projekt gewähren**: Wählen Sie die benutzerdefinierte Rolle aus, die Sie gerade erstellt haben.
   c. Wählen Sie **Fertig**.
6. Gehe zu "GCP-Speichereinstellungen" und erstellen Sie Zugriffsschlüssel für das Dienstkonto:
   a. Wählen Sie ein Projekt und dann **Interoperabilität** aus. Falls Sie dies noch nicht getan haben, wählen Sie **Interoperabilitätszugriff aktivieren**.
   b. Wählen Sie unter **Zugriffsschlüssel für Dienstkonten** die Option **Schlüssel für ein Dienstkonto erstellen** aus, wählen Sie das gerade erstellte Dienstkonto aus und klicken Sie auf **Schlüssel erstellen**.

      Sie müssen die Schlüssel später in NetApp Backup and Recovery eingeben, wenn Sie den Sicherungsdienst konfigurieren.

Erstellen Sie Ihre eigenen Eimer

Standardmäßig erstellt der Dienst Buckets für Sie. Wenn Sie Ihre eigenen Buckets verwenden möchten, können Sie diese auch erstellen, bevor Sie den Backup-Aktivierungsassistenten starten, und diese Buckets dann im Assistenten auswählen.

"Erfahren Sie mehr über das Erstellen eigener Buckets".

Einrichten von kundenverwalteten Verschlüsselungsschlüsseln (CMEK) zur Datenverschlüsselung

Sie können Ihre eigenen, vom Kunden verwalteten Schlüssel zur Datenverschlüsselung verwenden, anstatt die standardmäßig von Google verwalteten Verschlüsselungsschlüssel zu verwenden. Es werden sowohl regions- als auch projektübergreifende Schlüssel unterstützt, sodass Sie für einen Bucket ein Projekt auswählen können, das sich vom Projekt des CMEK-Schlüssels unterscheidet.

Wenn Sie Ihre eigenen, vom Kunden verwalteten Schlüssel verwenden möchten:

- Sie benötigen den Schlüsselbund und den Schlüsselnamen, damit Sie diese Informationen im Aktivierungsassistenten hinzufügen können. "Erfahren Sie mehr über vom Kunden verwaltete Verschlüsselungsschlüssel" .
- Sie müssen überprüfen, ob die folgenden erforderlichen Berechtigungen in der Rolle für den Konsolenagenten enthalten sind:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Sie müssen überprüfen, ob die Google-API „Cloud Key Management Service (KMS)“ in Ihrem Projekt aktiviert ist. Siehe die "Google Cloud-Dokumentation: APIs aktivieren" für Details.

CMEK-Überlegungen:

- Es werden sowohl HSM-Schlüssel (Hardware-gestützt) als auch softwaregenerierte Schlüssel unterstützt.
- Es werden sowohl neu erstellte als auch importierte Cloud KMS-Schlüssel unterstützt.
- Es werden nur regionale Schlüssel unterstützt, globale Schlüssel werden nicht unterstützt.
- Derzeit wird nur der Zweck „Symmetrische Verschlüsselung/Entschlüsselung“ unterstützt.
- Dem mit dem Speicherkonto verknüpften Service-Agent wird von NetApp Backup and Recovery die IAM-Rolle „CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)“ zugewiesen.

Aktivieren Sie Backups auf Ihren ONTAP -Volumes

Aktivieren Sie Backups jederzeit direkt von Ihrem lokalen System aus.

Ein Assistent führt Sie durch die folgenden Hauptschritte:

- die Sie sichern möchten
- Definieren Sie die Sicherungsstrategie
- Überprüfen Sie Ihre Auswahl

Sie können auchAPI-Befehle anzeigen im Überprüfungsschritt, damit Sie den Code kopieren können, um die Sicherungsaktivierung für zukünftige Systeme zu automatisieren.

Starten des Assistenten

Schritte

1. Greifen Sie auf eine der folgenden Arten auf den Assistenten „Sicherung und Wiederherstellung aktivieren“ zu:
    - Wählen Sie auf der Konsolenseite **Systeme** das System aus und wählen Sie im rechten Bereich neben „Sicherung und Wiederherstellung“ die Option „Aktivieren > Sicherungsvolumes“ aus.

Wenn das Google Cloud Storage-Ziel für Ihre Backups wie auf der Konsolenseite **Systeme** vorhanden ist, können Sie den ONTAP Cluster auf den Google Cloud-Objektspeicher ziehen.

- Wählen Sie in der Leiste „Sichern und Wiederherstellen“ **Volumes** aus. Wählen Sie auf der Registerkarte „Volumes“ die Option „Aktionen“ aus. ••• und wählen Sie **Sicherung aktivieren** für ein einzelnes Volume (für das die Replikation oder Sicherung in den Objektspeicher noch nicht aktiviert ist).

Auf der Einführungsseite des Assistenten werden die Schutzoptionen angezeigt, darunter lokale Snapshots, Replikation und Backups. Wenn Sie in diesem Schritt die zweite Option gewählt haben, wird die Seite „Sicherungsstrategie definieren“ mit einem ausgewählten Volume angezeigt.

2. Fahren Sie mit den folgenden Optionen fort:
   - Wenn Sie bereits über einen Konsolenagenten verfügen, sind Sie startklar. Wählen Sie einfach **Weiter**.
   - Wenn Sie noch keinen Konsolenagenten haben, wird die Option **Konsolenagenten hinzufügen** angezeigt. SieheVorbereiten Ihres Konsolenagenten .

Wählen Sie die Volumes aus, die Sie sichern möchten

Wählen Sie die Volumes aus, die Sie schützen möchten. Ein geschütztes Volume verfügt über eine oder mehrere der folgenden Optionen: Snapshot-Richtlinie, Replikationsrichtlinie, Backup-to-Object-Richtlinie.

Sie können FlexVol oder FlexGroup -Volumes schützen. Sie können jedoch keine Mischung dieser Volumes auswählen, wenn Sie die Sicherung für ein System aktivieren. Erfahren Sie, wie Sie"Aktivieren Sie die Sicherung für zusätzliche Volumes im System" (FlexVol oder FlexGroup), nachdem Sie die Sicherung für die ersten Volumes konfiguriert haben.

- Sie können eine Sicherung jeweils nur auf einem einzigen FlexGroup -Volume aktivieren.
- Die von Ihnen ausgewählten Volumes müssen über dieselbe SnapLock Einstellung verfügen. Auf allen Volumes muss SnapLock Enterprise aktiviert oder SnapLock sein.

Schritte

Wenn auf die von Ihnen ausgewählten Volumes bereits Snapshot- oder Replikationsrichtlinien angewendet wurden, werden diese vorhandenen Richtlinien durch die später ausgewählten Richtlinien überschrieben.

1. Wählen Sie auf der Seite „Volumes auswählen“ das oder die Volumes aus, die Sie schützen möchten.
   - Filtern Sie die Zeilen optional, um nur Datenträger mit bestimmten Datenträgertypen, Stilen usw. anzuzeigen und so die Auswahl zu vereinfachen.
   - Nachdem Sie das erste Volume ausgewählt haben, können Sie alle FlexVol Volumes auswählen (FlexGroup Volumes können jeweils nur einzeln ausgewählt werden). Um alle vorhandenen FlexVol Volumes zu sichern, markieren Sie zuerst ein Volume und aktivieren Sie dann das Kontrollkästchen in der Titelzeile.
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume.
2. Wählen Sie **Weiter**.

Definieren Sie die Sicherungsstrategie

Zum Definieren der Sicherungsstrategie müssen die folgenden Optionen festgelegt werden:

- Ob Sie eine oder alle der Backup-Optionen wünschen: lokale Snapshots, Replikation und Backup auf Objektspeicher

- Architektur
- Lokale Snapshot-Richtlinie
- Replikationsziel und -richtlinie

> Wenn die von Ihnen ausgewählten Volumes andere Snapshot- und Replikationsrichtlinien haben als die Richtlinien, die Sie in diesem Schritt auswählen, werden die vorhandenen Richtlinien überschrieben.

- Informationen zur Sicherung in Objektspeichern (Anbieter, Verschlüsselung, Netzwerk, Sicherungsrichtlinie und Exportoptionen).

Schritte

1. Wählen Sie auf der Seite „Sicherungsstrategie definieren“ eine oder alle der folgenden Optionen aus. Alle drei sind standardmäßig ausgewählt:
   - **Lokale Snapshots**: Wenn Sie eine Replikation oder Sicherung im Objektspeicher durchführen, müssen lokale Snapshots erstellt werden.
   - **Replikation**: Erstellt replizierte Volumes auf einem anderen ONTAP Speichersystem.
   - **Backup**: Sichert Volumes im Objektspeicher.
2. **Architektur**: Wenn Sie Replikation und Sicherung gewählt haben, wählen Sie einen der folgenden Informationsflüsse:
   - **Kaskadierung**: Informationen fließen vom primären zum sekundären und vom sekundären zum Objektspeicher.
   - **Fan-out**: Informationen fließen vom primären zum sekundären *und* vom primären zum Objektspeicher.

   Weitere Informationen zu diesen Architekturen finden Sie unter"Planen Sie Ihren Schutzweg" .
3. **Lokaler Snapshot**: Wählen Sie eine vorhandene Snapshot-Richtlinie oder erstellen Sie eine neue.

   > Informationen zum Erstellen einer benutzerdefinierten Richtlinie finden Sie unter"Erstellen einer Richtlinie" .

   Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:
   - Geben Sie den Namen der Richtlinie ein.
   - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
   - Wählen Sie **Erstellen**.
4. **Replikation**: Legen Sie die folgenden Optionen fest:
   - **Replikationsziel**: Wählen Sie das Zielsystem und die SVM aus. Wählen Sie optional das oder die Zielaggregate sowie das Präfix oder Suffix aus, das dem Namen des replizierten Volumes hinzugefügt wird.
   - **Replikationsrichtlinie**: Wählen Sie eine vorhandene Replikationsrichtlinie aus oder erstellen Sie eine neue.

     > Informationen zum Erstellen einer benutzerdefinierten Richtlinie finden Sie unter"Erstellen einer Richtlinie" .

     Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:

- Geben Sie den Namen der Richtlinie ein.
- Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
- Wählen Sie **Erstellen**.

5. **Sichern auf Objekt**: Wenn Sie **Sichern** ausgewählt haben, legen Sie die folgenden Optionen fest:
   - **Anbieter**: Wählen Sie **Google Cloud**.
   - **Anbietereinstellungen**: Geben Sie die Anbieterdetails und die Region ein, in der die Backups gespeichert werden.

     Erstellen Sie entweder einen neuen Bucket oder wählen Sie einen bereits erstellten Bucket aus.

     Wenn Sie ältere Sicherungsdateien zur weiteren Kostenoptimierung in den Google Cloud Archive-Speicher verschieben möchten, stellen Sie sicher, dass der Bucket über die entsprechende Lebenszyklusregel verfügt.

     Geben Sie den Google Cloud-Zugriffsschlüssel und den geheimen Schlüssel ein.

   - **Verschlüsselungsschlüssel**: Wenn Sie ein neues Google Cloud-Speicherkonto erstellt haben, geben Sie die Informationen zum Verschlüsselungsschlüssel ein, die Sie vom Anbieter erhalten haben. Wählen Sie, ob Sie die standardmäßigen Google Cloud-Verschlüsselungsschlüssel verwenden oder Ihre eigenen, vom Kunden verwalteten Schlüssel aus Ihrem Google Cloud-Konto auswählen möchten, um die Verschlüsselung Ihrer Daten zu verwalten.

     Wenn Sie ein vorhandenes Google Cloud-Speicherkonto ausgewählt haben, sind die Verschlüsselungsinformationen bereits verfügbar, sodass Sie sie jetzt nicht eingeben müssen.

     Wenn Sie Ihre eigenen, vom Kunden verwalteten Schlüssel verwenden möchten, geben Sie den Schlüsselbund und den Schlüsselnamen ein. "Erfahren Sie mehr über vom Kunden verwaltete Verschlüsselungsschlüssel" .

   - **Netzwerk**: Wählen Sie den IP-Bereich.

     Der IP-Bereich im ONTAP -Cluster, in dem sich die Volumes befinden, die Sie sichern möchten. Die Intercluster-LIFs für diesen IPspace müssen über ausgehenden Internetzugang verfügen.

   - **Sicherungsrichtlinie**: Wählen Sie eine vorhandene Richtlinie zum Sichern in einem Objektspeicher aus oder erstellen Sie eine neue.

     Informationen zum Erstellen einer benutzerdefinierten Richtlinie finden Sie unter"Erstellen einer Richtlinie" .

     Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:

     - Geben Sie den Namen der Richtlinie ein.
     - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
     - Wählen Sie **Erstellen**.

   - **Vorhandene Snapshots als Sicherungskopien in den Objektspeicher exportieren**: Wenn es lokale Snapshots für Volumes in diesem System gibt, die mit der von Ihnen soeben für dieses System ausgewählten Sicherungszeitplanbezeichnung übereinstimmen (z. B. täglich, wöchentlich usw.), wird diese zusätzliche Aufforderung angezeigt. Aktivieren Sie dieses Kontrollkästchen, um alle historischen

Snapshots als Sicherungsdateien in den Objektspeicher zu kopieren und so den umfassendsten Schutz für Ihre Volumes zu gewährleisten.

6. Wählen Sie **Weiter**.

Überprüfen Sie Ihre Auswahl

Dies ist die Gelegenheit, Ihre Auswahl zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

Schritte

1. Überprüfen Sie Ihre Auswahl auf der Überprüfungsseite.
2. Aktivieren Sie optional das Kontrollkästchen, um **die Snapshot-Richtlinienbezeichnungen automatisch mit den Replikations- und Sicherungsrichtlinienbezeichnungen zu synchronisieren**. Dadurch werden Snapshots mit einer Bezeichnung erstellt, die mit den Bezeichnungen in den Replikations- und Sicherungsrichtlinien übereinstimmt.
3. Wählen Sie **Backup aktivieren**.

Ergebnis

NetApp Backup and Recovery beginnt mit der Durchführung der ersten Sicherungen Ihrer Volumes. Die Basisübertragung des replizierten Volumes und der Sicherungsdatei umfasst eine vollständige Kopie der Daten des primären Speichersystems. Nachfolgende Übertragungen enthalten differentielle Kopien der Daten des primären Speichersystems, die in Snapshots enthalten sind.

Im Zielcluster wird ein repliziertes Volume erstellt, das mit dem Quellvolume synchronisiert wird.

In dem durch den von Ihnen eingegebenen Google-Zugriffsschlüssel und geheimen Schlüssel angegebenen Dienstkonto wird automatisch ein Google Cloud Storage-Bucket erstellt und die Sicherungsdateien werden dort gespeichert. Das Volume-Backup-Dashboard wird angezeigt, damit Sie den Status der Backups überwachen können.

Sie können den Status von Sicherungs- und Wiederherstellungsaufträgen auch mithilfe der"Seite „Jobüberwachung“" .

API-Befehle anzeigen

Möglicherweise möchten Sie die im Assistenten „Sicherung und Wiederherstellung aktivieren“ verwendeten API-Befehle anzeigen und optional kopieren. Möglicherweise möchten Sie dies tun, um die Sicherungsaktivierung in zukünftigen Systemen zu automatisieren.

Schritte

1. Wählen Sie im Assistenten „Sicherung und Wiederherstellung aktivieren“ die Option „API-Anforderung anzeigen“ aus.
2. Um die Befehle in die Zwischenablage zu kopieren, wählen Sie das Symbol **Kopieren**.

Sichern Sie lokale ONTAP -Daten auf ONTAP S3 mit NetApp Backup and Recovery

Führen Sie einige Schritte in NetApp Backup and Recovery aus, um mit der Sicherung von Volumedaten von Ihren primären lokalen ONTAP Systemen zu beginnen. Sie können Backups an ein sekundäres ONTAP Speichersystem (ein repliziertes Volume) oder an einen Bucket auf einem als S3-Server konfigurierten ONTAP System (eine Backup-Datei) oder an beides senden.

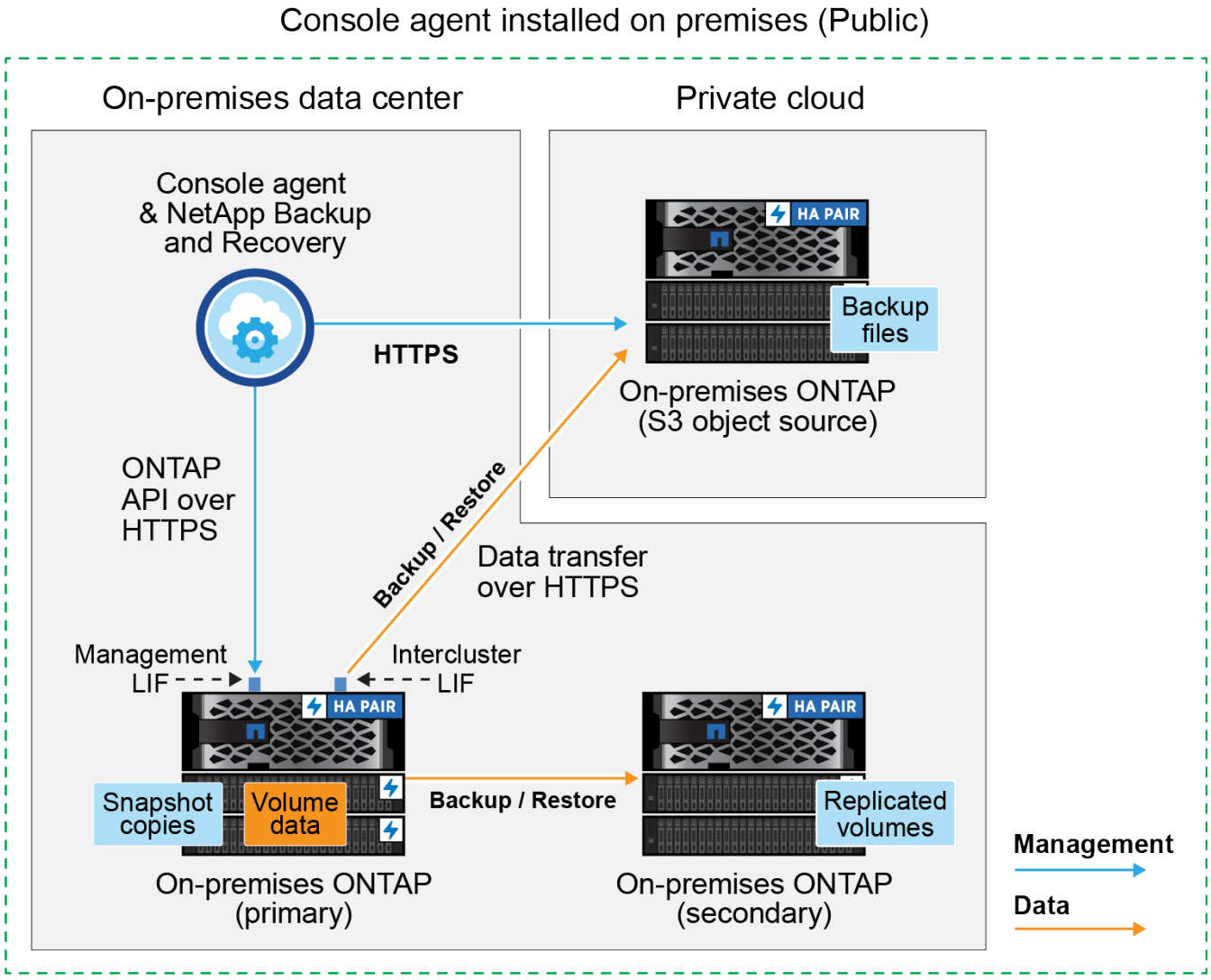
Das primäre lokale ONTAP -System kann ein FAS, AFF oder ONTAP Select System sein. Das sekundäre ONTAP -System kann ein lokales ONTAP oder Cloud Volumes ONTAP System sein. Der Objektspeicher kann sich auf einem lokalen ONTAP -System oder einem Cloud Volumes ONTAP System befinden, auf dem Sie einen Simple Storage Service (S3)-Objektspeicherserver aktiviert haben.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

Identifizieren Sie die Verbindungsmethode

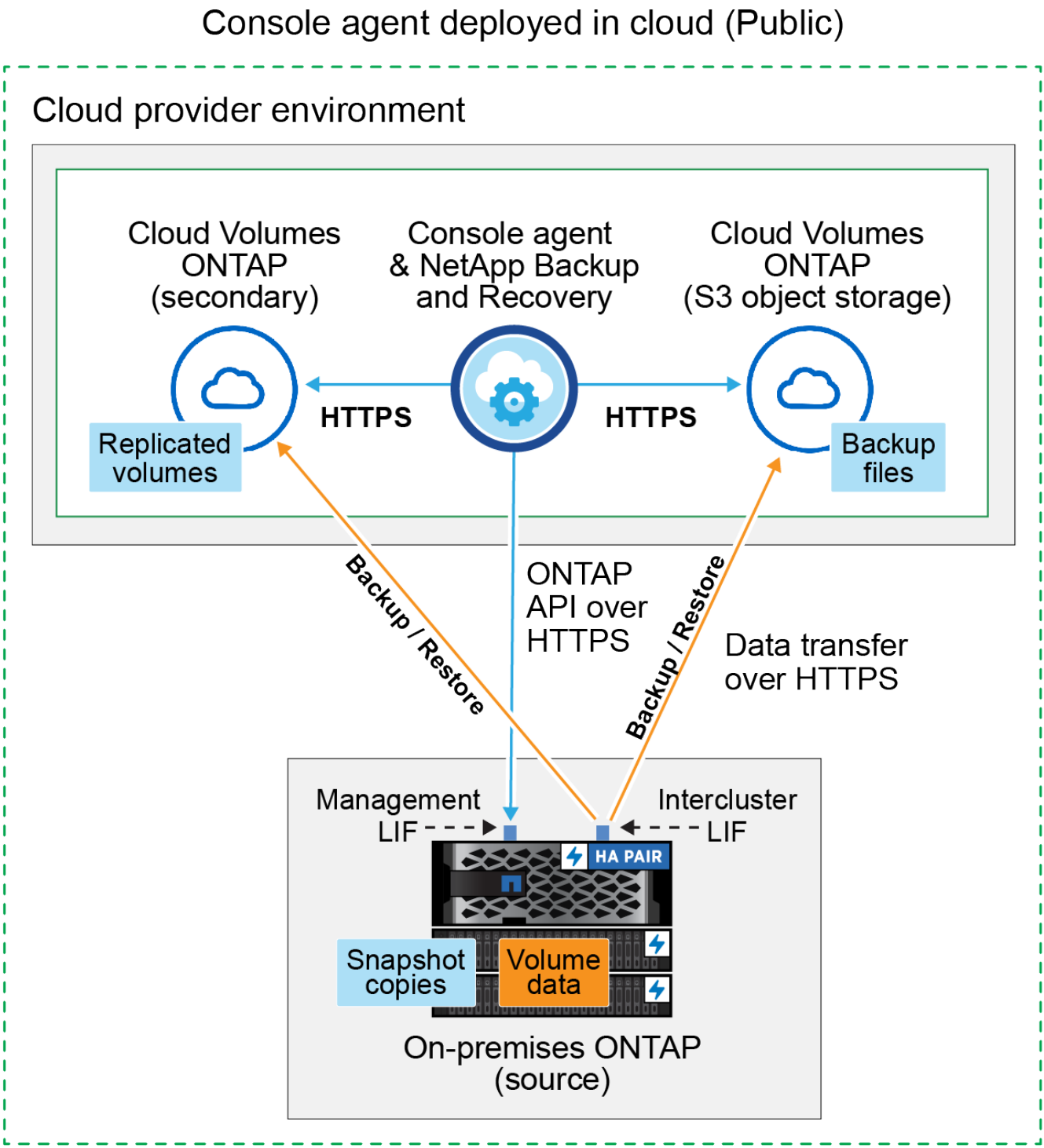
Es gibt viele Konfigurationen, in denen Sie Backups in einem S3-Bucket auf einem ONTAP System erstellen können. Nachfolgend werden zwei Szenarien dargestellt.

Das folgende Bild zeigt jede Komponente beim Sichern eines primären lokalen ONTAP -Systems auf ein für S3 konfiguriertes lokales ONTAP System und die Verbindungen, die Sie zwischen ihnen vorbereiten müssen. Es zeigt auch eine Verbindung zu einem sekundären ONTAP -System am selben Standort vor Ort, um Volumes zu replizieren.



Wenn der Konsolenagent und das primäre lokale ONTAP -System an einem lokalen Standort ohne Internetzugang installiert sind (eine Bereitstellung im „privaten“ Modus), muss sich das ONTAP S3-System im selben lokalen Rechenzentrum befinden.

Das folgende Bild zeigt jede Komponente beim Sichern eines primären lokalen ONTAP -Systems auf ein für S3 konfiguriertes Cloud Volumes ONTAP System und die Verbindungen, die Sie zwischen ihnen vorbereiten müssen. Es zeigt auch eine Verbindung zu einem sekundären Cloud Volumes ONTAP -System in derselben Cloud-Provider-Umgebung, um Volumes zu replizieren.



In diesem Szenario sollte der Konsolenagent in derselben Cloud-Provider-Umgebung bereitgestellt werden, in der die Cloud Volumes ONTAP -Systeme bereitgestellt werden.

Vorbereiten Ihres Konsolenagenten

Der Konsolenagent ist die Hauptsoftware für die Konsolenfunktionalität. Zum Sichern und Wiederherstellen Ihrer ONTAP Daten ist ein Konsolenagent erforderlich.

Erstellen oder Wechseln von Konsolenagenten

Wenn Sie Daten auf ONTAP S3 sichern, muss ein Konsolenagent bei Ihnen vor Ort oder in der Cloud verfügbar sein. Sie müssen entweder einen neuen Konsolenagenten installieren oder sicherstellen, dass sich der aktuell ausgewählte Konsolenagent an einem dieser Speicherorte befindet. Der lokale Konsolenagent kann an einem Standort mit oder ohne Internetzugang installiert werden.

- "Erfahren Sie mehr über Konsolenagenten"
- "Installieren Sie den Konsolenagenten in Ihrer Cloudumgebung"
- "Installieren des Konsolenagenten auf einem Linux-Host mit Internetzugang"
- "Installieren des Konsolenagenten auf einem Linux-Host ohne Internetzugang"
- "Wechseln zwischen Konsolenagenten"

Netzwerkanforderungen für den Konsolenagenten vorbereiten

Stellen Sie sicher, dass das Netzwerk, in dem der Konsolenagent installiert ist, die folgenden Verbindungen ermöglicht:

- Eine HTTPS-Verbindung über Port 443 zum ONTAP S3-Server
- Eine HTTPS-Verbindung über Port 443 zu Ihrem Quell ONTAP Cluster-Management-LIF
- Eine ausgehende Internetverbindung über Port 443 zu NetApp Backup and Recovery (nicht erforderlich, wenn der Konsolenagent an einem „dunklen“ Standort installiert ist)

Überlegungen zum privaten Modus (Dark Site)

Die NetApp Backup and Recovery Funktionalität ist in den Konsolenagenten integriert. Wenn es im privaten Modus installiert ist, müssen Sie die Konsolenagent-Software regelmäßig aktualisieren, um Zugriff auf neue Funktionen zu erhalten. Überprüfen Sie die"NetApp Backup and Recovery – Neuigkeiten" um die neuen Funktionen in jeder Version von NetApp Backup and Recovery anzuzeigen. Wenn Sie die neuen Funktionen nutzen möchten, folgen Sie den Schritten zum "Aktualisieren Sie die Konsolenagentsoftware" .

Wenn Sie NetApp Backup and Recovery in einer Standard-SaaS-Umgebung verwenden, werden die Konfigurationsdaten von NetApp Backup and Recovery in der Cloud gesichert. Wenn Sie NetApp Backup and Recovery an einem Standort ohne Internetzugang verwenden, werden die Konfigurationsdaten von NetApp Backup and Recovery im ONTAP S3-Bucket gesichert, in dem Ihre Backups gespeichert werden.

Überprüfen der Lizenzanforderungen

Bevor Sie NetApp Backup and Recovery für Ihren Cluster aktivieren können, müssen Sie eine NetApp Backup and Recovery BYOL-Lizenz von NetApp erwerben und aktivieren. Die Lizenz gilt für die Datensicherung und -wiederherstellung im Objektspeicher – für die Erstellung von Snapshots oder replizierten Volumes ist keine Lizenz erforderlich. Diese Lizenz gilt für das Konto und kann systemübergreifend verwendet werden.

Sie benötigen die Seriennummer von NetApp , die Ihnen die Nutzung des Dienstes für die Dauer und Kapazität der Lizenz ermöglicht. "Erfahren Sie, wie Sie Ihre BYOL-Lizenzen verwalten".

Die PAYGO-Lizenzierung wird beim Sichern von Dateien auf ONTAP S3 nicht unterstützt.

Bereiten Sie Ihre ONTAP -Cluster vor

Bereiten Sie Ihr lokales ONTAP -Quellsystem und alle sekundären lokalen ONTAP oder Cloud Volumes ONTAP Systeme vor.

Die Vorbereitung Ihrer ONTAP Cluster umfasst die folgenden Schritte:

- Entdecken Sie Ihre ONTAP -Systeme in der NetApp Console
- Überprüfen der ONTAP Systemanforderungen
- Überprüfen Sie die ONTAP Netzwerkanforderungen für die Datensicherung im Objektspeicher
- Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replikation von Volumes

Entdecken Sie Ihre ONTAP -Systeme in der NetApp Console

Sowohl Ihr lokales ONTAP Quellsystem als auch alle sekundären lokalen ONTAP oder Cloud Volumes ONTAP -Systeme müssen auf der Seite **Systeme** der NetApp Console verfügbar sein.

Sie müssen die IP-Adresse der Clusterverwaltung und das Kennwort für das Administratorbenutzerkonto kennen, um den Cluster hinzuzufügen. "Erfahren Sie, wie Sie einen Cluster erkennen".

Überprüfen der ONTAP Systemanforderungen

Stellen Sie sicher, dass Ihr ONTAP -System die folgenden Anforderungen erfüllt:

- Mindestens ONTAP 9.8; ONTAP 9.8P13 und höher wird empfohlen.
- Eine SnapMirror -Lizenz (im Premium-Paket oder Datenschutz-Paket enthalten).

  Hinweis: Das „Hybrid Cloud Bundle“ ist bei der Verwendung von NetApp Backup and Recovery nicht erforderlich.

  Erfahren Sie, wie Sie "Verwalten Sie Ihre Cluster-Lizenzen" .
- Uhrzeit und Zeitzone sind richtig eingestellt. Erfahren Sie, wie Sie "Konfigurieren Sie Ihre Clusterzeit" .
- Wenn Sie Daten replizieren, überprüfen Sie, ob auf den Quell- und Zielsystemen kompatible ONTAP Versionen ausgeführt werden.

  "Kompatible ONTAP -Versionen für SnapMirror -Beziehungen anzeigen".

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Datensicherung im Objektspeicher

Sie müssen sicherstellen, dass die folgenden Anforderungen auf dem System erfüllt sind, das eine Verbindung zum Objektspeicher herstellt.

- Wenn Sie eine Fan-Out-Backup-Architektur verwenden, müssen die Einstellungen auf dem *primären* Speichersystem konfiguriert werden.
- Wenn Sie eine kaskadierte Sicherungsarchitektur verwenden, müssen die Einstellungen auf dem *sekundären* Speichersystem konfiguriert werden.

  "Erfahren Sie mehr über die Arten der Backup-Architektur".

Die folgenden ONTAP Cluster-Netzwerkanforderungen sind erforderlich:

- Der ONTAP Cluster initiiert für Sicherungs- und Wiederherstellungsvorgänge eine HTTPS-Verbindung über einen benutzerdefinierten Port vom Intercluster-LIF zum ONTAP S3-Server. Der Port kann während der Sicherungseinrichtung konfiguriert werden.

  ONTAP liest und schreibt Daten in den und aus dem Objektspeicher. Der Objektspeicher wird nie initiiert, er reagiert nur.

- ONTAP erfordert eine eingehende Verbindung vom Konsolenagenten zum Cluster-Management-LIF.
- Auf jedem ONTAP Knoten, der die zu sichernden Volumes hostet, ist ein Intercluster-LIF erforderlich. Das LIF muss mit dem *IPspace* verknüpft sein, den ONTAP für die Verbindung mit dem Objektspeicher verwenden soll. "Erfahren Sie mehr über IPspaces" .

  Wenn Sie NetApp Backup and Recovery einrichten, werden Sie nach dem zu verwendenden IPspace gefragt. Sie sollten den IPspace auswählen, mit dem jedes LIF verknüpft ist. Dies kann der „Standard“-IP-Bereich oder ein benutzerdefinierter IP-Bereich sein, den Sie erstellt haben.

- Die Intercluster-LIFs der Knoten können auf den Objektspeicher zugreifen (nicht erforderlich, wenn der Konsolenagent an einem „dunklen“ Standort installiert ist).
- Für die Speicher-VM, auf der sich die Volumes befinden, wurden DNS-Server konfiguriert. Erfahren Sie, wie Sie "Konfigurieren Sie DNS-Dienste für die SVM" .
- Wenn Sie einen anderen IP-Bereich als den Standard-IP-Bereich verwenden, müssen Sie möglicherweise eine statische Route erstellen, um Zugriff auf den Objektspeicher zu erhalten.
- Aktualisieren Sie bei Bedarf die Firewall-Regeln, um Verbindungen des NetApp Backup and Recovery -Dienstes von ONTAP zum Objektspeicher über den von Ihnen angegebenen Port (normalerweise Port 443) und Namensauflösungsdatenverkehr von der Speicher-VM zum DNS-Server über Port 53 (TCP/UDP) zuzulassen.

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replikation von Volumes

Wenn Sie mit NetApp Backup and Recovery replizierte Volumes auf einem sekundären ONTAP System erstellen möchten, stellen Sie sicher, dass die Quell- und Zielsysteme die folgenden Netzwerkanforderungen erfüllen.

On-Premises ONTAP Netzwerkanforderungen

- Wenn sich der Cluster vor Ort befindet, sollten Sie über eine Verbindung von Ihrem Unternehmensnetzwerk zu Ihrem virtuellen Netzwerk beim Cloud-Anbieter verfügen. Dies ist normalerweise eine VPN-Verbindung.
- ONTAP -Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Clusteranforderungen erfüllen.

  Da Sie auf Cloud Volumes ONTAP oder lokale Systeme replizieren können, überprüfen Sie die Peering-Anforderungen für lokale ONTAP -Systeme. "Voraussetzungen für Cluster-Peering in der ONTAP Dokumentation anzeigen" .

Netzwerkanforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen Regeln für eingehenden und ausgehenden Datenverkehr enthalten, insbesondere Regeln für ICMP und die Ports 11104 und 11105. Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.

Bereiten Sie ONTAP S3 als Ihr Backup-Ziel vor

Sie müssen einen Simple Storage Service (S3)-Objektspeicherserver im ONTAP Cluster aktivieren, den Sie für Objektspeichersicherungen verwenden möchten. Siehe die "ONTAP S3-Dokumentation" für Details.

Hinweis: Sie können diesen Cluster zur Konsolenseite **Systeme** hinzufügen, er wird jedoch nicht als S3-Objektspeicherserver identifiziert und Sie können kein Quellsystem per Drag & Drop auf dieses S3-System ziehen, um die Aktivierung der Sicherung zu starten.

Dieses ONTAP -System muss die folgenden Anforderungen erfüllen.

Unterstützte ONTAP-Versionen

Für lokale ONTAP -Systeme ist ONTAP 9.8 und höher erforderlich. Für Cloud Volumes ONTAP -Systeme ist ONTAP 9.9.1 und höher erforderlich.

S3-Anmeldeinformationen

Sie müssen einen S3-Benutzer erstellt haben, um den Zugriff auf Ihren ONTAP S3-Speicher zu steuern. "Weitere Informationen finden Sie in der ONTAP S3-Dokumentation." .

Wenn Sie die Sicherung auf ONTAP S3 einrichten, fordert Sie der Sicherungsassistent zur Eingabe eines S3-Zugriffsschlüssels und eines geheimen Schlüssels für ein Benutzerkonto auf. Das Benutzerkonto ermöglicht NetApp Backup and Recovery die Authentifizierung und den Zugriff auf die ONTAP S3-Buckets, die zum Speichern von Backups verwendet werden. Die Schlüssel werden benötigt, damit ONTAP S3 weiß, wer die Anfrage stellt.

