Schützen Sie ONTAP Volume-Workloads

NetApp Backup and Recovery

NetApp
February 11, 2026

Inhalt

Schützen Sie ONTAP Volume-Workloads

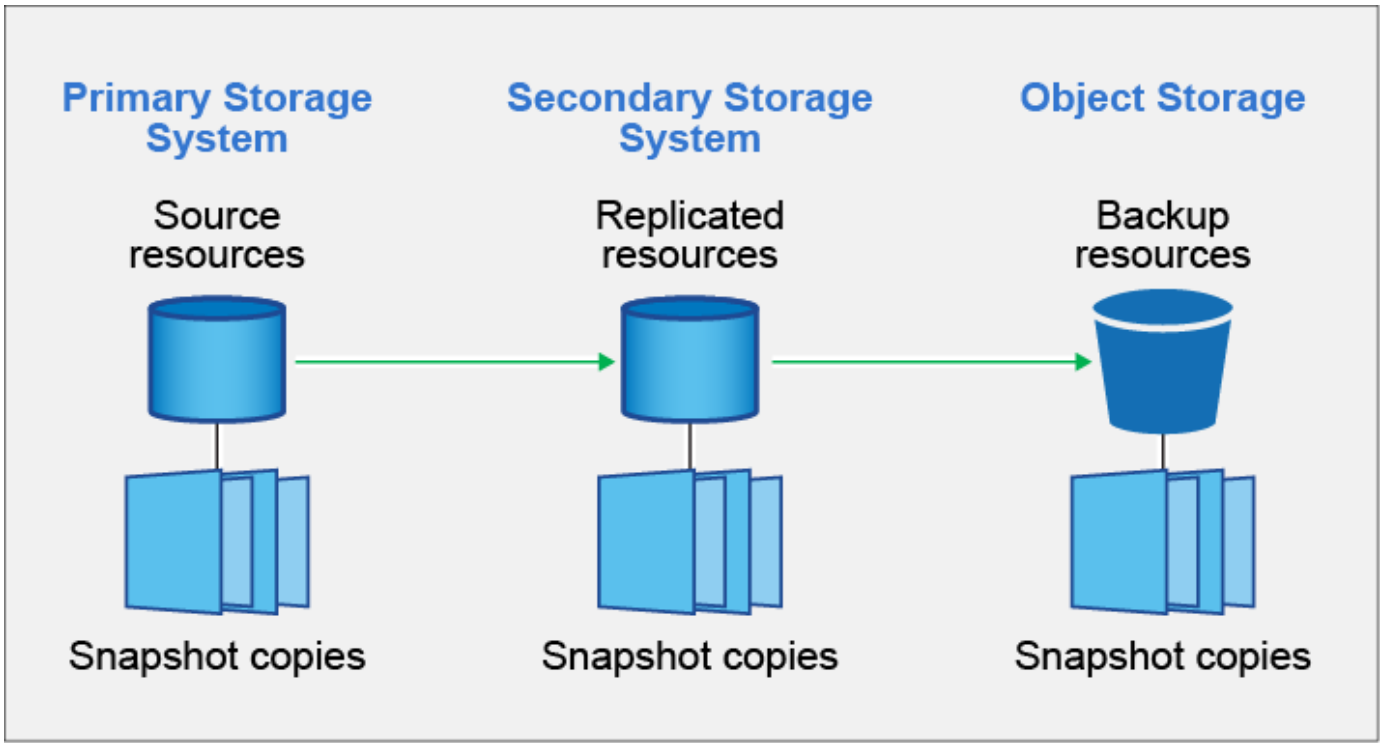
Schützen Sie Ihre ONTAP Volume-Daten mit NetApp Backup and Recovery

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
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".

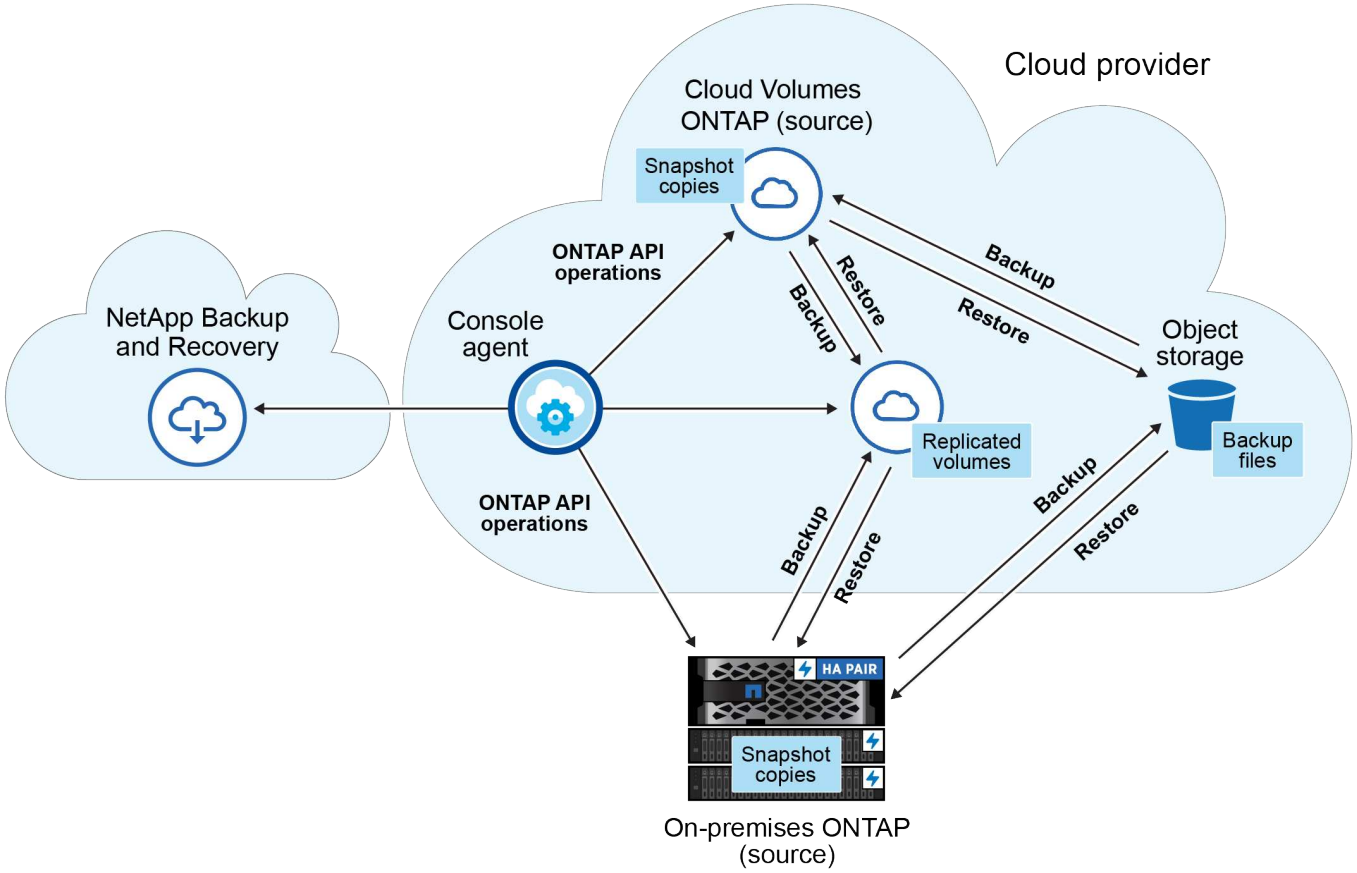
So funktioniert NetApp Backup and Recovery

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?

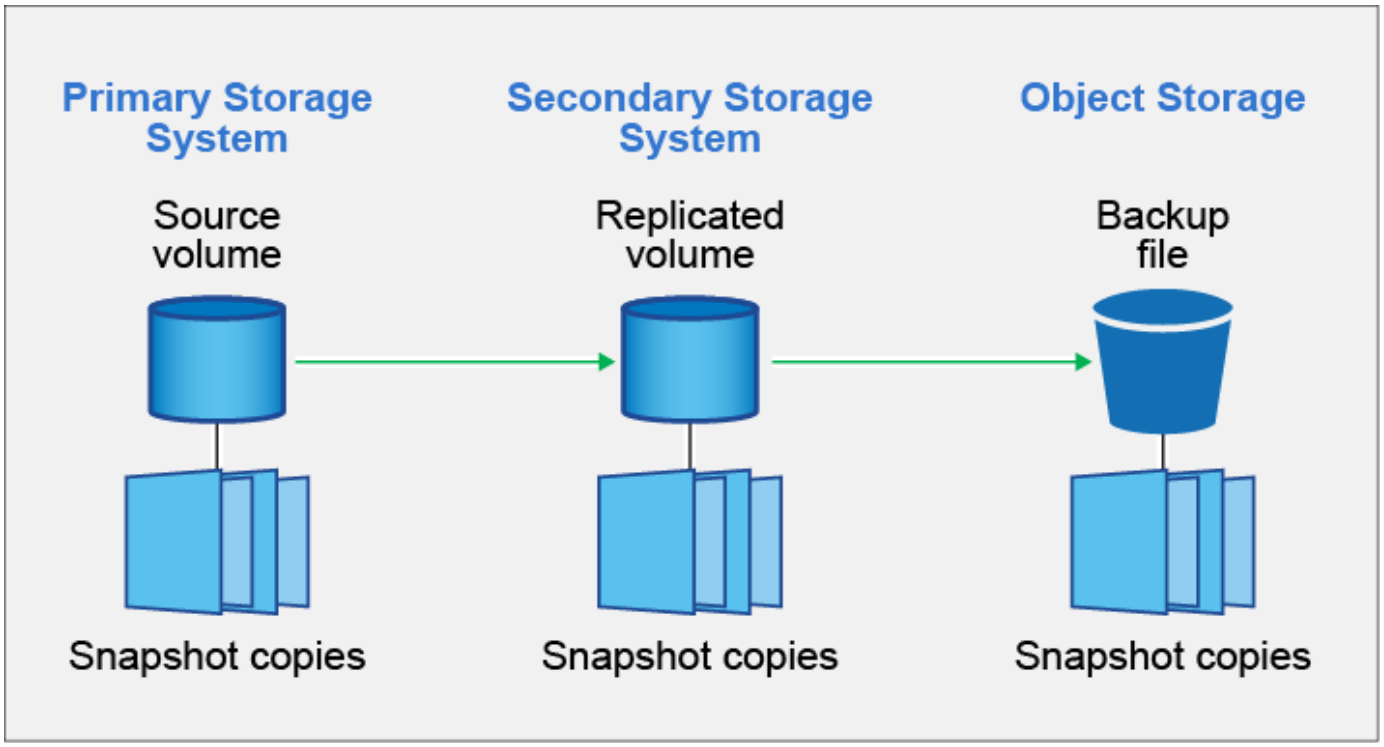
- Möchten Sie, dass der Dienst die Cloud-Buckets für Sie erstellt, oder möchten Sie Ihre Objektspeichercontainer erstellen, bevor Sie beginnen?
- Welchen Bereitstellungsmodus des Konsolenagenten verwenden Sie (Standard-, eingeschränkter oder privater Modus)?

