Backup und Restore von ONTAP Daten

Cloud Backup

NetApp
December 07, 2022

This PDF was generated from https://docs.netapp.com/de-de/cloud-manager-backup-restore/aws/concept-ontap-backup-to-cloud.html on December 07, 2022. Always check docs.netapp.com for the latest.

Inhaltsverzeichnis

Backup und Restore von ONTAP Daten . . . 1
ONTAP-Cluster-Daten mit Cloud Backup schützen . . . 1
Sichern von Cloud Volumes ONTAP-Daten in Amazon S3 . . . 9
Sichern von On-Premises-ONTAP-Daten in Amazon S3 . . . 18
Sichern von lokalen ONTAP Daten in StorageGRID . . . 32
Verwalten von Backups für Ihre ONTAP Systeme . . . 40
Verwalten von Backup-Einstellungen auf Cluster-Ebene . . . 60
Wiederherstellen von ONTAP Daten aus Backup-Dateien . . . 65

Backup und Restore von ONTAP Daten

ONTAP-Cluster-Daten mit Cloud Backup schützen

Cloud Backup bietet Backup- und Restore-Funktionen zum Schutz und zur langfristigen Archivierung Ihrer ONTAP Cluster-Daten. Backups werden automatisch erstellt und auf einem Objektspeicher Ihres Public- oder Private-Cloud-Kontos gespeichert. Dabei gibt es keine Volume Snapshot Kopien, die für die kurzfristige Wiederherstellung oder das Klonen verwendet werden.

Bei Bedarf können Sie ein ganzes *Volume*, einen *folder* oder eine oder mehrere *Files* von einem Backup in dieselbe oder andere Arbeitsumgebung wiederherstellen.

Funktionen

Backup-Funktionen:

- Erstellen Sie Backups unabhängiger Kopien Ihrer Datenvolumen auf kostengünstigem Objekt-Storage.
- Anwendung einer einzelnen Backup-Richtlinie auf alle Volumes in einem Cluster oder Zuweisen verschiedener Backup-Richtlinien zu Volumes mit eindeutigen Recovery-Punkten
- Erstellen Sie eine Backup-Richtlinie, die auf alle zukünftigen Volumes angewendet wird, die im Cluster erstellt wurden.
- Stellen Sie unveränderliche Backup-Dateien so vor, dass diese für den Aufbewahrungszeitraum gesperrt sind.
- Scannen Sie Backup-Dateien auf einen möglichen Ransomware-Angriff und entfernen/ersetzen Sie infizierte Backups automatisch.
- Tiering älterer Backup-Dateien auf Archiv-Storage, um Kosten zu sparen
- Löschen Sie die Backup-Beziehung, damit Sie nicht benötigte Quell-Volumes archivieren können, während Sie Volume-Backups beibehalten.
- Backup von der Cloud in die Cloud und von On-Premises-Systemen in die Public oder Private Cloud.
- Bei Cloud Volumes ONTAP Systemen befinden sich Backups auf einem anderen Abonnement/Konto oder einer anderen Region.
- Backup-Daten werden mit AES-256-Bit-Verschlüsselung im Ruhezustand und TLS 1.2 HTTPS-Verbindungen im Übertragungsprozess gesichert.
- Verwenden Sie Ihre eigenen, vom Kunden gemanagten Schlüssel für die Datenverschlüsselung, statt die Standard-Verschlüsselungsschlüssel Ihres Cloud-Providers zu verwenden.
- Unterstützung für bis zu 4,000 Backups eines einzelnen Volumes.

Wiederherstellungsfunktionen:

- Wiederherstellung von Daten aus einem bestimmten Zeitpunkt
- Stellen Sie ein Volume, einen Ordner oder einzelne Dateien auf dem Quellsystem oder einem anderen System wieder her.
- Wiederherstellung von Daten in einer Arbeitsumgebung mit einem anderen Abonnement/Konto oder in einer anderen Region.

- Stellt Daten auf Blockebene wieder her, indem die Daten direkt an dem von Ihnen angegebenen Speicherort platziert werden, während gleichzeitig die ursprünglichen ACLs beibehalten werden.
- Durchsuchbare und durchsuchbare Dateikataloge zur Auswahl einzelner Ordner und Dateien für die Wiederherstellung einzelner Dateien.

Unterstützte ONTAP-Arbeitsumgebungen und Objekt-Storage-Provider

Cloud Backup ermöglicht Ihnen das Backup von ONTAP Volumes aus den folgenden Arbeitsumgebungen in Objekt-Storage bei folgenden Public- und Private-Cloud-Providern:

Quelle Arbeitsumgebung	Ziel der Backup-Datei ifdef::aws[]
Cloud Volumes ONTAP in AWS	Amazon S3 endif::aws[] ifdef::Azure[]
Cloud Volumes ONTAP in Azure	Azure Blob endif::Azure[] ifdef::gcp[]
Cloud Volumes ONTAP in Google	Google Cloud Storage endif::gcp[]
Lokales ONTAP System	Ifdef::aws[] Amazon S3 endif::aws[] ifdef::azurAzure[] Azure Blob endif::Azure[] ifdef::gcp[] Google Cloud Storage endif::gcp[] NetApp StorageGRID

Sie können ein Volume, einen Ordner oder einzelne Dateien aus einer ONTAP-Sicherungsdatei in folgenden Arbeitsumgebungen wiederherstellen:

Speicherort Der Sicherungsdatei	Zielarbeitsumgebung ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP in AWS On-Premises ONTAP System endif::aws[] ifdef::azurAzure[]
Azure Blob	Cloud Volumes ONTAP in Azure On-Premises ONTAP System endif::Azure[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP in Google On-Premises ONTAP System endif::gcp[]
NetApp StorageGRID	Lokales ONTAP System

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

Unterstützung für Websites ohne Internetverbindung

Cloud Backup kann an einem Standort ohne Internetverbindung verwendet werden (auch als „offline“ oder „Dark“-Standort bekannt), um Volume-Daten von lokalen ONTAP Systemen auf lokalen NetApp StorageGRID Systemen zu sichern. In dieser Konfiguration werden auch die Volume- und Dateiwiederherstellung unterstützt. In diesem Fall müssen Sie den BlueXP Connector (mindestens Version 3.9.20) in der dunklen Site bereitstellen. Siehe "Sichern von lokalen ONTAP Daten in StorageGRID" Entsprechende Details.

Unterstützte Volumes

Cloud Backup unterstützt die folgenden Volume-Typen:

- FlexVol Volumes für Lese- und Schreibvorgänge
- SnapMirror Data Protection (DP) Ziel-Volumes

- SnapLock Enterprise Volumes (erfordert ONTAP 9.11.1 oder höher)
  - SnapLock-Compliance-Volumes werden derzeit nicht unterstützt.
- FlexGroup Volumes (erfordert ONTAP 9.12.1 oder höher)

> **FlexGroup-Einschränkungen**:
>
> - Die vollständige Volume-Wiederherstellung wird für ONTAP-Systeme vor Ort unterstützt; Cloud Volumes ONTAP-Systeme werden aktuell nicht unterstützt.
> - Wiederherstellung auf Dateiebene wird sowohl für lokale ONTAP- als auch für Cloud Volumes ONTAP-Systeme unterstützt.
> - Die Wiederherstellung von Verzeichnissen/Ordnern wird derzeit nicht unterstützt.
> - Backups können nicht in Archiv-Storage verschoben werden.
> - Backups können nicht DataLock- und Ransomware-Schutz nutzen.

Kosten

Bei der Nutzung von Cloud Backup mit ONTAP-Systemen fallen zwei Kostenarten an: Ressourcengebühren und Servicegebühren.

Ressourcengebühren

Ressourcengebühren werden beim Cloud-Provider für Objekt-Storage-Kapazität sowie für das Schreiben und Lesen von Backup-Dateien in die Cloud gezahlt.

- Für Backup bezahlen Sie Ihren Cloud-Provider für Objekt-Storage-Kosten.

  Da Cloud Backup die Storage-Effizienzfunktionen des Quell-Volume beibehalten, bezahlen Sie die Objekt-Storage-Kosten des Cloud-Providers für die Daten *nach* ONTAP-Effizienz (für die geringere Datenmenge, die nach der Deduplizierung und Komprimierung angewendet wurde).

- Beim Wiederherstellen von Daten mithilfe von Suchen und Wiederherstellen werden bestimmte Ressourcen vom Cloud-Provider bereitgestellt. Die Datenmenge, die von Ihren Suchanfragen gescannt wird, kostet pro tib. (Diese Ressourcen sind für Durchsuchen und Wiederherstellen nicht erforderlich.)
  - In AWS, "Amazon Athena" Und "AWS Klue" Ressourcen werden in einem neuen S3-Bucket implementiert.
- Falls Sie Volume-Daten aus einer Backup-Datei wiederherstellen müssen, die in den Archiv-Storage verschoben wurde, erhalten Sie eine zusätzliche Gebühr für den pro gib-Abruf und die Gebühr pro Anfrage vom Cloud-Provider.

Servicegebühren

Servicegebühren werden an NetApp gezahlt und decken sowohl die Kosten für die Erstellung „_ Backups“ und „ *Wiederherstellung* Volumes oder Dateien“ aus diesen Backups ab. Sie bezahlen nur für die Daten, die Sie sichern, berechnet anhand der verwendeten logischen Quellkapazität (*before* ONTAP-Effizienzfunktionen) der ONTAP Volumes, die in Objekt-Storage gesichert werden. Diese Kapazität wird auch als Front-End Terabyte (FETB) bezeichnet.

Es gibt drei Möglichkeiten, für den Backup-Service zu bezahlen. Als erste Option können Sie Ihren Cloud-Provider abonnieren, sodass Sie monatlich bezahlen können. Die zweite Möglichkeit besteht darin, einen Jahresvertrag zu erhalten. Als dritte Option können Lizenzen direkt von NetApp erworben werden. Lesen Sie die Lizenzierung Weitere Informationen finden Sie in diesem Abschnitt.

Lizenzierung

Cloud Backup ist mit den folgenden Nutzungsmodellen verfügbar:

- **BYOL**: Eine von NetApp erworbene Lizenz, die zusammen mit jedem Cloud-Provider verwendet werden kann.
- **PAYGO**: Ein stündliches Abonnement vom Markt Ihres Cloud-Providers.
- **Jahr**: Ein Jahresvertrag über den Markt Ihres Cloud-Providers.

> Wenn Sie eine BYOL-Lizenz von NetApp erwerben, müssen Sie auch das PAYGO-Angebot über den Markt Ihres Cloud-Providers abonnieren. Ihre Lizenz wird immer zuerst berechnet, aber Sie werden vom Stundensatz auf dem Markt in diesen Fällen berechnet:
>
> - Wenn Sie Ihre lizenzierte Kapazität überschreiten
> - Wenn die Laufzeit Ihrer Lizenz abläuft
>
> Wenn Sie über einen Jahresvertrag eines Marktes verfügen, wird der gesamte Cloud Backup-Verbrauch über diesen Vertrag abgerechnet. Man kann einen jährlichen Marktplatzvertrag nicht mit einem Byol kombinieren.

Mit Ihrer eigenen Lizenz

Byol ist nach Terminus basiert (12, 24 oder 36 Monate) *und* kapazitätsbasiert in Schritten von 1 tib. Sie bezahlen NetApp für einen Zeitraum, sagen wir 1 Jahr und für eine maximale Kapazität, sagen wir 10 tib.

Sie erhalten eine Seriennummer, die Sie auf der Seite BlueXP Digital Wallet eingeben, um den Dienst zu aktivieren. Wenn eine der beiden Limits erreicht ist, müssen Sie die Lizenz erneuern. Die BYOL-Lizenz für Backup gilt für alle mit dem verbundenen Quellsysteme "BlueXP-Konto".

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

Pay-as-you-go-Abonnement

Cloud Backup bietet eine nutzungsbasierte Lizenzierung in einem Pay-as-you-go-Modell. Nachdem Sie sich über den Marktplatz Ihres Cloud-Providers registriert haben, zahlen Sie pro gib für gesicherte Daten – there keine Vorauszahlung. Die Abrechnung erfolgt von Ihrem Cloud-Provider über Ihre monatliche Abrechnung.

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

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

Jahresvertrag

Bei Nutzung von AWS stehen zwei Jahresverträge für 12, 24 oder 36 Monate zur Verfügung:

- Ein Plan für „Cloud Backup“, mit dem Sie Backups von Cloud Volumes ONTAP Daten und ONTAP Daten vor Ort erstellen können
- Ein „CVO Professional“-Plan, mit dem Sie Cloud Volumes ONTAP und Cloud-Backup bündeln können. Dazu zählen unbegrenzte Backups für Cloud Volumes ONTAP Volumes, die gegen diese Lizenz verrechnet werden (die Backup-Kapazität wird nicht von der Lizenz angerechnet).

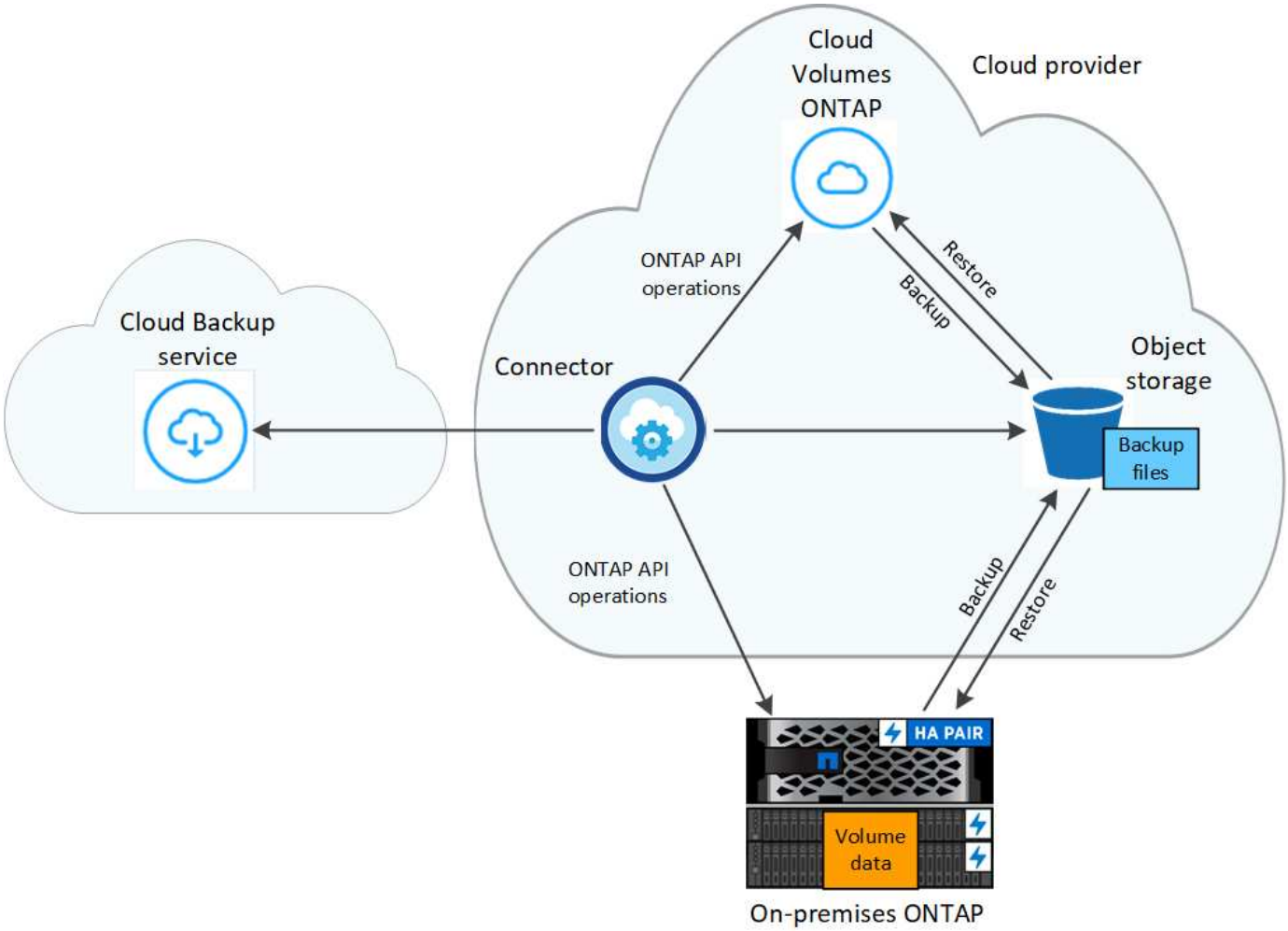
"Hier erfahren Sie, wie Sie Jahresverträge einrichten können".

Funktionsweise von Cloud Backup

Wenn Sie Cloud-Backups auf einem Cloud Volumes ONTAP- oder lokalen ONTAP-System aktivieren, führt der Service ein vollständiges Backup Ihrer Daten durch. Volume Snapshots werden nicht im Backup-Image berücksichtigt. Nach dem ersten Backup sind alle weiteren Backups inkrementell, das heißt, dass nur geänderte Blöcke und neue Blöcke gesichert werden. Dadurch wird der Netzwerkverkehr auf ein Minimum reduziert. Cloud Backup baut auf dem Fundament auf "NetApp SnapMirror Cloud Technologie".

> Alle Aktionen, die direkt aus Ihrer Cloud-Provider-Umgebung zum Verwalten oder Ändern von Backup-Dateien übernommen werden, können die Dateien beschädigen und führen zu einer nicht unterstützten Konfiguration.

Die folgende Abbildung zeigt die Beziehung zwischen den einzelnen Komponenten:



Speicherort von Backups

Backup-Kopien werden in einem Objektspeicher gespeichert, den BlueXP in Ihrem Cloud-Konto erstellt. Pro Cluster und Arbeitsumgebung gibt es einen Objektspeicher, und BlueXP benennt den Objektspeicher wie folgt: „netapp-Backup-clusterUUID“. Stellen Sie sicher, dass Sie diesen Objektspeicher nicht löschen.

- In AWS ermöglicht BlueXP das "Amazon S3 Block – Public Access-Funktion" Auf dem S3-Bucket.
- In StorageGRID verwendet BlueXP ein vorhandenes Storage-Konto für den Objektspeicher-Bucket.

Wenn Sie künftig den Zielobjektspeicher für ein Cluster ändern möchten, müssen Sie unbedingt fortfahren "Heben Sie die Registrierung für Cloud Backup für die Arbeitsumgebung auf", Und aktivieren Sie dann Cloud Backup mit den neuen Cloud-Provider-Informationen.

Anpassbare Backup-Planungs- und Aufbewahrungseinstellungen

Wenn Sie Cloud-Backup für eine Arbeitsumgebung aktivieren, werden alle Volumes, die Sie anfangs auswählen, mithilfe der definierten Standard-Backup-Richtlinie gesichert. Wenn Sie bestimmten Volumes mit unterschiedlichen Recovery-Zeitpunkten (Recovery Point Objectives, RPO) unterschiedliche Backup-Richtlinien zuweisen möchten, können Sie für diesen Cluster zusätzliche Richtlinien erstellen und diese Richtlinien den anderen Volumes zuweisen, nachdem Cloud Backup aktiviert ist.

Es steht eine Kombination aus stündlichen, täglichen, wöchentlichen, monatlichen und jährlichen Backups aller Volumes zur Verfügung. Sie haben außerdem die Wahl zwischen einer der systemdefinierten Richtlinien, die 3 Monate, 1 Jahr und 7 Jahre Backups und Aufbewahrung bieten. Im Folgenden werden die Richtlinien aufgeführt:

Name Der Backup-Richtlinie	**Backups pro Intervall…**			**Maximale Backups**
	* Daily*	**Wöchentlich**	**Monatlich**	
Netapp3MonatDatenhaltung	30	13	3	46
Netapp1YearRetention	30	13	12	55
Netapp7YearsRetention	30	53	84	167

Backup-Sicherungsrichtlinien, die Sie mit ONTAP System Manager oder der ONTAP CLI auf dem Cluster erstellt haben, werden ebenfalls als Auswahl angezeigt. Dies schließt Richtlinien ein, die mithilfe von benutzerdefinierten SnapMirror-Labels erstellt werden.

Sobald Sie die maximale Anzahl von Backups für eine Kategorie oder Intervall erreicht haben, werden ältere Backups entfernt, sodass Sie immer über die aktuellsten Backups verfügen (und veraltete Backups belegen somit nicht mehr Speicherplatz in der Cloud).

Siehe "Backup-Pläne" Weitere Informationen zu den verfügbaren Terminplanoptionen.

Beachten Sie, dass Sie können "Erstellung eines On-Demand-Backups eines Volumes" Über das Backup Dashboard können Sie jederzeit zusätzlich zu den Backup-Dateien zugreifen, die aus den geplanten Backups erstellt wurden.

> Die Aufbewahrungsdauer für Backups von Datensicherungs-Volumes ist identisch mit der in der SnapMirror Quell-Beziehung definierten Aufbewahrungsdauer. Sie können dies gegebenenfalls mithilfe der API ändern.

Sicherungseinstellungen für Dateien sichern

Wenn Ihr Cluster ONTAP 9.11.1 oder höher verwendet, können Sie Ihre Backups vor dem Löschen und Ransomware-Angriffen schützen. Jede Backup-Richtlinie enthält einen Abschnitt für *DataLock und Ransomware-Schutz*, der für einen bestimmten Zeitraum auf Ihre Backup-Dateien angewendet werden kann - die *Aufbewahrungsfrist*. *DataLock* schützt Ihre Sicherungsdateien vor Änderungen oder Löschung. *Ransomware Protection* scannt Ihre Backup-Dateien, um nach einem Ransomware-Angriff zu suchen, wenn eine Backup-Datei erstellt wird und wann die Daten aus einer Backup-Datei wiederhergestellt werden.

Die Backup-Aufbewahrungsdauer ist identisch mit der Aufbewahrungsfrist des Backup-Zeitplans plus 14 Tage. Beispielsweise werden bei *Weekly* Backups mit gespeicherten *5* Kopien jede Backup-Datei 5 Wochen lang

gesperrt. *Monatliche* Backups mit *6* Kopien zurückbehaltenen Kopien werden jede Backup-Datei 6 Monate lang gesperrt.

Wenn Ihr Backup-Ziel Amazon S3 oder NetApp StorageGRID ist, wird derzeit Unterstützung verfügbar. In zukünftigen Versionen werden weitere Ziele für Storage-Provider hinzugefügt.

Siehe "DataLock- und Ransomware-Schutz" Für weitere Informationen, wie DataLock und Ransomware-Schutz funktioniert.

DataLock kann nicht aktiviert werden, wenn Sie Backups in Archiv-Storage Tiering sind.

Archiv-Storage für ältere Backup-Dateien

Bei Nutzung eines bestimmten Cloud-Storage können Sie ältere Backup-Dateien nach einer bestimmten Anzahl von Tagen auf eine kostengünstigere Storage-Klasse bzw. Zugriffsebene verschieben. Beachten Sie, dass Archivspeicher nicht verwendet werden kann, wenn Sie DataLock aktiviert haben.

- In AWS beginnen Backups in der Klasse „ *Standard* Storage“ und wechseln nach 30 Tagen in die Storage-Klasse „ *Standard-infrequent Access*“.

  Wenn Ihr Cluster ONTAP 9.10.1 oder höher verwendet, können Sie ältere Backups nach einer bestimmten Anzahl von Tagen entweder auf *S3 Glacier oder _S3 Glacier Deep Archive* Storage in der Cloud Backup UI verschieben, um die Kosten weiter zu optimieren. "Weitere Informationen zu AWS Archiv-Storage".

- In StorageGRID sind Backups der Klasse *Standard* Storage zugeordnet.

Siehe "Einstellungen für Archiv-Storage" Weitere Informationen zur Archivierung älterer Backup-Dateien.

Überlegungen zu den Tiering-Richtlinien von FabricPool

Es gibt bestimmte Dinge, die Sie beachten müssen, wenn das Backup-Volume auf einem FabricPool Aggregat gespeichert ist und eine andere Richtlinie als zugewiesen ist `none`:

- Für das erste Backup eines FabricPool-Tiered Volumes müssen alle lokalen und alle Tiered Daten (aus dem Objektspeicher) gelesen werden. Ein Backup-Vorgang erhitzt nicht die kalten Daten im Objekt-Storage „wieder“.

  Das Lesen der Daten von Ihrem Cloud-Provider kann zu einem einmalig erhöhten Kostenaufwand führen.

  - Nachfolgende Backups sind inkrementell und haben diese Auswirkungen nicht.
  - Wenn die Tiering-Richtlinie dem Volume bei ihrer ersten Erstellung zugewiesen ist, wird dieses Problem nicht sehen.

- Berücksichtigen Sie die Auswirkungen von Backups, bevor Sie das zuweisen `all` tiering-Richtlinie zu Volumes. Da die Daten sofort in Tiered Storage verschoben werden, liest Cloud Backup Daten eher aus der Cloud-Tier als aus der lokalen Tier. Da parallele Backup-Vorgänge die Netzwerkverbindung zum Cloud-Objektspeicher teilen, kann es zu Performance-Einbußen kommen, wenn die Netzwerkressourcen gesättigt werden. In diesem Fall möchten Sie möglicherweise proaktiv mehrere Netzwerkschnittstellen (LIFs) konfigurieren, um diese Art der Netzwerksättigung zu reduzieren.

Backup-Einschränkungen

- Um ältere Backup-Dateien per Tiering in Archiv-Storage zu verschieben, muss der Cluster ONTAP 9.10.1 oder höher ausführen. Für die Wiederherstellung von Volumes aus Backup-Dateien, die sich im Archiv-

Storage befinden, muss im Ziel-Cluster zudem ONTAP 9.10.1+ ausgeführt werden.

- Wenn eine Backup-Richtlinie erstellt oder bearbeitet wird, wenn dieser Richtlinie keine Volumes zugewiesen werden, kann die Anzahl der zurückbehaltenen Backups maximal 1018 sein. Als Workaround können Sie die Anzahl der Backups zur Erstellung der Richtlinie verringern. Anschließend können Sie die Richtlinie bearbeiten, um bis zu 4000 Backups zu erstellen, nachdem Sie der Richtlinie Volumes zugewiesen haben.
- Bei der Sicherung von Datensicherungs-Volumes (DP):
  - Beziehungen zu den SnapMirror-Labels `app_consistent` Und `all_source_snapshot` Wird nicht in der Cloud gesichert werden.
  - Wenn Sie lokale Kopien der Snapshots auf dem SnapMirror Ziel-Volume erstellen (unabhängig von den verwendeten SnapMirror Bezeichnungen), werden diese Snapshots nicht als Backups in die Cloud verschoben. Zu diesem Zeitpunkt müssen Sie eine Snapshot-Richtlinie mit den gewünschten Labels auf dem Quell-DP-Volume erstellen, um Cloud Backup zu sichern.
- SVM-DR-Volume-Backup wird unter den folgenden Einschränkungen unterstützt:
  - Backups werden nur von der sekundären ONTAP unterstützt.
  - Die auf das Volume angewandte Snapshot Richtlinie muss eine der vom Cloud Backup anerkannten Richtlinien sein, einschließlich täglich, wöchentlich, monatlich usw. die standardmäßige „SM_created“ Richtlinie (wird für **Spiegelung aller Snapshots** verwendet) Das DP-Volume wird nicht erkannt und in der Liste der Volumes, die gesichert werden können, nicht angezeigt.
- Das MetroCluster (MCC) Backup wird nur von ONTAP sekundär unterstützt: MCC > SnapMirror > ONTAP > Cloud Backup > Objekt-Storage.
- Ad-hoc-Volume-Backup mit der **Backup Now**-Taste wird auf Datensicherungs-Volumes nicht unterstützt.
- SM-BC-Konfigurationen werden nicht unterstützt.
- ONTAP unterstützt keine Fan-out-of-SnapMirror-Beziehungen von einem einzelnen Volume zu mehreren Objektspeicher. Daher wird diese Konfiguration nicht von Cloud Backup unterstützt.
- WORM-/Compliance-Modus auf einem Objektspeicher wird derzeit nur von Amazon S3 und StorageGRID unterstützt. Dies wird als DataLock-Funktion bezeichnet und muss mit Cloud Backup-Einstellungen verwaltet werden.

Einschränkungen bei der Datei- und Ordnerwiederherstellung

Diese Einschränkungen gelten sowohl für die Such- und Wiederherstellungsmethoden als auch für die Such- und Wiederherstellungsmethoden für die Wiederherstellung von Dateien und Ordnern, sofern nicht ausdrücklich genannt.

- Browse & Restore kann bis zu 100 einzelne Dateien gleichzeitig wiederherstellen.
- Search & Restore kann 1 Datei gleichzeitig wiederherstellen.
- Suchen und Wiederherstellen und Suchen und Wiederherstellen können 1 Ordner gleichzeitig wiederherstellen.
- Die Wiederherstellung von FlexGroup Volumes auf FlexVol Volumes oder FlexVol Volumes auf FlexGroup Volumes wird nicht unterstützt.
- Wiederherstellung auf Dateiebene wird nicht unterstützt, wenn Sie dasselbe Konto mit verschiedenen BlueXP-Systemen in unterschiedlichen Subnetzen verwenden.
- Wiederherstellung auf Dateiebene mithilfe von Suchen & Wiederherstellen wird nicht unterstützt, wenn der Connector auf einer Website ohne Internetzugang installiert wird (dunkle Seite).
- Sie können einzelne Ordner nicht wiederherstellen, wenn sich die Sicherungsdatei im Archiv-Speicher

befindet.

- Die wiederherzustellende Datei muss die gleiche Sprache verwenden wie die Sprache auf dem Zielvolume. Wenn die Sprachen nicht identisch sind, wird eine Fehlermeldung angezeigt.

Sichern von Cloud Volumes ONTAP-Daten in Amazon S3

Führen Sie einige Schritte aus, um mit dem Backup von Daten von Cloud Volumes ONTAP in Amazon S3 zu beginnen.

Schnellstart

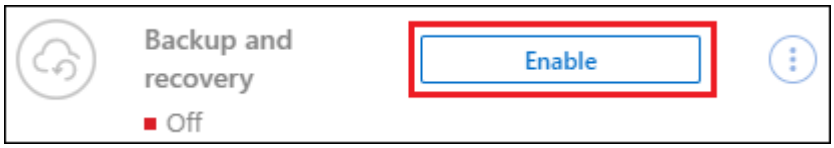
Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

1 Überprüfen Sie die Unterstützung Ihrer Konfiguration

- Sie nutzen Cloud Volumes ONTAP 9.7P5 oder höher in AWS.
- Sie verfügen über ein gültiges Cloud-Provider-Abonnement für den Speicherplatz, auf dem sich Ihre Backups befinden.
- Sie haben sich für das angemeldet "BlueXP Marketplace Backup-Angebot", An "AWS Jahresvertrag", Oder Sie haben gekauft "Und aktiviert" Eine Cloud Backup BYOL-Lizenz von NetApp
- Die IAM-Rolle, die den BlueXP Connector mit Berechtigungen bereitstellt, umfasst die neuesten S3-Berechtigungen "BlueXP-Richtlinie".

2 Cloud Backup auf Ihrem neuen oder vorhandenen System aktivieren

- Neue Systeme: Cloud Backup ist standardmäßig im Assistenten für die Arbeitsumgebung aktiviert. Achten Sie darauf, dass die Option aktiviert bleibt.
- Bestehende Systeme: Wählen Sie die Arbeitsumgebung aus und klicken Sie auf **Aktivieren** neben dem Backup- und Recovery-Dienst im rechten Fenster, und folgen Sie dann dem Setup-Assistenten.



3 Geben Sie die Anbieterdetails ein

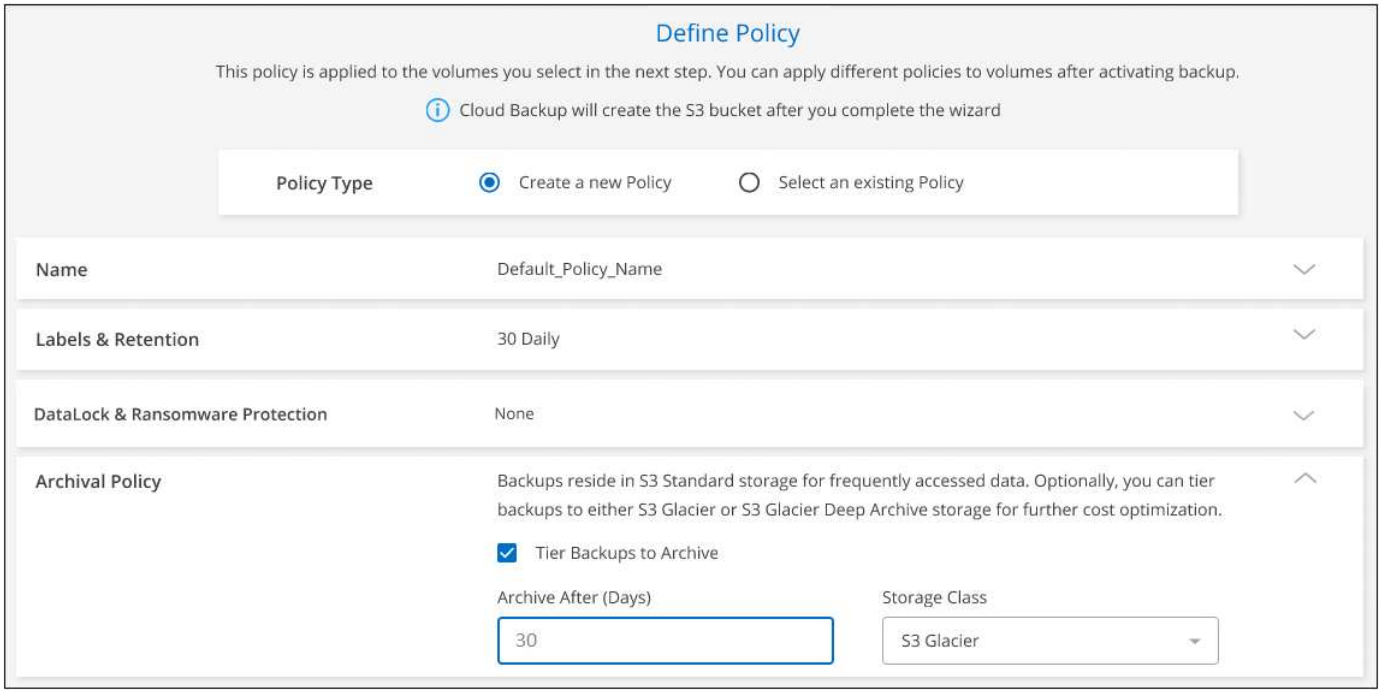
Wählen Sie das AWS Konto und die Region aus, in der die Backups erstellt werden sollen. Anstelle der standardmäßigen Amazon S3-Verschlüsselung haben Sie auch die Möglichkeit, Ihren eigenen vom Kunden gemanagten Schlüssel für die Datenverschlüsselung auszuwählen.

4 **Legen Sie die standardmäßige Backup-Richtlinie fest**

Die Standardrichtlinie sichert Volumes täglich und speichert die letzten 30 Backup-Kopien jedes Volumes. Änderung zu stündlichen, täglichen, wöchentlichen, monatlichen oder jährlichen Backups Oder wählen Sie eine der systemdefinierten Richtlinien aus, die mehr Optionen bieten. Sie können auch die Anzahl der zu behaltenden Backup-Kopien ändern.

Backups werden standardmäßig in S3 Standard-Storage gespeichert. Wenn in Ihrem Cluster ONTAP 9.10.1 oder neuer verwendet wird, können Sie Backups nach einer bestimmten Anzahl von Tagen entweder auf S3 Glacier oder in S3 Glacier Deep Archive Storage abstufen, um die Kosten weiter zu optimieren.

Optional können Sie bei Verwendung von ONTAP 9.11.1 und höher Ihre Backups vor dem Löschen und Ransomware-Angriffen schützen, indem Sie eine der Einstellungen *DataLock und Ransomware Protection* konfigurieren. "Weitere Informationen über die verfügbaren Konfigurationseinstellungen für Cloud Backup-Richtlinien".