Diese Zugriffsschlüssel müssen einem Benutzer zugeordnet sein, der über die folgenden Berechtigungen verfügt:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket",
"s3:GetBucketLocation"
```

Aktivieren Sie Backups auf Ihren ONTAP -Volumes

Aktivieren Sie Backups jederzeit direkt von Ihrem lokalen System aus.

Ein Assistent führt Sie durch die folgenden Hauptschritte:

- Wählen Sie die Volumes aus, die Sie sichern möchten
- Definieren Sie die Sicherungsstrategie und -richtlinien
- Überprüfen Sie Ihre Auswahl

Sie können auchAPI-Befehle anzeigen im Überprüfungsschritt, damit Sie den Code kopieren können, um die Sicherungsaktivierung für zukünftige Systeme zu automatisieren.

Starten des Assistenten

Schritte

1. Greifen Sie auf eine der folgenden Arten auf den Assistenten „Sicherung und Wiederherstellung aktivieren“ zu:

   - Wählen Sie auf der Konsolenseite **Systeme** das System aus und wählen Sie im rechten Bereich neben „Sicherung und Wiederherstellung“ die Option „Aktivieren > Sicherungsvolumes“ aus.
   - Wählen Sie in der Leiste „Sichern und Wiederherstellen“ **Volumes** aus. Wählen Sie auf der Registerkarte „Volumes“ die Option **Aktionen (…)** und wählen Sie **Sicherung aktivieren** für ein einzelnes Volume (für das die Replikation oder Sicherung in den Objektspeicher noch nicht aktiviert ist).

   Auf der Einführungsseite des Assistenten werden die Schutzoptionen angezeigt, darunter lokale Snapshots, Replikationen und Backups. Wenn Sie in diesem Schritt die zweite Option gewählt haben, wird die Seite „Sicherungsstrategie definieren“ mit einem ausgewählten Volume angezeigt.

2. Fahren Sie mit den folgenden Optionen fort:

   - Wenn Sie bereits über einen Konsolenagenten verfügen, sind Sie startklar. Wählen Sie einfach **Weiter**.
   - Wenn Sie keinen Konsolenagenten haben, wird die Option **Konsolenagenten hinzufügen** angezeigt. SieheVorbereiten Ihres Konsolenagenten .

Wählen Sie die Volumes aus, die Sie sichern möchten

Wählen Sie die Volumes aus, die Sie schützen möchten. Ein geschütztes Volume ist ein Volume, das über eine oder mehrere der folgenden Optionen verfügt: Snapshot-Richtlinie, Replikationsrichtlinie, Backup-to-Object-Richtlinie.

Sie können FlexVol oder FlexGroup -Volumes schützen. Sie können jedoch keine Mischung dieser Volumes auswählen, wenn Sie die Sicherung für ein System aktivieren. Erfahren Sie, wie Sie"Aktivieren Sie die Sicherung für zusätzliche Volumes im System" (FlexVol oder FlexGroup), nachdem Sie die Sicherung für die ersten Volumes konfiguriert haben.

- Sie können eine Sicherung jeweils nur auf einem einzigen FlexGroup -Volume aktivieren.
- Die von Ihnen ausgewählten Volumes müssen über dieselbe SnapLock Einstellung verfügen. Auf allen Volumes muss SnapLock Enterprise aktiviert oder SnapLock sein.

Schritte

Beachten Sie: Wenn auf die von Ihnen ausgewählten Volumes bereits Snapshot- oder Replikationsrichtlinien angewendet wurden, werden diese vorhandenen Richtlinien durch die später ausgewählten Richtlinien überschrieben.

1. Wählen Sie auf der Seite „Volumes auswählen“ das oder die Volumes aus, die Sie schützen möchten.

   - Filtern Sie die Zeilen optional, um nur Datenträger mit bestimmten Datenträgertypen, Stilen usw. anzuzeigen und so die Auswahl zu vereinfachen.
   - Nachdem Sie das erste Volume ausgewählt haben, können Sie alle FlexVol Volumes auswählen (FlexGroup Volumes können jeweils nur einzeln ausgewählt werden). Um alle vorhandenen FlexVol Volumes zu sichern, markieren Sie zuerst ein Volume und aktivieren Sie dann das Kontrollkästchen in der Titelzeile.
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume.

2. Wählen Sie **Weiter**.

Definieren Sie die Sicherungsstrategie

Zum Definieren der Sicherungsstrategie müssen die folgenden Optionen konfiguriert werden:

- Schutzoptionen: Ob Sie eine oder alle der Backup-Optionen implementieren möchten: lokale Snapshots, Replikation und Backup auf Objektspeicher
- Architektur: Ob Sie eine Fan-Out- oder eine kaskadierende Backup-Architektur verwenden möchten
- Lokale Snapshot-Richtlinie
- Replikationsziel und -richtlinie
- Informationen zur Sicherung in Objektspeichern (Anbieter, Verschlüsselung, Netzwerk, Sicherungsrichtlinie und Exportoptionen).

Schritte

1. Wählen Sie auf der Seite „Sicherungsstrategie definieren“ eine oder alle der folgenden Optionen aus. Alle drei sind standardmäßig ausgewählt:
   - **Lokale Snapshots**: Erstellt lokale Snapshots.
   - **Replikation**: Erstellt replizierte Volumes auf einem anderen ONTAP Speichersystem.
   - **Backup**: Sichert Volumes in einem Bucket auf einem für S3 konfigurierten ONTAP System.
2. **Architektur**: Wenn Sie sowohl Replikation als auch Sicherung gewählt haben, wählen Sie einen der folgenden Informationsflüsse:
   - **Kaskadierung**: Sicherungsdaten fließen vom primären zum sekundären System und dann vom sekundären zum Objektspeicher.
   - **Fan-Out**: Sicherungsdaten fließen vom primären zum sekundären System *und* vom primären zum Objektspeicher.

     Weitere Informationen zu diesen Architekturen finden Sie unter"Planen Sie Ihren Schutzweg" .
3. **Lokaler Snapshot**: Wählen Sie eine vorhandene Snapshot-Richtlinie oder erstellen Sie eine neue.

   Wenn Sie vor der Aktivierung des Snapshots eine benutzerdefinierte Richtlinie erstellen möchten, können Sie den System Manager oder die ONTAP CLI verwenden. `snapmirror policy create` Befehl. Siehe .

   Informationen zum Erstellen einer benutzerdefinierten Richtlinie mithilfe von Backup und Recovery finden Sie unter"Erstellen einer Richtlinie" .

   Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:
   - Geben Sie den Namen der Richtlinie ein.
   - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
   - Wählen Sie **Erstellen**.
4. **Replikation**: Wenn Sie **Replikation** ausgewählt haben, legen Sie die folgenden Optionen fest:
   - **Replikationsziel**: Wählen Sie das Zielsystem und die SVM aus. Wählen Sie optional das Zielaggregat (oder die Aggregate für FlexGroup -Volumes) und ein Präfix oder Suffix aus, das dem Namen des replizierten Volumes hinzugefügt wird.
   - **Replikationsrichtlinie**: Wählen Sie eine vorhandene Replikationsrichtlinie aus oder erstellen Sie eine neue.

Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:

- Geben Sie den Namen der Richtlinie ein.
- Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
- Wählen Sie **Erstellen**.

5. **Sichern auf Objekt**: Wenn Sie **Sichern** ausgewählt haben, legen Sie die folgenden Optionen fest:
   - **Anbieter**: Wählen Sie * ONTAP S3*.
   - **Anbietereinstellungen**: Geben Sie die FQDN-Details, den Port sowie den Zugriffsschlüssel und den geheimen Schlüssel des S3-Servers ein.

     Der Zugriffsschlüssel und der geheime Schlüssel sind für den von Ihnen erstellten Benutzer, um dem ONTAP Cluster Zugriff auf den S3-Bucket zu gewähren.

   - **Netzwerk**: Wählen Sie den IP-Bereich im Quell- ONTAP Cluster aus, in dem sich die Volumes befinden, die Sie sichern möchten. Die Intercluster-LIFs für diesen IPspace müssen über ausgehenden Internetzugang verfügen (nicht erforderlich, wenn der Konsolenagent an einem „dunklen“ Standort installiert ist).

     Durch die Auswahl des richtigen IPspace wird sichergestellt, dass NetApp Backup and Recovery eine Verbindung von ONTAP zu Ihrem ONTAP S3-Objektspeicher herstellen kann.

   - **Sicherungsrichtlinie**: Wählen Sie eine vorhandene Sicherungsrichtlinie aus oder erstellen Sie eine neue.

     Sie können eine Richtlinie mit System Manager oder der ONTAP CLI erstellen. So erstellen Sie eine benutzerdefinierte Richtlinie mit der ONTAP CLI `snapmirror policy create` Befehl, siehe .

     Informationen zum Erstellen einer benutzerdefinierten Richtlinie mithilfe von Backup und Recovery finden Sie unter"Erstellen einer Richtlinie" .

     Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:

     - Geben Sie den Namen der Richtlinie ein.
     - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
     - Legen Sie für Backup-to-Object-Richtlinien die Einstellungen „DataLock“ und „Ransomware Resilience“ fest. Weitere Informationen zu DataLock und Ransomware Resilience finden Sie unter"Einstellungen der Backup-to-Object-Richtlinie" .
     - Wählen Sie **Erstellen**.

   - **Vorhandene Snapshots als Sicherungsdateien in den Objektspeicher exportieren**: Wenn es lokale Snapshots für Volumes in diesem System gibt, die mit der von Ihnen soeben ausgewählten Sicherungszeitplanbezeichnung (z. B. täglich, wöchentlich usw.) übereinstimmen, wird diese zusätzliche Aufforderung angezeigt. Aktivieren Sie dieses Kontrollkästchen, um alle historischen Snapshots als Sicherungsdateien in den Objektspeicher zu kopieren und so den umfassendsten Schutz für Ihre Volumes zu gewährleisten.
6. Wählen Sie **Weiter**.

Überprüfen Sie Ihre Auswahl

Dies ist die Gelegenheit, Ihre Auswahl zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

Schritte

1. Überprüfen Sie Ihre Auswahl auf der Überprüfungsseite.
2. Aktivieren Sie optional das Kontrollkästchen, um **die Snapshot-Richtlinienbezeichnungen automatisch mit den Replikations- und Sicherungsrichtlinienbezeichnungen zu synchronisieren**. Dadurch werden Snapshots mit einer Bezeichnung erstellt, die mit den Bezeichnungen in den Replikations- und Sicherungsrichtlinien übereinstimmt. Wenn die Richtlinien nicht übereinstimmen, werden keine Sicherungen erstellt.
3. Wählen Sie **Backup aktivieren**.

Ergebnis

NetApp Backup and Recovery beginnt mit der Durchführung der ersten Sicherungen Ihrer Volumes. Die Basisübertragung des replizierten Volumes und der Sicherungsdatei umfasst eine vollständige Kopie der Quelldaten. Nachfolgende Übertragungen enthalten differentielle Kopien der im Primärspeicher enthaltenen Daten, die in Snapshots gespeichert sind.

Im Zielcluster wird ein repliziertes Volume erstellt, das mit dem primären Speichervolume synchronisiert wird.

Im durch den von Ihnen eingegebenen S3-Zugriffsschlüssel und geheimen Schlüssel angegebenen Dienstkonto wird ein S3-Bucket erstellt und die Sicherungsdateien werden dort gespeichert.

Das Volume-Backup-Dashboard wird angezeigt, damit Sie den Status der Backups überwachen können.

Sie können den Status von Sicherungs- und Wiederherstellungsaufträgen auch mithilfe der"Seite „Jobüberwachung“" .

API-Befehle anzeigen

Möglicherweise möchten Sie die im Assistenten „Sicherung und Wiederherstellung aktivieren“ verwendeten API-Befehle anzeigen und optional kopieren. Möglicherweise möchten Sie dies tun, um die Sicherungsaktivierung in zukünftigen Systemen zu automatisieren.

Schritte

1. Wählen Sie im Assistenten „Sicherung und Wiederherstellung aktivieren“ die Option „API-Anforderung anzeigen“ aus.
2. Um die Befehle in die Zwischenablage zu kopieren, wählen Sie das Symbol **Kopieren**.

Sichern Sie lokale ONTAP Daten mit NetApp Backup and Recovery auf StorageGRID

Führen Sie einige Schritte in NetApp Backup and Recovery aus, um mit der Sicherung von Volume-Daten von Ihren lokalen primären ONTAP Systemen auf ein sekundäres Speichersystem und auf Objektspeicher in Ihren NetApp StorageGRID Systemen zu beginnen.

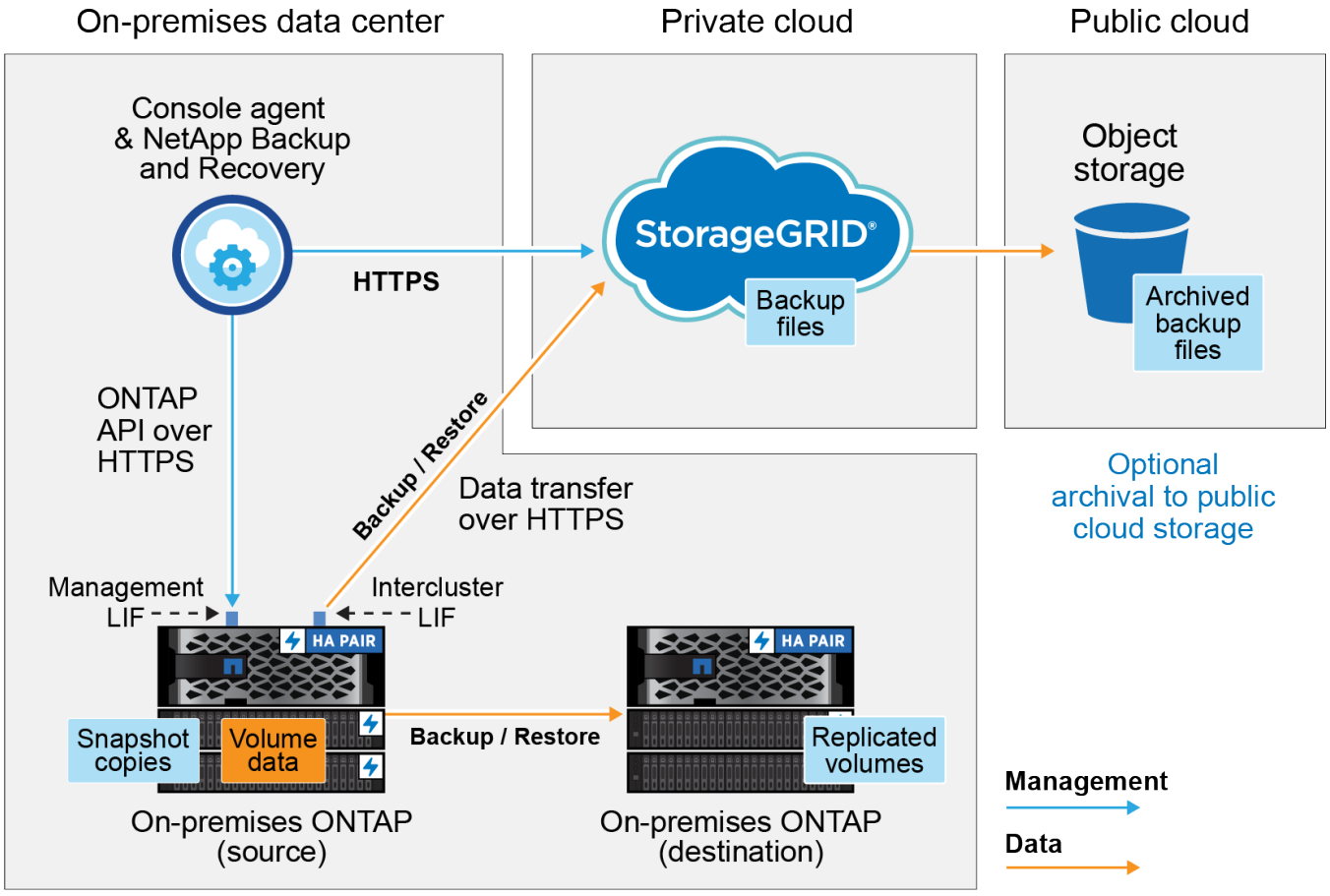
Zu den „On-Premises ONTAP -Systemen“ gehören FAS, AFF und ONTAP Select Systeme.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

Identifizieren Sie die Verbindungsmethode

Das folgende Bild zeigt jede Komponente beim Sichern eines lokalen ONTAP Systems auf StorageGRID und die Verbindungen, die Sie zwischen ihnen vorbereiten müssen.

Optional können Sie eine Verbindung zu einem sekundären ONTAP -System am selben Standort vor Ort herstellen, um Volumes zu replizieren.



Wenn der Konsolenagent und das lokale ONTAP -System an einem lokalen Standort ohne Internetzugang (einem „Dark Site“) installiert sind, muss sich das StorageGRID -System im selben lokalen Rechenzentrum befinden. Die Archivierung älterer Sicherungsdateien in der öffentlichen Cloud wird in Dark-Site-Konfigurationen nicht unterstützt.

Vorbereiten Ihres Konsolenagenten

Der Konsolenagent ist die Hauptsoftware für die Konsolenfunktionalität. Zum Sichern und Wiederherstellen Ihrer ONTAP Daten ist ein Konsolenagent erforderlich.

Erstellen oder Wechseln von Konsolenagenten

Wenn Sie Daten in StorageGRID sichern, muss bei Ihnen vor Ort ein Konsolenagent verfügbar sein. Sie müssen entweder einen neuen Konsolen-Agenten installieren oder sicherstellen, dass der aktuell ausgewählte

Konsolen-Agent vor Ort vorhanden ist. Der Konsolenagent kann an einem Standort mit oder ohne Internetzugang installiert werden.

- "Erfahren Sie mehr über Konsolenagenten"
- "Installieren des Konsolenagenten auf einem Linux-Host mit Internetzugang"
- "Installieren des Konsolenagenten auf einem Linux-Host ohne Internetzugang"
- "Wechseln zwischen Konsolenagenten"

Netzwerkanforderungen für den Konsolenagenten vorbereiten

Stellen Sie sicher, dass das Netzwerk, in dem der Konsolenagent installiert ist, die folgenden Verbindungen ermöglicht:

- Eine HTTPS-Verbindung über Port 443 zum StorageGRID Gateway Node
- Eine HTTPS-Verbindung über Port 443 zu Ihrem ONTAP Cluster-Management-LIF
- Eine ausgehende Internetverbindung über Port 443 zu NetApp Backup and Recovery (nicht erforderlich, wenn der Konsolenagent an einem „dunklen“ Standort installiert ist)

Überlegungen zum privaten Modus (Dark Site)

- Die NetApp Backup and Recovery Funktionalität ist in den Konsolenagenten integriert. Wenn es im privaten Modus installiert ist, müssen Sie die Konsolenagent-Software regelmäßig aktualisieren, um Zugriff auf neue Funktionen zu erhalten. Überprüfen Sie die"NetApp Backup and Recovery – Neuigkeiten" um die neuen Funktionen in jeder Version von NetApp Backup and Recovery anzuzeigen. Wenn Sie die neuen Funktionen nutzen möchten, folgen Sie den Schritten zum "Aktualisieren Sie die Konsolenagentsoftware" .

  Die neue Version von NetApp Backup and Recovery , die neben der Erstellung von Backups auf Objektspeicher auch die Möglichkeit bietet, Snapshots und replizierte Volumes zu planen und zu erstellen, erfordert die Verwendung der Version 3.9.31 oder höher des Console-Agenten. Es wird daher empfohlen, dass Sie sich diese neueste Version besorgen, um alle Ihre Backups zu verwalten.

- Wenn Sie NetApp Backup and Recovery in einer SaaS-Umgebung verwenden, werden die NetApp Backup and Recovery -Konfigurationsdaten in der Cloud gesichert. Wenn Sie NetApp Backup and Recovery an einem Standort ohne Internetzugang verwenden, werden die Konfigurationsdaten von NetApp Backup and Recovery im StorageGRID Bucket gesichert, in dem Ihre Backups gespeichert werden.

Überprüfen der Lizenzanforderungen

Bevor Sie NetApp Backup and Recovery für Ihren Cluster aktivieren können, müssen Sie eine NetApp Backup and Recovery BYOL-Lizenz von NetApp erwerben und aktivieren. Diese Lizenz gilt für das Konto und kann systemübergreifend verwendet werden.

Sie benötigen die Seriennummer von NetApp , die Ihnen die Nutzung des Dienstes für die Dauer und Kapazität der Lizenz ermöglicht. "Erfahren Sie, wie Sie Ihre BYOL-Lizenzen verwalten".

Die PAYGO-Lizenzierung wird beim Sichern von Dateien auf StorageGRID nicht unterstützt.

Bereiten Sie Ihre ONTAP -Cluster vor

Bereiten Sie Ihr lokales ONTAP -Quellsystem und alle sekundären lokalen ONTAP oder Cloud Volumes ONTAP Systeme vor.

Die Vorbereitung Ihrer ONTAP Cluster umfasst die folgenden Schritte:

- Entdecken Sie Ihre ONTAP -Systeme in der NetApp Console
- Überprüfen der ONTAP Systemanforderungen
- Überprüfen Sie die ONTAP Netzwerkanforderungen für die Datensicherung im Objektspeicher
- Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replikation von Volumes

Entdecken Sie Ihre ONTAP -Systeme in der NetApp Console

Sowohl Ihr lokales ONTAP Quellsystem als auch alle sekundären lokalen ONTAP oder Cloud Volumes ONTAP -Systeme müssen auf der Seite **Systeme** der NetApp Console verfügbar sein.

Sie müssen die IP-Adresse der Clusterverwaltung und das Kennwort für das Administratorbenutzerkonto kennen, um den Cluster hinzuzufügen. "Erfahren Sie, wie Sie einen Cluster erkennen".

Überprüfen der ONTAP Systemanforderungen

Stellen Sie sicher, dass Ihr ONTAP -System die folgenden Anforderungen erfüllt:

- Mindestens ONTAP 9.8; ONTAP 9.8P13 und höher wird empfohlen.
- Eine SnapMirror -Lizenz (im Premium-Paket oder Datenschutz-Paket enthalten).

  Hinweis: Das „Hybrid Cloud Bundle“ ist bei der Verwendung von NetApp Backup and Recovery nicht erforderlich.

  Erfahren Sie, wie Sie "Verwalten Sie Ihre Cluster-Lizenzen" .
- Uhrzeit und Zeitzone sind richtig eingestellt. Erfahren Sie, wie Sie "Konfigurieren Sie Ihre Clusterzeit" .
- Wenn Sie Daten replizieren, überprüfen Sie, ob auf den Quell- und Zielsystemen kompatible ONTAP Versionen ausgeführt werden.

  "Kompatible ONTAP -Versionen für SnapMirror -Beziehungen anzeigen".

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Datensicherung im Objektspeicher

Sie müssen die folgenden Anforderungen auf dem System konfigurieren, das eine Verbindung zum Objektspeicher herstellt.

- Wenn Sie eine Fan-Out-Backup-Architektur verwenden, müssen die folgenden Einstellungen auf dem *primären* Speichersystem konfiguriert werden.
- Wenn Sie eine kaskadierte Sicherungsarchitektur verwenden, müssen die folgenden Einstellungen auf dem *sekundären* Speichersystem konfiguriert werden.

Die folgenden ONTAP Cluster-Netzwerkanforderungen sind erforderlich:

- Der ONTAP Cluster initiiert für Sicherungs- und Wiederherstellungsvorgänge eine HTTPS-Verbindung über einen benutzerdefinierten Port vom Intercluster-LIF zum StorageGRID -Gateway-Knoten. Der Port kann während der Sicherungseinrichtung konfiguriert werden.

  ONTAP liest und schreibt Daten in den und aus dem Objektspeicher. Der Objektspeicher wird nie initiiert, er reagiert nur.

- ONTAP erfordert eine eingehende Verbindung vom Konsolenagenten zum Cluster-Management-LIF. Der Konsolenagent muss sich in Ihren Räumlichkeiten befinden.
- Auf jedem ONTAP Knoten, der die zu sichernden Volumes hostet, ist ein Intercluster-LIF erforderlich. Das LIF muss mit dem *IPspace* verknüpft sein, den ONTAP für die Verbindung mit dem Objektspeicher verwenden soll. "Erfahren Sie mehr über IPspaces" .

  Wenn Sie NetApp Backup and Recovery einrichten, werden Sie nach dem zu verwendenden IPspace gefragt. Sie sollten den IPspace auswählen, mit dem jedes LIF verknüpft ist. Dies kann der „Standard“-IP-Bereich oder ein benutzerdefinierter IP-Bereich sein, den Sie erstellt haben.
- Die Intercluster-LIFs der Knoten können auf den Objektspeicher zugreifen (nicht erforderlich, wenn der Konsolenagent an einem „dunklen“ Standort installiert ist).
- Für die Speicher-VM, auf der sich die Volumes befinden, wurden DNS-Server konfiguriert. Erfahren Sie, wie Sie "Konfigurieren Sie DNS-Dienste für die SVM" .
- Wenn Sie einen anderen IP-Bereich als den Standard verwenden, müssen Sie möglicherweise eine statische Route erstellen, um Zugriff auf den Objektspeicher zu erhalten.
- Aktualisieren Sie bei Bedarf die Firewall-Regeln, um Verbindungen des NetApp Backup and Recovery -Dienstes von ONTAP zum Objektspeicher über den von Ihnen angegebenen Port (normalerweise Port 443) und Namensauflösungsdatenverkehr von der Speicher-VM zum DNS-Server über Port 53 (TCP/UDP) zuzulassen.

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replikation von Volumes

Wenn Sie mit NetApp Backup and Recovery replizierte Volumes auf einem sekundären ONTAP System erstellen möchten, stellen Sie sicher, dass die Quell- und Zielsysteme die folgenden Netzwerkanforderungen erfüllen.

On-Premises ONTAP Netzwerkanforderungen

- Wenn sich der Cluster vor Ort befindet, sollten Sie über eine Verbindung von Ihrem Unternehmensnetzwerk zu Ihrem virtuellen Netzwerk beim Cloud-Anbieter verfügen. Dies ist normalerweise eine VPN-Verbindung.
- ONTAP -Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Clusteranforderungen erfüllen.

  Da Sie auf Cloud Volumes ONTAP oder lokale Systeme replizieren können, überprüfen Sie die Peering-Anforderungen für lokale ONTAP -Systeme. "Voraussetzungen für Cluster-Peering in der ONTAP Dokumentation anzeigen" .

Netzwerkanforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen Regeln für eingehenden und ausgehenden Datenverkehr enthalten, insbesondere Regeln für ICMP und die Ports 11104 und 11105. Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.

Bereiten Sie StorageGRID als Ihr Sicherungsziel vor

StorageGRID muss die folgenden Anforderungen erfüllen. Siehe die "StorageGRID -Dokumentation" für weitere Informationen.

Weitere Informationen zu den DataLock- und Ransomware-Resilienzanforderungen für StorageGRID finden Sie unter"Optionen für die Backup-to-Object-Richtlinie" .

Unterstützte StorageGRID Versionen

StorageGRID 10.3 und höher wird unterstützt.

Um DataLock & Ransomware Resilience für Ihre Backups zu verwenden, müssen Ihre StorageGRID -Systeme in der Version 11.6.0.3 oder höher ausgeführt werden.

Um ältere Backups in den Cloud-Archivspeicher zu verschieben, müssen Ihre StorageGRID -Systeme mit Version 11.3 oder höher laufen. Darüber hinaus müssen Ihre StorageGRID -Systeme auf der Konsolenseite **Systeme** erkannt werden.

Zur Nutzung des Archivspeichers ist ein IP-Zugriff auf den Admin-Knoten erforderlich.

Gateway-IP-Zugriff ist immer erforderlich.

S3-Anmeldeinformationen

Sie müssen ein S3-Mandantenkonto erstellt haben, um den Zugriff auf Ihren StorageGRID Speicher zu steuern. "Weitere Informationen finden Sie in der StorageGRID -Dokumentation." .

Wenn Sie die Sicherung auf StorageGRID einrichten, fordert Sie der Sicherungsassistent zur Eingabe eines S3-Zugriffsschlüssels und eines geheimen Schlüssels für ein Mandantenkonto auf. Das Mandantenkonto ermöglicht NetApp Backup and Recovery die Authentifizierung und den Zugriff auf die StorageGRID -Buckets, die zum Speichern von Backups verwendet werden. Die Schlüssel werden benötigt, damit StorageGRID weiß, wer die Anfrage stellt.

Diese Zugriffsschlüssel müssen einem Benutzer zugeordnet sein, der über die folgenden Berechtigungen verfügt:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Objektversionierung

Sie dürfen die StorageGRID Objektversionierung im Objektspeicher-Bucket nicht manuell aktivieren.

Bereiten Sie die Archivierung älterer Sicherungsdateien im öffentlichen Cloud-Speicher vor

Durch die Auslagerung älterer Sicherungsdateien in einen Archivspeicher sparen Sie Geld, da für Sicherungen, die Sie möglicherweise nicht benötigen, eine weniger teure Speicherklasse verwendet wird. StorageGRID ist eine lokale (private Cloud-)Lösung, die keinen Archivspeicher bietet, Sie können jedoch ältere Sicherungsdateien in den öffentlichen Cloud-Archivspeicher verschieben. Bei dieser Verwendung werden Daten, die in den Cloud-Speicher verschoben oder aus dem Cloud-Speicher wiederhergestellt werden, zwischen StorageGRID und dem Cloud-Speicher übertragen – die Konsole ist an dieser Datenübertragung nicht beteiligt.

Mit der aktuellen Unterstützung können Sie Sicherungen im AWS-Speicher *S3 Glacier*/*S3 Glacier Deep Archive* oder *Azure Archive* archivieren.

- ONTAP Anforderungen*

- Ihr Cluster muss ONTAP 9.12.1 oder höher verwenden.
- StorageGRID Anforderungen*
- Ihr StorageGRID muss 11.4 oder höher verwenden.
- Ihr StorageGRID muss "in der Konsole erkannt und verfügbar" .

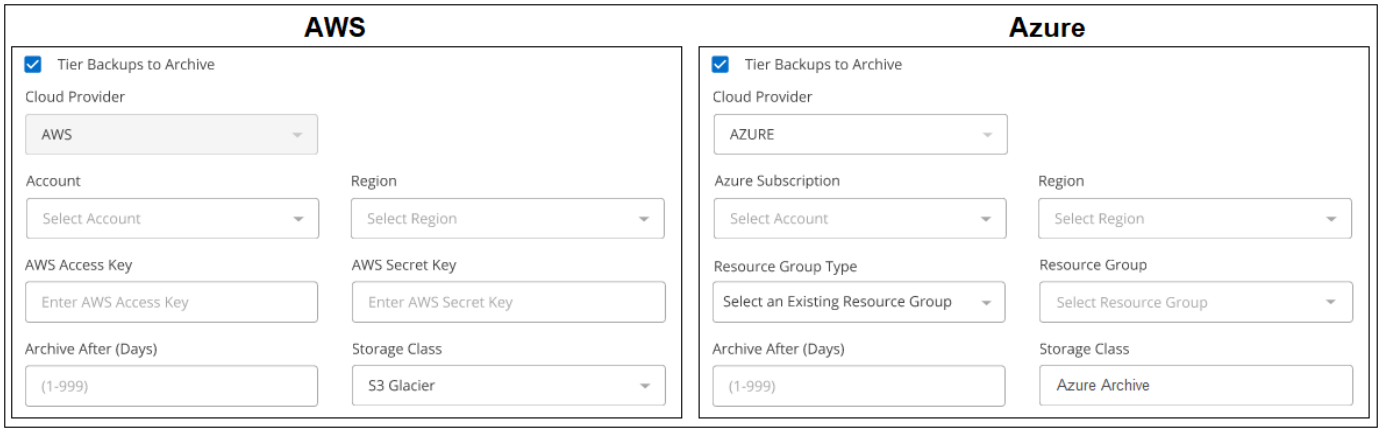
Anforderungen für Amazon S3

- Sie müssen sich für ein Amazon S3-Konto für den Speicherplatz anmelden, auf dem Ihre archivierten Backups gespeichert werden.
- Sie können wählen, ob Sie Backups auf AWS S3 Glacier oder S3 Glacier Deep Archive-Speicher stufen möchten. "Erfahren Sie mehr über AWS-Archivierungsebenen".
- StorageGRID sollte vollen Zugriff auf den Bucket haben(`s3:*`); wenn dies jedoch nicht möglich ist, muss die Bucket-Richtlinie StorageGRID die folgenden S3-Berechtigungen erteilen:
  - `s3:AbortMultipartUpload`
  - `s3:DeleteObject`
  - `s3:GetObject`
  - `s3:ListBucket`
  - `s3:ListBucketMultipartUploads`
  - `s3:ListMultipartUploadParts`
  - `s3:PutObject`
  - `s3:RestoreObject`

Azure Blob-Anforderungen

- Sie müssen sich für ein Azure-Abonnement für den Speicherplatz anmelden, auf dem Ihre archivierten Sicherungen gespeichert werden.
- Mit dem Aktivierungsassistenten können Sie eine vorhandene Ressourcengruppe zum Verwalten des Blob-Containers verwenden, in dem die Sicherungen gespeichert werden, oder Sie können eine neue Ressourcengruppe erstellen.

Wenn Sie die Archivierungseinstellungen für die Sicherungsrichtlinie für Ihren Cluster definieren, geben Sie die Anmeldeinformationen Ihres Cloud-Anbieters ein und wählen die Speicherklasse aus, die Sie verwenden möchten. NetApp Backup and Recovery erstellt den Cloud-Bucket, wenn Sie die Sicherung für den Cluster aktivieren. Die für die Archivspeicherung in AWS und Azure erforderlichen Informationen werden unten angezeigt.



Die von Ihnen ausgewählten Archivierungsrichtlinieneinstellungen generieren eine Richtlinie für das Information Lifecycle Management (ILM) in StorageGRID und fügen die Einstellungen als „Regeln“ hinzu.

- Wenn bereits eine aktive ILM-Richtlinie vorhanden ist, werden der ILM-Richtlinie neue Regeln hinzugefügt, um die Daten in die Archivebene zu verschieben.
- Wenn eine vorhandene ILM-Richtlinie den Status „Vorgeschlagen“ aufweist, ist die Erstellung und Aktivierung einer neuen ILM-Richtlinie nicht möglich. "Erfahren Sie mehr über die ILM-Richtlinien und -Regeln von StorageGRID" .

Aktivieren Sie Backups auf Ihren ONTAP -Volumes

Aktivieren Sie Backups jederzeit direkt von Ihrem lokalen System aus.

Ein Assistent führt Sie durch die folgenden Hauptschritte:

- die Sie sichern möchten
- Definieren Sie die Sicherungsstrategie
- Überprüfen Sie Ihre Auswahl

Sie können auchAPI-Befehle anzeigen im Überprüfungsschritt, damit Sie den Code kopieren können, um die Sicherungsaktivierung für zukünftige Systeme zu automatisieren.

Starten des Assistenten

Schritte

1. Greifen Sie auf eine der folgenden Arten auf den Assistenten „Sicherung und Wiederherstellung aktivieren“ zu:

   - Wählen Sie auf der Konsolenseite **Systeme** das System aus und wählen Sie im rechten Bereich neben „Sicherung und Wiederherstellung“ die Option „Aktivieren > Sicherungsvolumes“ aus.

     Wenn das Ziel für Ihre Backups als System auf der Konsolenseite **Systeme** vorhanden ist, können Sie den ONTAP Cluster auf den Objektspeicher ziehen.

   - Wählen Sie in der Leiste „Sichern und Wiederherstellen“ **Volumes** aus. Wählen Sie auf der Registerkarte „Volumes“ die Option **Aktionen (…)** und wählen Sie **Sicherung aktivieren** für ein einzelnes Volume (für das die Replikation oder Sicherung in den Objektspeicher noch nicht aktiviert ist).

   Auf der Einführungsseite des Assistenten werden die Schutzoptionen angezeigt, darunter lokale Snapshots, Replikation und Backups. Wenn Sie in diesem Schritt die zweite Option gewählt haben, wird

die Seite „Sicherungsstrategie definieren“ mit einem ausgewählten Volume angezeigt.

2. Fahren Sie mit den folgenden Optionen fort:
   - Wenn Sie bereits über einen Konsolenagenten verfügen, sind Sie startklar. Wählen Sie einfach **Weiter**.
   - Wenn Sie noch keinen Konsolenagenten haben, wird die Option **Konsolenagenten hinzufügen** angezeigt. SieheVorbereiten Ihres Konsolenagenten .

Wählen Sie die Volumes aus, die Sie sichern möchten

Wählen Sie die Volumes aus, die Sie schützen möchten. Ein geschütztes Volume verfügt über eine oder mehrere der folgenden Optionen: Snapshot-Richtlinie, Replikationsrichtlinie, Backup-to-Object-Richtlinie.

Sie können FlexVol oder FlexGroup -Volumes schützen. Sie können jedoch keine Mischung dieser Volumes auswählen, wenn Sie die Sicherung für ein System aktivieren. Erfahren Sie, wie Sie"Aktivieren Sie die Sicherung für zusätzliche Volumes im System" (FlexVol oder FlexGroup), nachdem Sie die Sicherung für die ersten Volumes konfiguriert haben.

- Sie können eine Sicherung jeweils nur auf einem einzigen FlexGroup -Volume aktivieren.
- Die von Ihnen ausgewählten Volumes müssen über dieselbe SnapLock Einstellung verfügen. Auf allen Volumes muss SnapLock Enterprise aktiviert oder SnapLock sein.

Schritte

Wenn auf die von Ihnen ausgewählten Volumes bereits Snapshot- oder Replikationsrichtlinien angewendet wurden, werden diese vorhandenen Richtlinien durch die später ausgewählten Richtlinien überschrieben.

1. Wählen Sie auf der Seite „Volumes auswählen“ das oder die Volumes aus, die Sie schützen möchten.
   - Filtern Sie die Zeilen optional, um nur Datenträger mit bestimmten Datenträgertypen, Stilen usw. anzuzeigen und so die Auswahl zu vereinfachen.
   - Nachdem Sie das erste Volume ausgewählt haben, können Sie alle FlexVol Volumes auswählen (FlexGroup Volumes können jeweils nur einzeln ausgewählt werden). Um alle vorhandenen FlexVol Volumes zu sichern, markieren Sie zuerst ein Volume und aktivieren Sie dann das Kontrollkästchen in der Titelzeile.
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume.
2. Wählen Sie **Weiter**.

Definieren Sie die Sicherungsstrategie

Zum Definieren der Sicherungsstrategie müssen die folgenden Optionen festgelegt werden:

- Ob Sie eine oder alle Backup-Optionen wünschen: lokale Snapshots, Replikation und Backup auf Objektspeicher
- Architektur
- Lokale Snapshot-Richtlinie
- Replikationsziel und -richtlinie

Wenn die von Ihnen ausgewählten Volumes andere Snapshot- und Replikationsrichtlinien haben als die Richtlinien, die Sie in diesem Schritt auswählen, werden die vorhandenen Richtlinien überschrieben.

- Informationen zur Sicherung in Objektspeichern (Anbieter, Verschlüsselung, Netzwerk, Sicherungsrichtlinie und Exportoptionen).

Schritte

1. Wählen Sie auf der Seite „Sicherungsstrategie definieren“ eine oder alle der folgenden Optionen aus. Alle drei sind standardmäßig ausgewählt:
   - **Lokale Snapshots**: Wenn Sie eine Replikation oder Sicherung im Objektspeicher durchführen, müssen lokale Snapshots erstellt werden.
   - **Replikation**: Erstellt replizierte Volumes auf einem anderen ONTAP Speichersystem.
   - **Backup**: Sichert Volumes im Objektspeicher.
2. **Architektur**: Wenn Sie sowohl Replikation als auch Sicherung gewählt haben, wählen Sie einen der folgenden Informationsflüsse:
   - **Kaskadierung**: Informationen fließen vom primären zum sekundären und dann vom sekundären zum Objektspeicher.
   - **Fan-out**: Informationen fließen vom primären zum sekundären *und* vom primären zum Objektspeicher.

     Weitere Informationen zu diesen Architekturen finden Sie unter"Planen Sie Ihren Schutzweg" .
3. **Lokaler Snapshot**: Wählen Sie eine vorhandene Snapshot-Richtlinie oder erstellen Sie eine neue.

   Informationen zum Erstellen einer benutzerdefinierten Richtlinie finden Sie unter"Erstellen einer Richtlinie" .

   Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:
   - Geben Sie den Namen der Richtlinie ein.
   - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
   - Wählen Sie **Erstellen**.
4. **Replikation**: Legen Sie die folgenden Optionen fest:
   - **Replikationsziel**: Wählen Sie das Zielsystem und die SVM aus. Wählen Sie optional das oder die Zielaggregate sowie das Präfix oder Suffix aus, das dem Namen des replizierten Volumes hinzugefügt wird.
   - **Replikationsrichtlinie**: Wählen Sie eine vorhandene Replikationsrichtlinie aus oder erstellen Sie eine.

     Informationen zum Erstellen einer benutzerdefinierten Richtlinie finden Sie unter"Erstellen einer Richtlinie" .

     Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:
     - Geben Sie den Namen der Richtlinie ein.
     - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
     - Wählen Sie **Erstellen**.
5. **Sichern auf Objekt**: Wenn Sie **Sichern** ausgewählt haben, legen Sie die folgenden Optionen fest:
   - **Anbieter**: Wählen Sie * StorageGRID*.
   - **Anbietereinstellungen**: Geben Sie die FQDN-Details, den Port, den Zugriffsschlüssel und den geheimen Schlüssel des Anbieter-Gateway-Knotens ein.

Der Zugriffsschlüssel und der geheime Schlüssel sind für den IAM-Benutzer, den Sie erstellt haben, um dem ONTAP Cluster Zugriff auf den Bucket zu gewähren.

- **Netzwerk**: Wählen Sie den IP-Bereich im ONTAP -Cluster aus, in dem sich die Volumes befinden, die Sie sichern möchten. Die Intercluster-LIFs für diesen IPspace müssen über ausgehenden Internetzugang verfügen (nicht erforderlich, wenn der Konsolenagent an einem „dunklen“ Standort installiert ist).

  Durch die Auswahl des richtigen IPspace wird sichergestellt, dass NetApp Backup and Recovery eine Verbindung von ONTAP zu Ihrem StorageGRID Objektspeicher herstellen kann.

- **Sicherungsrichtlinie**: Wählen Sie eine vorhandene Richtlinie zum Sichern in einem Objektspeicher aus oder erstellen Sie eine.

  Informationen zum Erstellen einer benutzerdefinierten Richtlinie finden Sie unter"Erstellen einer Richtlinie" .

  Um eine Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und gehen Sie wie folgt vor:

  - Geben Sie den Namen der Richtlinie ein.
  - Wählen Sie bis zu fünf Zeitpläne aus, normalerweise mit unterschiedlicher Häufigkeit.
  - Legen Sie für Backup-to-Object-Richtlinien die Einstellungen „DataLock“ und „Ransomware Resilience“ fest. Weitere Informationen zu DataLock und Ransomware Resilience finden Sie unter"Einstellungen der Backup-to-Object-Richtlinie" .

    Wenn Ihr Cluster ONTAP 9.11.1 oder höher verwendet, können Sie Ihre Backups vor Löschung und Ransomware-Angriffen schützen, indem Sie *DataLock und Ransomware Resilience* konfigurieren. *DataLock* schützt Ihre Sicherungsdateien vor Änderungen oder Löschungen und *Ransomware Resilience* durchsucht Ihre Sicherungsdateien nach Hinweisen auf einen Ransomware-Angriff.

  - Wählen Sie **Erstellen**.

  Wenn Ihr Cluster ONTAP 9.12.1 oder höher verwendet und Ihr StorageGRID System Version 11.4 oder höher verwendet, können Sie ältere Backups nach einer bestimmten Anzahl von Tagen in öffentliche Cloud-Archivebenen verschieben. Derzeit wird die Speicherebene AWS S3 Glacier/S3 Glacier Deep Archive oder Azure Archive unterstützt. Erfahren Sie, wie Sie Ihre Systeme für diese Funktionalität konfigurieren..

- **Tier-Backup in die öffentliche Cloud**: Wählen Sie den Cloud-Anbieter aus, zu dem Sie Backups tieren möchten, und geben Sie die Anbieterdetails ein.

  Wählen oder erstellen Sie einen neuen StorageGRID Cluster. Weitere Informationen zum Erstellen eines StorageGRID -Clusters, damit die Konsole ihn erkennen kann, finden Sie unter "StorageGRID -Dokumentation" .

- **Vorhandene Snapshots als Sicherungskopien in den Objektspeicher exportieren**: Wenn es lokale Snapshots für Volumes in diesem System gibt, die mit der von Ihnen soeben für dieses System ausgewählten Sicherungszeitplanbezeichnung übereinstimmen (z. B. täglich, wöchentlich usw.), wird diese zusätzliche Aufforderung angezeigt. Aktivieren Sie dieses Kontrollkästchen, um alle historischen Snapshots als Sicherungsdateien in den Objektspeicher zu kopieren und so den umfassendsten Schutz für Ihre Volumes zu gewährleisten.

6. Wählen Sie **Weiter**.

Überprüfen Sie Ihre Auswahl

Dies ist die Gelegenheit, Ihre Auswahl zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

Schritte

1. Überprüfen Sie Ihre Auswahl auf der Überprüfungsseite.
2. Aktivieren Sie optional das Kontrollkästchen, um **die Snapshot-Richtlinienbezeichnungen automatisch mit den Replikations- und Sicherungsrichtlinienbezeichnungen zu synchronisieren**. Dadurch werden Snapshots mit einer Bezeichnung erstellt, die mit den Bezeichnungen in den Replikations- und Sicherungsrichtlinien übereinstimmt.
3. Wählen Sie **Backup aktivieren**.

Ergebnis

NetApp Backup and Recovery beginnt mit der Durchführung der ersten Sicherungen Ihrer Volumes. Die Basisübertragung des replizierten Volumes und der Sicherungsdatei umfasst eine vollständige Kopie der Quelldaten. Nachfolgende Übertragungen enthalten differentielle Kopien der im Primärspeicher enthaltenen Daten, die in Snapshots gespeichert sind.

Im Zielcluster wird ein repliziertes Volume erstellt, das mit dem primären Speichervolume synchronisiert wird.

Im durch den von Ihnen eingegebenen S3-Zugriffsschlüssel und geheimen Schlüssel angegebenen Dienstkonto wird ein S3-Bucket erstellt und die Sicherungsdateien werden dort gespeichert.

Das Volume-Backup-Dashboard wird angezeigt, damit Sie den Status der Backups überwachen können.

Sie können den Status von Sicherungs- und Wiederherstellungsaufträgen auch mithilfe der"Seite „Jobüberwachung“" .

API-Befehle anzeigen

Möglicherweise möchten Sie die im Assistenten „Sicherung und Wiederherstellung aktivieren“ verwendeten API-Befehle anzeigen und optional kopieren. Möglicherweise möchten Sie dies tun, um die Sicherungsaktivierung in zukünftigen Systemen zu automatisieren.

Schritte

1. Wählen Sie im Assistenten „Sicherung und Wiederherstellung aktivieren“ die Option „API-Anforderung anzeigen“ aus.
2. Um die Befehle in die Zwischenablage zu kopieren, wählen Sie das Symbol **Kopieren**.

Migrieren Sie Volumes mit SnapMirror zu Cloud Resync in NetApp Backup and Recovery

Die SnapMirror to Cloud Resync-Funktion in NetApp Backup and Recovery optimiert den Datenschutz und die Kontinuität bei Volumemigrationen in NetApp -Umgebungen. Wenn ein Volume mithilfe von SnapMirror Logical Replication (LRSE) von einer lokalen NetApp Bereitstellung zu einer anderen oder zu einer Cloud-basierten Lösung wie Cloud Volumes ONTAP migriert wird, stellt SnapMirror to Cloud Resync sicher, dass bestehende Cloud-Backups intakt und betriebsbereit bleiben.

Diese Funktion macht einen erneuten Baseline-Prozess überflüssig und ermöglicht die Fortsetzung der Backups nach der Migration. Diese Funktion ist in Workload-Migrationsszenarien wertvoll, unterstützt sowohl FlexVols als auch FlexGroups und ist ab ONTAP Version 9.16.1 verfügbar.

Diese Funktion ist ab NetApp Backup and Recovery Version 4.0.3 verfügbar, die im Mai 2025 veröffentlicht wurde.

SnapMirror to Cloud Resync gewährleistet die Kontinuität der Datensicherung über verschiedene Umgebungen hinweg und erleichtert so die Datenverwaltung in Hybrid- und Multi-Cloud-Setups.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

Bevor Sie beginnen

Stellen Sie sicher, dass diese Voraussetzungen erfüllt sind:

- Auf dem Ziel ONTAP -Cluster muss ONTAP Version 9.16.1 oder höher ausgeführt werden.
- Der alte Quell- ONTAP Cluster muss mit NetApp Backup and Recovery geschützt werden.
- Die SnapMirror to Cloud Resync-Funktion ist ab NetApp Backup and Recovery Version 4.0.3 verfügbar, die im Mai 2025 veröffentlicht wurde.
- Stellen Sie sicher, dass die letzte Sicherung im Objektspeicher der gemeinsame Snapshot für die alte Quelle, die neue Quelle und den Objektspeicher ist. Verwenden Sie keinen gemeinsamen Snapshot, der älter ist als der letzte im Objektspeicher gesicherte Snapshot.
- Sowohl die Snapshot- als auch die SnapMirror Richtlinien, die auf dem älteren ONTAP -Cluster verwendet wurden, müssen auf dem neuen ONTAP -Cluster erstellt werden, bevor der Resynchronisierungsvorgang gestartet werden kann. Wenn Sie im Resynchronisierungsprozess eine Richtlinie verwenden, müssen Sie diese Richtlinie auch erstellen. Der Resync-Vorgang erstellt keine Richtlinien.
- Stellen Sie sicher, dass die SnapMirror -Richtlinie, die auf die SnapMirror -Beziehung des Migrationsvolumes angewendet wird, dieselbe Bezeichnung enthält, die die Cloud-Beziehung verwendet. Um Probleme zu vermeiden, verwenden Sie die Richtlinie, die eine exakte Spiegelung des Volumes und aller Snapshots regelt.

SnapMirror to Cloud Resync nach Migrationen mit den Methoden SVM-Migrate, SVM-DR oder Head Swap wird derzeit nicht unterstützt.

So funktioniert NetApp Backup and Recovery SnapMirror to Cloud Resync

Wenn Sie eine technische Aktualisierung durchführen oder Volumes von einem ONTAP Cluster zu einem anderen migrieren, ist es wichtig, dass Ihre Backups weiterhin ohne Unterbrechung funktionieren. NetApp Backup and Recovery SnapMirror to Cloud Resync hilft dabei, indem es sicherstellt, dass Ihre Cloud-Backups auch nach einer Volume-Migration konsistent bleiben.

Hier ist ein Beispiel:

Stellen Sie sich vor, Sie haben ein lokales Volume namens Vol1a. Dieses Volume verfügt über drei Snapshots: S1, S2 und S3. Diese Momentaufnahmen sind Wiederherstellungspunkte. Band 1 wird mit SnapMirror to Cloud (SM-C) in der Cloud gesichert, aber nur S1 und S2 befinden sich im Objektspeicher.

Jetzt möchten Sie Vol1 auf einen anderen ONTAP Cluster migrieren. Dazu erstellen Sie eine SnapMirror Logical Replication (LRSE)-Beziehung zu einem neuen Cloud-Volume namens Vol1b. Dadurch werden alle drei Snapshots – S1, S2 und S3 – von Vol1a nach Vol1b übertragen.

Nach Abschluss der Migration verfügen Sie über das folgende Setup:

- Die ursprüngliche SM-C-Beziehung (Vol1a → Objektspeicher) wird gelöscht.
- Die LRSE-Beziehung (Vol1a → Vol1b) wird ebenfalls gelöscht.
- Vol1b ist jetzt Ihr aktives Volume.

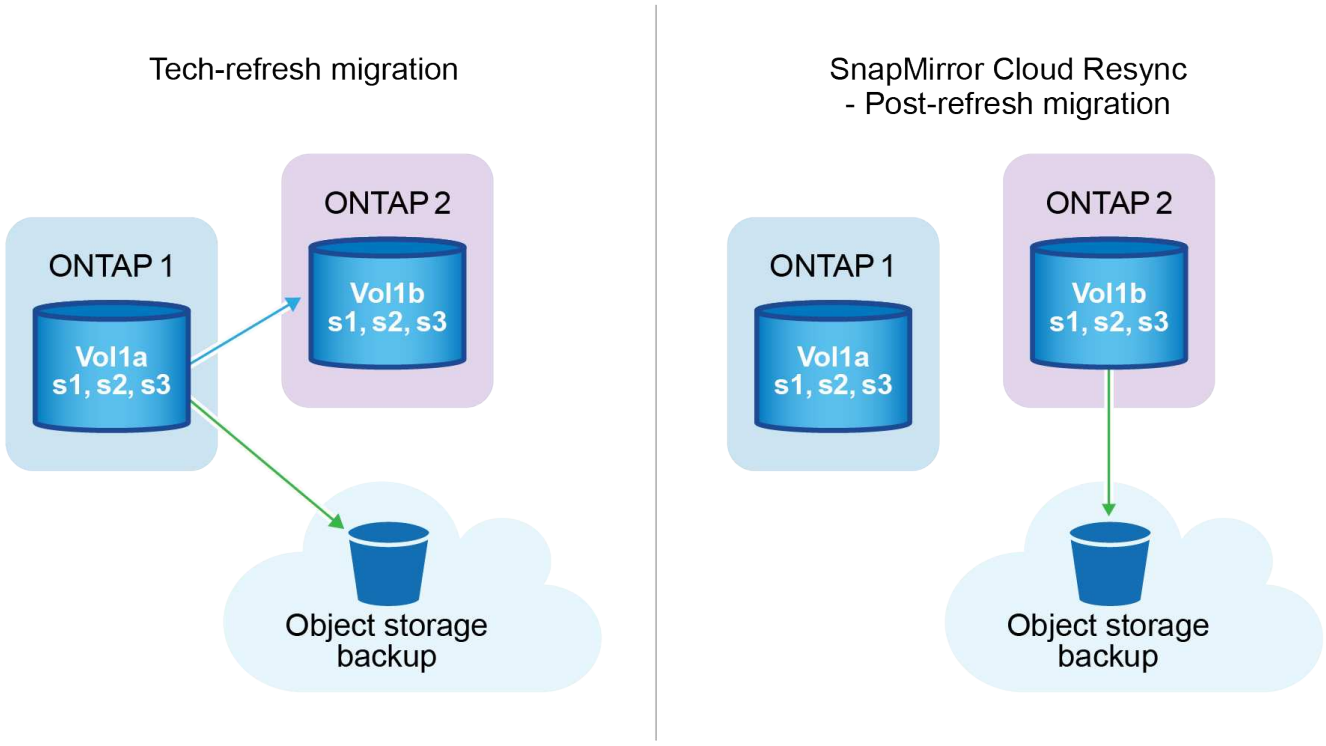
An diesem Punkt möchten Sie mit der Sicherung von Vol1b auf demselben Cloud-Endpunkt fortfahren. Aber anstatt eine vollständige Sicherung von Grund auf neu zu starten (was Zeit und Ressourcen kosten würde), verwenden Sie SnapMirror to Cloud Resync.

So funktioniert die Neusynchronisierung:

- Das System sucht nach einem gemeinsamen Snapshot zwischen Vol1a und Object Store. In diesem Fall haben beide S2.
- Aufgrund dieses gemeinsamen Snapshots muss das System nur die inkrementellen Änderungen zwischen S2 und S3 übertragen.

Dies bedeutet, dass nur die nach S2 hinzugefügten neuen Daten an den Objektspeicher gesendet werden, nicht das gesamte Volume.

Dieser Prozess verhindert doppelte Datensicherungen, spart Bandbreite und sorgt dafür, dass die Datensicherung auch nach der Migration weiterläuft.



Verfahrenshinweise

- Migrationen und technische Aktualisierungen werden nicht mit NetApp Backup and Recovery durchgeführt. Sie sollten von einem professionellen Serviceteam oder einem qualifizierten Speicheradministrator durchgeführt werden.
- Ein NetApp Migrationsteam erstellt die SnapMirror Beziehung zwischen den Quell- und Ziel ONTAP

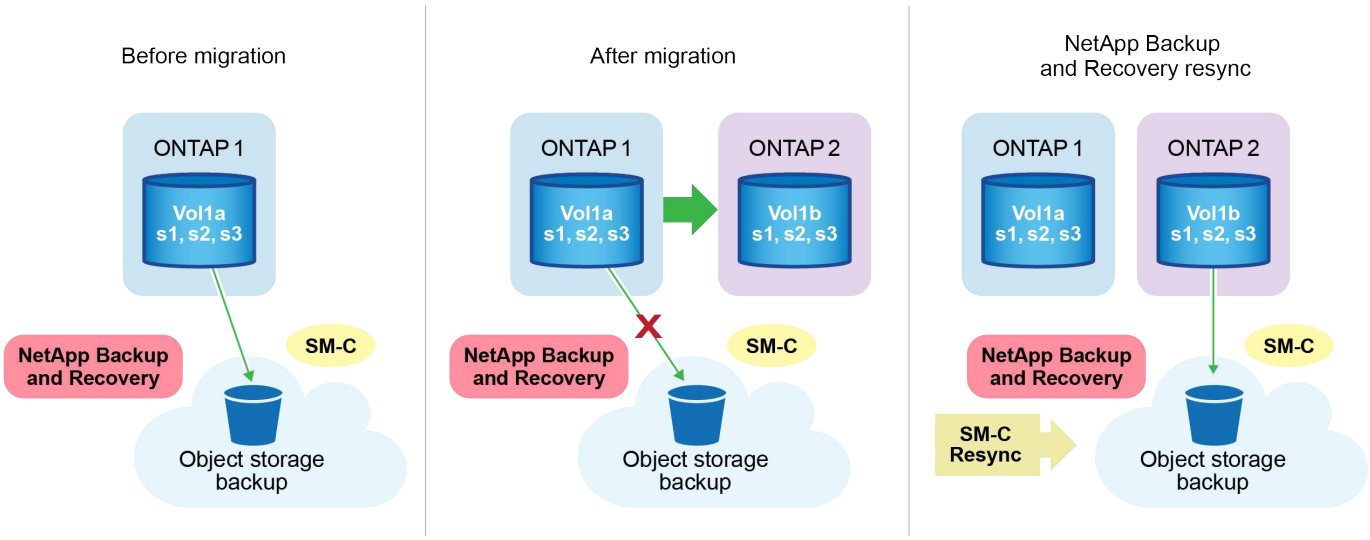
Clustern, um die Migration von Volumes zu erleichtern.

- Stellen Sie sicher, dass die Migration während einer technischen Aktualisierung auf einer SnapMirror-basierten Migration basiert.

So migrieren Sie Volumes mit SnapMirror zu Cloud Resync

Die Migration von Volumes mit SnapMirror zu Cloud Resync umfasst die folgenden Hauptschritte, die im Folgenden jeweils ausführlicher beschrieben werden:

- **Befolgen Sie eine Checkliste vor der Migration**: Vor Beginn der Migration stellt ein NetApp Tech Refresh-Team sicher, dass die folgenden Voraussetzungen erfüllt sind, um Datenverluste zu vermeiden und einen reibungslosen Migrationsprozess zu gewährleisten.
- **Befolgen Sie eine Checkliste nach der Migration**: Nach der Migration stellt ein NetApp Tech Refresh-Team sicher, dass die folgenden Schritte abgeschlossen sind, um Schutz zu gewährleisten und die Neusynchronisierung vorzubereiten.
- **Führen Sie eine SnapMirror zu-Cloud-Resynchronisierung durch**: Nach der Migration führt ein NetApp Tech Refresh-Team eine SnapMirror -zu-Cloud-Resynchronisierung durch, um die Cloud-Backups von den neu migrierten Volumes fortzusetzen.



Befolgen Sie eine Checkliste vor der Migration

Vor der Migration prüft das NetApp Tech Refresh-Team diese Voraussetzungen, um Datenverlust zu vermeiden und einen reibungslosen Ablauf zu gewährleisten.

1. Stellen Sie sicher, dass alle zu migrierenden Volumes mit NetApp Backup and Recovery geschützt sind.
2. Zeichnen Sie die UUIDs der Volume-Instanz auf. Notieren Sie sich die Instanz-UUIDs aller Volumes, bevor Sie mit der Migration beginnen. Diese Kennungen sind für spätere Zuordnungs- und Neusynchronisierungsvorgänge von entscheidender Bedeutung.
3. Erstellen Sie einen letzten Snapshot jedes Volumes, um den aktuellen Status beizubehalten, bevor Sie alle SnapMirror -Beziehungen löschen.
4. Dokumentieren Sie die SnapMirror -Richtlinien. Notieren Sie die SnapMirror Richtlinie, die derzeit mit der Beziehung jedes Volumes verknüpft ist. Dies wird später während des SnapMirror zu-Cloud-Resynchronisierungsprozesses benötigt.
5. Löschen Sie die SnapMirror Cloud-Beziehungen mit dem Objektspeicher.

6. Erstellen Sie eine standardmäßige SnapMirror -Beziehung mit dem neuen ONTAP Cluster, um das Volume auf den neuen Ziel ONTAP -Cluster zu migrieren.

Befolgen Sie eine Checkliste nach der Migration

Nach der Migration stellt ein NetApp Tech Refresh-Team sicher, dass die folgenden Schritte abgeschlossen werden, um den Schutz herzustellen und die Neusynchronisierung vorzubereiten.

1. Notieren Sie die neuen Volume-Instanz-UUIDs aller migrierten Volumes im Ziel ONTAP Cluster.
2. Bestätigen Sie, dass alle erforderlichen SnapMirror Richtlinien, die im alten ONTAP Cluster verfügbar waren, im neuen ONTAP Cluster korrekt konfiguriert sind.
3. Fügen Sie den neuen ONTAP Cluster als System auf der Konsolenseite **Systeme** hinzu.

> Es sollte die UUID der Volume-Instanz verwendet werden, nicht die Volume-ID. Die UUID der Volume-Instanz ist eine eindeutige Kennung, die bei Migrationen konsistent bleibt, während sich die Volume-ID nach der Migration ändern kann.

Führen Sie eine SnapMirror zu-Cloud-Neusynchronisierung durch

Nach der Migration führt ein NetApp Tech Refresh-Team einen SnapMirror -zu-Cloud-Resync-Vorgang durch, um die Cloud-Backups von den neu migrierten Volumes fortzusetzen.

1. Fügen Sie den neuen ONTAP Cluster als System auf der Konsolenseite **Systeme** hinzu.
2. Sehen Sie sich die Seite „NetApp Backup and Recovery Volumes“ an, um sicherzustellen, dass die Details des alten Quellsystems verfügbar sind.
3. Wählen Sie auf der Seite „NetApp Backup and Recovery Volumes“ die Option „Sicherungseinstellungen“ aus.
   - Wählen Sie auf der Seite „Sicherungseinstellungen“ die Option „Alle anzeigen“ aus.
   - Wählen Sie im Menü „Aktionen …“ rechts neben der *neuen* Quelle die Option „Sicherung erneut synchronisieren“ aus.
4. Führen Sie auf der Seite „System erneut synchronisieren“ die folgenden Schritte aus:
   a. **Neues Quellsystem**: Geben Sie den neuen ONTAP Cluster ein, in den die Volumes migriert wurden.
   b. **Vorhandener Zielobjektspeicher**: Wählen Sie den Zielobjektspeicher aus, der die Sicherungen vom alten Quellsystem enthält.
5. Wählen Sie **CSV-Vorlage herunterladen**, um das Excel-Blatt mit den Resynchronisierungsdetails herunterzuladen. Verwenden Sie dieses Blatt, um die Details der zu migrierenden Volumes einzugeben. Geben Sie in der CSV-Datei die folgenden Details ein:
   - Die alte Volume-Instanz-UUID aus dem Quellcluster
   - Die neue Volume-Instanz-UUID aus dem Zielcluster
   - Die SnapMirror -Richtlinie, die auf die neue Beziehung angewendet werden soll.
6. Wählen Sie unter „Volume-Mapping-Details hochladen“ die Option „Hochladen“, um das ausgefüllte CSV-Blatt in die NetApp Backup and Recovery Benutzeroberfläche hochzuladen.

> Es sollte die UUID der Volume-Instanz verwendet werden, nicht die Volume-ID. Die UUID der Volume-Instanz ist eine eindeutige Kennung, die bei Migrationen konsistent bleibt, während sich die Volume-ID nach der Migration ändern kann.

7. Geben Sie die für den Resynchronisierungsvorgang erforderlichen Anbieter- und Netzwerkkonfigurationsinformationen ein.
8. Wählen Sie **Senden**, um den Validierungsprozess zu starten.

   NetApp Backup and Recovery überprüft, ob jedes für die Neusynchronisierung ausgewählte Volume den neuesten Snapshot aufweist und mindestens einen gemeinsamen Snapshot hat. Dadurch wird sichergestellt, dass die Volumes für den SnapMirror -zu-Cloud-Resync-Vorgang bereit sind.

9. Überprüfen Sie die Validierungsergebnisse, einschließlich der neuen Quellvolume-Namen und des Resynchronisierungsstatus für jedes Volume.
10. Überprüfen Sie die Volumenberechtigung. Das System prüft, ob die Volumes für eine erneute Synchronisierung geeignet sind. Wenn ein Volume nicht geeignet ist, bedeutet dies, dass es sich nicht um den neuesten Snapshot handelt oder kein gemeinsamer Snapshot gefunden wurde.

   Um sicherzustellen, dass die Volumes weiterhin für den SnapMirror zu-Cloud-Resync-Vorgang geeignet sind, erstellen Sie einen letzten Snapshot jedes Volumes, bevor Sie während der Phase vor der Migration alle SnapMirror -Beziehungen löschen. Dadurch bleibt der aktuelle Stand der Daten erhalten.

11. Wählen Sie **Resync**, um den Resynchronisierungsvorgang zu starten. Das System verwendet den aktuellsten und gemeinsamen Snapshot, um nur die inkrementellen Änderungen zu übertragen und so die Kontinuität der Sicherung sicherzustellen.
12. Überwachen Sie den Resynchronisierungsprozess auf der Seite „Job Monitor“.

Wiederherstellen der NetApp Backup and Recovery -Konfigurationsdaten in einer Dark Site

Wenn Sie NetApp Backup and Recovery an einem Standort ohne Internetzugang verwenden (bekannt als *privater Modus*), werden die Konfigurationsdaten von NetApp Backup and Recovery im StorageGRID oder ONTAP S3-Bucket gesichert, in dem Ihre Backups gespeichert werden. Wenn Sie ein Problem mit dem Hostsystem des Konsolenagenten haben, können Sie einen neuen Konsolenagenten bereitstellen und die kritischen NetApp Backup and Recovery -Daten wiederherstellen.

Dieses Verfahren gilt nur für ONTAP Volume-Daten.

Wenn Sie NetApp Backup and Recovery in einer SaaS-Umgebung verwenden und der Konsolenagent bei Ihrem Cloud-Anbieter oder auf Ihrem eigenen mit dem Internet verbundenen Host bereitgestellt wird, sichert und schützt das System alle wichtigen Konfigurationsdaten in der Cloud. Wenn Sie ein Problem mit dem Konsolenagenten haben, erstellen Sie einen neuen Konsolenagenten und fügen Sie Ihre Systeme hinzu. Die Sicherungsdetails werden automatisch wiederhergestellt.

Es werden zwei Arten von Daten gesichert:

- NetApp Backup and Recovery -Datenbank – enthält eine Liste aller Volumes, Sicherungsdateien, Sicherungsrichtlinien und Konfigurationsinformationen.
- Indizierte Katalogdateien – enthalten detaillierte Indizes, die für die Such- und Wiederherstellungsfunktion verwendet werden und Ihre Suche nach Volumedaten, die Sie wiederherstellen möchten, sehr schnell und effizient machen.

Diese Daten werden einmal täglich um Mitternacht gesichert und es werden maximal 7 Kopien jeder Datei aufbewahrt. Wenn der Konsolenagent mehrere lokale ONTAP -Systeme verwaltet, werden die NetApp Backup and Recovery im Bucket des zuerst aktivierten Systems gespeichert.

In der NetApp Backup and Recovery -Datenbank oder in den indizierten Katalogdateien sind niemals Volumedaten enthalten.

Wiederherstellen von NetApp Backup and Recovery -Daten auf einem neuen Konsolenagenten

Wenn Ihr lokaler Konsolenagent nicht mehr funktioniert, müssen Sie einen neuen Konsolenagenten installieren und dann die NetApp Backup and Recovery -Daten auf dem neuen Konsolenagenten wiederherstellen.

Sie müssen die folgenden Aufgaben ausführen, um Ihr NetApp Backup and Recovery -System wieder in einen funktionsfähigen Zustand zu versetzen:

- Installieren Sie einen neuen Konsolenagenten
- Wiederherstellen der NetApp Backup and Recovery -Datenbank
- Wiederherstellen der indizierten Katalogdateien
- Erkennen Sie alle Ihre On-Premise ONTAP -Systeme und StorageGRID Systeme erneut in der NetApp Console Benutzeroberfläche.

Nachdem Sie überprüft haben, ob Ihr System funktioniert, erstellen Sie neue Sicherungsdateien.

Was du brauchst

Sie müssen auf die aktuellsten Datenbank- und Indexsicherungen aus dem StorageGRID oder ONTAP S3-Bucket zugreifen, in dem Ihre Sicherungsdateien gespeichert sind:

- NetApp Backup and Recovery MySQL-Datenbankdatei

  Diese Datei befindet sich am folgenden Speicherort im Bucket `netapp-backup-<GUID>/mysql_backup/` und es heißt `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- ZIP-Sicherungsdatei des indizierten Katalogs

  Diese Datei befindet sich am folgenden Speicherort im Bucket `netapp-backup-<GUID>/catalog_backup/` und es heißt `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

Installieren Sie einen neuen Konsolen-Agenten auf einem neuen lokalen Linux-Host

Laden Sie beim Installieren eines neuen Konsolenagenten dieselbe Softwareversion herunter wie beim ursprünglichen Agenten. Änderungen an der NetApp Backup and Recovery -Datenbank können dazu führen, dass neuere Softwareversionen nicht mit alten Datenbanksicherungen funktionieren. Du kannst "Aktualisieren Sie die Konsolen-Agent-Software auf die neueste Version, nachdem Sie die Backup-Datenbank wiederhergestellt haben." .

1. "Installieren Sie den Konsolen-Agenten auf einem neuen lokalen Linux-Host"
2. Melden Sie sich mit den soeben erstellten Administrator-Benutzeranmeldeinformationen bei der Konsole an.

Wiederherstellen der NetApp Backup and Recovery -Datenbank

1. Kopieren Sie die MySQL-Sicherung vom Sicherungsspeicherort auf den neuen Konsolen-Agent-Host. Wir verwenden unten den Beispieldateinamen „CBS_DB_Backup_23_05_2023.sql“.
2. Kopieren Sie die Sicherung mit einem der folgenden Befehle in den MySQL-Docker-Container, je nachdem, ob Sie einen Docker- oder Podman-Container verwenden:

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Rufen Sie die MySQL-Container-Shell mit einem der folgenden Befehle auf, je nachdem, ob Sie einen Docker- oder Podman-Container verwenden:

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. Stellen Sie in der Container-Shell die „Umgebung“ bereit.
5. Sie benötigen das MySQL-DB-Passwort. Kopieren Sie daher den Wert des Schlüssels „MYSQL_ROOT_PASSWORD“.
6. Stellen Sie die MySQL-Datenbank von NetApp Backup and Recovery mit dem folgenden Befehl wieder her:

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Überprüfen Sie mit den folgenden SQL-Befehlen, ob die MySQL-Datenbank von NetApp Backup and Recovery korrekt wiederhergestellt wurde:

```
mysql -u root -p cloud_backup
```

8. Geben Sie das Passwort ein.

```
mysql> show tables;
mysql> select * from volume;
```

9. Stellen Sie sicher, dass die angezeigten Volumina mit denen Ihrer ursprünglichen Umgebung übereinstimmen.

Wiederherstellen der indizierten Katalogdateien

1. Kopieren Sie die ZIP-Sicherungsdatei des indizierten Katalogs (wir verwenden den Beispieldateinamen „Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip“) vom Sicherungsspeicherort auf den neuen Konsolenagent-Host im Ordner „/opt/application/netapp/cbs“.
2. Entpacken Sie die Datei „Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip“ mit dem folgenden Befehl:

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Führen Sie den Befehl **ls** aus, um sicherzustellen, dass der Ordner „catalogdb1“ mit den darunter liegenden Unterordnern „changes“ und „snapshots“ erstellt wurde.

Entdecken Sie Ihre ONTAP -Cluster und StorageGRID Systeme

1. "Entdecken Sie alle On-Premise ONTAP Systeme"die in Ihrer vorherigen Umgebung verfügbar waren. Dazu gehört auch das ONTAP -System, das Sie als S3-Server verwendet haben.
2. "Entdecken Sie Ihre StorageGRID -Systeme".

Einrichten der StorageGRID -Umgebungsdetails

Fügen Sie die Details des StorageGRID -Systems hinzu, das mit Ihren ONTAP -Systemen verknüpft ist, wie sie im ursprünglichen Konsolen-Agent-Setup eingerichtet wurden, mithilfe des "NetApp Console -APIs" .

Die folgenden Informationen gelten für Installationen im privaten Modus ab NetApp Console 3.9.xx. Bei älteren Versionen gehen Sie wie folgt vor: "DarkSite Cloud Backup: MySQL und indizierter Katalog sichern und wiederherstellen" .

Sie müssen diese Schritte für jedes System ausführen, das Daten auf StorageGRID sichert.

1. Extrahieren Sie das Autorisierungstoken mithilfe der folgenden OAuth/Token-API.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '
{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"pas
sword"}
> '
```

   Während es sich bei der IP-Adresse, dem Benutzernamen und den Passwörtern um benutzerdefinierte Werte handelt, ist dies beim Kontonamen nicht der Fall. Der Kontoname lautet immer „account-DARKSITE1“. Außerdem muss der Benutzername einen Namen im E-Mail-Format verwenden.