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.

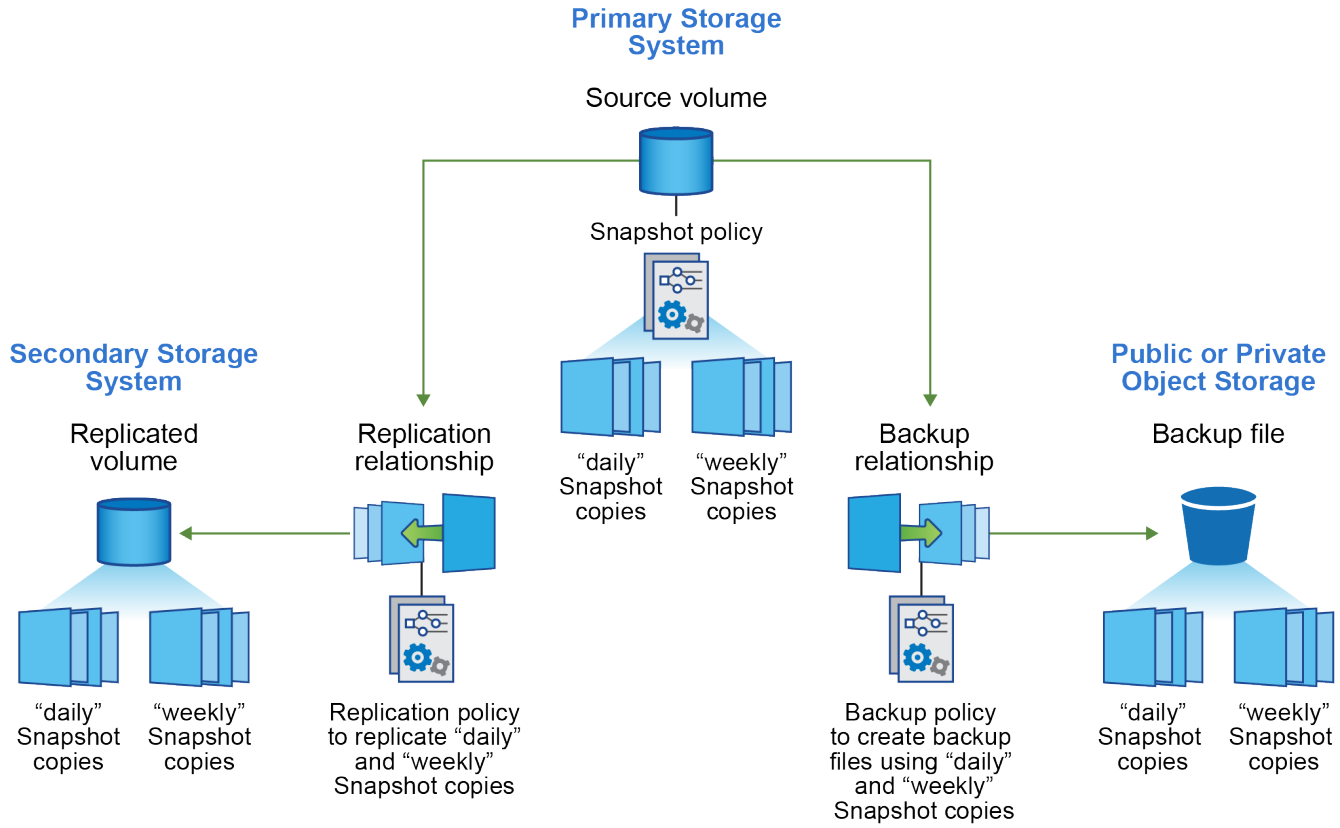
Zusätzlich zu diesen Kriterien bietet der Cloud-Speicher zusätzliche Sicherheitsoptionen, wenn Sie die Funktionen DataLock und Ransomware Resilience verwenden, und zusätzliche Kosteneinsparungen durch die Auswahl von Archivspeicherklassen für ältere Sicherungsdateien. "Erfahren Sie mehr über DataLock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

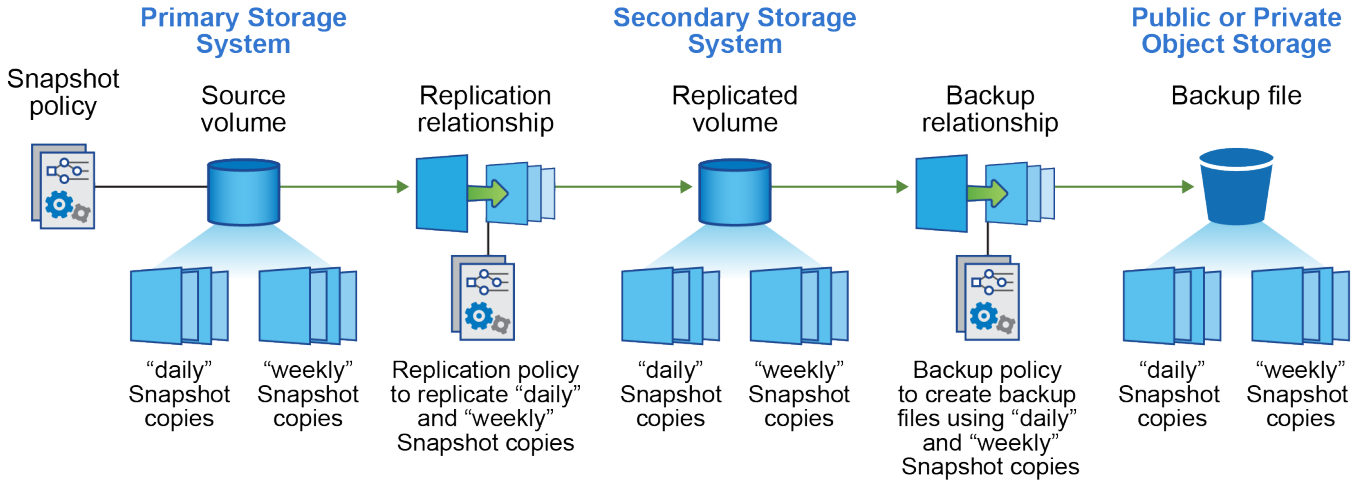
Welche Backup-Architektur werden Sie verwenden?

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
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.

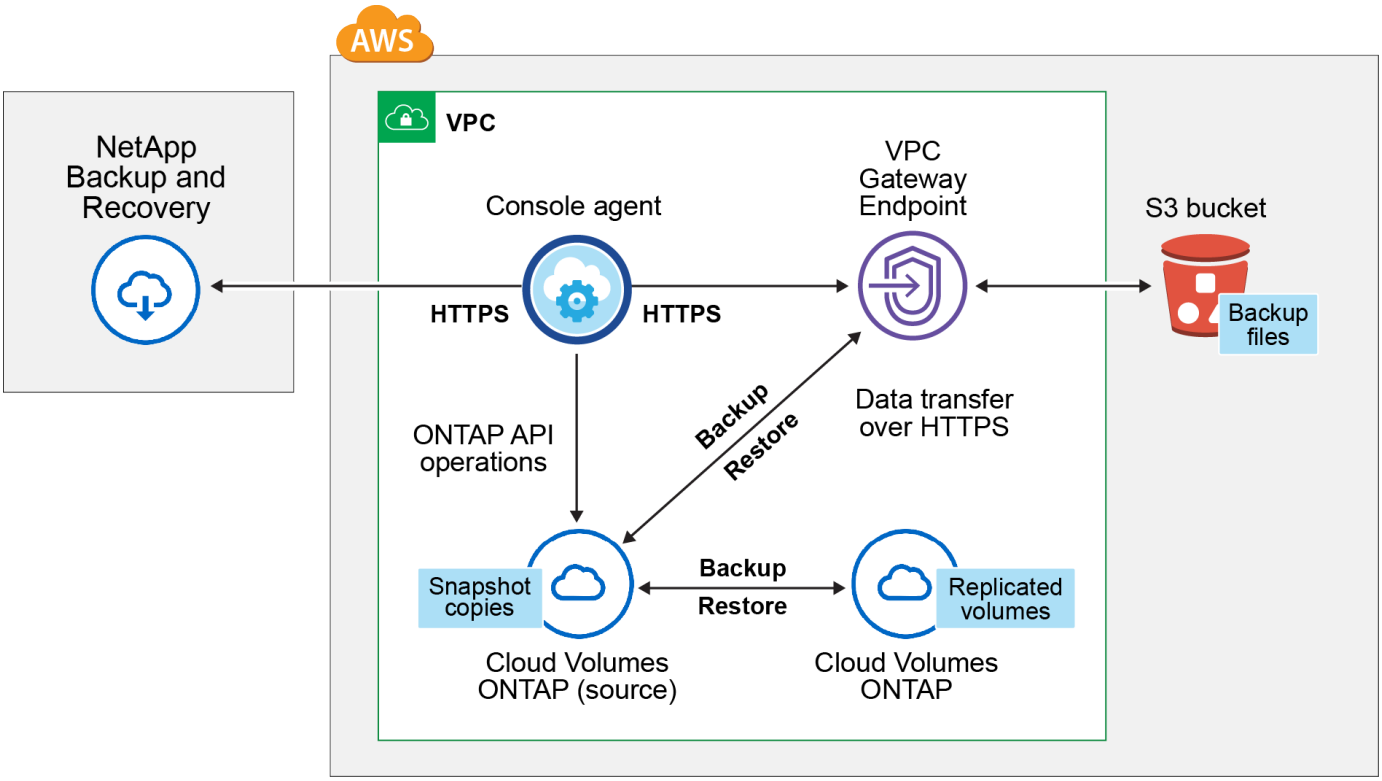
Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

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.