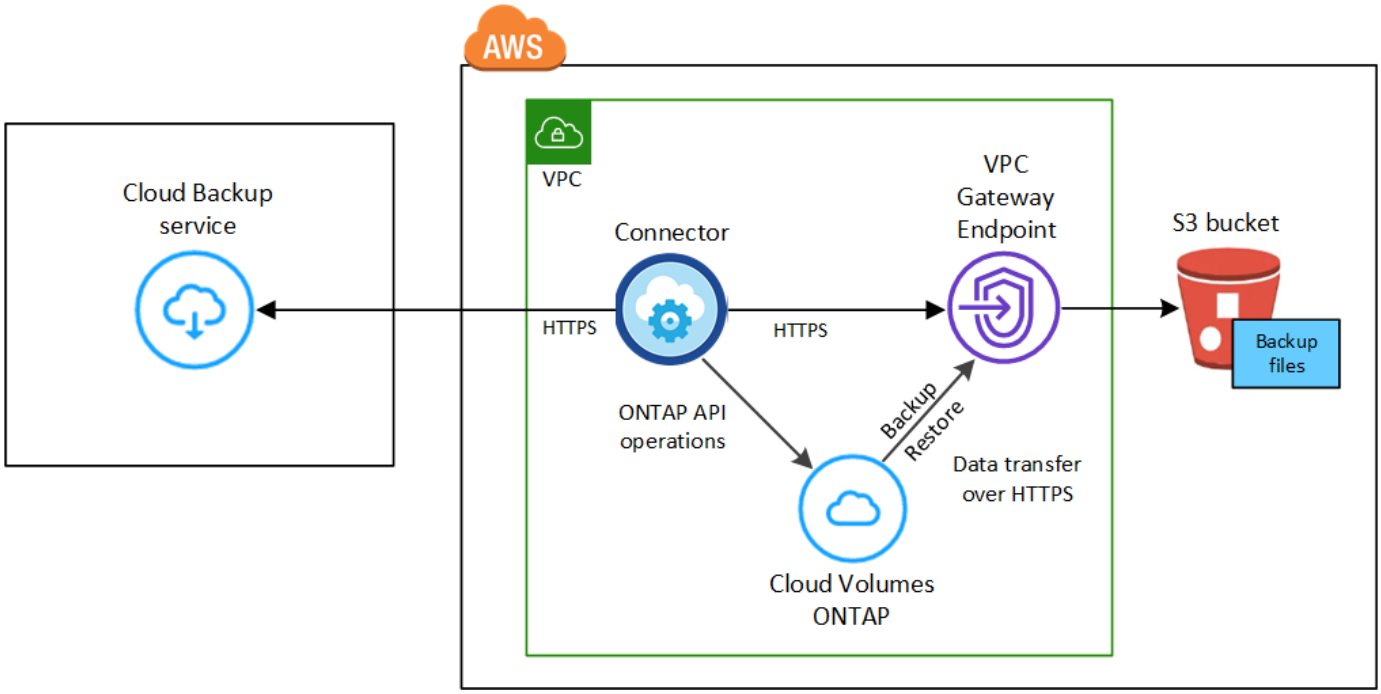
5 **Wählen Sie die Volumes aus, die Sie sichern möchten**

Legen Sie auf der Seite Volumes auswählen fest, welche Volumes gesichert werden sollen. Verwenden Sie dazu die Standard-Backup-Richtlinie. Um bestimmten Volumes unterschiedliche Backup-Richtlinien zuzuweisen, können Sie weitere Richtlinien erstellen und diese später auf Volumes anwenden.

Anforderungen

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie mit dem Backup von Volumes in S3 beginnen.

Die folgende Abbildung zeigt die einzelnen Komponenten und die Verbindungen, die zwischen den Komponenten vorbereitet werden müssen:



Der VPC-Gateway-Endpunkt muss bereits in der VPC vorhanden sein.

Unterstützte ONTAP-Versionen

Minimum ONTAP 9.7P5; ONTAP 9.8P13 und höher wird empfohlen.

Lizenzanforderungen

Für Cloud Backup PAYGO-Lizenzen ist im AWS Marketplace ein BlueXP-Abonnement verfügbar, das die Implementierung von Cloud Volumes ONTAP und Cloud Backup ermöglicht. Sie müssen "Melden Sie sich für dieses BlueXP-Abonnement an" Vor Aktivierung von Cloud Backup: Die Abrechnung für Cloud Backup erfolgt über dieses Abonnement.

Bei einem Jahresvertrag, mit dem Sie sowohl Cloud Volumes ONTAP Daten als auch ONTAP Daten vor Ort sichern können, müssen Sie den Abonnement von abonnieren "AWS Marketplace Seite" Und dann "Verbinden Sie das Abonnement mit Ihren AWS Zugangsdaten".

Für einen Jahresvertrag, mit dem Sie Cloud Volumes ONTAP und Cloud Backup bündeln können, müssen Sie bei der Erstellung einer Cloud Volumes ONTAP Arbeitsumgebung den Jahresvertrag abschließen. Mit dieser Option können Sie Backups von Daten vor Ort nicht erstellen.

Für die BYOL-Lizenzierung von Cloud Backup benötigen Sie die Seriennummer von NetApp, mit der Sie den Service für die Dauer und die Kapazität der Lizenz nutzen können. "Erfahren Sie, wie Sie Ihre BYOL-Lizenzen managen".

Zudem benötigen Sie ein AWS-Konto für den Speicherplatz, auf dem sich Ihre Backups befinden.

Unterstützte AWS-Regionen

Cloud Backup wird in allen AWS Regionen unterstützt "Wobei Cloud Volumes ONTAP unterstützt wird"; Einschließlich Regionen von AWS GovCloud.

Einrichtung zur Erstellung von Backups in einem anderen AWS Konto erforderlich

Standardmäßig werden Backups mit demselben Konto erstellt wie für das Cloud Volumes ONTAP-System. Falls Sie ein anderes AWS Konto für Ihre Backups verwenden möchten, müssen Sie folgende Anforderungen erfüllen:

- Fügen Sie die Anmeldeinformationen für das AWS Zielkonto in BlueXP hinzu. "So geht's".
- Fügen Sie die Berechtigungen „s3:PutBucketPolicy“ und „s3:PutBucketEigentümership Controls“ zur IAM-Rolle hinzu, die dem BlueXP Connector Berechtigungen erteilt.

Erforderliche Informationen zur Nutzung von vom Kunden gemanagten Schlüsseln für die Datenverschlüsselung

Im Aktivierungsassistenten können Sie Ihre eigenen, von Kunden gemanagten Schlüssel für die Datenverschlüsselung auswählen und nicht die standardmäßigen Amazon S3-Verschlüsselungsschlüssel verwenden. In diesem Fall müssen Sie bereits die über die Verschlüsselung gemanagten Schlüssel eingerichtet haben. "Sehen Sie, wie Sie Ihre eigenen Schlüssel verwenden".

Erforderliche AWS Connector Berechtigungen

Die IAM-Rolle, die BlueXP Berechtigungen bereitstellt, muss die neuesten S3-Berechtigungen enthalten "BlueXP-Richtlinie".

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:ListBucketByTags",
                "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 den Connector mit Version 3.9.21 oder höher bereitgestellt haben, sollten diese Berechtigungen bereits Teil der IAM-Rolle sein. Andernfalls müssen Sie die fehlenden Berechtigungen hinzufügen. Insbesondere die "athena" und "Leim" Berechtigungen, wie sie für die Suche und Wiederherstellung erforderlich sind.

Erforderliche AWS Cloud Volumes ONTAP Berechtigungen

Wenn auf Ihrem Cloud Volumes ONTAP System ONTAP 9.12.1 oder höher ausgeführt wird, muss die IAM-Rolle, die die Arbeitsumgebung mit Berechtigungen bereitstellt, einen neuen Satz von S3-Berechtigungen

enthalten, speziell für Cloud Backup von der neuesten zum Einsatz kommen "Cloud Volumes ONTAP-Richtlinie".

Wenn Sie die Cloud Volumes ONTAP-Arbeitsumgebung mit BlueXP Version 3.9.23 oder höher erstellt haben, sollten diese Berechtigungen bereits Teil der IAM-Rolle sein. Andernfalls müssen Sie die fehlenden Berechtigungen hinzufügen.

Aktivierung von Cloud Backup auf einem neuen System

Cloud Backup ist standardmäßig im Assistenten für die Arbeitsumgebung aktiviert. Achten Sie darauf, dass die Option aktiviert bleibt.

Siehe "Starten von Cloud Volumes ONTAP in AWS" Anforderungen und Details für die Erstellung Ihres Cloud Volumes ONTAP Systems.

Schritte

1. Klicken Sie auf **Cloud Volumes ONTAP erstellen**.
2. Wählen Sie Amazon Web Services als Cloud-Provider und wählen Sie dann einen einzelnen Node oder ein HA-System.
3. Füllen Sie die Seite „Details & Credentials“ aus.
4. Lassen Sie auf der Seite Dienste den Dienst aktiviert, und klicken Sie auf **Weiter**.

5. Führen Sie die Seiten im Assistenten aus, um das System bereitzustellen.

Ergebnis

Cloud Backup ist auf dem System aktiviert und sichert täglich Volumes und speichert die letzten 30 Backup-Kopien.

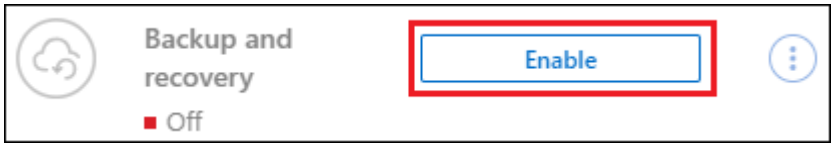
Aktivierung von Cloud Backup auf einem vorhandenen System

Cloud Backup kann jederzeit direkt aus der Arbeitsumgebung aktiviert werden.

Schritte

1. Wählen Sie die Arbeitsumgebung aus und klicken Sie auf **Aktivieren** neben dem Backup- und Recovery-Dienst im rechten Fenster.

   Wenn das Amazon S3 Ziel für Ihre Backups als Arbeitsumgebung auf dem Canvas existiert, können Sie den Cluster auf die Amazon S3-Arbeitsumgebung ziehen, um den Setup-Assistenten zu starten.

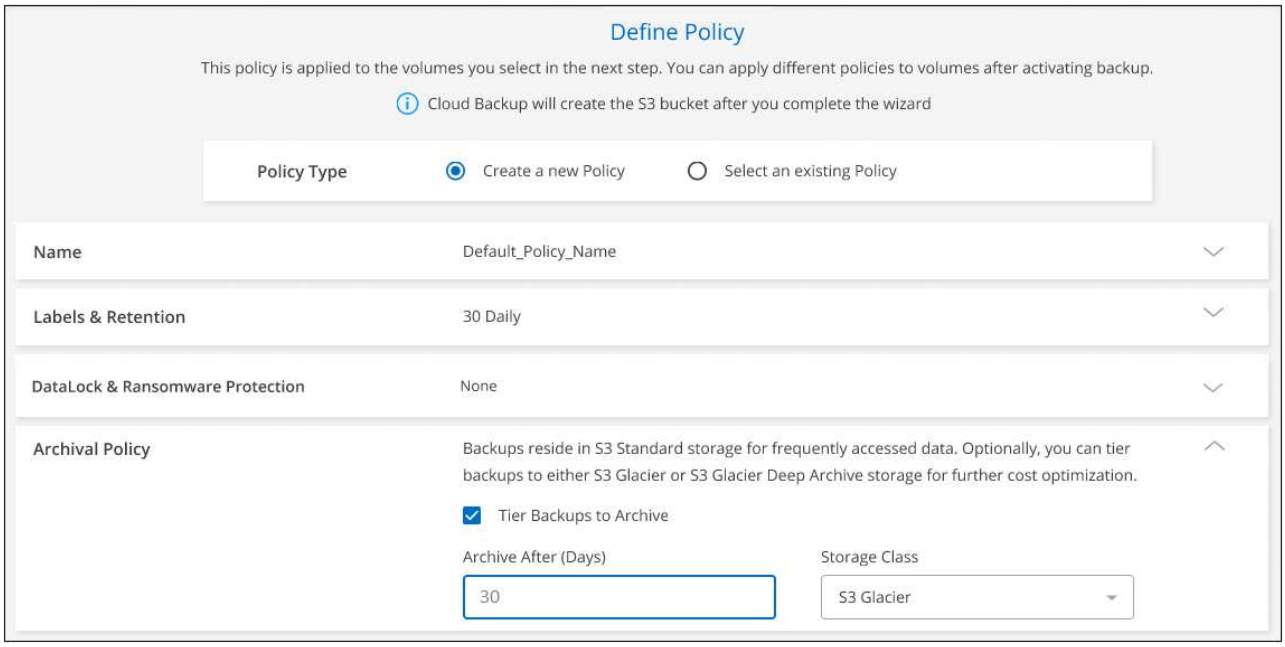


2. Wählen Sie die Provider-Details aus und klicken Sie auf **Weiter**.
   a. Das AWS Konto, mit dem die Backups gespeichert werden. Dies kann ein anderes Konto sein als der Speicherort des Cloud Volumes ONTAP Systems.

      Wenn Sie ein anderes AWS Konto für Ihre Backups verwenden möchten, müssen Sie die Zielanmeldeinformationen für AWS in BlueXP hinzufügen und die Berechtigungen „s3:PutBucketPolicy“ und „s3:PutBucketOwnershipControls“ zur IAM-Rolle hinzufügen, die BlueXP mit Berechtigungen versorgt.

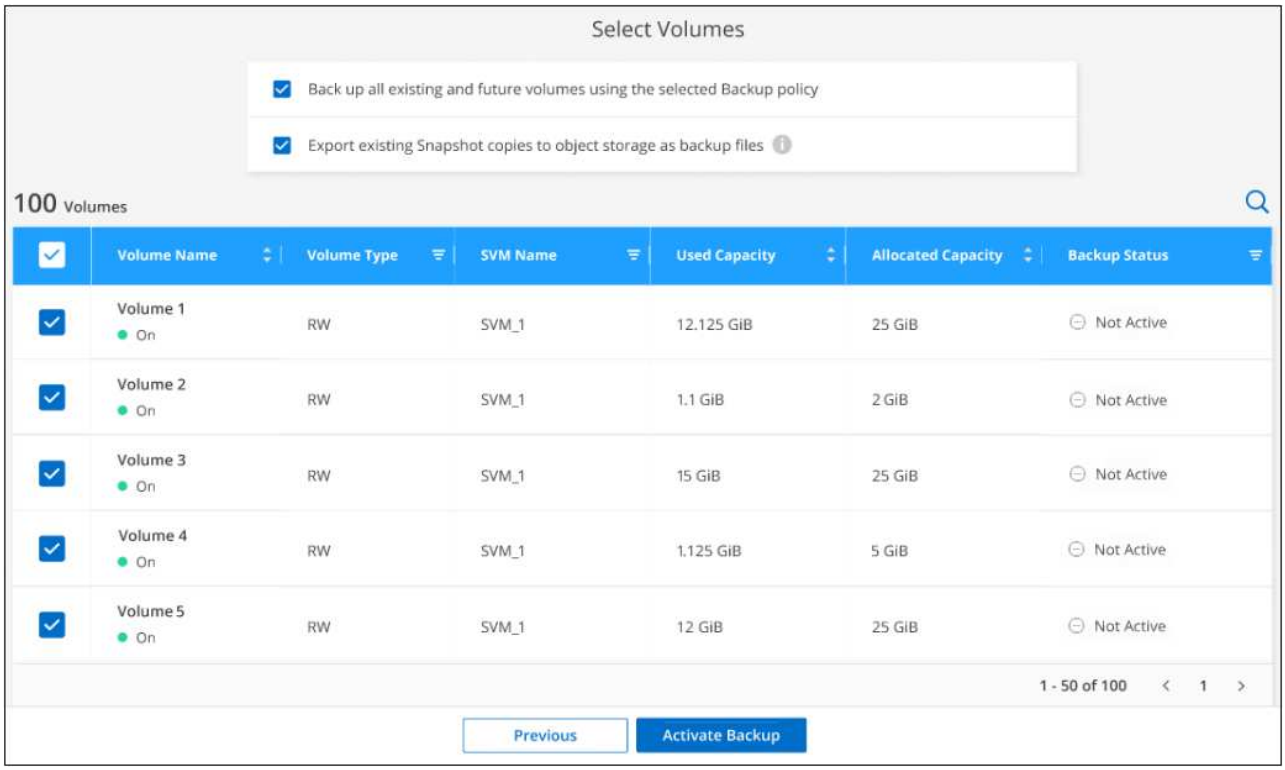
   b. Der Bereich, in dem die Backups gespeichert werden. Dies kann eine andere Region sein als der Speicherort des Cloud Volumes ONTAP Systems.
   c. Unabhängig davon, ob Sie die standardmäßigen Amazon S3-Verschlüsselungsschlüssel verwenden oder Ihre eigenen, von Kunden gemanagten Schlüssel über Ihr AWS-Konto auswählen, um die Verschlüsselung Ihrer Daten zu managen. ("Nutzen Sie Ihre eigenen Schlüssel").

3. Geben Sie die Backup Policy Details ein, die für Ihre Standard Policy verwendet werden, und klicken Sie auf **Weiter**. Sie können eine vorhandene Richtlinie auswählen oder eine neue Richtlinie erstellen, indem Sie in den einzelnen Abschnitten Ihre Auswahl eingeben:
   a. Geben Sie den Namen für die Standardrichtlinie ein. Sie müssen den Namen nicht ändern.
   b. Legen Sie den Backup-Zeitplan fest und wählen Sie die Anzahl der zu behaltenden Backups aus. "Die Liste der vorhandenen Richtlinien, die Sie auswählen können, wird angezeigt".
   c. Optional können Sie bei Verwendung von ONTAP 9.11.1 und höher Ihre Backups vor dem Löschen und Ransomware-Angriffen schützen, indem Sie eine der Einstellungen *DataLock und Ransomware Protection* konfigurieren. *DataLock* schützt Ihre Backup-Dateien vor Modified oder Deleted, und *Ransomware Protection* scannt Ihre Backup-Dateien, um nach Anzeichen für einen Ransomware-Angriff in Ihren Backup-Dateien zu suchen. "Erfahren Sie mehr über die verfügbaren DataLock-Einstellungen".
   d. Wenn Sie ONTAP 9.10.1 und höher einsetzen, können Sie optional nach einer bestimmten Anzahl von Tagen Backups entweder auf S3 Glacier oder in S3 Glacier Deep Archive Storage abstufen, um die Kosten weiter zu optimieren. "Erfahren Sie mehr über die Verwendung von Archivierungs-Tiers".



Wichtig: Wenn Sie DataLock verwenden möchten, müssen Sie es bei der Aktivierung von Cloud Backup in Ihrer ersten Richtlinie aktivieren.

4. Wählen Sie auf der Seite Volumes auswählen die Volumes aus, für die ein Backup mit der definierten Backup-Richtlinie gesichert werden soll. Falls Sie bestimmten Volumes unterschiedliche Backup-Richtlinien zuweisen möchten, können Sie später zusätzliche Richtlinien erstellen und auf diese Volumes anwenden.
   - Um alle bestehenden Volumes und Volumes zu sichern, die in der Zukunft hinzugefügt wurden, markieren Sie das Kontrollkästchen „Alle bestehenden und zukünftigen Volumen sichern…“. Wir empfehlen diese Option, damit alle Ihre Volumes gesichert werden und Sie nie vergessen müssen, Backups für neue Volumes zu aktivieren.
   - Um nur vorhandene Volumes zu sichern, aktivieren Sie das Kontrollkästchen in der Titelzeile (☑ Volume Name).
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume (☑ Volume_1).



- Wenn es lokale Snapshot-Kopien für Lese-/Schreib-Volumes in dieser Arbeitsumgebung gibt, die dem Backup-Schedule-Label entsprechen, das Sie gerade für diese Arbeitsumgebung ausgewählt haben (z. B. täglich, wöchentlich usw.), wird eine zusätzliche Eingabeaufforderung angezeigt: „Export vorhandener Snapshot Kopien in Objekt-Storage als Backup-Kopien“. Aktivieren Sie dieses Kontrollkästchen, wenn alle historischen Snapshots als Backup-Dateien in Objekt-Storage kopiert werden sollen, um sicherzustellen, dass die umfassendste Sicherung für Ihre Volumes gewährleistet ist.

5. Klicken Sie auf **Activate Backup** und Cloud Backup beginnt die Erstellung der ersten Backups jedes ausgewählten Volumes.

Ergebnis

Ein S3-Bucket wird automatisch in dem Service-Konto erstellt, das durch den S3-Zugriffsschlüssel und den eingegebenen Geheimschlüssel angegeben ist und die Backup-Dateien dort gespeichert werden. Das Dashboard für Volume Backup wird angezeigt, sodass Sie den Status der Backups überwachen können. Sie können den Status von Backup- und Wiederherstellungsjobs auch mit dem überwachen "Fenster Job-Überwachung".

Was kommt als Nächstes?

- Das können Sie "Management von Backup Files und Backup-Richtlinien". Dies umfasst das Starten und Stoppen von Backups, das Löschen von Backups, das Hinzufügen und Ändern des Backup-Zeitplans und vieles mehr.
- Das können Sie "Management von Backup-Einstellungen auf Cluster-Ebene". Dies umfasst die Änderung der Storage-Schlüssel, die ONTAP für den Zugriff auf den Cloud-Storage verwendet, die Änderung der verfügbaren Netzwerkbandbreite für das Hochladen von Backups in den Objekt-Storage, die Änderung der automatischen Backup-Einstellung für zukünftige Volumes und vieles mehr.
- Das können Sie auch "Wiederherstellung von Volumes, Ordnern oder einzelnen Dateien aus einer Sicherungsdatei" Zu einem Cloud Volumes ONTAP System in AWS oder zu einem ONTAP System vor Ort

Sichern von On-Premises-ONTAP-Daten in Amazon S3

Unternehmen Sie einige Schritte, um den Backup von Daten von On-Premises-ONTAP-Systemen in Amazon S3 Storage zu starten.

Zu beachten ist, dass „On-Premises ONTAP Systeme“ FAS, AFF und ONTAP Select Systeme umfassen.

Schnellstart

Führen Sie die folgenden Schritte aus, um schnell zu beginnen: In den folgenden Abschnitten dieses Themas finden Sie Details zu jedem Schritt.

1 **Geben Sie die Konfigurationsmethode an, die Sie verwenden möchten**

Legen Sie fest, ob Sie Ihr ONTAP Cluster vor Ort über das öffentliche Internet direkt mit AWS S3 verbinden oder ob Sie ein VPN oder AWS Direct Connect verwenden und den Datenverkehr über eine private VPC Endpunktschnittstelle zu AWS S3 leiten möchten.

Siehe die verfügbaren Verbindungsmethoden.

2 **Bereiten Sie Ihren BlueXP Connector vor**

Wenn Sie bereits einen Connector in Ihrer AWS VPC oder Ihrem Standort implementiert haben, sind Sie alle festgelegt. Ist dies nicht der Fall, müssen Sie einen Connector erstellen, um ONTAP-Daten in AWS S3 Storage zu sichern. Außerdem müssen Sie die Netzwerkeinstellungen für den Connector anpassen, damit er eine Verbindung zu AWS S3 herstellen kann.

Lesen Sie, wie Sie einen Konnektor erstellen und wie Sie die erforderlichen Netzwerkeinstellungen definieren.

3 **Vorbereiten Ihres lokalen ONTAP Clusters**

Erkennung des ONTAP Clusters in BlueXP, Überprüfung der Mindestanforderungen des Clusters und Anpassung der Netzwerkeinstellungen, damit die Verbindung zum AWS S3 Cluster möglich ist

Erfahren Sie, wie der ONTAP Cluster vor Ort bereit ist.

4 **Amazon S3 als Backup-Ziel vorbereiten**

Richten Sie Berechtigungen für den Connector ein, um den S3-Bucket zu erstellen und zu managen. Darüber hinaus müssen Berechtigungen für den On-Premises-ONTAP-Cluster eingerichtet werden, damit er Daten lesen und in den S3-Bucket schreiben kann.

Optional können Sie Ihre eigenen, von Ihnen gemanagten Schlüssel für die Datenverschlüsselung einrichten statt dazu die standardmäßigen Amazon S3-Verschlüsselungsschlüssel zu verwenden. Erfahren Sie, wie Sie Ihre AWS S3-Umgebung für den Erhalt von ONTAP-Backups vorbereiten.

5 **Aktivieren Sie Cloud Backup auf dem System**

Wählen Sie die Arbeitsumgebung aus und klicken Sie auf **Aktivieren > Backup Volumes** neben dem Backup-

und Recovery-Dienst im rechten Fenster. Anschließend können Sie im Setup-Assistenten die Standard-Backup-Richtlinie und die Anzahl der beizubehaltenden Backups festlegen und die Volumes auswählen, für die Sie ein Backup erstellen möchten.

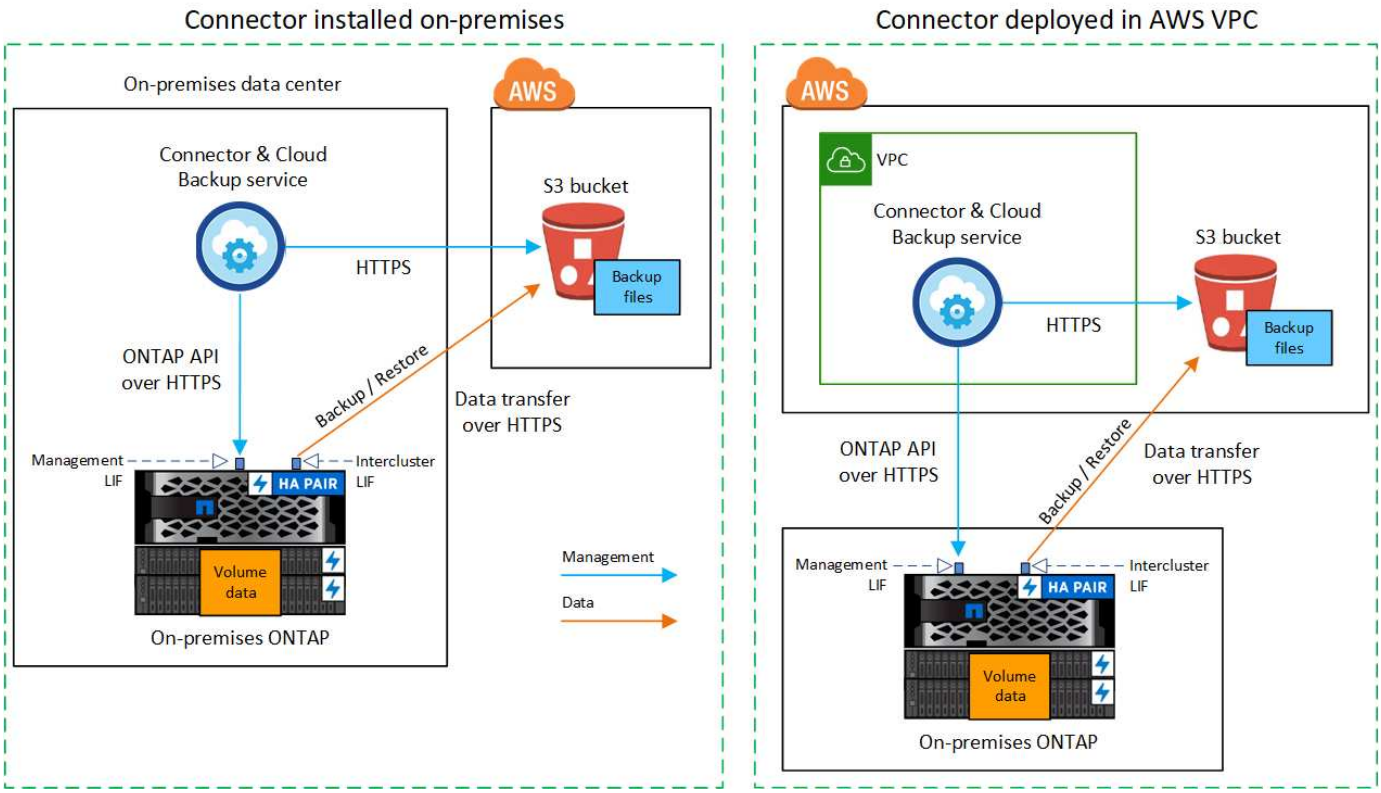
So aktivieren Sie Cloud Backup auf Ihren Volumes.

Netzwerkdiagramme für Verbindungsoptionen

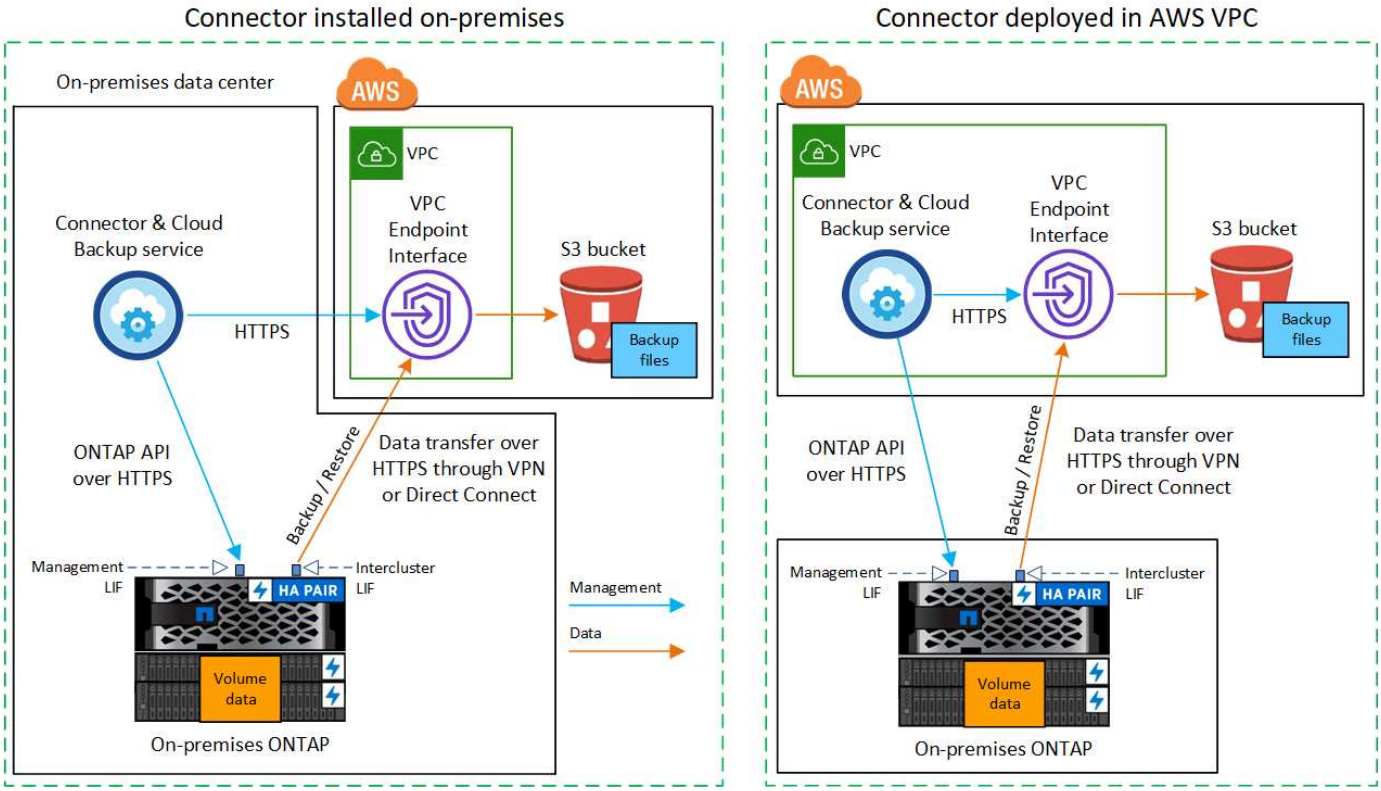
Bei der Konfiguration von Backups von On-Premises-ONTAP-Systemen in AWS S3 gibt es zwei Verbindungsmethoden.

- Öffentliche Verbindung: Über einen öffentlichen S3-Endpunkt wird das ONTAP System direkt mit AWS S3 verbunden.
- Private Verbindung: Verwenden Sie ein VPN oder AWS Direct Connect und leiten Sie den Datenverkehr über eine VPC-Endpunktschnittstelle mit einer privaten IP-Adresse weiter.

Das folgende Diagramm zeigt die Methode **Public Connection** und die Verbindungen, die Sie zwischen den Komponenten vorbereiten müssen. Sie können einen Connector, den Sie an Ihrem Standort installiert haben, oder einen Connector verwenden, den Sie in der AWS VPC implementiert haben.



Das folgende Diagramm zeigt die Methode **private Verbindung** und die Verbindungen, die Sie zwischen den Komponenten vorbereiten müssen. Sie können einen Connector, den Sie an Ihrem Standort installiert haben, oder einen Connector verwenden, den Sie in der AWS VPC implementiert haben.



Bereiten Sie den Konnektor vor

Der BlueXP Connector ist die Hauptsoftware für BlueXP-Funktionen. Zum Sichern und Wiederherstellen Ihrer ONTAP-Daten ist ein Connector erforderlich.

Erstellen oder Umschalten von Anschlüssen

Wenn Sie bereits einen Connector in Ihrer AWS VPC oder Ihrem Standort implementiert haben, sind Sie alle festgelegt. Falls nicht, müssen Sie an einem dieser Standorte einen Connector erstellen, um ONTAP-Daten in AWS S3 Storage zu sichern. Sie können keinen Connector verwenden, der bei einem anderen Cloud-Provider bereitgestellt wird.

- "Erfahren Sie mehr über Steckverbinder"
- "Erste Schritte mit den Anschlüssen"
- "Installieren eines Connectors in AWS"
- "Installieren eines Connectors in Ihrem Haus"
- "Installieren eines Connectors in einer AWS GovCloud Region"

  Cloud Backup wird in GovCloud Regionen unterstützt, wenn der Connector in der Cloud bereitgestellt wird – und nicht, wenn er in Ihrem Unternehmen installiert ist. Darüber hinaus müssen Sie den Connector über AWS Marketplace implementieren. Sie können den Connector nicht in einer Regierungsregion von der BlueXP SaaS-Website bereitstellen.

Anforderungen für Connector-Netzwerke

- Stellen Sie sicher, dass das Netzwerk, in dem der Connector installiert ist, folgende Verbindungen ermöglicht:

- Eine HTTPS-Verbindung über Port 443 zum Cloud Backup Service und zum S3-Objekt-Storage ("Siehe die Liste der Endpunkte")
- Eine HTTPS-Verbindung über Port 443 an Ihre ONTAP-Cluster-Management-LIF
- Für AWS und AWS GovCloud Implementierungen sind zusätzliche Regeln für ein- und ausgehende Sicherheitsgruppen erforderlich. Siehe "Regeln für den Connector in AWS" Entsprechende Details.

- "Stellen Sie sicher, dass der Connector über Berechtigungen zum Management des S3-Buckets verfügt".
- Wenn Sie über eine direkte Verbindung oder eine VPN-Verbindung zwischen Ihrem ONTAP-Cluster und der VPC verfügen und die Kommunikation zwischen dem Connector und S3 im internen AWS Netzwerk verbleiben soll (eine **private** Verbindung), müssen Sie eine VPC Endpunkt-Schnittstelle zu S3 aktivieren. Informationen zur Einrichtung einer VPC-Endpunktschnittstelle finden Sie unter.

Bereiten Sie den ONTAP Cluster vor

Entdecken Sie Ihren ONTAP Cluster in BlueXP

Bevor Sie mit dem Backup von Volume-Daten beginnen können, müssen Sie das lokale ONTAP Cluster in BlueXP ermitteln. Sie müssen die Cluster-Management-IP-Adresse und das Passwort kennen, mit dem das Admin-Benutzerkonto den Cluster hinzufügen kann.

"Entdecken Sie ein Cluster".

ONTAP-Anforderungen erfüllt

- Minimum ONTAP 9.7P5; ONTAP 9.8P13 und höher wird empfohlen.
- SnapMirror Lizenz (im Rahmen des Premium Bundle oder Datensicherungs-Bundles enthalten)

  Hinweis: bei der Verwendung von Cloud Backup ist das „Hybrid Cloud Bundle“ nicht erforderlich.