   Diese API gibt eine Antwort wie die folgende zurück. Sie können das Autorisierungstoken wie unten gezeigt abrufen.

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```

2. Extrahieren Sie die System-ID und die X-Agent-ID mithilfe der Tenancy/External/Resource-API.

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Diese API gibt eine Antwort wie die folgende zurück. Der Wert unter „resourceIdentifier“ bezeichnet die *WorkingEnvironment-ID* und der Wert unter „agentId“ bezeichnet *x-agent-id*.

```
[{"resourceIdentifier":"OnPremWorkingEnvironment-
pMtZND0M","resourceType":"ON_PREM","agentId":"vB_1xShPpBtUosjD7wfBlLIhqD
gIPA0wclients","resourceClass":"ON_PREM","name":"CBSFAS8300-01-
02","metadata":"{\"clusterUuid\": \"2cb6cb4b-dc07-11ec-9114-
d039ea931e09\"}","workspaceIds":["workspace2wKYjTy9"],"agentIds":["vB_1x
ShPpBtUosjD7wfBlLIhqDgIPA0wclients"]}]
```

3. Aktualisieren Sie die NetApp Backup and Recovery -Datenbank mit den Details des mit den Systemen verknüpften StorageGRID Systems. Stellen Sie sicher, dass Sie den vollqualifizierten Domänennamen des StorageGRID sowie den Zugriffsschlüssel und den Speicherschlüssel wie unten gezeigt eingeben:

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

Überprüfen der NetApp Backup and Recovery -Einstellungen

1. Wählen Sie jedes ONTAP -System aus und klicken Sie im rechten Bereich neben dem Sicherungs- und Wiederherstellungsdienst auf **Sicherungen anzeigen**.

   Sie sollten alle für Ihre Volumes erstellten Backups sehen.

2. Klicken Sie im Wiederherstellungs-Dashboard im Abschnitt „Suchen und Wiederherstellen“ auf **Indizierungseinstellungen**.

   Stellen Sie sicher, dass die Systeme, bei denen die indizierte Katalogisierung zuvor aktiviert war, aktiviert bleiben.

3. Führen Sie auf der Seite „Suchen und Wiederherstellen“ einige Katalogsuchen durch, um zu bestätigen, dass die Wiederherstellung des indizierten Katalogs erfolgreich abgeschlossen wurde.

Verwalten Sie Backups für Ihre ONTAP -Systeme mit NetApp Backup and Recovery

Verwalten Sie mit NetApp Backup and Recovery Backups für Ihre Cloud Volumes ONTAP und lokalen ONTAP Systeme, indem Sie den Backup-Zeitplan ändern, Volume-Backups aktivieren/deaktivieren, Backups anhalten, Backups löschen, das Löschen von Backups erzwingen und vieles mehr. Dies umfasst alle Arten von Backups, einschließlich Snapshots, replizierter Volumes und Sicherungsdateien im Objektspeicher. Sie können die Registrierung von NetApp Backup and Recovery auch aufheben.

Verwalten oder ändern Sie Sicherungsdateien nicht direkt auf Ihren Speichersystemen oder in der Umgebung Ihres Cloud-Anbieters. Dies kann zu einer Beschädigung der Dateien führen und zu einer nicht unterstützten Konfiguration.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

Den Sicherungsstatus der Volumes in Ihren Systemen anzeigen

Sie können im Volumes Backup Dashboard eine Liste aller Volumes anzeigen, die derzeit gesichert werden. Dies umfasst alle Arten von Backups, einschließlich Snapshots, replizierter Volumes und Sicherungsdateien im Objektspeicher. Sie können auch die Volumes in den Systemen anzeigen, die derzeit nicht gesichert werden.

Schritte

1. Wählen Sie im Konsolenmenü **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie das Menü **Volumes** aus, um die Liste der gesicherten Volumes für Ihre Cloud Volumes ONTAP und lokalen ONTAP Systeme anzuzeigen.
3. Wenn Sie nach bestimmten Volumes in bestimmten Systemen suchen, können Sie die Liste nach System und Volume verfeinern. Sie können auch den Suchfilter verwenden oder die Spalten nach Volume-Stil (FlexVol oder FlexGroup), Volume-Typ usw. sortieren.

   Um zusätzliche Spalten anzuzeigen (Aggregate, Sicherheitsstil (Windows oder UNIX), Snapshot-Richtlinie, Replikationsrichtlinie und Sicherungsrichtlinie), wählen Sie das Pluszeichen aus.

4. Überprüfen Sie den Status der Schutzoptionen in der Spalte „Vorhandener Schutz“. Die 3 Symbole stehen für „Lokale Snapshots“, „Replizierte Volumes“ und „Backups im Objektspeicher“.

   Das jeweilige Symbol leuchtet auf, wenn der entsprechende Sicherungstyp aktiviert ist, und ist grau, wenn der Sicherungstyp inaktiv ist. Sie können den Mauszeiger über jedes Symbol bewegen, um die verwendete Sicherungsrichtlinie und weitere relevante Informationen zu jedem Sicherungstyp anzuzeigen.

Aktivieren Sie die Sicherung auf zusätzlichen Volumes in einem System

Wenn Sie bei der ersten Aktivierung von NetApp Backup and Recovery die Sicherung nur auf einigen Volumes in einem System aktiviert haben, können Sie später Sicherungen auf weiteren Volumes aktivieren.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes** das Volume aus, auf dem Sie Backups aktivieren möchten, und anschließend das Menü „Aktionen“ aus. ••• Am Ende der Zeile wählen Sie **3-2-1-Schutz aktivieren**.
2. Auf der Seite *Sicherungsstrategie definieren* wählen Sie die Sicherungsarchitektur aus und definieren dann die Richtlinien und weitere Details für lokale Snapshots, replizierte Volumes und Sicherungsdateien. Sehen Sie sich die Details zu den Sicherungsoptionen der ursprünglichen Volumes an, die Sie in diesem System aktiviert haben. Wählen Sie dann **Weiter**.
3. Überprüfen Sie die Sicherungseinstellungen für dieses Volume und wählen Sie dann **Sicherung aktivieren**.

Ändern Sie die Sicherungseinstellungen, die vorhandenen Volumes zugewiesen sind

Sie können die Sicherungsrichtlinien ändern, die Ihren vorhandenen Volumes mit zugewiesenen Richtlinien zugewiesen sind. Sie können die Richtlinien für Ihre lokalen Snapshots, replizierten Volumes und Sicherungsdateien ändern. Alle neuen Snapshot-, Replikations- oder Sicherungsrichtlinien, die Sie auf die

Volumes anwenden möchten, müssen bereits vorhanden sein.

Bearbeiten der Sicherungseinstellungen auf einem einzelnen Volume

Schritte

1. Suchen Sie im Menü **Volumes** das Volume, dessen Richtlinieneinstellungen Sie ändern möchten, und wählen Sie dann das Menü „Aktionen“ aus. ••• Am Ende der Zeile und wählen Sie **Backup-Strategie bearbeiten**.
2. Auf der Seite „Sicherungsstrategie bearbeiten“ können Sie die vorhandenen Sicherungsrichtlinien für lokale Snapshots, replizierte Volumes und Sicherungsdateien ändern und anschließend „Weiter“ auswählen.

   Wenn Sie beim Aktivieren von NetApp Backup and Recovery für diesen Cluster in der anfänglichen Sicherungsrichtlinie *DataLock und Ransomware Resilience* für Cloud-Sicherungen aktiviert haben, werden Ihnen nur andere Richtlinien angezeigt, die mit DataLock konfiguriert wurden. Und wenn Sie beim Aktivieren von NetApp Backup and Recovery_DataLock und Ransomware Resilience_ nicht aktiviert haben, werden Ihnen nur andere Cloud-Backup-Richtlinien angezeigt, für die DataLock nicht konfiguriert ist.

3. Überprüfen Sie die Sicherungseinstellungen für dieses Volume und wählen Sie dann **Sicherung aktivieren**.

Bearbeiten der Sicherungseinstellungen auf mehreren Volumes

Wenn Sie dieselben Sicherungseinstellungen auf mehreren Volumes verwenden möchten, können Sie die Sicherungseinstellungen auf mehreren Volumes gleichzeitig aktivieren oder bearbeiten. Sie können Volumes auswählen, die keine Sicherungseinstellungen, nur Snapshot-Einstellungen, nur Einstellungen für die Sicherung in der Cloud usw. haben, und Massenänderungen an allen diesen Volumes mit unterschiedlichen Sicherungseinstellungen vornehmen.

Wenn Sie mit mehreren Volumes arbeiten, müssen alle Volumes die folgenden gemeinsamen Merkmale aufweisen:

- gleiches System
- gleicher Stil (FlexVol oder FlexGroup -Volume)
- gleicher Typ (Lese-/Schreib- oder Datenschutz-Volume)

Wenn mehr als fünf Volumes für die Sicherung aktiviert sind, initialisiert NetApp Backup and Recovery jeweils nur fünf Volumes. Wenn diese abgeschlossen sind, wird der Vorgang in Gruppen von 5 fortgesetzt, bis alle Volumes initialisiert sind.

Schritte

1. Filtern Sie auf der Registerkarte **Volumes** nach dem System, auf dem sich die Volumes befinden.
2. Wählen Sie alle Volumes aus, auf denen Sie die Sicherungseinstellungen verwalten möchten.
3. Klicken Sie je nach Art der Sicherungsaktion, die Sie konfigurieren möchten, auf die Schaltfläche im Menü „Massenaktionen“:

Sicherungsaktion…	Wählen Sie diese Schaltfläche aus…
Verwalten der Snapshot-Sicherungseinstellungen	**Lokale Snapshots verwalten**
Verwalten der Replikationssicherungseinstellungen	**Replikation verwalten**

Sicherungsaktion…	Wählen Sie diese Schaltfläche aus…
Verwalten der Backup-Einstellungen in der Cloud	**Backup verwalten**
Verwalten Sie mehrere Arten von Sicherungseinstellungen. Mit dieser Option können Sie auch die Sicherungsarchitektur ändern.	**Sicherung und Wiederherstellung verwalten**

4. Nehmen Sie auf der daraufhin angezeigten Sicherungsseite Änderungen an den bestehenden Sicherungsrichtlinien für lokale Snapshots, replizierte Volumes oder Sicherungsdateien vor und wählen Sie **Speichern**.

   Wenn Sie beim Aktivieren von NetApp Backup and Recovery für diesen Cluster in der anfänglichen Sicherungsrichtlinie *DataLock und Ransomware Resilience* für Cloud-Sicherungen aktiviert haben, werden Ihnen nur andere Richtlinien angezeigt, die mit DataLock konfiguriert wurden. Und wenn Sie beim Aktivieren von NetApp Backup and Recovery_DataLock und Ransomware Resilience_ nicht aktiviert haben, werden Ihnen nur andere Cloud-Backup-Richtlinien angezeigt, für die DataLock nicht konfiguriert ist.

Erstellen Sie jederzeit eine manuelle Volume-Sicherung

Sie können jederzeit ein On-Demand-Backup erstellen, um den aktuellen Status des Volumes zu erfassen. Dies kann nützlich sein, wenn sehr wichtige Änderungen an einem Volume vorgenommen wurden und Sie nicht auf die nächste geplante Sicherung warten möchten, um diese Daten zu schützen. Sie können diese Funktion auch verwenden, um eine Sicherung für ein Volume zu erstellen, das derzeit nicht gesichert wird und dessen aktuellen Status Sie erfassen möchten.

Sie können einen Ad-hoc-Snapshot oder eine Sicherung eines Volumes im Objektspeicher erstellen. Es ist nicht möglich, ein ad hoc repliziertes Volume zu erstellen.

Der Sicherungsname enthält den Zeitstempel, sodass Sie Ihre On-Demand-Sicherung von anderen geplanten Sicherungen unterscheiden können.

Wenn Sie beim Aktivieren von NetApp Backup and Recovery für diesen Cluster *DataLock und Ransomware Resilience* aktiviert haben, wird das On-Demand-Backup auch mit DataLock konfiguriert und die Aufbewahrungsdauer beträgt 30 Tage. Ransomware-Scans werden für Ad-hoc-Backups nicht unterstützt. "Erfahren Sie mehr über DataLock und Ransomware-Schutz".

Wenn Sie ein Ad-hoc-Backup erstellen, wird auf dem Quellvolume ein Snapshot erstellt. Da dieser Snapshot nicht Teil eines normalen Snapshot-Zeitplans ist, wird er nicht deaktiviert. Möglicherweise möchten Sie diesen Snapshot manuell vom Quellvolume löschen, sobald die Sicherung abgeschlossen ist. Dadurch können Blöcke freigegeben werden, die mit diesem Snapshot in Zusammenhang stehen. Der Name des Snapshots beginnt mit `cbs-snapshot-adhoc-` . "Erfahren Sie, wie Sie einen Snapshot mit der ONTAP CLI löschen" .

Die On-Demand-Volume-Sicherung wird auf Datenschutzvolumes nicht unterstützt.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes*••• für das Volume und wählen Sie *Backup** > **Ad-hoc-Backup erstellen**.

In der Spalte „Sicherungsstatus“ für dieses Volume wird „In Bearbeitung“ angezeigt, bis die Sicherung erstellt ist.

Sehen Sie sich die Liste der Backups für jedes Volume an

Sie können die Liste aller Sicherungsdateien anzeigen, die für jedes Volume vorhanden sind. Auf dieser Seite werden Details zum Quellvolume, zum Zielspeicherort und zu Sicherungsdetails angezeigt, z. B. die zuletzt durchgeführte Sicherung, die aktuelle Sicherungsrichtlinie, die Größe der Sicherungsdatei und mehr.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes*** für das Quellvolume und wählen Sie *Volumedetails anzeigen**.

   Es werden die Details zum Volume und die Liste der Snapshots angezeigt.

2. Wählen Sie **Snapshot**, **Replikation** oder **Backup**, um die Liste aller Backup-Dateien für jeden Backup-Typ anzuzeigen.

Führen Sie einen Ransomware-Scan auf einem Volume-Backup im Objektspeicher durch

NetApp Backup and Recovery durchsucht Ihre Sicherungsdateien nach Hinweisen auf einen Ransomware-Angriff, wenn eine Sicherung in einer Objektdatei erstellt wird und wenn Daten aus einer Sicherungsdatei wiederhergestellt werden. Sie können auch jederzeit einen On-Demand-Scan ausführen, um die Verwendbarkeit einer bestimmten Sicherungsdatei im Objektspeicher zu überprüfen. Dies kann nützlich sein, wenn auf einem bestimmten Volume ein Ransomware-Problem aufgetreten ist und Sie überprüfen möchten, ob die Sicherungen für dieses Volume betroffen sind.

Diese Funktion ist nur verfügbar, wenn das Volume-Backup von einem System mit ONTAP 9.11.1 oder höher erstellt wurde und Sie in der Backup-to-Object-Richtlinie „DataLock und Ransomware Resilience“ aktiviert haben.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes*** für das Quellvolume und wählen Sie *Volumedetails anzeigen**.

   Die Details zum Volumen werden angezeigt.

2. Wählen Sie **Backup** aus, um die Liste der Sicherungsdateien im Objektspeicher anzuzeigen.
3. Wählen für die Volume-Sicherungsdatei, die Sie auf Ransomware scannen möchten, und klicken Sie auf **Nach Ransomware scannen**.

   Die Spalte „Ransomware-Resilienz“ zeigt, dass der Scan läuft.

Verwalten der Replikationsbeziehung mit dem Quellvolume

Nachdem Sie die Datenreplikation zwischen zwei Systemen eingerichtet haben, können Sie die Datenreplikationsbeziehung verwalten.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes*** für das Quellvolume und wählen Sie die Option *Replikation**. Sie können alle verfügbaren Optionen sehen.
2. Wählen Sie die Replikationsaktion aus, die Sie ausführen möchten.

   In der folgenden Tabelle werden die verfügbaren Aktionen beschrieben:

Aktion	Beschreibung
Replikation anzeigen	Zeigt Ihnen Details zur Volume-Beziehung: Übertragungsinformationen, Informationen zur letzten Übertragung, Details zum Volume und Informationen zur der Beziehung zugewiesenen Schutzrichtlinie.
Update-Replikation	Startet eine inkrementelle Übertragung, um das Zielvolume zu aktualisieren, das mit dem Quellvolume synchronisiert werden soll.
Replikation anhalten	Unterbrechen Sie die inkrementelle Übertragung von Snapshots, um das Zielvolume zu aktualisieren. Sie können den Vorgang später fortsetzen, wenn Sie die inkrementellen Updates neu starten möchten.
Replikation unterbrechen	Bricht die Beziehung zwischen Quell- und Zielvolume ab und aktiviert das Zielvolume für den Datenzugriff – macht es lese- und schreibgeschützt. Diese Option wird normalerweise verwendet, wenn das Quellvolume aufgrund von Ereignissen wie Datenbeschädigung, versehentlichem Löschen oder einem Offline-Status keine Daten bereitstellen kann.https://docs.netapp.com/us-en/ontap-sm-classic/volume-disaster-recovery/index.html["Erfahren Sie in der ONTAP -Dokumentation, wie Sie ein Zielvolume für den Datenzugriff konfigurieren und ein Quellvolume reaktivieren."^]
Replikation abbrechen	Deaktiviert Sicherungen dieses Volumes auf dem Zielsystem und deaktiviert auch die Möglichkeit, ein Volume wiederherzustellen. Eventuell vorhandene Backups werden nicht gelöscht. Dadurch wird die Datenschutzbeziehung zwischen Quell- und Zielvolume nicht gelöscht.
Umgekehrte Neusynchronisierung	Vertauscht die Rollen der Quell- und Zielvolumes. Inhalte des ursprünglichen Quellvolumes werden durch Inhalte des Zielvolumes überschrieben. Dies ist hilfreich, wenn Sie ein Quellvolume reaktivieren möchten, das offline gegangen ist. Alle Daten, die zwischen der letzten Datenreplikation und der Deaktivierung des Quellvolumes auf das ursprüngliche Quellvolume geschrieben wurden, bleiben nicht erhalten.
Beziehung löschen	Löscht die Datenschutzbeziehung zwischen Quell- und Zielvolumes, was bedeutet, dass keine Datenreplikation mehr zwischen den Volumes stattfindet. Durch diese Aktion wird das Zielvolume nicht für den Datenzugriff aktiviert, d. h., es wird kein Lese-/Schreibzugriff darauf ermöglicht. Diese Aktion löscht auch die Cluster-Peer-Beziehung und die Storage-VM (SVM)-Peer-Beziehung, wenn keine anderen Datenschutzbeziehungen zwischen den Systemen bestehen.

Ergebnis

Nachdem Sie eine Aktion ausgewählt haben, aktualisiert die Konsole die Beziehung.

Bearbeiten einer vorhandenen Backup-to-Cloud-Richtlinie

Sie können die Attribute für eine Sicherungsrichtlinie ändern, die derzeit auf Volumes in einem System angewendet wird. Das Ändern der Sicherungsrichtlinie wirkt sich auf alle vorhandenen Volumes aus, die die Richtlinie verwenden.

- Wenn Sie beim Aktivieren von NetApp Backup and Recovery für diesen Cluster in der ursprünglichen Richtlinie „DataLock und Ransomware Resilience“ aktiviert haben, müssen alle von Ihnen bearbeiteten Richtlinien mit derselben DataLock-Einstellung (Governance oder Compliance) konfiguriert werden. Und wenn Sie beim Aktivieren von NetApp Backup and Recovery_DataLock und Ransomware Resilience_ nicht aktiviert haben, können Sie DataLock jetzt nicht aktivieren.
- Wenn Sie beim Erstellen von Backups auf AWS bei der Aktivierung von NetApp Backup and Recovery in Ihrer ersten Backup-Richtlinie *S3 Glacier* oder *S3 Glacier Deep Archive* ausgewählt haben, ist diese Ebene die einzige verfügbare Archivebene beim Bearbeiten von Backup-Richtlinien. Und wenn Sie in Ihrer ersten Sicherungsrichtlinie keine Archivebene ausgewählt haben, ist *S3 Glacier* Ihre einzige Archivierungsoption beim Bearbeiten einer Richtlinie.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.
2. Wählen Sie auf der Seite „Backup-Einstellungen“••• für das System, auf dem Sie die Richtlinieneinstellungen ändern möchten, und wählen Sie **Richtlinien verwalten**.
3. Wählen Sie auf der Seite „Richtlinien verwalten“ **Bearbeiten** für die Sicherungsrichtlinie aus, die Sie in diesem System ändern möchten.
4. Wählen Sie auf der Seite „Richtlinie bearbeiten“ den Abwärtspfeil aus, um den Abschnitt „Beschriftungen und Aufbewahrung“ zu erweitern und den Zeitplan und/oder die Sicherungsaufbewahrung zu ändern, und wählen Sie „Speichern“ aus.

   Wenn auf Ihrem Cluster ONTAP 9.10.1 oder höher ausgeführt wird, haben Sie auch die Möglichkeit, die Einstufung von Backups in den Archivspeicher nach einer bestimmten Anzahl von Tagen zu aktivieren oder zu deaktivieren.

   "Erfahren Sie mehr über die Verwendung von AWS-Archivspeicher"Die "Weitere Informationen zur Verwendung des Azure-Archivspeichers"Die "Erfahren Sie mehr über die Verwendung des Google-Archivspeichers"Die (Erfordert ONTAP 9.12.1.)

   Beachten Sie, dass alle Sicherungsdateien, die in den Archivspeicher verschoben wurden, in dieser Ebene verbleiben, wenn Sie die Verschiebung von Sicherungen in den Archivspeicher beenden – sie werden nicht automatisch zurück in die Standardebene verschoben. Nur neue Volume-Backups werden im Standard-Tier gespeichert.

Hinzufügen einer neuen Backup-to-Cloud-Richtlinie

Wenn Sie NetApp Backup and Recovery für ein System aktivieren, werden alle ursprünglich ausgewählten Volumes mit der von Ihnen definierten Standard-Sicherungsrichtlinie gesichert. Wenn Sie bestimmten Volumes mit unterschiedlichen Recovery Point Objectives (RPO) unterschiedliche Sicherungsrichtlinien zuweisen möchten, können Sie zusätzliche Richtlinien für diesen Cluster erstellen und diese Richtlinien anderen Volumes zuweisen.

Wenn Sie eine neue Sicherungsrichtlinie auf bestimmte Volumes in einem System anwenden möchten, müssen Sie zuerst die Sicherungsrichtlinie zum System hinzufügen. Dann können Siedie vorhandenen Volumes zugewiesen sind,Wenden Sie die Richtlinie auf Volumes in diesem System an .

- Wenn Sie beim Aktivieren von NetApp Backup and Recovery für diesen Cluster in der anfänglichen Richtlinie „DataLock und Ransomware Resilience“ aktiviert haben, müssen alle weiteren Richtlinien, die Sie erstellen, mit derselben DataLock-Einstellung (Governance oder Compliance) konfiguriert werden. Und wenn Sie beim Aktivieren von NetApp Backup and Recovery_DataLock und Ransomware Resilience_ nicht aktiviert haben, können Sie keine neuen Richtlinien erstellen, die DataLock verwenden.
- Wenn Sie beim Erstellen von Backups auf AWS bei der Aktivierung von NetApp Backup and Recovery in Ihrer ersten Backup-Richtlinie *S3 Glacier* oder *S3 Glacier Deep Archive* ausgewählt haben, ist diese Ebene die einzige Archivebene, die für zukünftige Backup-Richtlinien für diesen Cluster verfügbar ist. Und wenn Sie in Ihrer ersten Sicherungsrichtlinie keine Archivierungsebene ausgewählt haben, ist *S3 Glacier* Ihre einzige Archivierungsoption für zukünftige Richtlinien.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.
2. Wählen Sie auf der Seite „Backup-Einstellungen“••• für das System, dem Sie die neue Richtlinie hinzufügen möchten, und wählen Sie **Richtlinien verwalten**.
3. Wählen Sie auf der Seite „Richtlinien verwalten“ die Option „Neue Richtlinie hinzufügen“ aus.
4. Wählen Sie auf der Seite „Neue Richtlinie hinzufügen“ den Abwärtspfeil aus, um den Abschnitt „Beschriftungen und Aufbewahrung“ zu erweitern und den Zeitplan und die Sicherungsaufbewahrung zu definieren, und wählen Sie „Speichern“ aus.

   Wenn auf Ihrem Cluster ONTAP 9.10.1 oder höher ausgeführt wird, haben Sie auch die Möglichkeit, die Einstufung von Backups in den Archivspeicher nach einer bestimmten Anzahl von Tagen zu aktivieren oder zu deaktivieren.

   "Erfahren Sie mehr über die Verwendung von AWS-Archivspeicher"Die "Weitere Informationen zur Verwendung des Azure-Archivspeichers"Die "Erfahren Sie mehr über die Verwendung des Google-Archivspeichers"Die (Erfordert ONTAP 9.12.1.)

Backups löschen

Mit NetApp Backup and Recovery können Sie eine einzelne Sicherungsdatei löschen, alle Sicherungen für ein Volume löschen oder alle Sicherungen aller Volumes in einem System löschen. Möglicherweise möchten Sie alle Sicherungen löschen, wenn Sie die Sicherungen nicht mehr benötigen oder wenn Sie das Quellvolume gelöscht haben und alle Sicherungen entfernen möchten.

Sie können keine Sicherungsdateien löschen, die Sie mit DataLock und Ransomware-Schutz gesperrt haben. Die Option „Löschen“ ist in der Benutzeroberfläche nicht verfügbar, wenn Sie eine oder mehrere gesperrte Sicherungsdateien ausgewählt haben.

Wenn Sie ein System oder einen Cluster löschen möchten, das bzw. der über Sicherungen verfügt, müssen Sie die Sicherungen **vor** dem Löschen des Systems löschen. NetApp Backup and Recovery löscht Backups nicht automatisch, wenn Sie ein System löschen, und in der Benutzeroberfläche gibt es derzeit keine Unterstützung zum Löschen der Backups, nachdem das System gelöscht wurde. Für alle verbleibenden Sicherungen werden Ihnen weiterhin die Kosten für die Objektspeicherung in Rechnung gestellt.

Löschen aller Sicherungsdateien für ein System

Das Löschen aller Sicherungen im Objektspeicher für ein System deaktiviert nicht zukünftige Sicherungen von

Volumes in diesem System. Wenn Sie die Erstellung von Backups aller Volumes in einem System beenden möchten, können Sie Backups deaktivierenwie hier beschrieben .

Beachten Sie, dass diese Aktion keine Auswirkungen auf Snapshots oder replizierte Volumes hat – diese Arten von Sicherungsdateien werden nicht gelöscht.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.
2. Wählen••• für das System, auf dem Sie alle Sicherungen löschen möchten, und wählen Sie **Alle Sicherungen löschen**.
3. Geben Sie im Bestätigungsdialogfeld den Namen des Systems ein.
4. Wählen Sie **Erweiterte Einstellungen**.
5. **Löschen von Backups erzwingen**: Geben Sie an, ob Sie das Löschen aller Backups erzwingen möchten oder nicht.

   In einigen extremen Fällen möchten Sie möglicherweise, dass NetApp Backup and Recovery keinen Zugriff mehr auf Backups hat. Dies kann beispielsweise passieren, wenn der Dienst keinen Zugriff mehr auf den Backup-Bucket hat oder Backups durch DataLock geschützt sind, Sie diese aber nicht mehr möchten. Bisher konnten Sie diese nicht selbst löschen und mussten den NetApp -Support anrufen. Mit dieser Version können Sie die Option zum erzwungenen Löschen von Sicherungen (auf Volume- und Systemebene) verwenden.

   Verwenden Sie diese Option mit Vorsicht und nur bei extremem Reinigungsbedarf. NetApp Backup and Recovery hat keinen Zugriff mehr auf diese Backups, auch wenn sie nicht im Objektspeicher gelöscht werden. Sie müssen zu Ihrem Cloud-Anbieter gehen und die Backups manuell löschen.

6. Wählen Sie **Löschen**.

Löschen aller Sicherungsdateien für ein Volume

Durch das Löschen aller Sicherungen für ein Volume werden auch zukünftige Sicherungen für dieses Volume deaktiviert.

Schritte

1. Klicken Sie auf der Registerkarte **Volumes** auf••• für das Quellvolume und wählen Sie **Details & Sicherungsliste**.

   Die Liste aller Sicherungsdateien wird angezeigt.

2. Wählen Sie **Aktionen** > **Alle Backups löschen**.
3. Geben Sie den Datenträgernamen ein.
4. Wählen Sie **Erweiterte Einstellungen**.
5. **Löschen von Backups erzwingen**: Geben Sie an, ob Sie das Löschen aller Backups erzwingen möchten oder nicht.

   In einigen extremen Fällen möchten Sie möglicherweise, dass NetApp Backup and Recovery keinen Zugriff mehr auf Backups hat. Dies kann beispielsweise passieren, wenn der Dienst keinen Zugriff mehr auf den Backup-Bucket hat oder Backups durch DataLock geschützt sind, Sie diese aber nicht mehr möchten. Bisher konnten Sie diese nicht selbst löschen und mussten den NetApp -Support anrufen. Mit dieser Version können Sie die Option zum erzwungenen Löschen von Sicherungen (auf Volume- und

Systemebene) verwenden.

> Verwenden Sie diese Option mit Vorsicht und nur bei extremem Reinigungsbedarf. NetApp Backup and Recovery hat keinen Zugriff mehr auf diese Backups, auch wenn sie nicht im Objektspeicher gelöscht werden. Sie müssen zu Ihrem Cloud-Anbieter gehen und die Backups manuell löschen.

6. Wählen Sie **Löschen**.

Löschen einer einzelnen Sicherungsdatei für ein Volume

Sie können eine einzelne Sicherungsdatei löschen, wenn Sie sie nicht mehr benötigen. Dies umfasst das Löschen einer einzelnen Sicherung eines Volume-Snapshots oder einer Sicherung im Objektspeicher.

Sie können replizierte Volumes (Datensicherungsvolumes) nicht löschen.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes*••• für das Quellvolume und wählen Sie *Volumedetails anzeigen**.

   Die Details zum Volume werden angezeigt und Sie können **Snapshot**, **Replikation** oder **Backup** auswählen, um die Liste aller Backup-Dateien für das Volume anzuzeigen. Standardmäßig werden die verfügbaren Snapshots angezeigt.

2. Wählen Sie **Snapshot** oder **Backup**, um den Typ der Sicherungsdateien anzuzeigen, die Sie löschen möchten.
3. Wählen••• für die Volume-Sicherungsdatei, die Sie löschen möchten, und wählen Sie **Löschen**.
4. Wählen Sie im Bestätigungsdialogfeld **Löschen** aus.

Löschen von Volume-Sicherungsbeziehungen

Durch das Löschen der Sicherungsbeziehung für ein Volume steht Ihnen ein Archivierungsmechanismus zur Verfügung, wenn Sie die Erstellung neuer Sicherungsdateien stoppen und das Quellvolume löschen, aber alle vorhandenen Sicherungsdateien beibehalten möchten. Dadurch haben Sie die Möglichkeit, das Volume bei Bedarf in der Zukunft aus der Sicherungsdatei wiederherzustellen und gleichzeitig Speicherplatz auf Ihrem Quellspeichersystem freizugeben.

Sie müssen das Quellvolume nicht unbedingt löschen. Sie können die Sicherungsbeziehung für ein Volume löschen und das Quellvolume beibehalten. In diesem Fall können Sie die Sicherung auf dem Volume zu einem späteren Zeitpunkt „aktivieren“. Die ursprüngliche Basissicherungskopie wird in diesem Fall weiterhin verwendet – eine neue Basissicherungskopie wird nicht erstellt und in die Cloud exportiert. Beachten Sie, dass dem Volume die Standard-Sicherungsrichtlinie zugewiesen wird, wenn Sie eine Sicherungsbeziehung reaktivieren.

Diese Funktion ist nur verfügbar, wenn auf Ihrem System ONTAP 9.12.1 oder höher ausgeführt wird.

Sie können das Quellvolume nicht aus der Benutzeroberfläche von NetApp Backup and Recovery löschen. Sie können jedoch die Seite „Volume-Details“ auf der Seite „Konsole **Systeme**“ öffnen und "Löschen Sie das Volume von dort" .

> Sie können einzelne Volume-Sicherungsdateien nicht löschen, nachdem die Beziehung gelöscht wurde. Sie können jedoch alle Sicherungen für das Volume löschen.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes*** für das Quellvolume und wählen Sie *Backup > **Beziehung löschen**.

NetApp Backup and Recovery für ein System deaktivieren

Durch die Deaktivierung von NetApp Backup and Recovery für ein System werden die Sicherungen aller Volumes auf dem System deaktiviert und auch die Möglichkeit zur Wiederherstellung eines Volumes wird deaktiviert. Eventuell vorhandene Backups werden nicht gelöscht. Dadurch wird der Sicherungsdienst nicht von diesem System abgemeldet. Im Grunde können Sie damit alle Sicherungs- und Wiederherstellungsaktivitäten für einen bestimmten Zeitraum anhalten.

Beachten Sie, dass Ihnen Ihr Cloud-Anbieter weiterhin die Kosten für die Objektspeicherung für die Kapazität berechnet, die Ihre Backups nutzen, es sei denn, SieLöschen Sie die Backups .

Schritte

1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.
2. Wählen Sie auf der Seite „Backup-Einstellungen“ für das System, auf dem Sie Backups deaktivieren möchten, und wählen Sie **Backup deaktivieren**.
3. Wählen Sie im Bestätigungsdialogfeld **Deaktivieren** aus.

Während die Sicherung deaktiviert ist, wird für dieses System die Schaltfläche **Sicherung aktivieren** angezeigt. Sie können diese Schaltfläche auswählen, wenn Sie die Sicherungsfunktion für dieses System erneut aktivieren möchten.

Aufheben der Registrierung von NetApp Backup and Recovery für ein System

Sie können die Registrierung von NetApp Backup and Recovery für ein System aufheben, wenn Sie die Sicherungsfunktion nicht mehr verwenden möchten und für die Sicherungen in diesem System keine Gebühren mehr anfallen sollen. Normalerweise wird diese Funktion verwendet, wenn Sie ein System löschen möchten und den Sicherungsdienst kündigen möchten.

Sie können diese Funktion auch verwenden, wenn Sie den Zielobjektspeicher ändern möchten, in dem Ihre Cluster-Backups gespeichert werden. Nachdem Sie die Registrierung von NetApp Backup and Recovery für das System aufgehoben haben, können Sie NetApp Backup and Recovery für diesen Cluster mithilfe der neuen Cloud-Anbieterinformationen aktivieren.

Bevor Sie die Registrierung von NetApp Backup and Recovery aufheben können, müssen Sie die folgenden Schritte in dieser Reihenfolge ausführen:

- Deaktivieren Sie NetApp Backup and Recovery für das System
- Löschen Sie alle Backups für dieses System

Die Option zum Aufheben der Registrierung ist erst verfügbar, wenn diese beiden Aktionen abgeschlossen sind.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.
2. Wählen Sie auf der Seite „Backup-Einstellungen“ für das System, bei dem Sie die Registrierung des Sicherungsdienstes aufheben möchten, und wählen Sie **Registrierung aufheben**.
3. Wählen Sie im Bestätigungsdialogfeld **Abmelden** aus.

Wiederherstellung aus ONTAP -Backups

Stellen Sie ONTAP -Daten aus Sicherungsdateien mit NetApp Backup and Recovery wieder her

Backups Ihrer ONTAP -Volume-Daten werden als Snapshots, auf replizierten Volumes oder im Objektspeicher gespeichert. Sie können Daten von jedem dieser Speicherorte zu einem bestimmten Zeitpunkt wiederherstellen. Mit NetApp Backup and Recovery können Sie je nach Bedarf ein gesamtes Volume, einen Ordner oder einzelne Dateien wiederherstellen.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

- Sie können ein **Volume** (als neues Volume) auf dem ursprünglichen System, auf einem anderen System, das dasselbe Cloud-Konto verwendet, oder auf einem lokalen ONTAP -System wiederherstellen.
- Sie können einen **Ordner** auf einem Volume im ursprünglichen System, auf einem Volume in einem anderen System, das dasselbe Cloud-Konto verwendet, oder auf einem Volume auf einem lokalen ONTAP System wiederherstellen.
- Sie können **Dateien** auf einem Volume im ursprünglichen System, auf einem Volume in einem anderen System, das dasselbe Cloud-Konto verwendet, oder auf einem Volume auf einem lokalen ONTAP System wiederherstellen.

Sie benötigen eine gültige NetApp Backup and Recovery -Lizenz, um Daten in einem Produktionssystem wiederherzustellen.

Zusammenfassend sind dies die gültigen Flows, die Sie zum Wiederherstellen von Volume-Daten auf einem ONTAP System verwenden können:

- Sicherungsdatei → wiederhergestelltes Volume
- Repliziertes Volume → wiederhergestelltes Volume
- Snapshot → wiederhergestelltes Volume

Wenn der Wiederherstellungsvorgang nicht abgeschlossen werden kann, warten Sie, bis der Job Monitor „Fehlgeschlagen“ anzeigt, bevor Sie den Wiederherstellungsvorgang wiederholen.

Informationen zu Einschränkungen im Zusammenhang mit der Wiederherstellung von ONTAP -Daten finden Sie unter"Einschränkungen bei der Sicherung und Wiederherstellung von ONTAP -Volumes" .

Das Wiederherstellungs-Dashboard

Sie verwenden das Wiederherstellungs-Dashboard, um Volume-, Ordner- und Dateiwiederherstellungsvorgänge durchzuführen. Um auf das Wiederherstellungs-Dashboard zuzugreifen, wählen Sie im Konsolenmenü **Sicherung und Wiederherstellung** und anschließend die Registerkarte **Wiederherstellung**. Sie können auch auswählen > **Wiederherstellungs-Dashboard anzeigen** Sie können es über den Sicherungs- und Wiederherstellungsdienst im Dienstebereich aufrufen.

NetApp Backup and Recovery muss bereits für mindestens ein System aktiviert sein und erste Sicherungsdateien müssen vorhanden sein.

Das Wiederherstellungs-Dashboard bietet zwei verschiedene Möglichkeiten zum Wiederherstellen von Daten aus Sicherungsdateien: **Durchsuchen und Wiederherstellen** und **Suchen und Wiederherstellen**.

Vergleich von „Browse & Restore“ und „Search & Restore“

Im Großen und Ganzen ist „Durchsuchen und Wiederherstellen“ normalerweise besser geeignet, wenn Sie ein bestimmtes Volume, einen bestimmten Ordner oder eine bestimmte Datei aus der letzten Woche oder dem letzten Monat wiederherstellen müssen – und Sie den Namen und Speicherort der Datei sowie das Datum kennen, an dem sie zuletzt in gutem Zustand war. „Suchen und Wiederherstellen“ ist normalerweise besser, wenn Sie ein Volume, einen Ordner oder eine Datei wiederherstellen müssen, sich aber nicht an den genauen Namen, das Volume, auf dem es sich befindet, oder das Datum erinnern, an dem es zuletzt in gutem Zustand war.

Diese Tabelle bietet einen Funktionsvergleich der beiden Methoden.

Durchsuchen und Wiederherstellen	Suchen und Wiederherstellen
Durchsuchen Sie eine ordnerartige Struktur, um das Volume, den Ordner oder die Datei innerhalb einer einzelnen Sicherungsdatei zu finden.	Suchen Sie in **allen Sicherungsdateien** nach einem Volume, Ordner oder einer Datei anhand des teilweisen oder vollständigen Volumenamens, des teilweisen oder vollständigen Ordner-/Dateinamens, des Größenbereichs und zusätzlicher Suchfilter.
Führt keine Dateiwiederherstellung durch, wenn die Datei gelöscht oder umbenannt wurde und der Benutzer den ursprünglichen Dateinamen nicht kennt	Verarbeitet neu erstellte/gelöschte/umbenannte Verzeichnisse und neu erstellte/gelöschte/umbenannte Dateien
Die schnelle Wiederherstellung wird unterstützt.	Die schnelle Wiederherstellung wird nicht unterstützt.

Diese Tabelle enthält eine Liste gültiger Wiederherstellungsvorgänge basierend auf dem Speicherort Ihrer Sicherungsdateien.

Sicherungstyp	Durchsuchen und Wiederherstellen			Suchen und Wiederherstellen		
	Lautstärke wiederherstellen	Dateien wiederherstellen	Ordner wiederherstellen	Lautstärke wiederherstellen	Dateien wiederherstellen	Ordner wiederherstellen
Schnappschuss	Ja	Nein	Nein	Ja	Ja	Ja
Repliziertes Volume	Ja	Nein	Nein	Ja	Ja	Ja
Sicherungsdatei	Ja	Ja	Ja	Ja	Ja	Ja

Bevor Sie eine der beiden Wiederherstellungsmethoden anwenden, konfigurieren Sie Ihre Umgebung so, dass sie die Ressourcenanforderungen erfüllt. Einzelheiten finden Sie in den folgenden Abschnitten.

Informieren Sie sich über die Anforderungen und Wiederherstellungsschritte für den Wiederherstellungsvorgangstyp, den Sie verwenden möchten:

- "Wiederherstellen von Volumes mit „Durchsuchen und Wiederherstellen“"
- "Stellen Sie Ordner und Dateien mit „Durchsuchen und Wiederherstellen“ wieder her"

- "Stellen Sie Volumes, Ordner und Dateien mit „Suchen und Wiederherstellen“ wieder her"

Wiederherstellung aus ONTAP -Backups mithilfe von Suchen & Wiederherstellen

Mit Search & Restore können Sie Volumes, Ordner oder Dateien aus ONTAP Sicherungsdateien wiederherstellen. Mit Search & Restore können Sie alle Backups durchsuchen (einschließlich lokaler Snapshots, replizierter Volumes und Objektspeicher), ohne dass Sie genaue System-, Volume- oder Dateinamen benötigen.

Die Wiederherstellung aus lokalen Snapshots oder replizierten Volumes ist in der Regel schneller und kostengünstiger als die Wiederherstellung aus dem Objektspeicher.

Bei der Wiederherstellung eines vollständigen Volumes erstellt NetApp Backup and Recovery ein neues Volume unter Verwendung der Sicherungsdaten. Sie können die Wiederherstellung auf dem ursprünglichen System, einem anderen System innerhalb desselben Cloud-Kontos oder einem lokalen ONTAP System durchführen. Ordner und Dateien können an ihrem ursprünglichen Speicherort, auf einem anderen Volume im selben System, auf einem anderen System im selben Cloud-Konto oder auf einem lokalen System wiederhergestellt werden.

Die Wiederherstellungsmöglichkeiten hängen von Ihrer ONTAP Version ab:

- **Ordner:** Mit ONTAP 9.13.0 oder höher können Sie Ordner mit allen Dateien und Unterordnern wiederherstellen; mit früheren Versionen können Sie nur die Dateien im Ordner wiederherstellen.
- **Archivspeicher:** Die Wiederherstellung aus dem Archivspeicher (verfügbar ab ONTAP 9.10.1) ist langsamer und kann zusätzliche Kosten verursachen.
- **Anforderungen an den Destination Cluster:**
  - Volumenwiederherstellung: ONTAP 9.10.1 oder höher
  - Dateiwiederherstellung: ONTAP 9.11.1 oder höher
  - Google Archive and StorageGRID: ONTAP 9.12.1 oder höher
  - Ordnerwiederherstellung: ONTAP 9.13.1 oder höher

"Erfahren Sie mehr über die Wiederherstellung aus dem AWS-Archivspeicher"Die "Weitere Informationen zur Wiederherstellung aus dem Azure-Archivspeicher"Die "Erfahren Sie mehr über die Wiederherstellung aus dem Google-Archivspeicher"Die

- Wenn die Sicherungsdatei im Objektspeicher mit DataLock- und Ransomware-Schutz konfiguriert wurde, wird die Wiederherstellung auf Ordnerebene nur unterstützt, wenn die ONTAP -Version 9.13.1 oder höher ist. Wenn Sie eine frühere Version von ONTAP verwenden, können Sie das gesamte Volume aus der Sicherungsdatei wiederherstellen und dann auf die benötigten Ordner und Dateien zugreifen.
- Wenn sich die Sicherungsdatei im Objektspeicher im Archivspeicher befindet, wird die Wiederherstellung auf Ordnerebene nur unterstützt, wenn die ONTAP -Version 9.13.1 oder höher ist. Wenn Sie eine frühere Version von ONTAP verwenden, können Sie den Ordner aus einer neueren, nicht archivierten Sicherungsdatei wiederherstellen oder das gesamte Volume aus der archivierten Sicherung wiederherstellen und dann auf den benötigten Ordner und die benötigten Dateien zugreifen.
- Die Wiederherstellungspriorität „Hoch“ wird beim Wiederherstellen von Daten aus dem Azure-Archivspeicher auf StorageGRID -Systemen nicht unterstützt.
- Das Wiederherstellen von Ordnern aus Volumes im ONTAP S3-Objektspeicher wird derzeit nicht unterstützt.

Bevor Sie beginnen, sollten Sie eine Vorstellung vom Namen oder Speicherort des Datenträgers oder der Datei haben, die Sie wiederherstellen möchten.

Von Search & Restore unterstützte Systeme und Objektspeicheranbieter

Sie können ONTAP Daten aus einer Sicherungsdatei, die sich in einem sekundären System (einem replizierten Volume) oder im Objektspeicher (einer Sicherungsdatei) befindet, auf den folgenden Systemen wiederherstellen. Snapshots befinden sich auf dem Quellsystem und können nur auf demselben System wiederhergestellt werden.

Hinweis: Sie können Volumes und Dateien aus jeder Art von Sicherungsdatei wiederherstellen, einen Ordner können Sie derzeit jedoch nur aus Sicherungsdateien im Objektspeicher wiederherstellen.

Speicherort der Sicherungsdatei		**Zielsystem**
Objektspeicher (Backup)	**Sekundäres System (Replikation)**	
Amazon S3	Cloud Volumes ONTAP in AWS On-Premises- ONTAP -System	Cloud Volumes ONTAP in AWS On-Premises- ONTAP -System
Azure-Blob	Cloud Volumes ONTAP in Azure On-Premises- ONTAP -System	Cloud Volumes ONTAP in Azure On-Premises- ONTAP -System
Google Cloud-Speicher	Cloud Volumes ONTAP im lokalen ONTAP -System von Google	Cloud Volumes ONTAP im lokalen ONTAP -System von Google
NetApp StorageGRID	On-Premises- ONTAP -System Cloud Volumes ONTAP	On-Premises- ONTAP -System
ONTAP S3	On-Premises- ONTAP -System Cloud Volumes ONTAP	On-Premises- ONTAP -System

Für Search & Restore kann der Konsolenagent an den folgenden Speicherorten installiert werden:

- Für Amazon S3 kann der Konsolenagent in AWS oder in Ihren Räumlichkeiten bereitgestellt werden
- Für Azure Blob kann der Konsolenagent in Azure oder in Ihren Räumlichkeiten bereitgestellt werden
- Für Google Cloud Storage muss der Konsolenagent in Ihrem Google Cloud Platform VPC bereitgestellt werden

- Für StorageGRID muss der Konsolenagent in Ihren Räumlichkeiten bereitgestellt werden; mit oder ohne Internetzugang
- Für ONTAP S3 kann der Konsolenagent in Ihren Räumlichkeiten (mit oder ohne Internetzugang) oder in einer Cloud-Provider-Umgebung bereitgestellt werden

Beachten Sie, dass Verweise auf „On-Premises ONTAP Systeme“ FAS, AFF und ONTAP Select Systeme umfassen.

Voraussetzungen suchen und wiederherstellen

Stellen Sie sicher, dass Ihre Umgebung diese Anforderungen erfüllt, bevor Sie die Such- und Wiederherstellungsfunktion aktivieren:

- Clusteranforderungen:
  - Die ONTAP -Version muss 9.8 oder höher sein.
  - Die Speicher-VM (SVM), auf der sich das Volume befindet, muss über ein konfiguriertes Daten-LIF verfügen.
  - NFS muss auf dem Volume aktiviert sein (sowohl NFS- als auch SMB/CIFS-Volumes werden unterstützt).
  - Der SnapDiff RPC-Server muss auf der SVM aktiviert werden. Die Konsole führt dies automatisch aus, wenn Sie die Indizierung auf dem System aktivieren. (SnapDiff ist die Technologie, die schnell die Datei- und Verzeichnisunterschiede zwischen Snapshots identifiziert.)
- NetApp empfiehlt, ein separates Volume auf dem Console-Agenten einzubinden, um die Ausfallsicherheit von Search & Restore zu erhöhen. Anweisungen finden Sie unterDas Volume muss eingebunden werden, um den Katalog neu zu indizieren. Die

Voraussetzungen für die Legacy-Suche und -Wiederherstellung (bei Verwendung von Indexed Catalog v1)

Folgende Anforderungen gelten für die Funktion „Suchen & Wiederherstellen“ bei Verwendung der Legacy-Indexierung:

- AWS-Anforderungen:
  - Der Benutzerrolle, die der Konsole Berechtigungen erteilt, müssen bestimmte Amazon Athena-, AWS Glue- und AWS S3-Berechtigungen hinzugefügt werden. "Stellen Sie sicher, dass alle Berechtigungen richtig konfiguriert sind".

    Beachten Sie: Wenn Sie NetApp Backup and Recovery bereits mit einem zuvor konfigurierten Konsolenagenten verwendet haben, müssen Sie der Konsolenbenutzerrolle jetzt die Athena- und Glue-Berechtigungen hinzufügen. Sie werden für Search & Restore benötigt.

- Azure-Anforderungen:
  - Sie müssen den Azure Synapse Analytics-Ressourcenanbieter (genannt „Microsoft.Synapse“) mit Ihrem Abonnement registrieren. "Erfahren Sie, wie Sie diesen Ressourcenanbieter für Ihr Abonnement registrieren." . Sie müssen der **Eigentümer** oder **Mitwirkende** des Abonnements sein, um den Ressourcenanbieter zu registrieren.
  - Der Benutzerrolle, die der Konsole Berechtigungen erteilt, müssen bestimmte Berechtigungen für den Azure Synapse-Arbeitsbereich und das Data Lake Storage-Konto hinzugefügt werden. "Stellen Sie sicher, dass alle Berechtigungen richtig konfiguriert sind".

    Beachten Sie: Wenn Sie NetApp Backup and Recovery bereits mit einem zuvor konfigurierten Konsolenagenten verwendet haben, müssen Sie der Konsolenbenutzerrolle jetzt die Berechtigungen für den Azure Synapse-Arbeitsbereich und das Data Lake Storage-Konto hinzufügen. Sie werden für Search & Restore benötigt.

  - Der Konsolenagent muss **ohne** Proxyserver für die HTTP-Kommunikation mit dem Internet konfiguriert werden. Wenn Sie einen HTTP-Proxyserver für Ihren Konsolenagenten konfiguriert haben, können Sie die Such- und Wiederherstellungsfunktion nicht verwenden.
- Google Cloud-Anforderungen:
  - Der Benutzerrolle, die der NetApp Console Berechtigungen erteilt, müssen bestimmte Google BigQuery-Berechtigungen hinzugefügt werden. "Stellen Sie sicher, dass alle Berechtigungen richtig konfiguriert sind".

    Wenn Sie NetApp Backup and Recovery bereits mit einem zuvor konfigurierten Konsolenagenten verwendet haben, müssen Sie jetzt der Konsolenbenutzerrolle die BigQuery-Berechtigungen hinzufügen. Sie werden für Search & Restore benötigt.

- StorageGRID und ONTAP S3-Anforderungen:

  Abhängig von Ihrer Konfiguration gibt es zwei Möglichkeiten, Search & Restore zu implementieren:

  - Wenn in Ihrem Konto keine Anmeldeinformationen des Cloud-Anbieters vorhanden sind, werden die Informationen des indizierten Katalogs auf dem Konsolenagenten gespeichert.

    Informationen zum indizierten Katalog v2 finden Sie im folgenden Abschnitt zum Aktivieren des indizierten Katalogs.

  - Wenn Sie einen Konsolenagenten auf einer privaten (dunklen) Site verwenden, werden die indizierten Kataloginformationen auf dem Konsolenagenten gespeichert (erfordert Konsolenagentenversion 3.9.25 oder höher).
  - Wenn Sie "AWS -Anmeldeinformationen" oder "Azure-Anmeldeinformationen" im Konto, dann wird der indizierte Katalog beim Cloud-Anbieter gespeichert, genau wie bei einem in der Cloud bereitgestellten Konsolenagenten. (Wenn Sie über beide Anmeldeinformationen verfügen, ist

AWS standardmäßig ausgewählt.)

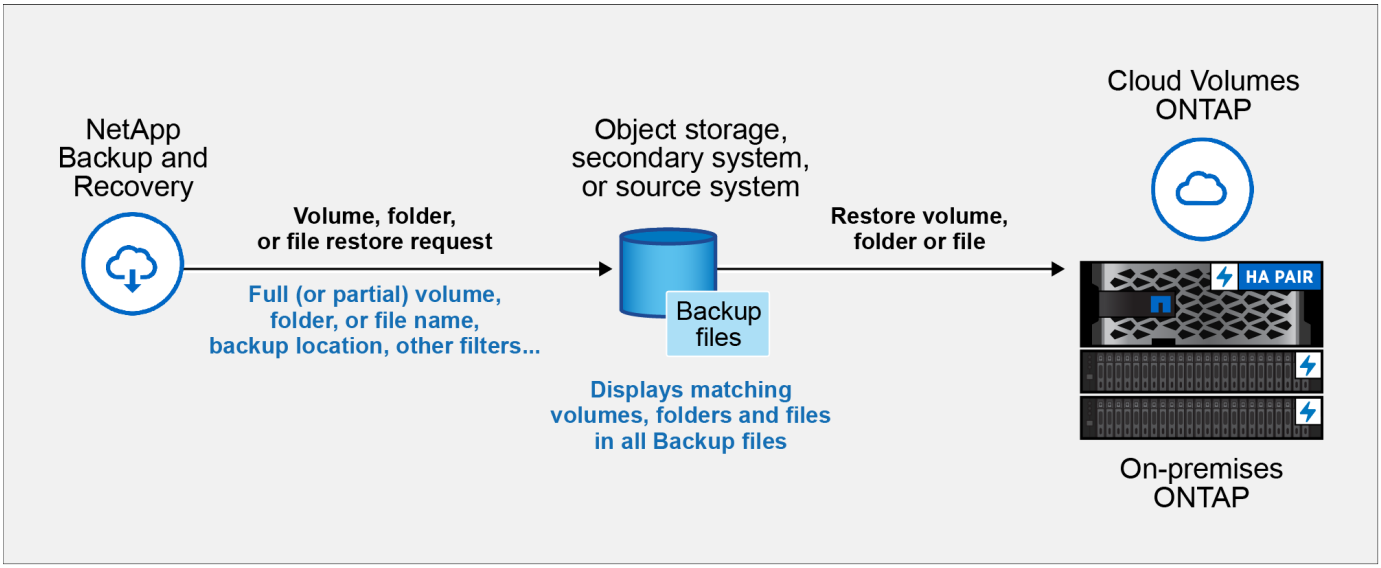
Auch wenn Sie einen lokalen Konsolen-Agenten verwenden, müssen die Anforderungen des Cloud-Anbieters sowohl für die Berechtigungen des Konsolen-Agenten als auch für die Ressourcen des Cloud-Anbieters erfüllt sein. Beachten Sie bei Verwendung dieser Implementierung die oben aufgeführten AWS- und Azure-Anforderungen.