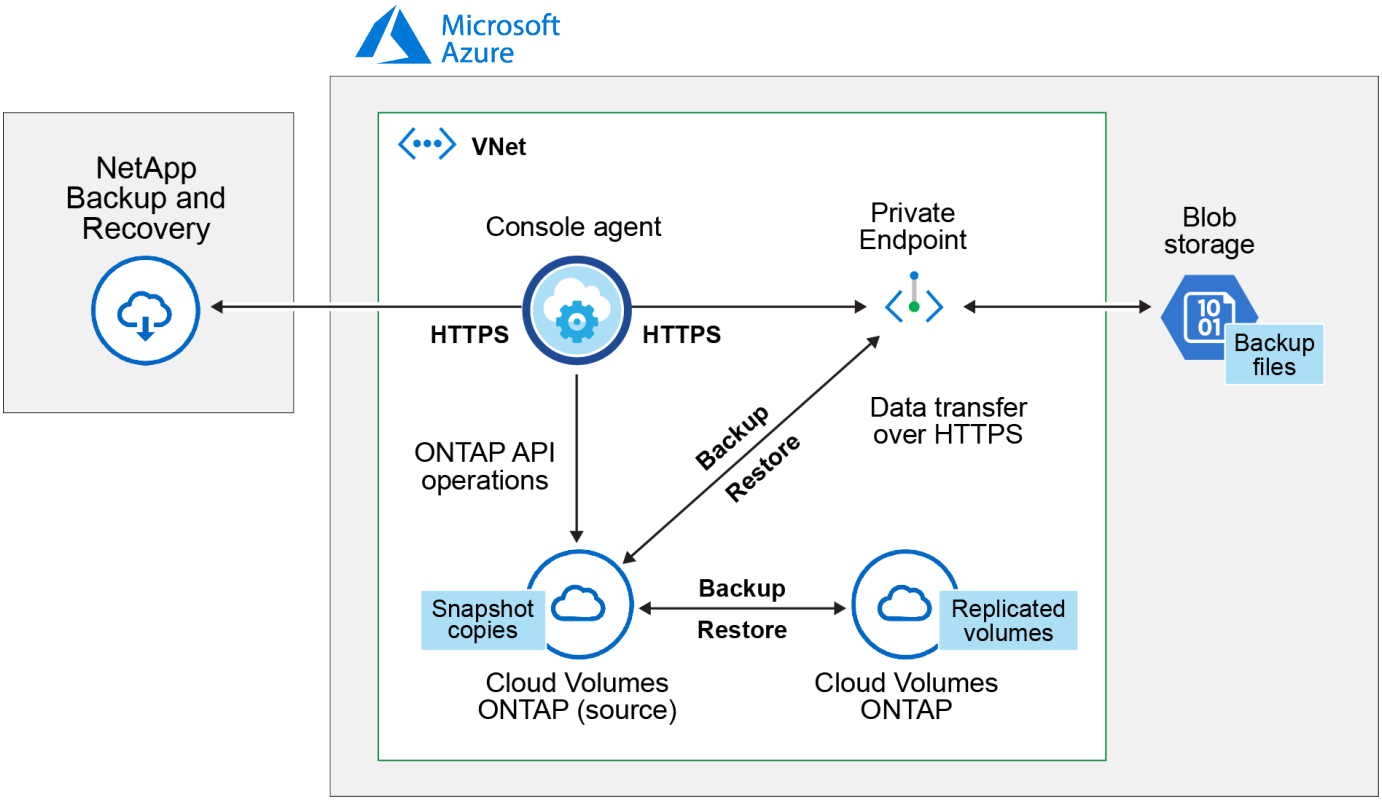
Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

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.

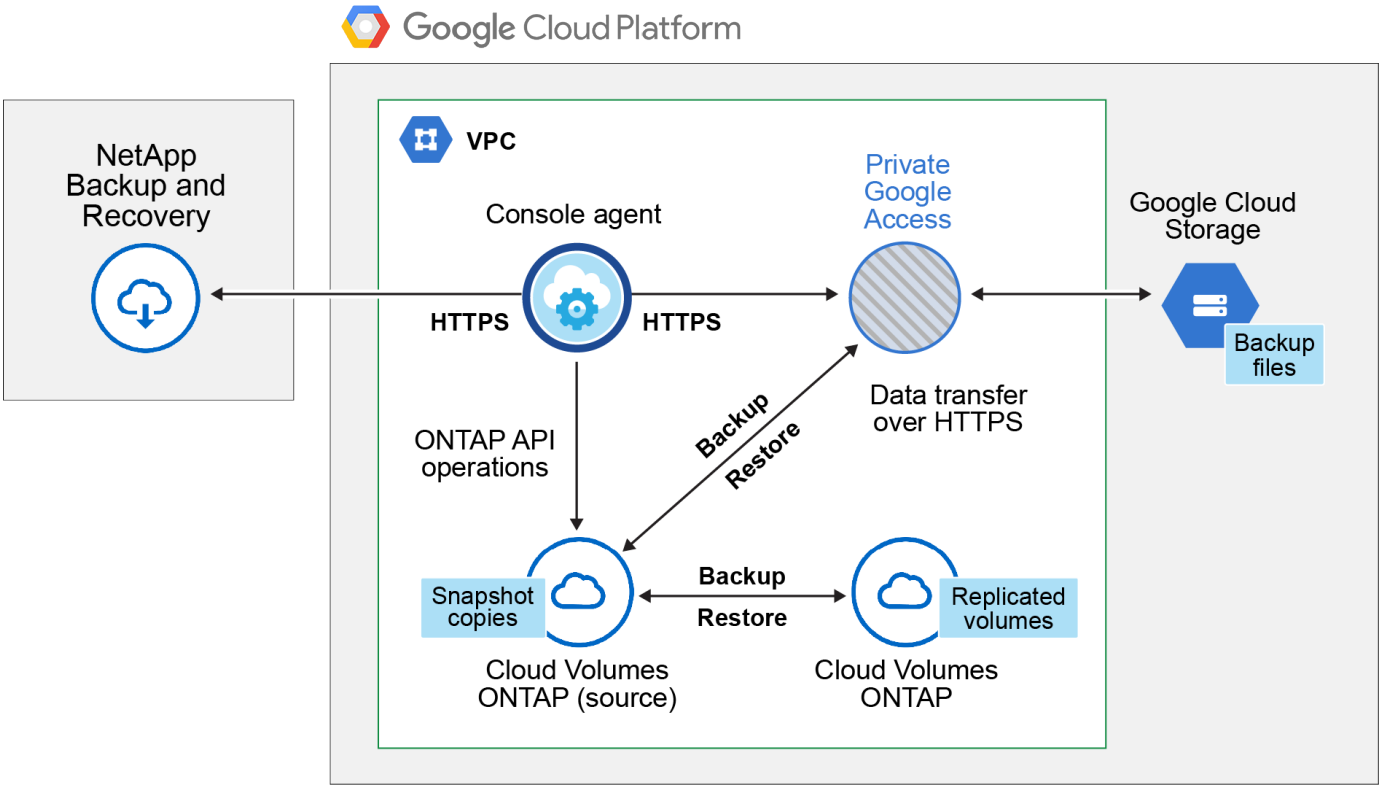
Informationen zum Wechseln zwischen NetApp Backup and Recovery -Workloads finden Sie unter"Wechseln Sie zu anderen NetApp Backup and Recovery -Workloads" .

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" .

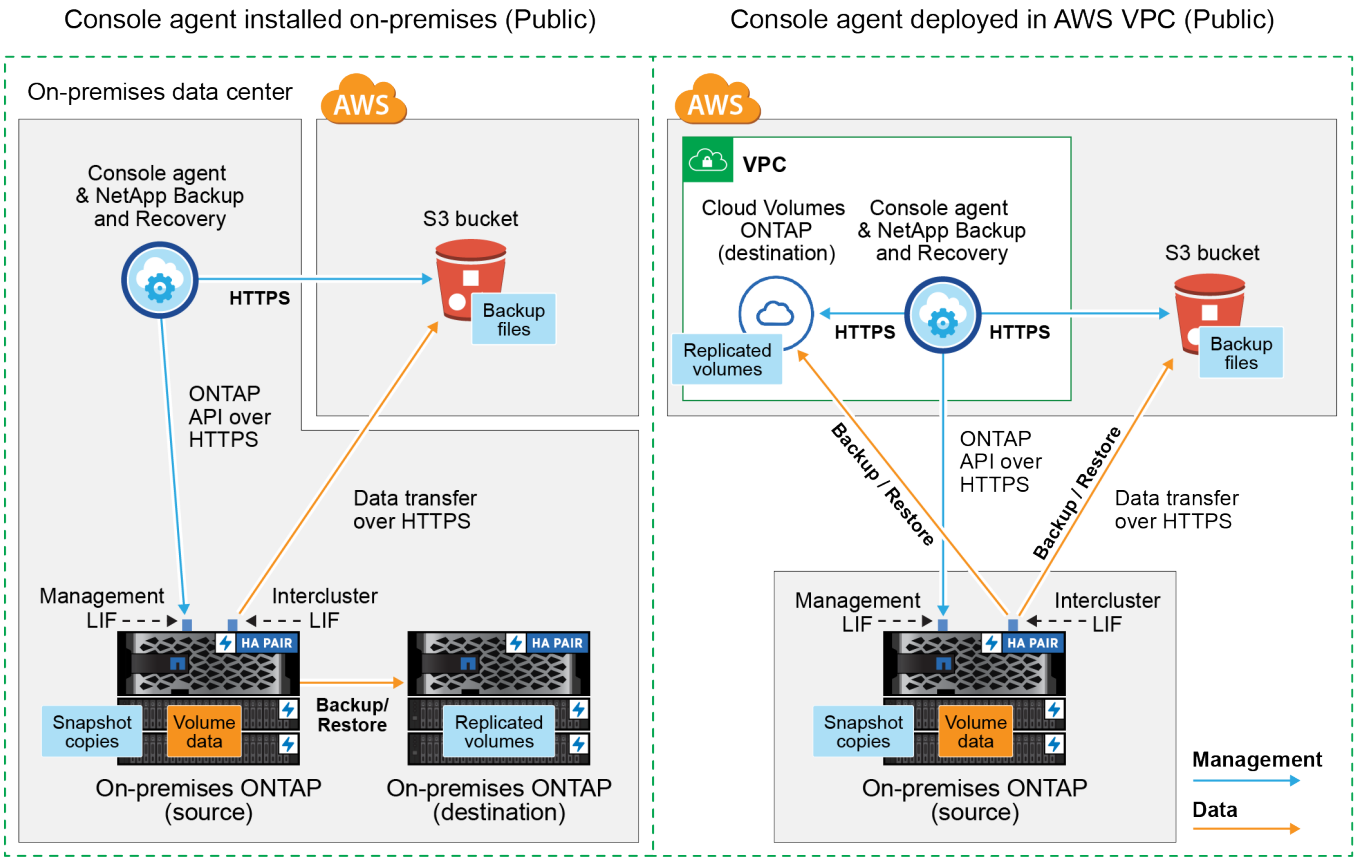
Identifizieren Sie die Verbindungsmethode

Wählen Sie aus, welche der beiden Verbindungsmethoden Sie beim Konfigurieren von Backups von lokalen ONTAP -Systemen zu AWS S3 verwenden möchten.