  Informieren Sie sich darüber "Management Ihrer Cluster-Lizenzen".

- Zeit und Zeitzone sind korrekt eingestellt.

  Informieren Sie sich darüber "Konfigurieren Sie die Cluster-Zeit".

Netzwerkanforderungen für Cluster

- Das Cluster erfordert eine eingehende HTTPS-Verbindung vom Connector zur Cluster-Management-LIF.
- Auf jedem ONTAP Node ist eine Intercluster-LIF erforderlich, die die Volumes hostet, die Sie sichern möchten. Diese Intercluster LIFs müssen in der Lage sein, auf den Objektspeicher zuzugreifen.

  Das Cluster initiiert eine ausgehende HTTPS-Verbindung über Port 443 von den Intercluster-LIFs zum Amazon S3 Storage für Backup- und Restore-Vorgänge. ONTAP liest und schreibt Daten in und aus dem Objekt-Storage – der Objekt-Storage initiiert nie – er reagiert einfach darauf.

- Die Intercluster-LIFs müssen dem *IPspace* zugewiesen werden, den ONTAP für die Verbindung mit dem Objekt-Storage verwenden sollte. "Erfahren Sie mehr über IPspaces".

  Wenn Sie Cloud Backup einrichten, werden Sie aufgefordert, den IP-Speicherplatz zu verwenden. Sie sollten den IPspace auswählen, dem diese LIFs zugeordnet sind. Dies kann der „Standard“-IPspace oder ein benutzerdefinierter IPspace sein, den Sie erstellt haben.

Wenn Sie einen anderen IPspace als „Standard“ verwenden, müssen Sie möglicherweise eine statische Route erstellen, um Zugriff auf den Objekt-Storage zu erhalten.

Alle Intercluster-LIFs im IPspace müssen auf den Objektspeicher zugreifen können. Wenn Sie dies nicht für den aktuellen IPspace konfigurieren können, müssen Sie einen dedizierten IPspace erstellen, wo alle intercluster LIFs Zugriff auf den Objektspeicher haben.

- DNS-Server müssen für die Storage-VM konfiguriert worden sein, auf der sich die Volumes befinden. Informieren Sie sich darüber "Konfigurieren Sie DNS-Services für die SVM".
- Aktualisieren Sie ggf. Firewall-Regeln, um Cloud Backup-Verbindungen von ONTAP zu Objektspeicher über Port 443 und Datenverkehr zur Namensauflösung von der Storage VM zum DNS-Server über Port 53 (TCP/UDP) zu ermöglichen.
- Wenn Sie für die S3-Verbindung einen privaten VPC-Schnittstellenendpunkt in AWS verwenden, muss das S3-Endpunktzertifikat in das ONTAP-Cluster geladen werden, damit HTTPS/443 verwendet werden kann. Informationen zum Einrichten einer VPC-Endpunkt-Schnittstelle und zum Laden des S3-Zertifikats finden Sie unter.
- "Stellen Sie sicher, dass Ihr ONTAP Cluster über Berechtigungen für den Zugriff auf den S3-Bucket verfügt".

Lizenzanforderungen prüfen

- Bevor Sie Cloud Backup für Ihren Cluster aktivieren können, müssen Sie entweder ein „Pay-as-you-go“-Angebot (PAYGO) mit BlueXP Marketplace von AWS abonnieren oder eine Cloud Backup BYOL-Lizenz von NetApp erwerben und aktivieren. Diese Lizenzen sind für Ihr Konto und können für mehrere Systeme verwendet werden.
  - Für die Cloud Backup-PAYGO-Lizenzierung benötigen Sie ein Abonnement für den "AWS BlueXP Marketplace Angebot" Für Cloud-Backup. Die Abrechnung für Cloud Backup erfolgt über dieses Abonnement.
  - Für die BYOL-Lizenzierung von Cloud Backup benötigen Sie die Seriennummer von NetApp, mit der Sie den Service für die Dauer und die Kapazität der Lizenz nutzen können. "Erfahren Sie, wie Sie Ihre BYOL-Lizenzen managen".
- Sie benötigen ein AWS Abonnement für den Objekt-Storage, an dem sich Ihre Backups befinden.

  Backups von On-Premises-Systemen zu Amazon S3 lassen sich in allen Regionen erstellen "Wobei Cloud Volumes ONTAP unterstützt wird"; Einschließlich Regionen von AWS GovCloud. Sie geben die Region an, in der Backups beim Einrichten des Dienstes gespeichert werden sollen.

Bereiten Sie die AWS-Umgebung vor

Richten Sie S3-Berechtigungen ein

Sie müssen zwei Berechtigungssätze konfigurieren:

- Berechtigungen für den Connector zum Erstellen und Managen des S3-Buckets.
- Berechtigungen für den On-Premises-ONTAP-Cluster, damit er Daten lesen und in den S3-Bucket schreiben kann

Schritte

1. Vergewissern Sie sich, dass die folgenden S3-Berechtigungen (von neuestem) vorliegen "BlueXP-Richtlinie") Sind Teil der IAM-Rolle, die den Connector mit Berechtigungen versorgt.

```
{
            "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:ListBucketByTags",
                "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 den Connector mit Version 3.9.21 oder höher bereitgestellt haben, sollten diese Berechtigungen bereits Teil der IAM-Rolle sein. Andernfalls müssen Sie die fehlenden Berechtigungen hinzufügen. Insbesondere die "athena" und "Leim" Berechtigungen, wie sie für die Suche und Wiederherstellung erforderlich sind. Siehe "AWS Dokumentation: Bearbeiten der IAM-Richtlinien".

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

```
{
    "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"
        }
    ]
}
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "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"
        }
    ]
}
```

Siehe "AWS Documentation: Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer" Entsprechende Details.

Vom Kunden verwaltete AWS Schlüssel zur Datenverschlüsselung einrichten

Falls Sie die standardmäßigen Amazon S3-Verschlüsselungsschlüssel verwenden möchten, um die Daten zu verschlüsseln, die zwischen Ihrem On-Premises-Cluster und dem S3-Bucket übergeben wurden, sind die Daten für die Standardinstallation über diesen Verschlüsselungstyp festgelegt.

Wenn Sie Ihre eigenen, vom Kunden gemanagten Schlüssel zur Datenverschlüsselung verwenden möchten, statt die Standardschlüssel zu verwenden, müssen Sie die über die Verschlüsselung gemanagten Schlüssel bereits eingerichtet haben, bevor Sie den Cloud Backup Wizard starten. "Sehen Sie, wie Sie Ihre eigenen Schlüssel verwenden".

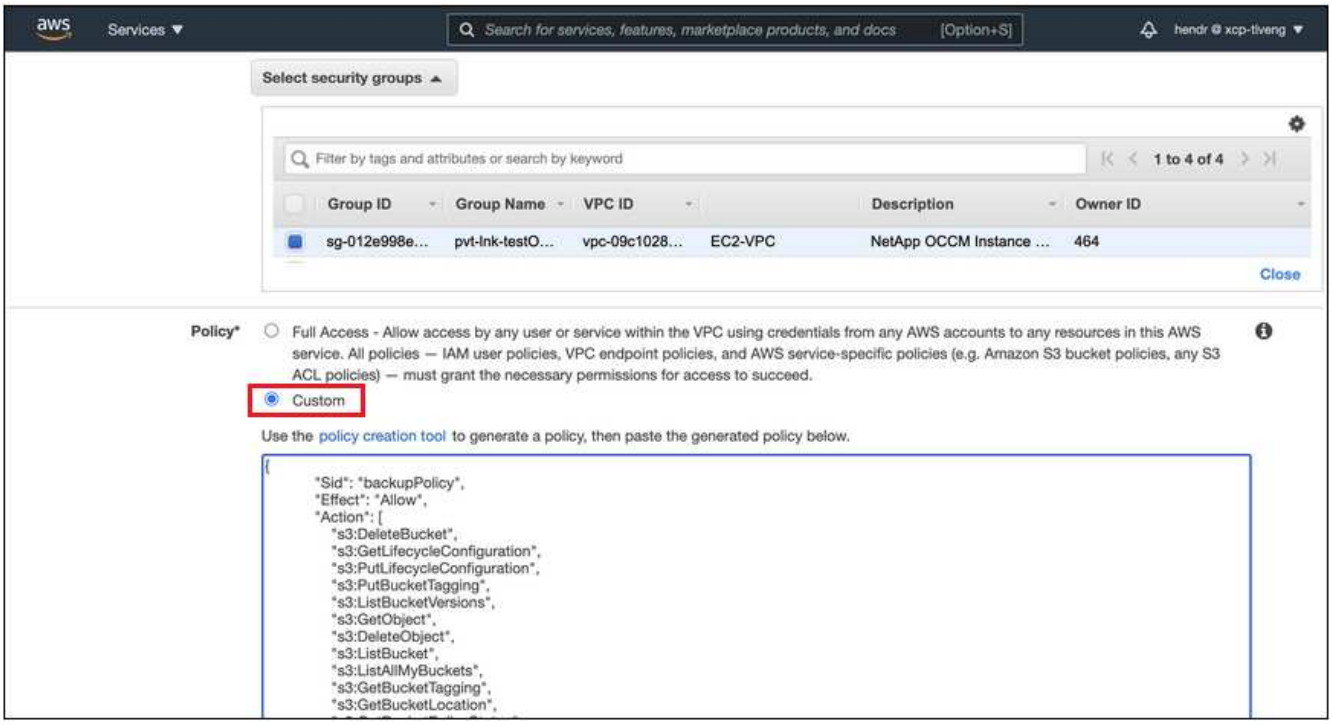
Konfigurieren Sie Ihr System für eine private Verbindung mithilfe einer VPC-Endpunktschnittstelle

Wenn Sie eine standardmäßige öffentliche Internetverbindung nutzen möchten, werden alle Berechtigungen vom Connector festgelegt und es gibt nichts anderes, was Sie tun müssen. Diese Art der Verbindung wird im angezeigt "Erstes Diagramm".

Wenn Sie eine sicherere Verbindung über das Internet von Ihrem On-Prem-Rechenzentrum zur VPC haben möchten, gibt es eine Option, eine AWS PrivateLink-Verbindung im Backup-Aktivierungs-Assistenten auszuwählen. Wenn Sie ein VPN oder AWS Direct Connect verwenden möchten, ist es erforderlich, das On-Premises-System über eine VPC-Endpunktschnittstelle, die eine private IP-Adresse verwendet, zu verbinden.

Diese Art der Verbindung wird im angezeigt "Zweites Diagramm".

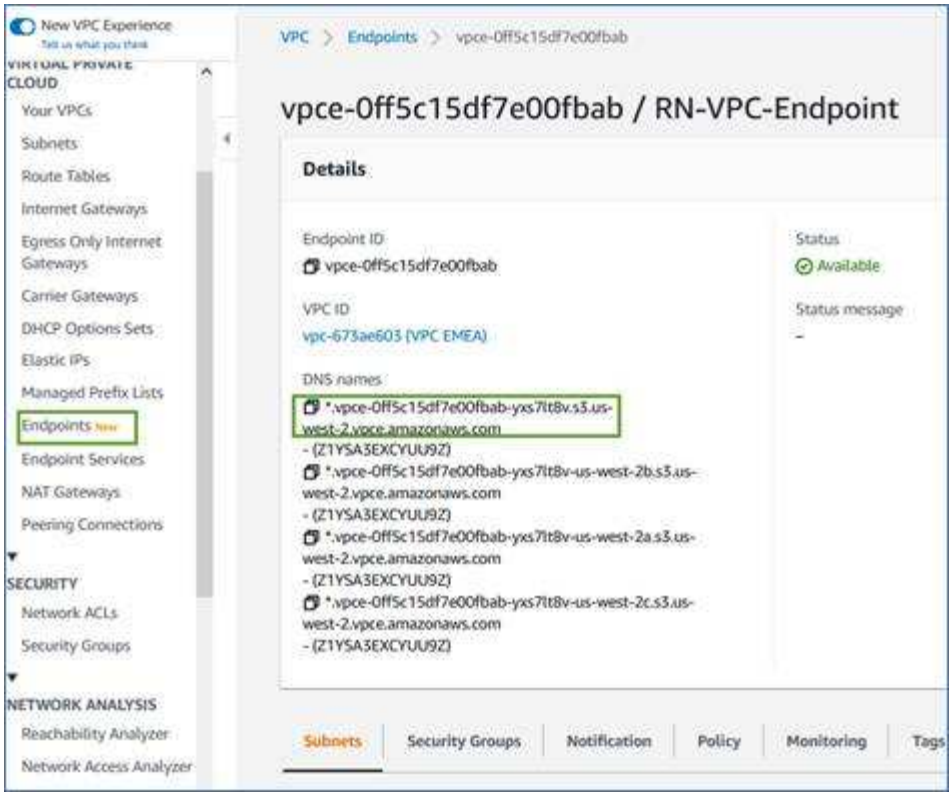
1. Konfiguration eines Schnittstellenendpunkts über die Amazon VPC Konsole oder die Befehlszeile erstellen. "Weitere Informationen zur Verwendung von AWS PrivateLink für Amazon S3 finden Sie unter".
2. Ändern Sie die Konfiguration der Sicherheitsgruppe, die dem BlueXP Connector zugeordnet ist. Sie müssen die Richtlinie in „Benutzerdefiniert“ (von „Vollzugriff“) ändern und müssen Fügen Sie die S3-Berechtigungen aus der Backup-Richtlinie hinzu Wie bereits dargestellt.



Wenn Sie Port 80 (HTTP) für die Kommunikation mit dem privaten Endpunkt verwenden, sind Sie alle festgelegt. Sie können jetzt Cloud-Backup auf dem Cluster aktivieren.

Wenn Sie Port 443 (HTTPS) für die Kommunikation zum privaten Endpunkt verwenden, müssen Sie das Zertifikat aus dem VPC S3-Endpunkt kopieren und zum ONTAP-Cluster hinzufügen, wie in den nächsten 4 Schritten dargestellt.

3. Ermitteln Sie den DNS-Namen des Endpunkts über die AWS Konsole.



4. Beziehen des Zertifikats vom VPC-S3-Endpunkt Dies tun Sie durch "Anmelden bei der VM, die den BlueXP Connector hostet" Und Ausführen des folgenden Befehls. Wenn Sie den DNS-Namen des Endpunkts eingeben, fügen Sie „Eimer“ zum Anfang hinzu und ersetzen das „*“:

```
[ec2-user@ip-10-160-4-68 ~]$ openssl s_client -connect bucket.vpce-
0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443
-showcerts
```

5. Aus der Ausgabe dieses Befehls kopieren Sie die Daten für das S3-Zertifikat (alle Daten zwischen und einschließlich DER START-/END-ZERTIFIKAT-Tags):

```
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 ONTAP Cluster CLI an und wenden Sie das mit dem folgenden Befehl kopierte Zertifikat an (ersetzen Sie Ihren eigenen Storage-VM-Namen):

```
cluster1::> security certificate install -vserver cluster1 -type server-
ca
Please enter Certificate: Press <Enter> when done
```

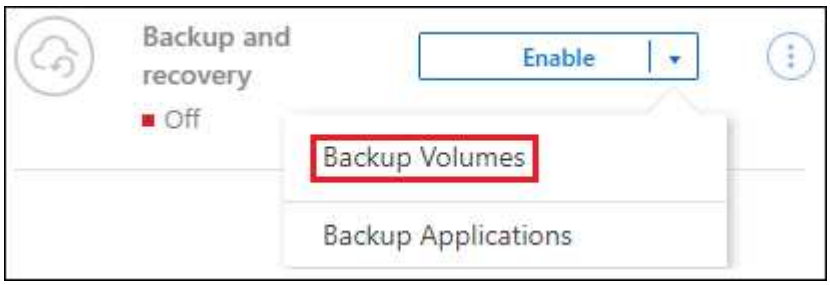
Cloud Backup Aktivieren

Cloud Backup kann jederzeit direkt aus der lokalen Arbeitsumgebung aktiviert werden.

Schritte

1. Wählen Sie in der Arbeitsfläche die Arbeitsumgebung aus und klicken Sie auf **Aktivieren > Backup Volumes** neben dem Backup- und Recovery-Service im rechten Fenster.

   Wenn das Amazon S3 Ziel für Ihre Backups als Arbeitsumgebung auf dem Canvas existiert, können Sie den Cluster auf die Amazon S3-Arbeitsumgebung ziehen, um den Setup-Assistenten zu starten.

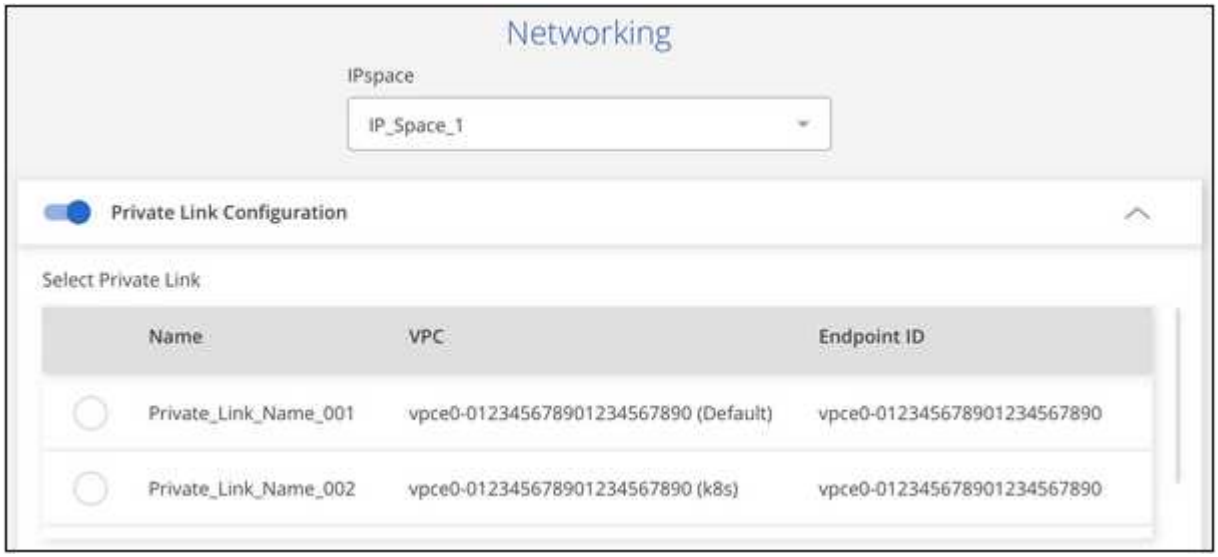


2. Wählen Sie Amazon Web Services als Anbieter und klicken Sie auf **Weiter**.
3. Geben Sie die Provider-Daten ein und klicken Sie auf **Weiter**.
   a. AWS-Konto, AWS-Zugriffsschlüssel und der zum Speichern der Backups verwendete geheime Schlüssel.

      Der Zugriffsschlüssel und der geheime Schlüssel gelten für den von Ihnen erstellten IAM-Benutzer, um dem ONTAP-Cluster Zugriff auf den S3-Bucket zu geben.

   b. Der Region AWS, in der die Backups gespeichert werden.
   c. Unabhängig davon, ob Sie die standardmäßigen Amazon S3-Verschlüsselungsschlüssel verwenden oder Ihre eigenen, von Kunden gemanagten Schlüssel über Ihr AWS Konto auswählen, um die Verschlüsselung Ihrer Daten zu managen. ("Sehen Sie, wie Sie Ihre eigenen Schlüssel verwenden").

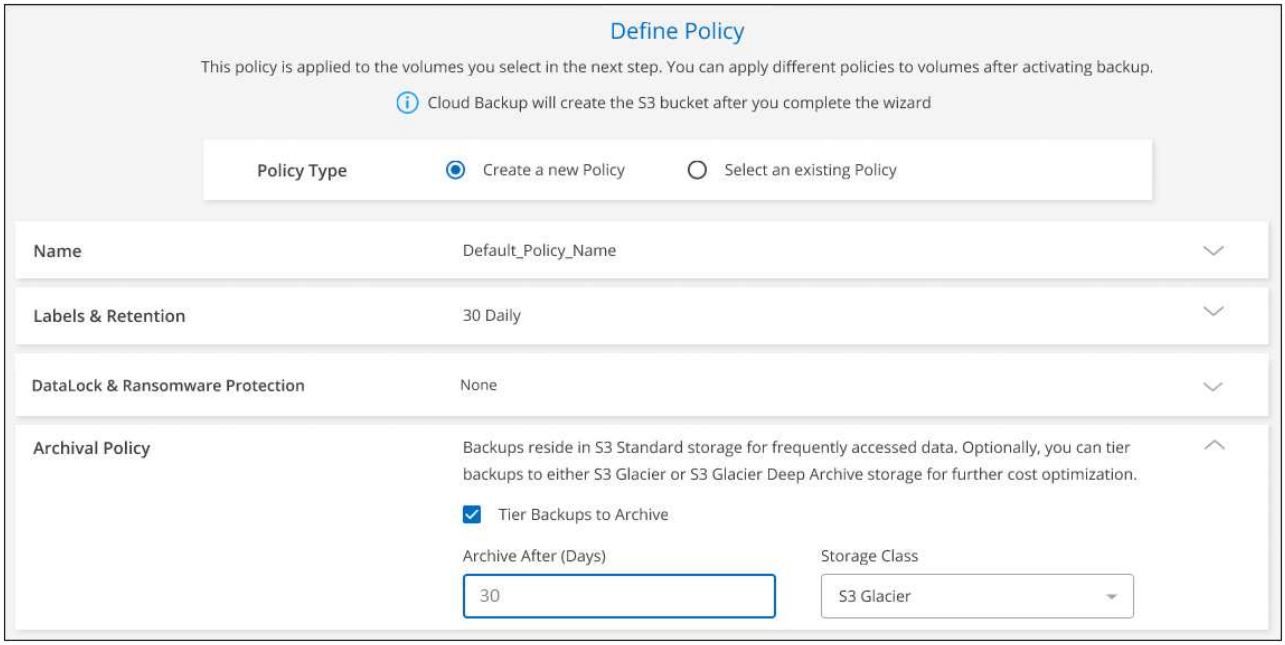
4. Wenn Sie für Ihr Konto keine Lizenz für Cloud Backup besitzen, werden Sie zu diesem Zeitpunkt aufgefordert, die gewünschte Gebührenart auszuwählen. Sie können ein Prepaid-Marketplace-Angebot (PAYGO) für BlueXP Marketplace von AWS (oder bei mehreren Abonnements eine auswählen) abonnieren oder eine Cloud Backup BYOL-Lizenz von NetApp erwerben und aktivieren. "Erfahren Sie, wie Sie Cloud Backup-Lizenzen einrichten."
5. Geben Sie die Netzwerkdaten ein und klicken Sie auf **Weiter**.
   a. Der IPspace im ONTAP Cluster, in dem sich die Volumes, die Sie sichern möchten, befinden. Die Intercluster-LIFs für diesen IPspace müssen über Outbound-Internetzugang verfügen.
   b. Wählen Sie optional aus, ob Sie einen AWS PrivateLink verwenden möchten, den Sie zuvor konfiguriert haben. "Weitere Informationen zur Verwendung von AWS PrivateLink für Amazon S3 finden Sie unter".



6. Geben Sie die Backup Policy Details ein, die für Ihre Standard Policy verwendet werden, und klicken Sie auf **Weiter**. Sie können eine vorhandene Richtlinie auswählen oder eine neue Richtlinie erstellen, indem Sie in den einzelnen Abschnitten Ihre Auswahl eingeben:
   a. Geben Sie den Namen für die Standardrichtlinie ein. Sie müssen den Namen nicht ändern.
   b. Legen Sie den Backup-Zeitplan fest und wählen Sie die Anzahl der zu behaltenden Backups aus. "Die Liste der vorhandenen Richtlinien, die Sie auswählen können, wird angezeigt".
   c. Optional können Sie bei Verwendung von ONTAP 9.11.1 und höher Ihre Backups vor dem Löschen und Ransomware-Angriffen schützen, indem Sie eine der Einstellungen *DataLock und Ransomware*

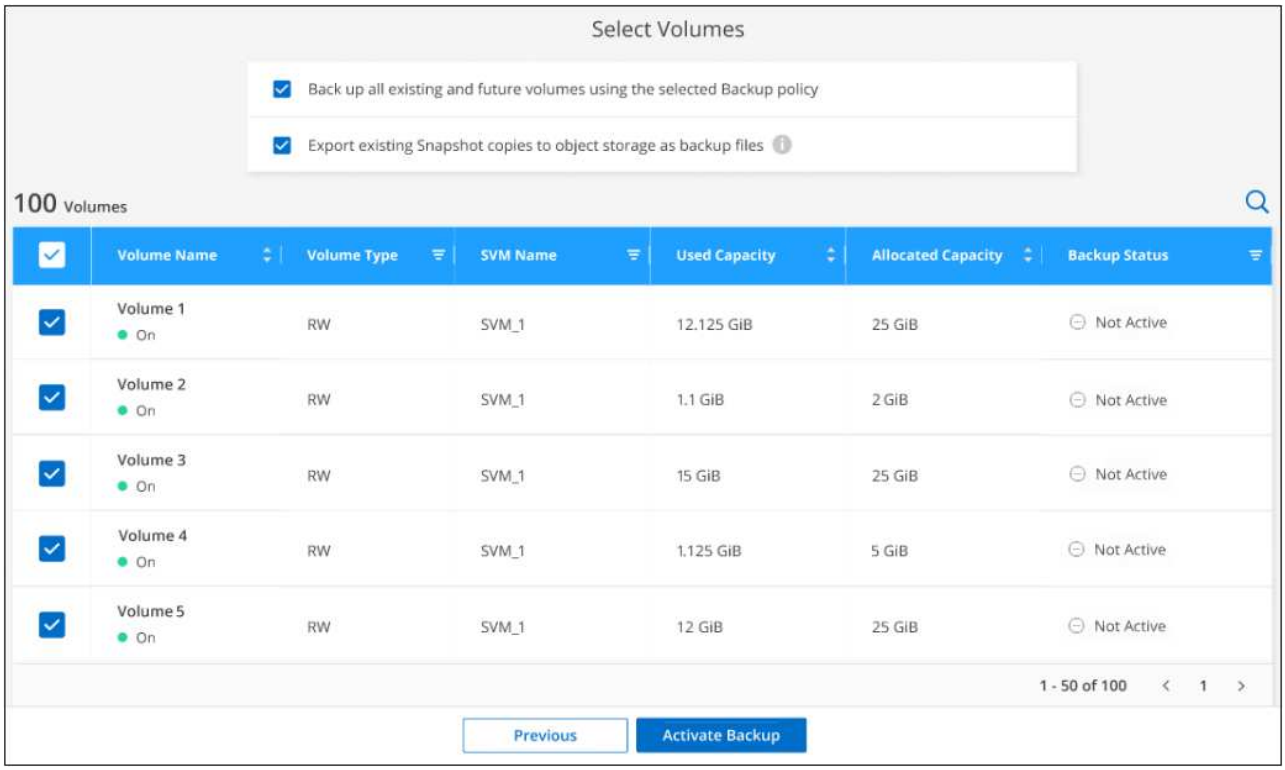
Protection konfigurieren. *DataLock* schützt Ihre Backup-Dateien vor Modified oder Deleted, und *Ransomware Protection* scannt Ihre Backup-Dateien, um nach Anzeichen für einen Ransomware-Angriff in Ihren Backup-Dateien zu suchen. "Erfahren Sie mehr über die verfügbaren DataLock-Einstellungen".

d. Wenn Sie ONTAP 9.10.1 und höher einsetzen, können Sie optional nach einer bestimmten Anzahl von Tagen Backups entweder auf S3 Glacier oder in S3 Glacier Deep Archive Storage abstufen, um die Kosten weiter zu optimieren. "Erfahren Sie mehr über die Verwendung von Archivierungs-Tiers".



Wichtig: Wenn Sie DataLock verwenden möchten, müssen Sie es bei der Aktivierung von Cloud Backup in Ihrer ersten Richtlinie aktivieren.

7. Wählen Sie auf der Seite Volumes auswählen die Volumes aus, für die ein Backup mit der definierten Backup-Richtlinie gesichert werden soll. Falls Sie bestimmten Volumes unterschiedliche Backup-Richtlinien zuweisen möchten, können Sie später zusätzliche Richtlinien erstellen und auf diese Volumes anwenden.
   - Um alle bestehenden Volumes und Volumes zu sichern, die in der Zukunft hinzugefügt wurden, markieren Sie das Kontrollkästchen „Alle bestehenden und zukünftigen Volumen sichern…“. Wir empfehlen diese Option, damit alle Ihre Volumes gesichert werden und Sie nie vergessen müssen, Backups für neue Volumes zu aktivieren.
   - Um nur vorhandene Volumes zu sichern, aktivieren Sie das Kontrollkästchen in der Titelzeile (☑ Volume Name).
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume (☑ Volume_1).



- Wenn es lokale Snapshot-Kopien für Lese-/Schreib-Volumes in dieser Arbeitsumgebung gibt, die dem Backup-Schedule-Label entsprechen, das Sie gerade für diese Arbeitsumgebung ausgewählt haben (z. B. täglich, wöchentlich usw.), wird eine zusätzliche Eingabeaufforderung angezeigt: „Export vorhandener Snapshot Kopien in Objekt-Storage als Backup-Kopien“. Aktivieren Sie dieses Kontrollkästchen, wenn alle historischen Snapshots als Backup-Dateien in Objekt-Storage kopiert werden sollen, um sicherzustellen, dass die umfassendste Sicherung für Ihre Volumes gewährleistet ist.

8. Klicken Sie auf **Activate Backup** und Cloud Backup beginnt mit der Erstellung der ersten Backups Ihrer Volumes.

Ergebnis

Ein S3-Bucket wird automatisch in dem Service-Konto erstellt, das durch den S3-Zugriffsschlüssel und den eingegebenen Geheimschlüssel angegeben ist und die Backup-Dateien dort gespeichert werden. Das Dashboard für Volume Backup wird angezeigt, sodass Sie den Status der Backups überwachen können. Sie können den Status von Backup- und Wiederherstellungsjobs auch mit dem überwachen "Fenster Job-Überwachung".

Was kommt als Nächstes?

- Das können Sie "Management von Backup Files und Backup-Richtlinien". Dies umfasst das Starten und Stoppen von Backups, das Löschen von Backups, das Hinzufügen und Ändern des Backup-Zeitplans und vieles mehr.
- Das können Sie "Management von Backup-Einstellungen auf Cluster-Ebene". Dies umfasst die Änderung der Storage-Schlüssel, die ONTAP für den Zugriff auf den Cloud-Storage verwendet, die Änderung der verfügbaren Netzwerkbandbreite für das Hochladen von Backups in den Objekt-Storage, die Änderung der automatischen Backup-Einstellung für zukünftige Volumes und vieles mehr.
- Das können Sie auch "Wiederherstellung von Volumes, Ordnern oder einzelnen Dateien aus einer Sicherungsdatei" Zu einem Cloud Volumes ONTAP System in AWS oder zu einem ONTAP System vor Ort

Sichern von lokalen ONTAP Daten in StorageGRID

Unternehmen Sie einige Schritte, um den Backup von Daten von ONTAP On-Premises-Systemen auf Objekt-Storage in NetApp StorageGRID Systemen durchzuführen.

Zu beachten ist, dass „On-Premises ONTAP Systeme“ FAS, AFF und ONTAP Select Systeme umfassen.

Schnellstart

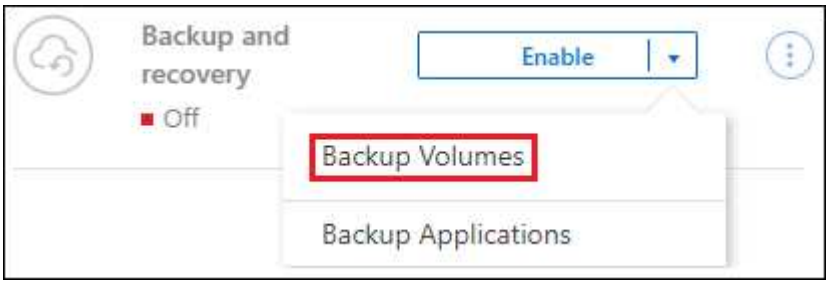
Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

1 Überprüfen Sie die Unterstützung Ihrer Konfiguration

- Sie haben den lokalen Cluster erkannt und zu einer Arbeitsumgebung in BlueXP hinzugefügt. Siehe "Erkennung von ONTAP Clustern" Entsprechende Details.
  - Auf dem Cluster läuft ONTAP 9.7P5 oder höher.
  - Das Cluster verfügt über eine SnapMirror Lizenz – es ist im Premium Bundle oder in der Datensicherungs-Bundle enthalten.
  - Der Cluster muss über die erforderlichen Netzwerkverbindungen zu StorageGRID und zum Connector verfügen.
- Sie haben einen Connector auf Ihrem Gelände installiert.
  - Der Connector kann auf einer Website mit oder ohne Internetzugang installiert werden.
  - Das Networking für den Connector ermöglicht eine ausgehende HTTPS-Verbindung zum ONTAP-Cluster und zu StorageGRID.
- Sie haben gekauft "Und aktiviert" Eine Cloud Backup BYOL-Lizenz von NetApp
- Ihre StorageGRID hat Version 10.3 oder höher mit Zugriffsschlüsseln, die S3-Berechtigungen aufweisen.

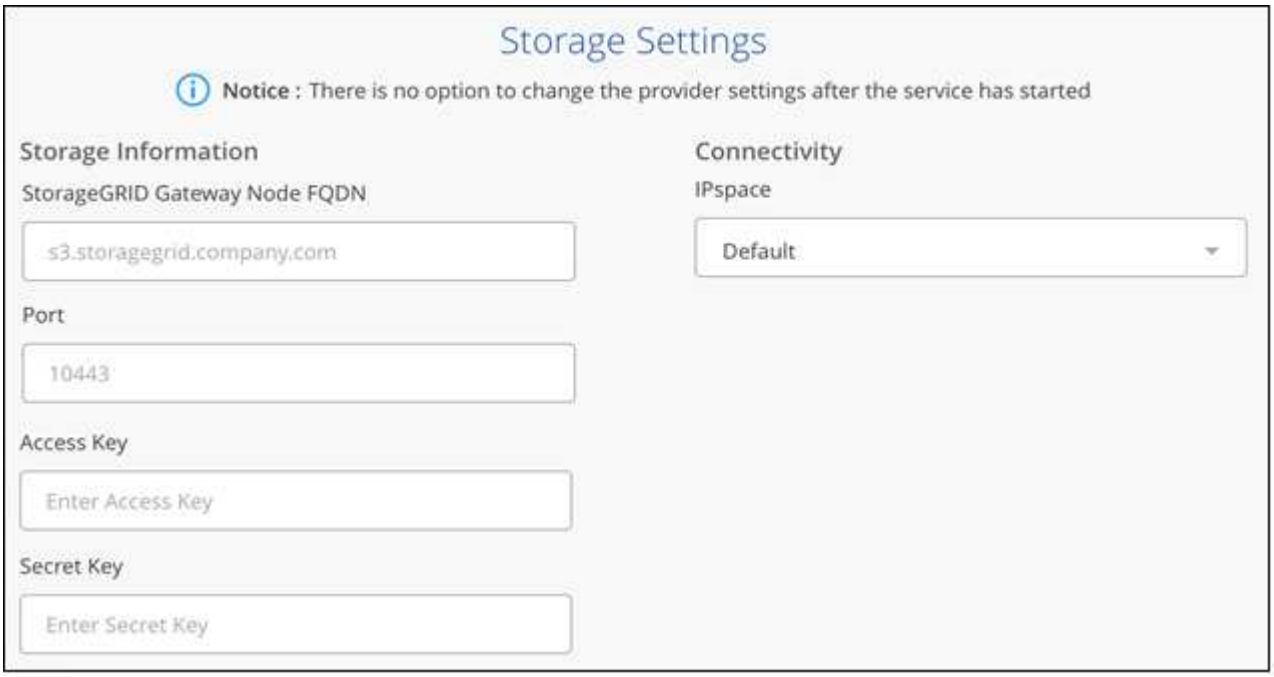
2 Aktivieren Sie Cloud Backup auf dem System

Wählen Sie die Arbeitsumgebung aus und klicken Sie auf **Aktivieren > Backup Volumes** neben dem Backup- und Recovery-Dienst im rechten Fenster, und folgen Sie dann dem Setup-Assistenten.