Such- und Wiederherstellungsprozess

Der Vorgang läuft folgendermaßen ab:

1. Bevor Sie „Suchen und Wiederherstellen“ verwenden können, müssen Sie die „Indizierung“ auf jedem Quellsystem aktivieren, von dem Sie Volumedaten wiederherstellen möchten. Dadurch kann der indizierte Katalog die Sicherungsdateien für jedes Volume verfolgen.
2. Wenn Sie ein Volume oder Dateien aus einer Volumesicherung wiederherstellen möchten, wählen Sie unter *Suchen und Wiederherstellen* die Option **Suchen und Wiederherstellen**.
3. Geben Sie die Suchkriterien für ein Volume, einen Ordner oder eine Datei nach teilweisem oder vollständigem Volumenamen, teilweisem oder vollständigem Dateinamen, Sicherungsspeicherort, Größenbereich, Erstellungsdatumsbereich und anderen Suchfiltern ein und wählen Sie **Suchen**.

   Auf der Seite „Suchergebnisse“ werden alle Speicherorte angezeigt, die über eine Datei oder ein Volume verfügen, das Ihren Suchkriterien entspricht.
4. Wählen Sie **Alle Sicherungen anzeigen** für den Speicherort, den Sie zum Wiederherstellen des Volumes oder der Datei verwenden möchten, und wählen Sie dann **Wiederherstellen** für die tatsächliche Sicherungsdatei, die Sie verwenden möchten.
5. Wählen Sie den Speicherort aus, an dem das Volume, der Ordner oder die Datei(en) wiederhergestellt werden sollen, und wählen Sie **Wiederherstellen**.
6. Das Volume, der Ordner oder die Datei(en) werden wiederhergestellt.



Sie müssen nur einen Teil des Namens kennen, und NetApp Backup and Recovery durchsucht alle Sicherungsdateien, die Ihrer Suche entsprechen.

Aktivieren Sie den indizierten Katalog für jedes System

Bevor Sie „Suchen und Wiederherstellen“ verwenden können, müssen Sie die „Indizierung“ auf jedem Quellsystem aktivieren, von dem Sie Volumes oder Dateien wiederherstellen möchten. Dadurch kann der indizierte Katalog jedes Volume und jede Sicherungsdatei verfolgen – und Ihre Suchvorgänge werden dadurch sehr schnell und effizient.

Der indizierte Katalog ist eine Datenbank, die Metadaten zu allen Volumes und Sicherungsdateien in Ihrem System speichert. Es wird von der Such- und Wiederherstellungsfunktion verwendet, um schnell die Sicherungsdateien zu finden, die die Daten enthalten, die Sie wiederherstellen möchten.

Funktionen des Indexkatalogs

NetApp Backup and Recovery stellt keinen separaten Bucket bereit, wenn Sie den Indexed Catalog verwenden. Stattdessen stellt der Dienst für in AWS, Azure, Google Cloud Platform, StorageGRID oder ONTAP S3 gespeicherte Backups Speicherplatz auf dem Konsolenagenten oder in der Umgebung des Cloud-Anbieters bereit.

Der Indexkatalog unterstützt Folgendes:

- Globale Sucheffizienz in weniger als 3 Minuten
- Bis zu 5 Milliarden Dateien
- Bis zu 5000 Volumes pro Cluster
- Bis zu 100.000 Snapshots pro Volume
- Die maximale Zeit für die Basisindexierung beträgt weniger als 7 Tage. Die tatsächliche Zeit hängt von Ihrer Umgebung ab.

Schritte zum Aktivieren der Indizierung für ein System:

Wenn die Indizierung für Ihr System bereits aktiviert wurde, fahren Sie mit dem nächsten Abschnitt fort, um Ihre Daten wiederherzustellen.

Zuerst müssen Sie ein separates Volume einbinden, um die Katalogdateien aufzunehmen. Dadurch wird ein Datenverlust verhindert, falls die Größe der Dateien, die die Snapshots enthalten, zu groß wird. Dies ist nicht auf jedem Cluster erforderlich; Sie können ein beliebiges Volume von einem beliebigen Cluster in Ihrer Umgebung einbinden. Wenn Sie dies nicht tun, funktioniert die Indizierung möglicherweise nicht richtig.

Für das Einbauvolumen sind folgende Größenrichtlinien zu beachten:

- Verwenden Sie ein NetApp NFS-Volume
- Empfohlener AFF Speicher mit einer Festplattendurchsatzrate von 300 MB/s. Geringerer Durchsatz wird sich auf die Suche und andere Vorgänge auswirken.
- Aktivieren Sie NetApp Snapshots, um zusätzlich zu den Katalog-Backup-ZIP-Dateien auch die Katalogmetadaten zu sichern.
- 50 GB pro 1 Milliarde Dateien
- 20 GB für die Katalogdaten mit zusätzlichem Speicherplatz für die Erstellung von ZIP-Dateien und temporären Dateien

Schritt zum Einbinden des Volumes, um den Katalog neu zu indizieren

1. Montieren Sie das Volumen an `/opt/application/netapp/cbs` durch Eingabe des folgenden Befehls, wobei:

    ◦ `volume name` ist das Volume auf dem Cluster, auf dem die Katalogdateien gespeichert werden.

- `/opt/application/netapp/cbs` ist der Weg, auf dem es montiert wird.

```
mount <cluster IP address>:/<volume name> /opt/application/netapp/cbs
```

Beispiel:

```
mount 10.192.24.17:/CATALOG_SCALE_234 /opt/application/netapp/cbs
```

Schritte zur Aktivierung des Index

1. Führen Sie einen der folgenden Schritte aus:
   - Wenn keine Systeme indiziert wurden, wählen Sie im Wiederherstellungs-Dashboard unter *Suchen und Wiederherstellen* die Option **Indizierung für Systeme aktivieren**.
   - Wenn mindestens ein System bereits indiziert wurde, wählen Sie im Wiederherstellungs-Dashboard unter *Suchen und Wiederherstellen* die Option **Indizierungseinstellungen** aus.
2. Wählen Sie **Indizierung aktivieren** für das System.

Ergebnis

Nachdem alle Dienste bereitgestellt und der indizierte Katalog aktiviert wurde, wird das System als „Aktiv“ angezeigt.

Abhängig von der Größe der Volumes im System und der Anzahl der Sicherungsdateien an allen drei Sicherungsorten kann der anfängliche Indizierungsprozess bis zu einer Stunde dauern. Danach wird es stündlich transparent mit inkrementellen Änderungen aktualisiert, um auf dem neuesten Stand zu bleiben.

Wiederherstellen von Volumes, Ordnern und Dateien mit „Suchen und Wiederherstellen“

Nachdem SieAktivierte Indizierung für Ihr System können Sie Volumes, Ordner und Dateien mithilfe von „Suchen und Wiederherstellen“ wiederherstellen. Auf diese Weise können Sie eine breite Palette von Filtern verwenden, um aus allen Sicherungsdateien genau die Datei oder das Volume zu finden, das Sie wiederherstellen möchten.

Schritte

1. Wählen Sie im Konsolenmenü **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie die Registerkarte **Wiederherstellen** und das Wiederherstellungs-Dashboard wird angezeigt.
3. Wählen Sie im Abschnitt „Suchen und Wiederherstellen“ die Option „Suchen und Wiederherstellen“ aus.
4. Wählen Sie im Abschnitt „Suchen und Wiederherstellen“ die Option „Suchen und Wiederherstellen“ aus.
5. Auf der Seite „Suchen und Wiederherstellen“:
   a. Geben Sie in der Suchleiste einen vollständigen oder teilweisen Datenträgernamen, Ordnernamen oder Dateinamen ein.
   b. Wählen Sie den Ressourcentyp aus: **Volumes**, **Dateien**, **Ordner** oder **Alle**.
   c. Wählen Sie im Bereich *Filtern nach* die Filterkriterien aus. Sie können beispielsweise das System auswählen, auf dem sich die Daten befinden, und den Dateityp, beispielsweise eine JPEG-Datei. Alternativ können Sie den Typ des Sicherungsspeicherorts auswählen, wenn Sie die Ergebnisse nur in verfügbaren Snapshots oder Sicherungsdateien im Objektspeicher suchen möchten.

6. Wählen Sie **Suchen** und im Bereich „Suchergebnisse“ werden alle Ressourcen angezeigt, die über eine Datei, einen Ordner oder ein Volume verfügen, das Ihrer Suche entspricht.
7. Suchen Sie die Ressource mit den Daten, die Sie wiederherstellen möchten, und wählen Sie **Alle Sicherungen anzeigen** aus, um alle Sicherungsdateien anzuzeigen, die das entsprechende Volume, den entsprechenden Ordner oder die entsprechende Datei enthalten.
8. Suchen Sie die Sicherungsdatei, die Sie zum Wiederherstellen der Daten verwenden möchten, und wählen Sie **Wiederherstellen**.

   Beachten Sie, dass die Ergebnisse lokale Volume-Snapshots und Remote-Replicated-Volumes identifizieren, die die in Ihrer Suche enthaltene Datei enthalten. Sie können die Wiederherstellung entweder aus der Cloud-Sicherungsdatei, aus dem Snapshot oder aus dem replizierten Volume durchführen.

9. Wählen Sie den Zielspeicherort aus, an dem das Volume, der Ordner oder die Datei(en) wiederhergestellt werden sollen, und wählen Sie **Wiederherstellen**.
   - Für Volumes können Sie das ursprüngliche Zielsystem oder ein alternatives System auswählen. Beim Wiederherstellen eines FlexGroup -Volumes müssen Sie mehrere Aggregate auswählen.
   - Bei Ordnern können Sie den ursprünglichen Speicherort wiederherstellen oder einen alternativen Speicherort auswählen, einschließlich System, Volume und Ordner.
   - Sie können Dateien am ursprünglichen Speicherort wiederherstellen oder einen alternativen Speicherort auswählen, einschließlich System, Volume und Ordner. Bei der Auswahl des ursprünglichen Speicherorts können Sie wählen, ob die Quelldatei(en) überschrieben oder neue Dateien erstellt werden sollen.

     Wenn Sie ein lokales ONTAP -System auswählen und die Clusterverbindung zum Objektspeicher noch nicht konfiguriert haben, werden Sie zur Eingabe zusätzlicher Informationen aufgefordert:

     - Wählen Sie beim Wiederherstellen von Amazon S3 den IPspace im ONTAP Cluster aus, in dem sich das Zielvolume befinden soll, geben Sie den Zugriffsschlüssel und den geheimen Schlüssel für den Benutzer ein, den Sie erstellt haben, um dem ONTAP Cluster Zugriff auf den S3-Bucket zu gewähren, und wählen Sie optional einen privaten VPC-Endpunkt für die sichere Datenübertragung. "Details zu diesen Anforderungen anzeigen".
     - Wählen Sie beim Wiederherstellen aus Azure Blob den IPspace im ONTAP Cluster aus, in dem sich das Zielvolume befinden soll, und wählen Sie optional einen privaten Endpunkt für die sichere Datenübertragung, indem Sie das VNet und das Subnetz auswählen. "Details zu diesen Anforderungen anzeigen".
     - Wählen Sie beim Wiederherstellen aus Google Cloud Storage den IPspace im ONTAP Cluster aus, in dem sich das Zielvolume befinden wird, sowie den Zugriffsschlüssel und den geheimen Schlüssel für den Zugriff auf den Objektspeicher. "Details zu diesen Anforderungen anzeigen".
     - Geben Sie beim Wiederherstellen von StorageGRID den FQDN des StorageGRID -Servers und den Port ein, den ONTAP für die HTTPS-Kommunikation mit StorageGRID verwenden soll, geben Sie den für den Zugriff auf den Objektspeicher erforderlichen Zugriffsschlüssel und Geheimschlüssel sowie den IP-Bereich im ONTAP -Cluster ein, in dem sich das Zielvolume befindet. "Details zu diesen Anforderungen anzeigen".
     - Geben Sie beim Wiederherstellen von ONTAP S3 den FQDN des ONTAP S3-Servers und den Port ein, den ONTAP für die HTTPS-Kommunikation mit ONTAP S3 verwenden soll, wählen Sie den für den Zugriff auf den Objektspeicher erforderlichen Zugriffsschlüssel und Geheimschlüssel sowie den IP-Bereich im ONTAP Cluster aus, in dem sich das Zielvolume befinden wird. "Details zu diesen Anforderungen anzeigen".

Ergebnisse

Das Volume, der Ordner oder die Datei(en) werden wiederhergestellt und Sie werden zum Wiederherstellungs-Dashboard zurückgeleitet, damit Sie den Fortschritt des Wiederherstellungsvorgangs überprüfen können. Sie können auch die Registerkarte **Jobüberwachung** auswählen, um den Wiederherstellungsfortschritt anzuzeigen. Sehen"Job-Monitor-Seite" .

Wiederherstellen von ONTAP -Daten mithilfe von „Durchsuchen und Wiederherstellen“

Mit NetApp Backup and Recovery können Sie ONTAP Daten über die Funktion „Durchsuchen & Wiederherstellen“ wiederherstellen. Notieren Sie sich vor der Wiederherstellung den Namen des Quellvolumes, das Quellsystem und die SVM sowie das Datum der Sicherungsdatei. Sie können ONTAP Daten aus einem Snapshot, einem replizierten Volume oder aus in Objektspeichern gespeicherten Backups wiederherstellen.

Die Wiederherstellungsmöglichkeiten hängen von Ihrer ONTAP Version ab:

- **Ordner:** Mit ONTAP 9.13.0 oder höher können Sie Ordner mit allen Dateien und Unterordnern wiederherstellen; mit früheren Versionen können Sie nur die Dateien im Ordner wiederherstellen.
- **Archivspeicher:** Die Wiederherstellung aus dem Archivspeicher (verfügbar ab ONTAP 9.10.1) ist langsamer und kann zusätzliche Kosten verursachen.
- **Anforderungen an den Destination Cluster:**
  - Volumenwiederherstellung: ONTAP 9.10.1 oder höher
  - Dateiwiederherstellung: ONTAP 9.11.1 oder höher
  - Google Archive and StorageGRID: ONTAP 9.12.1 oder höher
  - Ordnerwiederherstellung: ONTAP 9.13.1 oder höher

"Erfahren Sie mehr über die Wiederherstellung aus dem AWS-Archivspeicher"Die "Weitere Informationen zur Wiederherstellung aus dem Azure-Archivspeicher"Die "Erfahren Sie mehr über die Wiederherstellung aus dem Google-Archivspeicher"Die

Die hohe Priorität wird beim Wiederherstellen von Daten aus dem Azure-Archivspeicher auf StorageGRID -Systemen nicht unterstützt.

Durchsuchen und Wiederherstellen unterstützter Systeme und Objektspeicheranbieter

Sie können ONTAP Daten aus einer Sicherungsdatei, die sich in einem sekundären System (einem replizierten Volume) oder im Objektspeicher (einer Sicherungsdatei) befindet, auf den folgenden Systemen wiederherstellen. Snapshots befinden sich auf dem Quellsystem und können nur auf demselben System wiederhergestellt werden.

Hinweis: Sie können ein Volume aus jeder Art von Sicherungsdatei wiederherstellen, einen Ordner oder einzelne Dateien können Sie derzeit jedoch nur aus einer Sicherungsdatei im Objektspeicher wiederherstellen.

Aus dem Objektspeicher (Backup)	Vom Primär (Schnappschuss)	Vom sekundären System (Replikation)	Zum Zielsystem
Amazon S3	Cloud Volumes ONTAP in AWS On-Premises-ONTAP -System	Cloud Volumes ONTAP in AWS On-Premises-ONTAP -System	Azure-Blob

Aus dem Objektspeicher (Backup)	Vom Primär (Schnappschuss)	Vom sekundären System (Replikation)	Zum Zielsystem
Cloud Volumes ONTAP in Azure On-Premises-ONTAP -System	Cloud Volumes ONTAP in Azure On-Premises-ONTAP -System	Google Cloud-Speicher	Cloud Volumes ONTAP im lokalen ONTAP -System von Google
Cloud Volumes ONTAP im lokalen ONTAP -System von Google	NetApp StorageGRID	On-Premises- ONTAP -System	On-Premises- ONTAP -System Cloud Volumes ONTAP
Zum lokalen ONTAP -System	ONTAP S3	On-Premises- ONTAP -System	On-Premises- ONTAP -System Cloud Volumes ONTAP

Für „Durchsuchen und Wiederherstellen“ kann der Konsolenagent an den folgenden Speicherorten installiert werden:

- Für Amazon S3 kann der Konsolenagent in AWS oder in Ihren Räumlichkeiten bereitgestellt werden
- Für Azure Blob kann der Konsolenagent in Azure oder in Ihren Räumlichkeiten bereitgestellt werden
- Für Google Cloud Storage muss der Konsolenagent in Ihrem Google Cloud Platform VPC bereitgestellt werden
- Für StorageGRID muss der Konsolenagent in Ihren Räumlichkeiten bereitgestellt werden; mit oder ohne Internetzugang
- Für ONTAP S3 kann der Konsolenagent in Ihren Räumlichkeiten (mit oder ohne Internetzugang) oder in einer Cloud-Provider-Umgebung bereitgestellt werden

Beachten Sie, dass Verweise auf „On-Premises ONTAP Systeme“ FAS, AFF und ONTAP Select Systeme umfassen.

Wenn die ONTAP Version auf Ihrem System niedriger als 9.13.1 ist, können Sie keine Ordner oder Dateien wiederherstellen, wenn die Sicherungsdatei mit DataLock & Ransomware konfiguriert wurde. In diesem Fall können Sie das gesamte Volume aus der Sicherungsdatei wiederherstellen und dann auf die benötigten Dateien zugreifen.

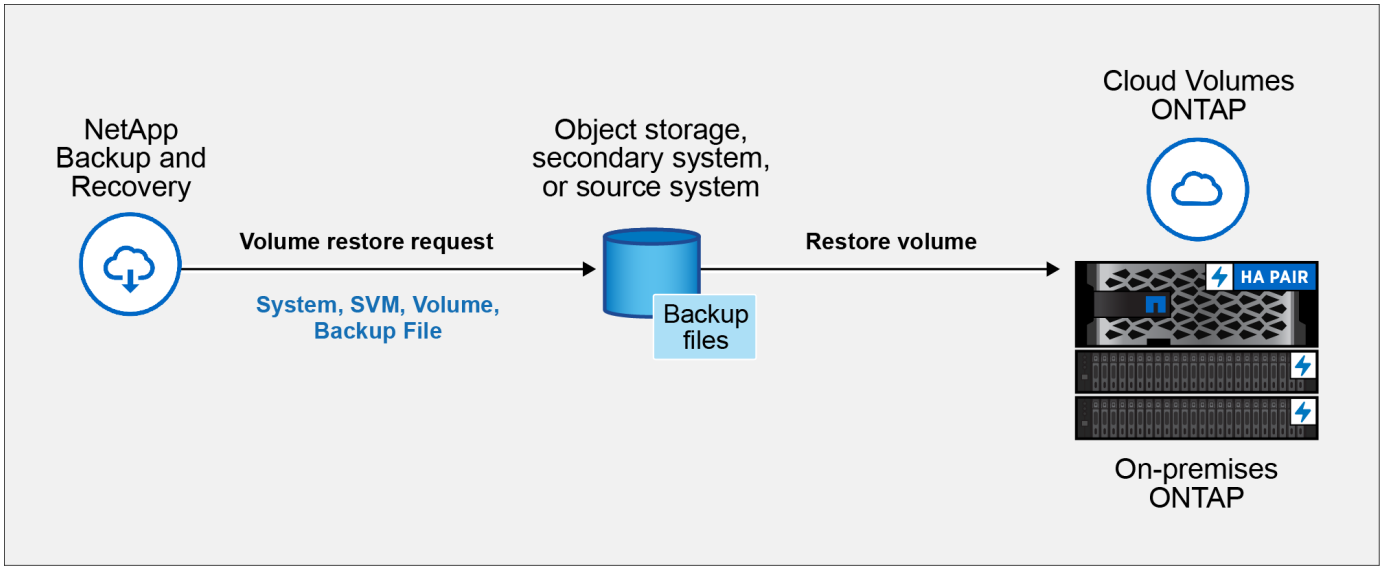
Wiederherstellen von Volumes mithilfe von „Durchsuchen und Wiederherstellen“

Wenn Sie ein Volume aus einer Sicherungsdatei wiederherstellen, erstellt NetApp Backup and Recovery mithilfe der Daten aus der Sicherung ein *neues* Volume. Wenn Sie ein Backup aus dem Objektspeicher verwenden, können Sie die Daten auf einem Volume im Originalsystem, auf einem anderen System, das sich im selben Cloud-Konto wie das Quellsystem befindet, oder auf einem lokalen ONTAP -System wiederherstellen.

Wenn Sie ein Cloud-Backup auf einem Cloud Volumes ONTAP -System mit ONTAP 9.13.0 oder höher oder auf einem lokalen ONTAP System mit ONTAP 9.14.1 wiederherstellen, haben Sie die Möglichkeit, eine *schnelle Wiederherstellung* durchzuführen. Die schnelle Wiederherstellung ist ideal für Notfallwiederherstellungssituationen, in denen Sie so schnell wie möglich Zugriff auf ein Volume bereitstellen müssen. Bei einer schnellen Wiederherstellung werden die Metadaten aus der Sicherungsdatei auf einem Volume wiederhergestellt, anstatt die gesamte Sicherungsdatei wiederherzustellen. Die schnelle Wiederherstellung wird für leistungs- oder latenzempfindliche Anwendungen nicht empfohlen und wird bei Sicherungen im Archivspeicher nicht unterstützt.

Die schnelle Wiederherstellung wird für FlexGroup -Volumes nur unterstützt, wenn auf dem Quellsystem, von dem das Cloud-Backup erstellt wurde, ONTAP 9.12.1 oder höher ausgeführt wurde. Und es wird für SnapLock -Volumes nur unterstützt, wenn auf dem Quellsystem ONTAP 9.11.0 oder höher ausgeführt wurde.

Bei der Wiederherstellung von einem replizierten Volume können Sie das Volume auf dem ursprünglichen System oder auf einem Cloud Volumes ONTAP oder On-Premises ONTAP -System wiederherstellen.



Um ein Volume wiederherzustellen, benötigen Sie den Namen des Quellsystems, die Speicher-VM, den Volume-Namen und das Datum der Sicherungsdatei.

Schritte

1. Wählen Sie im Konsolenmenü **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie die Registerkarte **Wiederherstellen** und das Wiederherstellungs-Dashboard wird angezeigt.
3. Wählen Sie im Abschnitt „Durchsuchen und Wiederherstellen“ die Option „Volume wiederherstellen“ aus.
4. Navigieren Sie auf der Seite „Quelle auswählen“ zur Sicherungsdatei für das Volume, das Sie wiederherstellen möchten. Wählen Sie das **System**, das **Volume** und die **Sicherungsdatei** mit dem Datums-/Zeitstempel aus, von dem Sie wiederherstellen möchten.

   Die Spalte **Speicherort** zeigt an, ob die Sicherungsdatei (Snapshot) **lokal** (ein Snapshot auf dem Quellsystem), **sekundär** (ein repliziertes Volume auf einem sekundären ONTAP System) oder **Objektspeicher** (eine Sicherungsdatei im Objektspeicher) ist. Wählen Sie die Datei aus, die Sie wiederherstellen möchten.

5. Wählen Sie **Weiter**.

   Beachten Sie: Wenn Sie eine Sicherungsdatei im Objektspeicher auswählen und Ransomware Resilience für diese Sicherung aktiv ist (wenn Sie DataLock und Ransomware Resilience in der Sicherungsrichtlinie aktiviert haben), werden Sie aufgefordert, vor der Wiederherstellung der Daten einen zusätzlichen Ransomware-Scan für die Sicherungsdatei auszuführen. Wir empfehlen Ihnen, die Sicherungsdatei auf Ransomware zu scannen. (Für den Zugriff auf den Inhalt der Sicherungsdatei fallen bei Ihrem Cloud-Anbieter zusätzliche Kosten für den Datenverkehr an.)

6. Wählen Sie auf der Seite „Ziel auswählen“ das **System** aus, auf dem Sie das Volume wiederherstellen möchten.

7. Wenn Sie beim Wiederherstellen einer Sicherungsdatei aus dem Objektspeicher ein lokales ONTAP -System auswählen und die Clusterverbindung zum Objektspeicher noch nicht konfiguriert haben, werden Sie zur Eingabe zusätzlicher Informationen aufgefordert:
    - Wählen Sie beim Wiederherstellen von Amazon S3 den IPspace im ONTAP Cluster aus, in dem sich das Zielvolume befinden soll, geben Sie den Zugriffsschlüssel und den geheimen Schlüssel für den Benutzer ein, den Sie erstellt haben, um dem ONTAP Cluster Zugriff auf den S3-Bucket zu gewähren, und wählen Sie optional einen privaten VPC-Endpunkt für die sichere Datenübertragung.
    - Wählen Sie beim Wiederherstellen aus Azure Blob den IPspace im ONTAP Cluster aus, in dem sich das Zielvolume befinden soll, wählen Sie das Azure-Abonnement für den Zugriff auf den Objektspeicher aus und wählen Sie optional einen privaten Endpunkt für die sichere Datenübertragung, indem Sie das VNet und das Subnetz auswählen.
    - Wählen Sie beim Wiederherstellen aus Google Cloud Storage das Google Cloud-Projekt sowie den Zugriffsschlüssel und den geheimen Schlüssel aus, um auf den Objektspeicher, die Region, in der die Sicherungen gespeichert sind, und den IP-Bereich im ONTAP Cluster zuzugreifen, in dem sich das Zielvolume befinden wird.
    - Geben Sie beim Wiederherstellen von StorageGRID den FQDN des StorageGRID -Servers und den Port ein, den ONTAP für die HTTPS-Kommunikation mit StorageGRID verwenden soll, wählen Sie den für den Zugriff auf den Objektspeicher erforderlichen Zugriffsschlüssel und Geheimschlüssel sowie den IP-Bereich im ONTAP Cluster aus, in dem sich das Zielvolume befinden wird.
    - Geben Sie beim Wiederherstellen von ONTAP S3 den FQDN des ONTAP S3-Servers und den Port ein, den ONTAP für die HTTPS-Kommunikation mit ONTAP S3 verwenden soll, wählen Sie den für den Zugriff auf den Objektspeicher erforderlichen Zugriffsschlüssel und Geheimschlüssel sowie den IP-Bereich im ONTAP Cluster aus, in dem sich das Zielvolume befinden wird.
8. Geben Sie den Namen ein, den Sie für das wiederhergestellte Volume verwenden möchten, und wählen Sie die Speicher-VM und das Aggregat aus, in dem sich das Volume befinden soll. Beim Wiederherstellen eines FlexGroup -Volumes müssen Sie mehrere Aggregate auswählen. Standardmäßig wird **<source_volume_name>_restore** als Volumename verwendet.

    Wenn Sie ein Backup vom Objektspeicher auf einem Cloud Volumes ONTAP -System mit ONTAP 9.13.0 oder höher oder auf einem lokalen ONTAP System mit ONTAP 9.14.1 wiederherstellen, haben Sie die Möglichkeit, eine *schnelle Wiederherstellung* durchzuführen.

    Und wenn Sie das Volume aus einer Sicherungsdatei wiederherstellen, die sich in einer Archivspeicherebene befindet (verfügbar ab ONTAP 9.10.1), können Sie die Wiederherstellungspriorität auswählen.

    "Erfahren Sie mehr über die Wiederherstellung aus dem AWS-Archivspeicher". "Weitere Informationen zur Wiederherstellung aus dem Azure-Archivspeicher". "Erfahren Sie mehr über die Wiederherstellung aus dem Google-Archivspeicher". Sicherungsdateien in der Speicherebene des Google-Archivs werden fast sofort wiederhergestellt und erfordern keine Wiederherstellungspriorität.

9. Wählen Sie **Weiter**, um auszuwählen, ob Sie eine normale Wiederherstellung oder eine schnelle Wiederherstellung durchführen möchten:
    - **Normale Wiederherstellung**: Verwenden Sie die normale Wiederherstellung auf Volumes, die eine hohe Leistung erfordern. Die Volumes sind erst verfügbar, wenn der Wiederherstellungsvorgang abgeschlossen ist.
    - **Schnelle Wiederherstellung**: Wiederhergestellte Volumes und Daten sind sofort verfügbar. Verwenden Sie dies nicht auf Volumes, die eine hohe Leistung erfordern, da der Zugriff auf die Daten während des schnellen Wiederherstellungsprozesses langsamer als gewöhnlich sein kann.
10. Wählen Sie **Wiederherstellen** und Sie kehren zum Wiederherstellungs-Dashboard zurück, damit Sie den

Fortschritt des Wiederherstellungsvorgangs überprüfen können.

Ergebnis

NetApp Backup and Recovery erstellt basierend auf dem von Ihnen ausgewählten Backup ein neues Volume.

Beachten Sie, dass die Wiederherstellung eines Volumes aus einer Sicherungsdatei, die sich im Archivspeicher befindet, je nach Archivebene und Wiederherstellungspriorität viele Minuten oder Stunden dauern kann. Sie können die Registerkarte **Jobüberwachung** auswählen, um den Wiederherstellungsfortschritt anzuzeigen.

Stellen Sie Ordner und Dateien mit „Durchsuchen und Wiederherstellen“ wieder her

Wenn Sie nur einige Dateien aus einer ONTAP Volume-Sicherung wiederherstellen müssen, können Sie anstelle der Wiederherstellung des gesamten Volumes einen Ordner oder einzelne Dateien wiederherstellen. Sie können Ordner und Dateien auf einem vorhandenen Volume im ursprünglichen System oder auf einem anderen System wiederherstellen, das dasselbe Cloud-Konto verwendet. Sie können Ordner und Dateien auch auf einem Volume auf einem lokalen ONTAP System wiederherstellen.

Sie können einen Ordner oder einzelne Dateien derzeit nur aus einer Sicherungsdatei im Objektspeicher wiederherstellen. Das Wiederherstellen von Dateien und Ordnern aus einem lokalen Snapshot oder aus einer Sicherungsdatei, die sich auf einem sekundären System (einem replizierten Volume) befindet, wird derzeit nicht unterstützt.

Wenn Sie mehrere Dateien auswählen, werden diese auf demselben Zielvolume wiederhergestellt. Um Dateien auf verschiedenen Datenträgern wiederherzustellen, führen Sie den Vorgang mehrmals aus.

Wenn Sie ONTAP 9.13.0 oder höher verwenden, können Sie einen Ordner zusammen mit allen darin enthaltenen Dateien und Unterordnern wiederherstellen. Wenn Sie eine ONTAP -Version vor 9.13.0 verwenden, werden nur Dateien aus diesem Ordner wiederhergestellt – keine Unterordner oder Dateien in Unterordnern.

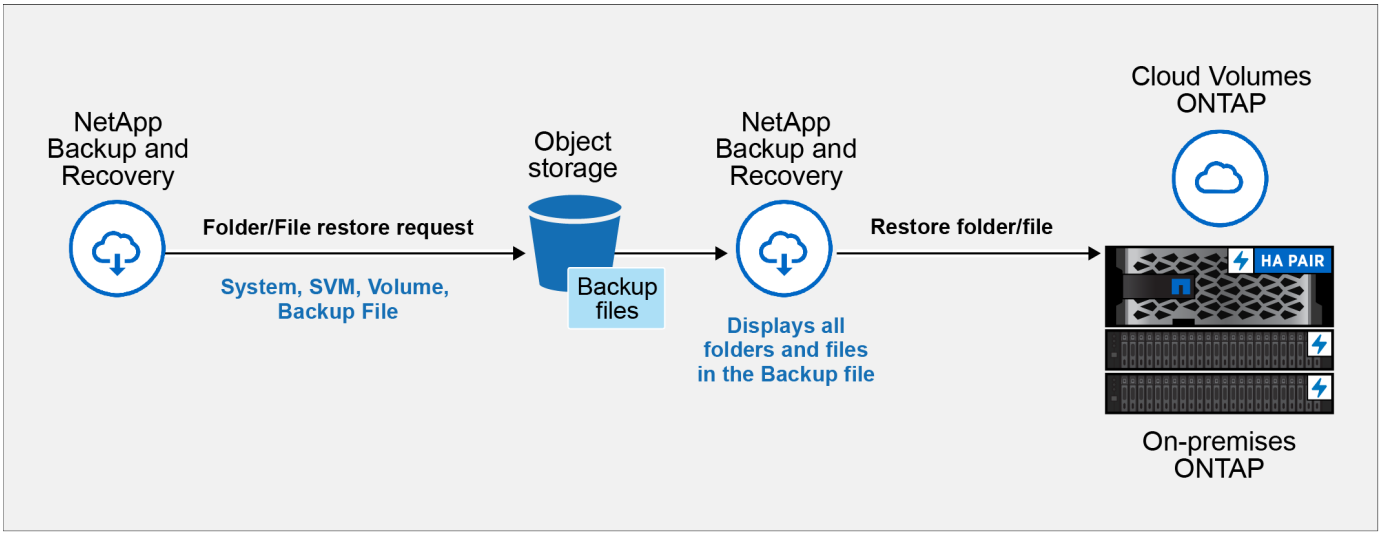
- Wenn die Sicherungsdatei mit DataLock- und Ransomware-Schutz konfiguriert wurde, wird die Wiederherstellung auf Ordnerebene nur unterstützt, wenn die ONTAP -Version 9.13.1 oder höher ist. Wenn Sie eine frühere Version von ONTAP verwenden, können Sie das gesamte Volume aus der Sicherungsdatei wiederherstellen und dann auf die benötigten Ordner und Dateien zugreifen.
- Wenn sich die Sicherungsdatei im Archivspeicher befindet, wird die Wiederherstellung auf Ordnerebene nur unterstützt, wenn die ONTAP Version 9.13.1 oder höher ist. Wenn Sie eine frühere Version von ONTAP verwenden, können Sie den Ordner aus einer neueren, nicht archivierten Sicherungsdatei wiederherstellen oder das gesamte Volume aus der archivierten Sicherung wiederherstellen und dann auf den benötigten Ordner und die benötigten Dateien zugreifen.
- Mit ONTAP 9.15.1 können Sie FlexGroup -Ordner mit der Option „Durchsuchen und wiederherstellen“ wiederherstellen. Diese Funktion befindet sich im Technologievorschaumodus.

  Sie können es mit einem speziellen Flag testen, das im "Blog zur NetApp Backup and Recovery Version vom Juli 2024" .

Ordner und Dateien wiederherstellen

Befolgen Sie diese Schritte, um Ordner oder Dateien aus einer ONTAP Volume-Sicherung auf einem Volume

wiederherzustellen. Sie sollten den Namen des Datenträgers und das Datum der Sicherungsdatei kennen, die Sie zum Wiederherstellen des Ordners oder der Datei(en) verwenden möchten. Diese Funktion verwendet Live Browsing, sodass Sie die Liste der Verzeichnisse und Dateien in jeder Sicherungsdatei anzeigen können.



Bevor Sie beginnen

- Die ONTAP Version muss 9.6 oder höher sein, um Dateiwiederherstellungsvorgänge durchführen zu können.
- Die ONTAP Version muss 9.11.1 oder höher sein, um *Ordner*-Wiederherstellungsvorgänge durchführen zu können. ONTAP Version 9.13.1 ist erforderlich, wenn sich die Daten im Archivspeicher befinden oder wenn die Sicherungsdatei DataLock- und Ransomware-Schutz verwendet.
- Die ONTAP Version muss 9.15.1 p2 oder höher sein, um FlexGroup -Verzeichnisse mit der Option „Durchsuchen und wiederherstellen“ wiederherzustellen.

Schritte

1. Wählen Sie im Konsolenmenü **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie die Registerkarte **Wiederherstellen** und das Wiederherstellungs-Dashboard wird angezeigt.
3. Wählen Sie im Abschnitt „Durchsuchen und Wiederherstellen“ die Option „Dateien oder Ordner wiederherstellen“ aus.
4. Navigieren Sie auf der Seite „Quelle auswählen“ zur Sicherungsdatei für das Volume, das den Ordner oder die Dateien enthält, die Sie wiederherstellen möchten. Wählen Sie das **System**, das **Volume** und das **Backup** mit dem Datums-/Zeitstempel aus, aus dem Sie Dateien wiederherstellen möchten.
5. Wählen Sie **Weiter** und die Liste der Ordner und Dateien aus der Volume-Sicherung wird angezeigt.

   Wenn Sie Ordner oder Dateien aus einer Sicherungsdatei wiederherstellen, die sich in einer Archivspeicherebene befindet, können Sie die Wiederherstellungspriorität auswählen.

   "Erfahren Sie mehr über die Wiederherstellung aus dem AWS-Archivspeicher". "Weitere Informationen zur Wiederherstellung aus dem Azure-Archivspeicher". "Erfahren Sie mehr über die Wiederherstellung aus dem Google-Archivspeicher". Sicherungsdateien in der Speicherebene des Google-Archivs werden fast sofort wiederhergestellt und erfordern keine Wiederherstellungspriorität.

   Und wenn Ransomware Resilience für die Sicherungsdatei aktiv ist (wenn Sie DataLock und Ransomware Resilience in der Sicherungsrichtlinie aktiviert haben), werden Sie aufgefordert, vor der Wiederherstellung der Daten einen zusätzlichen Ransomware-Scan für die Sicherungsdatei auszuführen. Wir empfehlen Ihnen, die Sicherungsdatei auf Ransomware zu scannen. (Für den Zugriff auf den Inhalt der

Sicherungsdatei fallen bei Ihrem Cloud-Anbieter zusätzliche Kosten für den Datenverkehr an.)

6. Wählen Sie auf der Seite „Elemente auswählen“ den Ordner oder die Datei(en) aus, die Sie wiederherstellen möchten, und wählen Sie „Weiter“ aus. So können Sie den Artikel leichter finden:
   - Sie können den Ordner- oder Dateinamen auswählen, wenn Sie ihn sehen.
   - Sie können das Suchsymbol auswählen und den Namen des Ordners oder der Datei eingeben, um direkt zum Element zu navigieren.
   - Sie können in Ordnern mit dem Abwärtspfeil am Ende der Zeile nach unten navigieren, um bestimmte Dateien zu finden.

     Wenn Sie Dateien auswählen, werden diese auf der linken Seite der Seite hinzugefügt, sodass Sie die Dateien sehen können, die Sie bereits ausgewählt haben. Sie können eine Datei bei Bedarf aus dieser Liste entfernen, indem Sie das **x** neben dem Dateinamen auswählen.
7. Wählen Sie auf der Seite „Ziel auswählen“ das **System** aus, auf dem Sie die Elemente wiederherstellen möchten.

   Wenn Sie einen lokalen Cluster auswählen und die Clusterverbindung zum Objektspeicher noch nicht konfiguriert haben, werden Sie zur Eingabe zusätzlicher Informationen aufgefordert:

   - Geben Sie beim Wiederherstellen von Amazon S3 den IPspace im ONTAP Cluster ein, in dem sich das Zielvolume befindet, sowie den AWS-Zugriffsschlüssel und den geheimen Schlüssel, die für den Zugriff auf den Objektspeicher erforderlich sind. Sie können auch eine Private Link-Konfiguration für die Verbindung zum Cluster auswählen.
   - Geben Sie beim Wiederherstellen aus Azure Blob den IPspace im ONTAP Cluster ein, in dem sich das Zielvolume befindet. Sie können auch eine private Endpunktkonfiguration für die Verbindung zum Cluster auswählen.
   - Geben Sie beim Wiederherstellen aus Google Cloud Storage den IP-Bereich im ONTAP Cluster ein, in dem sich die Zielvolumes befinden, sowie den Zugriffsschlüssel und den geheimen Schlüssel, die für den Zugriff auf den Objektspeicher erforderlich sind.
   - Geben Sie beim Wiederherstellen von StorageGRID den FQDN des StorageGRID -Servers und den Port ein, den ONTAP für die HTTPS-Kommunikation mit StorageGRID verwenden soll, geben Sie den für den Zugriff auf den Objektspeicher erforderlichen Zugriffsschlüssel und Geheimschlüssel sowie den IP-Bereich im ONTAP -Cluster ein, in dem sich das Zielvolume befindet.
8. Wählen Sie dann das **Volume** und den **Ordner** aus, in dem Sie den Ordner oder die Datei(en) wiederherstellen möchten.

   Beim Wiederherstellen von Ordnern und Dateien stehen Ihnen einige Optionen für den Speicherort zur Verfügung.

   - Wenn Sie wie oben gezeigt „Zielordner auswählen“ ausgewählt haben:
     - Sie können einen beliebigen Ordner auswählen.
     - Sie können mit der Maus über einen Ordner fahren und am Ende der Zeile klicken, um in die Unterordner zu gelangen, und dann einen Ordner auswählen.
   - Wenn Sie dasselbe Zielsystem und Volume ausgewählt haben, in dem sich der Quellordner/die Quelldatei befand, können Sie „Pfad des Quellordners beibehalten“ auswählen, um den Ordner oder die Datei(en) in demselben Ordner wiederherzustellen, in dem sie in der Quellstruktur vorhanden waren. Alle Ordner und Unterordner müssen bereits vorhanden sein; es werden keine Ordner erstellt. Beim Wiederherstellen von Dateien an ihrem ursprünglichen Speicherort können Sie die Quelldatei(en) überschreiben oder neue Dateien erstellen.

9. Wählen Sie **Wiederherstellen**, um zum Wiederherstellungs-Dashboard zurückzukehren und den Fortschritt des Wiederherstellungsvorgangs zu überprüfen.

Schützen Sie Microsoft SQL Server-Workloads

Schützen Sie Microsoft SQL-Workloads mit NetApp Backup and Recovery – Übersicht

Sichern Sie Ihre Microsoft SQL Server-Anwendungsdaten von lokalen ONTAP -Systemen auf AWS, Azure oder StorageGRID mit NetApp Backup and Recovery. Das System erstellt und speichert automatisch Backups in Ihrem Cloud-Konto und befolgt dabei Ihre Richtlinien. Verwenden Sie eine 3-2-1-Strategie: Bewahren Sie drei Kopien Ihrer Daten auf zwei Speichersystemen und eine Kopie in der Cloud auf.

Zu den Vorteilen des 3-2-1-Ansatzes gehören:

- Mehrere Datenkopien schützen vor internen und externen Cybersicherheitsbedrohungen.
- Die Verwendung unterschiedlicher Medientypen erleichtert Ihnen die Wiederherstellung, wenn ein Typ ausfällt.
- Sie können die Wiederherstellung schnell von der Vor-Ort-Kopie durchführen und die Offsite-Kopien verwenden, wenn die Vor-Ort-Kopie kompromittiert ist.

NetApp Backup and Recovery verwendet NetApp SnapMirror , um Backups zu synchronisieren, indem Snapshots erstellt und an die Backup-Speicherorte übertragen werden.

Zum Schutz Ihrer Daten können Sie Folgendes tun:

- "Konfigurieren Sie zusätzliche Elemente beim Importieren aus SnapCenter"
- "Entdecken Sie Microsoft SQL Server-Workloads und importieren Sie optional SnapCenter -Ressourcen"
- "Sichern Sie Workloads mit lokalen Snapshots auf dem lokalen ONTAP Primärspeicher"
- "Replizieren Sie Workloads auf den sekundären ONTAP -Speicher"
- "Sichern Sie Workloads an einem Objektspeicherort"
- "Sichern Sie Workloads jetzt"
- "Wiederherstellen von Workloads"
- "Klonen von Workloads"
- "Verwalten des Workload-Inventars"
- "Verwalten von Snapshots"

Zum Sichern von Workloads erstellen Sie Richtlinien, die Sicherungs- und Wiederherstellungsvorgänge verwalten. Sehen"Erstellen von Richtlinien" für weitere Informationen.

Unterstützte Sicherungsziele

NetApp Backup and Recovery ermöglicht die Sicherung von Microsoft SQL Server-Instanzen und -Datenbanken von den folgenden Quellsystemen auf die folgenden Sekundärsysteme und Objektspeicher bei öffentlichen und privaten Cloud-Anbietern. Die Snapshots werden auf dem Quellsystem gespeichert.

Quellsystem	Sekundärsystem (Replikation)	Zielobjektspeicher (Backup)
Cloud Volumes ONTAP in AWS	Cloud Volumes ONTAP in AWS On-Premises- ONTAP -System	Amazon S3 ONTAP S3
Cloud Volumes ONTAP in Azure	Cloud Volumes ONTAP in Azure On-Premises- ONTAP -System	Azure Blob ONTAP S3
On-Premises- ONTAP -System	Cloud Volumes ONTAP On-Premises ONTAP -System	Amazon S3 Azure Blob NetApp StorageGRID ONTAP S3
Amazon FSx for NetApp ONTAP	Amazon FSx for NetApp ONTAP	N / A

Unterstützte Wiederherstellungsziele

Sie können Microsoft SQL Server-Instanzen und -Datenbanken aus einer Sicherung, die sich im Primärspeicher oder einem Sekundärsystem (einem replizierten Volume) oder im Objektspeicher (einer Sicherungsdatei) befindet, auf den folgenden Systemen wiederherstellen. Snapshots befinden sich auf dem Quellsystem und können nur auf demselben System wiederhergestellt werden.

Vom Speicherort der Sicherungsdatei		Zum Zielsystem
Objektspeicher (Backup)	**Sekundäres System (Replikation)**	
Amazon S3	Cloud Volumes ONTAP in AWS On-Premises- ONTAP -System	Cloud Volumes im AWS On-Premises ONTAP -System ONTAP S3
Azure-Blob	Cloud Volumes ONTAP in Azure On-Premises- ONTAP -System	Cloud Volumes ONTAP in Azure Lokales ONTAP -System ONTAP S3
StorageGRID	Cloud Volumes ONTAP On-Premises ONTAP -System	On-Premises ONTAP -System ONTAP S3
Amazon FSx for NetApp ONTAP	Amazon FSx for NetApp ONTAP	N / A

Verweise auf „On-Premises ONTAP -Systeme“ umfassen FAS und AFF Systeme.

Voraussetzungen für den Import vom Plug-in-Dienst in NetApp Backup and Recovery

Wenn Sie Ressourcen aus dem SnapCenter Plug-in-Dienst für Microsoft SQL Server in NetApp Backup and Recovery importieren möchten, müssen Sie noch einige weitere Elemente konfigurieren.

Erstellen Sie zuerst Systeme in der NetApp Console

Wenn Sie Ressourcen aus SnapCenter importieren möchten, sollten Sie vor dem Importieren aus SnapCenter zunächst den gesamten lokalen SnapCenter -Clusterspeicher zur Konsolenseite **Systeme** hinzufügen. Dadurch wird sichergestellt, dass Hostressourcen korrekt erkannt und importiert werden können.

Stellen Sie sicher, dass die Hostanforderungen für die Installation des SnapCenter -Plug-Ins erfüllt sind

Um Ressourcen aus dem SnapCenter -Plug-in für Microsoft SQL Server zu importieren, stellen Sie sicher, dass die Hostanforderungen für die Installation des SnapCenter -Plug-ins für Microsoft SQL Server erfüllt sind.

Informieren Sie sich insbesondere über die SnapCenter -Anforderungen in"Voraussetzungen für NetApp Backup and Recovery" .

Deaktivieren Sie die Remote-Einschränkungen der Benutzerkontensteuerung

Deaktivieren Sie vor dem Importieren von Ressourcen aus SnapCenter die Remote-Einschränkungen der Benutzerkontensteuerung (UAC) auf dem SnapCenter Windows-Host. Deaktivieren Sie UAC, wenn Sie ein lokales Administratorkonto verwenden, um eine Remoteverbindung mit dem SnapCenter Server-Host oder dem SQL-Host herzustellen.

Sicherheitsüberlegungen

Berücksichtigen Sie die folgenden Probleme, bevor Sie die Remote-Einschränkungen der Benutzerkontensteuerung deaktivieren:

- Sicherheitsrisiken: Durch die Deaktivierung der Token-Filterung kann Ihr System Sicherheitslücken ausgesetzt sein, insbesondere wenn lokale Administratorkonten von böswilligen Akteuren kompromittiert werden.
- Mit Vorsicht verwenden:
  - Ändern Sie diese Einstellung nur, wenn dies für Ihre Verwaltungsaufgaben unbedingt erforderlich ist.
  - Stellen Sie sicher, dass sichere Passwörter und andere Sicherheitsmaßnahmen zum Schutz der Administratorkonten vorhanden sind.

Alternative Lösungen

- Wenn ein Remote-Verwaltungszugriff erforderlich ist, sollten Sie die Verwendung von Domänenkonten mit entsprechenden Berechtigungen in Betracht ziehen.
- Verwenden Sie sichere Remote-Management-Tools, die den besten Sicherheitspraktiken entsprechen, um Risiken zu minimieren.

Schritte zum Deaktivieren der Remote-Einschränkungen der Benutzerkontensteuerung

1. Ändern Sie die `LocalAccountTokenFilterPolicy` Registrierungsschlüssel auf dem SnapCenter Windows-Host.

   Verwenden Sie dazu eine der folgenden Methoden (Anweisungen folgen):

   - Methode 1: Registrierungseditor
   - Methode 2: PowerShell-Skript

Methode 1: Deaktivieren Sie die Benutzerkontensteuerung mithilfe des Registrierungseditors

Dies ist eine der Methoden, mit denen Sie die Benutzerkontensteuerung deaktivieren können.

Schritte

1. Öffnen Sie den Registrierungseditor auf dem SnapCenter Windows-Host, indem Sie die folgenden Schritte ausführen:
   a. Drücken `Windows+R` , um das Dialogfeld „Ausführen“ zu öffnen.
   b. Typ `regedit` und drücken Sie `Enter` .
2. Navigieren Sie zum Richtlinienschlüssel:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`

3. Erstellen oder ändern Sie die `DWORD` Wert:
   a. Lokalisieren: `LocalAccountTokenFilterPolicy`
   b. Wenn es nicht existiert, erstellen Sie ein neues `DWORD` (32-Bit) Wert mit dem Namen `LocalAccountTokenFilterPolicy` .
4. Die folgenden Werte werden unterstützt. Setzen Sie für dieses Szenario den Wert auf `1` :
   - `0`(Standard): UAC-Remotebeschränkungen sind aktiviert. Lokale Konten verfügen beim Remotezugriff über gefilterte Token.
   - `1`: UAC-Remotebeschränkungen sind deaktiviert. Lokale Konten umgehen die Token-Filterung und verfügen beim Remote-Zugriff über vollständige Administratorrechte.
5. Klicken Sie auf **OK**.
6. Schließen Sie den Registrierungseditor.
7. Starten Sie den SnapCenter Windows-Host neu.

Beispiel einer Registrierungsänderung

In diesem Beispiel wird LocalAccountTokenFilterPolicy auf „1“ gesetzt, wodurch UAC-Remotebeschränkungen deaktiviert werden.

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Sys
tem]

"LocalAccountTokenFilterPolicy"=dword:00000001
```

Methode 2: Deaktivieren der Benutzerkontensteuerung mithilfe eines PowerShell-Skripts

Dies ist eine weitere Methode, mit der Sie die Benutzerkontensteuerung deaktivieren können.

> Das Ausführen von PowerShell-Befehlen mit erhöhten Rechten kann sich auf die Systemeinstellungen auswirken. Stellen Sie sicher, dass Sie die Befehle und ihre Auswirkungen verstehen, bevor Sie sie ausführen.

Schritte

1. Öffnen Sie ein PowerShell-Fenster mit Administratorrechten auf dem SnapCenter Windows-Host:
   a. Klicken Sie auf das Startmenü.
   b. Suchen Sie nach **PowerShell 7** oder **Windows Powershell**.
   c. Klicken Sie mit der rechten Maustaste auf diese Option und wählen Sie **Als Administrator ausführen**.
2. Stellen Sie sicher, dass PowerShell auf Ihrem System installiert ist. Nach der Installation sollte es im **Start** -Menü erscheinen.

   > PowerShell ist standardmäßig in Windows 7 und späteren Versionen enthalten.

3. Um die Remote-Einschränkungen der Benutzerkontensteuerung zu deaktivieren, setzen Sie LocalAccountTokenFilterPolicy auf „1“, indem Sie den folgenden Befehl ausführen:

```
Set-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy" -Value 1 -Type DWord
```

4. Überprüfen Sie, ob der aktuelle Wert auf „1“ eingestellt ist in `LocalAccountTokenFilterPolicy` durch Ausführen von:

```
Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy"
```

   - Wenn der Wert 1 ist, sind UAC-Remotebeschränkungen deaktiviert.
   - Wenn der Wert 0 ist, sind UAC-Remotebeschränkungen aktiviert.

5. Starten Sie Ihren Computer neu, um die Änderungen zu übernehmen.

Beispiele für PowerShell 7-Befehle zum Deaktivieren von UAC-Remotebeschränkungen:

Dieses Beispiel mit dem Wert „1“ zeigt an, dass die UAC-Remotebeschränkungen deaktiviert sind.