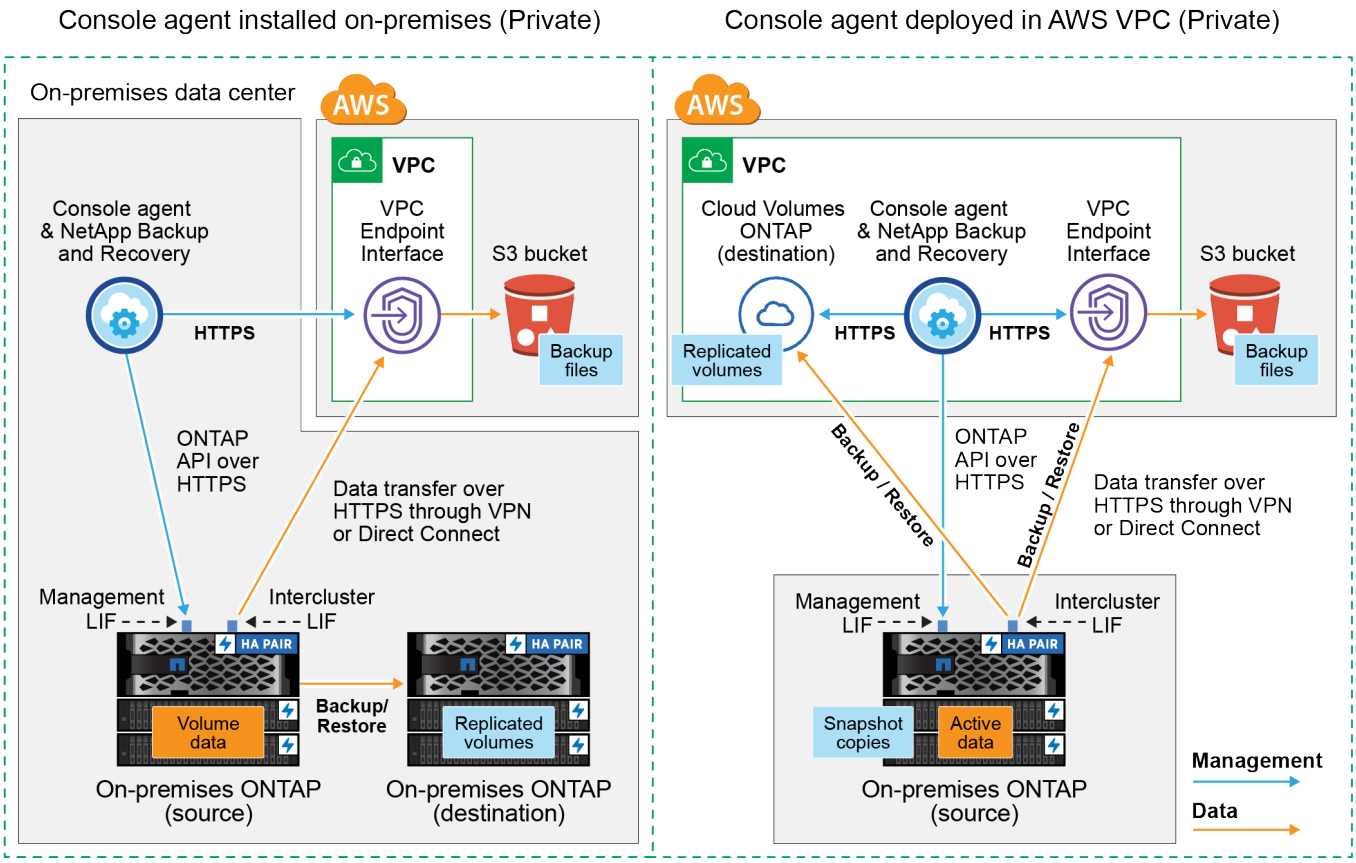
- **Öffentliche Verbindung** – Verbinden Sie das ONTAP -System über einen öffentlichen S3-Endpunkt direkt mit AWS S3.
- **Private Verbindung** – Verwenden Sie ein VPN oder AWS Direct Connect und leiten Sie den Datenverkehr über eine VPC-Endpunktschnittstelle, die eine private IP-Adresse verwendet.

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" .

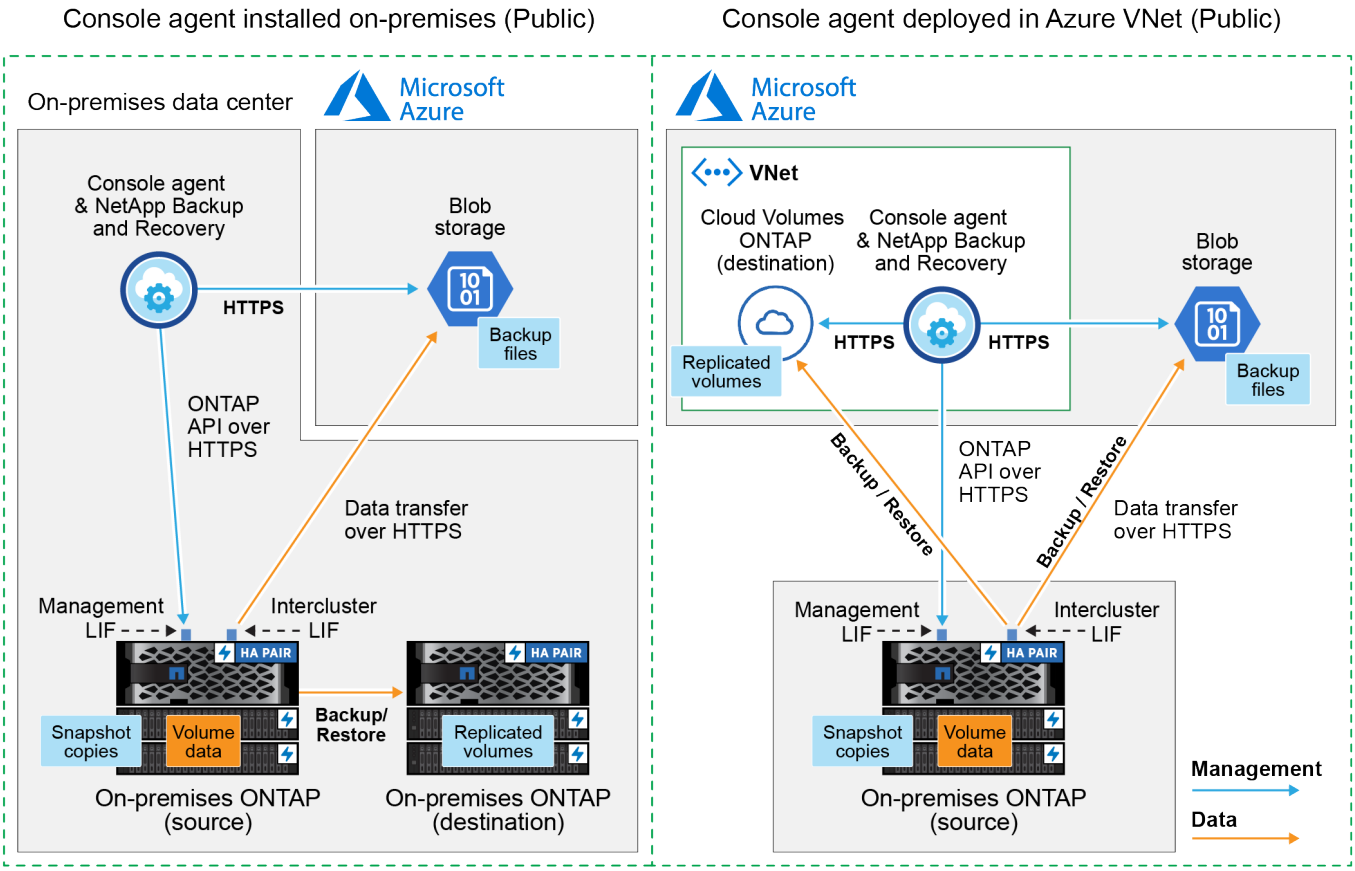
Identifizieren Sie die Verbindungsmethode

Wählen Sie aus, welche der beiden Verbindungsmethoden Sie beim Konfigurieren von Sicherungen von lokalen ONTAP -Systemen zu Azure Blob verwenden möchten.