3 Geben Sie die Details zum StorageGRID ein

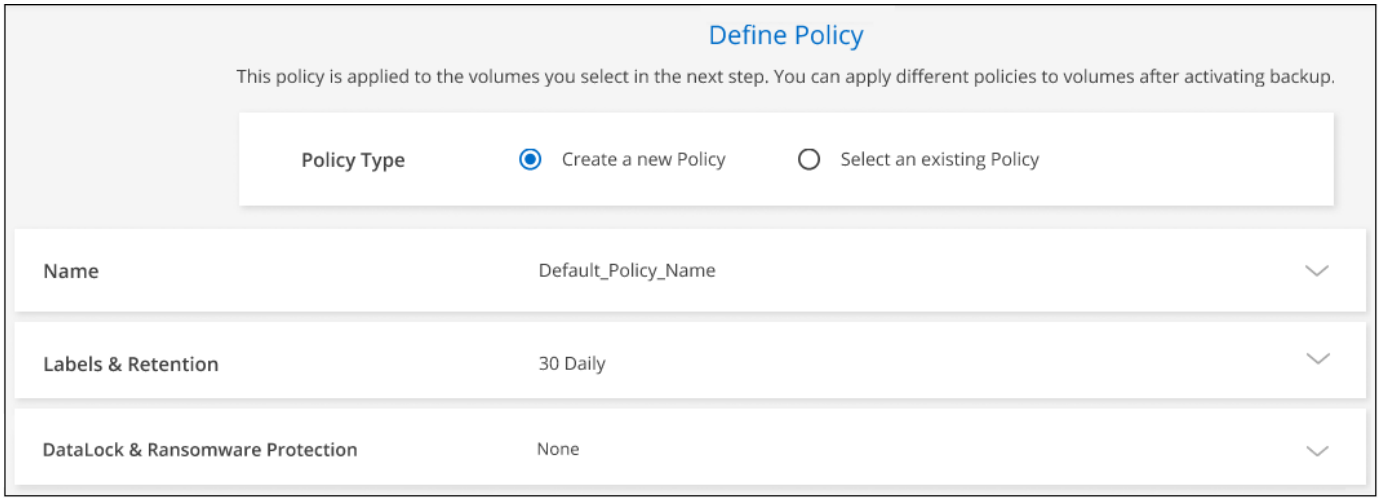
Wählen Sie als Provider StorageGRID aus, und geben Sie dann die Details zum StorageGRID-Server und dem S3-Mandantenkonto ein. Sie müssen außerdem den IPspace im ONTAP Cluster angeben, auf dem sich die Volumes befinden.



4 **Legen Sie die standardmäßige Backup-Richtlinie fest**

Die Standardrichtlinie sichert Volumes täglich und speichert die letzten 30 Backup-Kopien jedes Volumes. Änderung zu stündlichen, täglichen, wöchentlichen, monatlichen oder jährlichen Backups Oder wählen Sie eine der systemdefinierten Richtlinien aus, die mehr Optionen bieten. Sie können auch die Anzahl der zu behaltenden Backup-Kopien ändern.

Optional können Sie bei Verwendung von ONTAP 9.11.1 und höher Ihre Backups vor dem Löschen und Ransomware-Angriffen schützen, indem Sie eine der Einstellungen *DataLock und Ransomware Protection* konfigurieren. "Weitere Informationen über die verfügbaren Konfigurationseinstellungen für Cloud Backup-Richtlinien".



5 **Wählen Sie die Volumes aus, die Sie sichern möchten**

Legen Sie auf der Seite Volumes auswählen fest, welche Volumes gesichert werden sollen. Verwenden Sie dazu die Standard-Backup-Richtlinie. Um bestimmten Volumes unterschiedliche Backup-Richtlinien

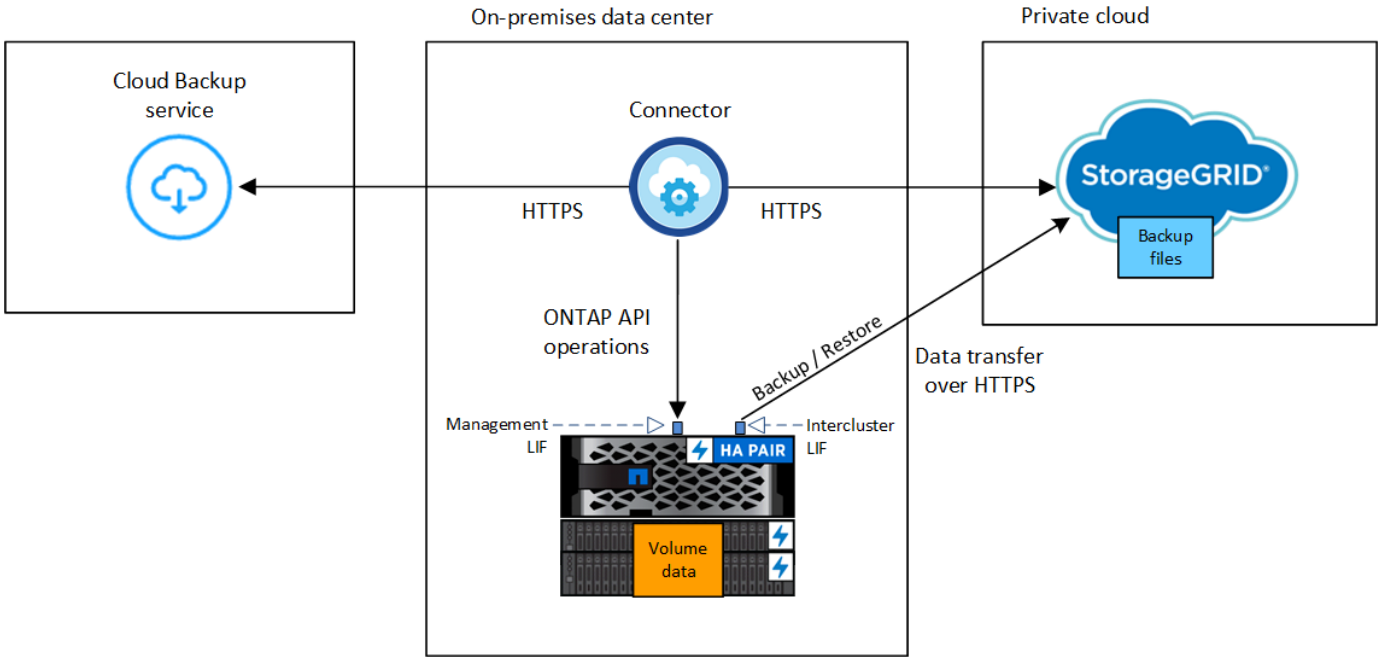
zuzuweisen, können Sie weitere Richtlinien erstellen und diese später auf Volumes anwenden.

Ein S3-Bucket wird automatisch in dem Service-Konto erstellt, das durch den S3-Zugriffsschlüssel und den eingegebenen Geheimschlüssel angegeben ist und die Backup-Dateien dort gespeichert werden.

Anforderungen

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie mit dem Backup von On-Premises-Volumes in StorageGRID beginnen.

Das folgende Bild zeigt jede Komponente beim Backup eines On-Prem-ONTAP-Systems in StorageGRID und den Verbindungen, die zwischen ihnen vorbereitet werden müssen:



Wenn der Connector und das lokale ONTAP-System an einem lokalen Standort ohne Internetzugang installiert werden, muss sich das StorageGRID-System im selben On-Premises-Datacenter befinden.

Vorbereiten der ONTAP Cluster

Bevor Sie mit dem Backup von Volume-Daten beginnen können, müssen Sie die ONTAP Cluster vor Ort in BlueXP ermitteln.

"Entdecken Sie ein Cluster".

ONTAP-Anforderungen erfüllt

- Minimum ONTAP 9.7P5; ONTAP 9.8P13 und höher wird empfohlen.
- SnapMirror Lizenz (im Rahmen des Premium Bundle oder Datensicherungs-Bundles enthalten)

  Hinweis: bei der Verwendung von Cloud Backup ist das „Hybrid Cloud Bundle“ nicht erforderlich.

  Informieren Sie sich darüber "Management Ihrer Cluster-Lizenzen".

- Zeit und Zeitzone sind korrekt eingestellt.

  Informieren Sie sich darüber "Konfigurieren Sie die Cluster-Zeit".

Netzwerkanforderungen für Cluster

- Der ONTAP-Cluster initiiert eine HTTPS-Verbindung über einen vom Benutzer angegebenen Port von der Intercluster-LIF zum StorageGRID-Gateway-Node für Backup- und Restore-Vorgänge. Der Port kann während der Backup-Einrichtung konfiguriert werden.

  ONTAP liest und schreibt Daten auf und aus dem Objekt-Storage. Objekt-Storage startet nie, er reagiert einfach nur.

- ONTAP erfordert eine eingehende Verbindung vom Connector zur Cluster-Management-LIF. Der Stecker muss sich in Ihrem Haus befinden.
- Auf jedem ONTAP Node ist eine Intercluster-LIF erforderlich, die die Volumes hostet, die Sie sichern möchten. Die LIF muss dem *IPspace* zugewiesen sein, den ONTAP zur Verbindung mit Objekt-Storage verwenden sollte. "Erfahren Sie mehr über IPspaces".

  Wenn Sie Cloud Backup einrichten, werden Sie aufgefordert, den IP-Speicherplatz zu verwenden. Sie sollten den IPspace auswählen, dem jede LIF zugeordnet ist. Dies kann der „Standard“-IPspace oder ein benutzerdefinierter IPspace sein, den Sie erstellt haben.

- Die Intercluster-LIFs der Nodes können auf den Objektspeicher zugreifen (nicht erforderlich, wenn der Connector an einem „dunklen“ Standort installiert ist).
- DNS-Server wurden für die Storage-VM konfiguriert, auf der sich die Volumes befinden. Informieren Sie sich darüber "Konfigurieren Sie DNS-Services für die SVM".
- Wenn Sie einen anderen IPspace als den Standard verwenden, müssen Sie möglicherweise eine statische Route erstellen, um Zugriff auf den Objekt-Storage zu erhalten.
- Aktualisieren Sie bei Bedarf Firewall-Regeln, um Cloud Backup Service-Verbindungen von ONTAP zu Objektspeicher über den angegebenen Port (normalerweise Port 443) und den Datenverkehr zur Namensauflösung von der Speicher-VM zum DNS-Server über Port 53 (TCP/UDP) zuzulassen.

StorageGRID wird vorbereitet

StorageGRID muss folgende Anforderungen erfüllen: Siehe "StorageGRID-Dokumentation" Finden Sie weitere Informationen.

Unterstützte StorageGRID-Versionen

StorageGRID 10.3 und höher wird unterstützt.

Damit Sie für Ihre Backups DataLock & Ransomware Protection verwenden können, müssen Ihre StorageGRID Systeme ab Version 11.6.0.3 laufen.

S3-Anmeldedaten

Sie müssen ein S3-Mandantenkonto erstellt haben, um den Zugriff auf Ihren StorageGRID Storage zu kontrollieren. "Weitere Informationen finden Sie in der StorageGRID Dokumentation".

Wenn Sie das Backup in StorageGRID einrichten, werden Sie vom Backup-Assistenten aufgefordert, einen S3-Zugriffsschlüssel und einen geheimen Schlüssel für ein Mandantenkonto einzugeben. Das Mandantenkonto ermöglicht Cloud Backup die Authentifizierung und den Zugriff auf die StorageGRID-Buckets, die für das Speichern von Backups verwendet werden. Die Schlüssel sind erforderlich, damit StorageGRID weiß, wer die Anforderung macht.

Diese Zugriffsschlüssel müssen einem Benutzer mit den folgenden Berechtigungen zugeordnet sein:

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Objektversionierung

Sie dürfen die StorageGRID Objektversionierung auf dem Objektspeicher-Bucket nicht manuell aktivieren.

Erstellen oder Umschalten von Anschlüssen

Beim Daten-Backup in StorageGRID muss am Standort ein Connector verfügbar sein. Sie müssen entweder einen neuen Konnektor installieren oder sicherstellen, dass sich der aktuell ausgewählte Connector auf der Prem befindet. Der Connector kann auf einer Website mit oder ohne Internetzugang installiert werden.

- "Erfahren Sie mehr über Steckverbinder"
- "Installieren des Connectors auf einem Linux-Host mit Internetzugang"
- "Installieren des Connectors auf einem Linux-Host ohne Internetzugang"
- "Wechseln zwischen den Anschlüssen"

> Die Funktion Cloud Backup ist in BlueXP Connector integriert. Wenn Sie auf einer Website ohne Internetverbindung installiert sind, müssen Sie die Connector-Software regelmäßig aktualisieren, um Zugang zu neuen Funktionen zu erhalten. Prüfen Sie die "Cloud Backup Was ist neu" Um die neuen Funktionen in jeder Cloud Backup Version anzuzeigen, gehen Sie folgendermaßen vor "Aktualisieren Sie die Connector-Software" Wann Sie neue Funktionen nutzen möchten.

Vorbereiten der Vernetzung für den Connector

Stellen Sie sicher, dass der Connector über die erforderlichen Netzwerkverbindungen verfügt.

Schritte

1. Stellen Sie sicher, dass das Netzwerk, in dem der Connector installiert ist, folgende Verbindungen ermöglicht:
   - Eine HTTPS-Verbindung über Port 443 zum StorageGRID-Gateway-Node
   - Eine HTTPS-Verbindung über Port 443 an Ihre ONTAP-Cluster-Management-LIF
   - Eine ausgehende Internetverbindung über Port 443 zu Cloud Backup (bei Installation des Connectors an einem „dunklen“ Standort nicht erforderlich)

Lizenzanforderungen

Bevor Sie Cloud Backup für Ihren Cluster aktivieren können, müssen Sie eine Cloud Backup BYOL-Lizenz von NetApp erwerben und aktivieren. Diese Lizenz gilt für das Konto und kann auf mehreren Systemen verwendet werden.

Sie benötigen die Seriennummer von NetApp, mit der Sie den Service für die Dauer und die Kapazität der Lizenz nutzen können. "Erfahren Sie, wie Sie Ihre BYOL-Lizenzen managen".

PAYGO-Lizenzierung wird beim Backup von Dateien in StorageGRID nicht unterstützt.

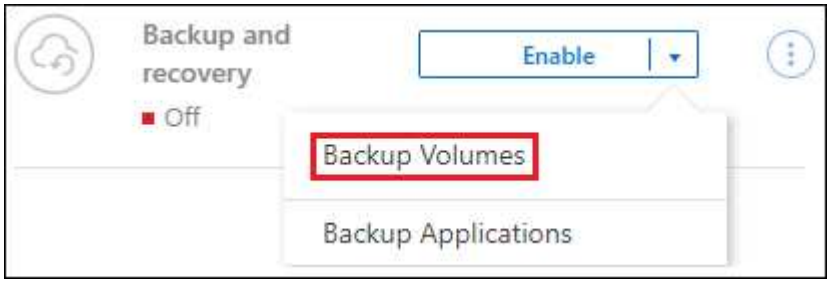
Unterstützung von Cloud Backup für StorageGRID

Cloud Backup kann jederzeit direkt aus der lokalen Arbeitsumgebung aktiviert werden.

Schritte

1. Wählen Sie auf dem Bildschirm die lokale Arbeitsumgebung aus und klicken Sie auf **Aktivieren > Backup Volumes** neben dem Backup- und Recovery-Service im rechten Fenster.

   Wenn das StorageGRID Ziel für Ihre Backups als eine Arbeitsumgebung auf dem Canvas existiert, können Sie den Cluster auf die StorageGRID Arbeitsumgebung ziehen, um den Setup-Assistenten zu starten.



2. Wählen Sie als Anbieter **StorageGRID** aus, klicken Sie auf **Weiter** und geben Sie dann die Provider-Daten ein:

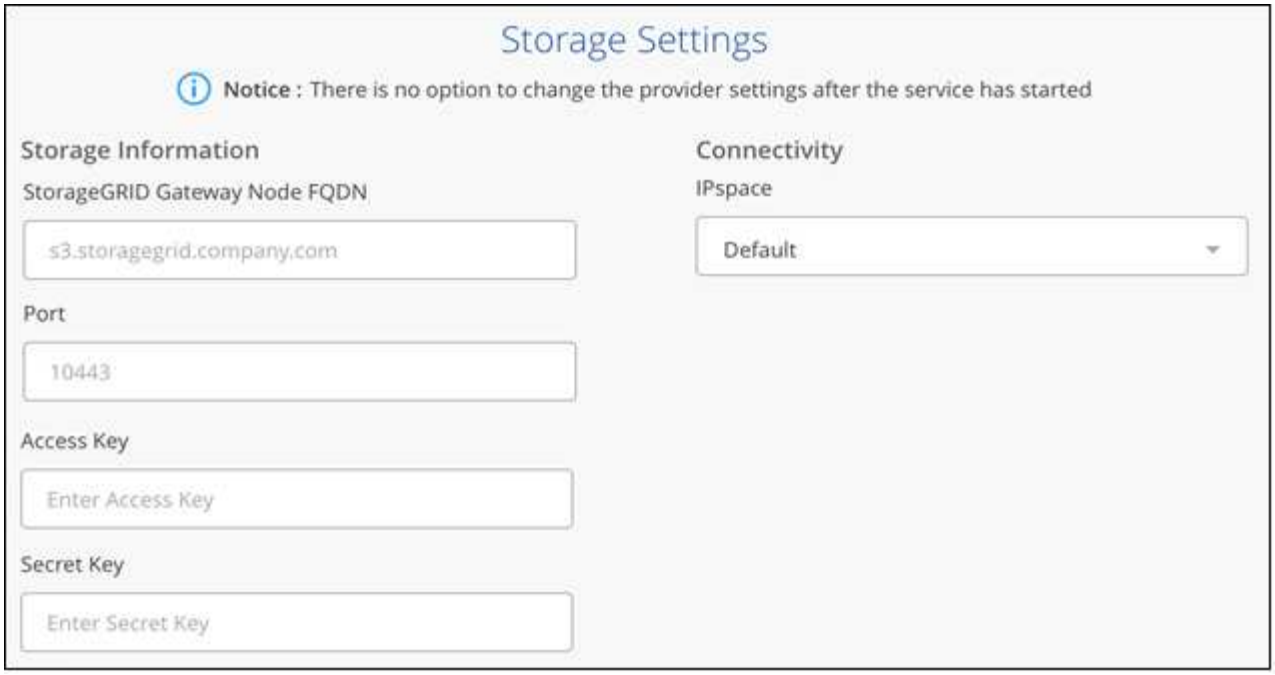
   a. Der FQDN des StorageGRID-Gateway-Knotens.

   b. Der Port, den ONTAP für die HTTPS-Kommunikation mit StorageGRID verwenden sollte.

   c. Der Zugriffsschlüssel und der geheime Schlüssel, mit dem auf den Bucket zugegriffen wird, um Backups zu speichern.

   d. Der IPspace im ONTAP Cluster, in dem sich die Volumes, die Sie sichern möchten, befinden. Die Intercluster-LIFs für diesen IPspace müssen über Outbound-Internetzugang verfügen (nicht erforderlich, wenn der Connector auf einer „dunklen“ Seite installiert ist).

      Durch die Auswahl des richtigen IPspaces wird sichergestellt, dass Cloud Backup eine Verbindung von ONTAP zu Ihrem StorageGRID Objekt-Storage einrichten kann.

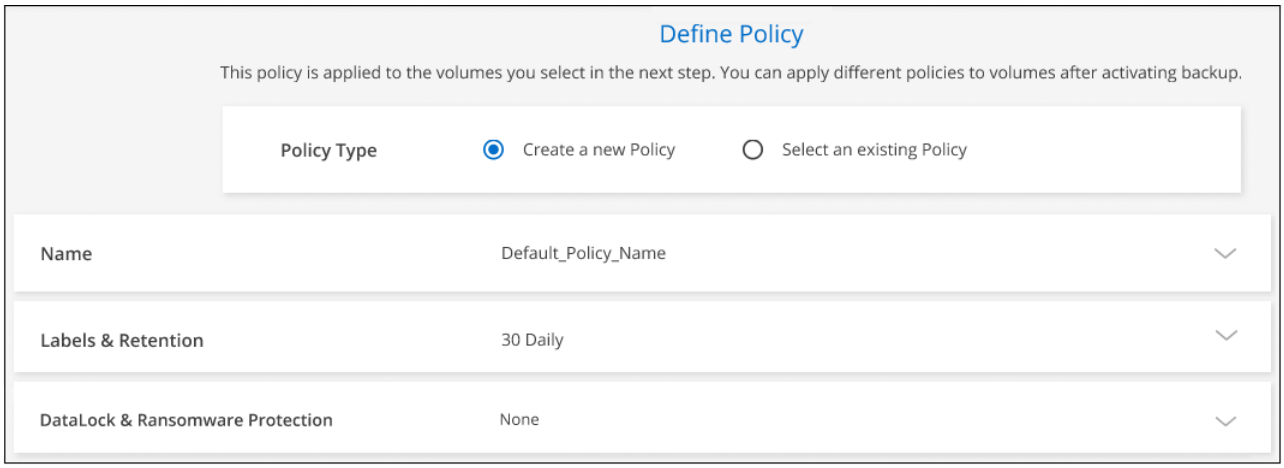


3. Geben Sie die Backup Policy Details ein, die für Ihre Standard Policy verwendet werden, und klicken Sie auf **Weiter**. Sie können eine vorhandene Richtlinie auswählen oder eine neue Richtlinie erstellen, indem Sie in den einzelnen Abschnitten Ihre Auswahl eingeben:

   a. Geben Sie den Namen für die Standardrichtlinie ein. Sie müssen den Namen nicht ändern.

   b. Legen Sie den Backup-Zeitplan fest und wählen Sie die Anzahl der zu behaltenden Backups aus. "Die Liste der vorhandenen Richtlinien, die Sie auswählen können, wird angezeigt".

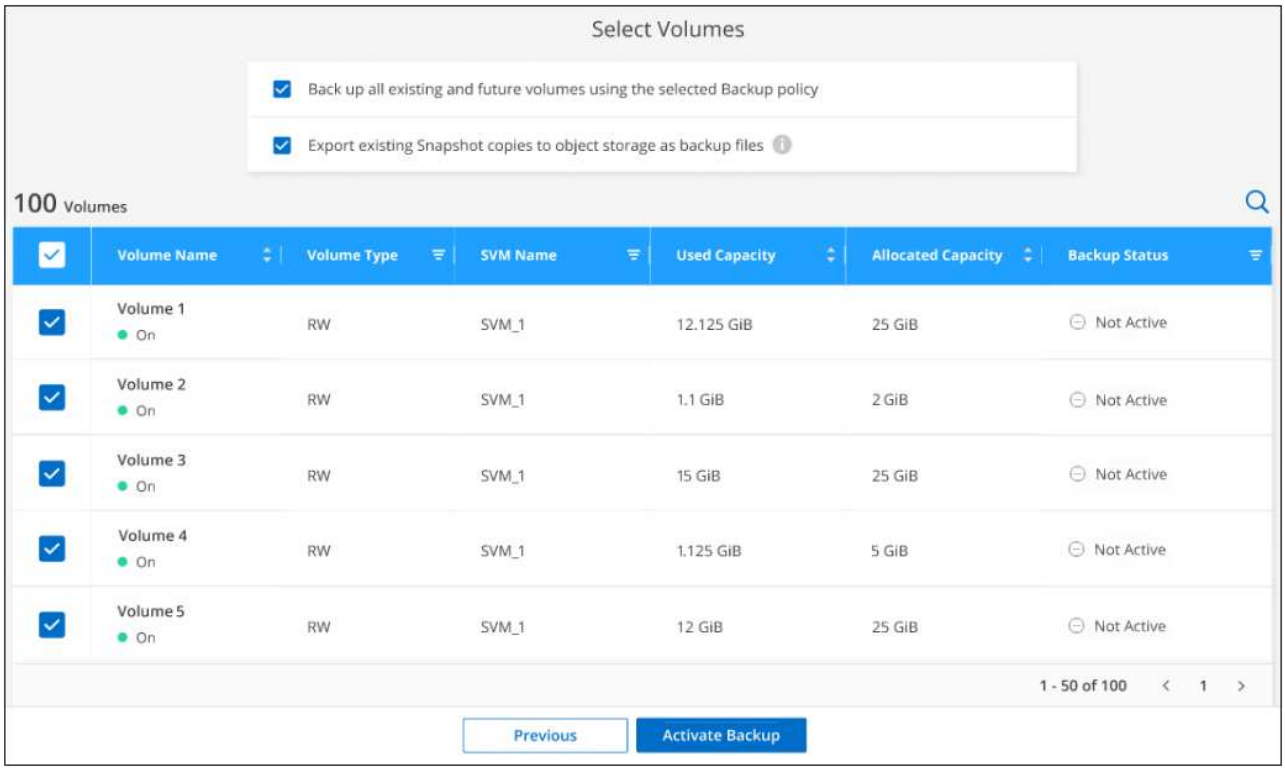
   c. Optional können Sie bei der Verwendung von ONTAP 9.11.1 und höher Ihre Backups vor dem Löschen und Ransomware-Angriffen schützen, indem Sie *DataLock und Ransomware Protection* konfigurieren. *DataLock* schützt Ihre Backup-Dateien vor Modified oder Deleted, und *Ransomware Protection* scannt Ihre Backup-Dateien, um nach Anzeichen für einen Ransomware-Angriff in Ihren Backup-Dateien zu suchen. "Erfahren Sie mehr über die verfügbaren DataLock-Einstellungen".



   Wichtig: Wenn Sie DataLock verwenden möchten, müssen Sie es bei der Aktivierung von Cloud Backup in Ihrer ersten Richtlinie aktivieren.

4. Wählen Sie auf der Seite Volumes auswählen die Volumes aus, für die ein Backup mit der definierten Backup-Richtlinie gesichert werden soll. Falls Sie bestimmten Volumes unterschiedliche Backup-Richtlinien zuweisen möchten, können Sie später zusätzliche Richtlinien erstellen und auf diese Volumes anwenden.

- Um alle bestehenden Volumes und Volumes zu sichern, die in der Zukunft hinzugefügt wurden, markieren Sie das Kontrollkästchen „Alle bestehenden und zukünftigen Volumen sichern…“. Wir empfehlen diese Option, damit alle Ihre Volumes gesichert werden und Sie nie vergessen müssen, Backups für neue Volumes zu aktivieren.
- Um nur vorhandene Volumes zu sichern, aktivieren Sie das Kontrollkästchen in der Titelzeile (☑ Volume Name).
- Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume (☑ Volume_1).



- Wenn es lokale Snapshot-Kopien für Lese-/Schreib-Volumes in dieser Arbeitsumgebung gibt, die dem Backup-Schedule-Label entsprechen, das Sie gerade für diese Arbeitsumgebung ausgewählt haben (z. B. täglich, wöchentlich usw.), wird eine zusätzliche Eingabeaufforderung angezeigt: „Export vorhandener Snapshot Kopien in Objekt-Storage als Backup-Kopien“. Aktivieren Sie dieses Kontrollkästchen, wenn alle historischen Snapshots als Backup-Dateien in Objekt-Storage kopiert werden sollen, um sicherzustellen, dass die umfassendste Sicherung für Ihre Volumes gewährleistet ist.

5. Klicken Sie auf **Activate Backup** und Cloud Backup beginnt die Erstellung der ersten Backups jedes ausgewählten Volumes.

Ergebnis

Ein S3-Bucket wird automatisch in dem Service-Konto erstellt, das durch den S3-Zugriffsschlüssel und den eingegebenen Geheimschlüssel angegeben ist und die Backup-Dateien dort gespeichert werden. Das Dashboard für Volume Backup wird angezeigt, sodass Sie den Status der Backups überwachen können. Sie können den Status von Backup- und Wiederherstellungsjobs auch mit dem überwachen "Fenster Job-Überwachung".

Was kommt als Nächstes?

- Das können Sie "Management von Backup Files und Backup-Richtlinien". Dies umfasst das Starten und Stoppen von Backups, das Löschen von Backups, das Hinzufügen und Ändern des Backup-Zeitplans und

vieles mehr.

- Das können Sie "Management von Backup-Einstellungen auf Cluster-Ebene". Dies umfasst die Änderung der Storage-Schlüssel, die ONTAP für den Zugriff auf den Cloud-Storage verwendet, die Änderung der verfügbaren Netzwerkbandbreite für das Hochladen von Backups in den Objekt-Storage, die Änderung der automatischen Backup-Einstellung für zukünftige Volumes und vieles mehr.
- Das können Sie auch "Wiederherstellung von Volumes, Ordnern oder einzelnen Dateien aus einer Sicherungsdatei" Auf ein lokales ONTAP System zugreifen:

Verwalten von Backups für Ihre ONTAP Systeme

Sie können die Backups für Ihre Cloud Volumes ONTAP und lokalen ONTAP Systeme verwalten, indem Sie den Backup-Zeitplan ändern, neue Backup-Richtlinien erstellen, Volume-Backups aktivieren/deaktivieren, Backups anhalten, Backups löschen und vieles mehr.

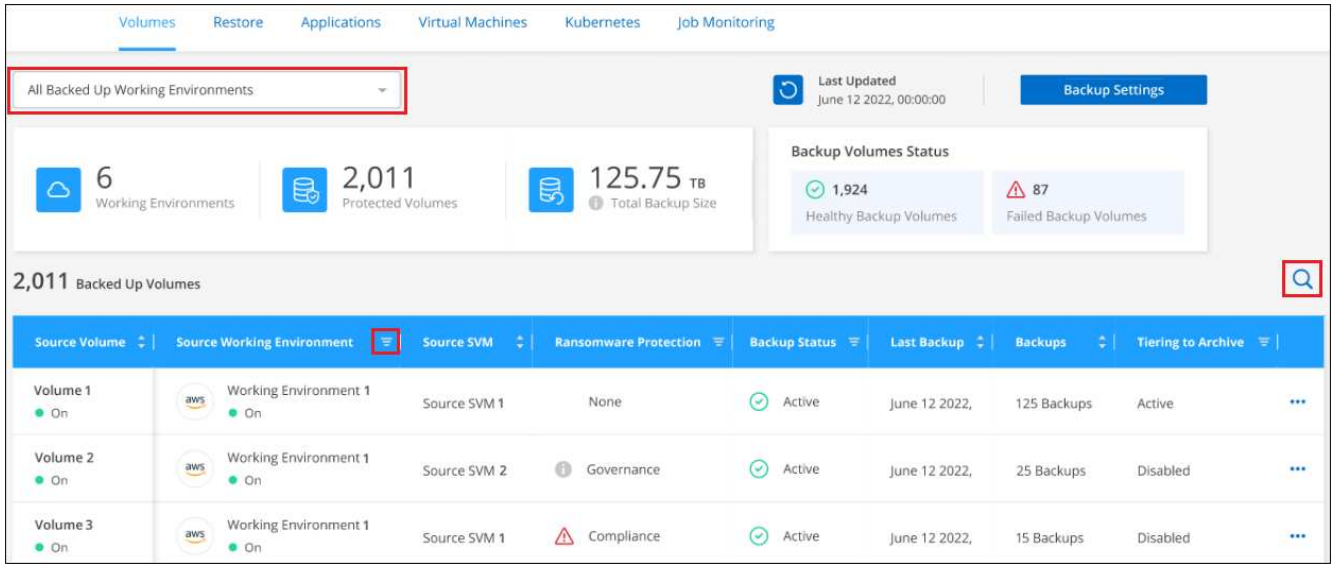
> Backup-Dateien lassen sich nicht direkt in der Umgebung Ihrer Cloud-Provider managen oder ändern. Dies kann die Dateien beschädigen und zu einer nicht unterstützten Konfiguration führen.

Anzeigen der Volumes, die gesichert werden

Sie können eine Liste aller Volumes anzeigen, die derzeit im Backup Dashboard gesichert werden.

Schritte

1. Wählen Sie im Menü BlueXP die Option **Schutz > Sicherung und Wiederherstellung**.
2. Klicken Sie auf die Registerkarte **Volumes**, um eine Liste der gesicherten Volumes für Cloud Volumes ONTAP und On-Premises ONTAP Systeme anzuzeigen.



Wenn Sie in bestimmten Arbeitsumgebungen nach bestimmten Volumes suchen, können Sie die Liste nach Arbeitsumgebung und Volumen verfeinern, oder Sie können den Suchfilter verwenden.

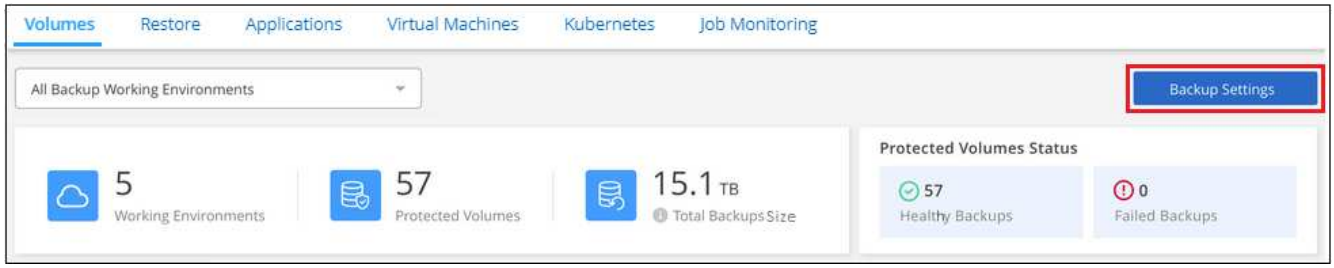
Aktivieren und Deaktivieren von Backups von Volumes

Sie können Backups für neue Volumes aktivieren, wenn diese derzeit nicht gesichert werden. Darüber hinaus können Sie Backups auch für Volumes aktivieren, die Sie zuvor deaktiviert hatten.

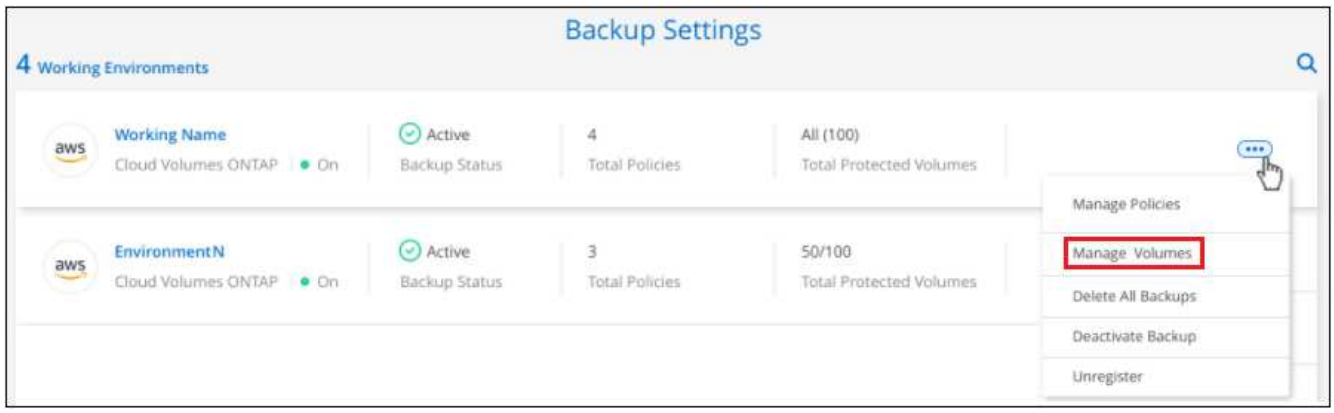
Sie können Backups für Volumes deaktivieren, sodass keine weiteren Backups erstellt werden. Dadurch wird auch die Möglichkeit deaktiviert, Volume-Daten aus einer Sicherungsdatei wiederherzustellen. So können Sie im Prinzip alle Backup- und Wiederherstellungsaktivitäten für einen bestimmten Zeitraum anhalten. Alle bestehenden Backups werden nicht gelöscht, so dass Sie weiterhin von Ihrem Cloud-Provider für Objekt-Storage-Kosten für die Kapazität, die Ihre Backups verwenden, es sei denn, Sie Löschen Sie die Backups.