```
# Disable UAC remote restrictions

Set-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy" -Value 1 -Type DWord

# Verify the change

Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy"

# Output

LocalAccountTokenFilterPolicy : 1
```

Ermitteln Sie Microsoft SQL Server-Workloads und importieren Sie sie optional aus SnapCenter in NetApp Backup and Recovery.

NetApp Backup and Recovery muss zunächst Microsoft SQL Server-Workloads erkennen, damit Sie den Dienst nutzen können. Sie können optional Sicherungsdaten und Richtlinien aus SnapCenter importieren, wenn Sie SnapCenter bereits installiert haben.

*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 Microsoft SQL Server-Workloads und importieren Sie optional SnapCenter -Ressourcen

Während der Erkennung analysiert NetApp Backup and Recovery Microsoft SQL Server-Instanzen und Datenbanken in Systemen innerhalb Ihres Unternehmens.

NetApp Backup and Recovery bewertet Microsoft SQL Server-Anwendungen. Der Dienst bewertet den aktuellen Schutzstatus einschließlich der bestehenden Backup-Richtlinien, Snapshots sowie Backup- und Wiederherstellungsoptionen.

Die Ermittlung erfolgt auf folgende Weise:

- Wenn Sie bereits über SnapCenter verfügen, importieren Sie SnapCenter -Ressourcen mithilfe der NetApp Backup and Recovery -Benutzeroberfläche in NetApp Backup and Recovery .

> Wenn Sie bereits über SnapCenter verfügen, überprüfen Sie zunächst, ob Sie die Voraussetzungen erfüllt haben, bevor Sie aus SnapCenter importieren. Beispielsweise sollten Sie lokale SnapCenter -Cluster-Speichersysteme zuerst zur NetApp Console hinzufügen, bevor Sie sie aus SnapCenter importieren. Sehen"Voraussetzungen für den Import von Ressourcen aus SnapCenter" .

- Wenn Sie noch kein SnapCenter haben, können Sie Workloads trotzdem ermitteln, indem Sie manuell ein vCenter hinzufügen und die Erkennung durchführen.

Wenn SnapCenter bereits installiert ist, importieren Sie SnapCenter -Ressourcen in NetApp Backup and Recovery

Wenn Sie SnapCenter bereits installiert haben, importieren Sie SnapCenter -Ressourcen mit diesen Schritten in NetApp Backup and Recovery . NetApp Console erkennt Ressourcen, Hosts, Anmeldeinformationen und Zeitpläne von SnapCenter; Sie müssen diese Informationen nicht alle neu erstellen.

Sie können dies auf folgende Weise tun:

- Wählen Sie während der Erkennung eine Option zum Importieren von Ressourcen aus SnapCenter aus.
- Wählen Sie nach der Erkennung auf der Inventarseite eine Option zum Importieren von SnapCenter -Ressourcen aus.
- Wählen Sie nach der Erkennung im Menü „Einstellungen“ eine Option zum Importieren von SnapCenter -Ressourcen aus. Weitere Einzelheiten finden Sie unter"Konfigurieren von NetApp Backup and Recovery" .

Dies ist ein zweiteiliger Prozess:

- Importieren Sie SnapCenter Server-Anwendungs- und Hostressourcen
- Verwalten ausgewählter SnapCenter -Hostressourcen

Importieren Sie SnapCenter Server-Anwendungs- und Hostressourcen

Dieser erste Schritt importiert Host-Ressourcen aus SnapCenter und zeigt diese Ressourcen auf der NetApp Backup and Recovery Inventory-Seite an. Zu diesem Zeitpunkt werden die Ressourcen noch nicht von NetApp Backup and Recovery verwaltet.

Nachdem Sie SnapCenter -Hostressourcen importiert haben, übernimmt NetApp Backup and Recovery die Schutzverwaltung nicht automatisch. Dazu müssen Sie explizit auswählen, dass die importierten Ressourcen in NetApp Backup and Recovery verwaltet werden sollen. Dadurch wird sichergestellt, dass Sie bereit sind, diese Ressourcen durch NetApp Backup and Recovery sichern zu lassen.

Schritte

1. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie **Inventar**.
3. Wählen Sie **Ressourcen entdecken**.
4. Wählen Sie auf der Seite „Workload-Ressourcen von NetApp Backup and Recovery ermitteln“ die Option „Aus SnapCenter importieren“ aus.
5. Geben Sie * Anmeldeinformationen für die SnapCenter -Anwendung* ein:
   a. * SnapCenter FQDN oder IP-Adresse*: Geben Sie den FQDN oder die IP-Adresse der SnapCenter -Anwendung selbst ein.
   b. **Port**: Geben Sie die Portnummer für den SnapCenter -Server ein.
   c. **Benutzername** und **Passwort**: Geben Sie den Benutzernamen und das Passwort für den SnapCenter -Server ein.
   d. **Konsolenagent**: Wählen Sie den Konsolenagenten für SnapCenter aus.
6. Geben Sie * SnapCenter -Server-Host-Anmeldeinformationen* ein:
   a. **Vorhandene Anmeldeinformationen**: Wenn Sie diese Option auswählen, können Sie die vorhandenen Anmeldeinformationen verwenden, die Sie bereits hinzugefügt haben. Wählen Sie den Namen der Anmeldeinformationen.
   b. **Neue Anmeldeinformationen hinzufügen**: Wenn Sie keine vorhandenen SnapCenter -Host -Anmeldeinformationen haben, können Sie neue Anmeldeinformationen hinzufügen. Geben Sie den Anmeldenamen, den Authentifizierungsmodus, den Benutzernamen und das Kennwort ein.
7. Wählen Sie **Importieren**, um Ihre Eingaben zu bestätigen und den SnapCenter -Server zu registrieren.

Wenn der SnapCenter -Server bereits registriert ist, können Sie die vorhandenen Registrierungsdetails aktualisieren.

Ergebnis

Auf der Inventarseite werden die importierten SnapCenter -Ressourcen angezeigt, darunter MS SQL-Hosts, -Instanzen und -Datenbanken.

Um die Details der importierten SnapCenter -Ressourcen anzuzeigen, wählen Sie im Menü „Aktionen“ die Option „Details anzeigen“ aus.

Verwalten von SnapCenter -Hostressourcen

Nachdem Sie die SnapCenter -Ressourcen importiert haben, verwalten Sie diese Hostressourcen in NetApp Backup and Recovery. Nachdem Sie die Verwaltung dieser Ressourcen ausgewählt haben, kann NetApp Backup and Recovery die aus SnapCenter importierten Ressourcen sichern und wiederherstellen. Sie verwalten diese Ressourcen nicht mehr im SnapCenter Server.

Schritte

1. Nachdem Sie die SnapCenter -Ressourcen importiert haben, wählen Sie im Menü „Sichern und Wiederherstellen“ die Option „Inventar“ aus.
2. Wählen Sie auf der Inventarseite den importierten SnapCenter -Host aus, den NetApp Backup and Recovery ab sofort verwalten soll.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**, um die Arbeitslastdetails anzuzeigen.
4. Wählen Sie auf der Seite Inventar > Arbeitslast das Symbol Aktionen ••• > **Verwalten**, um die Seite „Host verwalten“ anzuzeigen.
5. Wählen Sie **Verwalten**.
6. Wählen Sie auf der Seite „Host verwalten“ entweder die Verwendung eines vorhandenen vCenters oder das Hinzufügen eines neuen vCenters aus.
7. Wählen Sie **Verwalten**.

   Auf der Inventarseite werden die neu verwalteten SnapCenter -Ressourcen angezeigt.

Sie können optional einen Bericht der verwalteten Ressourcen erstellen, indem Sie im Menü „Aktionen“ die Option „Berichte erstellen“ auswählen.

Importieren Sie SnapCenter -Ressourcen nach der Erkennung von der Inventarseite

Wenn Sie bereits Ressourcen entdeckt haben, können Sie SnapCenter -Ressourcen von der Inventarseite importieren.

Schritte

1. Wählen Sie in der linken Navigation der Konsole **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie **Inventar**.
3. Wählen Sie auf der Inventarseite * SnapCenter -Ressourcen importieren* aus.
4. Befolgen Sie die Schritte im Abschnitt * SnapCenter -Ressourcen importieren* oben, um SnapCenter -Ressourcen zu importieren.

Wenn Sie SnapCenter nicht installiert haben, fügen Sie ein vCenter hinzu und ermitteln Sie Ressourcen

Wenn Sie SnapCenter noch nicht installiert haben, können Sie vCenter-Informationen hinzufügen und die Workloads von NetApp Backup and Recovery ermitteln lassen. Wählen Sie in jedem Konsolenagenten die Systeme aus, auf denen Sie Workloads ermitteln möchten.

Dies ist optional, wenn Sie eine VMware-Umgebung haben.

Schritte

1. Wählen Sie in der linken Navigation der Konsole **Schutz** > **Sicherung und Wiederherstellung**.

   Wenn Sie sich zum ersten Mal bei Backup and Recovery anmelden und zwar ein System in der Konsole haben, aber keine Ressourcen erkannt wurden, wird die Seite *Willkommen bei der neuen NetApp Backup and Recovery* mit einer Option zum **Erkennen von Ressourcen** angezeigt.

2. Wählen Sie **Ressourcen entdecken**.
3. Geben Sie die folgenden Informationen ein:
   a. **Workload-Typ**: Für diese Version ist nur Microsoft SQL Server verfügbar.
   b. **vCenter-Einstellungen**: Wählen Sie ein vorhandenes vCenter aus oder fügen Sie ein neues hinzu.

Um ein neues vCenter hinzuzufügen, geben Sie den FQDN oder die IP-Adresse, den Benutzernamen, das Kennwort, den Port und das Protokoll des vCenters ein.

Wenn Sie vCenter-Informationen eingeben, geben Sie Informationen sowohl für die vCenter-Einstellungen als auch für die Host-Registrierung ein. Wenn Sie hier vCenter-Informationen hinzugefügt oder eingegeben haben, müssen Sie als Nächstes auch Plugin-Informationen in den erweiterten Einstellungen hinzufügen.

c. **Hostregistrierung**: Wählen Sie **Anmeldeinformationen hinzufügen** und geben Sie Informationen zu den Hosts ein, die die Workloads enthalten, die Sie ermitteln möchten.

Wenn Sie einen eigenständigen Server und keinen vCenter-Server hinzufügen, geben Sie nur die Hostinformationen ein.

4. Wählen Sie **Entdecken**.

Dieser Vorgang kann einige Minuten dauern.

5. Fahren Sie mit den erweiterten Einstellungen fort.

Legen Sie während der Erkennung erweiterte Einstellungsoptionen fest und installieren Sie das Plugin

Mit den erweiterten Einstellungen können Sie den Plugin-Agenten manuell auf allen registrierten Servern installieren. Dadurch können Sie alle SnapCenter -Workloads in NetApp Backup and Recovery importieren, sodass Sie dort Backups und Wiederherstellungen verwalten können. NetApp Backup and Recovery zeigt die erforderlichen Schritte zur Installation des Plug-Ins.

Schritte

1. Fahren Sie auf der Seite „Ressourcen entdecken“ mit den erweiterten Einstellungen fort, indem Sie rechts auf den Abwärtspfeil klicken.
2. Geben Sie auf der Seite „Workload-Ressourcen ermitteln“ die folgenden Informationen ein.
   - **Plug-in-Portnummer eingeben**: Geben Sie die Portnummer ein, die das Plug-in verwendet.
   - **Installationspfad**: Geben Sie den Pfad ein, in dem das Plugin installiert werden soll.
3. Wenn Sie den SnapCenter -Agenten manuell installieren möchten, aktivieren Sie die Kontrollkästchen für die folgenden Optionen:
   - **Manuelle Installation verwenden**: Aktivieren Sie dieses Kontrollkästchen, um das Plugin manuell zu installieren.
   - **Alle Hosts im Cluster hinzufügen**: Aktivieren Sie dieses Kontrollkästchen, um während der Erkennung alle Hosts im Cluster zu NetApp Backup and Recovery hinzuzufügen.
   - **Optionale Vorinstallationsprüfungen überspringen**: Aktivieren Sie dieses Kontrollkästchen, um optionale Vorinstallationsprüfungen zu überspringen. Dies ist beispielsweise dann sinnvoll, wenn Sie wissen, dass sich die Speicher- oder Speicherplatzanforderungen in naher Zukunft ändern werden und Sie das Plug-In jetzt installieren möchten.
4. Wählen Sie **Entdecken**.

Weiter zum NetApp Backup and Recovery Dashboard

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".

Sichern Sie Microsoft SQL Server-Workloads mit NetApp Backup and Recovery

Sichern Sie Microsoft SQL Server-Anwendungsdaten von lokalen ONTAP -Systemen auf Amazon Web Services, Microsoft Azure oder StorageGRID. Das System erstellt automatisch Backups und speichert diese zum Schutz Ihrer Daten in einem Objektspeicher in Ihrem Cloud-Konto.

- Um Workloads nach einem Zeitplan zu sichern, erstellen Sie Richtlinien, die Sicherungs- und Wiederherstellungsvorgänge verwalten. Sehen"Erstellen von Richtlinien" Anweisungen hierzu finden Sie unter.
- Konfigurieren Sie das Protokollverzeichnis für erkannte Hosts, bevor Sie eine Sicherung starten.
- Sichern Sie jetzt Workloads (erstellen Sie jetzt ein On-Demand-Backup).

Status des Workload-Schutzes anzeigen

Bevor Sie eine Sicherung starten, sehen Sie sich den Schutzstatus Ihrer Workloads an.

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

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Überprüfen Sie die Details auf den Registerkarten „Hosts“, „Schutzgruppen“, „Verfügbarkeitsgruppen“, „Instanzen“ und „Datenbanken“.

Konfigurieren des Protokollverzeichnisses für erkannte Hosts

Legen Sie den Aktivitätsprotokollpfad für erkannte Hosts fest, um den Betriebsstatus vor dem Sichern von Workloads zu verfolgen.

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Wiederherstellung, Backup-Administrator für Backup und Wiederherstellung oder Administratorrolle für Backup und Wiederherstellung zur Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.

2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie einen Host aus.
5. Wählen Sie das Symbol Aktionen ••• > **Protokollverzeichnis konfigurieren**.
6. Geben Sie den Hostpfad ein oder durchsuchen Sie eine Liste von Hosts oder Knoten, um herauszufinden, wo Sie das Hostprotokoll speichern möchten.
7. Wählen Sie diejenigen aus, auf denen Sie die Protokolle speichern möchten.

   Die angezeigten Felder unterscheiden sich je nach ausgewähltem Bereitstellungsmodell, z. B. Failoverclusterinstanz oder Standalone.

8. Wählen Sie **Speichern**.

Erstellen einer Schutzgruppe

Erstellen Sie eine Schutzgruppe, um Sicherungs- und Wiederherstellungsvorgänge für mehrere Workloads zu verwalten. Eine Schutzgruppe ist eine logische Gruppierung von Workloads.

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Wiederherstellung oder Backup-Administratorrolle für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.
5. Wählen Sie **Schutzgruppe erstellen**.
6. Geben Sie einen Namen für die Schutzgruppe ein.
7. Wählen Sie die Instanzen oder Datenbanken aus, die Sie in die Schutzgruppe aufnehmen möchten.
8. Wählen Sie **Weiter**.
9. Wählen Sie die **Sicherungsrichtlinie** aus, die Sie auf die Schutzgruppe anwenden möchten.

   Wenn Sie eine Richtlinie erstellen möchten, wählen Sie **Neue Richtlinie erstellen** und folgen Sie den Anweisungen zum Erstellen einer Richtlinie. Sehen"Erstellen von Richtlinien" für weitere Informationen.

10. Wählen Sie **Weiter**.
11. Überprüfen Sie die Konfiguration.
12. Wählen Sie **Erstellen** aus, um die Schutzgruppe zu erstellen.

Sichern Sie Workloads jetzt mit einem On-Demand-Backup

Führen Sie vor der Durchführung von Änderungen an Ihrem System eine On-Demand-Sicherung durch, um sicherzustellen, dass Ihre Daten geschützt sind.

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Wiederherstellung oder Backup-Administratorrolle für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen

der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppe**, **Instanzen** oder **Datenbanken**.
5. Wählen Sie die Instanz oder Datenbank aus, die Sie sichern möchten.
6. Wählen Sie das Symbol Aktionen ••• > **Jetzt sichern**.
7. Wählen Sie die Richtlinie aus, die Sie auf die Sicherung anwenden möchten.
8. Wählen Sie die Zeitplanstufe aus.
9. Wählen Sie **Jetzt sichern**.

Aussetzen des Sicherungszeitplans

Unterbrechen Sie den Zeitplan, um Sicherungen während der Wartung oder Fehlerbehebung vorübergehend zu stoppen.

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Wiederherstellung oder Backup-Administratorrolle für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppe**, **Instanzen** oder **Datenbanken**.
5. Wählen Sie die Schutzgruppe, Instanz oder Datenbank aus, die Sie anhalten möchten.
6. Wählen Sie das Symbol Aktionen ••• > **Aussetzen**.

Löschen einer Schutzgruppe

Durch das Löschen einer Schutzgruppe werden diese und alle zugehörigen Sicherungszeitpläne entfernt. Möglicherweise möchten Sie eine Schutzgruppe löschen, wenn sie nicht mehr benötigt wird.

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Wiederherstellung oder Backup-Administratorrolle für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.
5. Wählen Sie das Symbol Aktionen ••• > **Schutzgruppe löschen**.

Entfernen des Schutzes von einer Arbeitslast

Sie können den Schutz eines Workloads entfernen, wenn Sie ihn nicht mehr sichern möchten oder die Verwaltung in NetApp Backup and Recovery beenden möchten.

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Wiederherstellung oder Backup-Administratorrolle für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppe**, **Instanzen** oder **Datenbanken**.
5. Wählen Sie die Schutzgruppe, Instanz oder Datenbank aus.
6. Wählen Sie das Symbol Aktionen ••• > **Schutz entfernen**.
7. Wählen Sie im Dialogfeld „Schutz entfernen“ aus, ob Sie Sicherungen und Metadaten behalten oder löschen möchten.
8. Wählen Sie **Entfernen**, um die Aktion zu bestätigen.

Wiederherstellen von Microsoft SQL Server-Workloads mit NetApp Backup and Recovery

Stellen Sie Microsoft SQL Server-Workloads mit NetApp Backup and Recovery wieder her. Verwenden Sie Snapshots, auf Sekundärspeicher replizierte Backups oder Backups im Objektspeicher. Stellen Sie Workloads auf dem ursprünglichen System, einem anderen System mit demselben Cloud-Konto oder einem lokalen ONTAP -System wieder her.

Von diesen Speicherorten wiederherstellen

Sie können Workloads von verschiedenen Startorten wiederherstellen:

- Wiederherstellung von einem primären Speicherort
- Wiederherstellen aus einer replizierten Ressource
- Wiederherstellung aus einer Objektspeichersicherung

Stellen Sie diese Punkte wieder her

Sie können Daten bis zum letzten Snapshot oder bis zu diesen Punkten wiederherstellen:

- Wiederherstellen aus Snapshots
- Wiederherstellung zu einem bestimmten Zeitpunkt, wenn Sie den Dateinamen, den Speicherort und das letzte gültige Datum kennen
- Wiederherstellen der neuesten Sicherung

Überlegungen zur Wiederherstellung aus dem Objektspeicher

Wenn Sie eine Sicherungsdatei im Objektspeicher auswählen und Ransomware Resilience für diese Sicherung aktiv ist (wenn Sie DataLock und Ransomware Resilience in der Sicherungsrichtlinie aktiviert

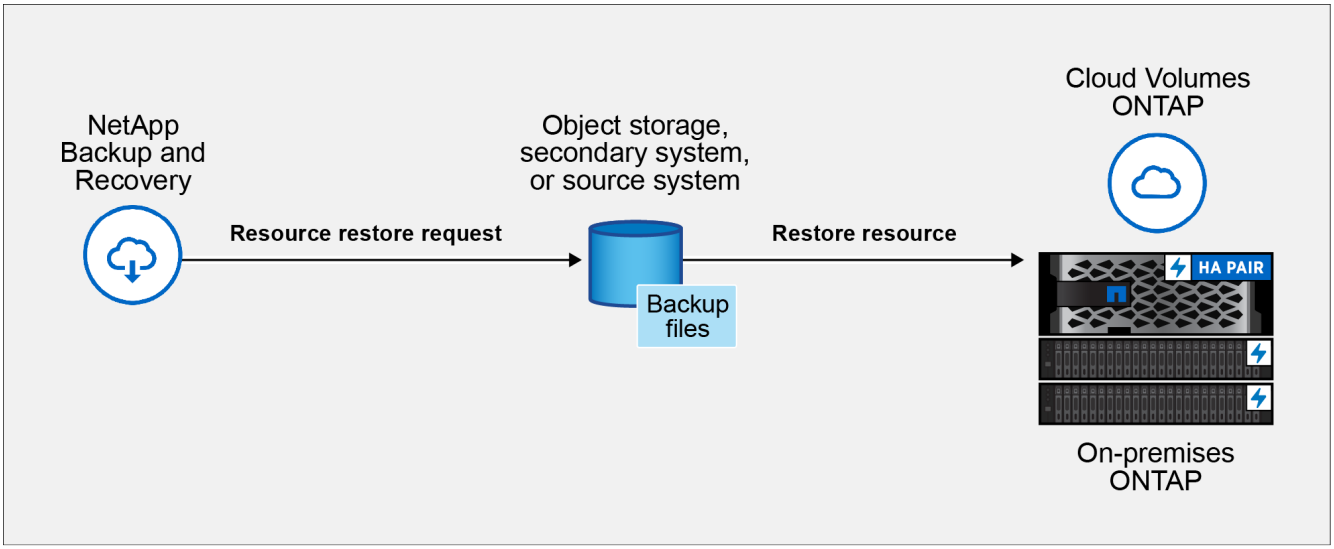
haben), werden Sie aufgefordert, vor der Wiederherstellung der Daten eine zusätzliche Integritätsprüfung der Sicherungsdatei durchzuführen. Wir empfehlen Ihnen, den Scan durchzuführen.

Für den Zugriff auf die Sicherungsdatei zahlen Sie Ihrem Cloud-Anbieter zusätzliche Gebühren.

So funktioniert die Wiederherstellung von Workloads

Beim Wiederherstellen von Workloads geschieht Folgendes:

- Wenn Sie eine Arbeitslast aus einer Sicherungsdatei wiederherstellen, erstellt NetApp Backup and Recovery mithilfe der Daten aus der Sicherung eine *neue* Ressource.
- Wenn Sie eine Wiederherstellung aus einem replizierten Workload durchführen, können Sie den Workload auf dem ursprünglichen System oder auf einem lokalen ONTAP System wiederherstellen.



- Wenn Sie eine Sicherung aus dem Objektspeicher wiederherstellen, können Sie die Daten auf dem ursprünglichen System oder auf einem lokalen ONTAP -System wiederherstellen.

Wiederherstellungsmethoden

Stellen Sie Workloads mit einer der folgenden Methoden wieder her:

- **Von der Seite „Wiederherstellen“**: Verwenden Sie diese Option, um eine Ressource wiederherzustellen, wenn Sie ihren Namen, ihren Standort oder ihr letztes Gültigkeitsdatum nicht kennen. Suchen Sie mithilfe von Filtern nach dem Schnappschuss.
- **Von der Inventarseite**: Verwenden Sie diese Option, um eine bestimmte Ressource wiederherzustellen, wenn Sie ihren Namen, ihren Standort und ihr letztes Gültigkeitsdatum kennen. Durchsuchen Sie die Liste, um die Ressource zu finden.

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Wiederherstellung oder Backup-Administratorrolle für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Wiederherstellen von Workload-Daten über die Option „Wiederherstellen“

Stellen Sie Datenbank-Workloads mithilfe der Option „Wiederherstellen“ wieder her.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Wiederherstellen** aus.
2. Wählen Sie die Datenbank aus, die Sie wiederherstellen möchten. Verwenden Sie die Filter zur Suche.
3. Wählen Sie die Wiederherstellungsoption:
    - Wiederherstellen aus Snapshots
    - Wiederherstellung zu einem bestimmten Zeitpunkt, wenn Sie den Dateinamen, den Speicherort und das letzte gültige Datum kennen
    - Wiederherstellen der neuesten Sicherung

Wiederherstellen von Workloads aus Snapshots

1. Wählen Sie auf der Seite „Wiederherstellungsoptionen“ die Option „Aus Snapshots wiederherstellen“ aus.

   Es wird eine Liste mit Snapshots angezeigt.

2. Wählen Sie den Snapshot aus, den Sie wiederherstellen möchten.
3. Wählen Sie **Weiter**.

   Als Nächstes werden die Zieloptionen angezeigt.

4. Geben Sie auf der Seite „Zieldetails“ die folgenden Informationen ein:
    - **Zieleinstellungen**: Wählen Sie, ob Sie die Daten an ihrem ursprünglichen Speicherort oder an einem anderen Speicherort wiederherstellen möchten. Wählen Sie für einen alternativen Speicherort den Hostnamen und die Instanz aus, geben Sie den Datenbanknamen ein und geben Sie den Zielpfad ein, in dem Sie den Snapshot wiederherstellen möchten.
    - **Optionen vor der Wiederherstellung**:
        - **Datenbank beim Wiederherstellen mit gleichem Namen überschreiben**: Beim Wiederherstellen bleibt der ursprüngliche Datenbankname erhalten.
        - **Replikationseinstellungen der SQL-Datenbank beibehalten**: Behält die Replikationseinstellungen für die SQL-Datenbank nach dem Wiederherstellungsvorgang bei.
        - **Transaktionsprotokollsicherung vor der Wiederherstellung erstellen**: Erstellt vor dem Wiederherstellungsvorgang eine Transaktionsprotokollsicherung.*** Wiederherstellung beenden, wenn die Sicherung des Transaktionsprotokolls vor der Wiederherstellung fehlschlägt**: Beendet den Wiederherstellungsvorgang, wenn die Sicherung des Transaktionsprotokolls fehlschlägt.
        - **Prescript**: Geben Sie den vollständigen Pfad für ein Skript ein, das vor dem Wiederherstellungsvorgang ausgeführt werden soll, alle Argumente, die das Skript benötigt, und wie lange auf die Fertigstellung des Skripts gewartet werden soll.
    - **Optionen nach der Wiederherstellung**:
        - **Betriebsbereit**, aber nicht zum Wiederherstellen zusätzlicher Transaktionsprotokolle verfügbar. Dadurch wird die Datenbank nach der Anwendung der Transaktionsprotokollsicherungen wieder online geschaltet.
        - **Nicht betriebsbereit**, aber zum Wiederherstellen zusätzlicher Transaktionsprotokolle verfügbar. Hält die Datenbank nach dem Wiederherstellungsvorgang in einem nicht betriebsbereiten Zustand, während die Sicherungen des Transaktionsprotokolls wiederhergestellt werden. Diese Option ist nützlich, um zusätzliche Transaktionsprotokolle wiederherzustellen.
        - **Nur-Lese-Modus** und verfügbar zum Wiederherstellen zusätzlicher Transaktionsprotokolle. Stellt die Datenbank im schreibgeschützten Modus wieder her und wendet

Transaktionsprotokollsicherungen an.

- **Postscript**: Geben Sie den vollständigen Pfad für ein Skript ein, das nach dem Wiederherstellungsvorgang ausgeführt werden soll, sowie alle Argumente, die das Skript verwendet.

5. Wählen Sie **Wiederherstellen**.

Wiederherstellung zu einem bestimmten Zeitpunkt

NetApp Backup and Recovery verwendet Protokolle und die aktuellsten Snapshots, um eine zeitpunktbezogene Wiederherstellung Ihrer Daten zu erstellen.

1. Wählen Sie auf der Seite „Wiederherstellungsoptionen“ die Option „Zu einem bestimmten Zeitpunkt wiederherstellen“ aus.
2. Wählen Sie **Weiter**.
3. Geben Sie auf der Seite „Zu einem bestimmten Zeitpunkt wiederherstellen“ die folgenden Informationen ein:
   - **Datum und Uhrzeit der Datenwiederherstellung**: Geben Sie das genaue Datum und die Uhrzeit der Daten ein, die Sie wiederherstellen möchten. Dieses Datum und diese Uhrzeit stammen vom Microsoft SQL Server-Datenbankhost.
4. Wählen Sie **Suchen**.
5. Wählen Sie den Snapshot aus, den Sie wiederherstellen möchten.
6. Wählen Sie **Weiter**.
7. Geben Sie auf der Seite „Zieldetails“ die folgenden Informationen ein:
   - **Zieleinstellungen**: Wählen Sie, ob Sie die Daten an ihrem ursprünglichen Speicherort oder an einem anderen Speicherort wiederherstellen möchten. Wählen Sie für einen alternativen Speicherort den Hostnamen und die Instanz aus, geben Sie den Datenbanknamen ein und geben Sie den Zielpfad ein.
   - **Optionen vor der Wiederherstellung**:
     - **Ursprünglichen Datenbanknamen beibehalten**: Während der Wiederherstellung bleibt der ursprüngliche Datenbankname erhalten.
     - **Replikationseinstellungen der SQL-Datenbank beibehalten**: Behält die Replikationseinstellungen für die SQL-Datenbank nach dem Wiederherstellungsvorgang bei.
     - **Prescript**: Geben Sie den vollständigen Pfad für ein Skript ein, das vor dem Wiederherstellungsvorgang ausgeführt werden soll, alle Argumente, die das Skript benötigt, und wie lange auf die Fertigstellung des Skripts gewartet werden soll.
   - **Optionen nach der Wiederherstellung**:
     - **Betriebsbereit**, aber nicht zum Wiederherstellen zusätzlicher Transaktionsprotokolle verfügbar. Dadurch wird die Datenbank nach der Anwendung der Transaktionsprotokollsicherungen wieder online geschaltet.
     - **Nicht betriebsbereit**, aber zum Wiederherstellen zusätzlicher Transaktionsprotokolle verfügbar. Hält die Datenbank nach dem Wiederherstellungsvorgang in einem nicht betriebsbereiten Zustand, während die Sicherungen des Transaktionsprotokolls wiederhergestellt werden. Diese Option ist nützlich, um zusätzliche Transaktionsprotokolle wiederherzustellen.
     - **Nur-Lese-Modus** und verfügbar zum Wiederherstellen zusätzlicher Transaktionsprotokolle. Stellt die Datenbank im schreibgeschützten Modus wieder her und wendet Transaktionsprotokollsicherungen an.
     - **Postscript**: Geben Sie den vollständigen Pfad für ein Skript ein, das nach dem

Wiederherstellungsvorgang ausgeführt werden soll, sowie alle Argumente, die das Skript verwendet.

8. Wählen Sie **Wiederherstellen**.

Wiederherstellen der neuesten Sicherung

Diese Option verwendet die neuesten vollständigen und Protokollsicherungen, um Ihre Daten in den letzten fehlerfreien Zustand zurückzusetzen. Das System scannt Protokolle vom letzten Snapshot bis zur Gegenwart. Der Prozess verfolgt Änderungen und Aktivitäten, um die aktuellste und genaueste Version Ihrer Daten wiederherzustellen.

1. Fahren Sie auf der Seite „Wiederherstellungsoptionen“ fort und wählen Sie „Auf die neueste Sicherung wiederherstellen“ aus.

   NetApp Backup and Recovery zeigt Ihnen die Snapshots, die für den Wiederherstellungsvorgang verfügbar sind.

2. Wählen Sie auf der Seite „Auf den neuesten Stand wiederherstellen“ den Snapshot-Speicherort des lokalen, sekundären Speichers oder Objektspeichers aus.
3. Wählen Sie **Weiter**.
4. Geben Sie auf der Seite „Zieldetails“ die folgenden Informationen ein:
   - **Zieleinstellungen**: Wählen Sie, ob Sie die Daten an ihrem ursprünglichen Speicherort oder an einem anderen Speicherort wiederherstellen möchten. Wählen Sie für einen alternativen Speicherort den Hostnamen und die Instanz aus, geben Sie den Datenbanknamen ein und geben Sie den Zielpfad ein.
   - **Optionen vor der Wiederherstellung**:
     - **Datenbank beim Wiederherstellen mit gleichem Namen überschreiben**: Beim Wiederherstellen bleibt der ursprüngliche Datenbankname erhalten.
     - **Replikationseinstellungen der SQL-Datenbank beibehalten**: Behält die Replikationseinstellungen für die SQL-Datenbank nach dem Wiederherstellungsvorgang bei.
     - **Vor der Wiederherstellung eine Sicherungskopie des Transaktionsprotokolls erstellen**: Erstellt vor dem Wiederherstellungsvorgang eine Sicherungskopie des Transaktionsprotokolls.
     - **Wiederherstellung beenden, wenn die Sicherung des Transaktionsprotokolls vor der Wiederherstellung fehlschlägt**: Beendet den Wiederherstellungsvorgang, wenn die Sicherung des Transaktionsprotokolls fehlschlägt.
     - **Prescript**: Geben Sie den vollständigen Pfad für ein Skript ein, das vor dem Wiederherstellungsvorgang ausgeführt werden soll, alle Argumente, die das Skript benötigt, und wie lange auf die Fertigstellung des Skripts gewartet werden soll.
   - **Optionen nach der Wiederherstellung**:
     - **Betriebsbereit**, aber nicht zum Wiederherstellen zusätzlicher Transaktionsprotokolle verfügbar. Dadurch wird die Datenbank nach der Anwendung der Transaktionsprotokollsicherungen wieder online geschaltet.
     - **Nicht betriebsbereit**, aber zum Wiederherstellen zusätzlicher Transaktionsprotokolle verfügbar. Hält die Datenbank nach dem Wiederherstellungsvorgang in einem nicht betriebsbereiten Zustand, während die Sicherungen des Transaktionsprotokolls wiederhergestellt werden. Diese Option ist nützlich, um zusätzliche Transaktionsprotokolle wiederherzustellen.
     - **Nur-Lese-Modus** und verfügbar zum Wiederherstellen zusätzlicher Transaktionsprotokolle. Stellt die Datenbank im schreibgeschützten Modus wieder her und wendet Transaktionsprotokollsicherungen an.

- **Postscript**: Geben Sie den vollständigen Pfad für ein Skript ein, das nach dem Wiederherstellungsvorgang ausgeführt werden soll, sowie alle Argumente, die das Skript verwendet.

5. Wählen Sie **Wiederherstellen**.

Wiederherstellen von Workload-Daten aus der Inventaroption

Stellen Sie Datenbank-Workloads von der Inventarseite aus wieder her. Mit der Inventaroption können Sie nur Datenbanken, keine Instanzen wiederherstellen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie den Host aus, auf dem sich die Ressource befindet, die Sie wiederherstellen möchten.
3. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Details anzeigen**.
4. Wählen Sie auf der Microsoft SQL Server-Seite die Registerkarte **Datenbanken** aus.
5. Wählen Sie im Menü „Datenbanken“ eine Datenbank mit dem Status „Geschützt“ aus.
6. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Wiederherstellen**.

   Es werden dieselben drei Optionen angezeigt wie beim Wiederherstellen über die Seite „Wiederherstellen“:

   - Wiederherstellen aus Snapshots
   - Wiederherstellung zu einem bestimmten Zeitpunkt
   - Wiederherstellen der neuesten Sicherung
7. Fahren Sie mit den gleichen Schritten für die Wiederherstellungsoption auf der Seite „Wiederherstellen“ fort

Klonen Sie Microsoft SQL Server-Workloads mit NetApp Backup and Recovery

Klonen Sie Microsoft SQL Server-Anwendungsdaten zur Entwicklung, zum Testen oder zum Schutz mit NetApp Backup and Recovery auf eine VM. Erstellen Sie Klone aus sofortigen oder vorhandenen Snapshots Ihrer SQL Server-Workloads.

Wählen Sie zwischen den folgenden Klontypen:

- **Sofortiger Snapshot und Klon**: Sie können einen Klon Ihrer Microsoft SQL Server-Workloads aus einem sofortigen Snapshot erstellen. Dabei handelt es sich um eine zeitpunktbezogene Kopie der Quelldaten, die aus einer Sicherung erstellt wird. Der Klon wird in einem Objektspeicher in Ihrem öffentlichen oder privaten Cloud-Konto gespeichert. Sie können den Klon verwenden, um Ihre Workloads im Falle eines Datenverlusts oder einer Datenbeschädigung wiederherzustellen.
- **Klonen von einem vorhandenen Snapshot**: Sie können einen vorhandenen Snapshot aus einer Liste von Snapshots auswählen, die für die Arbeitslast verfügbar sind. Diese Option ist nützlich, wenn Sie einen Klon von einem bestimmten Zeitpunkt erstellen möchten. Klonen Sie entweder auf den primären oder sekundären Speicher.

Sie können die folgenden Schutzziele erreichen:

- Erstellen eines Klons
- Aktualisieren eines Klons
- Einen Klon teilen

- Löschen eines Klons

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Wiederherstellung oder Backup-Administratorrolle für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Erstellen eines Klons

Sie können einen Klon Ihrer Microsoft SQL Server-Workloads erstellen. Ein Klon ist eine Kopie der Quelldaten, die aus einer Sicherung erstellt wird. Der Klon wird in einem Objektspeicher in Ihrem öffentlichen oder privaten Cloud-Konto gespeichert. Sie können den Klon verwenden, um Ihre Workloads im Falle eines Datenverlusts oder einer Datenbeschädigung wiederherzustellen.

Sie können einen Klon aus einem vorhandenen Snapshot oder aus einem sofortigen Snapshot erstellen. Ein sofortiger Snapshot ist eine zeitpunktbezogene Kopie der Quelldaten, die aus einer Sicherung erstellt wird. Sie können den Klon verwenden, um Ihre Workloads im Falle eines Datenverlusts oder einer Datenbeschädigung wiederherzustellen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Klonen** aus.
2. Wählen Sie **Neuen Klon erstellen**.
3. Wählen Sie den Klontyp aus:
   - **Klonen und Datenbankaktualisierung aus vorhandenem Snapshot**: Wählen Sie einen Snapshot und konfigurieren Sie die Klonoptionen.
   - **Sofortiger Snapshot und Klon**: Machen Sie jetzt einen Snapshot der Quelldaten und erstellen Sie aus diesem Snapshot einen Klon. Diese Option ist nützlich, wenn Sie einen Klon aus den neuesten Daten im Ursprungs-Workload erstellen möchten.
4. Füllen Sie den Abschnitt **Datenbankquelle** aus:
   - **Einzelner Klon oder Massenklon**: Wählen Sie aus, ob ein einzelner Klon oder mehrere Klone erstellt werden sollen. Wenn Sie **Massenklon** auswählen, können Sie mithilfe einer bereits erstellten Schutzgruppe mehrere Klone gleichzeitig erstellen. Diese Option ist nützlich, wenn Sie mehrere Klone für unterschiedliche Workloads erstellen möchten.
   - **Host, Instanz und Name der Quelldatenbank**: Wählen Sie den Host, die Instanz und den Namen der Quelldatenbank für den Klon aus. Die Quelldatenbank ist die Datenbank, aus der der Klon erstellt wird.
5. Füllen Sie den Abschnitt **Datenbankziel** aus:
   - **Zieldatenbankhost, -instanz und -name**: Wählen Sie den Zieldatenbankhost, die -instanz und den Namen für den Klon aus. Die Zieldatenbank ist der Speicherort, an dem der Klon erstellt wird.

     Wählen Sie optional **Suffix** aus der Dropdown-Liste „Zielname“ aus und fügen Sie dem Namen der geklonten Datenbank ein Suffix hinzu. Wenn Sie kein Suffix hinzufügen, ist der Name der geklonten Datenbank derselbe wie der Name der Quelldatenbank.

   - **QoS (maximaler Durchsatz)**: Wählen Sie den maximalen Quality of Service (QoS)-Durchsatz in MBps für den Klon. Die QoS definiert die Leistungsmerkmale des Klons, wie beispielsweise den maximalen Durchsatz und IOPS.
6. Füllen Sie den Abschnitt **Mount** aus:
   - **Mount-Punkt automatisch zuweisen**: Weisen Sie dem Klon im Objektspeicher automatisch einen Mount-Punkt zu.
   - **Mountpoint-Pfad definieren**: Geben Sie einen Mountpoint für den Klon ein. Der Einhängepunkt ist der

Ort, an dem der Klon im Objektspeicher eingehängt wird. Wählen Sie den Laufwerksbuchstaben aus, geben Sie den Datendateipfad ein und geben Sie den Protokolldateipfad ein.

7. Wählen Sie **Weiter**.
8. Wählen Sie den Wiederherstellungspunkt aus:
   - **Vorhandene Snapshots**: Wählen Sie einen vorhandenen Snapshot aus der Liste der für die Arbeitslast verfügbaren Snapshots aus. Diese Option ist nützlich, wenn Sie einen Klon von einem bestimmten Zeitpunkt erstellen möchten.
   - **Sofortiger Snapshot und Klon**: Wählen Sie den neuesten Snapshot aus der Liste der Snapshots aus, die für die Arbeitslast verfügbar sind. Diese Option ist nützlich, wenn Sie einen Klon aus den neuesten Daten im Ursprungs-Workload erstellen möchten.
9. Wenn Sie sich für die Erstellung eines **Sofort-Snapshots und Klons** entschieden haben, wählen Sie den Speicherort für den Klon:
   - **Lokaler Speicher**: Wählen Sie diese Option, um den Klon im lokalen Speicher des ONTAP -Systems zu erstellen. Der lokale Speicher ist der Speicher, der direkt an das ONTAP -System angeschlossen ist.
   - **Sekundärspeicher**: Wählen Sie diese Option, um den Klon im Sekundärspeicher des ONTAP -Systems zu erstellen. Der sekundäre Speicher ist der Speicher, der für Sicherungs- und Wiederherstellungs-Workloads verwendet wird.
10. Wählen Sie den Zielspeicherort für die Daten und Protokolle aus.
11. Wählen Sie **Weiter**.
12. Füllen Sie den Abschnitt **Erweiterte Optionen** aus.
13. Wenn Sie **Sofortiger Snapshot und Klon** gewählt haben, führen Sie die folgenden Optionen aus:
   - **Zeitplan und Ablauf der Klonaktualisierung**: Wenn Sie **Sofortklon** gewählt haben, geben Sie das Datum ein, an dem mit der Aktualisierung des Klons begonnen werden soll. Der Klonzeitplan definiert, wann der Klon erstellt wird.
     - **Klon löschen, wenn Zeitplan abläuft**: Wenn Sie den Klon nach Ablauf des Klons löschen möchten.
     - **Klon aktualisieren alle**: Wählen Sie aus, wie oft der Klon aktualisiert werden soll. Sie können den Klon stündlich, täglich, wöchentlich, monatlich oder vierteljährlich aktualisieren. Diese Option ist nützlich, wenn Sie den Klon auf dem neuesten Stand mit dem Quell-Workload halten möchten.
   - **Prescripts und Postscripts**: Fügen Sie optional Skripte hinzu, die vor und nach der Erstellung des Klons ausgeführt werden sollen. Diese Skripte können zusätzliche Aufgaben ausführen, beispielsweise das Einrichten des Klons oder das Senden von Benachrichtigungen.
   - **Benachrichtigung**: Geben Sie optional E-Mail-Adressen an, um Benachrichtigungen über den Status der Klonerstellung zusammen mit dem Jobbericht zu erhalten. Sie können auch eine Webhook-URL angeben, um Benachrichtigungen über den Status der Klonerstellung zu erhalten. Sie können angeben, ob Sie Erfolgs- und Fehlerbenachrichtigungen oder nur die eine oder die andere erhalten möchten.
   - **Tags**: Wählen Sie Bezeichnungen aus, die Ihnen später bei der Suche nach Ressourcengruppen helfen, und wählen Sie **Übernehmen**. Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem Tag „HR“ verknüpften Ressourcengruppen finden.
14. Wählen Sie **Erstellen**.
15. Wenn der Klon erstellt ist, können Sie ihn auf der Seite **Inventar** anzeigen.

Aktualisieren eines Klons

Sie können einen Klon Ihrer Microsoft SQL Server-Workloads aktualisieren. Durch das Aktualisieren eines Klons wird der Klon mit den neuesten Daten aus dem Quell-Workload aktualisiert. Dies ist nützlich, wenn Sie den Klon auf dem neuesten Stand der Quell-Workload halten möchten.

Sie haben die Möglichkeit, den Datenbanknamen zu ändern, den neuesten Sofort-Snapshot zu verwenden oder von einem vorhandenen Produktions-Snapshot zu aktualisieren.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Klonen** aus.
2. Wählen Sie den Klon aus, den Sie aktualisieren möchten.
3. Wählen Sie das Symbol Aktionen ••• > **Klon aktualisieren**.
4. Füllen Sie den Abschnitt **Erweiterte Einstellungen** aus:
   - **Wiederherstellungsbereich**: Wählen Sie, ob alle Protokollsicherungen oder Protokollsicherungen bis zu einem bestimmten Zeitpunkt wiederhergestellt werden sollen. Diese Option ist nützlich, wenn Sie den Klon zu einem bestimmten Zeitpunkt wiederherstellen möchten.
   - **Zeitplan und Ablauf der Klonaktualisierung**: Wenn Sie **Sofortklon** gewählt haben, geben Sie das Datum ein, an dem mit der Aktualisierung des Klons begonnen werden soll. Der Klonzeitplan definiert, wann der Klon erstellt wird.
     - **Klon löschen, wenn Zeitplan abläuft**: Wenn Sie den Klon nach Ablauf des Klons löschen möchten.
     - **Klon aktualisieren alle**: Wählen Sie aus, wie oft der Klon aktualisiert werden soll. Sie können den Klon stündlich, täglich, wöchentlich, monatlich oder vierteljährlich aktualisieren. Diese Option ist nützlich, wenn Sie den Klon auf dem neuesten Stand mit dem Quell-Workload halten möchten.
   - **iGroup-Einstellungen**: Wählen Sie die iGroup für den Klon aus. Die iGroup ist eine logische Gruppierung von Initiatoren, die für den Zugriff auf den Klon verwendet werden. Sie können eine vorhandene iGroup auswählen oder eine neue erstellen. Wählen Sie die iGroup aus dem primären oder sekundären ONTAP Speichersystem aus.
   - **Prescripts und Postscripts**: Fügen Sie optional Skripte hinzu, die vor und nach der Erstellung des Klons ausgeführt werden sollen. Diese Skripte können zusätzliche Aufgaben ausführen, beispielsweise das Einrichten des Klons oder das Senden von Benachrichtigungen.
   - **Benachrichtigung**: Geben Sie optional E-Mail-Adressen an, um Benachrichtigungen über den Status der Klonerstellung zusammen mit dem Jobbericht zu erhalten. Sie können auch eine Webhook-URL angeben, um Benachrichtigungen über den Status der Klonerstellung zu erhalten. Sie können angeben, ob Sie Erfolgs- und Fehlerbenachrichtigungen oder nur die eine oder die andere erhalten möchten.
   - **Tags**: Geben Sie ein oder mehrere Labels ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.
5. Wählen Sie im Bestätigungsdialogfeld „Aktualisieren“ die Option „**Aktualisieren**“ aus, um fortzufahren.

Überspringen einer Klonaktualisierung

Überspringen Sie eine Klonaktualisierung, um den Klon unverändert zu lassen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Klonen** aus.

2. Wählen Sie den Klon aus, für den Sie die Aktualisierung überspringen möchten.
3. Wählen Sie das Symbol Aktionen ••• > **Aktualisierung überspringen**.
4. Führen Sie im Dialogfeld „Bestätigung für Aktualisierung überspringen“ die folgenden Schritte aus:
    a. Um nur den nächsten Aktualisierungsplan zu überspringen, wählen Sie **Nur den nächsten Aktualisierungsplan überspringen**.
    b. Um fortzufahren, wählen Sie **Überspringen**.

Einen Klon teilen

Sie können einen Klon Ihrer Microsoft SQL Server-Workloads aufteilen. Durch das Aufteilen eines Klons wird aus dem Klon ein neues Backup erstellt. Mit dem neuen Backup können die Workloads wiederhergestellt werden.

Sie können einen Klon in unabhängige oder langfristige Klone aufteilen. Ein Assistent zeigt die Liste der Aggregate an, die Teil der SVM sind, ihre Größen und wo sich das geklonte Volume befindet. NetApp Backup and Recovery zeigt außerdem an, ob genügend Speicherplatz zum Aufteilen des Klons vorhanden ist. Nachdem der Klon aufgeteilt wurde, wird er zum Schutz zu einer unabhängigen Datenbank.

Der Klonauftrag wird nicht entfernt und kann für andere Klone erneut verwendet werden.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Klonen** aus.
2. Wählen Sie einen Klon aus.
3. Wählen Sie das Symbol Aktionen ••• > **Geteilter Klon**.
4. Überprüfen Sie die Details zum geteilten Klon und wählen Sie **Teilen**.
5. Wenn der geteilte Klon erstellt ist, können Sie ihn auf der Seite **Inventar** anzeigen.

Löschen eines Klons

Sie können einen Klon Ihrer Microsoft SQL Server-Workloads löschen. Durch das Löschen eines Klons wird der Klon aus dem Objektspeicher entfernt und Speicherplatz freigegeben.

Wenn eine Richtlinie den Klon schützt, werden sowohl der Klon als auch sein Job gelöscht.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Klonen** aus.
2. Wählen Sie einen Klon aus.
3. Wählen Sie das Symbol Aktionen ••• > **Klon löschen**.
4. Überprüfen Sie im Bestätigungsdialogfeld zum Löschen des Klons die Löschdetails.
    a. Um die geklonten Ressourcen aus SnapCenter zu löschen, auch wenn auf die Klone oder ihren Speicher nicht zugegriffen werden kann, wählen Sie **Löschen erzwingen**.
    b. Wählen Sie **Löschen**.
5. Wenn der Klon gelöscht wird, wird er von der Seite **Inventar** entfernt.

Verwalten Sie den Microsoft SQL Server-Bestand mit NetApp Backup and Recovery

NetApp Backup and Recovery unterstützt Sie bei der Verwaltung Ihrer Microsoft SQL

Server-Hosts, -Datenbanken und -Instanzen. Sie können die Schutzeinstellungen für Ihr Inventar anzeigen, ändern oder entfernen.

Sie können die folgenden Aufgaben im Zusammenhang mit der Verwaltung Ihres Inventars ausführen:

- Hostinformationen verwalten
  - Zeitpläne aussetzen
  - Hosts bearbeiten oder löschen
- Verwalten von Instanzinformationen
  - Anmeldeinformationen einer Ressource zuordnen
  - Sichern Sie jetzt, indem Sie ein On-Demand-Backup starten
  - Schutzeinstellungen bearbeiten
- Verwalten von Datenbankinformationen
  - Schützen Sie Datenbanken
  - Datenbanken wiederherstellen
  - Schutzeinstellungen bearbeiten
  - Sichern Sie jetzt, indem Sie ein On-Demand-Backup starten
- Konfigurieren Sie das Protokollverzeichnis (unter **Inventar** > **Hosts**). Wenn Sie Protokolle für Ihre Datenbankhosts im Snapshot sichern möchten, konfigurieren Sie zuerst die Protokolle in NetApp Backup and Recovery. Weitere Einzelheiten finden Sie unter"Konfigurieren der NetApp Backup and Recovery -Einstellungen" .

Hostinformationen verwalten

Sie können Hostinformationen verwalten, um sicherzustellen, dass die richtigen Hosts geschützt sind. Sie können Hostinformationen anzeigen, bearbeiten und löschen.

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Recovery, Backupadministrator für Backup und Recovery, Wiederherstellungsadministrator für Backup und Recovery oder Administratorrolle für Klonadministrator für Backup und Recovery. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

- Konfigurieren Sie das Protokollverzeichnis. Weitere Einzelheiten finden Sie unter"Konfigurieren der NetApp Backup and Recovery -Einstellungen" .
- Zeitpläne aussetzen
- Einen Host bearbeiten
- Löschen eines Hosts

Hosts verwalten

Sie können die in Ihrem System erkannten Hosts verwalten. Sie können sie einzeln oder als Gruppe verwalten.

Sie können Hosts mit dem Status „Nicht verwaltet“ in der Spalte „Hosts“ verwalten. NetApp Backup and Recovery verwaltet bereits Hosts mit dem Status „Managed“.

Nachdem Sie die Hosts in NetApp Backup and Recovery verwaltet haben, verwaltet SnapCenter die Ressourcen auf diesen Hosts nicht mehr.

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

Schritte

1. Wählen Sie im Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Hosts**.
5. Wählen Sie einen oder mehrere Hosts aus. Wenn Sie mehrere Hosts auswählen, wird die Option „Massenaktionen“ angezeigt, in der Sie **Verwalten (bis zu 5 Hosts)** auswählen können.
6. Wählen Sie das Symbol Aktionen ••• > **Verwalten**.
7. Überprüfen Sie die Hostabhängigkeiten:
   - Wenn das vCenter nicht angezeigt wird, wählen Sie das Stiftsymbol aus, um die vCenter-Details hinzuzufügen oder zu bearbeiten.
   - Wenn Sie ein vCenter hinzufügen, müssen Sie das vCenter auch registrieren, indem Sie **vCenter registrieren** auswählen.
8. Wählen Sie **Einstellungen validieren**, um Ihre Einstellungen zu testen.
9. Wählen Sie **Verwalten**, um den Host zu verwalten.

Zeitpläne aussetzen

Unterbrechen Sie Zeitpläne, um Sicherungs- und Wiederherstellungsvorgänge während der Hostwartung zu stoppen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie den Host aus, auf dem Sie Zeitpläne aussetzen möchten.
3. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Zeitpläne aussetzen**.
4. Wählen Sie im Bestätigungsdialogfeld **Suspend** aus.

Einen Host bearbeiten

Sie können die vCenter-Serverinformationen, die Anmeldeinformationen für die Hostregistrierung und die erweiterten Einstellungsoptionen ändern.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie den Host aus, den Sie bearbeiten möchten.
3. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Host bearbeiten**.
4. Bearbeiten Sie die Hostinformationen.
5. Wählen Sie **Fertig**.

Löschen eines Hosts

Sie können die Host-Informationen löschen, um die Servicegebühren zu stoppen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie den Host aus, den Sie löschen möchten.
3. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Host löschen**.
4. Überprüfen Sie die Bestätigungsinformationen und wählen Sie **Löschen**.

Verwalten von Instanzinformationen

Sie können Instanzinformationen verwalten, um die entsprechenden Anmeldeinformationen für den Ressourcenschutz zuzuweisen und Ressourcen auf folgende Weise zu sichern:

- Schützen von Instanzen
- Anmeldeinformationen zuordnen
- Trennen der Anmeldeinformationen
- Bearbeitungsschutz
- Jetzt sichern

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

Schützen Sie Datenbankinstanzen

Sie können einer Datenbankinstanz eine Richtlinie zuweisen, indem Sie Richtlinien verwenden, die die Zeitpläne und die Beibehaltung des Ressourcenschutzes regeln.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie die Arbeitslast aus, die Sie anzeigen möchten, und wählen Sie **Anzeigen**.
3. Wählen Sie die Registerkarte **Instanzen**.
4. Wählen Sie die Instanz aus.
5. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Schützen**.
6. Wählen Sie eine Richtlinie aus oder erstellen Sie eine neue.

   Einzelheiten zum Erstellen einer Richtlinie finden Sie unter"Erstellen einer Richtlinie" .

7. Geben Sie Informationen zu den Skripten an, die Sie vor und nach der Sicherung ausführen möchten.
   - **Vorskript**: Geben Sie den Dateinamen und den Speicherort Ihres Skripts ein, um es automatisch auszuführen, bevor die Schutzaktion ausgelöst wird. Dies ist hilfreich, um zusätzliche Aufgaben oder Konfigurationen durchzuführen, die vor dem Schutz-Workflow ausgeführt werden müssen.
   - **Postskriptum**: Geben Sie den Dateinamen und den Speicherort Ihres Skripts ein, um es nach Abschluss der Schutzaktion automatisch auszuführen. Dies ist hilfreich, um zusätzliche Aufgaben oder Konfigurationen durchzuführen, die nach dem Schutz-Workflow ausgeführt werden müssen.
8. Geben Sie an, wie der Snapshot überprüft werden soll:
   - Speicherort: Wählen Sie den Speicherort aus, an dem der Überprüfungs-Snapshot gespeichert werden soll.

- Überprüfungsressource: Wählen Sie aus, ob sich die Ressource, die Sie überprüfen möchten, im lokalen Snapshot und im sekundären ONTAP -Speicher befindet.