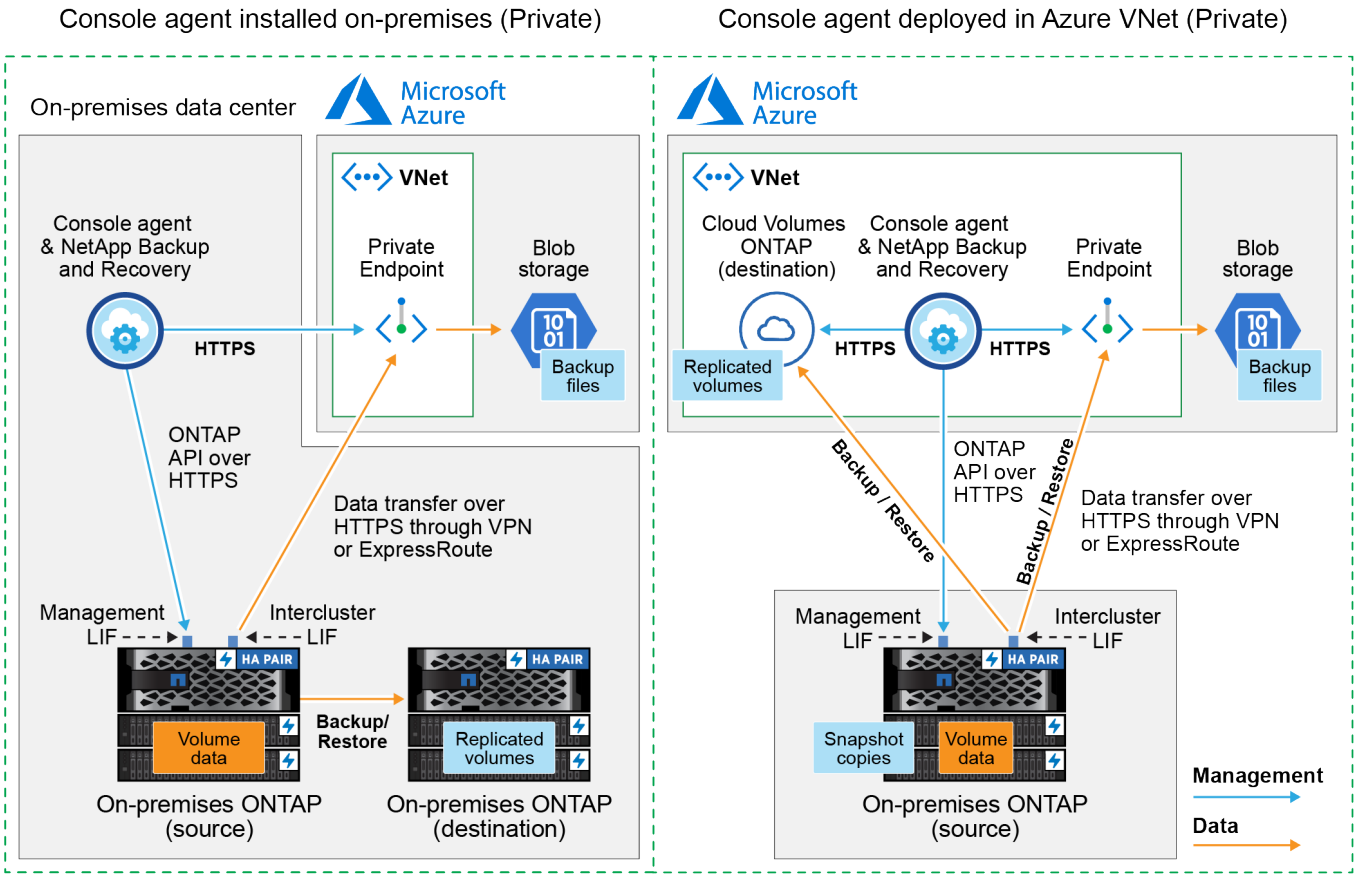
- **Öffentliche Verbindung** – Verbinden Sie das ONTAP -System über einen öffentlichen Azure-Endpunkt direkt mit dem Azure Blob-Speicher.
- **Private Verbindung** – Verwenden Sie ein VPN oder ExpressRoute und leiten Sie den Datenverkehr über einen privaten VNet-Endpunkt, der eine private IP-Adresse verwendet.

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" .

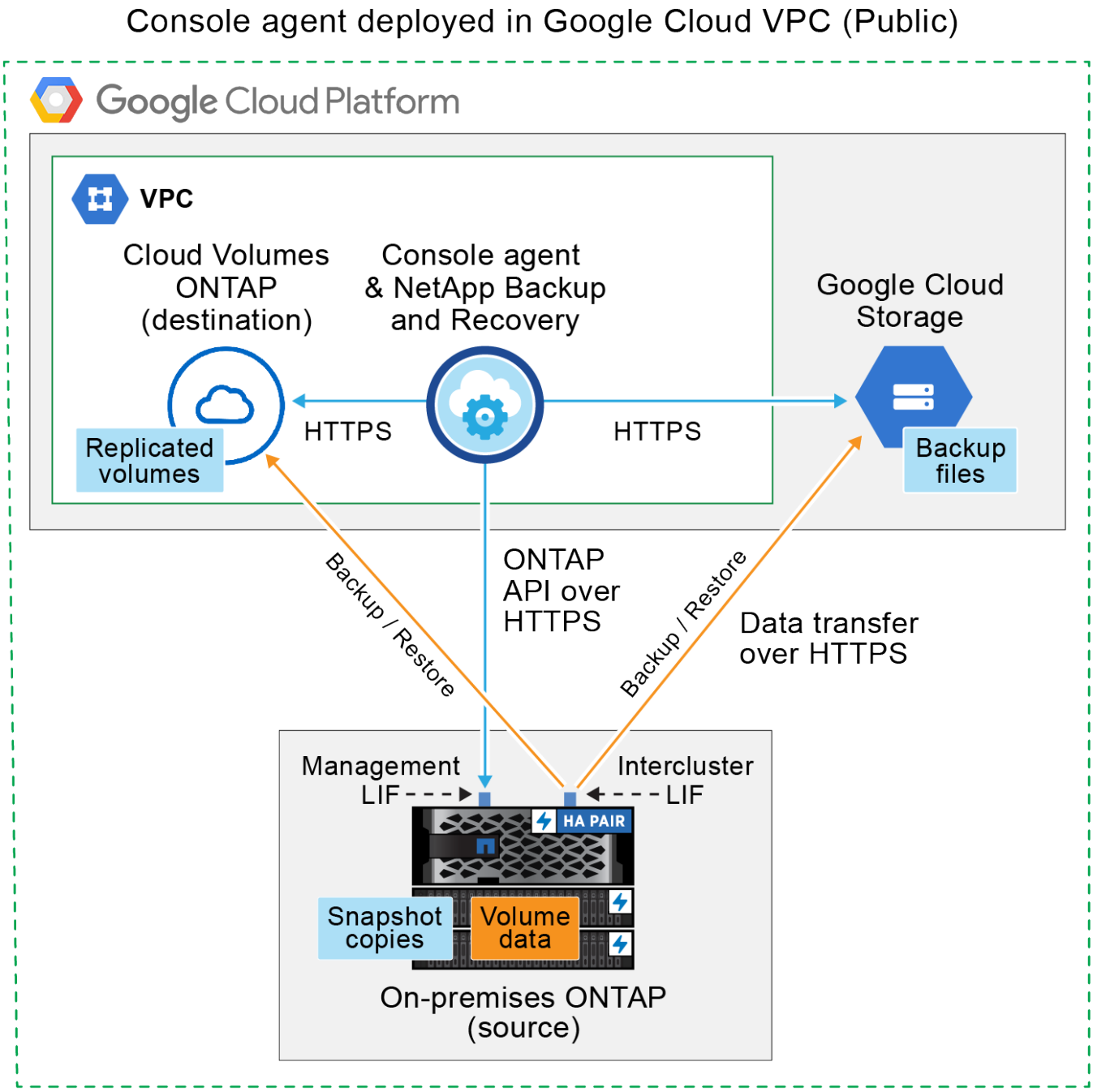
Identifizieren Sie die Verbindungsmethode

Wählen Sie aus, welche der beiden Verbindungsmethoden Sie beim Konfigurieren von Backups von lokalen ONTAP -Systemen zu Google Cloud Storage verwenden möchten.

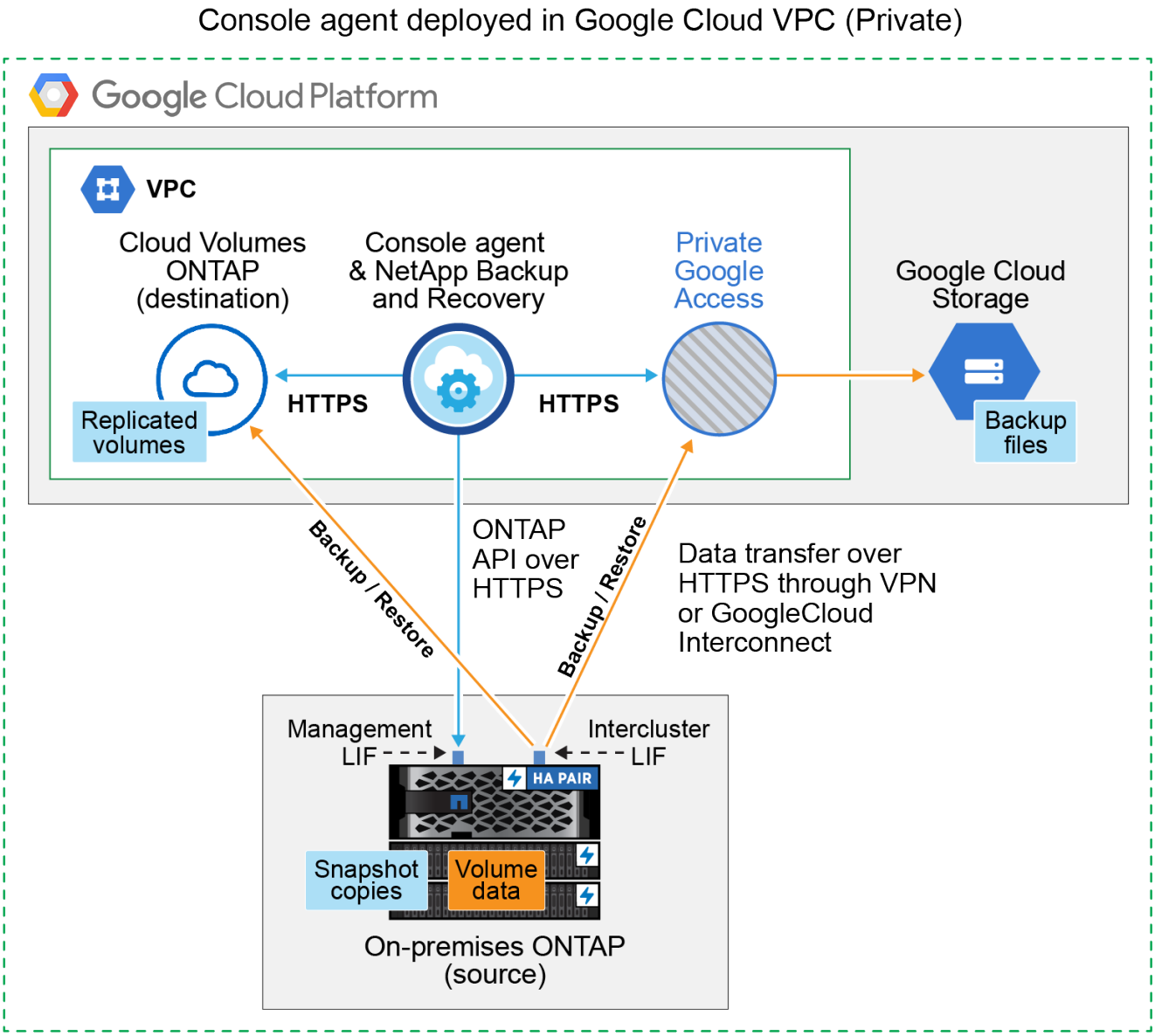
- **Öffentliche Verbindung** – Verbinden Sie das ONTAP -System über einen öffentlichen Google-Endpunkt direkt mit Google Cloud Storage.
- **Private Verbindung** – Verwenden Sie ein VPN oder Google Cloud Interconnect und leiten Sie den Datenverkehr über eine private Google Access-Schnittstelle, die eine 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.