Schritte

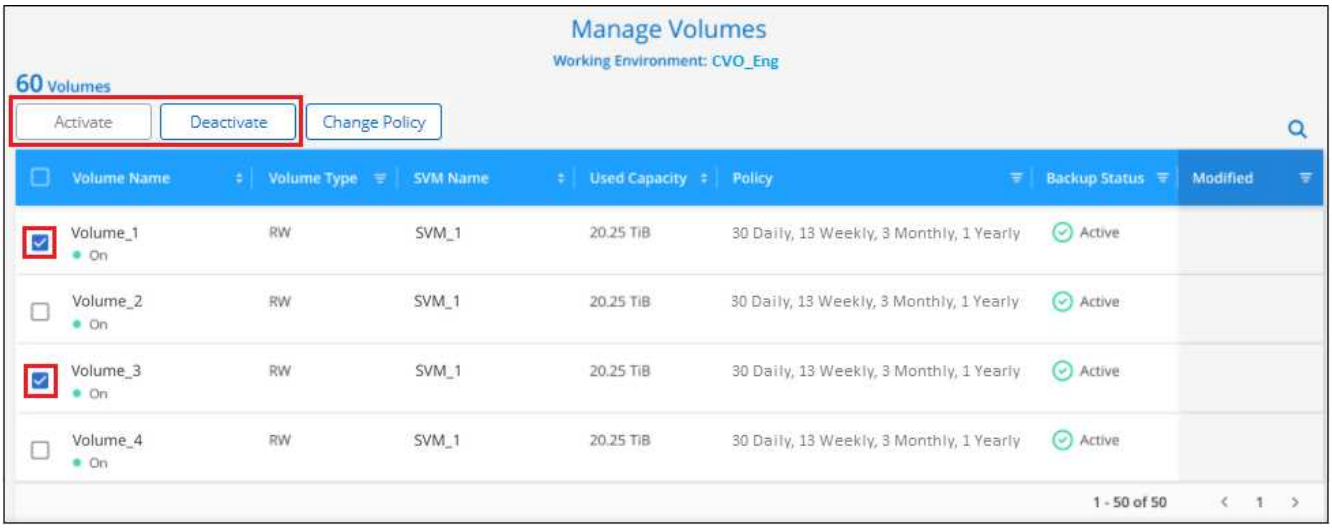
1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.



2. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Wählen Sie für die Arbeitsumgebung **Volumes verwalten** aus.



3. Aktivieren Sie das Kontrollkästchen für ein Volume oder ein Volume, das Sie ändern möchten, und klicken Sie dann auf **Aktivieren** oder **Deaktivieren**, je nachdem, ob Sie Backups für das Volume starten oder beenden möchten.



4. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.

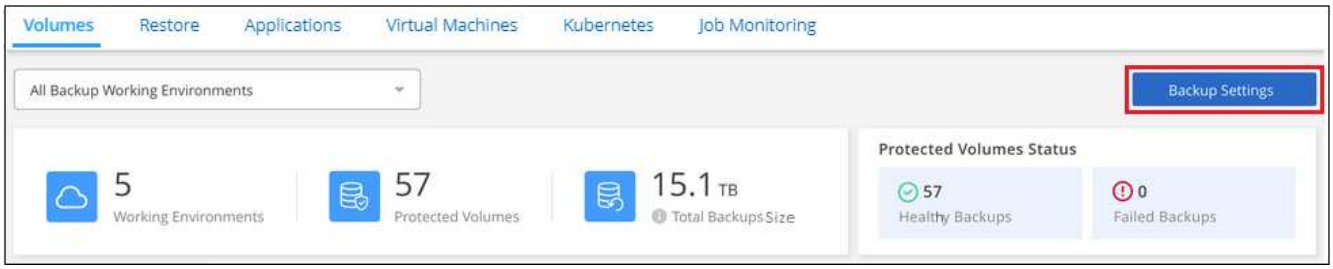
Bearbeiten einer vorhandenen Backup-Richtlinie

Sie können die Attribute für eine Backup-Richtlinie ändern, die derzeit auf Volumes in einer Arbeitsumgebung angewendet wird. Die Änderung der Backup-Richtlinie wirkt sich auf alle vorhandenen Volumes aus, die diese Richtlinie verwenden.

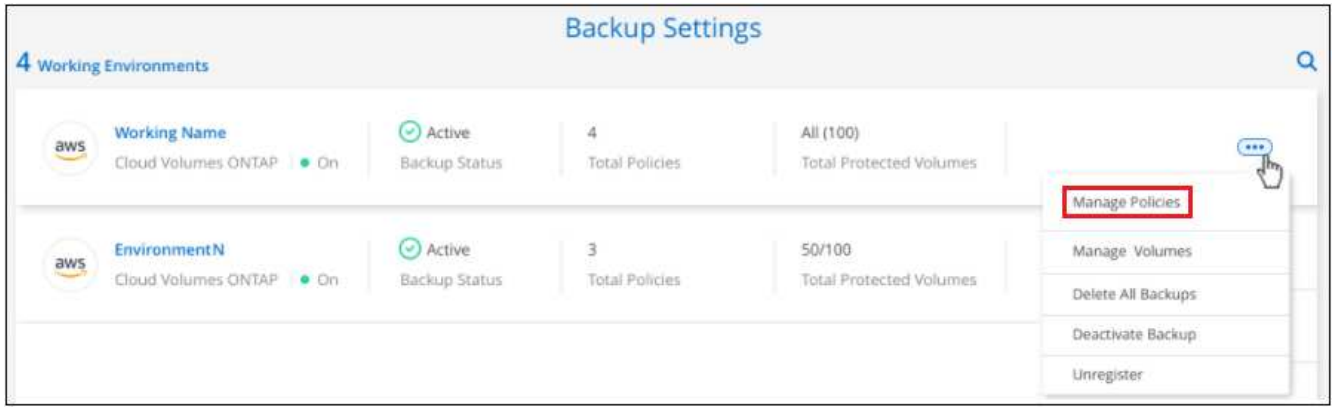
- Wenn Sie bei der Aktivierung von Cloud Backup für diesen Cluster *DataLock und Ransomware Protection* aktiviert haben, müssen alle Richtlinien, die Sie bearbeiten, mit derselben DataLock-Einstellung (Governance oder Compliance) konfiguriert werden. Und wenn Sie *DataLock und Ransomware Protection* bei der Aktivierung von Cloud Backup nicht aktiviert haben, können Sie DataLock jetzt nicht aktivieren.
- Wenn Sie bei der Erstellung von Backups auf AWS *S3 Glacier* oder *S3 Glacier Deep Archive* in Ihrer ersten Backup-Richtlinie bei der Aktivierung von Cloud Backup ausgewählt haben, ist dieser Tier die einzige Archiv-Tier, die bei der Bearbeitung von Backup-Richtlinien verfügbar ist. Falls Sie in Ihrer ersten Backup-Richtlinie keine Archivebene ausgewählt haben, ist *S3 Glacier* die einzige Archivoption beim Bearbeiten einer Richtlinie.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.

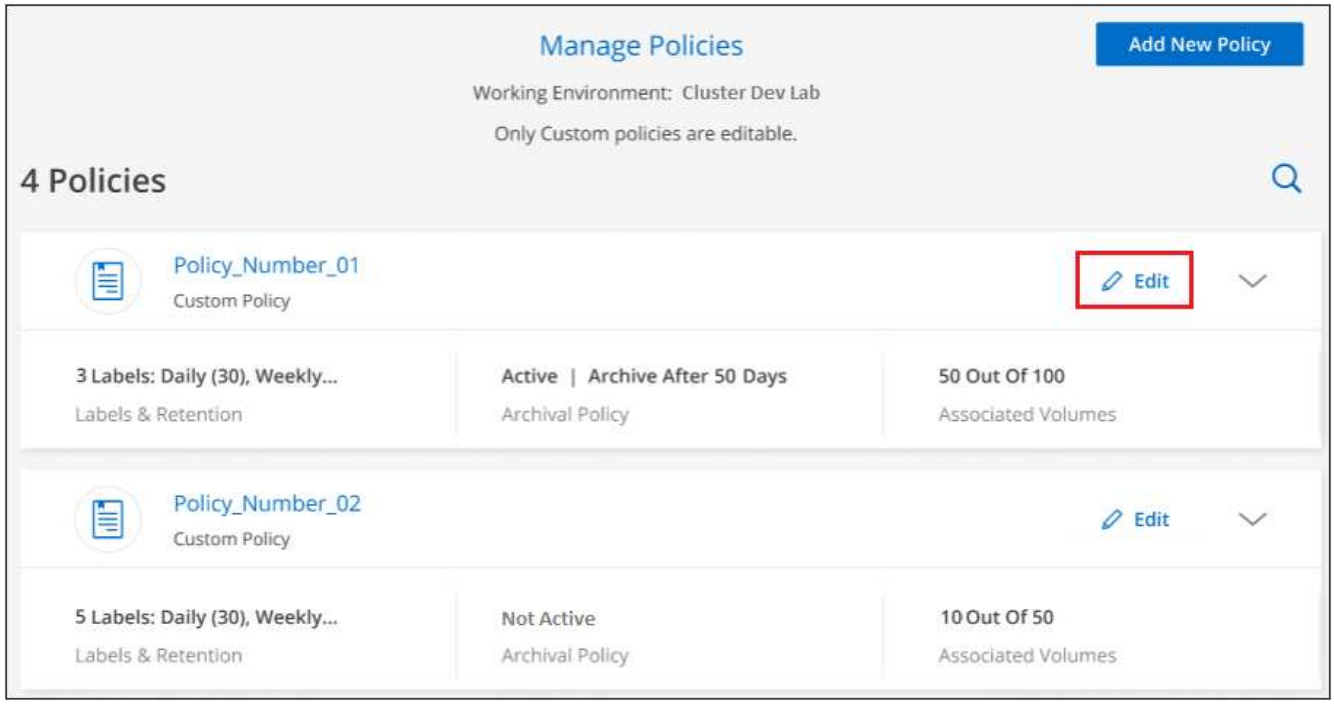


2. Klicken Sie auf der Seite „ Backup Settings_“ auf ••• Wählen Sie für die Arbeitsumgebung, in der Sie die Richtlinieneinstellungen ändern möchten, und wählen Sie **Richtlinien verwalten**.

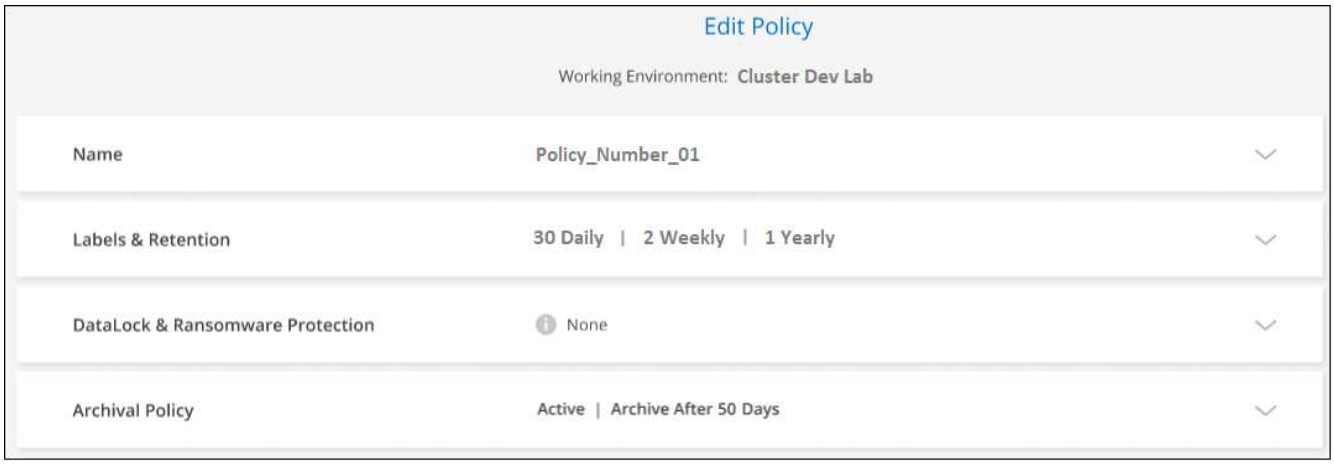


3. Klicken Sie auf der Seite *Policies verwalten* auf **Bearbeiten** für die Backup-Policy, die Sie in dieser Arbeitsumgebung ändern möchten.

   Hinweis: Klicken Sie auf ⌄ Um die vollständigen Details für die Richtlinie anzuzeigen.

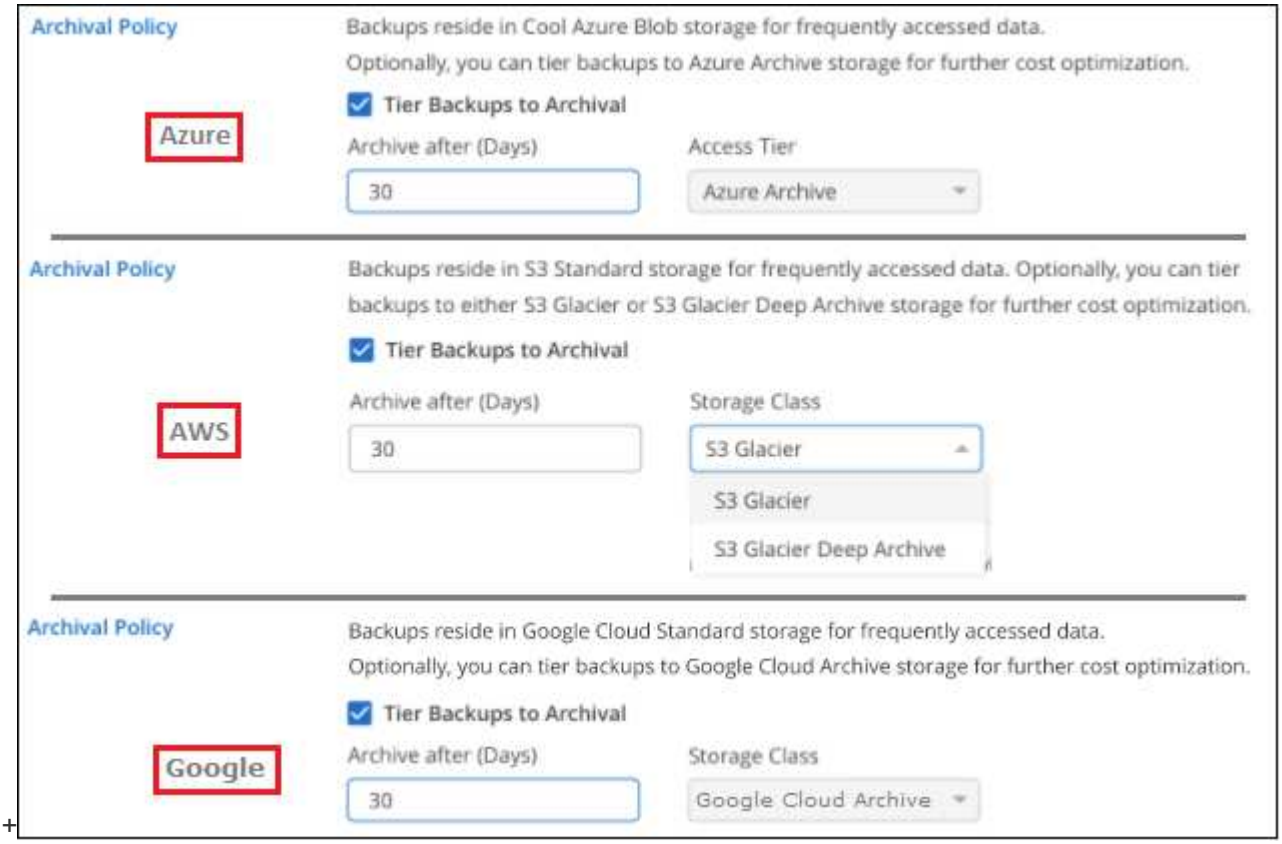


4. Klicken Sie auf der Seite *Edit Policy* auf ⌄ Erweitern Sie den Abschnitt *Labels & Retention*, um den Zeitplan und/oder die Backup-Aufbewahrung zu ändern, und klicken Sie auf **Speichern**.



Wenn in Ihrem Cluster ONTAP 9.10.1 oder höher ausgeführt wird, haben Sie außerdem die Möglichkeit, das Tiering von Backups in Archiv-Storage nach einer bestimmten Anzahl von Tagen zu aktivieren oder zu deaktivieren.

"Erfahren Sie mehr über die Verwendung von AWS Archiv-Storage".



+

+ Beachten Sie, dass alle Backup-Dateien, die in einen Archiv-Storage verschoben wurden, in diesem Tier belassen werden, wenn Sie die Tiering-Backups zur Archivierung anhalten - sie werden nicht automatisch zurück in die Standard-Tier verschoben. Es werden nur neue Volume-Backups in der Standard-Tier gespeichert.

Hinzufügen einer neuen Backup-Richtlinie

Wenn Sie Cloud-Backup für eine Arbeitsumgebung aktivieren, werden alle ausgewählten Volumes mit der von

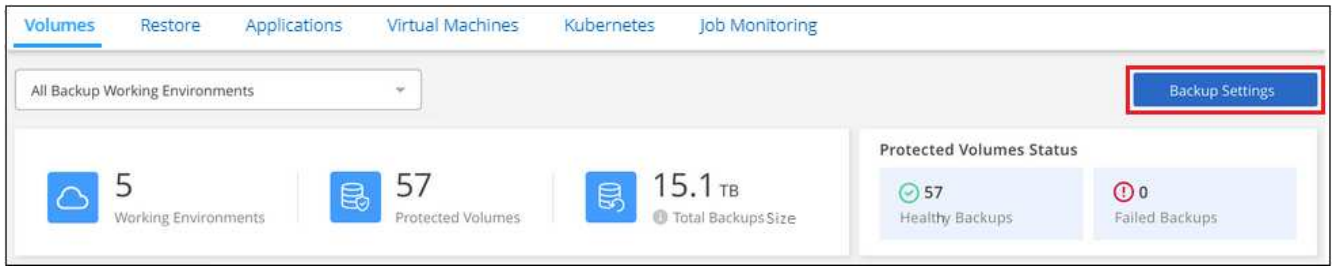
Ihnen definierten Standard-Backup-Richtlinie gesichert. Um bestimmten Volumes mit verschiedenen Recovery Point Objectives (RPOs) unterschiedliche Backup-Richtlinien zuzuweisen, können Sie zusätzliche Richtlinien für diesen Cluster erstellen und diese Richtlinien anderen Volumes zuweisen.

Wenn Sie eine neue Sicherungsrichtlinie auf bestimmte Volumes in einer Arbeitsumgebung anwenden möchten, müssen Sie zunächst die Sicherungsrichtlinie zur Arbeitsumgebung hinzufügen. Dann können Sie das die vorhandenen Volumes zugewiesen ist,Wenden Sie die Richtlinie auf Volumes in dieser Arbeitsumgebung an.

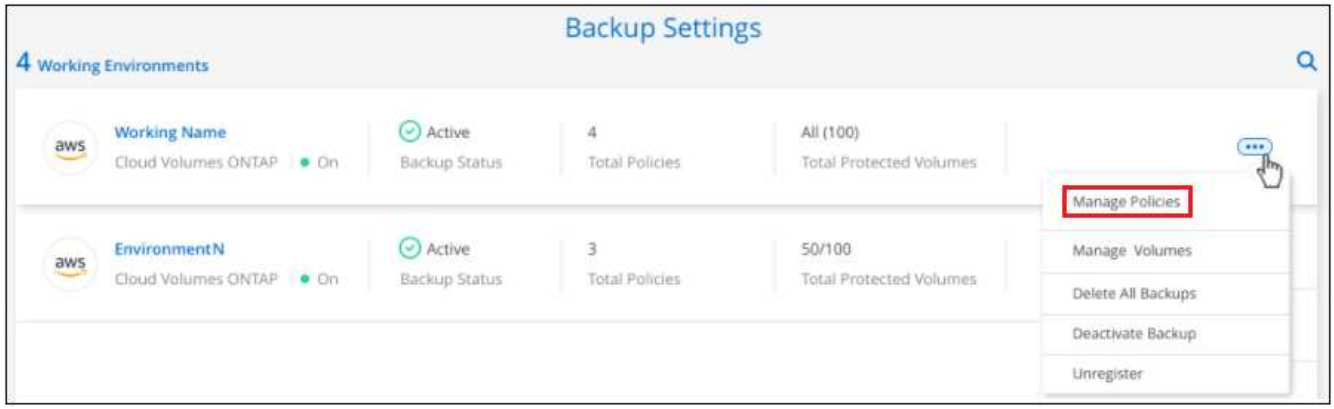
- Wenn Sie bei der Aktivierung von Cloud Backup für diesen Cluster *DataLock und Ransomware Protection* aktiviert haben, müssen alle von Ihnen erstellten zusätzlichen Richtlinien mit derselben DataLock-Einstellung (Governance oder Compliance) konfiguriert werden. Und wenn Sie bei der Aktivierung von Cloud Backup *DataLock und Ransomware Protection* nicht aktiviert haben, können Sie keine neuen Richtlinien erstellen, die DataLock verwenden.
- Wenn Sie bei der Erstellung von Backups auf AWS *S3 Glacier* oder *S3 Glacier Deep Archive* in Ihrer ersten Backup-Richtlinie bei der Aktivierung von Cloud Backup ausgewählt haben, wird dieser Tier die einzige Archiv-Tier sein, die für zukünftige Backup-Richtlinien für diesen Cluster verfügbar ist. Falls Sie in Ihrer ersten Backup-Richtlinie keine Archiv-Tier ausgewählt haben, ist *S3 Glacier* die einzige Archivoption für zukünftige Richtlinien.

Schritte

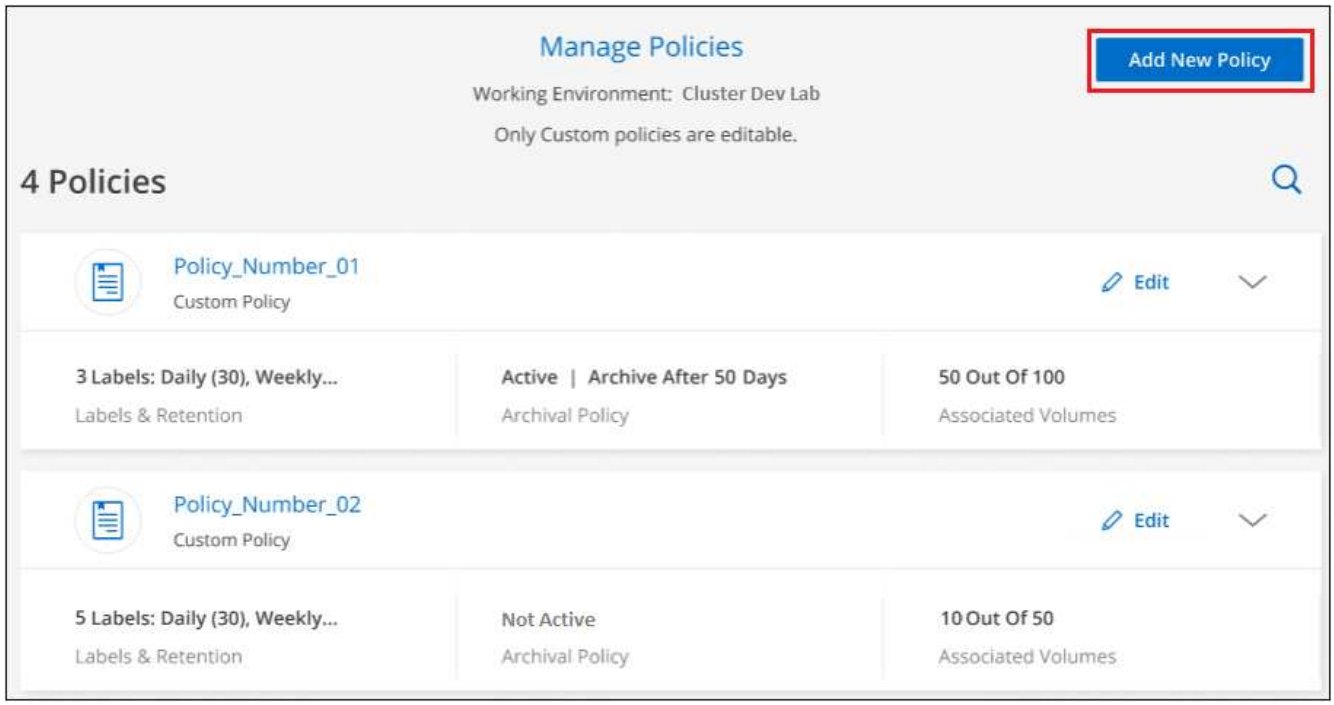
1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.



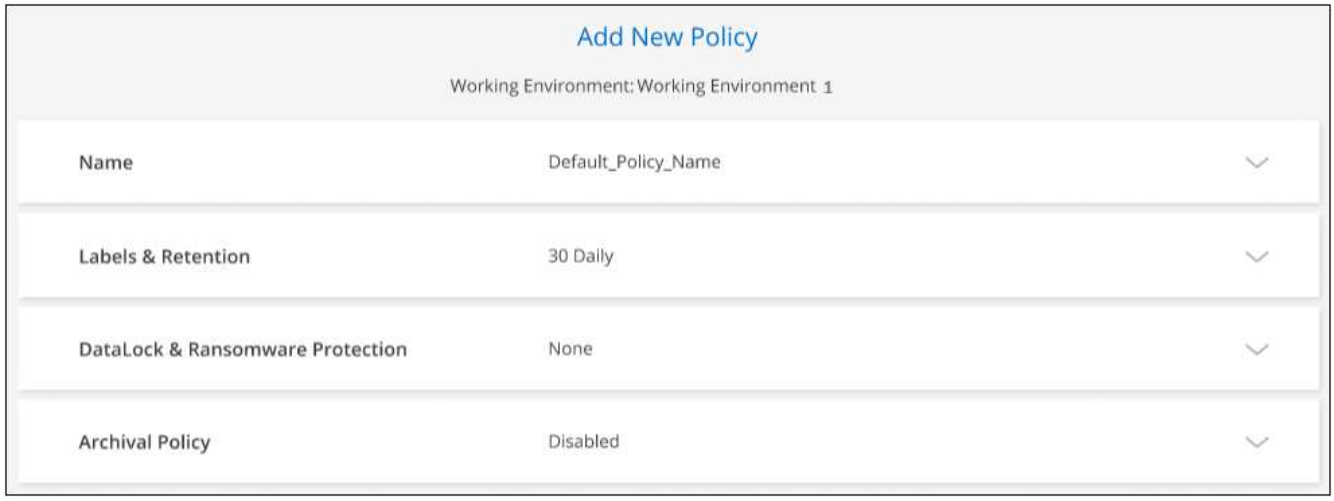
2. Klicken Sie auf der Seite „ Backup Settings_“ auf ••• Wählen Sie für die Arbeitsumgebung, in der Sie die neue Richtlinie hinzufügen möchten, und wählen Sie **Richtlinien verwalten**.



3. Klicken Sie auf der Seite *Policies verwalten* auf **Neue Richtlinie hinzufügen**.

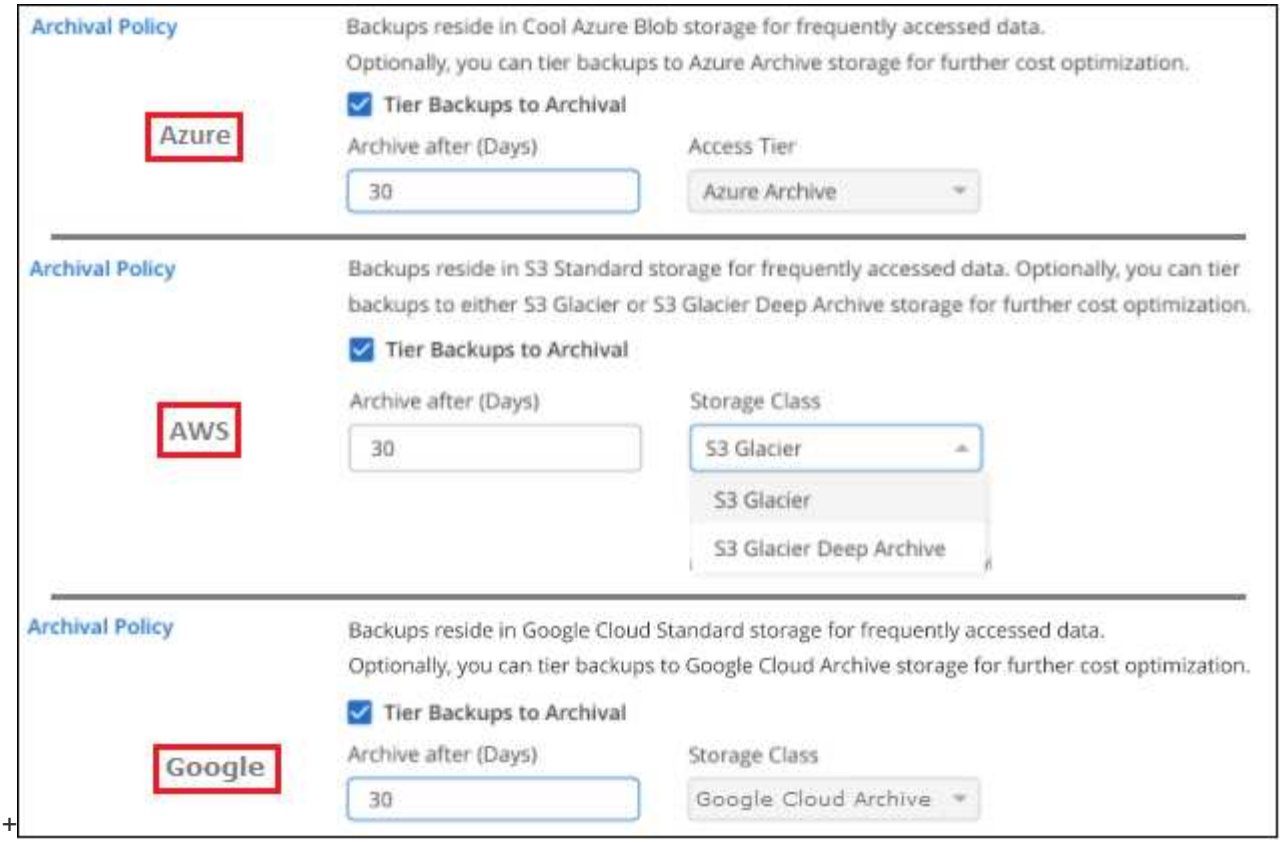


4. Klicken Sie auf der Seite „ Neue Richtlinie hinzufügen_“ auf ⌄ Erweitern Sie den Abschnitt *Labels & Retention*, um den Zeitplan und die Backup-Aufbewahrung zu definieren, und klicken Sie auf **Speichern**.



Wenn in Ihrem Cluster ONTAP 9.10.1 oder höher ausgeführt wird, haben Sie außerdem die Möglichkeit, das Tiering von Backups in Archiv-Storage nach einer bestimmten Anzahl von Tagen zu aktivieren oder zu deaktivieren.

"Erfahren Sie mehr über die Verwendung von AWS Archiv-Storage".



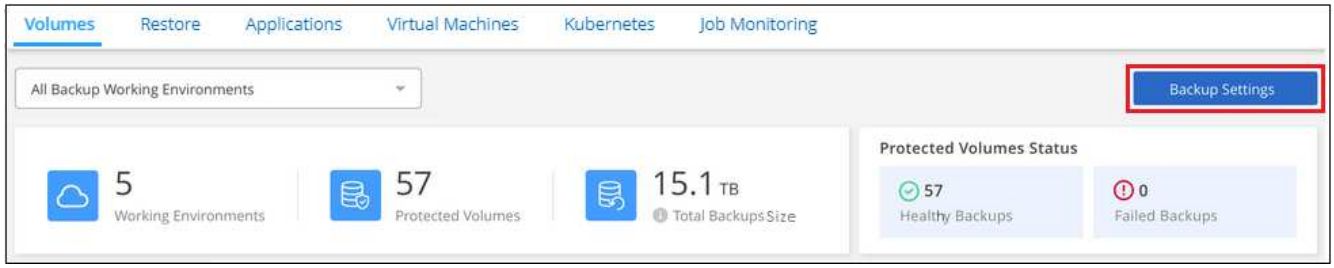
Ändern der Richtlinie, die vorhandenen Volumes zugewiesen ist

Sie können die Ihrer vorhandenen Volumes zugewiesene Backup-Richtlinie ändern, wenn Sie die Häufigkeit der Durchführung von Backups ändern möchten oder den Aufbewahrungswert ändern möchten.

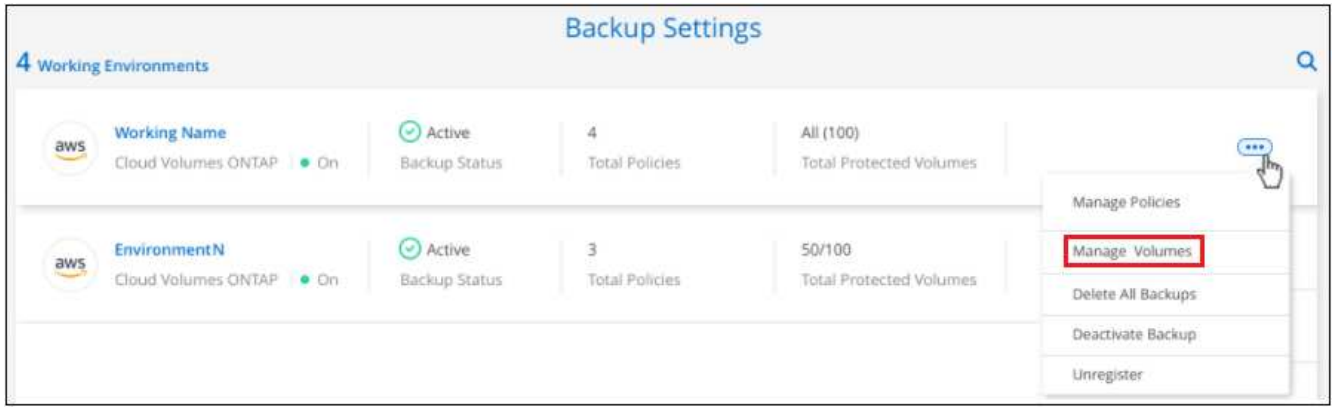
Beachten Sie, dass die Richtlinie, die Sie auf die Volumes anwenden möchten, bereits vorhanden sein muss. Erfahren Sie, wie Sie eine neue Backup-Richtlinie für eine Arbeitsumgebung hinzufügen.

Schritte

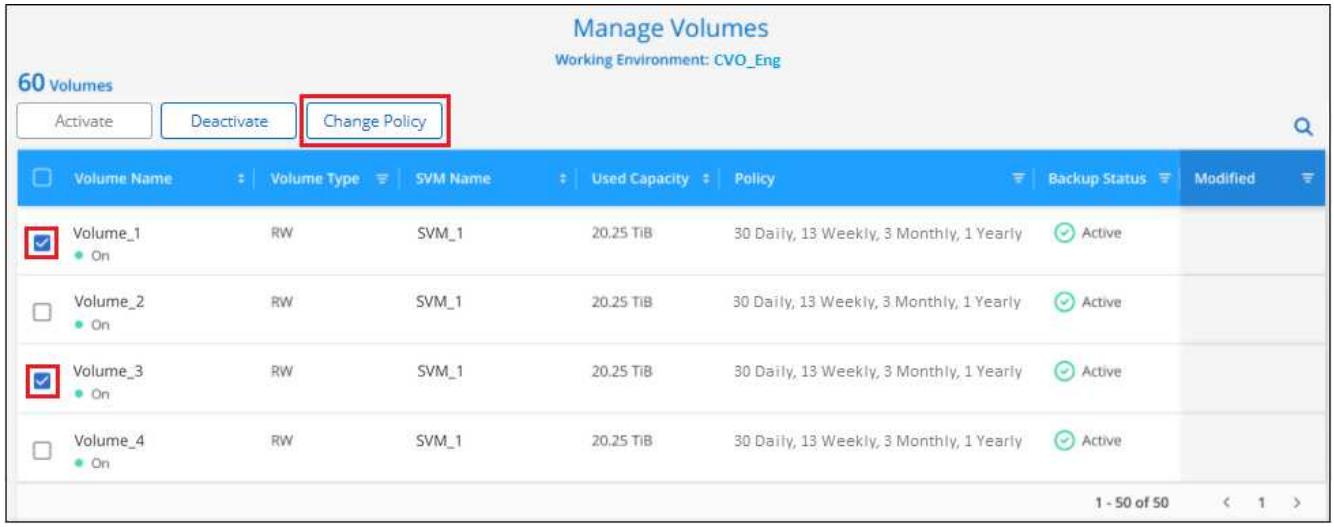
1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.