- Überprüfungsplan: Wählen Sie die Häufigkeit stündlich, täglich, wöchentlich, monatlich oder jährlich.

Anmeldeinformationen einer Ressource zuordnen

Sie können Anmeldeinformationen mit einer Ressource verknüpfen, um Schutz zu gewährleisten.

Weitere Einzelheiten finden Sie unter"Konfigurieren Sie die NetApp Backup and Recovery -Einstellungen, einschließlich der Anmeldeinformationen" .

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie die Arbeitslast aus, die Sie anzeigen möchten, und wählen Sie **Anzeigen**.
3. Wählen Sie die Registerkarte **Instanzen**.
4. Wählen Sie die Instanz aus.
5. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Anmeldeinformationen verknüpfen**.
6. Verwenden Sie vorhandene Anmeldeinformationen oder erstellen Sie neue.

Schutzeinstellungen bearbeiten

Sie können die Richtlinie ändern, eine neue Richtlinie erstellen, einen Zeitplan festlegen und Aufbewahrungseinstellungen festlegen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie die Arbeitslast aus, die Sie anzeigen möchten, und wählen Sie **Anzeigen**.
3. Wählen Sie die Registerkarte **Instanzen**.
4. Wählen Sie die Instanz aus.
5. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Schutz bearbeiten**.

   Einzelheiten zum Erstellen einer Richtlinie finden Sie unter"Erstellen einer Richtlinie" .

Jetzt sichern

Sichern Sie Ihre Daten jetzt, um sie sofort zu schützen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie die Arbeitslast aus, die Sie anzeigen möchten, und wählen Sie **Anzeigen**.
3. Wählen Sie die Registerkarte **Instanzen**.
4. Wählen Sie die Instanz aus.
5. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Jetzt sichern**.
6. Wählen Sie den Sicherungstyp und legen Sie den Zeitplan fest.

   Einzelheiten zum Erstellen einer Ad-hoc-Sicherung finden Sie unter"Erstellen einer Richtlinie" .

Verwalten von Datenbankinformationen

Sie können Datenbankinformationen auf folgende Weise verwalten:

- Schützen Sie Datenbanken
- Datenbanken wiederherstellen
- Schutzdetails anzeigen
- Schutzeinstellungen bearbeiten
- Jetzt sichern

Schützen Sie Datenbanken

Sie können die Richtlinie ändern, eine neue Richtlinie erstellen, einen Zeitplan festlegen und Aufbewahrungseinstellungen festlegen.

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

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie die Arbeitslast aus, die Sie anzeigen möchten, und wählen Sie **Anzeigen**.
3. Wählen Sie die Registerkarte **Datenbanken**.
4. Wählen Sie die Datenbank aus.
5. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Schützen**.

   Einzelheiten zum Erstellen einer Richtlinie finden Sie unter"Erstellen einer Richtlinie" .

Datenbanken wiederherstellen

Stellen Sie eine Datenbank wieder her, um Ihre Daten zu schützen.

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

1. Wählen Sie die Registerkarte **Datenbanken**.
2. Wählen Sie die Datenbank aus.
3. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Wiederherstellen**.

   Informationen zum Wiederherstellen von Workloads finden Sie unter"Wiederherstellen von Workloads" .

Schutzeinstellungen bearbeiten

Sie können die Richtlinie ändern, eine neue Richtlinie erstellen, einen Zeitplan festlegen und Aufbewahrungseinstellungen festlegen.

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

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie die Arbeitslast aus, die Sie anzeigen möchten, und wählen Sie **Anzeigen**.
3. Wählen Sie die Registerkarte **Datenbanken**.
4. Wählen Sie die Datenbank aus.
5. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Schutz bearbeiten**.

   Einzelheiten zum Erstellen einer Richtlinie finden Sie unter"Erstellen einer Richtlinie" .

Jetzt sichern

Sie können Ihre Microsoft SQL Server-Instanzen und -Datenbanken jetzt sichern, um Ihre Daten sofort zu schützen.

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

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie die Arbeitslast aus, die Sie anzeigen möchten, und wählen Sie **Anzeigen**.
3. Wählen Sie die Registerkarte **Instanzen** oder **Datenbanken**.
4. Wählen Sie die Instanz oder Datenbank aus.
5. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Jetzt sichern**.

Verwalten Sie Microsoft SQL Server-Snapshots mit NetApp Backup and Recovery

Sie können Microsoft SQL Server-Snapshots verwalten, indem Sie sie aus NetApp Backup and Recovery löschen.

Löschen eines Snapshots

Sie können nur lokale Snapshots löschen.

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

Schritte

1. Wählen Sie in NetApp Backup and Recovery*Inventar* aus.
2. Wählen Sie die Arbeitslast aus und wählen Sie **Anzeigen**.
3. Wählen Sie die Registerkarte **Datenbanken**.
4. Wählen Sie die Datenbank aus, für die Sie einen Snapshot löschen möchten.
5. Wählen Sie im Menü „Aktionen“ die Option „Schutzdetails anzeigen“ aus.
6. Wählen Sie den lokalen Snapshot aus, den Sie löschen möchten.

Stellen Sie sicher, dass das lokale Snapshot-Symbol in der Spalte **Standort** dieser Zeile blau angezeigt wird.

7. Wählen Sie die **Aktionen*** **Symbol und wählen Sie *Lokalen Snapshot löschen**.
8. Wählen Sie im Bestätigungsdialogfeld **Entfernen** aus.

Erstellen Sie Berichte für Microsoft SQL Server-Workloads in NetApp Backup and Recovery

In NetApp Backup and Recovery können Sie Berichte für Microsoft SQL Server-Workloads erstellen, um den Sicherungsstatus und Details anzuzeigen, einschließlich der Anzahl erfolgreicher und fehlgeschlagener Sicherungen, Sicherungstypen, Speichersysteme und Zeitstempel.

Erstellen eines Berichts

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Wiederherstellung, Backup-Administrator für Backup und Wiederherstellung, Wiederherstellungsadministrator für Backup und Wiederherstellung, Klonadministrator 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" .

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 Arbeitslast (Microsoft SQL Server) wünschen.
   - **Host auswählen**: Wenn Sie nach Arbeitslast ausgewählt haben, wählen Sie den Host aus, für den Sie den Bericht erstellen möchten.
   - **Inhalt auswählen**: Wählen Sie, ob der Bericht eine Zusammenfassung aller Sicherungen oder Details zu jeder Sicherung enthalten soll. (Wenn Sie „Nach Konto“ gewählt haben)
4. Geben Sie den Berichtszeitraum ein: 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 Details zur Berichtszustellung ein: Wenn Sie den Bericht per E-Mail zugestellt bekommen möchten, aktivieren Sie **Bericht per E-Mail senden**. Geben Sie die E-Mail-Adresse ein, an die der Bericht gesendet werden soll.

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

Schutz von VMware-Workloads

Überblick zum Schutz von VMware-Workloads mit NetApp Backup and Recovery

Schützen Sie Ihre VMware-VMs und Datenspeicher mit NetApp Backup and Recovery. NetApp Backup and Recovery bietet schnelle, platzsparende, absturzkonsistente und

VM-konsistente Sicherungs- und Wiederherstellungsvorgänge. Sie können VMware-Workloads auf Amazon Web Services S3 oder StorageGRID sichern und VMware-Workloads auf einem lokalen VMware-Host wiederherstellen.

Diese Version von NetApp Backup and Recovery unterstützt nur VMware vCenter und erkennt keine vVols oder VMs auf vVols.

Verwenden Sie NetApp Backup and Recovery , um eine 3-2-1-Strategie zu implementieren, bei der Sie 3 Kopien Ihrer Quelldaten auf 2 verschiedenen Speichersystemen sowie 1 Kopie in der Cloud haben. Zu den Vorteilen des 3-2-1-Ansatzes gehören:

- Mehrere Datenkopien schützen vor internen und externen Cybersicherheitsbedrohungen.
- Die Verwendung unterschiedlicher Medientypen erleichtert Ihnen die Wiederherstellung, wenn ein Typ ausfällt.
- Sie können die Wiederherstellung schnell von der Vor-Ort-Kopie durchführen und die Offsite-Kopien verwenden, wenn die Vor-Ort-Kopie kompromittiert ist.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -UI-Versionen finden Sie unter"Wechseln Sie zur vorherigen NetApp Backup and Recovery -Benutzeroberfläche" .

Mit NetApp Backup and Recovery können Sie die folgenden Aufgaben im Zusammenhang mit VMware-Workloads ausführen:

- "Entdecken Sie VMware-Workloads"
- "Erstellen und Verwalten von Schutzgruppen für VMware-Workloads"
- "Sichern Sie VMware-Workloads"
- "Wiederherstellen von VMware-Workloads"

Entdecken Sie VMware-Workloads mit NetApp Backup and Recovery

Damit Sie den Dienst nutzen können, muss der NetApp Backup and Recovery -Dienst zunächst VMware-Datenspeicher und VMs erkennen, die auf ONTAP -Systemen ausgeführt werden. Sie können optional Sicherungsdaten und Richtlinien aus dem SnapCenter Plug-in for VMware vSphere importieren, wenn Sie es bereits installiert haben.

Erforderliche Konsolenrolle 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 VMware-Workloads und importieren Sie optional SnapCenter -Ressourcen

Während der Erkennungsphase analysiert NetApp Backup and Recovery die VMware-Workloads innerhalb Ihrer Organisation und bewertet und importiert vorhandene Schutzrichtlinien, Snapshots sowie Backup- und Wiederherstellungsoptionen.

Sie können VMware NFS- und VMFS-Datenspeicher und VMs von ihrem lokalen SnapCenter Plug-in for VMware vSphere in das NetApp Backup and Recovery Inventar importieren.

Diese Version von NetApp Backup and Recovery unterstützt nur VMware vCenter und erkennt keine vVols oder VMs auf vVols.

Während des Importvorgangs führt NetApp Backup and Recovery die folgenden Aufgaben aus:

- Ermöglicht sicheren SSH-Zugriff auf den vCenter-Server.
- Aktiviert den Wartungsmodus für alle Ressourcengruppen im vCenter-Server.
- Bereitet die Metadaten des vCenters vor und markiert es in der NetApp Console als nicht verwaltet.
- Konfiguriert den Datenbankzugriff.
- Erkennt VMware vCenter, Datenspeicher und VMs.
- Importiert bestehende Schutzrichtlinien, Snapshots sowie Sicherungs- und Wiederherstellungsoptionen aus dem SnapCenter Plug-in for VMware vSphere.
- Zeigt die erkannten Ressourcen auf der Inventarseite von NetApp Backup and Recovery an.

Die Ermittlung erfolgt auf folgende Weise:

- Wenn Sie bereits über das SnapCenter Plug-in for VMware vSphere verfügen, importieren Sie SnapCenter Ressourcen mithilfe der NetApp Backup and Recovery -Benutzeroberfläche in NetApp Backup and Recovery and Recovery.

  Wenn Sie bereits über das SnapCenter -Plug-in verfügen, stellen Sie sicher, dass Sie die Voraussetzungen erfüllt haben, bevor Sie aus SnapCenter importieren. Beispielsweise sollten Sie zunächst in der NetApp Console Systeme für den gesamten lokalen SnapCenter -Clusterspeicher erstellen, bevor Sie aus SnapCenter importieren. Sehen"Voraussetzungen für den Import von Ressourcen aus SnapCenter" .

- Wenn Sie das SnapCenter -Plug-in noch nicht haben, können Sie Workloads in Ihren Systemen trotzdem ermitteln, indem Sie manuell ein vCenter hinzufügen und die Erkennung durchführen.

Wenn das SnapCenter Plug-in noch nicht installiert ist, fügen Sie ein vCenter hinzu und ermitteln Sie Ressourcen

Wenn Sie das SnapCenter Plug-in für VMware noch nicht installiert haben, fügen Sie vCenter-Informationen hinzu und lassen Sie NetApp Backup and Recovery die Workloads erkennen. Wählen Sie in jedem Konsolenagenten die Systeme aus, auf denen Sie Workloads ermitteln möchten.

Schritte

1. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Sicherung und Wiederherstellung**.

   Wenn Sie sich zum ersten Mal bei Backup and Recovery anmelden und zwar ein System in der Konsole haben, aber keine Ressourcen erkannt wurden, wird die Seite *Willkommen bei der neuen NetApp Backup and Recovery* mit einer Option zum **Erkennen von Ressourcen** angezeigt.

2. Wählen Sie **Ressourcen entdecken**.
3. Geben Sie die folgenden Informationen ein:
   a. **Workload-Typ**: Wählen Sie **VMware**.
   b. **vCenter-Einstellungen**: Fügen Sie ein neues vCenter hinzu. Um ein neues vCenter hinzuzufügen, geben Sie den FQDN oder die IP-Adresse, den Benutzernamen, das Kennwort, den Port und das Protokoll des vCenters ein.

Wenn Sie vCenter-Informationen eingeben, geben Sie Informationen sowohl für die vCenter-Einstellungen als auch für die Host-Registrierung ein. Wenn Sie hier vCenter-Informationen hinzugefügt oder eingegeben haben, müssen Sie als Nächstes auch Plugin-Informationen in den erweiterten Einstellungen hinzufügen.

c. **Host-Registrierung**: Für VMware nicht erforderlich.

4. Wählen Sie **Entdecken**.

Dieser Vorgang kann einige Minuten dauern.

5. Fahren Sie mit den erweiterten Einstellungen fort.

Wenn das SnapCenter -Plugin bereits installiert ist, importieren Sie das SnapCenter -Plugin für VMware-Ressourcen in NetApp Backup and Recovery

Wenn Sie das SnapCenter Plug-in für VMware bereits installiert haben, importieren Sie die SnapCenter Plug-in-Ressourcen mit diesen Schritten in NetApp Backup and Recovery . Die Konsole erkennt ESXi-Hosts, Datenspeicher und VMs in vCentern und plant sie vom Plug-in aus. Sie müssen diese Informationen nicht alle neu erstellen.

Sie können dies auf folgende Weise tun:

- Wählen Sie während der Erkennung eine Option zum Importieren von Ressourcen aus dem SnapCenter -Plug-in aus.
- Wählen Sie nach der Erkennung auf der Inventarseite eine Option zum Importieren von SnapCenter -Plug -in-Ressourcen aus.
- Wählen Sie nach der Erkennung im Menü „Einstellungen“ eine Option zum Importieren von SnapCenter -Plug-in-Ressourcen aus. Weitere Einzelheiten finden Sie unter"Konfigurieren von NetApp Backup and Recovery" . Dies wird für VMware nicht unterstützt.

Dies ist ein zweiteiliger Prozess, der in diesem Abschnitt beschrieben wird:

1. Importieren Sie die vCenter-Metadaten aus dem SnapCenter -Plug-in. Die importierten vCenter-Ressourcen werden noch nicht von NetApp Backup and Recovery verwaltet.
2. Starten Sie die Verwaltung ausgewählter vCenter, VMs und Datenspeicher in NetApp Backup and Recovery. Nachdem Sie die Verwaltung initiiert haben, kennzeichnet NetApp Backup and Recovery das vCenter auf der Inventarseite als „Verwaltet“ und kann die von Ihnen importierten Ressourcen sichern und wiederherstellen. Nachdem Sie die Verwaltung in NetApp Backup and Recovery initiiert haben, verwalten Sie diese Ressourcen nicht mehr im SnapCenter Plug-in.

Importieren Sie vCenter-Metadaten aus dem SnapCenter -Plug-in

In diesem ersten Schritt werden vCenter-Metadaten aus dem SnapCenter -Plug-in importiert. Zu diesem Zeitpunkt werden die Ressourcen noch nicht von NetApp Backup and Recovery verwaltet.

Nachdem Sie vCenter-Metadaten aus dem SnapCenter -Plug-in importiert haben, übernimmt NetApp Backup and Recovery die Schutzverwaltung nicht automatisch. Dazu müssen Sie explizit auswählen, dass die importierten Ressourcen in NetApp Backup and Recovery verwaltet werden sollen. Dadurch wird sichergestellt, dass Sie bereit sind, diese Ressourcen durch NetApp Backup and Recovery sichern zu lassen.

Schritte

1. Wählen Sie in der linken Navigation der Konsole **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie **Inventar**.
3. Wählen Sie auf der Seite „Workload-Ressourcen von NetApp Backup and Recovery ermitteln“ die Option „Aus SnapCenter importieren“ aus.
4. Wählen Sie im Feld „Importieren von“ die Option „SnapCenter Plug-in für VMware“ aus.
5. Geben Sie **VMware vCenter-Anmeldeinformationen** ein:
   a. **vCenter-IP/Hostname**: Geben Sie den FQDN oder die IP-Adresse des vCenters ein, das Sie in NetApp Backup and Recovery importieren möchten.
   b. **vCenter-Portnummer**: Geben Sie die Portnummer für das vCenter ein.
   c. **vCenter-Benutzername** und **Passwort**: Geben Sie den Benutzernamen und das Passwort für das vCenter ein.
   d. **Connector**: Wählen Sie den Konsolenagenten für das vCenter aus.
6. Geben Sie * Host-Anmeldeinformationen für das SnapCenter -Plug-in* ein:
   a. **Vorhandene Anmeldeinformationen**: Wenn Sie diese Option auswählen, können Sie die vorhandenen Anmeldeinformationen verwenden, die Sie bereits hinzugefügt haben. Wählen Sie den Namen der Anmeldeinformationen.
   b. **Neue Anmeldeinformationen hinzufügen**: Wenn Sie keine vorhandenen Anmeldeinformationen für den SnapCenter Plug-in-Host haben, können Sie neue Anmeldeinformationen hinzufügen. Geben Sie den Anmeldenamen, den Authentifizierungsmodus, den Benutzernamen und das Kennwort ein.
7. Wählen Sie **Importieren**, um Ihre Eingaben zu bestätigen und das SnapCenter -Plug-in zu registrieren.

> Wenn das SnapCenter Plug-in bereits registriert ist, können Sie die vorhandenen Registrierungsdetails aktualisieren.

Ergebnis

Auf der Inventarseite wird das vCenter in NetApp Backup and Recovery als nicht verwaltet angezeigt, bis Sie es explizit für die Verwaltung auswählen.

Verwalten von aus dem SnapCenter -Plug-in importierten Ressourcen

Nachdem Sie die vCenter-Metadaten aus dem SnapCenter -Plug-in für VMware importiert haben, verwalten Sie die Ressourcen in NetApp Backup and Recovery. Nachdem Sie die Verwaltung dieser Ressourcen ausgewählt haben, kann NetApp Backup and Recovery die importierten Ressourcen sichern und wiederherstellen. Nachdem Sie die Verwaltung in NetApp Backup and Recovery initiiert haben, verwalten Sie diese Ressourcen nicht mehr im SnapCenter Plug-in.

Nachdem Sie die Verwaltung der Ressourcen ausgewählt haben, werden die Ressourcen, VMs und Richtlinien aus dem SnapCenter -Plug-in für VMware importiert. Die Ressourcengruppen, Richtlinien und Snapshots werden vom Plug-in migriert und in NetApp Backup and Recovery verwaltet.

Schritte

1. Nachdem Sie die VMware-Ressourcen aus dem SnapCenter -Plug-in importiert haben, wählen Sie im Menü „Sichern und Wiederherstellen“ die Option „Inventar“ aus.
2. Wählen Sie auf der Inventarseite das importierte vCenter aus, das von nun an von NetApp Backup and Recovery verwaltet werden soll.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**, um die Arbeitslastdetails anzuzeigen.

4. Wählen Sie auf der Seite Inventar > Arbeitslast das Symbol Aktionen ••• > **Verwalten**, um die Seite „vCenter verwalten“ anzuzeigen.
5. Aktivieren Sie das Kontrollkästchen „Möchten Sie mit der Migration fortfahren?“ und wählen Sie **Migrieren**.

Ergebnis

Auf der Inventarseite werden die neu verwalteten vCenter-Ressourcen angezeigt.

Weiter zum NetApp Backup and Recovery Dashboard

1. Um das Dashboard anzuzeigen, wählen Sie im Menü „Sicherung und Wiederherstellung“ die Option **Dashboard**.
2. 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".

Erstellen und verwalten Sie Schutzgruppen für VMware-Workloads mit NetApp Backup and Recovery

Erstellen Sie Schutzgruppen, um die Sicherungs- und Wiederherstellungsvorgänge für eine Reihe von Workloads zu verwalten. Eine Schutzgruppe ist eine logische Gruppierung von Ressourcen wie VMs und Datenspeichern, die Sie gemeinsam schützen möchten.

Sie können die folgenden Aufgaben im Zusammenhang mit Schutzgruppen ausführen:

- Erstellen Sie eine Schutzgruppe.
- Schutzdetails anzeigen.
- Sichern Sie jetzt eine Schutzgruppe. Sehen"Sichern Sie jetzt VMware-Workloads" .
- Unterbrechen und Fortsetzen des Sicherungszeitplans einer Schutzgruppe.
- Löschen Sie eine Schutzgruppe.

Erstellen einer Schutzgruppe

Gruppieren Sie Workloads, die Sie schützen möchten, in einer Schutzgruppe, um sie gemeinsam zu sichern und wiederherzustellen.

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

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.
5. Wählen Sie **Schutzgruppe erstellen**.

6. Geben Sie einen Namen für die Schutzgruppe ein.
7. Wählen Sie die VMs oder Datenbanken aus, die Sie in die Schutzgruppe aufnehmen möchten.
8. Wählen Sie **Weiter**.
9. Wählen Sie die **Sicherungsrichtlinie** aus, die Sie auf die Schutzgruppe anwenden möchten.

   Wenn Sie eine Richtlinie erstellen möchten, wählen Sie **Neue Richtlinie erstellen** und folgen Sie den Anweisungen zum Erstellen einer Richtlinie. Sehen"Erstellen von Richtlinien" für weitere Informationen.

10. Wählen Sie **Weiter**.
11. Überprüfen Sie die Konfiguration.
12. Wählen Sie **Erstellen** aus, um die Schutzgruppe zu erstellen.

Aussetzen des Sicherungszeitplans einer Schutzgruppe

Setzen Sie eine Schutzgruppe aus, um ihre geplanten Sicherungen anzuhalten.

Wenn Sie eine Schutzgruppe aussetzen, ändert sich der Schutzstatus in „In Wartung“. Sie können den Sicherungszeitplan jederzeit fortsetzen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.
5. Wählen Sie das Symbol Aktionen ••• > **Schutzgruppe aussetzen**.
6. Überprüfen Sie die Bestätigungsnachricht und wählen Sie **Aussetzen**.

Fortsetzen des Sicherungszeitplans einer Schutzgruppe

Durch die Wiederaufnahme einer angehaltenen Schutzgruppe werden die geplanten Sicherungen für die Schutzgruppe neu gestartet.

Der Schutzstatus ändert sich von „In Wartung“, wenn Sie eine Schutzgruppe aussetzen, zu „Geschützt“, wenn Sie sie wieder aufnehmen. Sie können den Sicherungszeitplan jederzeit fortsetzen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.
5. Wählen Sie das Symbol Aktionen ••• > **Schutzgruppe fortsetzen**.
6. Überprüfen Sie die Bestätigungsnachricht und wählen Sie **Fortsetzen**.

Ergebnis

Das System validiert die Zeitpläne und ändert den Schutzstatus auf „Geschützt“, wenn die Zeitpläne gültig sind. Wenn die Zeitpläne ungültig sind, zeigt das System eine Fehlermeldung an und nimmt die Schutzgruppe nicht wieder auf.

Löschen einer Schutzgruppe

Wenn Sie eine Schutzgruppe löschen, entfernen Sie diese und alle Sicherungszeitpläne für die Gruppe. Löschen Sie eine Schutzgruppe, wenn Sie sie nicht mehr benötigen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.
5. Wählen Sie die Schutzgruppe aus, die Sie löschen möchten.
6. Wählen Sie das Symbol Aktionen ••• > **Löschen**.
7. Überprüfen Sie die Bestätigungsmeldung zum Löschen der zugehörigen Sicherungen und bestätigen Sie den Löschvorgang.

Sichern Sie VMware-Workloads mit NetApp Backup and Recovery

Sichern Sie VMware-VMs und Datenspeicher von lokalen ONTAP -Systemen auf Amazon Web Services, Azure NetApp Files oder StorageGRID , um sicherzustellen, dass Ihre Daten geschützt sind. Backups werden automatisch erstellt und in einem Objektspeicher in Ihrem öffentlichen oder privaten Cloud-Konto gespeichert.

- Um Workloads nach einem Zeitplan zu sichern, erstellen Sie Richtlinien, die die Sicherungs- und Wiederherstellungsvorgänge steuern. Sehen"Erstellen von Richtlinien" Anweisungen hierzu finden Sie unter.
- Erstellen Sie Schutzgruppen, um die Sicherungs- und Wiederherstellungsvorgänge für eine Reihe von Ressourcen zu verwalten. Sehen"Erstellen und verwalten Sie Schutzgruppen für VMware-Workloads mit NetApp Backup and Recovery" für weitere Informationen.
- Sichern Sie jetzt Workloads (erstellen Sie jetzt ein On-Demand-Backup).

Sichern Sie Workloads jetzt mit einem On-Demand-Backup

Erstellen Sie sofort ein On-Demand-Backup. Möglicherweise möchten Sie eine On-Demand-Sicherung ausführen, wenn Sie Änderungen an Ihrem System vornehmen und sicherstellen möchten, dass Sie vor dem Start über eine Sicherung verfügen.

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Wiederherstellung oder Backup-Administratorrolle für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im Menü „Sicherung und Wiederherstellung“ die Option „Inventar“ aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**, **Datenspeicher** oder **Virtuelle Maschinen**.
5. Wählen Sie die Schutzgruppe, Datenspeicher oder virtuellen Maschinen aus, die Sie sichern möchten.
6. Wählen Sie das Symbol Aktionen ••• > **Jetzt sichern**.

Die auf die Sicherung angewendete Richtlinie ist dieselbe Richtlinie, die der Schutzgruppe, dem Datenspeicher oder der virtuellen Maschine zugewiesen ist.

7. Wählen Sie die Zeitplanstufe aus.
8. Wählen Sie **Jetzt sichern**.

Wiederherstellen von VMware-Workloads

Wiederherstellen von VMware-Workloads mit NetApp Backup and Recovery

VMware-Workloads können mithilfe von NetApp Backup and Recovery aus Snapshots, aus einer auf einen Sekundärspeicher replizierten Workload-Sicherung oder aus in Objektspeichern gespeicherten Sicherungen wiederhergestellt werden.

Von diesen Speicherorten wiederherstellen

Sie können Workloads von verschiedenen Startorten wiederherstellen:

- Wiederherstellung von einem primären Standort (lokaler Snapshot)
- Wiederherstellen von einer replizierten Ressource auf einem sekundären Speicher
- Wiederherstellung aus einer Objektspeichersicherung

Stellen Sie diese Punkte wieder her

Sie können Daten bis zu diesen Punkten wiederherstellen:

- **Wiederherstellung am ursprünglichen Speicherort**: Die VM wird am ursprünglichen Speicherort wiederhergestellt, und zwar in derselben vCenter-Bereitstellung, auf demselben ESXi-Host und im selben Datenspeicher. Die VM und alle darauf befindlichen Daten werden überschrieben.
- **Wiederherstellung an einem alternativen Speicherort**: Sie können einen anderen vCenter-Server, ESXi-Host oder Datenspeicher als Wiederherstellungsziel für die VM auswählen. Dies ist nützlich, um verschiedene Kopien derselben VM an unterschiedlichen Standorten und in verschiedenen Zuständen zu verwalten.

Überlegungen zur Wiederherstellung aus dem Objektspeicher

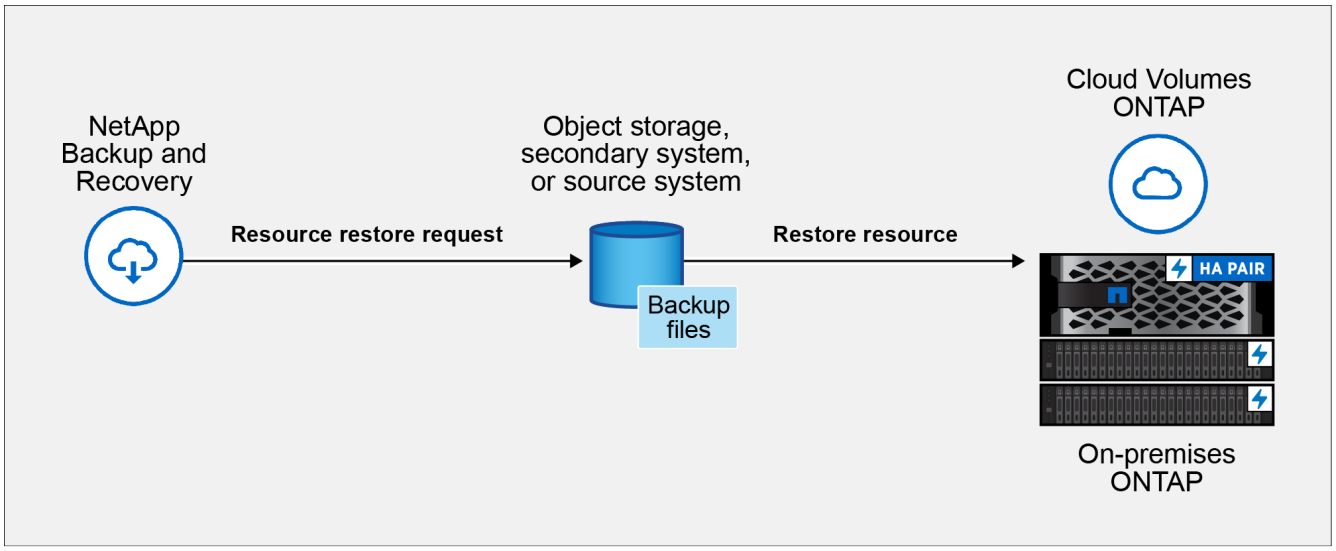
Wenn Ransomware Resilience für eine Sicherungsdatei im Objektspeicher aktiviert ist, werden Sie aufgefordert, vor der Wiederherstellung eine zusätzliche Prüfung durchzuführen. Wir empfehlen, den Scan durchzuführen.

Möglicherweise zahlen Sie Ihrem Cloud-Anbieter zusätzliche Gebühren für den Zugriff auf die Sicherungsdatei.

So funktioniert die Wiederherstellung von Workloads

Beim Wiederherstellen von Workloads geschieht Folgendes:

- Wenn Sie eine Arbeitslast aus einem lokalen Snapshot oder einem Remote-Backup wiederherstellen, überschreibt NetApp Backup and Recovery die ursprüngliche VM, wenn Sie die Wiederherstellung am ursprünglichen Speicherort vornehmen, und erstellt eine *neue* Ressource, wenn Sie die Wiederherstellung an einem alternativen Speicherort vornehmen.
- Bei der Wiederherstellung einer replizierten Arbeitslast können Sie die Arbeitslast auf dem ursprünglichen lokalen ONTAP System oder auf einem anderen lokalen ONTAP System wiederherstellen.



- Wenn Sie eine Sicherung aus dem Objektspeicher wiederherstellen, können Sie die Daten auf dem ursprünglichen System oder auf einem lokalen ONTAP -System wiederherstellen.

Auf der Seite „Wiederherstellen“ (Suchen und Wiederherstellen) können Sie eine Ressource wiederherstellen, indem Sie mithilfe von Filtern nach dem Snapshot suchen, auch wenn Sie sich nicht an den genauen Namen, den Speicherort oder das letzte bekannte Datum erinnern.

Wiederherstellen von Workload-Daten über die Option „Wiederherstellen“ (Suchen und Wiederherstellen)

Stellen Sie VMware-Workloads mithilfe der Option „Wiederherstellen“ wieder her. Sie können nach dem Snapshot anhand seines Namens oder mithilfe von Filtern suchen.

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Wiederherstellung, Administratorrolle für Backup- und Wiederherstellungswiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Wiederherstellen** aus.
2. Wählen Sie in der Dropdown-Liste rechts neben dem Namenssuchfeld **VMware** aus.
3. Geben Sie den Namen der Ressource ein, die Sie wiederherstellen möchten, oder filtern Sie nach dem vCenter, Rechenzentrum oder Datenspeicher, in dem sich die wiederherzustellende Ressource befindet.

   Es erscheint eine Liste virtueller Maschinen, die Ihren Suchkriterien entsprechen.

4. Suchen Sie in der Liste die VM, von der Sie die VM wiederherstellen möchten, und wählen Sie die entsprechende Menüschaltfläche für diese VM aus.
5. Wählen Sie im daraufhin angezeigten Menü die Option **Virtuelle Maschine wiederherstellen**.

   Es wird eine Liste der auf dieser virtuellen Maschine erstellten Snapshots (Wiederherstellungspunkte) angezeigt. Standardmäßig werden die neuesten Snapshots für den im Dropdown-Menü **Zeitraum** ausgewählten Zeitraum angezeigt.

   Für jeden Snapshot zeigen alle leuchtenden Symbole in der Spalte **Speicherort** die Speicherorte an, an denen der Snapshot verfügbar ist (primärer Speicher, sekundärer Speicher oder Objektspeicher).

6. Aktivieren Sie das Optionsfeld für den Snapshot, den Sie wiederherstellen möchten.

7. Wählen Sie **Weiter**.

   Optionen zum Speichern des Schnappschusses werden angezeigt.

8. Wählen Sie das Wiederherstellungsziel für den Snapshot aus:
   - **Lokal**: Stellt den Snapshot vom lokalen Speicherort wieder her.
   - **Sekundär**: Stellt den Snapshot von einem entfernten Speicherort wieder her.
   - **Objektspeicher**: Stellt den Snapshot aus dem Objektspeicher wieder her.

     Wenn Sie sich für einen sekundären Speicher entscheiden, wählen Sie den Zielspeicherort aus der Dropdown-Liste aus.

9. Wählen Sie **Weiter**, um fortzufahren.
10. Wählen Sie das Wiederherstellungsziel und die Einstellungen aus:

Zielauswahl

Am ursprünglichen Speicherort wiederherstellen

Bei der Wiederherstellung am ursprünglichen Speicherort können Sie weder das Ziel-vCenter, den ESXi-Host, den Datenspeicher noch den Namen der VM ändern. Die ursprüngliche VM wird bei der Wiederherstellungsoperation überschrieben.

1. Wählen Sie den Bereich **Ursprünglicher Speicherort** aus.
2. Wählen Sie aus den folgenden Optionen:
   - Abschnitt **Optionen vor der Wiederherstellung**:
     - **Vorgabe**: Aktivieren Sie diese Option, um zusätzliche Aufgaben zu automatisieren, indem Sie vor Beginn des Wiederherstellungsvorgangs ein benutzerdefiniertes Skript ausführen. Geben Sie den vollständigen Pfad zu dem auszuführenden Skript sowie alle Argumente an, die das Skript benötigt.
   - Abschnitt **Optionen nach der Wiederherstellung**:
     - **Virtuelle Maschine neu starten**: Aktivieren Sie diese Option, um die virtuelle Maschine nach Abschluss des Wiederherstellungsvorgangs und nach Anwendung des Nachwiederherstellungsskripts neu zu starten.
     - **Nachtrag**: Aktivieren Sie diese Option, um zusätzliche Aufgaben zu automatisieren, indem Sie nach Abschluss der Wiederherstellung ein benutzerdefiniertes Skript ausführen. Geben Sie den vollständigen Pfad zu dem auszuführenden Skript sowie alle Argumente an, die das Skript benötigt.
3. Wählen Sie **Wiederherstellen**.

An einem anderen Speicherort wiederherstellen

Bei der Wiederherstellung an einem alternativen Speicherort können Sie das Ziel-vCenter, den ESXi-Host, den Datenspeicher und den Namen der VM ändern, um eine neue Kopie der VM an einem anderen Speicherort oder mit einem anderen Namen zu erstellen.

1. Wählen Sie den Bereich **Alternativer Standort** aus.
2. Geben Sie die folgenden Informationen ein:
   - Abschnitt **Zieleinstellungen**:
     - **vCenter FQDN oder IP-Adresse**: Wählen Sie den vCenter-Server aus, auf dem Sie den Snapshot wiederherstellen möchten.
     - **ESXi-Host**: Wählen Sie den Host aus, auf dem Sie den Snapshot wiederherstellen möchten.
     - **Netzwerk**: Wählen Sie das Netzwerk aus, in dem Sie den Snapshot wiederherstellen möchten.
     - **Datenspeicher**: Wählen Sie in der Dropdown-Liste den Namen des Datenspeichers aus, in dem Sie den Snapshot wiederherstellen möchten.
     - **Name der virtuellen Maschine**: Geben Sie den Namen der VM ein, auf der Sie den Snapshot wiederherstellen möchten. Wenn der Name mit einer bereits im Datenspeicher vorhandenen VM übereinstimmt, sorgt Backup and Recovery für einen eindeutigen Namen, indem ein aktueller Zeitstempel angehängt wird.
   - Abschnitt **Optionen vor der Wiederherstellung**:
     - **Vorgabe**: Aktivieren Sie diese Option, um zusätzliche Aufgaben zu automatisieren, indem Sie vor Beginn des Wiederherstellungsvorgangs ein benutzerdefiniertes Skript ausführen. Geben Sie den vollständigen Pfad zu dem auszuführenden Skript sowie alle Argumente an, die das Skript benötigt.

- Abschnitt **Optionen nach der Wiederherstellung**:
  - **Virtuelle Maschine neu starten**: Aktivieren Sie diese Option, um die virtuelle Maschine nach Abschluss des Wiederherstellungsvorgangs und nach Anwendung des Nachwiederherstellungsskripts neu zu starten.
  - **Nachtrag**: Aktivieren Sie diese Option, um zusätzliche Aufgaben zu automatisieren, indem Sie nach Abschluss der Wiederherstellung ein benutzerdefiniertes Skript ausführen. Geben Sie den vollständigen Pfad zu dem auszuführenden Skript sowie alle Argumente an, die das Skript benötigt.

3. Wählen Sie **Wiederherstellen**.

Bestimmte virtuelle Festplatten aus Backups wiederherstellen

Sie können vorhandene virtuelle Festplatten (VMDKs) oder gelöschte bzw. getrennte virtuelle Festplatten aus primären oder sekundären Backups herkömmlicher VMs wiederherstellen. Dadurch können Sie nur bestimmte VM-Daten oder Anwendungen wiederherstellen, sodass Sie nicht die gesamte VM und alle zugehörigen virtuellen Festplatten wiederherstellen müssen, wenn nur bestimmte Daten betroffen sind. Nach der Wiederherstellung der virtuellen Festplatte wird diese wieder an die ursprüngliche VM angebunden und ist sofort einsatzbereit.

Sie können eine oder mehrere virtuelle Maschinenfestplatten (VMDKs) einer VM auf demselben Datenspeicher oder auf verschiedenen Datenspeichern wiederherstellen.

Aktivieren Sie die VMware-Anwendung vStorage API for Array Integration (VAAI), um die Leistung von Wiederherstellungsvorgängen in NFS-Umgebungen zu verbessern.

Bevor Sie beginnen

- Es muss ein Backup vorhanden sein.
- Die VM darf sich nicht im Transit befinden.

  Die VM, die Sie wiederherstellen möchten, darf sich nicht im Zustand vMotion oder Storage vMotion befinden.

Informationen zu diesem Vorgang

- Wenn das VMDK gelöscht oder von der VM getrennt wird, wird das VMDK beim Wiederherstellungsvorgang an die VM angehängt.
- Ein Wiederherstellungsvorgang kann fehlschlagen, wenn die Speicherebene des FabricPool , in dem sich die VM befindet, nicht verfügbar ist.
- Anfügen- und Wiederherstellungsvorgänge verbinden VMDKs mithilfe des Standard-SCSi-Controllers. Wenn jedoch VMDKs gesichert werden, die an eine VM mit einer NVMe-Festplatte angeschlossen sind, verwenden die Anfüge- und Wiederherstellungsvorgänge den NVMe-Controller, sofern verfügbar.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Wiederherstellen** aus.
2. Wählen Sie in der Dropdown-Liste rechts neben dem Namenssuchfeld **VMware** aus.
3. Geben Sie den Namen der Ressource ein, die Sie wiederherstellen möchten, oder filtern Sie nach dem vCenter, Rechenzentrum oder Datenspeicher, in dem sich die wiederherzustellende Ressource befindet.

Es erscheint eine Liste virtueller Maschinen, die Ihren Suchkriterien entsprechen.

4. Suchen Sie in der Liste die VM, von der Sie die VM wiederherstellen möchten, und wählen Sie die entsprechende Menüschaltfläche für diese VM aus.
5. Wählen Sie im daraufhin angezeigten Menü die Option **Virtuelle Festplatten wiederherstellen**.

   Es wird eine Liste der auf dieser virtuellen Maschine erstellten Snapshots (Wiederherstellungspunkte) angezeigt. Standardmäßig werden die neuesten Snapshots für den im Dropdown-Menü **Zeitraum** ausgewählten Zeitraum angezeigt.

   Für jeden Snapshot zeigen alle leuchtenden Symbole in der Spalte **Speicherort** die Speicherorte an, an denen der Snapshot verfügbar ist (primärer Speicher, sekundärer Speicher oder Objektspeicher).
6. Aktivieren Sie das Optionsfeld für den Snapshot, den Sie wiederherstellen möchten.
7. Wählen Sie **Weiter**.

   Optionen zum Speichern des Schnappschusses werden angezeigt.
8. Wählen Sie das Wiederherstellungsziel für den Snapshot aus:
   - **Lokal**: Stellt den Snapshot vom lokalen Speicherort wieder her.
   - **Sekundär**: Stellt den Snapshot von einem entfernten Speicherort wieder her.
   - **Objektspeicher**: Stellt den Snapshot aus dem Objektspeicher wieder her.

     Wenn Sie sich für einen sekundären Speicher entscheiden, wählen Sie den Zielspeicherort aus der Dropdown-Liste aus.
9. Wählen Sie **Weiter**, um fortzufahren.
10. Wählen Sie das Wiederherstellungsziel und die Einstellungen aus:

Zielauswahl

Am ursprünglichen Speicherort wiederherstellen

Bei der Wiederherstellung am ursprünglichen Speicherort können Sie weder das Ziel-vCenter, den ESXi-Host, den Datenspeicher noch den Namen der virtuellen Festplatte ändern. Die ursprüngliche virtuelle Festplatte wird überschrieben.

1. Wählen Sie den Bereich **Ursprünglicher Speicherort** aus.
2. Aktivieren Sie im Abschnitt **Zieleinstellungen** das Kontrollkästchen für alle virtuellen Festplatten, die Sie wiederherstellen möchten.
3. Wählen Sie aus den folgenden Optionen:
   - Abschnitt **Optionen vor der Wiederherstellung**:
     - **Vorgabe**: Aktivieren Sie diese Option, um zusätzliche Aufgaben zu automatisieren, indem Sie vor Beginn des Wiederherstellungsvorgangs ein benutzerdefiniertes Skript ausführen. Geben Sie den vollständigen Pfad zu dem auszuführenden Skript sowie alle Argumente an, die das Skript benötigt.
   - Abschnitt **Optionen nach der Wiederherstellung**:
     - **Nachtrag**: Aktivieren Sie diese Option, um zusätzliche Aufgaben zu automatisieren, indem Sie nach Abschluss der Wiederherstellung ein benutzerdefiniertes Skript ausführen. Geben Sie den vollständigen Pfad zu dem auszuführenden Skript sowie alle Argumente an, die das Skript benötigt.
4. Wählen Sie **Wiederherstellen**.

An einem anderen Speicherort wiederherstellen

Bei der Wiederherstellung an einem alternativen Speicherort kann der Zieldatenspeicher geändert werden. Die virtuelle Festplatte wird nach dem Wiederherstellungsvorgang unabhängig vom gewählten Datenspeicher an die ursprüngliche VM angehängt.

1. Wählen Sie den Bereich **Alternativer Standort** aus.
2. Aktivieren Sie im Abschnitt **Zieleinstellungen** das Kontrollkästchen für alle virtuellen Festplatten, die Sie wiederherstellen möchten.
3. Für alle von Ihnen ausgewählten virtuellen Festplatten:
   a. Wählen Sie **Datenspeicher auswählen**, um ein anderes Datenspeicherziel für die Wiederherstellung der virtuellen Festplatte auszuwählen.
   b. Wählen Sie **Auswählen**, um Ihre Auswahl zu bestätigen und das Auswahlfenster zu schließen.
4. Wählen Sie aus den folgenden Optionen:
   - Abschnitt **Optionen vor der Wiederherstellung**:
     - **Vorgabe**: Aktivieren Sie diese Option, um zusätzliche Aufgaben zu automatisieren, indem Sie vor Beginn des Wiederherstellungsvorgangs ein benutzerdefiniertes Skript ausführen. Geben Sie den vollständigen Pfad zu dem auszuführenden Skript sowie alle Argumente an, die das Skript benötigt.
   - Abschnitt **Optionen nach der Wiederherstellung**:
     - **Nachtrag**: Aktivieren Sie diese Option, um zusätzliche Aufgaben zu automatisieren, indem Sie nach Abschluss der Wiederherstellung ein benutzerdefiniertes Skript ausführen. Geben Sie den vollständigen Pfad zu dem auszuführenden Skript sowie alle Argumente an, die das Skript benötigt.
5. Wählen Sie **Wiederherstellen**.

Gastdateien und -ordner wiederherstellen

Anforderungen und Einschränkungen beim Wiederherstellen von Gastdateien und -ordnern

Sie können Dateien oder Ordner von einer virtuellen Maschinenfestplatte (VMDK) auf einem Windows-Gastbetriebssystem wiederherstellen.

Workflow zur Gastwiederherstellung

Die Wiederherstellungsvorgänge des Gastbetriebssystems umfassen die folgenden Schritte:

1. Befestigen

   Binden Sie eine virtuelle Festplatte an eine Gast-VM an und starten Sie eine Gastdatei-Wiederherstellungssitzung.

2. Warten

   Warten Sie, bis der Anfügevorgang abgeschlossen ist, bevor Sie durchsuchen und wiederherstellen können. Nach Abschluss des Anfügevorgangs wird automatisch eine Gastdatei-Wiederherstellungssitzung erstellt.

3. Dateien oder Ordner auswählen

   Durchsuchen Sie die VMDK-Dateien und wählen Sie eine oder mehrere Dateien oder Ordner zur Wiederherstellung aus.

4. Wiederherstellen

   Stellen Sie die ausgewählten Dateien oder Ordner an einem angegebenen Speicherort wieder her.

Voraussetzungen für die Wiederherstellung von Gastdateien und -ordnern

Prüfen Sie alle Voraussetzungen, bevor Sie Dateien oder Ordner aus einer VMDK-Datei auf einem Windows-Gastbetriebssystem wiederherstellen.

- VMware-Tools müssen installiert und ausgeführt werden.

  NetApp Backup and Recovery nutzt Informationen von VMware Tools, um eine Verbindung zum VMware-Gastbetriebssystem herzustellen.

- Als Gastbetriebssystem muss Windows Server 2008 R2 oder höher ausgeführt werden.

  Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperability Matrix Tool (IMT)" .

- Die Anmeldeinformationen für die Ziel-VM verwenden das integrierte Domänen- oder lokale Administratorkonto mit dem Benutzernamen „Administrator“. Bevor Sie mit dem Wiederherstellungsvorgang beginnen, konfigurieren Sie die Anmeldeinformationen für die VM, an die Sie die virtuelle Festplatte anhängen möchten. Für den Anfüge- und Wiederherstellungsvorgang werden Anmeldeinformationen benötigt. Benutzer von Arbeitsgruppen können das integrierte lokale Administratorkonto verwenden.

Wenn Sie ein Konto verwenden müssen, das nicht das integrierte Administratorkonto ist, aber über Administratorrechte innerhalb der VM verfügt, müssen Sie die Benutzerkontensteuerung auf der Gast-VM deaktivieren.

- Sie müssen den Sicherungs-Snapshot und das VMDK kennen, von dem die Wiederherstellung durchgeführt werden soll.

  NetApp Backup and Recovery unterstützt keine Suche nach wiederherzustellenden Dateien oder Ordnern. Bevor Sie beginnen, müssen Sie wissen, wo sich die Dateien oder Ordner im Snapshot und die zugehörige VMDK befinden.

- Die anzuhängende virtuelle Festplatte muss sich in einem NetApp Backup and Recovery -Backup befinden.

  Die virtuelle Festplatte, die die wiederherzustellende Datei oder den Ordner enthält, muss sich in einer VM-Sicherung befinden, die mit NetApp Backup and Recovery erstellt wurde.

- Dateien mit Namen, die nicht aus dem englischen Alphabet stammen, müssen Sie in einem Verzeichnis und nicht als einzelne Datei wiederherstellen.

  Sie können Dateien mit nicht-alphabetischen Namen, wie etwa japanische Kanji, wiederherstellen, indem Sie das Verzeichnis wiederherstellen, in dem sich die Dateien befinden.

Einschränkungen bei der Wiederherstellung von Gastdateien

Bevor Sie eine Datei oder einen Ordner aus einem Gastbetriebssystem wiederherstellen, sollten Sie sich über die Funktionsbeschränkungen im Klaren sein.

- Sie können dynamische Datenträgertypen nicht innerhalb eines Gastbetriebssystems wiederherstellen.
- Wenn Sie eine verschlüsselte Datei oder einen verschlüsselten Ordner wiederherstellen, bleibt das Verschlüsselungsattribut nicht erhalten.
- Sie können keine Dateien oder Ordner in einem verschlüsselten Ordner wiederherstellen.
- Versteckte Dateien und Ordner werden auf der Dateiauswahlseite angezeigt und können nicht gefiltert werden.
- Eine Wiederherstellung von einem Linux-Gastbetriebssystem ist nicht möglich.

  Sie können keine Dateien und Ordner von einer VM wiederherstellen, auf der ein Linux-Gastbetriebssystem ausgeführt wird. Sie können jedoch ein VMDK anhängen und die Dateien und Ordner dann manuell wiederherstellen. Aktuelle Informationen zu unterstützten Gastbetriebssystemen finden Sie im "NetApp Interoperability Matrix Tool (IMT)" .

- Sie können keine Wiederherstellung von einem NTFS-Dateisystem auf ein FAT-Dateisystem durchführen.

  Wenn Sie versuchen, vom NTFS-Format ins FAT-Format wiederherzustellen, wird der NTFS-Sicherheitsdeskriptor nicht kopiert, da das FAT-Dateisystem keine Windows-Sicherheitsattribute unterstützt.

- Sie können keine Gastdateien aus einem geklonten VMDK oder einem nicht initialisierten VMDK wiederherstellen.
- Sie können die Verzeichnisstruktur einer Datei nicht wiederherstellen.

  Wenn Sie eine Datei aus einem verschachtelten Verzeichnis wiederherstellen, stellt das System nur die

Datei selbst wieder her, nicht aber die Verzeichnisstruktur. Um die gesamte Verzeichnisstruktur wiederherzustellen, kopieren Sie das oberste Verzeichnis.

- Sie können keine Gastdateien von einer vVol-VM auf einem alternativen Host wiederherstellen.
- Sie können verschlüsselte Gastdateien nicht wiederherstellen.

Wiederherstellen von Gastdateien und -ordnern aus VMDKs

Sie können eine oder mehrere Dateien oder Ordner aus einem VMDK auf einem Windows-Gastbetriebssystem wiederherstellen.

Bevor Sie beginnen

Bevor Sie Dateien und Ordner der Gast-VM wiederherstellen können, müssen Sie in NetApp Backup and Recovery Anmeldeinformationen dafür erstellen. NetApp Backup and Recovery verwendet diese Anmeldeinformationen zur Authentifizierung bei der Gast-VM beim Anbinden der virtuellen Festplatte.

Informationen zu diesem Vorgang

Die Leistung der Wiederherstellung von Gastdateien oder -ordnern hängt von zwei Faktoren ab: der Größe der wiederherzustellenden Dateien oder Ordner und der Anzahl der wiederherzustellenden Dateien oder Ordner. Das Wiederherstellen einer großen Anzahl kleiner Dateien kann im Vergleich zum Wiederherstellen einer kleinen Anzahl großer Dateien länger dauern als erwartet, wenn der wiederherzustellende Datensatz dieselbe Größe hat.

Auf einer VM kann gleichzeitig nur ein Anfüge- oder Wiederherstellungsvorgang ausgeführt werden. Sie können auf derselben VM keine parallelen Anfüge- oder Wiederherstellungsvorgänge ausführen.

Mit der Gastwiederherstellungsfunktion können Sie Systemdateien und versteckte Dateien anzeigen und wiederherstellen sowie verschlüsselte Dateien anzeigen. Überschreiben Sie keine vorhandenen Systemdateien und stellen Sie verschlüsselte Dateien nicht in einem verschlüsselten Ordner wieder her. Während des Wiederherstellungsvorgangs werden die versteckten, System- und verschlüsselten Attribute der Gastdateien nicht in der wiederhergestellten Datei beibehalten. Das Anzeigen oder Durchsuchen reservierter Partitionen kann einen Fehler verursachen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie das Menü **Virtuelle Maschinen**.
3. Wählen Sie aus der Liste eine virtuelle Maschine aus, die die wiederherzustellenden Dateien enthält.
4. Wählen Sie das Symbol „Aktionen“ aus. ••• für diese VM.
5. Wählen Sie **Dateien und Ordner wiederherstellen**.
6. Wählen Sie einen Snapshot aus, aus dem die Wiederherstellung erfolgen soll, und klicken Sie dann auf **Weiter**.
7. Wählen Sie den Speicherort des Snapshots aus, von dem die Wiederherstellung erfolgen soll. Wenn Sie einen sekundären Speicherort auswählen, wählen Sie den sekundären Snapshot aus der Liste aus.
8. Wählen Sie **Weiter**.
9. Wählen Sie aus der Liste die virtuelle Festplatte aus, die an die VM angehängt werden soll, und klicken Sie dann auf **Weiter**.

10. Wenn Sie auf der Seite „Anmeldeinformationen für virtuelle Maschinen auswählen“ noch keine Anmeldeinformationen für die Gast-VM gespeichert haben, wählen Sie „Anmeldeinformationen hinzufügen“ und gehen Sie wie folgt vor:
    a. **Name der Anmeldeinformationen**: Geben Sie einen Namen für die Anmeldeinformationen ein.
    b. **Authentifizierungsmodus**: Wählen Sie **Windows**.
    c. **Agenten**: Wählen Sie aus der Liste einen Konsolenagenten aus, der die Kommunikation zwischen NetApp Backup and Recovery und diesem Host übernimmt.
    d. **Domänen- und Benutzername**: Geben Sie den NetBIOS- oder Domänen-FQDN und den Benutzernamen für die Anmeldeinformationen ein.
    e. **Passwort**: Geben Sie ein Passwort für die Anmeldeinformationen ein.
    f. Wählen Sie **Hinzufügen**.
11. Wählen Sie die Anmeldeinformationen der virtuellen Maschine aus, mit denen Sie sich bei der Gast-VM authentifizieren möchten.

    NetApp Backup and Recovery bindet die virtuelle Festplatte an die VM an und zeigt alle Dateien und Ordner an, einschließlich der versteckten. Es weist jeder Partition einen Laufwerksbuchstaben zu, einschließlich der systemreservierten Partitionen.

    Die von Ihnen ausgewählten Dateien und Ordner werden im rechten Bereich des Bildschirms aufgelistet.
12. Wählen Sie **Weiter**.
13. Geben Sie den UNC-Freigabepfad zum Gast ein, auf dem die ausgewählten Dateien wiederhergestellt werden.
    - Beispiel für eine IPv4-Adresse: `\\10.60.136.65\c$`
    - Beispiel für eine IPv6-Adresse: `\\fd20-8b1e-b255-832e—61.ipv6-literal.net\C\restore`

    Falls bereits Dateien mit demselben Namen existieren, können Sie diese überschreiben oder überspringen.
14. Wählen Sie **Wiederherstellen**.

    Den Fortschritt der Wiederherstellung können Sie auf der Seite „Auftragsüberwachung“ einsehen.

Fehlerbehebung bei der Wiederherstellung von Gastdateien

Beim Versuch, eine Gastdatei wiederherzustellen, können die folgenden Szenarien auftreten.

Die Gastdateiwiederherstellungssitzung ist leer

Dieses Problem tritt auf, wenn Sie eine Gastdatei-Wiederherstellungssitzung erstellen und das Gastbetriebssystem während der Sitzung neu startet. VMDKs im Gastbetriebssystem könnten offline bleiben, sodass die Liste der Wiederherstellungssitzungen für Gastdateien leer ist.

Um das Problem zu beheben, schalten Sie die VMDKs im Gastbetriebssystem manuell wieder online. Wenn die VMDKs online sind, zeigt die Dateiwiederherstellungssitzung des Gastes den richtigen Inhalt an.

Der Vorgang zum Anhängen der Festplatte beim Wiederherstellen der Gastdatei schlägt fehl

Dieses Problem tritt auf, wenn Sie einen Gastdateiwiederherstellungsvorgang starten, der Vorgang zum Anschließen der Festplatte jedoch fehlschlägt, obwohl VMware Tools ausgeführt wird und die Anmeldeinformationen des Gastbetriebssystems korrekt sind. In diesem Fall wird der folgende Fehler zurückgegeben:

```
Error while validating guest credentials, failed to access guest system using specified credentials: Verify VMWare tools is running properly on system and account used is Administrator account, Error is SystemError vix error codes = (3016, 0).
```

Um das Problem zu beheben, starten Sie den VMware Tools-Windows-Dienst auf dem Gastbetriebssystem neu und versuchen Sie dann erneut, die Gastdatei wiederherzustellen.

Sicherungen werden nicht getrennt, nachdem die Gastdateiwiederherstellungssitzung abgebrochen wurde

Dieses Problem tritt auf, wenn Sie einen Gastdateiwiederherstellungsvorgang aus einer VM-konsistenten Sicherung durchführen. Während die Gastdateiwiederherstellungssitzung aktiv ist, wird eine weitere VM-konsistente Sicherung für dieselbe VM durchgeführt. Wenn die Gastdateiwiederherstellungssitzung entweder manuell oder automatisch nach 24 Stunden getrennt wird, werden die Sicherungen für die Sitzung nicht getrennt.

Um das Problem zu beheben, trennen Sie die VMDKs, die an die aktive Gastdateiwiederherstellungssitzung angehängt waren, manuell.

KVM-Workloads schützen (Vorschau)

Übersicht über den Schutz von KVM-Workloads

Schützen Sie Ihre verwalteten KVM-VMs und Speicherpools mit NetApp Backup and Recovery. NetApp Backup and Recovery bietet schnelle, speichereffiziente, absturzsichere und VM-konsistente Backup- und Wiederherstellungsvorgänge. Bevor Sie Ihre KVM-Hosts und VMs mithilfe von Backup und Recovery schützen können, müssen diese über eine Managementplattform wie Apache CloudStack verwaltet werden.

Sie können KVM-Workloads auf Amazon Web Services S3, Azure NetApp Files oder StorageGRID sichern und KVM-Workloads auf einem lokalen KVM-Host wiederherstellen.

Verwenden Sie NetApp Backup and Recovery , um eine 3-2-1-Schutzstrategie zu implementieren, bei der Sie 3 Kopien Ihrer Quelldaten auf 2 verschiedenen Speichersystemen sowie 1 Kopie in der Cloud haben. Zu den Vorteilen des 3-2-1-Ansatzes gehören:

- Mehrere Datenkopien schützen vor internen und externen Cybersicherheitsbedrohungen.
- Die Verwendung unterschiedlicher Medientypen erleichtert Ihnen die Wiederherstellung, wenn ein Typ ausfällt.
- Sie können die Wiederherstellung schnell von der Vor-Ort-Kopie durchführen und die Offsite-Kopien verwenden, wenn die Vor-Ort-Kopie kompromittiert ist.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -UI-Versionen finden Sie unter"Wechseln Sie zur vorherigen NetApp Backup and Recovery -Benutzeroberfläche" .

Mit NetApp Backup and Recovery können Sie die folgenden Aufgaben im Zusammenhang mit KVM-Workloads ausführen:

- "Entdecken Sie KVM-Workloads"
- "Erstellen und Verwalten von Schutzgruppen für KVM-Workloads"
- "KVM-Workloads sichern"
- "KVM-Workloads wiederherstellen"

Entdecken Sie KVM-Workloads in NetApp Backup and Recovery

NetApp Backup and Recovery muss KVM-Hosts und virtuelle Maschinen erkennen, bevor diese geschützt werden können. Bevor Sie Ihre KVM-Hosts und VMs zu Backup und Recovery hinzufügen können, müssen diese über eine Managementplattform wie Apache CloudStack verwaltet werden.

Erforderliche Konsolenrolle 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" .

Fügen Sie eine Managementplattform und einen KVM-Host hinzu und ermitteln Sie die Ressourcen.

Fügen Sie Informationen zur Managementplattform und zum KVM-Host hinzu, damit NetApp Backup and Recovery die Workloads automatisch erkennt.

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie unter **Workloads** die Kachel **KVM** aus.

   Wenn Sie sich zum ersten Mal bei Backup and Recovery anmelden und zwar ein System in der Konsole haben, aber keine Ressourcen erkannt wurden, wird die Seite *Willkommen bei der neuen NetApp Backup and Recovery* mit einer Option zum **Erkennen von Ressourcen** angezeigt.

3. Wählen Sie **Ressourcen entdecken**.
4. Geben Sie die folgenden Informationen ein:
   a. **Workload-Typ**: Wählen Sie **KVM**.
   b. Falls Sie Ihre Managementplattform noch nicht in Backup and Recovery integriert haben, wählen Sie **Managementplattform hinzufügen**.
      i. Geben Sie die folgenden Informationen ein:
         - **IP-Adresse oder FQDN der Managementplattform**: Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen der Managementplattform ein.
         - **API-Schlüssel**: Geben Sie den API-Schlüssel ein, der zur Authentifizierung von API-Anfragen verwendet werden soll.
         - **Geheimer Schlüssel**: Geben Sie den geheimen Schlüssel ein, der zur Authentifizierung von API-Anfragen verwendet werden soll.

- **Port**: Geben Sie den Port ein, der für die Kommunikation zwischen Backup und Recovery und der Managementplattform verwendet werden soll.
- **Agenten**: Wählen Sie einen Konsolenagenten aus, der die Kommunikation zwischen Backup und Recovery und der Managementplattform erleichtern soll.

ii. Wenn Sie fertig sind, wählen Sie **Hinzufügen**.

c. **KVM-Einstellungen**: Fügen Sie einen neuen KVM-Host hinzu, indem Sie die folgenden Informationen eingeben:

- **KVM FQDN oder IP-Adresse**: Geben Sie den FQDN oder die IP-Adresse des Hosts ein.
- **Anmeldedaten**: Geben Sie den Benutzernamen und das Passwort für den KVM-Host ein.
- **Konsolenagent**: Wählen Sie den Konsolenagenten aus, der für die Kommunikation zwischen Backup und Recovery und dem KVM-Host verwendet werden soll.
- **Portnummer**: Geben Sie den Port ein, der für die Kommunikation zwischen Backup und Recovery und dem KVM-Host verwendet werden soll.
- **Verwaltungsplattform**: Wenn der KVM-Host verwaltet wird und Sie die Verwaltungsplattform zu Backup und Wiederherstellung hinzugefügt haben, wählen Sie die Verwaltungsplattform aus der Liste aus.

5. Wählen Sie **Entdecken**.

Dieser Vorgang kann einige Minuten dauern.

Ergebnis

Die KVM-Arbeitslast wird in der Liste der Arbeitslasten auf der Inventarseite angezeigt.

Weiter zum NetApp Backup and Recovery Dashboard

Schritte

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.

Erstellen und verwalten Sie Schutzgruppen für KVM-Workloads mit NetApp Backup and Recovery

Erstellen Sie Schutzgruppen, um die Sicherungsvorgänge für eine Reihe von KVM-Ressourcen zu verwalten. Eine Schutzgruppe ist eine logische Gruppierung von Ressourcen wie VMs und Speicherpools, die Sie gemeinsam schützen möchten. Sie müssen eine Schutzgruppe erstellen, um virtuelle KVM-Maschinen oder Speicherpools zu sichern.

Sie können die folgenden Aufgaben im Zusammenhang mit Schutzgruppen ausführen:

- Erstellen Sie eine Schutzgruppe.
- Schutzdetails anzeigen.

- Sichern Sie jetzt eine Schutzgruppe. Sehen"Sichern Sie jetzt KVM-Workloads" .
- Löschen Sie eine Schutzgruppe.

Erstellen einer Schutzgruppe

Gruppieren Sie VMs und Speicherpools, die Sie gemeinsam schützen möchten, in einer Schutzgruppe.

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

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.
5. Wählen Sie **Schutzgruppe erstellen**.
6. Geben Sie einen Namen für die Schutzgruppe ein.
7. Wählen Sie die VMs oder Speicherpools aus, die Sie in die Schutzgruppe aufnehmen möchten.
8. Wählen Sie **Weiter**.
9. Wählen Sie die **Sicherungsrichtlinie** aus, die Sie auf die Schutzgruppe anwenden möchten.

   Weitere Informationen zum Erstellen einer Sicherungsrichtlinie finden Sie unter"Erstellen und Verwalten von Richtlinien" .
10. Wählen Sie **Weiter**.
11. Überprüfen Sie die Konfiguration.
12. Wählen Sie **Erstellen** aus, um die Schutzgruppe zu erstellen.

Löschen einer Schutzgruppe

Durch das Löschen einer Schutzgruppe werden diese und alle zugehörigen Sicherungszeitpläne entfernt. Möglicherweise möchten Sie eine Schutzgruppe löschen, wenn sie nicht mehr benötigt wird.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.
5. Wählen Sie die Schutzgruppe aus, die Sie löschen möchten.
6. Wählen Sie das Symbol Aktionen ••• > **Löschen**.
7. Überprüfen Sie die Bestätigungsmeldung zum Löschen der zugehörigen Sicherungen und bestätigen Sie den Löschvorgang.

Sichern Sie KVM-Workloads mit NetApp Backup and Recovery

Sichern Sie KVM-Schutzgruppen von lokalen ONTAP -Systemen auf Amazon Web Services, Azure NetApp Files oder StorageGRID , um sicherzustellen, dass Ihre Daten geschützt sind. Wenn Sie eine Schutzgruppe sichern, sichert die NetApp Console die in der Schutzgruppe enthaltenen VMs und Speicherpools. Backups werden automatisch erstellt und in einem Objektspeicher in Ihrem öffentlichen oder privaten Cloud-Konto gespeichert.

Um Schutzgruppen nach einem Zeitplan zu sichern, erstellen Sie Richtlinien, die die Sicherungs- und Wiederherstellungsvorgänge steuern. Sehen"Erstellen von Richtlinien" Anweisungen hierzu finden Sie unter.

- Erstellen Sie Schutzgruppen, um die Sicherungs- und Wiederherstellungsvorgänge für eine Reihe von Ressourcen zu verwalten. Sehen"Erstellen und verwalten Sie Schutzgruppen für KVM-Workloads mit NetApp Backup and Recovery" für weitere Informationen.

Sichern Sie Schutzgruppen jetzt mit einem On-Demand-Backup

Sie können sofort eine On-Demand-Sicherung ausführen. Dies ist hilfreich, wenn Sie Änderungen an Ihrem System vornehmen und sicherstellen möchten, dass Sie vor dem Start über eine Sicherungskopie verfügen.

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

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie in der KVM-Kachel **Erkennen und verwalten** aus.
3. Wählen Sie **Inventar**.
4. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
5. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
6. Wählen Sie die Registerkarte **Schutzgruppen**, **Datenspeicher** oder **Virtuelle Maschinen**.
7. Wählen Sie die Schutzgruppe aus, die Sie sichern möchten.
8. Wählen Sie das Symbol Aktionen ••• > **Jetzt sichern**.

   Die auf die Sicherung angewendete Richtlinie ist dieselbe Richtlinie, die der Schutzgruppe zugewiesen ist.

9. Wählen Sie die Zeitplanstufe aus.
10. Wählen Sie **Sichern**.

Wiederherstellen virtueller KVM-Maschinen mit NetApp Backup and Recovery

Stellen Sie virtuelle KVM-Maschinen aus Snapshots, aus einer auf einen Sekundärspeicher replizierten Schutzgruppensicherung oder aus in Objektspeichern gespeicherten Sicherungen mithilfe von NetApp Backup and Recovery wieder her.

Von diesen Speicherorten wiederherstellen

Sie können virtuelle Maschinen von verschiedenen Startorten aus wiederherstellen:

- Wiederherstellung von einem primären Standort (lokaler Snapshot)
- Wiederherstellen von einer replizierten Ressource auf einem sekundären Speicher
- Wiederherstellung aus einer Objektspeichersicherung

Stellen Sie diese Punkte wieder her

Sie können Daten bis zu diesen Punkten wiederherstellen:

- Am ursprünglichen Speicherort wiederherstellen

Überlegungen zur Wiederherstellung aus dem Objektspeicher

Wenn Sie eine Sicherungsdatei im Objektspeicher auswählen und für diese Sicherung der Ransomware-Schutz aktiv ist (wenn Sie DataLock und Ransomware Resilience in der Sicherungsrichtlinie aktiviert haben), werden Sie aufgefordert, vor der Wiederherstellung der Daten eine zusätzliche Integritätsprüfung der Sicherungsdatei durchzuführen. Wir empfehlen Ihnen, den Scan durchzuführen.

Für den Zugriff auf den Inhalt der Sicherungsdatei fallen bei Ihrem Cloud-Anbieter zusätzliche Kosten für den Datenverkehr an.

So funktioniert die Wiederherstellung virtueller Maschinen

Wenn Sie virtuelle Maschinen wiederherstellen, geschieht Folgendes:

- Wenn Sie eine Workload aus einer lokalen Sicherungsdatei wiederherstellen, erstellt NetApp Backup and Recovery mithilfe der Daten aus der Sicherung eine *neue* Ressource.
- Wenn Sie eine Wiederherstellung von einer replizierten VM durchführen, können Sie diese auf dem Originalsystem oder auf einem lokalen ONTAP -System wiederherstellen.
- Wenn Sie eine Sicherung aus dem Objektspeicher wiederherstellen, können Sie die Daten auf dem ursprünglichen System oder auf einem lokalen ONTAP -System wiederherstellen.

Auf der Seite „Wiederherstellen“ (auch als „Suchen und Wiederherstellen“ bezeichnet) können Sie eine VM wiederherstellen, auch wenn Sie sich nicht an den genauen Namen, den Speicherort oder das Datum erinnern, an dem sie zuletzt in gutem Zustand war. Sie können mithilfe von Filtern nach dem Schnappschuss suchen.

Stellen Sie VMs über die Wiederherstellungsoption wieder her (Suchen und Wiederherstellen).

Stellen Sie virtuelle KVM-Maschinen mithilfe der Option „Wiederherstellen“ wieder her. Sie können nach dem Snapshot anhand seines Namens oder mithilfe von Filtern suchen.

Erforderliche Konsolenrolle Superadministrator für Backup und Wiederherstellung oder Administratorrolle für Backup und Wiederherstellung zur Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie im NetApp Backup and Recovery -Menü **Wiederherstellen** aus.
3. Wählen Sie aus der Dropdown-Liste rechts neben dem Namenssuchfeld **KVM** aus.
4. Geben Sie den Namen der VM ein, die Sie wiederherstellen möchten, oder filtern Sie nach dem VM-Host

oder Speicherpool, in dem sich die wiederherzustellende Ressource befindet.

Es wird eine Liste mit Snapshots angezeigt, die Ihren Suchkriterien entsprechen.

5. Wählen Sie die Schaltfläche **Wiederherstellen** für den Snapshot, den Sie wiederherstellen möchten.

   Es wird eine Liste möglicher Wiederherstellungspunkte angezeigt.

6. Wählen Sie den Wiederherstellungspunkt aus, den Sie verwenden möchten.
7. Wählen Sie einen Quellspeicherort für den Snapshot aus.
8. Wählen Sie **Weiter**, um fortzufahren.
9. Wählen Sie das Wiederherstellungsziel und die Einstellungen aus:

Zielauswahl

Am ursprünglichen Speicherort wiederherstellen

1. **Schnelle Wiederherstellung aktivieren**: Wählen Sie diese Option, um eine schnelle Wiederherstellung durchzuführen. Wiederhergestellte Volumes und Daten stehen sofort zur Verfügung. Verwenden Sie dies nicht auf Volumes, die eine hohe Leistung erfordern, da der Zugriff auf die Daten während des schnellen Wiederherstellungsprozesses langsamer als gewöhnlich sein kann.
2. **Optionen vor der Wiederherstellung**: Geben Sie den vollständigen Pfad für ein Skript ein, das vor dem Wiederherstellungsvorgang ausgeführt werden soll, sowie alle Argumente, die das Skript verwendet.
3. **Optionen nach der Wiederherstellung**:
   - **VM neu starten**: Wählen Sie diese Option aus, um die VM nach Abschluss des Wiederherstellungsvorgangs und nach Anwendung des Post-Restore-Skripts neu zu starten.
   - **Postscript**: Geben Sie den vollständigen Pfad für ein Skript ein, das nach dem Wiederherstellungsvorgang ausgeführt werden soll, sowie alle Argumente, die das Skript verwendet.
4. Abschnitt **Benachrichtigung**:
   - **E-Mail-Benachrichtigungen aktivieren**: Wählen Sie diese Option aus, um E-Mail-Benachrichtigungen über den Wiederherstellungsvorgang zu erhalten, und geben Sie an, welche Art von Benachrichtigungen Sie erhalten möchten.
5. Wählen Sie **Wiederherstellen**.

An einem anderen Speicherort wiederherstellen

Nicht verfügbar für die KVM-Workload-Vorschau.

Schützen Sie Hyper-V-Workloads

Übersicht zum Schützen von Hyper-V-Workloads

Schützen Sie Ihre Hyper-V-VMs mit NetApp Backup and Recovery. NetApp Backup and Recovery bietet schnelle, speichereffiziente, absturzsichere und VM-konsistente Backup- und Wiederherstellungsvorgänge sowohl für eigenständige Instanzen als auch für FCI-

Cluster-Instanzen. Sie können auch Hyper-V-VMs schützen, die mit System Center Virtual Machine Manager (SCVMM) bereitgestellt und auf einer CIFS-Freigabe gehostet werden.

Sie können Hyper-V-Workloads auf Amazon Web Services S3 oder StorageGRID sichern und Hyper-V-Workloads auf einem lokalen Hyper-V-Host wiederherstellen.

Verwenden Sie NetApp Backup and Recovery , um eine 3-2-1-Schutzstrategie zu implementieren, bei der Sie 3 Kopien Ihrer Quelldaten auf 2 verschiedenen Speichersystemen sowie 1 Kopie in der Cloud haben. Zu den Vorteilen des 3-2-1-Ansatzes gehören:

- Mehrere Datenkopien schützen vor internen und externen Cybersicherheitsbedrohungen.
- Mehrere Medientypen gewährleisten die Failover-Funktionalität im Falle eines physischen oder logischen Ausfalls eines Medientyps.
- Mithilfe der Vor-Ort-Kopie können Sie Daten schnell wiederherstellen und Sie können die Offsite-Kopien verwenden, wenn die Vor-Ort-Kopie kompromittiert ist.

Wenn Sie Hyper-V-Hosts hinzufügen und Ressourcen ermitteln, installiert NetApp Backup and Recovery das NetApp Hyper-V-Plug-in und das NetApp SnapCenter Windows FileSystem-Plug-in auf dem Hyper-V-Host, um die Verwaltung und den Schutz virtueller Maschinen zu unterstützen.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -UI-Versionen finden Sie unter"Wechseln Sie zur vorherigen NetApp Backup and Recovery -Benutzeroberfläche" .

Mit NetApp Backup and Recovery können Sie die folgenden Aufgaben im Zusammenhang mit Hyper-V-Workloads ausführen:

- "Entdecken Sie Hyper-V-Workloads"
- "Erstellen und Verwalten von Schutzgruppen für Hyper-V-Workloads"
- "Sichern Sie Hyper-V-Workloads"
- "Wiederherstellen von Hyper-V-Workloads"

Entdecken Sie Hyper-V-Workloads in NetApp Backup and Recovery

NetApp Backup and Recovery muss virtuelle Hyper-V-Maschinen erkennen, bevor Sie sie schützen können.

Erforderliche Konsolenrolle 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" .

Hinzufügen eines Hyper-V-Hosts und Ermitteln von Ressourcen

Fügen Sie Hyper-V-Hostinformationen hinzu und lassen Sie NetApp Backup and Recovery virtuelle Maschinen erkennen. Wählen Sie in jedem Konsolenagenten die Systeme aus, auf denen Sie die Ressourcen ermitteln möchten.

Wenn Sie Hyper-V-Hosts hinzufügen und Ressourcen ermitteln, installiert NetApp Backup and Recovery das NetApp Hyper-V-Plug-in und das NetApp SnapCenter Windows FileSystem-Plug-in auf dem Hyper-V-Host, um die Verwaltung und den Schutz virtueller Maschinen zu unterstützen.

Schritte

1. Wählen Sie im NetApp Console **Schutz** > **Sicherung und Wiederherstellung**.

   Wenn Sie sich zum ersten Mal bei NetApp Backup and Recovery anmelden und bereits ein System in der Konsole haben, aber noch keine Ressourcen entdeckt haben, wird die Zielseite „Willkommen beim neuen NetApp Backup and Recovery“ angezeigt und bietet die Option „Ressourcen entdecken“.

2. Wählen Sie **Ressourcen entdecken**.
3. Geben Sie die folgenden Informationen ein:
   a. **Workload-Typ**: Wählen Sie **Hyper-V**.
   b. Wenn Sie für diesen Hyper-V-Host noch keine Anmeldeinformationen gespeichert haben, wählen Sie **Anmeldeinformationen hinzufügen**.
      i. Wählen Sie den Konsolenagenten aus, der mit diesem Host verwendet werden soll.
      ii. Geben Sie einen Namen für diese Anmeldeinformationen ein.
      iii. Geben Sie den Benutzernamen und das Kennwort für das Konto ein.
      iv. Wählen Sie **Fertig**.
   c. **Hostregistrierung**: Fügen Sie einen neuen Hyper-V-Host hinzu, indem Sie den FQDN oder die IP-Adresse des Hosts, die Anmeldeinformationen, den Konsolenagenten und die Portnummer eingeben. Falls der FQDN vom Konsolenagenten nicht aufgelöst werden kann, verwenden Sie stattdessen die IP-Adresse. Geben Sie für FCI-Cluster die Management-IP-Adresse des FCI-Clusters ein.
4. Wählen Sie **Entdecken**.

   Dieser Vorgang kann einige Minuten dauern.

Ergebnis

Nachdem NetApp Backup and Recovery Ressourcen erkannt hat, wird auf der Seite „Inventar“ die Hyper-V-Arbeitslast in der Liste der Arbeitslasten angezeigt.

Weiter zum NetApp Backup and Recovery Dashboard

Schritte

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.

Erstellen und verwalten Sie Schutzgruppen für Hyper-V-Workloads mit NetApp Backup and Recovery

Erstellen Sie Schutzgruppen, um die Sicherungsvorgänge für eine Reihe virtueller

Maschinen zu verwalten. Eine Schutzgruppe ist eine logische Gruppierung von Ressourcen wie VMs, die Sie gemeinsam schützen möchten.

Sie können die folgenden Aufgaben im Zusammenhang mit Schutzgruppen ausführen:

- Erstellen Sie eine Schutzgruppe.
- Schutzdetails anzeigen.
- Sichern Sie jetzt eine Schutzgruppe. Sehen"Sichern Sie jetzt Hyper-V-Workloads" .
- Löschen Sie eine Schutzgruppe.

Erstellen einer Schutzgruppe

Gruppieren Sie Workloads, die Sie gemeinsam schützen möchten, in einer Schutzgruppe. Erstellen Sie eine Schutzgruppe, um Workloads gemeinsam zu sichern und wiederherzustellen.

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

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie das Menü **Schutzgruppen**.
5. Wählen Sie **Schutzgruppe erstellen**.
6. Geben Sie einen Namen für die Schutzgruppe ein.
7. Wählen Sie die VMs aus, die Sie in die Schutzgruppe aufnehmen möchten.
8. Wählen Sie **Weiter**.
9. Wählen Sie die **Sicherungsrichtlinie** aus, die Sie auf die Schutzgruppe anwenden möchten.
10. Wählen Sie **Weiter**.
11. Überprüfen Sie die Konfiguration.
12. Wählen Sie **Erstellen** aus, um die Schutzgruppe zu erstellen.

Bearbeiten Sie eine Schutzgruppe

Bearbeiten Sie eine Schutzgruppe, um deren Namen oder Einstellungen zu ändern. Möglicherweise möchten Sie eine Schutzgruppe bearbeiten, wenn sich die Ressourcen in der Gruppe geändert haben.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.
5. Wählen Sie die Schutzgruppe aus, die Sie bearbeiten möchten.
6. Wählen Sie das Symbol „Aktionen“ aus. ••• > **Bearbeiten**.

7. Ändern Sie beliebige Einstellungen für die Schutzgruppe, wie z. B. den Namen oder die in der Gruppe enthaltenen virtuellen Maschinen.
8. Wählen Sie **Weiter**.
9. Ändern Sie die Schutzrichtlinie gegebenenfalls. Wenn Sie fertig sind, wählen Sie **Weiter**.
10. Überprüfen Sie die Konfiguration und wählen Sie **Absenden**.

Löschen einer Schutzgruppe

Durch das Löschen einer Schutzgruppe werden diese und alle zugehörigen Sicherungszeitpläne entfernt. Möglicherweise möchten Sie eine Schutzgruppe löschen, wenn sie nicht mehr benötigt wird.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.
5. Wählen Sie die Schutzgruppe aus, die Sie löschen möchten.
6. Wählen Sie das Symbol Aktionen ••• > **Löschen**.
7. Überprüfen Sie die Bestätigungsmeldung zum Löschen der zugehörigen Sicherungen und bestätigen Sie den Löschvorgang.

Sichern Sie Hyper-V-Workloads mit NetApp Backup and Recovery

Sichern Sie Hyper-V-VMs von lokalen ONTAP Systemen auf Amazon Web Services, Azure NetApp Files oder StorageGRID, um sicherzustellen, dass Ihre Daten geschützt sind. Backups werden automatisch erstellt und in einem Objektspeicher in Ihrem öffentlichen oder privaten Cloud-Konto gespeichert.

- Um Workloads nach einem Zeitplan zu sichern, erstellen Sie Richtlinien, die die Sicherungs- und Wiederherstellungsvorgänge steuern. Sehen"Erstellen von Richtlinien" Anweisungen hierzu finden Sie unter.
- Erstellen Sie Schutzgruppen, um die Sicherungs- und Wiederherstellungsvorgänge für eine Reihe von Ressourcen zu verwalten. Sehen"Erstellen und verwalten Sie Schutzgruppen für Hyper-V-Workloads mit NetApp Backup and Recovery" für weitere Informationen.
- Sichern Sie jetzt Workloads (erstellen Sie jetzt ein On-Demand-Backup).

Sichern Sie Workloads jetzt mit einem On-Demand-Backup

Verwenden Sie On-Demand-Backups, damit Ihre Daten geschützt sind, bevor Sie Systemänderungen vornehmen.

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

Schritte

1. Wählen Sie im Menü **Inventar** aus.

2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**, **Datenspeicher** oder **Virtuelle Maschinen**.
5. Wählen Sie die Schutzgruppe oder virtuellen Maschinen aus, die Sie sichern möchten.
6. Wählen Sie das Symbol Aktionen ••• > **Jetzt sichern**.

> Für die Sicherung wird dieselbe Richtlinie verwendet, die Sie der Schutzgruppe oder virtuellen Maschine zugewiesen haben.

7. Wählen Sie die Zeitplanstufe aus.
8. Wählen Sie **Sichern**.

Wiederherstellen von Hyper-V-Workloads mit NetApp Backup and Recovery

Stellen Sie Hyper-V-Workloads aus Snapshots, aus einer auf Sekundärspeicher replizierten Workload-Sicherung oder aus in Objektspeichern gespeicherten Sicherungen mithilfe von NetApp Backup and Recovery wieder her.

Von diesen Speicherorten wiederherstellen

Sie können Workloads von verschiedenen Startorten wiederherstellen:

- Wiederherstellung von einem primären Standort (lokaler Snapshot)
- Wiederherstellen von einer replizierten Ressource auf einem sekundären Speicher
- Wiederherstellung aus einer Objektspeichersicherung

Stellen Sie diese Punkte wieder her

Sie können Daten bis zu diesen Punkten wiederherstellen:

- Am ursprünglichen Speicherort wiederherstellen
- An einem alternativen Speicherort wiederherstellen

Überlegungen zur Wiederherstellung aus dem Objektspeicher

Wenn Sie eine Sicherungsdatei im Objektspeicher auswählen und für diese Sicherung der Ransomware-Schutz aktiv ist (wenn Sie DataLock und Ransomware Resilience in der Sicherungsrichtlinie aktiviert haben), werden Sie aufgefordert, vor der Wiederherstellung der Daten eine zusätzliche Integritätsprüfung der Sicherungsdatei durchzuführen. Wir empfehlen Ihnen, den Scan durchzuführen.

> Für den Zugriff auf den Inhalt der Sicherungsdatei fallen bei Ihrem Cloud-Anbieter zusätzliche Kosten für den Datenverkehr an.

So funktioniert die Wiederherstellung von Workloads

Beim Wiederherstellen von Workloads geschieht Folgendes:

- Wenn Sie eine Workload aus einer lokalen Sicherungsdatei wiederherstellen, erstellt NetApp Backup and Recovery mithilfe der Daten aus der Sicherung eine *neue* Ressource.
- Wenn Sie eine Wiederherstellung aus einem replizierten Workload durchführen, können Sie den Workload auf dem ursprünglichen System oder auf einem lokalen ONTAP System wiederherstellen.

Auf der Seite „Wiederherstellen“ (auch als „Suchen und Wiederherstellen“ bezeichnet) können Sie eine Ressource wiederherstellen, auch wenn Sie sich nicht an den genauen Namen, den Speicherort oder das Datum erinnern, an dem sie zuletzt in gutem Zustand war. Sie können mithilfe von Filtern nach dem Schnappschuss suchen.

Wiederherstellen von Workload-Daten über die Option „Wiederherstellen“ (Suchen und Wiederherstellen)

Stellen Sie Hyper-V-Workloads mit der Option „Wiederherstellen“ wieder her. Sie können nach dem Snapshot anhand seines Namens oder mithilfe von Filtern suchen.

Erforderliche Konsolenrolle Superadministrator für Backup und Wiederherstellung oder Administratorrolle für Backup und Wiederherstellung zur Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Wiederherstellen** aus.
2. Wählen Sie aus der Dropdown-Liste rechts neben dem Namenssuchfeld **Hyper-V** aus.
3. Geben Sie den Namen der Ressource ein, die Sie wiederherstellen möchten, oder filtern Sie nach dem VM-Namen, VM-Host oder Speicherpool, in dem sich die wiederherzustellende Ressource befindet.

   Es wird eine Liste mit Snapshots angezeigt, die Ihren Suchkriterien entsprechen.

4. Wählen Sie die Schaltfläche **Wiederherstellen** für den Snapshot, den Sie wiederherstellen möchten.

   Es wird eine Liste möglicher Wiederherstellungspunkte angezeigt.

5. Wählen Sie den Wiederherstellungspunkt aus, den Sie verwenden möchten.
6. Wählen Sie einen Quellspeicherort für den Snapshot aus.
7. Wählen Sie **Weiter**, um fortzufahren.
8. Wählen Sie das Wiederherstellungsziel und die Einstellungen aus:

Zielauswahl

Am ursprünglichen Speicherort wiederherstellen

Wenn Sie zum ursprünglichen Speicherort zurückkehren, können Sie die Zieleinstellungen einsehen, indem Sie den Abschnitt **Zieleinstellungen** erweitern. Sie können diese jedoch nicht ändern.

1. Im Abschnitt **Optionen nach der Wiederherstellung** sollten Sie folgende Option in Betracht ziehen:
   - **Starten der virtuellen Maschine**: Aktivieren Sie diese Option, um die neue virtuelle Maschine nach der Wiederherstellung zu starten.
2. Wählen Sie **Wiederherstellen**.

An einem anderen Speicherort wiederherstellen

1. Geben Sie im Abschnitt **Zieleinstellungen** die folgenden Informationen ein:
   - **Hyper-V FQDN oder IP-Adresse**: Geben Sie den vollqualifizierten Domänennamen oder die IP-Adresse des Ziel-Hyper-V-Hosts ein.
   - **Netzwerk**: Wählen Sie das Zielnetzwerk aus, in dem Sie den Snapshot wiederherstellen möchten.
   - **Name der virtuellen Maschine**: Geben Sie den Namen der VM ein, die Sie wiederherstellen möchten.
   - **Zielort**: Geben Sie den Zielordner oder die CIFS-Freigabe ein, die die wiederhergestellten Daten enthalten soll.
2. Im Abschnitt **Vorbereitende Wiederherstellungsoptionen** sollten Sie folgende Optionen in Betracht ziehen:
   - **Schnellwiederherstellung**: Aktivieren Sie diese Option, um die wiederhergestellte VM sofort verfügbar zu machen. Aus dem Objektspeicher werden nur die zum Ausführen der VM benötigten Dateien wiederhergestellt, nicht das gesamte Volume.
3. Im Abschnitt **Optionen nach der Wiederherstellung** sollten Sie folgende Optionen in Betracht ziehen:
   - **Starten der virtuellen Maschine**: Aktivieren Sie diese Option, um die neue virtuelle Maschine nach der Wiederherstellung zu starten.
4. Wählen Sie **Wiederherstellen**.

Oracle Database-Workloads schützen (Preview)

Übersicht über den Schutz von Oracle Database-Workloads

Schützen Sie Oracle-Datenbanken und -Protokolle mit NetApp Backup und Recovery. Erhalten Sie schnelle, platzsparende, absturzkonsistente und datenbankkonsistente Backups und Wiederherstellungen. Sichern Sie Oracle Database-Workloads in AWS S3, NetApp StorageGRID, Azure Blob Storage oder ONTAP S3. Stellen Sie Backups auf einem lokalen Oracle-Host wieder her.

Verwenden Sie NetApp Backup and Recovery , um eine 3-2-1-Schutzstrategie zu implementieren, bei der Sie 3 Kopien Ihrer Quelldaten auf 2 verschiedenen Speichersystemen sowie 1 Kopie in der Cloud haben. Zu den Vorteilen des 3-2-1-Ansatzes gehören:

- Mehrere Datenkopien schützen vor internen und externen Cybersicherheitsbedrohungen.

- Die Verwendung unterschiedlicher Medientypen erleichtert Ihnen die Wiederherstellung, wenn ein Typ ausfällt.
- Sie können die Wiederherstellung schnell von der Vor-Ort-Kopie durchführen und die Offsite-Kopien verwenden, wenn die Vor-Ort-Kopie kompromittiert ist.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -UI-Versionen finden Sie unter"Wechseln Sie zur vorherigen NetApp Backup and Recovery -Benutzeroberfläche" .

Sie können NetApp Backup und Recovery verwenden, um die folgenden Aufgaben im Zusammenhang mit Oracle Database-Workloads durchzuführen:

- "Oracle Database-Workloads entdecken"
- "Erstellen und Verwalten von Schutzgruppen für Oracle Database-Workloads"
- "Oracle-Datenbank-Workloads sichern"
- "Oracle-Datenbank-Workloads wiederherstellen"

Entdecken Sie Oracle-Datenbank-Workloads in NetApp Backup and Recovery

NetApp Backup and Recovery muss zuerst Ihre Oracle-Datenbanken erkennen, damit Sie sie schützen können.

Erforderliche Konsolenrolle 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" .

Hinzufügen eines Oracle-Hosts und Ermitteln von Ressourcen

Fügen Sie Oracle-Hostinformationen hinzu und lassen Sie NetApp Backup and Recovery die Workloads erkennen. Wählen Sie in jedem Konsolenagenten die Systeme aus, auf denen Sie Workloads ermitteln möchten.

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie unter **Workloads** die Kachel **Oracle** aus.

   Wenn Sie sich zum ersten Mal bei Backup and Recovery anmelden und zwar ein System in der Konsole haben, aber keine Ressourcen erkannt wurden, wird die Seite *Willkommen bei der neuen NetApp Backup and Recovery* mit einer Option zum **Erkennen von Ressourcen** angezeigt.

3. Wählen Sie **Ressourcen entdecken**.
4. Geben Sie die folgenden Informationen ein:
   a. **Workload-Typ**: Wählen Sie **Oracle**.
   b. Wenn Sie für diesen Oracle-Host noch keine Anmeldeinformationen gespeichert haben, wählen Sie **Anmeldeinformationen hinzufügen**.
      i. Wählen Sie den Konsolenagenten aus, der mit diesem Host verwendet werden soll.
      ii. Geben Sie einen Namen für diese Anmeldeinformationen ein.
      iii. Geben Sie den Benutzernamen und das Kennwort für das Konto ein.

iv. Wählen Sie **Fertig**.

c. **Host-Registrierung**: Fügen Sie einen neuen Oracle-Host hinzu. Geben Sie den FQDN oder die IP-Adresse, die Anmeldeinformationen, den Konsolenagenten und die Portnummer des Hosts ein.

5. Wählen Sie **Entdecken**.

Dieser Vorgang kann einige Minuten dauern.

Ergebnis

Die Oracle-Workload wird in der Workload-Liste auf der Inventarseite angezeigt.

Weiter zum NetApp Backup and Recovery Dashboard

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.

Erstellen und Verwalten von Schutzgruppen für Oracle-Datenbank-Workloads mit NetApp Backup und Recovery

Erstellen Sie Schutzgruppen, um die Sicherungsvorgänge für eine Reihe von Oracle Database-Ressourcen zu verwalten. Eine Schutzgruppe ist eine logische Gruppierung von Ressourcen wie Datenbanken, die Sie gemeinsam schützen möchten. Sie müssen eine Schutzgruppe erstellen, um Oracle-Datenbanken zu sichern.

Sie können die folgenden Aufgaben im Zusammenhang mit Schutzgruppen ausführen:

- Erstellen Sie eine Schutzgruppe.
- Schutzdetails anzeigen.
- Sichern Sie jetzt eine Schutzgruppe. Siehe "Sichern Sie jetzt Oracle Database Workloads".
- Löschen Sie eine Schutzgruppe.

Erstellen einer Schutzgruppe

Gruppieren Sie VMs und Speicherpools, die Sie gemeinsam schützen möchten, in einer Schutzgruppe.

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

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.

5. Wählen Sie **Schutzgruppe erstellen**.
6. Geben Sie einen Namen für die Schutzgruppe ein.
7. Wählen Sie die VMs oder Speicherpools aus, die Sie in die Schutzgruppe aufnehmen möchten.
8. Wählen Sie **Weiter**.
9. Wählen Sie die **Sicherungsrichtlinie** aus, die Sie auf die Schutzgruppe anwenden möchten.

   Wenn Sie eine Richtlinie erstellen möchten, wählen Sie **Neue Richtlinie erstellen** und folgen Sie den Anweisungen zum Erstellen einer Richtlinie. Sehen"Erstellen von Richtlinien" für weitere Informationen.

10. Wählen Sie **Weiter**.
11. Überprüfen Sie die Konfiguration.
12. Wählen Sie **Erstellen** aus, um die Schutzgruppe zu erstellen.

Löschen einer Schutzgruppe

Durch das Löschen einer Schutzgruppe werden diese und alle zugehörigen Sicherungszeitpläne entfernt. Möglicherweise möchten Sie eine Schutzgruppe löschen, wenn sie nicht mehr benötigt wird.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.
5. Wählen Sie die Schutzgruppe aus, die Sie löschen möchten.
6. Wählen Sie das Symbol Aktionen ••• > **Schutz entfernen**.
7. Überprüfen Sie die Bestätigungsmeldung zum Löschen der zugehörigen Sicherungen und bestätigen Sie den Löschvorgang.

Sichern Sie Oracle-Datenbank-Workloads mit NetApp Backup und Recovery

Verwenden Sie NetApp Backup and Recovery , um Oracle Database-Schutzgruppen oder Datenbanken von lokalen ONTAP -Systemen in Cloud-Speicher zu sichern, einschließlich Amazon S3, NetApp StorageGRID, Microsoft Azure Blob Storage oder ONTAP S3. NetApp Backup and Recovery sichert Datenbanken und Protokolldaten in jeder Schutzgruppe.

Um Schutzgruppen oder einzelne Datenbanken nach einem Zeitplan zu sichern, erstellen Sie Richtlinien, die Sicherungs- und Wiederherstellungsvorgänge verwalten. Sehen"Erstellen von Richtlinien" Anweisungen hierzu finden Sie unter.

- Erstellen Sie Schutzgruppen, um die Backup- und Recovery-Vorgänge für eine Gruppe von Ressourcen zu verwalten. Siehe "Erstellen und Verwalten von Schutzgruppen für Oracle-Datenbank-Workloads mit NetApp Backup und Recovery" für weitere Informationen.
- Sichern Sie jetzt eine Schutzgruppe (erstellen Sie jetzt ein On-Demand-Backup).
- Sichern Sie jetzt eine Datenbank.

Sichern Sie Schutzgruppen jetzt mit einem On-Demand-Backup

Führen Sie vor Systemänderungen eine On-Demand-Sicherung durch, um sicherzustellen, dass Ihre Daten geschützt sind.

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

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie unter **Workloads** die Kachel **Oracle** aus.
3. Wählen Sie **Inventar**.
4. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
5. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
6. Wählen Sie die Registerkarte **Schutzgruppen**, **Datenspeicher** oder **Virtuelle Maschinen**.
7. Wählen Sie die Schutzgruppe aus, die Sie sichern möchten.
8. Wählen Sie das Symbol Aktionen ••• > **Jetzt sichern**.

   NetApp Backup and Recovery verwendet für die Sicherungs- und die Schutzgruppe dieselbe Richtlinie.

9. Wählen Sie die Zeitplanstufe aus.
10. Wählen Sie **Sichern**.

Sichern Sie jetzt eine Datenbank mit einem On-Demand-Backup

Sie können bei Bedarf eine Sicherung einer einzelnen Datenbank ausführen.

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

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie unter **Workloads** die Kachel **Oracle** aus.
3. Wählen Sie **Inventar**.
4. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
5. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
6. Wählen Sie die Registerkarte **Datenbanken**.
7. Wählen Sie die Datenbank aus, die Sie sichern möchten.
8. Wählen Sie das Symbol Aktionen ••• > **Jetzt sichern**.
9. Wählen Sie die Zeitplanstufe aus.
10. Wählen Sie **Sichern**.

Stellen Sie Oracle-Datenbanken mit NetApp Backup and Recovery wieder her

Stellen Sie Oracle-Datenbanken aus Snapshots, aus einem auf Sekundärspeicher replizierten Backup oder aus in Objektspeichern gespeicherten Backups mithilfe von NetApp Backup and Recovery wieder her.

Von diesen Speicherorten wiederherstellen

Sie können Datenbanken von verschiedenen Startorten wiederherstellen:

- Wiederherstellung von einem primären Standort (lokaler Snapshot)
- Wiederherstellen von einer replizierten Ressource auf einem sekundären Speicher
- Wiederherstellung aus einer Objektspeichersicherung

Stellen Sie diese Punkte wieder her

Sie können Daten am ursprünglichen Speicherort wiederherstellen. Die Wiederherstellung an einem anderen Speicherort ist in dieser privaten Vorschauversion nicht verfügbar.

- Am ursprünglichen Speicherort wiederherstellen

So funktioniert die Wiederherstellung von Oracle-Datenbanken

Wenn Sie Oracle-Datenbanken wiederherstellen, geschieht Folgendes:

- Wenn Sie eine Datenbank aus einem lokalen Snapshot wiederherstellen, erstellt NetApp Backup and Recovery eine *neue* Ressource mithilfe der Daten aus dem Backup.
- Wenn Sie aus einem replizierten Speicher wiederherstellen, können Sie es am ursprünglichen Speicherort wiederherstellen.
- Wenn Sie ein Backup aus dem Objektspeicher wiederherstellen, können Sie die Daten im Quellspeicher oder auf einem lokalen ONTAP -System wiederherstellen und die Datenbank von dort wiederherstellen.

Auf der Seite „Wiederherstellen“ (auch als „Suchen und Wiederherstellen“ bezeichnet) können Sie eine Datenbank wiederherstellen, auch wenn Sie sich nicht an den genauen Namen, den Speicherort oder das Datum erinnern, an dem sie zuletzt in gutem Zustand war. Sie können mithilfe von Filtern nach der Datenbank suchen.

Wiederherstellen einer Oracle-Datenbank

Stellen Sie je nach Bedarf eine Oracle-Datenbank zu einem bestimmten Zeitpunkt, zu einer bestimmten Systemänderungsnummer (SCN) oder zum letzten fehlerfreien Zustand wieder her. Sie können die Datenbank auch einfach aus Snapshots wiederherstellen und den automatisierten Wiederherstellungsprozess überspringen. Wenn Sie die Wiederherstellung manuell durchführen möchten, können Sie den automatisierten Wiederherstellungsprozess überspringen. Sie können die Datenbank anhand ihres Namens oder mit bestimmten Filtern suchen.

Erforderliche Konsolenrolle Superadministrator für Backup und Wiederherstellung oder Administratorrolle für Backup und Wiederherstellung zur Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie im NetApp Backup and Recovery -Menü **Wiederherstellen** aus.

3. Wählen Sie aus der Dropdown-Liste rechts neben dem Namenssuchfeld **Oracle** aus.
4. Geben Sie den Namen der Datenbank ein, die Sie wiederherstellen möchten, oder filtern Sie nach dem Datenbankhost, auf dem sich die wiederherzustellende Datenbank befindet.

   Es wird eine Liste mit Snapshots angezeigt, die Ihren Suchkriterien entsprechen.
5. Wählen Sie die Schaltfläche **Wiederherstellen** für die Datenbank, die Sie wiederherstellen möchten.
6. Wählen Sie eine Wiederherstellungsoption:

   Wiederherstellung zu einem bestimmten Zeitpunkt

   a. Wählen Sie **Zu einem bestimmten Zeitpunkt wiederherstellen**.
   b. Wählen Sie **Weiter**.
   c. Wählen Sie ein Datum aus der Dropdown-Liste und wählen Sie **Suchen**.

      Es wird eine Liste mit passenden Schnappschüssen zum angegebenen Datum angezeigt.

   Wiederherstellen auf eine bestimmte Systemänderungsnummer (SCN)

   a. Wählen Sie **Auf eine bestimmte Systemänderungsnummer (SCN) wiederherstellen**.
   b. Wählen Sie **Weiter**.
   c. Geben Sie die SCN ein, die als Wiederherstellungspunkt verwendet werden soll, und wählen Sie **Suchen**.

      Es wird eine Liste mit passenden Snapshots für die angegebene SCN angezeigt.

   Wiederherstellen auf die letzte Sicherung (letzter guter Zustand)

   a. Wählen Sie **Auf die neueste Sicherung wiederherstellen**.
   b. Wählen Sie **Weiter**.

      Es werden die neuesten Voll- und Protokollsicherungen angezeigt.

   Wiederherstellen aus Snapshots ohne Wiederherstellung

   a. Wählen Sie **Aus Snapshots ohne Wiederherstellung wiederherstellen**.
   b. Wählen Sie **Weiter**.

      Die passenden Schnappschüsse werden angezeigt.
7. Wählen Sie einen Quellspeicherort für den Snapshot aus.
8. Wählen Sie **Weiter**, um fortzufahren.
9. Wählen Sie das Wiederherstellungsziel und die Einstellungen aus:

Zielauswahl

Am ursprünglichen Speicherort wiederherstellen

1. **Zieleinstellungen**:
   - Wählen Sie, ob die gesamte Datenbank oder nur die Tablespaces für die Datenbank wiederhergestellt werden sollen.
   - **Steuerdateien**: Aktivieren Sie diese Option optional, um auch die Datenbank-Steuerdateien wiederherzustellen.
2. **Optionen vor der Wiederherstellung**:
   - Aktivieren Sie diese Option optional und geben Sie den vollständigen Pfad für ein Skript ein, das vor dem Wiederherstellungsvorgang ausgeführt werden soll, sowie alle Argumente, die das Skript verwendet.
   - Wählen Sie einen Timeout-Wert für das Skript. Wenn die Ausführung des Skripts innerhalb dieses Zeitraums fehlschlägt, wird die Wiederherstellung trotzdem fortgesetzt.
3. **Optionen nach der Wiederherstellung**:
   - **Postscript**: Aktivieren Sie diese Option optional und geben Sie den vollständigen Pfad für ein Skript ein, das nach dem Wiederherstellungsvorgang ausgeführt werden soll, sowie alle Argumente, die das Skript verwendet.
   - **Öffnen Sie die Datenbank oder Containerdatenbank nach der Wiederherstellung im LESE-/SCHREIB-Modus**: Nachdem der Wiederherstellungsvorgang abgeschlossen ist, aktiviert Backup and Recovery den LESE-/SCHREIB-Modus für die Datenbank.
4. Abschnitt **Benachrichtigung**:
   - **E-Mail-Benachrichtigungen aktivieren**: Wählen Sie diese Option aus, um E-Mail-Benachrichtigungen über den Wiederherstellungsvorgang zu erhalten, und geben Sie an, welche Art von Benachrichtigungen Sie erhalten möchten.
5. Wählen Sie **Wiederherstellen**.

An einem anderen Speicherort wiederherstellen

Nicht verfügbar für Oracle Database-Workloads Preview.

Mounten und Unmounten von Oracle-Datenbankwiederherstellungspunkten mit NetApp Backup and Recovery

Möglicherweise möchten Sie einen Wiederherstellungspunkt für die Oracle-Datenbank bereitstellen, wenn Sie zum Durchführen von Wiederherstellungsvorgängen in einem kontrollierten Zustand auf die Datenbank zugreifen müssen.

Mounten eines Oracle-Datenbank-Wiederherstellungspunkts

Wenn Sie die Schutzrichtlinie für eine Datenbank so konfigurieren, dass Archivprotokolle aufbewahrt werden, können Sie Wiederherstellungspunkte bereitstellen, um den Änderungsverlauf der Datenbank anzuzeigen.

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie die Oracle-Kachel aus.
3. Wählen Sie im Menü „Sichern und Wiederherstellen“ die Option „Inventar“ aus.

4. Wählen Sie für die Oracle-Datenbank-Workload in der Liste **Anzeigen** aus.
5. Wählen Sie das Menü **Datenbanken**.
6. Wählen Sie eine Datenbank aus der Liste und wählen Sie das Symbol Aktionen ••• > **Schutzdetails anzeigen**.

   Es wird eine Liste mit Wiederherstellungspunkten für diese Datenbank angezeigt.
7. Wählen Sie einen Wiederherstellungspunkt aus der Liste und wählen Sie das Symbol Aktionen ••• > **Mount**.
8. Führen Sie im angezeigten Dialogfeld die folgenden Schritte aus:
   a. Wählen Sie aus der Liste den Host aus, der den Wiederherstellungspunkt mounten soll.
   b. Wählen Sie den Speicherort aus, den Backup and Recovery zum Bereitstellen des Wiederherstellungspunkts verwenden soll. Für die Vorabversion wird das Mounten aus dem Objektspeicher nicht unterstützt.

      Der Mount-Pfad, den Backup und Recovery verwenden soll, wird angezeigt.
9. Wählen Sie **Mount**.

   Der Wiederherstellungspunkt wird auf dem Oracle-Host bereitgestellt.

Unmounten eines Oracle-Datenbank-Wiederherstellungspunkts

Heben Sie die Bereitstellung des Wiederherstellungspunkts auf, wenn Sie die an dieser Datenbank vorgenommenen Änderungen nicht mehr anzeigen müssen.

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie die Oracle-Kachel aus.
3. Wählen Sie im Menü „Sichern und Wiederherstellen“ die Option „Inventar“ aus.
4. Wählen Sie für die Oracle-Workload in der Liste **Anzeigen** aus.
5. Wählen Sie das Menü **Datenbanken**.
6. Wählen Sie eine Datenbank aus der Liste und wählen Sie das Symbol Aktionen ••• > **Schutzdetails anzeigen**.

   Es wird eine Liste mit Wiederherstellungspunkten für diese Datenbank angezeigt.
7. Wählen Sie einen Wiederherstellungspunkt aus der Liste und wählen Sie das Symbol Aktionen ••• > **Aushängen**.
8. Bestätigen Sie die Aktion, indem Sie **Unmount** auswählen.

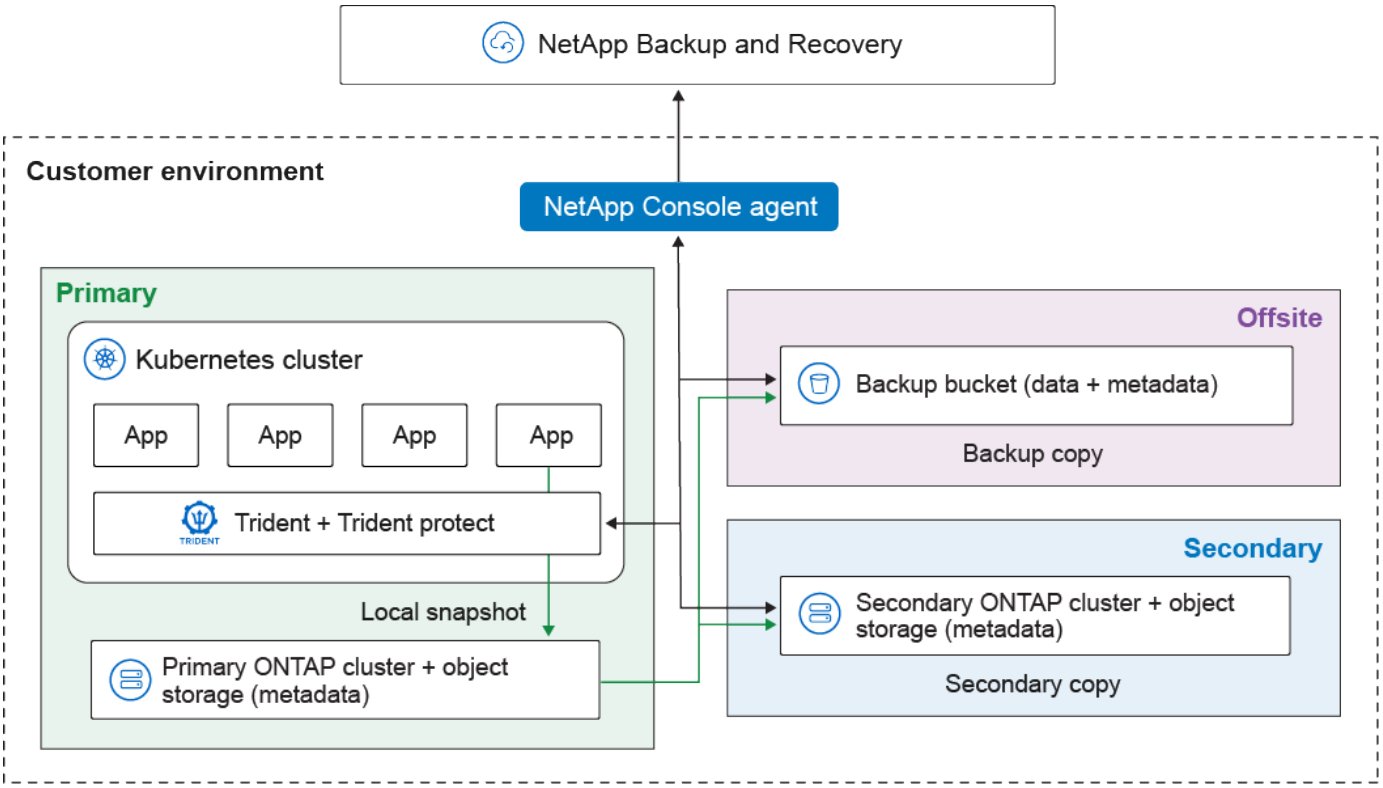
Schützen Sie Kubernetes-Workloads (Vorschau)

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-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*) 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:

```yaml
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"

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 `Bound` Phase erreichen, bevor die Operation fehlschlägt.	"1200" (20 Minuten)

Wiederherstellen von Kubernetes-Anwendungen

Kubernetes-Anwendungen mithilfe der Web-Benutzeroberfläche wiederherstellen

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

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

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

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

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

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

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

Ressource, die gefiltert werden soll.

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

  Beispiel:

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

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

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

Einen Snapshot im ursprünglichen Namensraum wiederherstellen

Sie können einen Snapshot jederzeit im ursprünglichen Namensraum wiederherstellen.

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_k
ey_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-Namespaces, 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-Namespaces vor der Wiederherstellungs- oder Failover-Operation:

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

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 Bestätigungsdialogfeld 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.

Überwachen von Jobs in NetApp Backup and Recovery

Überwachen Sie mit NetApp Backup and Recovery lokale Snapshots, Replikationen und Sicherungsjobs, die Sie starten. Verfolgen Sie von Ihnen initiierte Wiederherstellungsaufträge. Zeigen Sie abgeschlossene, laufende oder fehlgeschlagene Jobs an, um die Diagnose von Problemen zu erleichtern. Aktivieren Sie E-Mail-Benachrichtigungen im Benachrichtigungscenter der NetApp Console, um auch dann über die Systemaktivität informiert zu bleiben, wenn Sie nicht angemeldet sind. Verwenden Sie die Konsolenzeitleiste, um Details zu allen Aktionen anzuzeigen, die über die Benutzeroberfläche oder API gestartet wurden.

NetApp Backup and Recovery speichert Jobinformationen 15 Tage lang, löscht sie dann und entfernt sie aus dem Job Monitor.

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

Anzeigen des Auftragsstatus im Auftragsmonitor

Sie können eine Liste aller Snapshot-, Replikations-, Backup-to-Object-Storage- und Wiederherstellungsvorgänge sowie deren aktuellen Status auf der Registerkarte **Jobüberwachung** anzeigen. Dies umfasst Vorgänge von Ihrem Cloud Volumes ONTAP, Ihrem lokalen ONTAP, Ihren Anwendungen und virtuellen Maschinen. Jeder Vorgang oder Auftrag hat eine eindeutige ID und einen Status.

Der Status kann sein:

- Erfolg
- Im Gange
- In der Warteschlange
- Warnung
- Fehlgeschlagen

Snapshots, Replikationen, Backups auf Objektspeicher und Wiederherstellungsvorgänge, die Sie über die NetApp Backup and Recovery -Benutzeroberfläche und -API initiiert haben, sind auf der Registerkarte „Jobüberwachung“ verfügbar.

Wenn Sie Ihre ONTAP -Systeme auf 9.13.x aktualisiert haben und im Job Monitor keine laufenden geplanten Sicherungsvorgänge sehen, starten Sie NetApp Backup and Recovery neu. "Erfahren Sie, wie Sie NetApp Backup and Recovery neu starten".

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Überwachung** aus.
2. Um zusätzliche Spalten (System, SVM, Benutzername, Workload, Richtlinienname, Snapshot-Bezeichnung) anzuzeigen, wählen Sie das Pluszeichen aus.

Suchen und filtern Sie die Liste der Jobs

Sie können die Vorgänge auf der Seite „Auftragsüberwachung“ mithilfe verschiedener Filter filtern, z. B. nach Richtlinie, Snapshot-Bezeichnung, Art des Vorgangs (Schutz, Wiederherstellung, Aufbewahrung oder Sonstiges) und Schutztyp (lokaler Snapshot, Replikation oder Sicherung in die Cloud).

Standardmäßig werden auf der Seite „Jobüberwachung“ Schutz- und Wiederherstellungsjobs der letzten 24 Stunden angezeigt. Sie können den Zeitrahmen mithilfe des Zeitrahmenfilters ändern.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Überwachung** aus.
2. Um die Ergebnisse anders zu sortieren, wählen Sie jede Spaltenüberschrift aus, um sie nach Status, Startzeit, Ressourcenname usw. zu sortieren.
3. Wenn Sie nach bestimmten Jobs suchen, wählen Sie den Bereich **Erweiterte Suche und Filterung** aus, um das Suchfeld zu öffnen.

   Verwenden Sie dieses Feld, um eine Freitextsuche nach einer beliebigen Ressource einzugeben, beispielsweise „Band 1“ oder „Anwendung 3“. Sie können die Jobliste auch nach den Elementen in den Dropdown-Menüs filtern.

   Die meisten Filter sind selbsterklärend. Mit dem Filter „Arbeitsbelastung“ können Sie sich Jobs in folgenden Kategorien anzeigen lassen:

- ONTAP -Volumes (Cloud Volumes ONTAP und lokale ONTAP -Volumes)
- Microsoft SQL Server
- Virtuelle Maschinen
- Kubernetes

- Sie können nur dann innerhalb einer bestimmten „SVM“ nach Daten suchen, wenn Sie zuerst ein System ausgewählt haben.
- Sie können mit dem Filter „Schutzart“ nur suchen, wenn Sie die „Art“ von „Schutz“ ausgewählt haben.

4. Um die Seite sofort zu aktualisieren, wählen Sie das  Taste. Andernfalls wird diese Seite alle 15 Minuten aktualisiert, sodass Sie immer die aktuellsten Jobstatusergebnisse sehen.

Jobdetails anzeigen

Sie können Details zu einem bestimmten abgeschlossenen Auftrag anzeigen. Sie können Details für einen bestimmten Job in einem JSON-Format exportieren.

Sie können Details wie Auftragstyp (geplant oder auf Abruf), SnapMirror -Sicherungstyp (anfänglich oder regelmäßig), Start- und Endzeiten, Dauer, Menge der vom System zum Objektspeicher übertragenen Daten, durchschnittliche Übertragungsrate, Richtlinienname, aktivierte Aufbewahrungssperre, durchgeführter Ransomware-Scan, Details zur Schutzquelle und Details zum Schutzziel anzeigen.

Wiederherstellungsaufträge zeigen Details wie den Sicherungszielanbieter (Amazon Web Services, Microsoft Azure, Google Cloud, vor Ort), den S3-Bucket-Namen, den SVM-Namen, den Quellvolume-Namen, das Zielvolume, die Snapshot-Bezeichnung, die Anzahl der wiederhergestellten Objekte, Dateinamen, Dateigrößen, das Datum der letzten Änderung und den vollständigen Dateipfad an.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Überwachung** aus.
2. Wählen Sie den Namen des Jobs aus.
3. Wählen Sie das Menü Aktionen ••• und wählen Sie **Details anzeigen**.
4. Erweitern Sie jeden Abschnitt, um Details anzuzeigen.

Ergebnisse der Jobüberwachung als Bericht herunterladen

Sie können den Inhalt der Hauptseite zur Jobüberwachung als Bericht herunterladen, nachdem Sie die Ergebnisse gefiltert oder sortiert haben. NetApp Backup and Recovery generiert und lädt eine CSV-Datei herunter, die Sie überprüfen und bei Bedarf an andere Gruppen senden können. Die CSV-Datei enthält bis zu 10.000 Datenzeilen.

Aus den Informationen zu den Jobüberwachungsdetails können Sie eine JSON-Datei mit Details zu einem einzelnen Job herunterladen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Überwachung** aus.
2. Um eine CSV-Datei für alle Jobs herunterzuladen, wählen Sie die Schaltfläche „Herunterladen“ und suchen Sie die Datei in Ihrem Download-Verzeichnis.
3. Um eine JSON-Datei für einen einzelnen Job herunterzuladen, wählen Sie das Menü Aktionen ••• Wählen

Sie für den Job **JSON-Datei herunterladen** und suchen Sie die Datei in Ihrem Download-Verzeichnis.

Aufbewahrungsaufträge (Sicherungslebenszyklus) überprüfen

Überwachen Sie Aufbewahrungsflüsse (*Backup-Lebenszyklus*), um Backups zu überprüfen, sie zu schützen und Audits zu unterstützen. Ermitteln Sie, wann Sicherungskopien ablaufen, um den Lebenszyklus zu verfolgen.

Ein Backup-Lebenszyklus-Job verfolgt alle Snapshots, die gelöscht wurden oder sich in der Löschwarteschlange befinden. Ab ONTAP 9.13 können Sie alle Jobtypen mit der Bezeichnung „Retention“ auf der Seite „Job Monitoring“ anzeigen.

Der Auftragstyp „Aufbewahrung“ erfasst alle Snapshot-Löschaufträge, die auf einem Volume initiiert wurden, das durch NetApp Backup and Recovery geschützt ist.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Überwachung** aus.
2. Wählen Sie den Bereich **Erweiterte Suche und Filterung** aus, um das Suchfeld zu öffnen.
3. Wählen Sie als Auftragstyp „Aufbewahrung“ aus.

Überprüfen Sie Sicherungs- und Wiederherstellungswarnungen im Benachrichtigungscenter der NetApp Console

Das Benachrichtigungscenter der NetApp Console verfolgt den Fortschritt der von Ihnen initiierten Sicherungs- und Wiederherstellungsaufträge, sodass Sie überprüfen können, ob der Vorgang erfolgreich war oder nicht.

Sie können Warnungen im Benachrichtigungscenter anzeigen und die Konsole so konfigurieren, dass bei wichtigen Systemaktivitäten E-Mail-Warnungen gesendet werden, auch wenn Sie nicht angemeldet sind. "Erfahren Sie mehr über das Benachrichtigungscenter und wie Sie Warn-E-Mails für Sicherungs- und Wiederherstellungsaufträge senden" .

Das Benachrichtigungscenter zeigt zahlreiche Ereignisse im Zusammenhang mit Snapshots, Replikation, Cloud-Backups und Wiederherstellungen an, aber nur bestimmte Ereignisse lösen E-Mail-Benachrichtigungen aus:

Vorgangstyp	Ereignis	Alarm ausgelöst	E-Mail gesendet
Aktivierung	Die Aktivierung von Backup und Recovery für das System ist fehlgeschlagen	Ja	Ja
Aktivierung	Bearbeitung von Sicherung und Wiederherstellung für System fehlgeschlagen	Ja	Ja
Aktivierung	Volume ist jetzt der Snapshot-Richtlinie zugeordnet	Ja	Ja
Aktivierung	Datensicherung oder Statusänderung	Ja	Ja
Aktivierung	Sicherung und Wiederherstellung wurden für das System erfolgreich aktiviert.	Ja	Ja
Aktivierung	Ad-hoc-Volume-Backup fehlgeschlagen	Ja	Ja
Aktivierung	Ad-hoc-Volume-Backup erfolgreich	Ja	Nein

Vorgangstyp	Ereignis	Alarm ausgelöst	E-Mail gesendet
Aktivierung	Datensicherung über mehrere Volumes fehlgeschlagen	Ja	Ja
Cron-Operationen	Überprüfung auf fehlende Snapshot-Labels	Ja	Ja
Cron-Operationen	Das Senden des Sicherheitstokens an ONTAP für dieses System ist fehlgeschlagen.	Ja	Ja
Pub/Sub-Veranstaltungen	Verbindungsfehler	Ja	Nein
Pub/Sub-Veranstaltungen	Das Löschen eines geplanten Snapshots ist fehlgeschlagen.	Ja	Nein
Pub/Sub-Veranstaltungen	Geplante Datensicherung fehlgeschlagen	Ja	Nein
Pub/Sub-Veranstaltungen	Die Wiederherstellung des Volumes war erfolgreich.	Ja	Nein
Pub/Sub-Veranstaltungen	Wiederherstellung des Volumes fehlgeschlagen	Ja	Nein
Ransomware	Potenzieller Ransomware-Angriff auf Sicherungskopie identifiziert	Ja	Ja
Ransomware	Potenzieller Ransomware-Angriff auf der Sicherungskopie dieses Systems festgestellt	Ja	Ja
Lokaler Schnappschuss	Fehler beim Erstellen eines Ad-hoc-Snapshots bei NetApp Backup and Recovery	Ja	Ja
Replikation	Modifikation der Replikationsbeziehung des Volumenausfalls	Ja	Ja
Replikation	Fehler beim Ad-hoc-Replikationsjob von NetApp Backup and Recovery	Ja	Ja
Replikation	Fehler beim Anhalten des Replikationsjobs bei NetApp Backup and Recovery	Ja	Nein
Replikation	Fehler beim Abbrechen des Replikationsjobs bei NetApp Backup and Recovery	Ja	Nein
Replikation	Fehler beim Resynchronisierungsjob für NetApp Backup and Recovery -Replikation	Ja	Nein
Replikation	Fehler beim Stoppen des Replikationsjobs bei NetApp Backup and Recovery	Ja	Nein
Replikation	Fehler beim Reverse-Resync-Job für die Replikation von NetApp Backup and Recovery	Ja	Ja
Replikation	Fehler beim Löschen des Replikationsjobs bei NetApp Backup and Recovery	Ja	Ja

Vorgangstyp	Ereignis	Alarm ausgelöst	E-Mail gesendet
Zieloperationen	Wiederherstellung am lokalen oder Cloud-Ziel fehlgeschlagen	Ja	Ja
Zieloperationen	Fehler bei der Wiederherstellung auf Abruf	Ja	Ja
Systembetrieb	Fehler bei der Erstellung eines Ad-hoc-Volume-Snapshots	Ja	Ja

Ab ONTAP 9.13.0 werden alle Warnungen für Cloud Volumes ONTAP und lokale ONTAP -Systeme angezeigt. Bei Systemen mit Cloud Volumes ONTAP 9.13.0 und lokalem ONTAP wird nur die Warnmeldung „Wiederherstellungsauftrag abgeschlossen, aber mit Warnungen“ angezeigt.

Standardmäßig erhalten die Organisations- und Kontoadministratoren der NetApp Console E-Mails für alle Warnmeldungen vom Typ „Kritisch“ und „Empfehlung“. Standardmäßig richtet das System keine anderen Benutzer und Empfänger für den Empfang von Benachrichtigungs-E-Mails ein. Konfigurieren Sie E-Mail-Benachrichtigungen für alle Konsolenbenutzer in Ihrem NetApp Cloud-Konto oder für andere Empfänger, die über Sicherungs- und Wiederherstellungsaktivitäten informiert werden müssen.

Um E-Mail-Benachrichtigungen zu NetApp Backup and Recovery zu erhalten, müssen Sie auf der Einstellungsseite für Benachrichtigungen die Schweregrade „Kritisch“, „Warnung“ und „Fehler“ auswählen.

"Erfahren Sie, wie Sie Warn-E-Mails für Sicherungs- und Wiederherstellungsaufträge senden".

Schritte

1. Wählen Sie im Konsolenmenü die Option ( ).
2. Überprüfen Sie die Benachrichtigungen.

Überprüfen der Vorgangsaktivität in der Konsolenzeitleiste

Sie können Details zu Sicherungs- und Wiederherstellungsvorgängen zur weiteren Untersuchung in der Konsolenzeitleiste anzeigen. Die Konsolenzeitleiste bietet Details zu jedem Ereignis, unabhängig davon, ob es vom Benutzer oder vom System initiiert wurde, und zeigt Aktionen an, die in der Benutzeroberfläche oder über die API initiiert wurden.

"Erfahren Sie mehr über die Unterschiede zwischen der Timeline und dem Benachrichtigungscenter".

Starten Sie NetApp Backup and Recovery neu

Es kann Situationen geben, in denen Sie NetApp Backup and Recovery neu starten müssen.

Der Konsolenagent umfasst die NetApp Backup and Recovery .

Schritte

1. Stellen Sie eine Verbindung zum Linux-System her, auf dem der Konsolenagent ausgeführt wird.

Standort des Konsolenagenten	Verfahren
Cloud-Bereitstellung	Befolgen Sie die Anweisungen für "Herstellen einer Verbindung mit der virtuellen Linux-Maschine des Konsolenagenten" abhängig vom verwendeten Cloud-Anbieter.
Manuelle Installation	Melden Sie sich beim Linux-System an.

2. Geben Sie den Befehl zum Neustart des Dienstes ein.

Standort des Konsolenagenten	Docker-Befehl	Podman-Befehl
Cloud-Bereitstellung	`docker restart cloudmanager_cbs`	`podman restart cloudmanager_cbs`
Manuelle Installation mit Internetzugang	`docker restart cloudmanager_cbs`	`podman restart cloudmanager_cbs`
Manuelle Installation ohne Internetzugang	`docker restart ds_cloudmanager_cbs_1`	`podman restart ds_cloudmanager_cbs_1`

Automatisieren Sie mit NetApp Backup and Recovery REST APIs

Die über die Web-Benutzeroberfläche verfügbaren NetApp Backup and Recovery -Funktionen sind auch über die Backup- und Recovery-REST-API verfügbar.

In NetApp Backup and Recovery sind zehn Endpunktkategorien definiert:

- `backup`- verwaltet Sicherungsvorgänge von Cloud- und lokalen Ressourcen und ruft Details der Sicherungsdaten ab
- `catalog`- verwaltet die indizierte Katalogsuche nach Dateien basierend auf einer Abfrage (Suchen und Wiederherstellen)
- `cloud`- ruft Informationen zu verschiedenen Cloud-Anbieter-Ressourcen von der NetApp Console ab
- `job`- verwaltet Jobdetaileinträge in der NetApp Console Datenbank
- `license`- ruft die Lizenzgültigkeit der Systeme von der NetApp Console ab
- `ransomware scan`- initiiert einen Ransomware-Scan für eine bestimmte Sicherungsdatei
- `restore`- ermöglicht Ihnen die Durchführung von Wiederherstellungsvorgängen auf Volume-, Datei- und Ordnerebene
- `sfr`- Ruft Dateien aus einer Sicherungsdatei für Wiederherstellungsvorgänge auf einzelner Dateiebene ab (Durchsuchen und Wiederherstellen)
- `storagegrid`- ruft Details zu einem StorageGRID -Server ab und ermöglicht Ihnen, einen StorageGRID -Server zu erkennen
- `system`- verwaltet die Sicherungsrichtlinien und konfiguriert den Zielobjektspeicher, der einem System zugeordnet ist

API-Referenz

Dokumentation für jede NetApp Backup and Recovery -API ist verfügbar unter "NetApp Console Automatisierung für NetApp Backup and Recovery" .

Erste Schritte

Um mit den NetApp Backup and Recovery -APIs zu beginnen, benötigen Sie ein Benutzertoken, Ihre NetApp Console -ID und die Konsolenagent-ID.

Wenn Sie API-Aufrufe tätigen, fügen Sie das Benutzertoken im Autorisierungsheader und die Konsolenagent-ID im x-agent-id-Header hinzu. Sie sollten die NetApp Console -ID in den APIs verwenden.

> Wenn Sie ein Dienstkonto verwenden, sollten Sie anstelle eines Benutzertokens das Dienstzugriffstoken verwenden. Der Wert für „client_id“ („Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC“) ist ein fester Wert und kann nicht geändert werden. Befolgen Sie in diesem Fall die Anweisungen hier: "Erstellen eines Dienstzugriffstokens" .

Schritte

1. Besorgen Sie sich ein Benutzertoken von der NetApp NetApp Console -Website.

   Stellen Sie sicher, dass Sie das Aktualisierungstoken über den folgenden Link generieren: https://services.cloud.netapp.com/refresh-token/. Das Aktualisierungstoken ist eine alphanumerische Zeichenfolge, die Sie zum Generieren eines Benutzertokens verwenden.

```
curl --location --request POST 'https://netapp-cloud-
account.auth0.com/oauth/token?=' \
--header 'Content-Type: application/json' \
-d '{
    "grant_type": "refresh_token",
    "refresh_token": "JxaVHn9cGkX92aPVCkhat3zxxxxxwsC9qMl_pLHkZtsVA",
    "client_id": "Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC"
}'
```

   Das Benutzertoken von der NetApp Console hat ein Ablaufdatum. Die API-Antwort enthält ein Feld „expires_in“, das angibt, wann das Token abläuft. Um das Token zu aktualisieren, müssen Sie diese API erneut aufrufen.

2. Besorgen Sie sich Ihre NetApp Console Konto-ID.

```
GET 'https://api.bluexp.netapp.com/tenancy/account' -H 'authority:
api.bluexp.netapp.com'
Header:
-H 'accept: application/json'
-H 'accept-language: en-GB,en;q=0.9'
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR
```

   Diese API gibt eine Antwort wie die folgende zurück. Sie können die Konto-ID abrufen, indem Sie die Ausgabe von **[0].[accountPublicId]** analysieren.

```
{
  "accountPublicId": "account-i6vJXvZW",
  "accountName": "rashidn",
  "isSaas": true,
  "isGov": false,
  "isPrivatePreviewEnabled": false,
  "is3rdPartyServicesEnabled": false,
  "accountSerial": "96064469711530003565",
  "userRole": "Role-1"
}
```

3. Rufen Sie die X-Agent-ID ab, die die Konsolen-Agent-ID enthält.

```
GET 'https://api.services.cloud.netapp.com/occm/list-occms/account-
OOnAR4ZS?excludeStandalone=true&source=saas' \
Header:
  -H 'authority: api.services.cloud.netapp.com' \
  -H 'accept: application/json' \
  -H 'accept-language: en-GB,en;q=0.9' \
  -H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5……
```

Sie können die Agenten-ID aus der Antwort abrufen, indem Sie die Ausgabe von **occm.[0].[agent].[agentId]** analysieren.

Beispiel für die Verwendung der APIs

Das folgende Beispiel zeigt einen API-Aufruf zum Aktivieren von NetApp Backup and Recovery auf einem System mit einer neuen Richtlinie, in der tägliche, stündliche und wöchentliche Beschriftungen festgelegt sind und die Archivierung nach 180 Tagen in der Region „East-US-2“ in der Azure-Cloud erfolgt. Beachten Sie, dass hierdurch nur die Sicherung auf dem System aktiviert wird, jedoch keine Volumes gesichert werden.

API-Anforderung

Sie werden sehen, dass wir die NetApp Console Konto-ID verwenden `account-DpTFcxN3` , Konsolenagent-ID `iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients` und Benutzertoken `Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwkeMwHc4V alobjUmju2x0xUH48g` in diesem Befehl.

```
curl --location --request POST
'https://api.bluexp.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v3/backup/working-
environment/VsaWorkingEnvironment-99hPYEgk' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwk
eMwHc4ValobjUmju2x0xUH48g' \
--data-raw '{
    "provider":"AZURE",
    "backup-policy": {
      "archive-after-days": 180,
      "rule": [
        {
          "label": "hourly",
          "retention": "2"
        },
        {
          "label": "daily",
          "retention": "30"
        },
        {
          "label": "weekly",
          "retention": "52"
        }
      ]
    },
    "ip-space": "Default",
    "region": "eastus2",
    "azure": {
      "resource-group": "rn-test-backup-rg",
      "subscription": "3beb4dd0-25d4-464f-9bb0-303d7cf5c0c2"
    }
  }
```

Die Antwort ist eine Job-ID, die Sie dann überwachen können:

```
{
 "job-id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a"
}
```

Überwachen Sie die Antwort:

```
curl --location --request GET
'https://api.bluexp.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v1/job/1b34b6f6-8f43-40fb-9a52-
485b0dfe893a' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…hE9ss2Nub
K6wZRHUdSaORI7JvcOorUhJ8srqdiUiW6MvuGIFAQIh668of2M3dLbhVDBe8BBMtsa939UGnJx
7Qz6Eg'
```

Antwort:

```
{
  "job": [
    {
      "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
      "type": "backup-working-environment",
      "status": "PENDING",
      "error": "",
      "time": 1651852160000
    }
  ]
}
```

Überwachen, bis der „Status“ „ABGESCHLOSSEN“ ist:

```
{
  "job": [
    {
      "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
      "type": "backup-working-environment",
      "status": "COMPLETED",
      "error": "",
      "time": 1651852160000
    }
  ]
}
```

Referenz

Richtlinien in SnapCenter im Vergleich zu denen in NetApp Backup and Recovery

Es gibt einige Unterschiede zwischen den in SnapCenter und den in NetApp Backup and Recovery verwendeten Richtlinien, die sich auf die Anzeige nach dem Importieren von Ressourcen und Richtlinien aus SnapCenter auswirken können.

Zeitplanstufen

SnapCenter verwendet die folgenden Zeitplanebenen:

- **Stündlich**: Mehrere Stunden und Minuten mit beliebigen Stunden (0-23) und beliebigen Minuten (0-60).
- **Täglich**: Option zur Wiederholung nach einer festgelegten Anzahl von Tagen, beispielsweise alle 3 Tage.
- **Wöchentlich**: Sonntag bis Montag, mit der Option, am ersten Tag der Woche oder an mehreren Tagen der Woche einen Snapshot durchzuführen.
- **Monatlich**: Januar bis Dezember, mit der Option, an bestimmten oder mehreren Tagen im Monat aufzutreten, zum Beispiel am 7.

NetApp Backup and Recovery verwendet die folgenden Zeitplanebenen, die sich leicht unterscheiden:

- **Stündlich**: Führt Snapshots nur in 15-Minuten-Intervallen aus, beispielsweise alle 1 Stunde oder in 15-Minuten-Intervallen unter 60.
- **Täglich**: Stunden des Tages (0–23) mit Startzeit beispielsweise um 10:00 Uhr mit der Option, alle paar Stunden eine Ausführung durchzuführen.
- **Wöchentlich**: Wochentag (Sonntag bis Montag) mit der Option, an einem oder mehreren Tagen aufzutreten. Dies ist dasselbe wie SnapCenter.
- **Monatlich**: Daten des Monats (0–30) mit einer Startzeit an mehreren Daten des Monats.
- **Jährlich**: Monatlich. Dies entspricht dem monatlichen SnapCenter.

Mehrere Richtlinien in SnapCenter mit derselben Zeitplanebene

Sie können einer Ressource in SnapCenter mehrere Richtlinien mit derselben Zeitplanebene zuweisen. NetApp Backup and Recovery unterstützt jedoch nicht mehrere Richtlinien für eine Ressource, die dieselbe Zeitplanebene verwendet.

Beispiel: Wenn Sie in SnapCenter drei Richtlinien (für Daten, Protokoll und Protokoll von Snapshots) verwenden, verwendet NetApp Backup and Recovery nach der Migration von SnapCenter eine einzige Richtlinie anstelle aller drei.

Importierte SnapCenter -Tagespläne

NetApp Backup and Recovery passt die SnapCenter -Zeitpläne wie folgt an:

- Wenn der SnapCenter -Zeitplan auf weniger als oder gleich 7 Tage eingestellt ist, legt NetApp Backup and Recovery den Zeitplan auf wöchentlich fest. Einige Schnappschüsse werden während der Woche übersprungen.

Beispiel: Wenn Sie über eine SnapCenter -Tagesrichtlinie mit einem Wiederholungsintervall von drei Tagen ab Montag verfügen, legt NetApp Backup and Recovery den Zeitplan auf wöchentlich am Montag, Donnerstag und Sonntag fest. Einige Tage werden übersprungen, da es nicht genau alle 3 Tage ist.

- Wenn der SnapCenter -Zeitplan auf mehr als 7 Tage eingestellt ist, legt NetApp Backup and Recovery den Zeitplan auf monatlich fest. Einige Schnappschüsse werden im Laufe des Monats übersprungen.

  Beispiel: Wenn Sie über eine SnapCenter -Tagesrichtlinie mit einem Wiederholungsintervall von 10 Tagen ab dem 2. des Monats verfügen, legt NetApp Backup and Recovery den Zeitplan nach der Migration am 2., 12. und 22. Tag des Monats auf monatlich fest. Bei NetApp Backup and Recovery werden im nächsten Monat einige Tage ausgelassen.

Importierte SnapCenter -Stundenpläne

Stündliche SnapCenter -Richtlinien mit Wiederholungsintervallen von mehr als einer Stunde werden in NetApp Backup and Recovery in eine tägliche Richtlinie umgewandelt.

Bei jeder stündlichen Richtlinie mit Wiederholungsintervallen, die kein Faktor von 24 sind (z. B. 5, 7 usw.), werden einige Snapshots an einem Tag übersprungen.

Beispiel: Wenn Sie über eine stündliche SnapCenter -Richtlinie mit einem Wiederholungsintervall alle 5 Stunden ab 1:00 Uhr verfügen, legt NetApp Backup and Recovery (nach der Migration) den Zeitplan auf täglich mit 5-Stunden-Intervallen um 1:00 Uhr, 6:00 Uhr, 11:00 Uhr, 16:00 Uhr und 21:00 Uhr fest. Einige Stunden werden übersprungen. Nach 21:00 Uhr sollte es 2:00 Uhr sein, um es alle 5 Stunden zu wiederholen, aber es wird immer 1:00 Uhr sein.

Protokollaufbewahrung aus SnapCenter -Richtlinien

Wenn Sie in SnapCenter über eine Ressource mit mehreren Richtlinien verfügen, verwendet NetApp Backup and Recovery die folgende Prioritätsreihenfolge, um den Protokollaufbewahrungswert zuzuweisen:

- Für „Vollständige Sicherung mit Protokollsicherungsrichtlinie“ plus „Nur-Protokoll“-Richtlinien in SnapCenter verwendet NetApp Backup and Recovery den Aufbewahrungswert der Nur-Protokoll-Richtlinie.
- Für die Richtlinien „Vollständige Sicherung nur mit Protokoll“ und „Vollständig und Protokoll“ in SnapCenter verwendet NetApp Backup and Recovery den Nur-Protokoll-Aufbewahrungswert.
- Für „Vollständige Sicherung und Protokoll“ plus „Vollständige Sicherung“ in SnapCenter verwendet NetApp Backup and Recovery den Aufbewahrungswert „Vollständige Sicherung und Protokoll“.
- Wenn Sie in SnapCenter nur über eine vollständige Sicherung verfügen, aktiviert NetApp Backup and Recovery die Protokollsicherung nicht.

Aufbewahrungsdauer der Protokollsicherung

SnapCenter unterstützt mehrere Aufbewahrungswerte für Richtlinien für eine Ressource. NetApp Backup and Recovery unterstützt nur einen Aufbewahrungswert pro Ressource.

Aufbewahrungsanzahl aus SnapCenter -Richtlinien

Wenn Sie über eine Ressource mit aktiviertem sekundärem Schutz in SnapCenter mit mehreren Quellvolumes, mehreren Zielvolumes und mehreren SnapMirror -Beziehungen verfügen, verwendet NetApp Backup and Recovery nur die Aufbewahrungsanzahl der ersten Richtlinie.

Beispiel: Wenn Sie eine SnapCenter -Richtlinie mit einer Aufbewahrungsanzahl von 5 und eine andere

Richtlinie mit einer Aufbewahrungsanzahl von 10 haben, verwendet NetApp Backup and Recovery die Aufbewahrungsanzahl von 5.

SnapMirror -Labels aus SnapCenter -Richtlinien

SnapCenter behält nach der Migration SnapMirror -Beschriftungen für jede Richtlinie bei, auch wenn sich die Ebene ändert.

Beispiel: Eine stündliche Richtlinie von SnapCenter kann in NetApp Backup and Recovery auf täglich geändert werden. Die SnapMirror -Beschriftungen bleiben jedoch nach der Migration gleich.

NetApp Backup and Recovery Identity and Access Management (IAM)-Rollen

NetApp Backup and Recovery verwendet Identity and Access Management (IAM), um den Zugriff jedes Benutzers auf bestimmte Funktionen und Aktionen zu regeln.

Weitere Informationen zu IAM-Rollen, die speziell für NetApp Backup and Recovery gelten, finden Sie unter "NetApp Backup and Recovery -Rollen in der NetApp Console" .

Wiederherstellen der NetApp Backup and Recovery -Konfigurationsdaten in einer Dark Site

Wenn Sie NetApp Backup and Recovery an einem Standort ohne Internetzugang verwenden (bekannt als *privater Modus*), werden die Konfigurationsdaten von NetApp Backup and Recovery im StorageGRID oder ONTAP S3-Bucket gesichert, in dem Ihre Backups gespeichert werden. Wenn Sie ein Problem mit dem Hostsystem des Konsolenagenten haben, können Sie einen neuen Konsolenagenten bereitstellen und die kritischen NetApp Backup and Recovery -Daten wiederherstellen.

Dieses Verfahren gilt nur für ONTAP Volume-Daten.

Wenn Sie NetApp Backup and Recovery in einer SaaS-Umgebung verwenden und der Konsolenagent bei Ihrem Cloud-Anbieter oder auf Ihrem eigenen mit dem Internet verbundenen Host bereitgestellt wird, sichert und schützt das System alle wichtigen Konfigurationsdaten in der Cloud. Wenn Sie ein Problem mit dem Konsolenagenten haben, erstellen Sie einen neuen Konsolenagenten und fügen Sie Ihre Systeme hinzu. Die Sicherungsdetails werden automatisch wiederhergestellt.

Es werden zwei Arten von Daten gesichert:

- NetApp Backup and Recovery -Datenbank – enthält eine Liste aller Volumes, Sicherungsdateien, Sicherungsrichtlinien und Konfigurationsinformationen.
- Indizierte Katalogdateien – enthalten detaillierte Indizes, die für die Such- und Wiederherstellungsfunktion verwendet werden und Ihre Suche nach Volumedaten, die Sie wiederherstellen möchten, sehr schnell und effizient machen.

Diese Daten werden einmal täglich um Mitternacht gesichert und es werden maximal 7 Kopien jeder Datei aufbewahrt. Wenn der Konsolenagent mehrere lokale ONTAP -Systeme verwaltet, werden die NetApp Backup and Recovery im Bucket des zuerst aktivierten Systems gespeichert.

In der NetApp Backup and Recovery -Datenbank oder in den indizierten Katalogdateien sind niemals Volumedaten enthalten.

Wiederherstellen von NetApp Backup and Recovery -Daten auf einem neuen Konsolenagenten

Wenn Ihr lokaler Konsolenagent nicht mehr funktioniert, müssen Sie einen neuen Konsolenagenten installieren und dann die NetApp Backup and Recovery -Daten auf dem neuen Konsolenagenten wiederherstellen.

Sie müssen die folgenden Aufgaben ausführen, um Ihr NetApp Backup and Recovery -System wieder in einen funktionsfähigen Zustand zu versetzen:

- Installieren Sie einen neuen Konsolenagenten
- Wiederherstellen der NetApp Backup and Recovery -Datenbank
- Wiederherstellen der indizierten Katalogdateien
- Erkennen Sie alle Ihre On-Premise ONTAP -Systeme und StorageGRID Systeme erneut in der NetApp Console Benutzeroberfläche.

Nachdem Sie überprüft haben, ob Ihr System funktioniert, erstellen Sie neue Sicherungsdateien.

Was du brauchst

Sie müssen auf die aktuellsten Datenbank- und Indexsicherungen aus dem StorageGRID oder ONTAP S3-Bucket zugreifen, in dem Ihre Sicherungsdateien gespeichert sind:

- NetApp Backup and Recovery MySQL-Datenbankdatei

  Diese Datei befindet sich am folgenden Speicherort im Bucket `netapp-backup-<GUID>/mysql_backup/` und es heißt `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- ZIP-Sicherungsdatei des indizierten Katalogs

  Diese Datei befindet sich am folgenden Speicherort im Bucket `netapp-backup-<GUID>/catalog_backup/` und es heißt `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

Installieren Sie einen neuen Konsolen-Agenten auf einem neuen lokalen Linux-Host

Laden Sie beim Installieren eines neuen Konsolenagenten dieselbe Softwareversion herunter wie beim ursprünglichen Agenten. Änderungen an der NetApp Backup and Recovery -Datenbank können dazu führen, dass neuere Softwareversionen nicht mit alten Datenbanksicherungen funktionieren. Du kannst "Aktualisieren Sie die Konsolen-Agent-Software auf die neueste Version, nachdem Sie die Backup-Datenbank wiederhergestellt haben." .

1. "Installieren Sie den Konsolen-Agenten auf einem neuen lokalen Linux-Host"
2. Melden Sie sich mit den soeben erstellten Administrator-Benutzeranmeldeinformationen bei der Konsole an.

Wiederherstellen der NetApp Backup and Recovery -Datenbank

1. Kopieren Sie die MySQL-Sicherung vom Sicherungsspeicherort auf den neuen Konsolen-Agent-Host. Wir verwenden unten den Beispieldateinamen „CBS_DB_Backup_23_05_2023.sql“.

2. Kopieren Sie die Sicherung mit einem der folgenden Befehle in den MySQL-Docker-Container, je nachdem, ob Sie einen Docker- oder Podman-Container verwenden:

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Rufen Sie die MySQL-Container-Shell mit einem der folgenden Befehle auf, je nachdem, ob Sie einen Docker- oder Podman-Container verwenden:

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. Stellen Sie in der Container-Shell die „Umgebung“ bereit.
5. Sie benötigen das MySQL-DB-Passwort. Kopieren Sie daher den Wert des Schlüssels „MYSQL_ROOT_PASSWORD“.
6. Stellen Sie die MySQL-Datenbank von NetApp Backup and Recovery mit dem folgenden Befehl wieder her:

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Überprüfen Sie mit den folgenden SQL-Befehlen, ob die MySQL-Datenbank von NetApp Backup and Recovery korrekt wiederhergestellt wurde:

```
mysql -u root -p cloud_backup
```

8. Geben Sie das Passwort ein.

```
mysql> show tables;
mysql> select * from volume;
```

9. Stellen Sie sicher, dass die angezeigten Volumina mit denen Ihrer ursprünglichen Umgebung übereinstimmen.

Wiederherstellen der indizierten Katalogdateien

1. Kopieren Sie die ZIP-Sicherungsdatei des indizierten Katalogs (wir verwenden den Beispieldateinamen „Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip“) vom Sicherungsspeicherort auf den neuen Konsolenagent-Host im Ordner „/opt/application/netapp/cbs“.

2. Entpacken Sie die Datei „Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip“ mit dem folgenden Befehl:

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Führen Sie den Befehl **ls** aus, um sicherzustellen, dass der Ordner „catalogdb1“ mit den darunter liegenden Unterordnern „changes“ und „snapshots“ erstellt wurde.

Entdecken Sie Ihre ONTAP -Cluster und StorageGRID Systeme

1. "Entdecken Sie alle On-Premise ONTAP Systeme"die in Ihrer vorherigen Umgebung verfügbar waren. Dazu gehört auch das ONTAP -System, das Sie als S3-Server verwendet haben.
2. "Entdecken Sie Ihre StorageGRID -Systeme".

Einrichten der StorageGRID -Umgebungsdetails

Fügen Sie die Details des StorageGRID -Systems hinzu, das mit Ihren ONTAP -Systemen verknüpft ist, wie sie im ursprünglichen Konsolen-Agent-Setup eingerichtet wurden, mithilfe des "NetApp Console -APIs" .

Die folgenden Informationen gelten für Installationen im privaten Modus ab NetApp Console 3.9.xx. Bei älteren Versionen gehen Sie wie folgt vor: "DarkSite Cloud Backup: MySQL und indizierter Katalog sichern und wiederherstellen" .

Sie müssen diese Schritte für jedes System ausführen, das Daten auf StorageGRID sichert.

1. Extrahieren Sie das Autorisierungstoken mithilfe der folgenden OAuth/Token-API.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '
{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"pas
sword"}
> '
```

Während es sich bei der IP-Adresse, dem Benutzernamen und den Passwörtern um benutzerdefinierte Werte handelt, ist dies beim Kontonamen nicht der Fall. Der Kontoname lautet immer „account-DARKSITE1“. Außerdem muss der Benutzername einen Namen im E-Mail-Format verwenden.

Diese API gibt eine Antwort wie die folgende zurück. Sie können das Autorisierungstoken wie unten gezeigt abrufen.

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```

2. Extrahieren Sie die System-ID und die X-Agent-ID mithilfe der Tenancy/External/Resource-API.

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Diese API gibt eine Antwort wie die folgende zurück. Der Wert unter „resourceIdentifier“ bezeichnet die *WorkingEnvironment-ID* und der Wert unter „agentId“ bezeichnet *x-agent-id*.

```
[{"resourceIdentifier":"OnPremWorkingEnvironment-
pMtZND0M","resourceType":"ON_PREM","agentId":"vB_1xShPpBtUosjD7wfBlLIhqD
gIPA0wclients","resourceClass":"ON_PREM","name":"CBSFAS8300-01-
02","metadata":"{\"clusterUuid\": \"2cb6cb4b-dc07-11ec-9114-
d039ea931e09\"}","workspaceIds":["workspace2wKYjTy9"],"agentIds":["vB_1x
ShPpBtUosjD7wfBlLIhqDgIPA0wclients"]}]
```

3. Aktualisieren Sie die NetApp Backup and Recovery -Datenbank mit den Details des mit den Systemen verknüpften StorageGRID Systems. Stellen Sie sicher, dass Sie den vollqualifizierten Domänennamen des StorageGRID sowie den Zugriffsschlüssel und den Speicherschlüssel wie unten gezeigt eingeben:

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

Überprüfen der NetApp Backup and Recovery -Einstellungen

1. Wählen Sie jedes ONTAP -System aus und klicken Sie im rechten Bereich neben dem Sicherungs- und Wiederherstellungsdienst auf **Sicherungen anzeigen**.

   Sie sollten alle für Ihre Volumes erstellten Backups sehen.

2. Klicken Sie im Wiederherstellungs-Dashboard im Abschnitt „Suchen und Wiederherstellen“ auf **Indizierungseinstellungen**.

   Stellen Sie sicher, dass die Systeme, bei denen die indizierte Katalogisierung zuvor aktiviert war, aktiviert bleiben.

3. Führen Sie auf der Seite „Suchen und Wiederherstellen“ einige Katalogsuchen durch, um zu bestätigen, dass die Wiederherstellung des indizierten Katalogs erfolgreich abgeschlossen wurde.

Unterstützte AWS-Archivspeicherebenen mit NetApp Backup and Recovery

NetApp Backup and Recovery unterstützt zwei S3-Archivspeicherklassen und die meisten Regionen.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -UI-Versionen finden Sie unter"Wechseln Sie zur vorherigen NetApp Backup and Recovery -Benutzeroberfläche" .

Unterstützte S3-Archivspeicherklassen für NetApp Backup and Recovery

Wenn Sicherungsdateien zunächst erstellt werden, werden sie im S3-Standardspeicher gespeichert. Diese Ebene ist für die Speicherung selten abgerufener Daten optimiert, ermöglicht Ihnen aber auch den sofortigen Zugriff darauf. Nach 30 Tagen werden die Backups aus Kostengründen in die Speicherklasse S3 *Standard-Infrequent Access* verschoben.

Wenn auf Ihren Quellclustern ONTAP 9.10.1 oder höher ausgeführt wird, können Sie zur weiteren Kostenoptimierung Backups nach einer bestimmten Anzahl von Tagen (normalerweise mehr als 30 Tage) entweder auf *S3 Glacier*- oder *S3 Glacier Deep Archive*-Speicher verschieben. Sie können dies auf „0“ oder auf 1–999 Tage einstellen. Wenn Sie es auf „0“ Tage einstellen, können Sie es später nicht auf 1–999 Tage ändern.

Auf die Daten in diesen Ebenen kann bei Bedarf nicht sofort zugegriffen werden und der Abruf ist mit höheren Kosten verbunden. Sie müssen daher berücksichtigen, wie oft Sie Daten aus diesen archivierten Sicherungsdateien wiederherstellen müssen. Weitere Informationen zum Wiederherstellen von Daten aus dem Archivspeicher finden Sie im Abschnitt auf dieser Seite.

- Wenn Sie bei der Aktivierung von NetApp Backup and Recovery in Ihrer ersten Sicherungsrichtlinie keine Archivebene auswählen, ist *S3 Glacier* Ihre einzige Archivierungsoption für zukünftige Richtlinien.
- Wenn Sie in Ihrer ersten Sicherungsrichtlinie *S3 Glacier* auswählen, können Sie für zukünftige Sicherungsrichtlinien für diesen Cluster zur Ebene *S3 Glacier Deep Archive* wechseln.
- Wenn Sie in Ihrer ersten Sicherungsrichtlinie *S3 Glacier Deep Archive* auswählen, ist diese Ebene die einzige Archivebene, die für zukünftige Sicherungsrichtlinien für diesen Cluster verfügbar ist.

Beachten Sie, dass Sie beim Konfigurieren von NetApp Backup and Recovery mit dieser Art von Lebenszyklusregel beim Einrichten des Buckets in Ihrem AWS-Konto keine Lebenszyklusregeln konfigurieren dürfen.

"Erfahren Sie mehr über S3-Speicherklassen".

Daten aus dem Archivspeicher wiederherstellen

Während die Speicherung älterer Sicherungsdateien im Archivspeicher wesentlich weniger kostspielig ist als die Speicherung im Standard- oder Standard-IA-Speicher, dauert der Zugriff auf Daten aus einer Sicherungsdatei im Archivspeicher für Wiederherstellungsvorgänge länger und ist teurer.

Wie viel kostet die Wiederherstellung von Daten aus Amazon S3 Glacier und Amazon S3 Glacier Deep Archive?

Beim Abrufen von Daten aus Amazon S3 Glacier können Sie zwischen 3 Wiederherstellungsprioritäten und beim Abrufen von Daten aus Amazon S3 Glacier Deep Archive zwischen 2 Wiederherstellungsprioritäten wählen. S3 Glacier Deep Archive kostet weniger als S3 Glacier:

Archivebene	Wiederherstellungspriorität und -kosten		
	Hoch	Standard	Niedrig

Archivebene	Wiederherstellungspriorität und -kosten		
S3 Gletscher	Schnellster Abruf, höchste Kosten	Langsamere Abfrage, geringere Kosten	Langsamster Abruf, niedrigste Kosten
S3 Glacier Deep-Archiv		Schnellere Abfrage, höhere Kosten	Langsamerer Abruf, niedrigste Kosten

Für jede Methode fallen unterschiedliche Abruf- und Anforderungsgebühren pro GB an. Detaillierte S3 Glacier-Preise nach AWS-Region finden Sie auf der "Amazon S3-Preisseite" .

Wie lange dauert die Wiederherstellung meiner in Amazon S3 Glacier archivierten Objekte?

Die gesamte Wiederherstellungszeit besteht aus zwei Teilen:

- **Abrufzeit**: Die Zeit, die zum Abrufen der Sicherungsdatei aus dem Archiv und zum Platzieren im Standardspeicher benötigt wird. Dies wird manchmal als „Rehydratationszeit“ bezeichnet. Die Abrufzeit ist je nach gewählter Wiederherstellungspriorität unterschiedlich.

Archivebene	Wiederherstellungspriorität und Abrufzeit		
	Hoch	**Standard**	**Niedrig**
S3 Gletscher	3-5 Minuten	3-5 Stunden	5-12 Stunden
S3 Glacier Deep-Archiv		12 Stunden	48 Stunden

- **Wiederherstellungszeit**: Die Zeit, die zum Wiederherstellen der Daten aus der Sicherungsdatei im Standardspeicher benötigt wird. Diese Zeit unterscheidet sich nicht von der typischen Wiederherstellungsoperation direkt vom Standardspeicher – wenn keine Archivierungsebene verwendet wird.

Weitere Informationen zu den Abrufoptionen von Amazon S3 Glacier und S3 Glacier Deep Archive finden Sie unter "die Amazon FAQ zu diesen Lagerklassen" .

Unterstützte Azure-Archivzugriffsebenen mit NetApp Backup and Recovery

NetApp Backup and Recovery unterstützt eine Azure-Archivzugriffsebene und die meisten Regionen.

> ⓘ Informationen zum Wechseln zwischen NetApp Backup and Recovery -UI-Versionen finden Sie unter"Wechseln Sie zur vorherigen NetApp Backup and Recovery -Benutzeroberfläche" .

Unterstützte Azure Blob-Zugriffsebenen für NetApp Backup and Recovery

Wenn Sicherungsdateien zunächst erstellt werden, werden sie in der Zugriffsebene *Cool* gespeichert. Diese Ebene ist für die Speicherung von Daten optimiert, auf die selten zugegriffen wird, auf die bei Bedarf jedoch sofort zugegriffen werden kann.

Wenn auf Ihren Quellclustern ONTAP 9.10.1 oder höher ausgeführt wird, können Sie zur weiteren

Kostenoptimierung Backups nach einer bestimmten Anzahl von Tagen (normalerweise mehr als 30 Tage) vom *Cool*- in den *Azure Archive*-Speicher verschieben. Auf Daten dieser Ebene kann bei Bedarf nicht sofort zugegriffen werden und der Abruf ist mit höheren Kosten verbunden. Sie müssen daher berücksichtigen, wie oft Sie Daten aus diesen archivierten Sicherungsdateien wiederherstellen müssen. Weitere Informationen zum Wiederherstellen von Daten aus dem Archivspeicher finden Sie im Abschnitt auf dieser Seite.

Beachten Sie, dass Sie beim Konfigurieren von NetApp Backup and Recovery mit dieser Art von Lebenszyklusregel beim Einrichten des Containers in Ihrem Azure-Konto keine Lebenszyklusregeln konfigurieren dürfen.

"Informationen zu Azure Blob-Zugriffsebenen".

Daten aus dem Archivspeicher wiederherstellen

Während das Speichern älterer Sicherungsdateien im Archivspeicher wesentlich weniger kostspielig ist als die Speicherung im Cool-Speicher, dauert der Zugriff auf Daten aus einer Sicherungsdatei im Azure-Archiv für Wiederherstellungsvorgänge länger und ist teurer.

Wie viel kostet die Wiederherstellung von Daten aus Azure Archive?

Beim Abrufen von Daten aus dem Azure-Archiv können Sie zwischen zwei Wiederherstellungsprioritäten wählen:

- **Hoch**: Schnellster Abruf, höhere Kosten
- **Standard**: Langsamerer Abruf, geringere Kosten

Für jede Methode fallen unterschiedliche Abruf- und Anforderungsgebühren pro GB an. Detaillierte Azure Archive-Preise nach Azure-Region finden Sie auf der "Azure-Preisseite" .

> Die hohe Priorität wird beim Wiederherstellen von Daten von Azure auf StorageGRID -Systemen nicht unterstützt.

Wie lange dauert die Wiederherstellung meiner im Azure-Archiv archivierten Daten?

Die Wiederherstellungszeit besteht aus zwei Teilen:

- **Abrufzeit**: Die Zeit, die zum Abrufen der archivierten Sicherungsdatei aus dem Azure-Archiv und zum Platzieren im Cool-Speicher benötigt wird. Dies wird manchmal als „Rehydratationszeit“ bezeichnet. Die Abrufzeit ist je nach gewählter Wiederherstellungspriorität unterschiedlich:
  - **Hoch**: < 1 Stunde
  - **Standard**: < 15 Stunden
- **Wiederherstellungszeit**: Die Zeit zum Wiederherstellen der Daten aus der Sicherungsdatei im Cool-Speicher. Diese Zeit unterscheidet sich nicht von der typischen Wiederherstellungsoperation direkt aus dem Cool-Speicher – wenn keine Archivierungsebene verwendet wird.

Weitere Informationen zu den Abrufoptionen für Azure-Archive finden Sie unter "diese Azure-FAQ" .

Unterstützte Google-Archivspeicherebenen mit NetApp Backup and Recovery

NetApp Backup and Recovery unterstützt eine Archivspeicherklasse von Google und die meisten Regionen.

Informationen zum Wechseln zwischen NetApp Backup and Recovery -UI-Versionen finden Sie unter"Wechseln Sie zur vorherigen NetApp Backup and Recovery -Benutzeroberfläche" .

Unterstützte Google-Archivspeicherklassen für NetApp Backup and Recovery

Wenn Sicherungsdateien zunächst erstellt werden, werden sie im *Standard*-Speicher gespeichert. Diese Ebene ist für die Speicherung selten abgerufener Daten optimiert, ermöglicht Ihnen aber auch den sofortigen Zugriff darauf.

Wenn Ihr Cluster vor Ort ONTAP 9.12.1 oder höher verwendet, können Sie zur weiteren Kostenoptimierung in der NetApp Backup and Recovery Benutzeroberfläche ältere Backups nach einer bestimmten Anzahl von Tagen (normalerweise mehr als 30 Tage) in den Archivspeicher verschieben. Für die Datenabfrage in dieser Ebene fallen höhere Kosten an. Sie müssen daher berücksichtigen, wie oft Sie Daten aus diesen archivierten Sicherungsdateien wiederherstellen müssen. Weitere Informationen zum Wiederherstellen von Daten aus dem Archivspeicher finden Sie im Abschnitt auf dieser Seite.

Beachten Sie, dass Sie beim Konfigurieren von NetApp Backup and Recovery mit dieser Art von Lebenszyklusregel beim Einrichten des Buckets in Ihrem Google-Konto keine Lebenszyklusregeln konfigurieren dürfen.

"Informationen zu Google-Speicherklassen".

Daten aus dem Archivspeicher wiederherstellen

Während die Speicherung älterer Sicherungsdateien im Archivspeicher wesentlich günstiger ist als die Speicherung im Standardspeicher, dauert der Zugriff auf Daten aus einer Sicherungsdatei im Archivspeicher für Wiederherstellungsvorgänge etwas länger und ist teurer.

Wie viel kostet die Wiederherstellung von Daten aus dem Google-Archiv?

Detaillierte Preise für Google Cloud Storage nach Regionen finden Sie auf der "Preisseite für Google Cloud Storage" .

Wie lange dauert die Wiederherstellung meiner im Google-Archiv archivierten Objekte?

Die gesamte Wiederherstellungszeit besteht aus zwei Teilen:

- **Abrufzeit**: Die Zeit, die zum Abrufen der Sicherungsdatei aus dem Archiv und zum Platzieren im Standardspeicher benötigt wird. Dies wird manchmal als „Rehydratationszeit“ bezeichnet. Im Gegensatz zu den „kältesten“ Speicherlösungen anderer Cloud-Anbieter sind Ihre Daten innerhalb von Millisekunden zugänglich.
- **Wiederherstellungszeit**: Die Zeit, die zum Wiederherstellen der Daten aus der Sicherungsdatei im Standardspeicher benötigt wird. Diese Zeit unterscheidet sich nicht von der typischen Wiederherstellungsoperation direkt vom Standardspeicher – wenn keine Archivierungsebene verwendet wird.

Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtserklärungen, Marken, Patente und mehr.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marken

NETAPP, das NETAPP-Logo und die auf der NetApp -Markenseite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der Patente im Besitz von NetApp finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

Hinweisdateien enthalten Informationen zu Urheberrechten und Lizenzen Dritter, die in der NetApp -Software verwendet werden.

- "Hinweis zur NetApp Console"
- "Hinweis zum NetApp Backup and Recovery"
- "Hinweis zur Wiederherstellung einzelner Dateien"