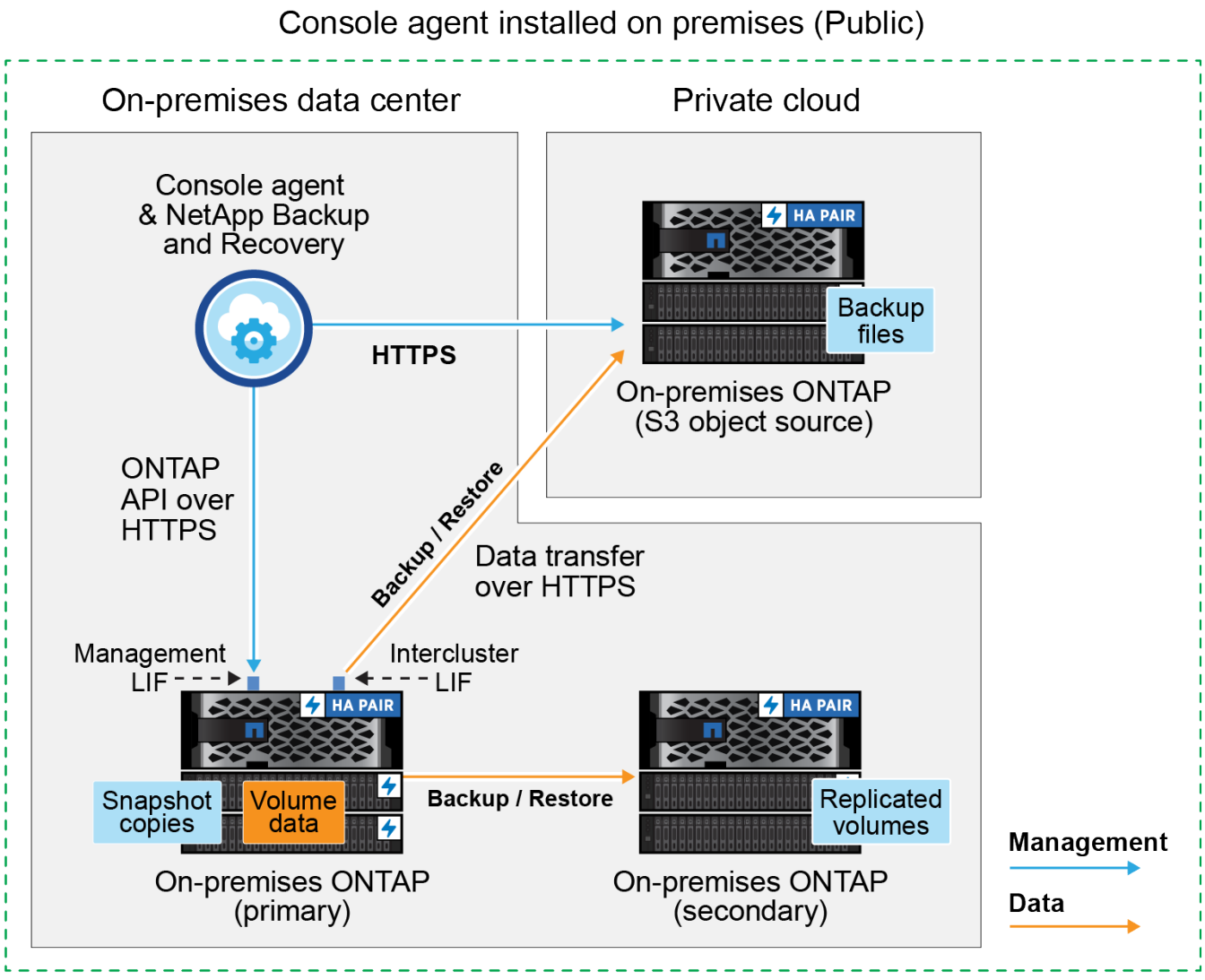
Das primäre lokale ONTAP -System kann ein FAS, AFF oder ONTAP Select System sein. Das sekundäre ONTAP -System kann ein lokales ONTAP oder Cloud Volumes ONTAP System sein. Der Objektspeicher kann sich auf einem lokalen ONTAP -System oder einem Cloud Volumes ONTAP System befinden, auf dem Sie einen Simple 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

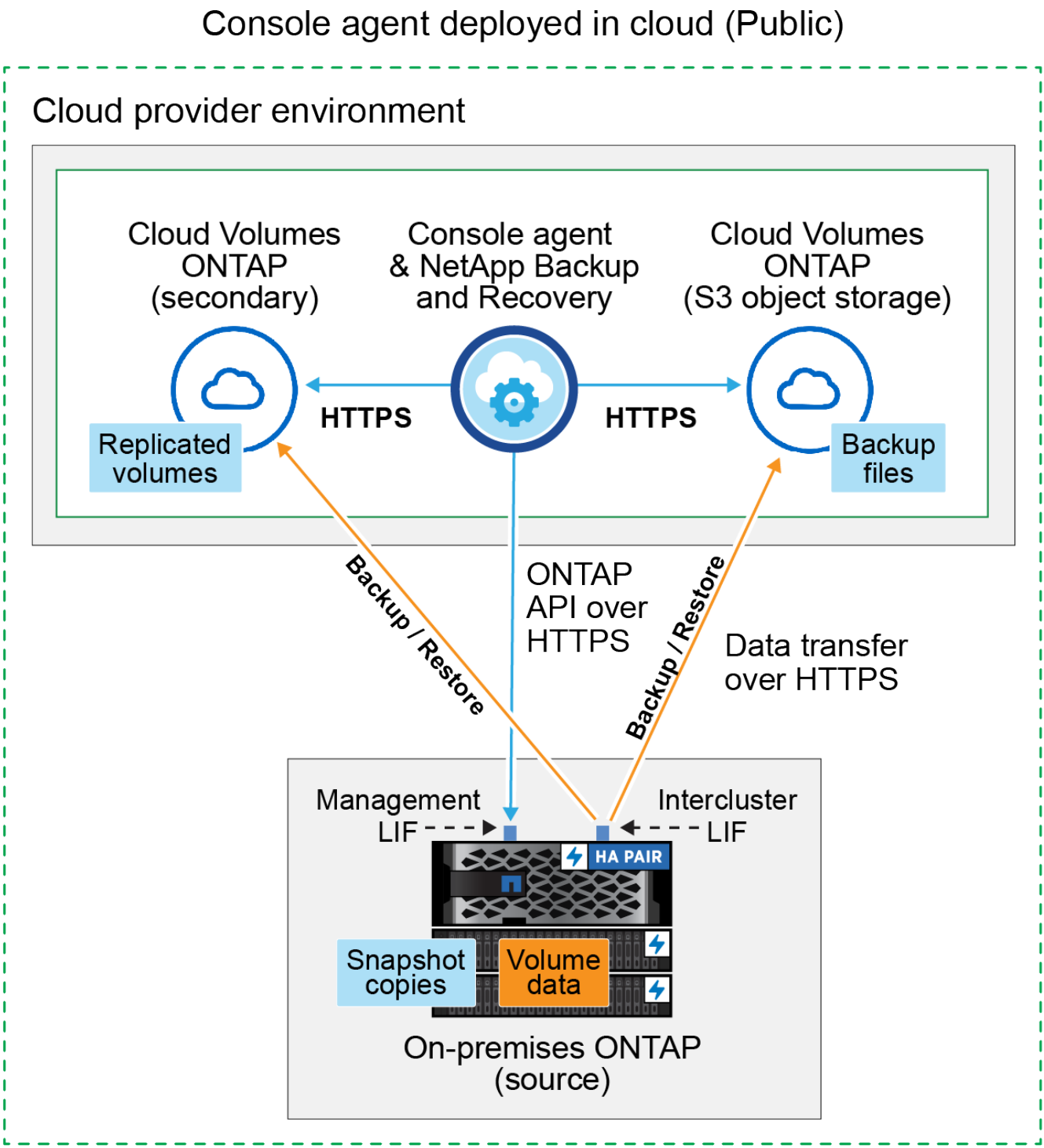
Es gibt viele Konfigurationen, in denen Sie Backups in einem S3-Bucket auf einem ONTAP System erstellen können. Nachfolgend werden zwei Szenarien dargestellt.

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.