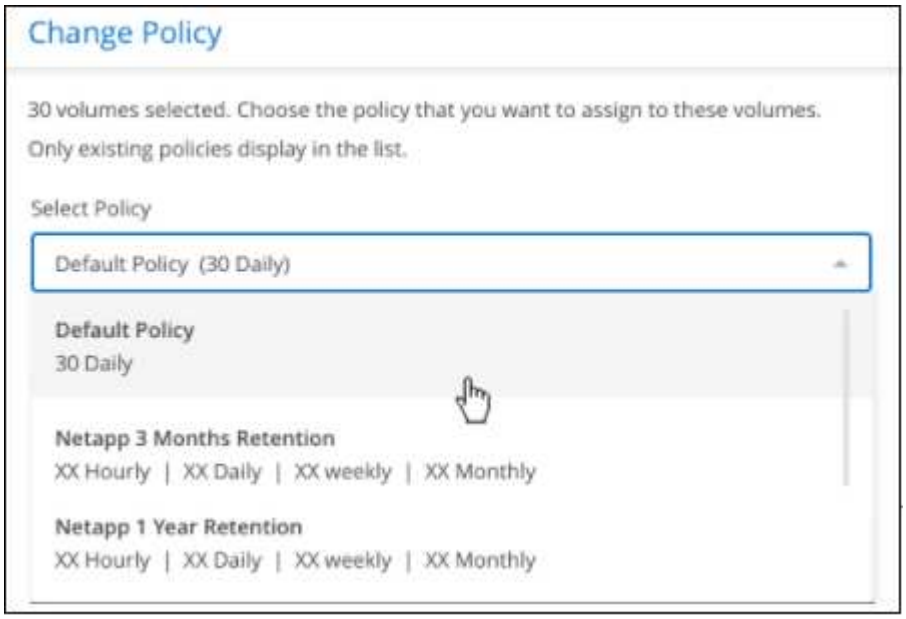
2. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Wählen Sie für die Arbeitsumgebung, in der die Volumina vorhanden sind, **Volumes verwalten** aus.



3. Aktivieren Sie das Kontrollkästchen für ein Volume oder Volumes, für das Sie die Richtlinie ändern möchten, und klicken Sie dann auf **Richtlinie ändern**.



4. Wählen Sie auf der Seite *Richtlinie ändern* die Richtlinie aus, die Sie auf die Volumes anwenden möchten, und klicken Sie auf **Richtlinie ändern**.



> Wenn Sie *DataLock und Ransomware Protection* in der ursprünglichen Richtlinie aktiviert haben, wenn Sie Cloud Backup für diesen Cluster aktivieren, sehen Sie nur andere Richtlinien, die mit DataLock konfiguriert wurden. Und wenn Sie bei der Aktivierung von Cloud Backup *DataLock und Ransomware Protection* nicht aktiviert haben, werden nur andere Richtlinien angezeigt, die DataLock nicht konfiguriert haben.

5. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.

Erstellung einer manuellen Volume-Sicherung zu jeder Zeit

Sie können jederzeit ein On-Demand-Backup erstellen, um den aktuellen Status des Volumes zu erfassen. Dies kann hilfreich sein, wenn auf einem Volume sehr wichtige Änderungen vorgenommen wurden und Sie nicht darauf warten möchten, dass das nächste geplante Backup zur Sicherung dieser Daten gesichert wird oder wenn das Volume nicht aktuell gesichert wird und Sie den aktuellen Zustand erfassen möchten.

Der Backup-Name enthält den Zeitstempel, sodass Sie Ihr On-Demand Backup aus anderen geplanten Backups identifizieren können.

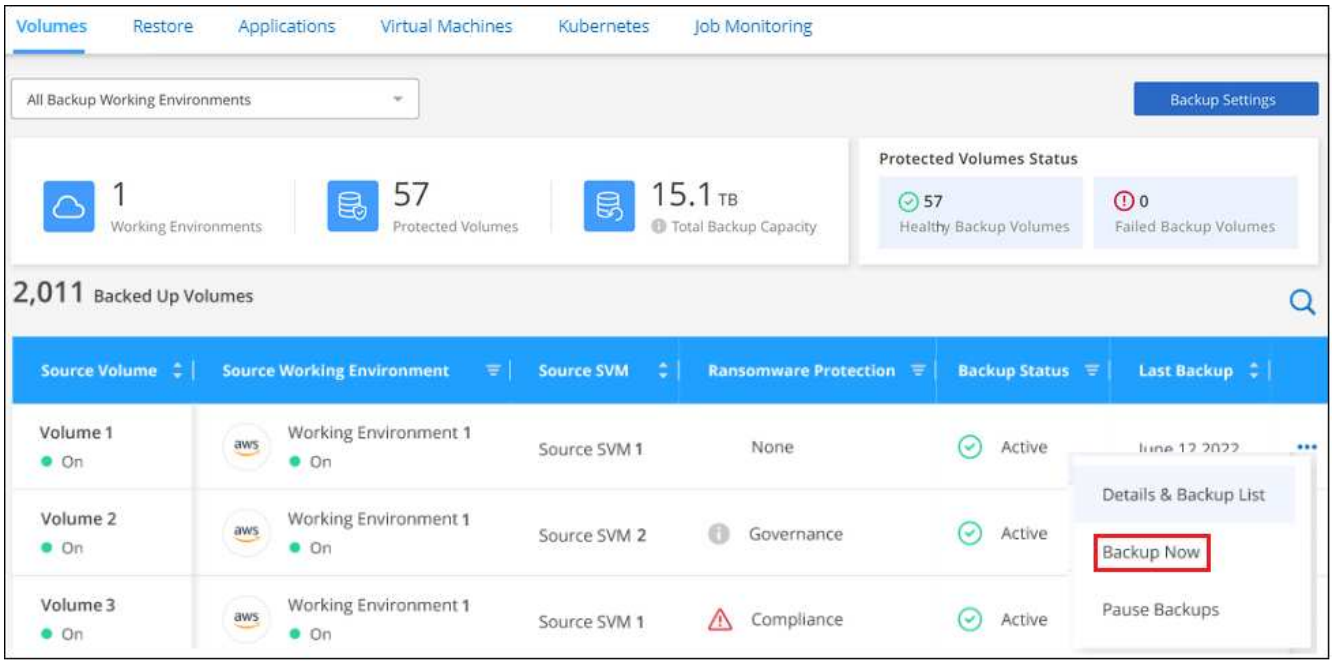
Wenn Sie *DataLock and Ransomware Protection* aktiviert haben, wenn Sie Cloud Backup für diesen Cluster aktivieren, wird das On-Demand-Backup auch mit DataLock konfiguriert, und die Aufbewahrungsfrist beträgt 30 Tage. Ransomware-Scans werden für Ad-hoc-Backups nicht unterstützt. "Erfahren Sie mehr über DataLock und Ransomware-Schutz".

Beachten Sie, dass beim Erstellen eines Ad-hoc-Backups ein Snapshot auf dem Quell-Volume erstellt wird. Da dieser Snapshot nicht Teil eines normalen Snapshot-Zeitplans ist, wird er nicht rotiert. Nach Abschluss des Backups kann dieser Snapshot manuell vom Quell-Volume gelöscht werden. Dadurch werden Blöcke freigegeben, die mit diesem Snapshot verbunden sind. Der Name des Snapshots beginnt mit `cbs-snapshot-adhoc-`. "Informationen zum Löschen eines Snapshots mit der ONTAP-CLI finden Sie unter".

> Volume-Backups werden auf Datensicherungs-Volumes nicht unterstützt.

Schritte

1. Klicken Sie auf der Registerkarte **Volumes** auf ••• Wählen Sie für das Volume die Option **Jetzt sichern** aus.



In der Spalte Backup Status für dieses Volume wird „in progress“ angezeigt, bis das Backup erstellt wird.

Anzeigen der Liste der Backups für jedes Volume

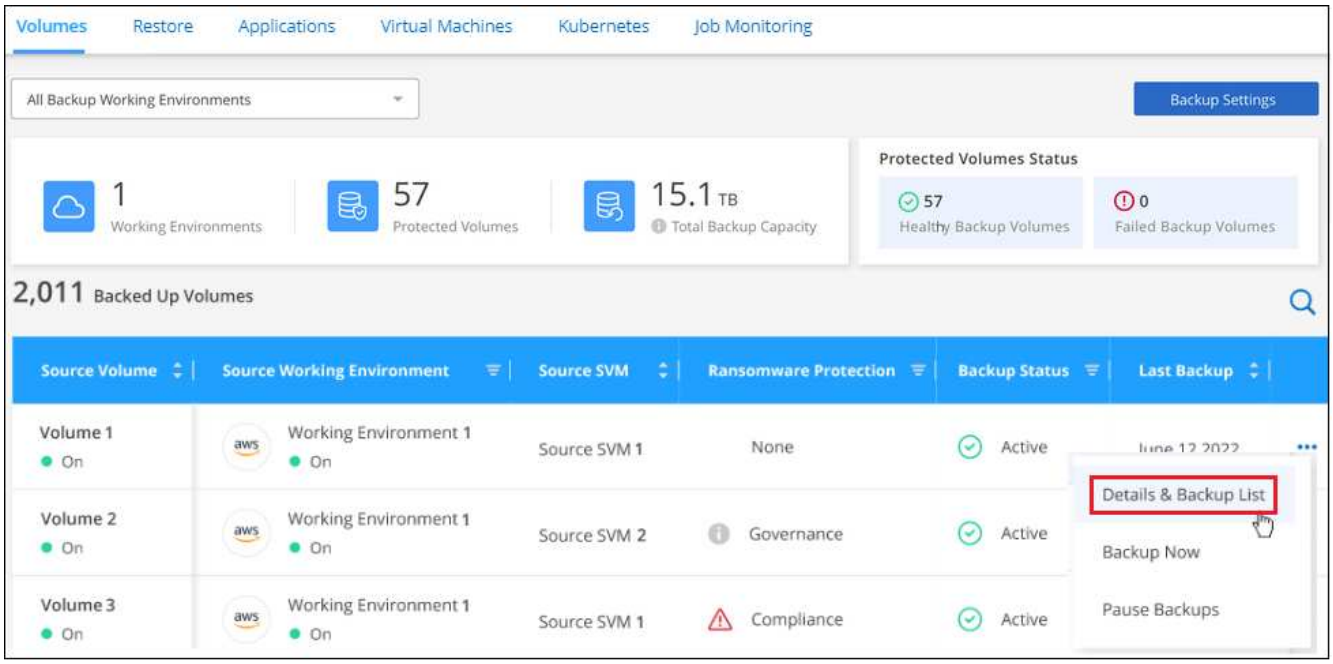
Sie können eine Liste aller Backup-Dateien anzeigen, die für jedes Volume vorhanden sind. Auf dieser Seite werden Details zum Quell-Volume, zum Zielort und zu Backup-Details wie zum Beispiel zum letzten Backup, zur aktuellen Backup-Richtlinie, zur Größe der Sicherungsdatei und mehr angezeigt.

Auf dieser Seite können Sie außerdem die folgenden Aufgaben ausführen:

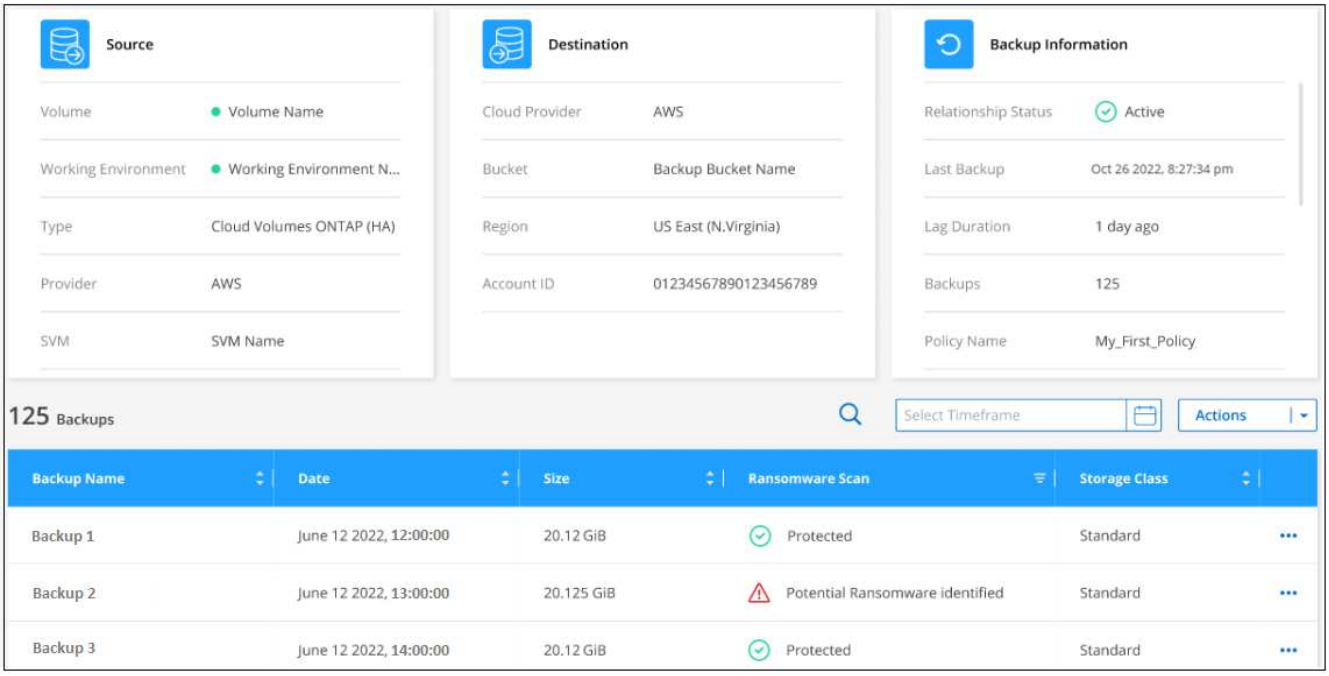
- Löschen Sie alle Sicherungsdateien für das Volume
- Löschen einzelner Backup-Dateien für das Volume
- Backup-Bericht für das Volume herunterladen

Schritte

1. Klicken Sie auf der Registerkarte **Volumes** auf ••• Wählen Sie für das Quellvolume **Details & Sicherungsliste** aus.



Die Liste aller Sicherungsdateien wird zusammen mit Details zum Quell-Volume, dem Zielspeicherort und Backup-Details angezeigt.



Durchführung eines Ransomware-Scans bei einem Volume-Backup

NetApp Software zur Ransomware-Sicherung scannt Ihre Backup-Dateien, um nach einem Ransomware-Angriff zu suchen, wenn eine Backup-Datei erstellt wird und wenn Daten aus einer Backup-Datei wiederhergestellt werden. Darüber hinaus können Sie jederzeit einen Ransomware-Sicherungsscan bei Bedarf ausführen und die Usability einer bestimmten Backup-Datei überprüfen. Die Folgen sind besonders dann hilfreich, wenn Ransomware-Probleme auf einem bestimmten Volume gehabt haben und man überprüfen möchte, ob die Backups für das Volume nicht betroffen sind.

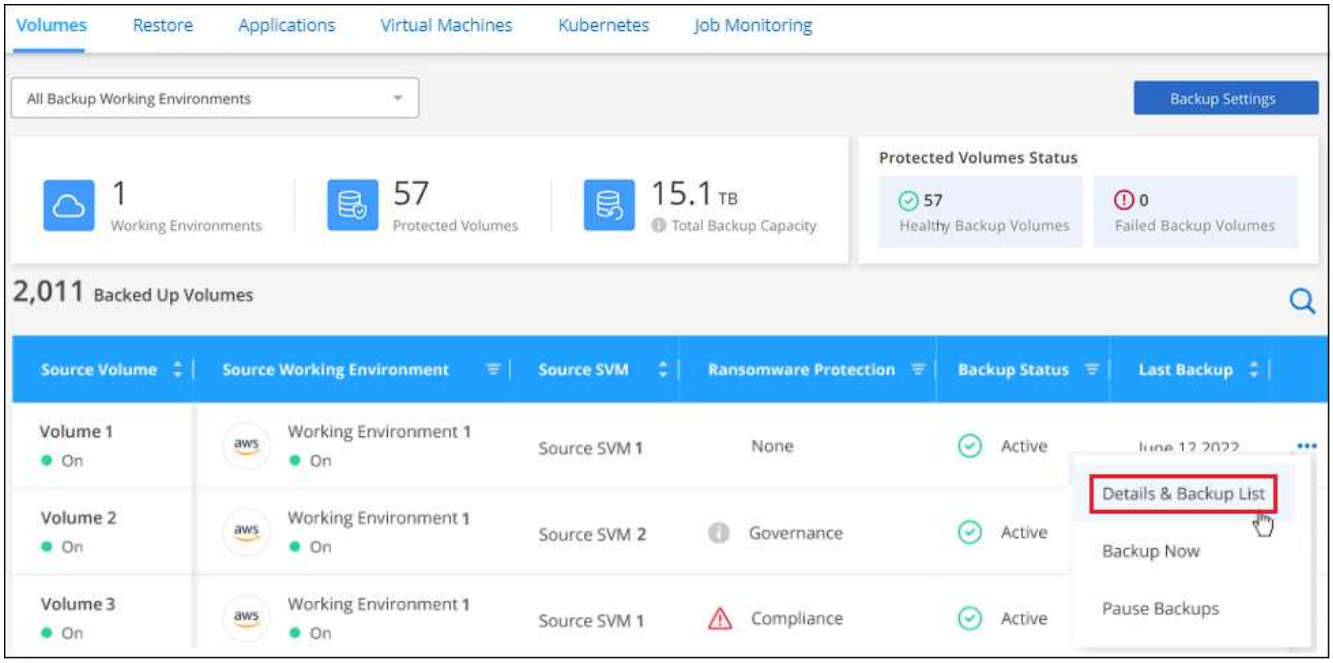
Diese Funktion ist nur verfügbar, wenn die Volume-Sicherung von einem System mit ONTAP 9.11.1 oder höher

erstellt wurde und wenn Sie *DataLock und Ransomware Protection* in der Backup-Policy aktiviert haben.

> Bei einem Ransomware-Scan muss die Sicherungsdatei in Ihre BlueXP-Umgebung (wo der Connector installiert ist) heruntergeladen werden. Bei der Implementierung des Connectors vor Ort können zusätzliche Kosten für den ausgehenden Datenverkehr von Ihrem Cloud-Provider anfallen. Daher empfehlen wir Ihnen, den Connector in der Cloud zu implementieren und sich in derselben Region wie der Bucket zu befinden, in der Ihre Backups gespeichert werden.

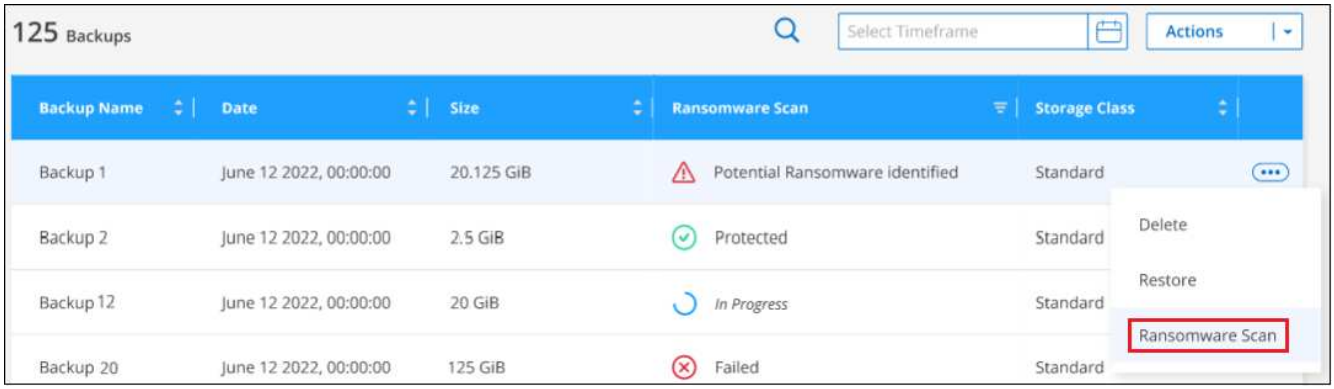
Schritte

1. Klicken Sie auf der Registerkarte **Volumes** auf ••• Wählen Sie für das Quellvolume **Details & Sicherungsliste** aus.



Die Liste aller Sicherungsdateien wird angezeigt.

2. Klicken Sie Auf ••• Für die Volume Backup Datei möchten Sie scannen und klicken Sie **Ransomware Scan**.



Die Spalte Ransomware Scan zeigt, dass der Scan gerade läuft.

Backups werden gelöscht

Mit Cloud Backup können Sie eine einzelne Backup-Datei löschen, alle Backups für ein Volume löschen oder alle Backups aller Volumes in einer Arbeitsumgebung löschen. Sie möchten eventuell alle Backups löschen, wenn Sie die Backups nicht mehr benötigen, oder wenn Sie das Quell-Volume gelöscht haben und alle Backups entfernen möchten.

Beachten Sie, dass Sie keine Sicherungsdateien löschen können, 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.

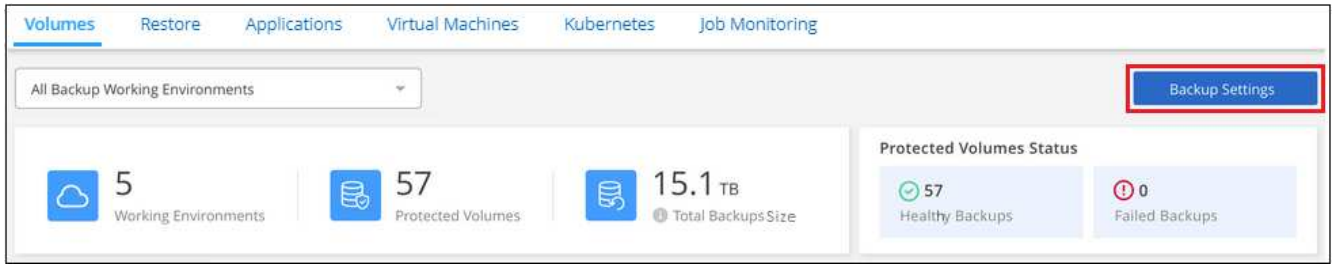
> Wenn Sie planen, eine Arbeitsumgebung oder ein Cluster mit Backups zu löschen, müssen Sie die Backups *löschen, bevor Sie das System löschen. Cloud Backup nicht automatisch löschen Backups, wenn Sie ein System löschen, und es gibt keine aktuelle Unterstützung in der UI, die Backups zu löschen, nachdem das System gelöscht wurde. Für alle verbleibenden Backups werden weiterhin die Kosten für Objekt-Storage in Rechnung gestellt.

Löschen aller Sicherungsdateien für eine Arbeitsumgebung

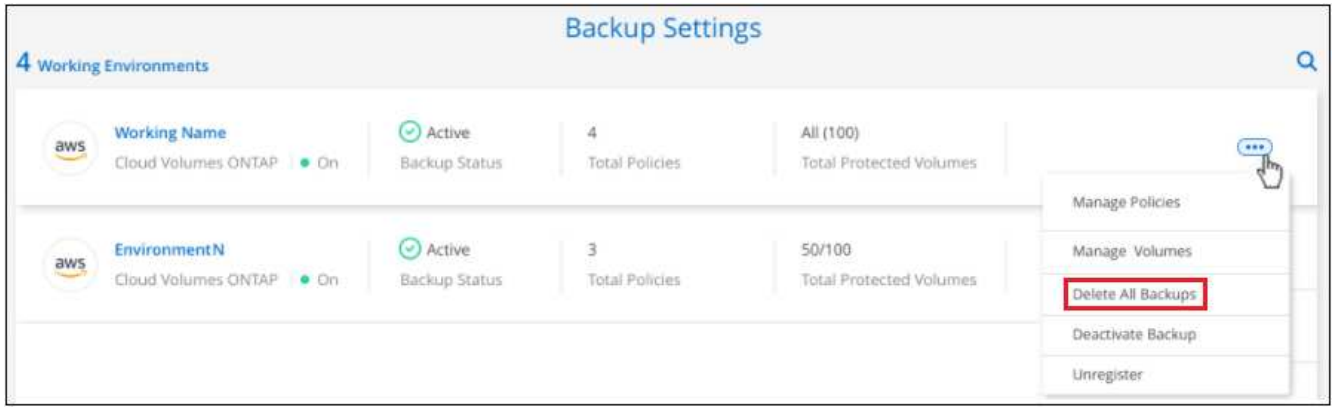
Durch das Löschen aller Backups für eine Arbeitsumgebung werden keine zukünftigen Backups von Volumes in dieser Arbeitsumgebung deaktiviert. Wenn Sie die Erstellung von Backups aller Volumes in einer Arbeitsumgebung beenden möchten, können Sie Backups deaktivieren Wie hier beschrieben.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.



2. Klicken Sie Auf ••• Für die Arbeitsumgebung, in der Sie alle Backups löschen und **Alle Backups löschen** auswählen möchten.



3. Geben Sie im Bestätigungsdialogfeld den Namen der Arbeitsumgebung ein und klicken Sie auf **Löschen**.

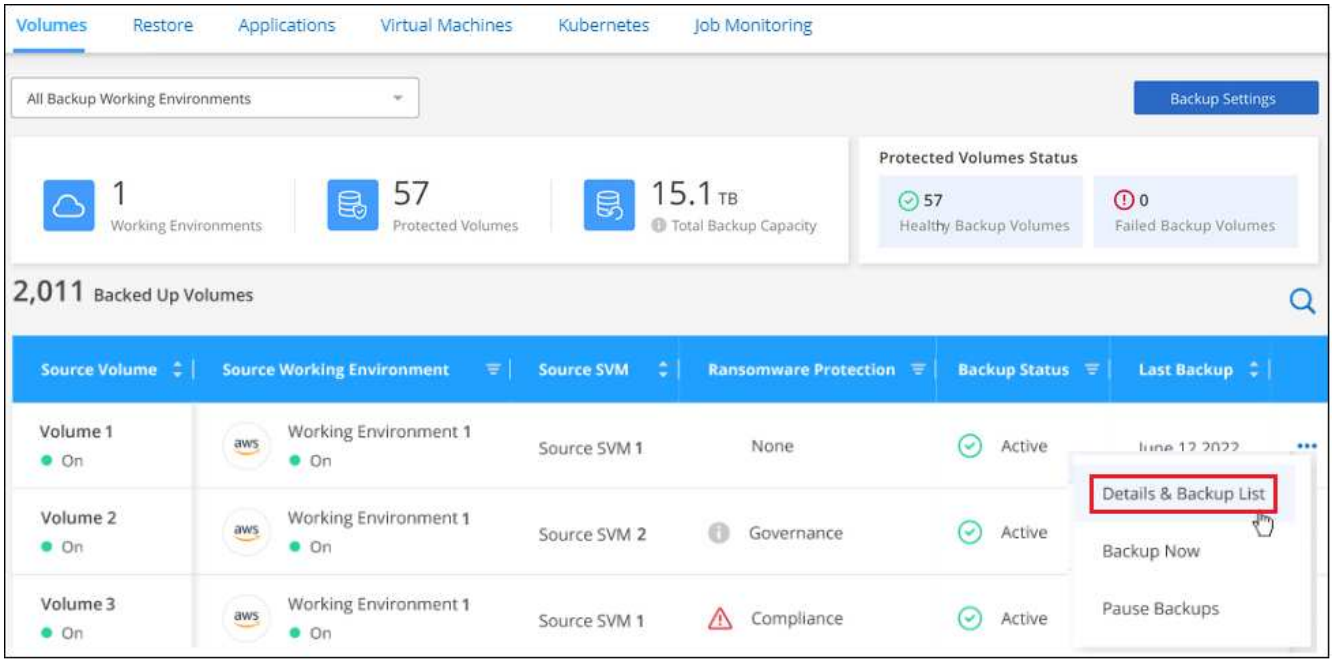
Löschen aller Sicherungsdateien für ein Volume

Durch das Löschen aller Backups für ein Volume werden auch künftige Backups für dieses Volume deaktiviert.

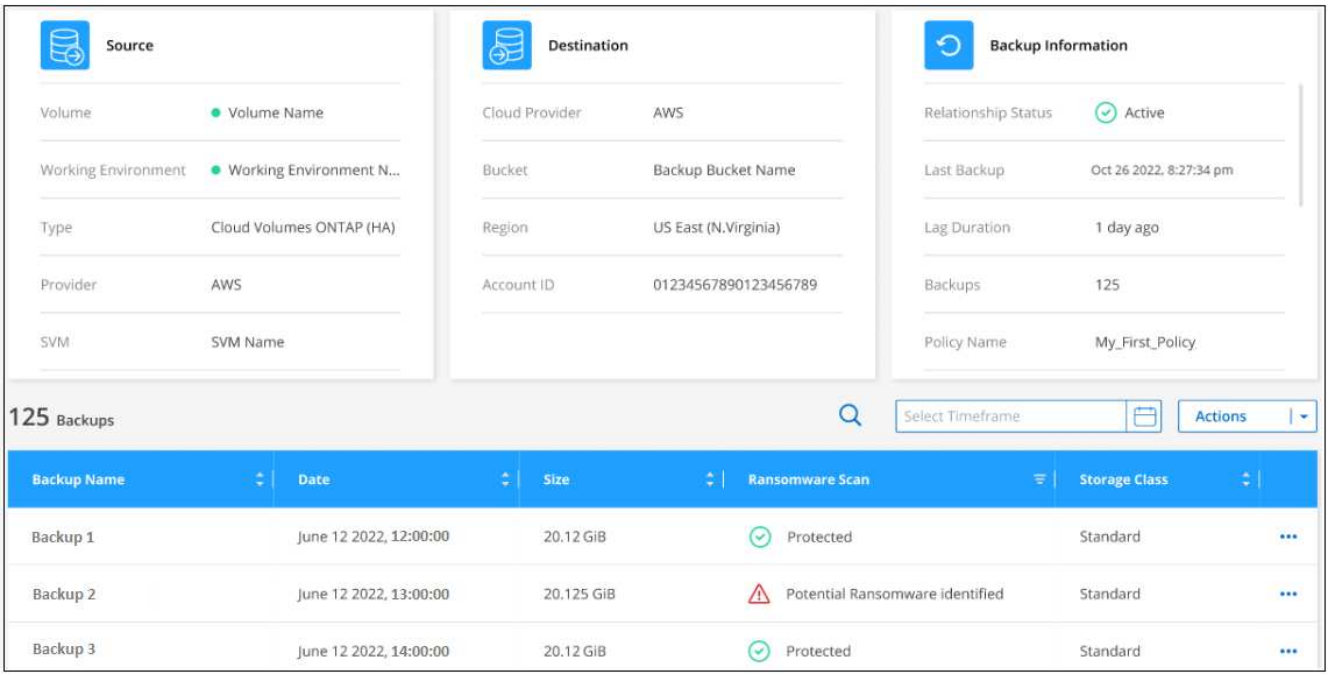
Das können Sie Starten Sie neu, um Backups für das Volume zu erstellen Auf der Seite „Backups verwalten“ können Sie jederzeit Backups managen.

Schritte

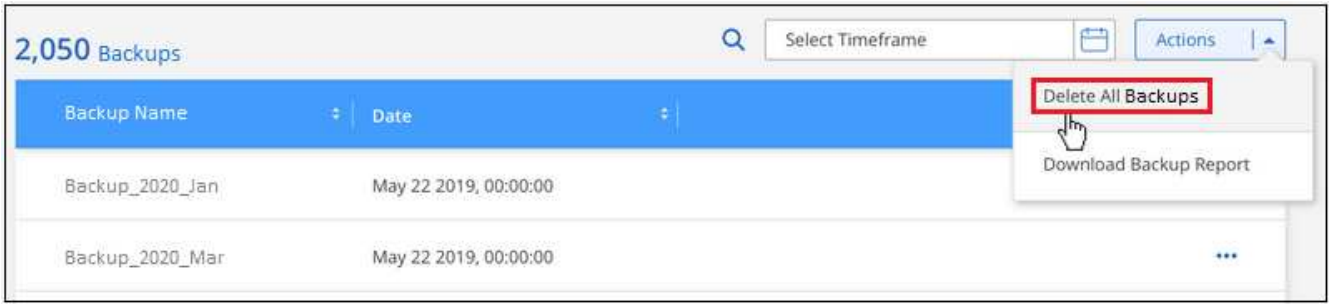
1. Klicken Sie auf der Registerkarte **Volumes** auf ••• Wählen Sie für das Quellvolume **Details & Sicherungsliste** aus.



Die Liste aller Sicherungsdateien wird angezeigt.



2. Klicken Sie auf **Aktionen** > **Alle Backups löschen**.



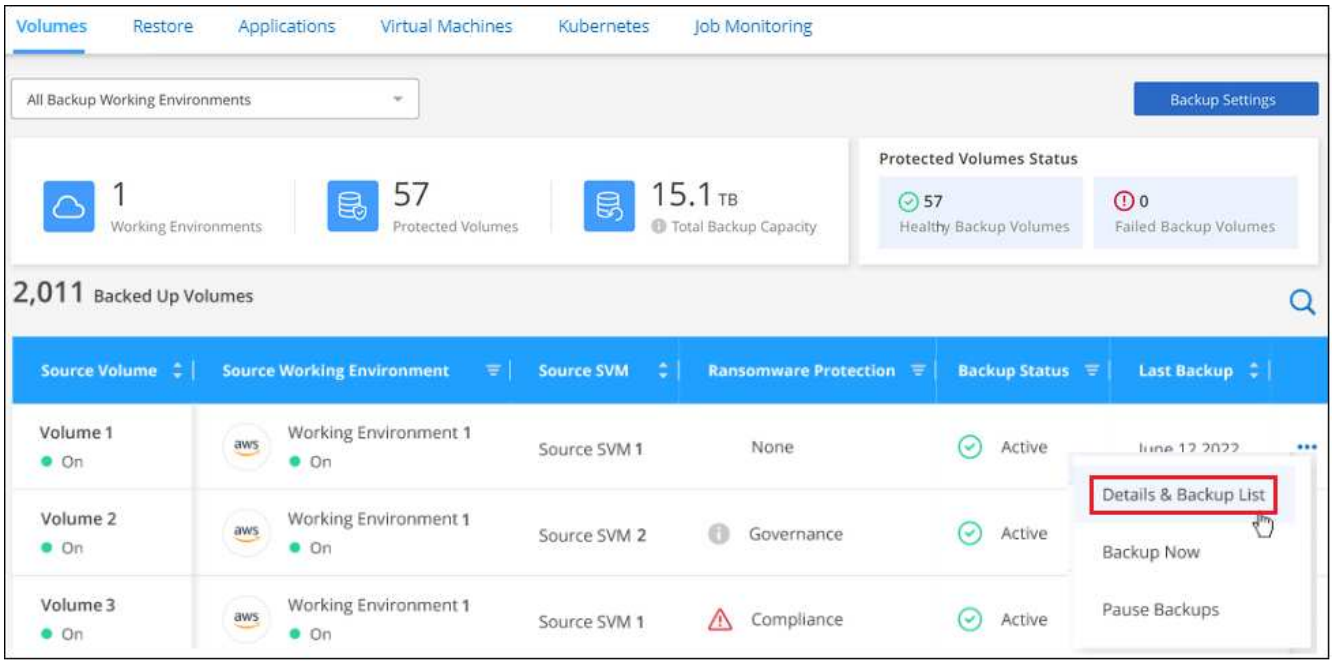
3. Geben Sie im Bestätigungsdialogfeld den Namen des Datenträgers ein und klicken Sie auf **Löschen**.