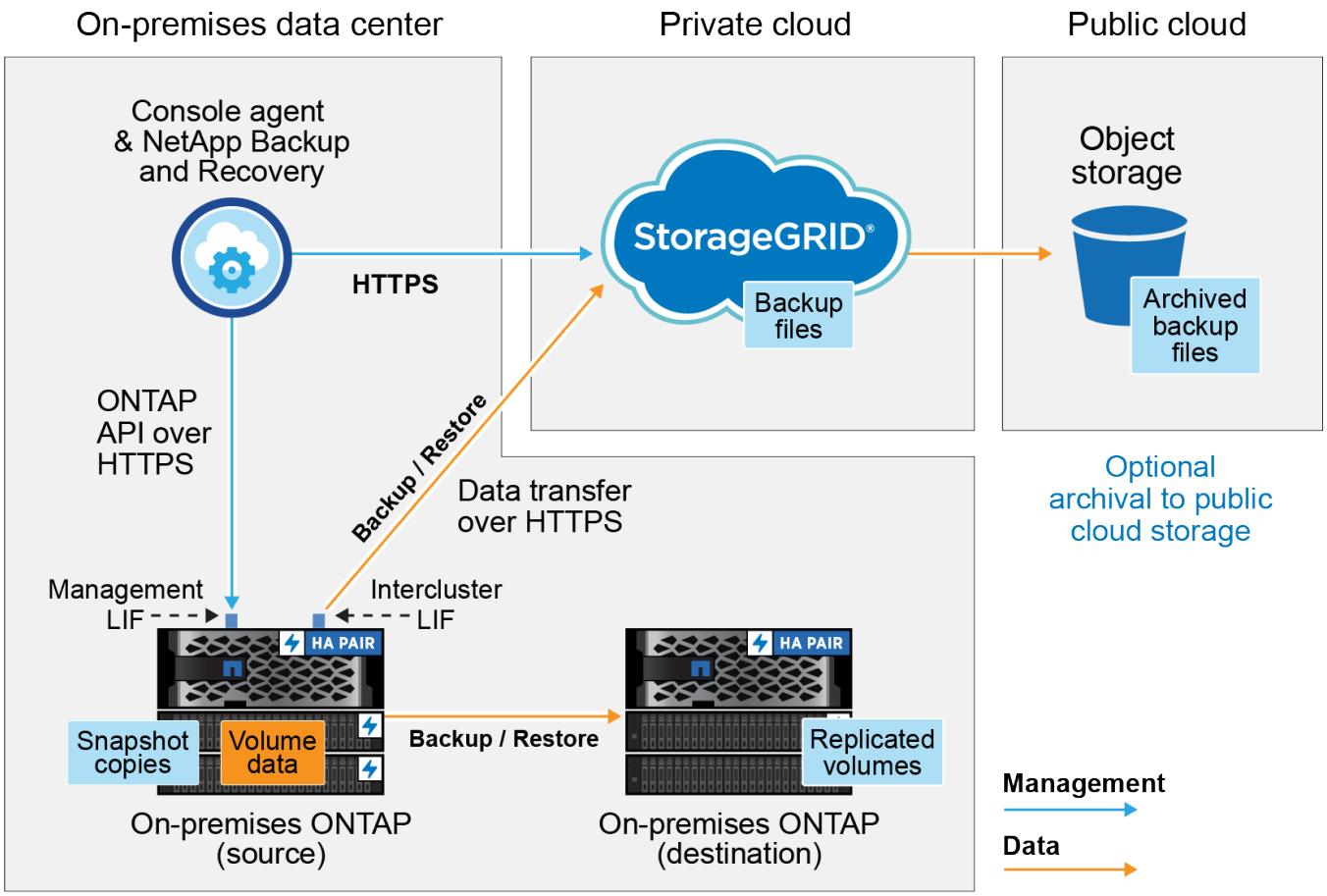
Zu den „On-Premises ONTAP -Systemen“ gehören FAS, AFF und ONTAP Select Systeme.

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" .

- 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

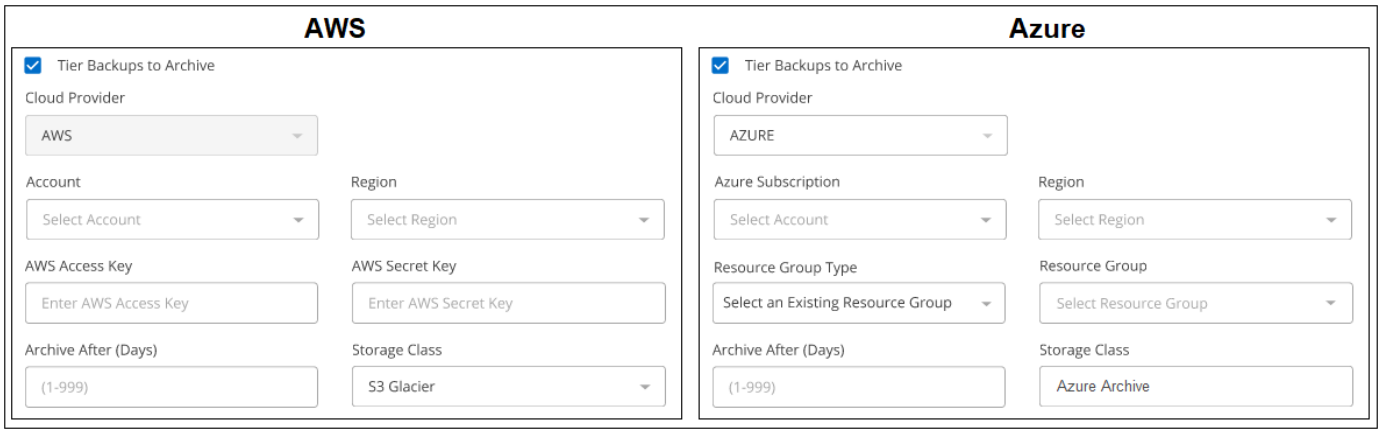
- Sie müssen sich für ein Amazon S3-Konto für den Speicherplatz anmelden, auf dem Ihre archivierten Backups gespeichert werden.
- Sie können wählen, ob Sie Backups auf AWS S3 Glacier oder S3 Glacier Deep Archive-Speicher stufen möchten. "Erfahren Sie mehr über AWS-Archivierungsebenen".
- StorageGRID 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.

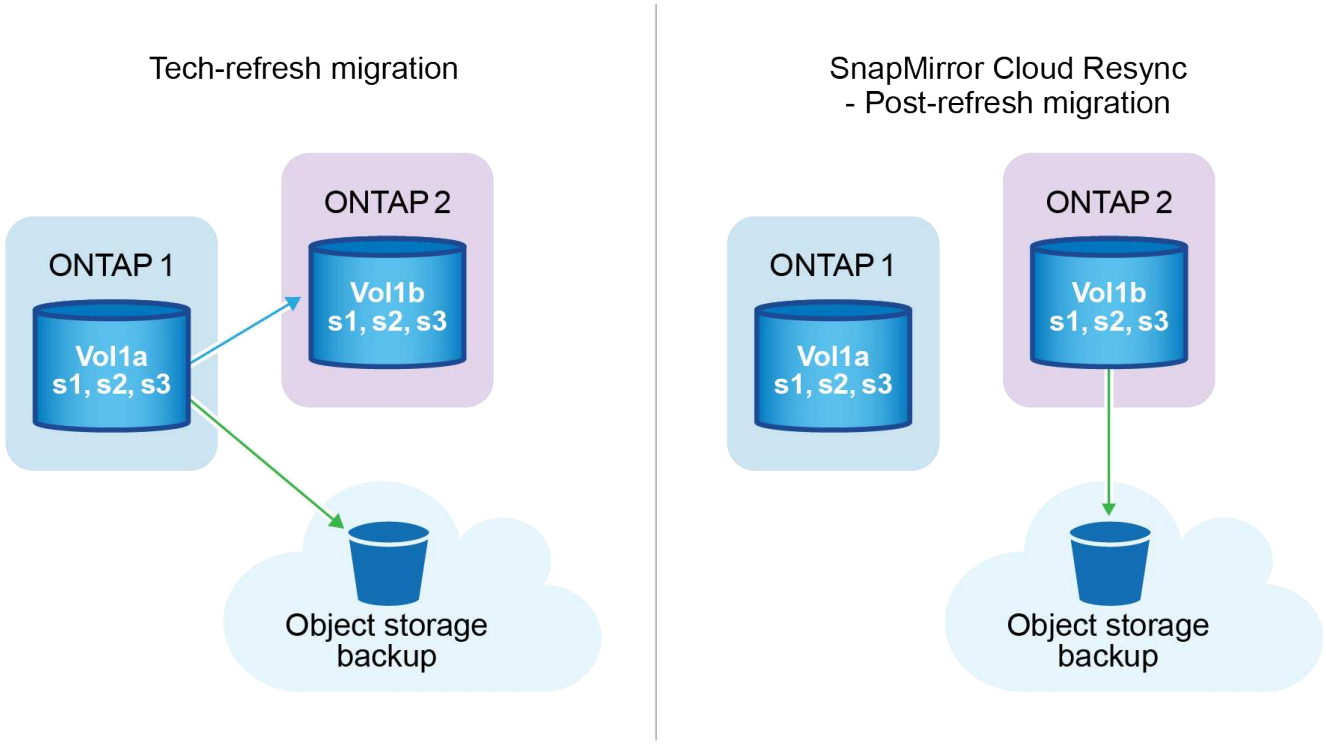
An diesem Punkt möchten Sie mit der Sicherung von Vol1b auf demselben Cloud-Endpunkt fortfahren. Aber anstatt eine vollständige Sicherung von Grund auf neu zu starten (was Zeit und Ressourcen kosten würde), verwenden Sie SnapMirror to Cloud Resync.

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.