Löschen einer einzelnen Backup-Datei für ein Volume

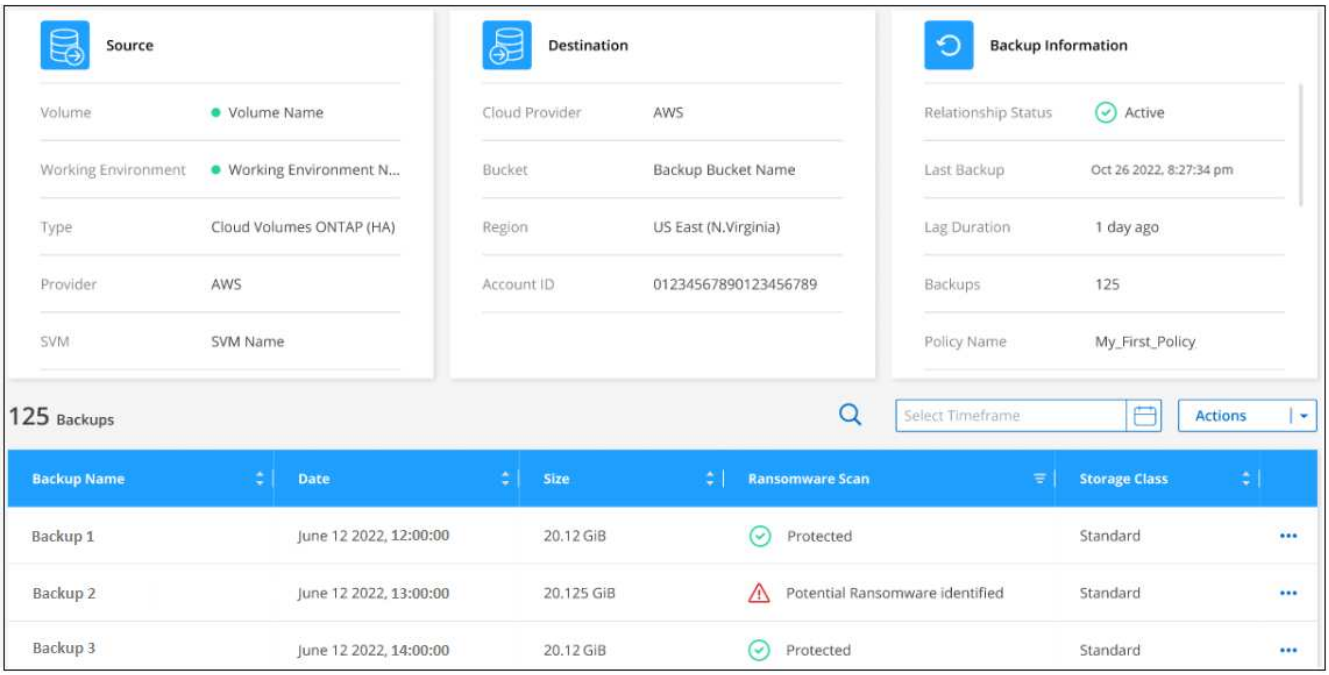
Sie können eine einzelne Sicherungsdatei löschen. Diese Funktion ist nur verfügbar, wenn das Volume Backup aus einem System mit ONTAP 9.8 oder neuer erstellt wurde.

Schritte

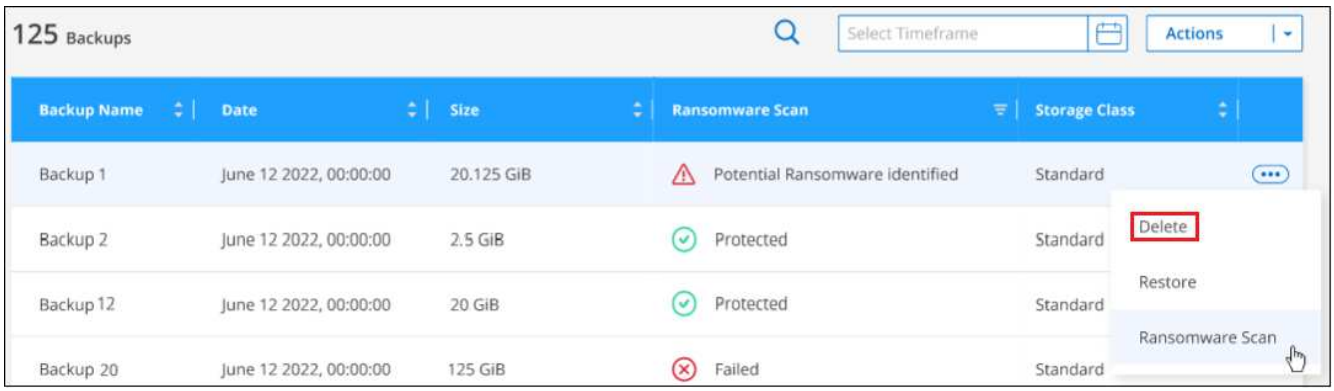
1. Klicken Sie auf der Registerkarte **Volumes** auf ••• Wählen Sie für das Quellvolume **Details & Sicherungsliste** aus.



Die Liste aller Sicherungsdateien wird angezeigt.



2. Klicken Sie Auf ••• Für die Sicherungsdatei des Datenträgers, die Sie löschen möchten, klicken Sie auf **Löschen**.



3. Klicken Sie im Bestätigungsdialogfeld auf **Löschen**.

Löschen von Volume-Backup-Beziehungen

Wenn Sie die Backup-Beziehung für ein Volume löschen, erhalten Sie einen Archivierungsmechanismus, wenn Sie die Erstellung neuer Backup-Dateien beenden und das Quell-Volume löschen möchten, aber alle bestehenden Backup-Dateien behalten möchten. So können Sie das Volume bei Bedarf später aus der Backup-Datei wiederherstellen und gleichzeitig Speicherplatz aus dem Quell-Storage-System löschen.

Das Quell-Volume muss nicht unbedingt gelöscht werden. Sie können die Backup-Beziehung für ein Volume löschen und das Quell-Volume behalten. In diesem Fall können Sie die Backups auf dem Volume zu einem späteren Zeitpunkt „aktivieren“. Die ursprüngliche Backup-Kopie des Basisplans wird in diesem Fall weiterhin verwendet. Eine neue Basis-Backup-Kopie wird nicht erstellt und in die Cloud exportiert. Beachten Sie, dass beim Reaktivieren einer Backup-Beziehung dem Volume die standardmäßige Backup-Richtlinie zugewiesen wird.

Diese Funktion ist nur verfügbar, wenn Ihr System ONTAP 9.12.1 oder höher ausführt.

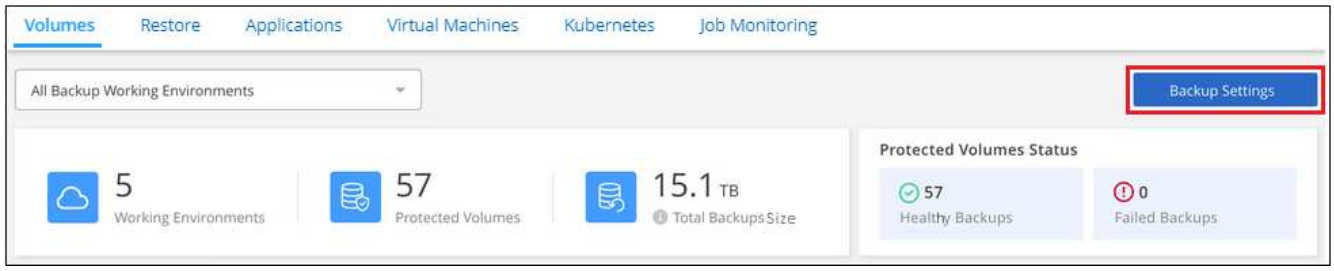
Sie können das Quell-Volume nicht aus der Cloud Backup Benutzeroberfläche löschen. Sie können jedoch die

Seite Volume Details auf dem Bildschirm öffnen, und "Löschen Sie das Volume von dort".

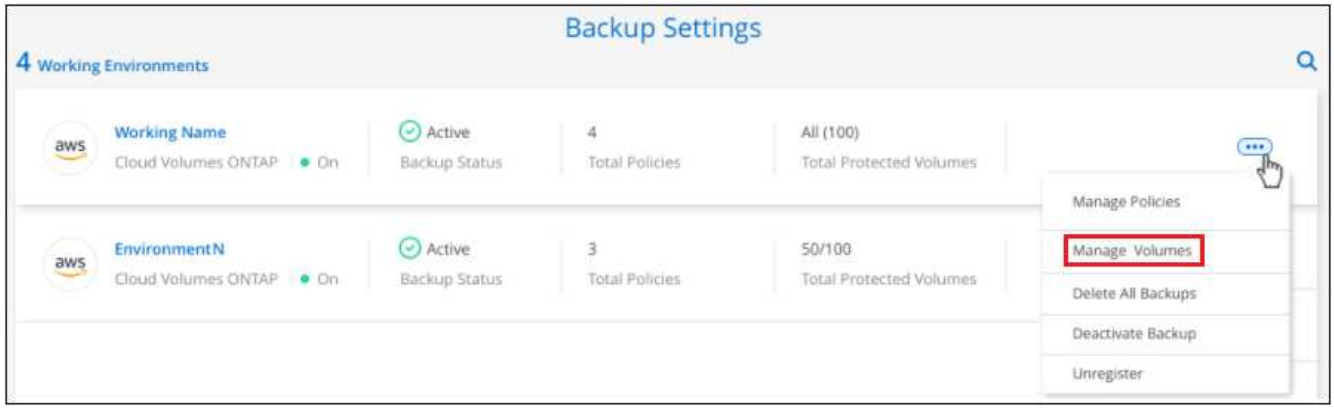
> Sie können einzelne Sicherungsdateien des Volumes nicht löschen, sobald die Beziehung gelöscht wurde. Sie können es jedoch "Löschen Sie alle Backups für das Volume" Wenn Sie alle Sicherungsdateien entfernen möchten.

Schritte

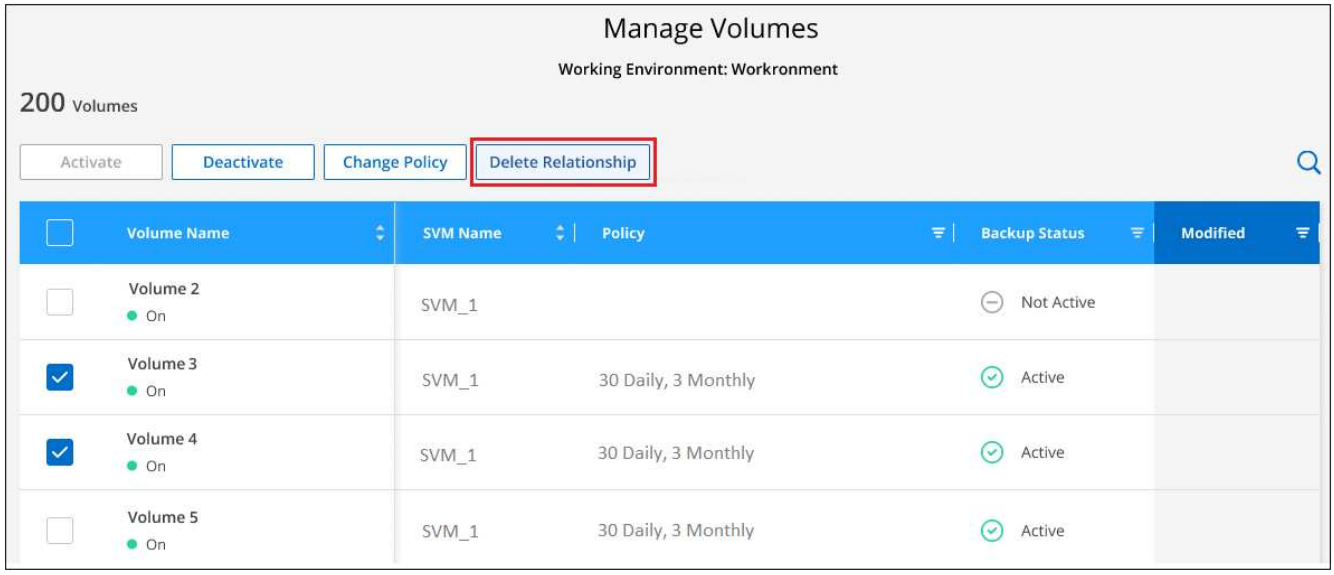
1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.



2. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Wählen Sie für die Arbeitsumgebung **Volumes verwalten** aus.

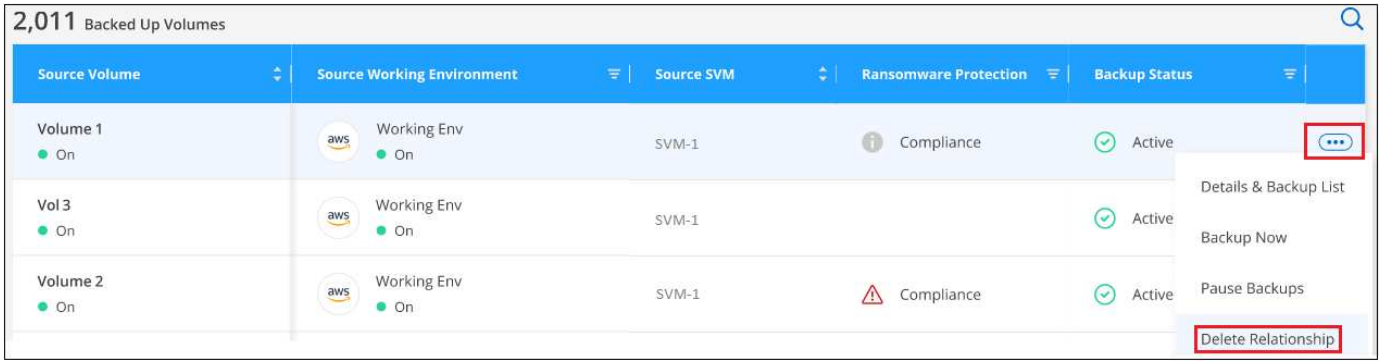


3. Aktivieren Sie das Kontrollkästchen für ein Volume oder Volumes, das Sie die Sicherungsbeziehung löschen möchten, und klicken Sie dann auf **Beziehung löschen**.

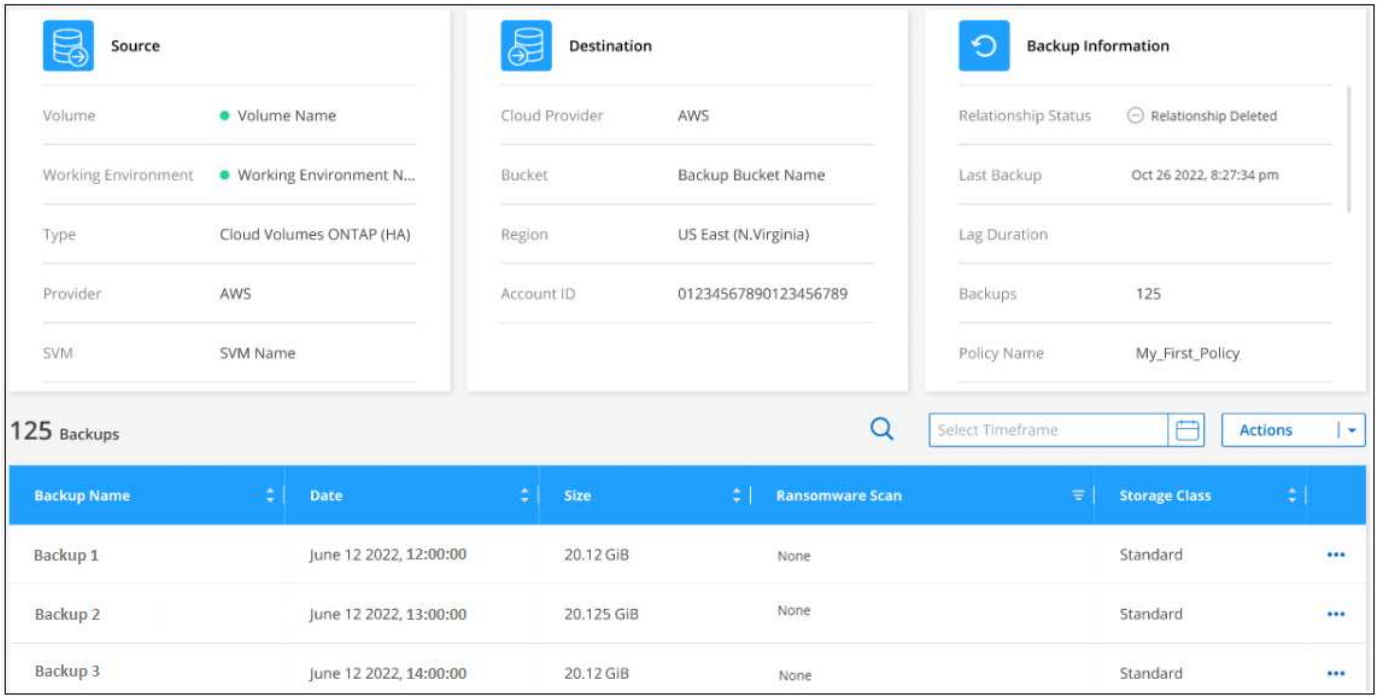


4. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.

Beachten Sie, dass Sie die Backup-Beziehung für ein einzelnes Volume auch von der Seite Volumes löschen können.



Wenn Sie die Liste der Backups für jedes Volume anzeigen, wird der „Beziehungsstatus“ als **Beziehung gelöscht** aufgeführt.



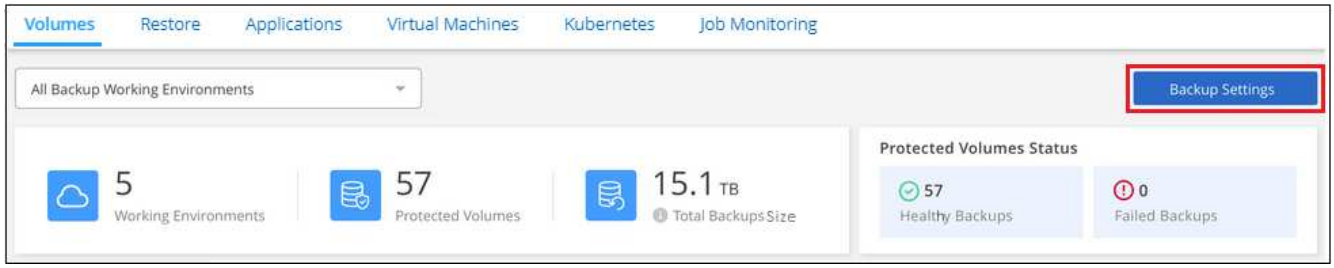
Deaktivieren von Cloud Backup für eine Arbeitsumgebung

Durch die Deaktivierung von Cloud Backup für eine funktionierende Umgebung werden Backups von jedem Volume im System deaktiviert und es wird auch die Möglichkeit zur Wiederherstellung eines Volumes deaktiviert. Vorhandene Backups werden nicht gelöscht. Dadurch wird die Registrierung des Backup-Service in dieser Arbeitsumgebung nicht aufgehoben. Im Grunde können Sie alle Backup- und Wiederherstellungsaktivitäten für einen bestimmten Zeitraum anhalten.

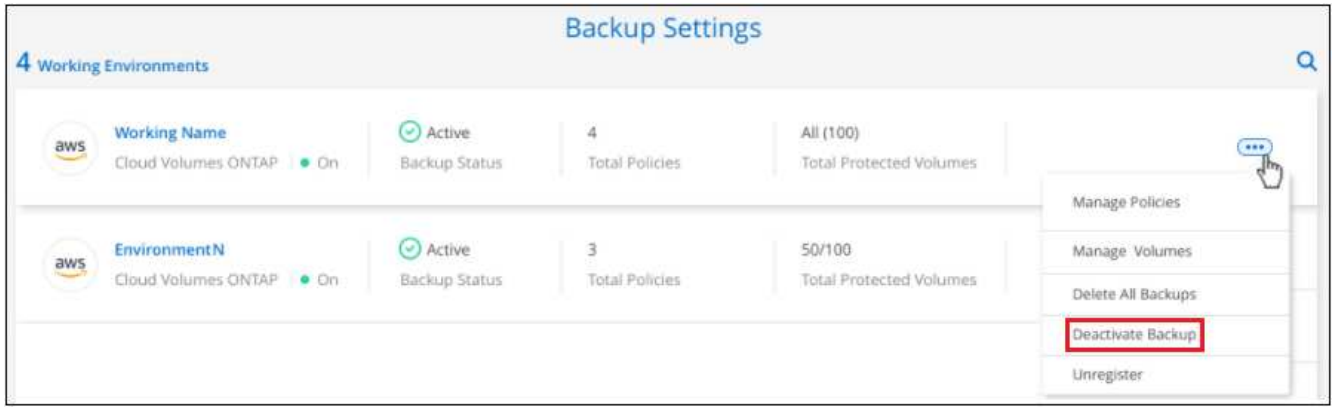
Beachten Sie, dass Cloud-Provider Ihnen weiterhin die Kosten für Objekt-Storage für die Kapazität in Ihrem Backup in Rechnung stellen, es sei denn, Sie sind erforderlich Löschen Sie die Backups.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.



2. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Für die Arbeitsumgebung, in der Sie Backups deaktivieren und **Sicherung deaktivieren** auswählen möchten.



3. Klicken Sie im Bestätigungsdialogfeld auf **Deaktivieren**.

> Für diese Arbeitsumgebung wird während der Sicherung eine **Sicherung aktivieren** -Schaltfläche angezeigt. Sie können auf diese Schaltfläche klicken, wenn Sie die Backup-Funktion in dieser Arbeitsumgebung erneut aktivieren möchten.

Registrieren von Cloud Backup für eine Arbeitsumgebung wird aufgehoben

Sie können Cloud Backup für eine Arbeitsumgebung unregistrieren, wenn Sie die Backup-Funktion nicht mehr verwenden möchten, und Sie nicht mehr mit dem Aufladen von Backups in dieser Arbeitsumgebung belastet werden möchten. Diese Funktion wird normalerweise verwendet, wenn Sie planen, eine Arbeitsumgebung zu löschen, und Sie möchten den Backup-Service abbrechen.

Sie können diese Funktion auch verwenden, wenn Sie den Zielobjektspeicher ändern möchten, in dem Ihre Cluster-Backups gespeichert werden. Nachdem Sie Cloud Backup für die Arbeitsumgebung registriert haben, können Sie Cloud Backup für diesen Cluster mithilfe der neuen Cloud-Provider-Informationen aktivieren.

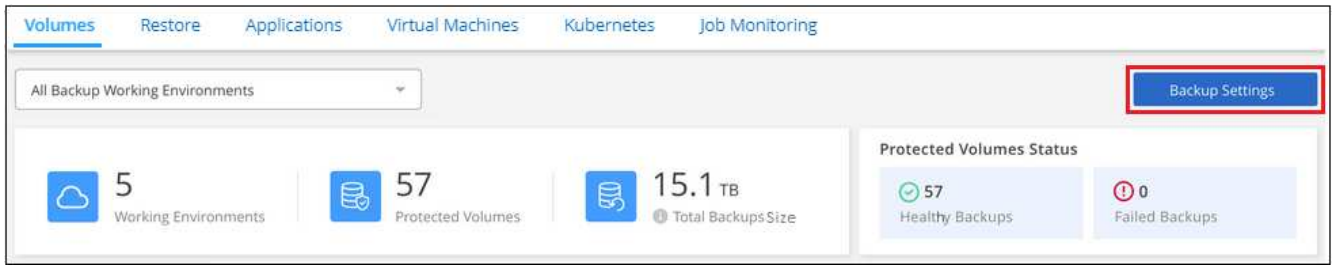
Bevor Sie die Registrierung von Cloud Backup aufheben können, müssen Sie die folgenden Schritte in der folgenden Reihenfolge durchführen:

- Deaktivieren Sie Cloud Backup für die Arbeitsumgebung
- Löschen Sie alle Backups für die Arbeitsumgebung

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. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Für die Arbeitsumgebung, in der Sie die Registrierung des Backup-Dienstes aufheben möchten, und wählen Sie **Registrierung aufheben** aus.

3. Klicken Sie im Bestätigungsdialogfeld auf **Registrierung aufheben**.

Verwalten von Backup-Einstellungen auf Cluster-Ebene

Bei der Aktivierung von Cloud Backup für jedes ONTAP System können viele Backup-Einstellungen auf Cluster-Ebene geändert werden. Sie können auch einige Einstellungen ändern, die als „Standard“-Backup-Einstellungen angewendet werden. Dies schließt das Ändern von Storage-Schlüsseln, die Übertragungsrate von Backups in den Objekt-Storage ein, unabhängig davon, ob historische Snapshot-Kopien als Backup-Dateien exportiert werden, und vieles mehr.

Die Backup-Einstellungen auf Cluster-Ebene sind auf der Seite „*Advanced Settings*“ verfügbar.

Die vollständigen Backup-Einstellungen, die Sie ändern können, umfassen:

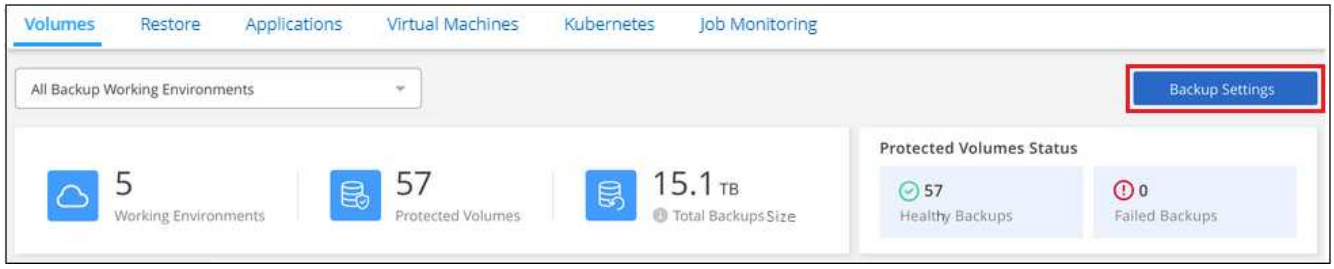
- Ändern der Storage-Schlüssel, die Ihrem ONTAP-System Zugriff auf Objekt-Storage gewähren
- Ändern des ONTAP-IPspaces, der mit Objekt-Storage verbunden ist
- Ändern der Netzwerkbandbreite, die für das Hochladen von Backups in den Objektspeicher zugewiesen ist
- Ändern der Archiv-Storage-Klasse (nur AWS)
- Ändern der automatischen Backup-Einstellung (und -Richtlinie) für zukünftige Volumes
- Änderung, ob historische Snapshot-Kopien in Ihren ersten Basis-Backup-Dateien für zukünftige Volumes enthalten sind
- Es wird geändert, ob „jährliche“ Snapshots aus dem Quellsystem entfernt werden

Zeigen Sie Backup-Einstellungen auf Cluster-Ebene an

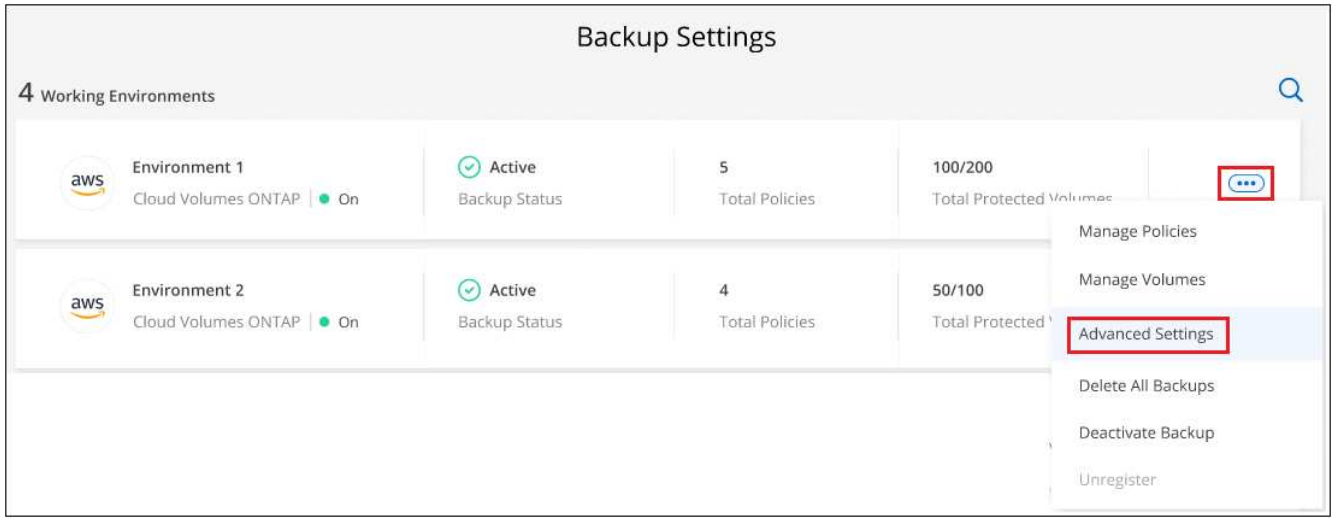
Sie können die Backup-Einstellungen auf Clusterebene für jede Arbeitsumgebung anzeigen.

Schritte

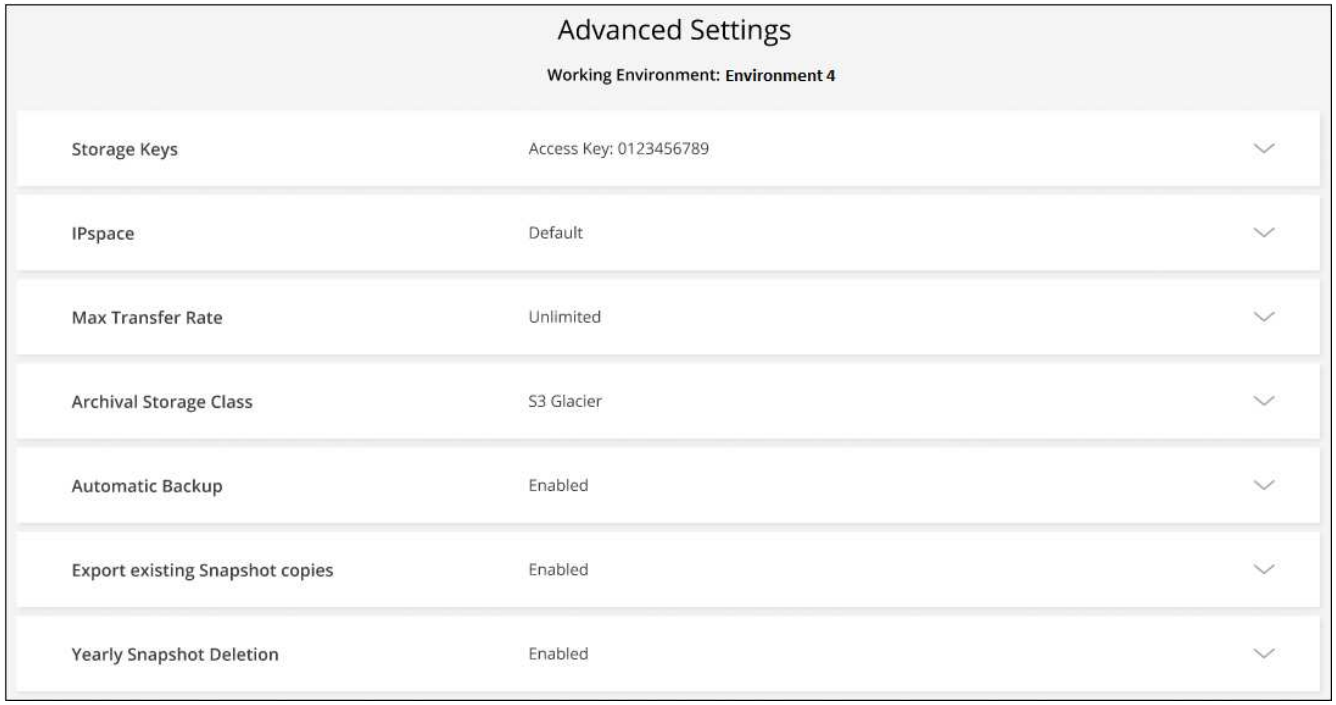
1. Wählen Sie im Menü BlueXP die Option **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.



3. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Wählen Sie für die Arbeitsumgebung die Option **Erweiterte Einstellungen** aus.



Auf der Seite *Erweiterte Einstellungen* werden die aktuellen Einstellungen für diese Arbeitsumgebung angezeigt.



Wenn Sie Änderungen vornehmen möchten, erweitern Sie einfach die Option und nehmen Sie die Änderung vor. Alle Backup-Vorgänge nach der Änderung verwenden die neuen Werte.

Beachten Sie, dass einige Optionen basierend auf der Version von ONTAP auf dem Quell-Cluster nicht verfügbar sind und auf dem Ziel des Cloud-Providers, in dem sich die Backups befinden, basieren.

Ändern der Storage-Schlüssel für ONTAP für den Zugriff auf Cloud-Storage

Wenn Sie über eine Firmenrichtlinie verfügen, bei der Sie alle Anmeldedaten, z. B. alle 6 Monate oder ein Jahr, regelmäßig rotieren müssen, so werden Sie den Zugriffsschlüssel und den geheimen Schlüssel Ihres Cloud-Providers mit Ihrem ONTAP-System synchronisieren. So können Sie Ihre Zugangsdaten für Cloud-Provider aktualisieren und die Schlüssel in Ihrem ONTAP-System ändern, damit die beiden Systeme weiterhin kommunizieren.

Diese Option steht nur für ONTAP Systeme vor Ort zur Verfügung und nur, wenn Sie Backups in Amazon S3, Google Cloud Storage und StorageGRID speichern.

Geben Sie einfach den neuen Zugriffsschlüssel und den geheimen Schlüssel ein und klicken Sie auf **Apply**.

Ändern Sie den ONTAP-IPspace, der mit dem Objekt-Storage verbunden ist

Sie können den ONTAP-IPspace, der mit Objekt-Storage verbunden ist, ändern. Diese Option ist nur beim Backup von Daten aus On-Premises-ONTAP-Systemen verfügbar - es ist nicht für Cloud Volumes ONTAP-

Systeme verfügbar.

Diese Option sollte nicht auf einem System verwendet werden, das Volume-Daten aktiv in den Objekt-Storage sichert. Es sollte nur verwendet werden, wenn bei der ersten Aktivierung von Backup auf einem lokalen ONTAP-System ein falscher IPspace ausgewählt wurde.

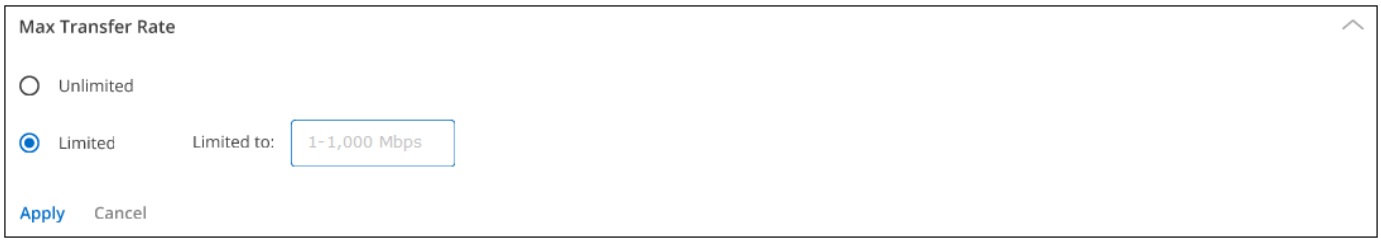
Lesen Sie die Dokumentation zu den ersten Schritten, um das Backup von Daten von ONTAP Systemen vor Ort an Ihren spezifischen Cloud-Provider zu erstellen. Überprüfen Sie, ob Ihr ONTAP-Setup für den neuen IPspace korrekt konfiguriert ist. Beispiel:

- Auf jedem ONTAP Node ist eine Intercluster-LIF erforderlich, die die Volumes hostet, die Sie sichern möchten.
- Die LIF muss dem IPspace zugewiesen sein, den ONTAP zum Herstellen einer Verbindung mit Objekt-Storage verwenden sollte.
- Die Intercluster-LIFs der Nodes müssen auf den Objektspeicher zugreifen können.
- Wenn Sie einen anderen IPspace als den *Default* verwenden, müssen Sie möglicherweise eine statische Route erstellen, um Zugriff auf den Objekt-Speicher zu erhalten.