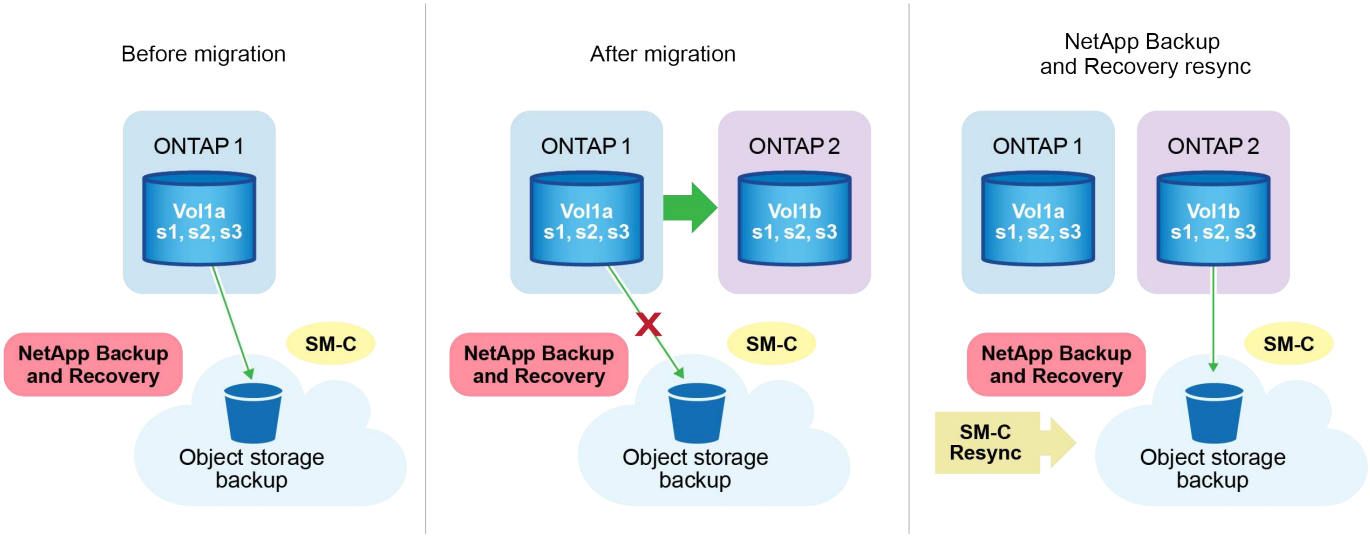
Verfahrenshinweise

- 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**
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.)

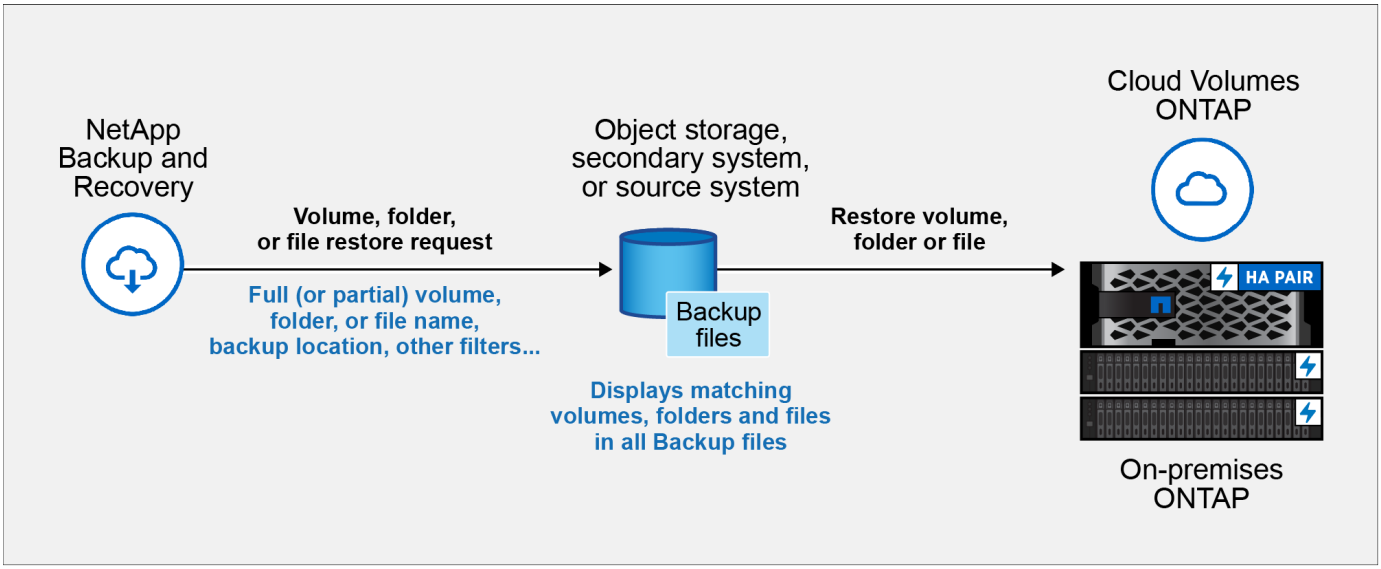
Auch wenn Sie einen lokalen Konsolen-Agenten verwenden, müssen die Anforderungen des Cloud-Anbieters sowohl für die Berechtigungen des Konsolen-Agenten als auch für die Ressourcen des Cloud-Anbieters erfüllt sein. Beachten Sie bei Verwendung dieser Implementierung die oben aufgeführten AWS- und Azure-Anforderungen.

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
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“

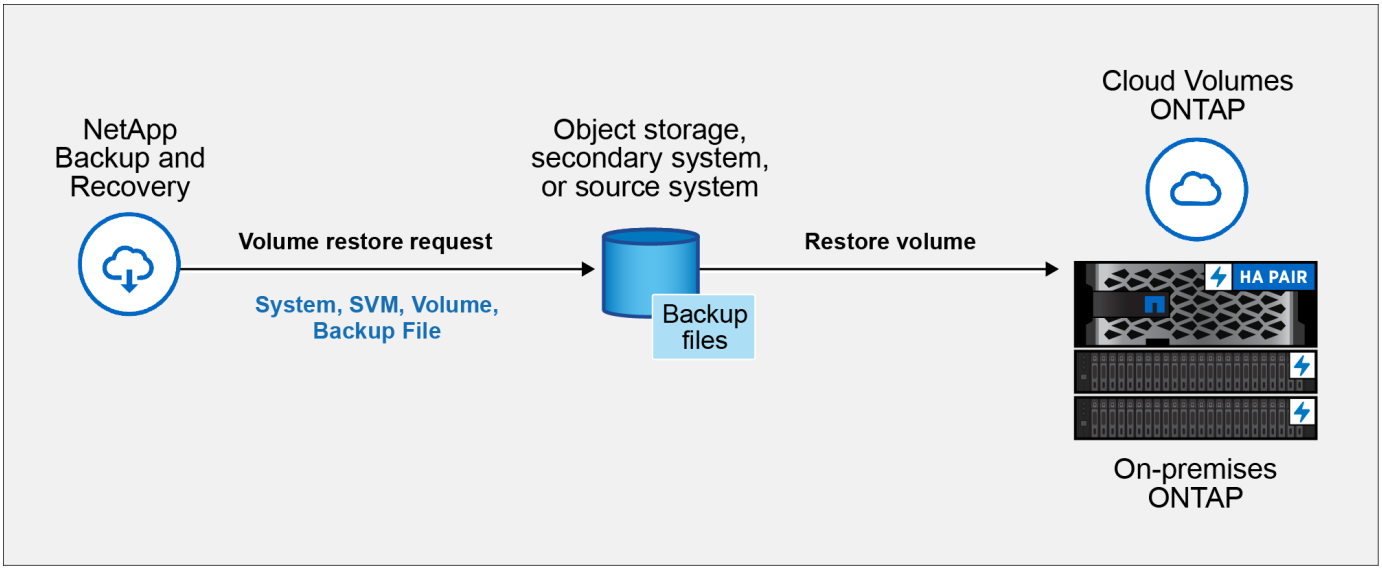
Wenn Sie ein Volume aus einer Sicherungsdatei wiederherstellen, erstellt NetApp Backup and Recovery mithilfe der Daten aus der Sicherung ein *neues* Volume. Wenn Sie ein Backup aus dem Objektspeicher verwenden, können Sie die Daten auf einem Volume im Originalsystem, auf einem anderen System, das sich 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.

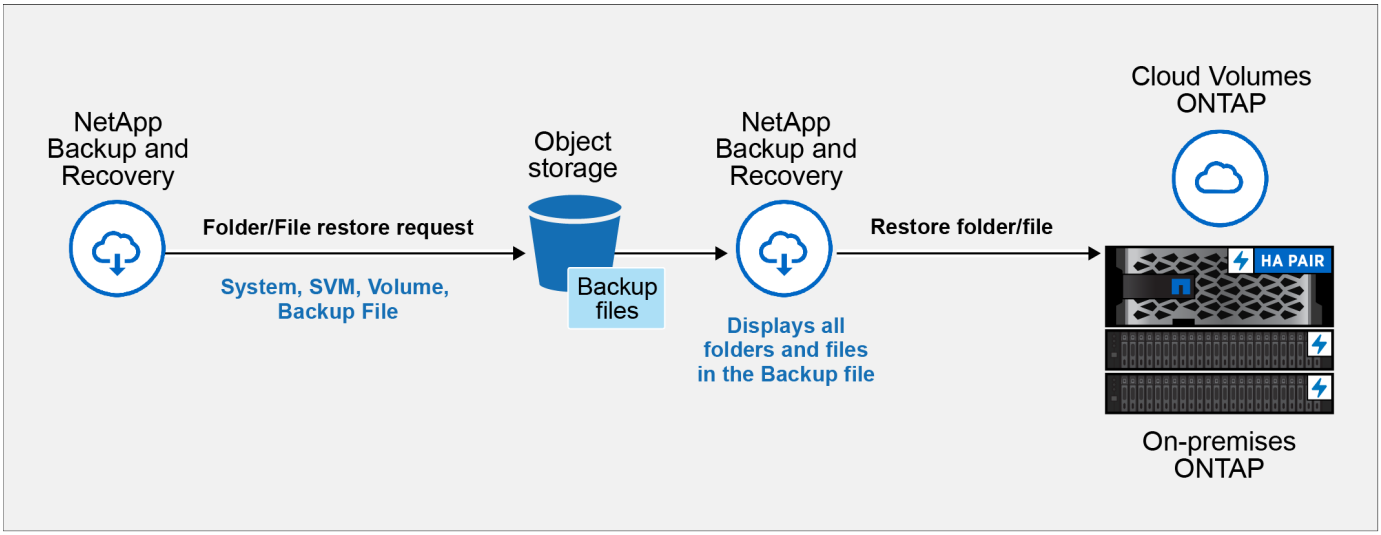
Wenn Sie mehrere Dateien auswählen, werden diese auf demselben Zielvolume wiederhergestellt. Um Dateien auf verschiedenen Datenträgern wiederherzustellen, führen Sie den Vorgang mehrmals aus.

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.