Wählen Sie einfach den neuen IPspace aus und klicken Sie auf **Apply**. Danach können Sie die Volumes auswählen, die Sie aus Aggregaten in diesem IPspace sichern möchten.

Ändern Sie die verfügbare Netzwerkbandbreite zum Hochladen von Backups in den Objektspeicher

Wenn Sie Cloud Backup für eine Arbeitsumgebung aktivieren, kann ONTAP die Backup-Daten standardmäßig mit einer unbegrenzten Bandbreite aus den Volumes in der Arbeitsumgebung in den Objekt-Storage übertragen. Wenn der Backup-Traffic sich auf normale Benutzer-Workloads auswirkt, kann die Menge an Netzwerkbandbreite, die während des Transfers verwendet wird, drosselt werden. Sie können einen Wert zwischen 1 und 1,000 Mbit/s als maximale Übertragungsrate auswählen.



Wählen Sie das Optionsfeld **begrenzt** und geben Sie die maximale Bandbreite ein, die verwendet werden kann, oder wählen Sie **unbegrenzt**, um anzuzeigen, dass keine Begrenzung vorhanden ist.

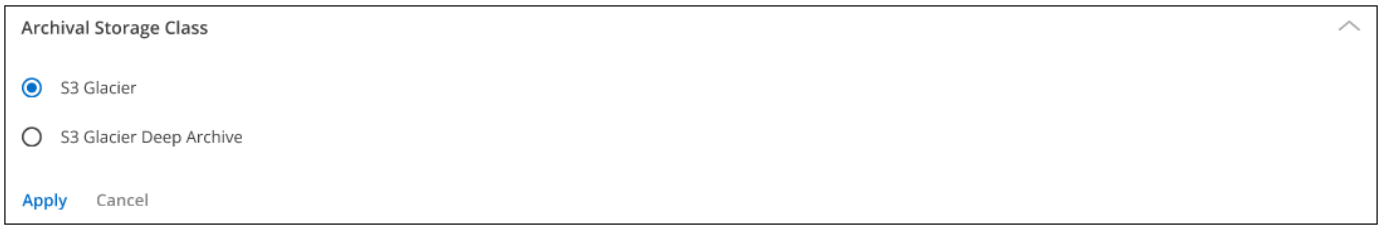
Ändern Sie die Storage-Klasse für die Archivierung

Wenn Sie die Speicherklasse ändern möchten, die verwendet wird, wenn Ihre Backup-Dateien für eine bestimmte Anzahl von Tagen gespeichert wurden (in der Regel mehr als 30 Tage), können Sie hier die

Änderung vornehmen. Alle Backup-Richtlinien, die Archiv-Storage nutzen, werden sofort geändert und nutzen diese neue Storage-Klasse.

Diese Option ist für On-Premises-ONTAP- und Cloud Volumes ONTAP-Systeme (über ONTAP 9.10.1 oder höher) verfügbar, wenn Sie Backup-Dateien in Amazon S3 schreiben.

Beachten Sie, dass Sie nur von *S3 Glacier* zu *S3 Glacier Deep Archive* wechseln können. Wenn du das Glacier Deep Archive ausgewählt hast, kannst du nicht wieder zu Glacier zurückkehren.



"Erfahren Sie mehr über die Storage-Einstellungen für Archive"."Erfahren Sie mehr über die Verwendung von AWS Archiv-Storage".

Ändern Sie die automatische Backup-Einstellung für zukünftige Volumes

Wenn Sie bei Aktivierung von Cloud Backup die automatische Sicherung zukünftiger Volumes nicht aktiviert haben, können Sie im Abschnitt Automatisches Backup die automatischen Backups neuer Volumes durchführen. Sie können auch die Backup-Richtlinie auswählen, die auf diese neuen Volumes angewendet wird. Eine Backup-Richtlinie, die neu erstellten Volumes zugewiesen wurde, stellt sicher, dass alle Ihre Daten geschützt sind.

Wenn Sie bei Aktivierung von Cloud Backup die automatische Sicherung zukünftiger Volumes aktiviert haben, können Sie die Backup-Richtlinie ändern, die für die neu erstellten Volumes im Abschnitt Automatisches Backup verwendet wird.

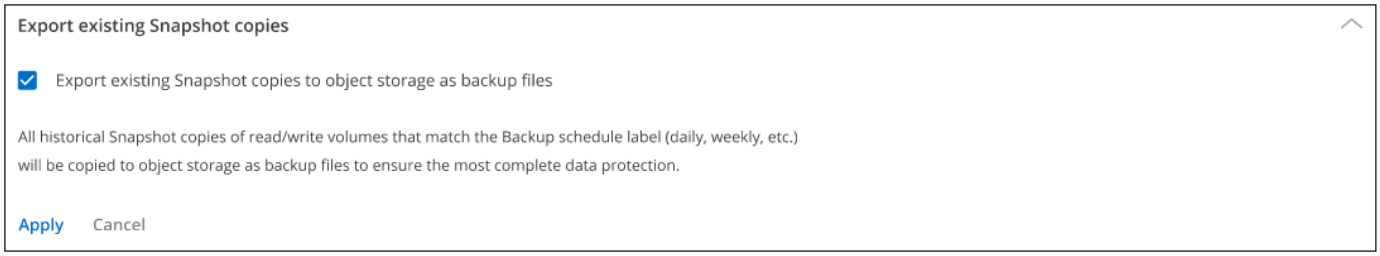
Beachten Sie, dass die Richtlinie, die Sie auf neue Volumes anwenden möchten, bereits vorhanden sein muss. "Lesen Sie, wie Sie eine neue Backup-Richtlinie für eine Arbeitsumgebung erstellen".

Sobald diese Backup-Richtlinie aktiviert ist, wird sie auf alle neuen Volumes angewendet, die in dieser Arbeitsumgebung mithilfe von BlueXP, System Manager, der ONTAP CLI oder den APIs erstellt wurden.

Ändern Sie, ob historische Snapshot Kopien als Backup-Dateien exportiert werden

Wenn es lokale Snapshot-Kopien für Volumes gibt, die mit dem Backup-Schedule-Label übereinstimmen, das Sie in dieser Arbeitsumgebung verwenden (z. B. täglich, wöchentlich usw.), können Sie diese historischen Snapshots als Backup-Dateien in Objekt-Storage exportieren. Damit können Sie Ihre Backups in die Cloud initialisieren, indem Sie ältere Snapshot-Kopien in die Basis-Backup-Kopie verschieben.

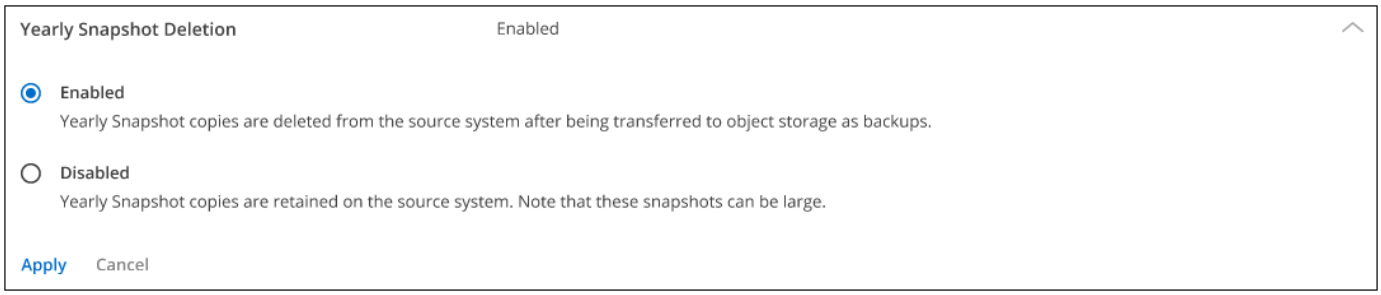
Beachten Sie, dass diese Option nur für neue Backup-Dateien für neue Lese-/Schreib-Volumes gilt und nicht für Datensicherungs-Volumes unterstützt wird.



Wählen Sie einfach aus, ob vorhandene Snapshot Kopien exportiert werden sollen, und klicken Sie auf **Apply**.

Ändern Sie, ob „jährliche“ Snapshots aus dem Quellsystem entfernt werden

Wenn Sie das „jährliche“ Backup-Etikett für eine Backup-Richtlinie für eines Ihrer Volumes auswählen, ist die erstellte Snapshot-Kopie sehr groß. Standardmäßig werden diese jährlichen Snapshots nach der Übertragung in den Objektspeicher automatisch aus dem Quellsystem gelöscht. Sie können dieses Standardverhalten im Abschnitt Jährlicher Snapshot-Löschvorgang ändern.



Wählen Sie **deaktiviert** und klicken Sie auf **Anwenden**, wenn Sie die jährlichen Snapshots auf dem Quellsystem beibehalten möchten.

Wiederherstellen von ONTAP Daten aus Backup-Dateien

Backups werden in einem Objektspeicher in Ihrem Cloud-Konto gespeichert, sodass Sie Daten von einem bestimmten Zeitpunkt wiederherstellen können. Sie können ein gesamtes ONTAP Volume aus einer Backup-Datei wiederherstellen. Wenn Sie aber nur einige Dateien wiederherstellen müssen, können Sie einen Ordner oder einzelne Dateien aus einer Backup-Datei wiederherstellen.

Sie können ein **Volume** (als neues Volume) in der ursprünglichen Arbeitsumgebung, in einer anderen Arbeitsumgebung, in der dieselben Cloud-Konten verwendet werden, oder auf einem lokalen ONTAP System wiederherstellen.

Sie können einen **Ordner** auf einem Volume in der ursprünglichen Arbeitsumgebung, auf einem Volume in einer anderen Arbeitsumgebung, die denselben Cloud-Account verwendet, oder auf einem Volume in einem lokalen ONTAP System wiederherstellen.

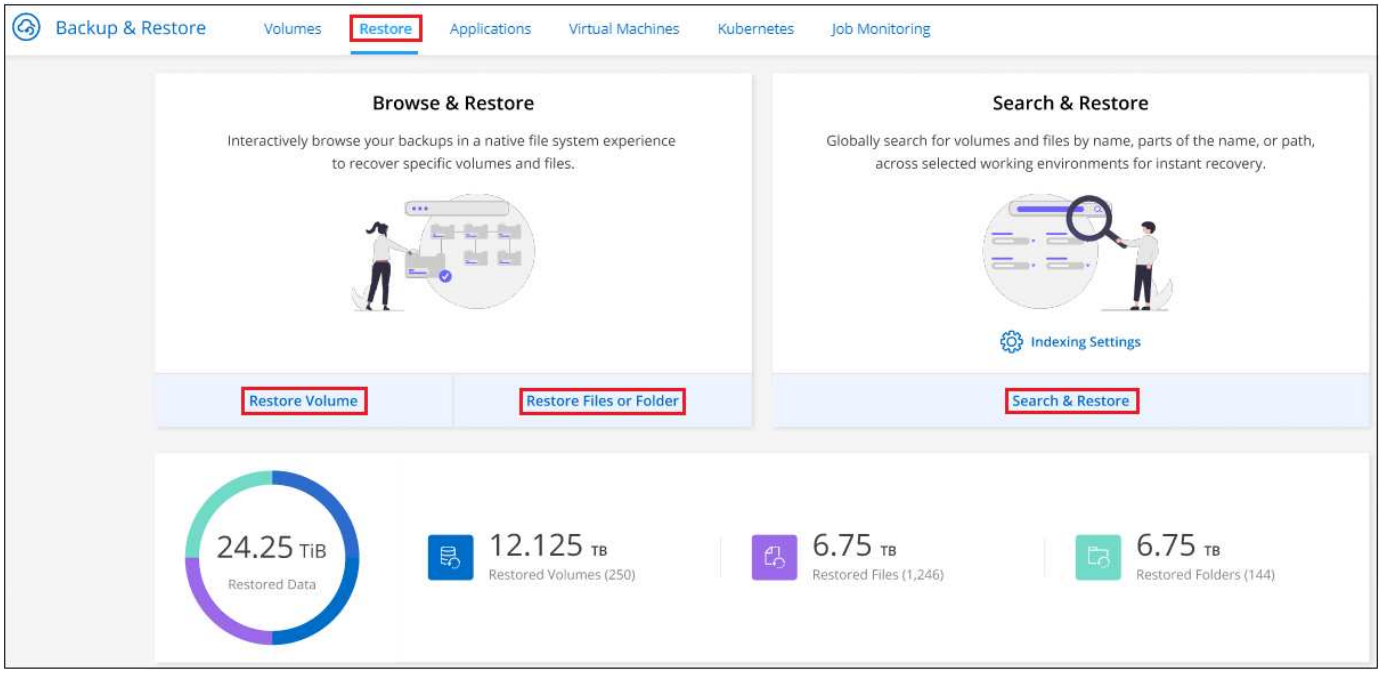
Sie können **Dateien** auf einem Volume in der ursprünglichen Arbeitsumgebung, auf einem Volume in einer anderen Arbeitsumgebung, in der dieselben Cloud-Konten verwendet werden, oder auf einem Volume in einem lokalen ONTAP System wiederherstellen.

Zum Wiederherstellen von Daten aus Backup-Dateien in einem Produktionssystem ist eine gültige Cloud Backup-Lizenz erforderlich.

Das Restore Dashboard

Mit dem Restore Dashboard können Sie Volume-, Ordner- und Dateiwiederherstellungsvorgänge durchführen. Sie öffnen das Restore Dashboard, indem Sie im BlueXP-Menü auf **Backup und Recovery** klicken und dann auf die Registerkarte **Restore** klicken. Sie können auch auf klicken > **Ansicht Restore Dashboard** vom Backup- und Recovery-Dienst aus dem Fenster Dienste.

> Cloud Backup muss bereits für mindestens eine Arbeitsumgebung aktiviert sein und es müssen erste Backup-Dateien vorhanden sein.



Wie Sie sehen können, bietet das Restore Dashboard 2 verschiedene Möglichkeiten, Daten aus Sicherungsdateien wiederherzustellen: **Durchsuchen & Wiederherstellen** und **Suchen & Wiederherstellen**.

Vergleichen von Durchsuchen und Wiederherstellen und Suchen und Wiederherstellen

In der Regel ist *Browse & Restore* besser, wenn Sie ein bestimmtes Volume, einen Ordner oder eine Datei aus der letzten Woche oder einem Monat wiederherstellen müssen - und Sie kennen den Namen und den Speicherort der Datei und das Datum, an dem sie zuletzt in gutem Zustand war. *Search & Restore* ist in der Regel besser, wenn Sie ein Volume, einen Ordner oder eine Datei wiederherstellen müssen, aber Sie erinnern sich nicht an den genauen Namen, oder das Volumen, in dem es sich befindet, oder das Datum, an dem es zuletzt in gutem Zustand war.

Diese Tabelle enthält einen Vergleich der beiden Methoden.

Suchen Und Wiederherstellen	Suche Und Wiederherstellung
Durchsuchen Sie eine Struktur im Ordnerstil, um nach Volumes, Ordnern oder Dateien in einer einzelnen Backup-Datei zu suchen	Suchen Sie nach einem Volume, einem Ordner oder einer Datei über **alle Backup-Dateien** nach einem partiellen oder vollständigen Volume-Namen, einem Teil- oder vollständigen Ordner-/Dateinamen, einem Größenbereich und zusätzlichen Suchfiltern
Die Wiederherstellung von Volumes und Dateien erfolgt mit Backup-Dateien, die in Amazon S3, Azure Blob, Google Cloud und NetApp StorageGRID gespeichert sind	Die Wiederherstellung von Volumes und Dateien erfolgt mit Backup-Dateien, die in Amazon S3, Azure Blob, Google Cloud und NetApp StorageGRID gespeichert sind
Stellen Sie Volumes, Ordner und Dateien von StorageGRID in Sites ohne Internetzugang wieder her	Wird nicht in dunklen Seiten unterstützt
Behandelt keine Dateien, die umbenannt oder gelöscht wurden	Verarbeitet neu erstellte/gelöschte/umbenannte Verzeichnisse und neu erstellte/gelöschte/umbenannte Dateien
Durchsuchen Sie nach Ergebnissen über Public und Private Clouds hinweg	Durchsuchen Sie Public Clouds und lokale Snapshot Kopien nach Ergebnissen
Es sind keine zusätzlichen Ressourcen für Cloud-Provider erforderlich	Pro Konto sind zusätzliche Bucket- und Public-Cloud-Provider-Ressourcen erforderlich
Es sind keine zusätzlichen Kosten für Cloud-Provider erforderlich	Kosten im Zusammenhang mit Public-Cloud-Provider-Ressourcen bei der Überprüfung Ihrer Backups und Volumes für Suchergebnisse

Bevor Sie eine der beiden Wiederherstellungsmethoden verwenden können, sollten Sie sicherstellen, dass Sie Ihre Umgebung für die speziellen Ressourcenanforderungen konfiguriert haben. Diese Anforderungen werden in den Abschnitten unten beschrieben.

Siehe Anforderungen und Wiederherstellungsschritte für den Typ der Wiederherstellungsoperation, die Sie verwenden möchten:

- <<Restoring volumes using Browse & Restore,Stellen Sie Volumes mithilfe von Browse Restore wieder her
- <<Restoring folders and files using Browse & Restore,Wiederherstellen von Ordnern und Dateien mit Durchsuchen Restore
- <<Restoring ONTAP data using Search & Restore,Stellen Sie Volumes, Ordner und Dateien mithilfe von Search Restore wieder her

Wiederherstellen von ONTAP-Daten mithilfe von Durchsuchen und Wiederherstellen

Bevor Sie mit der Wiederherstellung eines Volumes, Ordners oder einer Datei beginnen, sollten Sie den Namen des Volumes, aus dem Sie wiederherstellen möchten, den Namen der Arbeitsumgebung, in der sich das Volume befindet, sowie das ungefähre Datum der Sicherungsdatei, aus der Sie wiederherstellen möchten, kennen.

Hinweis: Wenn die Sicherungsdatei für das wiederherzustellende Volume im Archiv-Speicher liegt (beginnend mit ONTAP 9.10.1), dauert der Wiederherstellungsvorgang länger und es entstehen Kosten. Darüber hinaus muss auf dem Ziel-Cluster ONTAP 9.10.1 oder höher für Volume-Restores, 9.11.1 für die Dateiwiederherstellung und 9.12.1 für Google Archive ausgeführt werden.

"Erfahren Sie mehr über die Wiederherstellung aus AWS Archiv-Storage".

Unterstützte Arbeitsumgebungen und Objekt-Storage-Anbieter durchsuchen und wiederherstellen

Sie können ein Volume, einen Ordner oder einzelne Dateien aus einer ONTAP-Sicherungsdatei in folgenden Arbeitsumgebungen wiederherstellen:

Speicherort der Sicherungsdatei Zielumgebung ifdef::aws[]	Amazon S3
Cloud Volumes ONTAP in AWS On-Premises ONTAP System endif::aws[] ifdef::azurAzure[]	Azure Blob
Cloud Volumes ONTAP in Azure On-Premises ONTAP System endif::Azure[] ifdef::gcp[]	Google Cloud Storage
Cloud Volumes ONTAP in Google On-Premises ONTAP System endif::gcp[]	NetApp StorageGRID

Für Browse & Restore kann der Connector an folgenden Orten installiert werden:

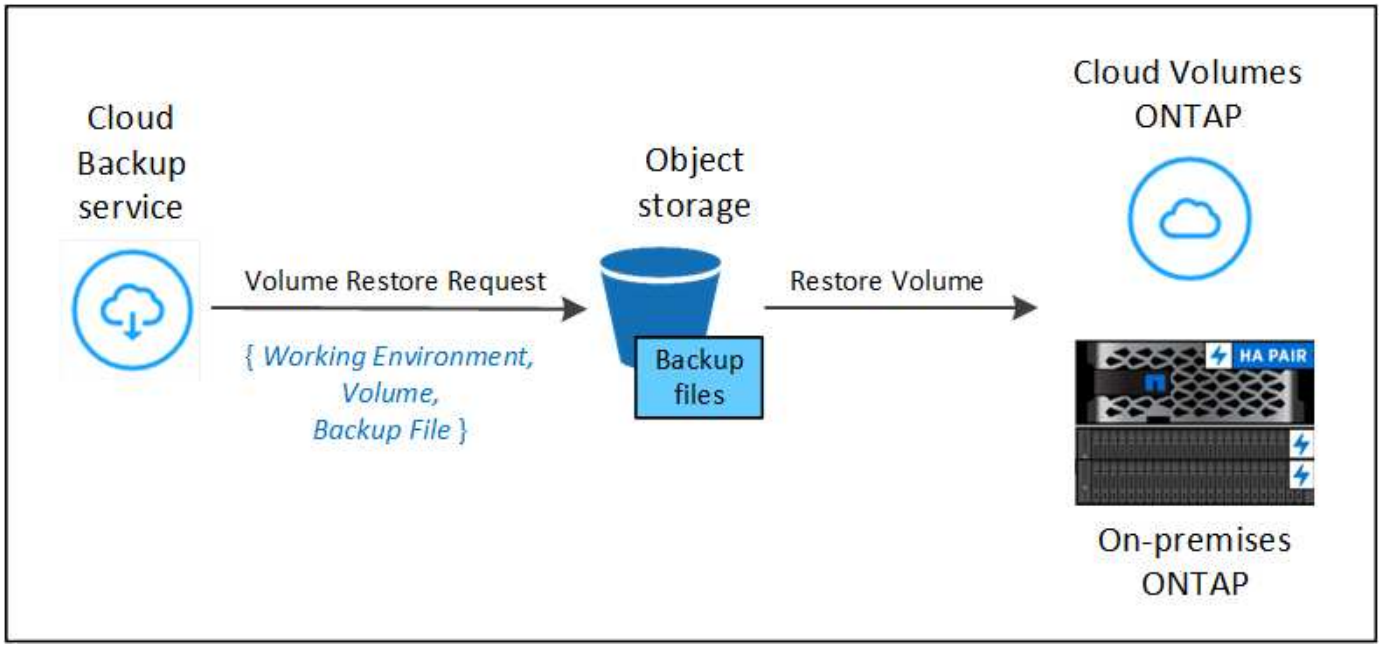
- Bei Amazon S3 kann der Connector in AWS oder lokal implementiert werden
- Für StorageGRID muss der Connector in Ihrem Haus bereitgestellt werden

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

> Sie können 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 anschließend auf die von Ihnen benötigten Dateien zugreifen.

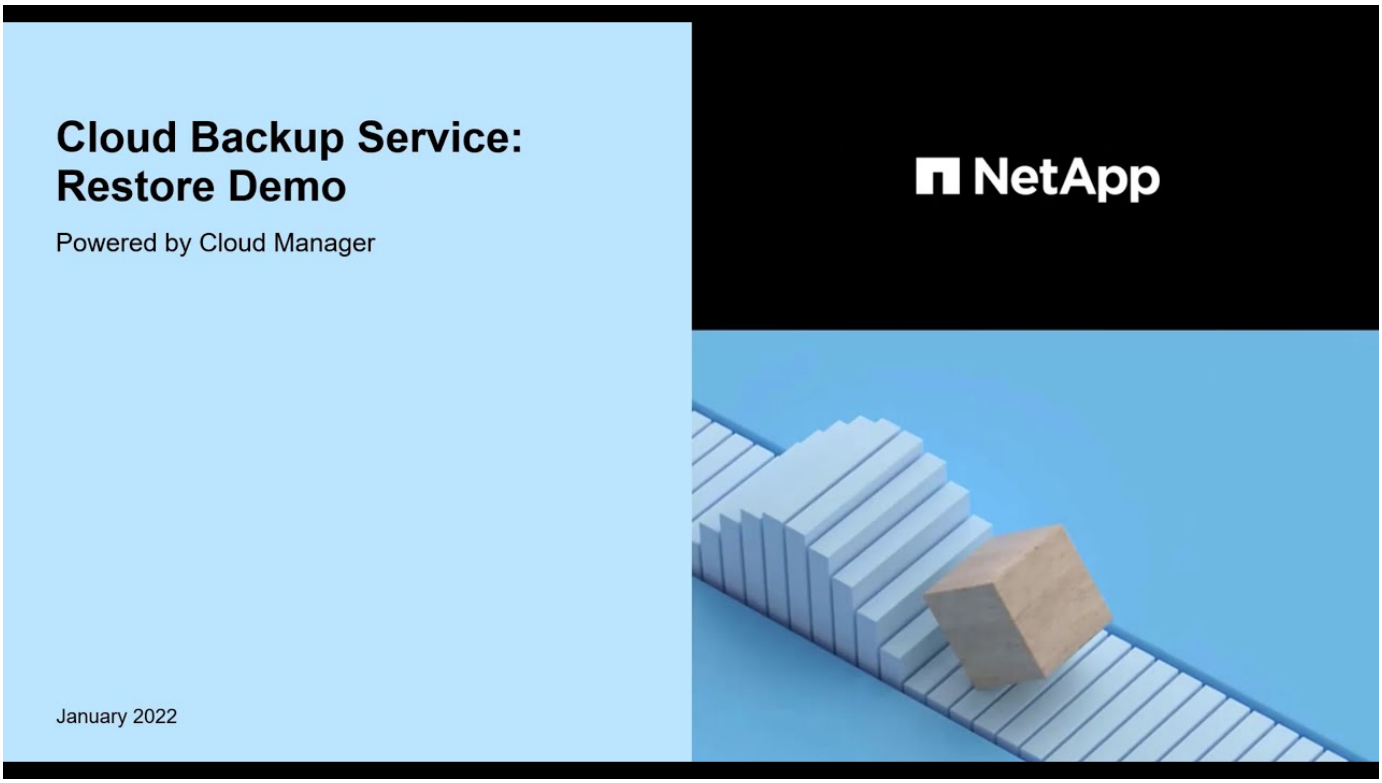
Wiederherstellen von Volumes mit Durchsuchen und Wiederherstellen

Wenn Sie ein Volume aus einer Backup-Datei wiederherstellen, erstellt Cloud Backup ein *neues* Volume, wobei die Daten aus dem Backup verwendet werden. Sie können die Daten auf einem Volume in der ursprünglichen Arbeitsumgebung oder in einer anderen Arbeitsumgebung wiederherstellen, die sich in demselben Cloud-Konto wie die Arbeitsumgebung der Quelle befindet. Sie können Volumes auch in einem ONTAP System vor Ort wiederherstellen.



Wie Sie sehen, müssen Sie den Namen der Arbeitsumgebung, den Namen des Volumes und das Datum der Sicherungsdatei kennen, um eine Wiederherstellung des Volumes durchzuführen.

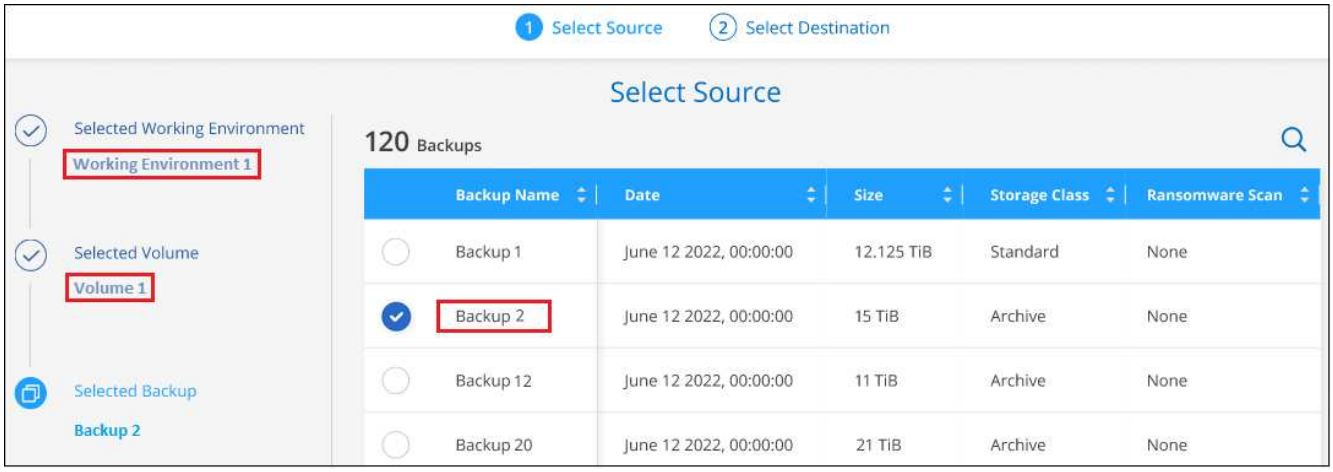
Das folgende Video zeigt einen kurzen Spaziergang zur Wiederherstellung eines Volumens:



Schritte

1. Wählen Sie im Menü BlueXP die Option **Schutz > Sicherung und Wiederherstellung**.
2. Klicken Sie auf die Registerkarte **Wiederherstellen**, und das Dashboard wiederherstellen wird angezeigt.
3. Klicken Sie im Abschnitt „*Browse & Restore*“ auf **Volume wiederherstellen**.

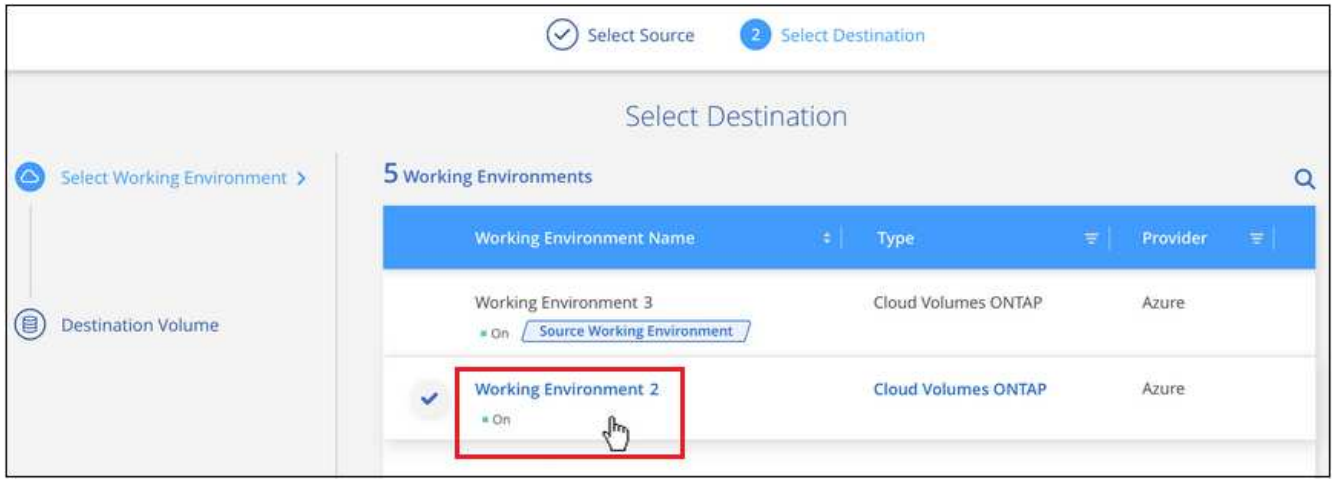
4. Navigieren Sie auf der Seite *Quelle auswählen* zur Sicherungsdatei für das Volume, das Sie wiederherstellen möchten. Wählen Sie die Datei * Working Environment*, **Volume** und die Datei **Backup** aus, die den Datums-/Zeitstempel enthält, aus dem Sie wiederherstellen möchten.



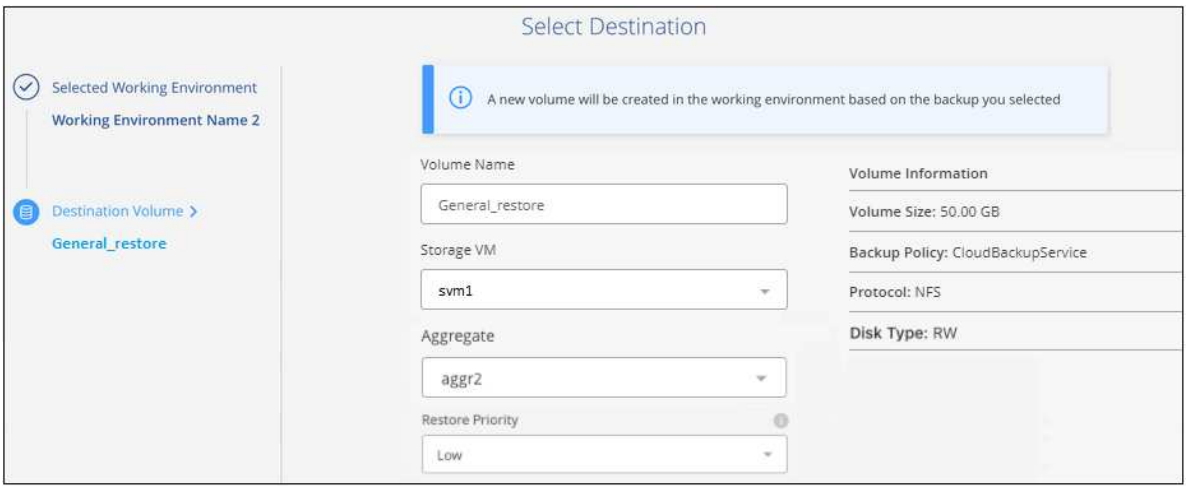
5. Klicken Sie Auf **Weiter**.

   Sollte der Ransomware-Schutz für die Backup-Datei aktiv sein (wenn Sie DataLock und Ransomware-Schutz in der Backup-Richtlinie aktiviert haben), werden Sie aufgefordert, vor dem Wiederherstellen der Daten einen zusätzlichen Ransomware-Scan auf der Backup-Datei durchzuführen. Wir empfehlen, die Backup-Datei nach Ransomware zu scannen.

6. Wählen Sie auf der Seite *Ziel auswählen* die Option **Arbeitsumgebung** aus, in der Sie das Volume wiederherstellen möchten.



7. Wenn Sie ein lokales ONTAP System auswählen und die Cluster-Verbindung mit dem Objekt-Storage nicht bereits konfiguriert haben, werden zusätzliche Informationen benötigt:
   - Wählen Sie bei der Wiederherstellung aus Amazon S3 den IPspace im ONTAP Cluster aus, auf dem sich das Ziel-Volume befindet, und 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 geben. Wählen Sie optional einen privaten VPC-Endpunkt für den sicheren Datentransfer aus.
     - Geben Sie beim Wiederherstellen aus StorageGRID den FQDN des StorageGRID-Servers und den Port ein, den ONTAP für die HTTPS-Kommunikation mit StorageGRID verwenden soll, wählen Sie den Zugriffsschlüssel und den geheimen Schlüssel aus, der für den Zugriff auf den Objektspeicher erforderlich ist, und den IPspace im ONTAP-Cluster, in dem sich das Ziel-Volume befindet.
       a. Geben Sie den Namen ein, den Sie für das wiederhergestellte Volume verwenden möchten, und wählen Sie die Storage VM und das Aggregat aus, auf dem sich das Volume befinden soll. Standardmäßig wird **<source_Volume_Name>_restore** als Volume-Name verwendet.



Wenn Sie das Volume aus einer Sicherungsdatei wiederherstellen, die sich in einer Archiv-Storage-Ebene befindet (verfügbar ab ONTAP 9.10.1), können Sie die Restore-Priorität auswählen.

"Erfahren Sie mehr über die Wiederherstellung aus AWS Archiv-Storage".

1. Klicken Sie auf **Wiederherstellen** und Sie werden wieder zum Restore Dashboard zurückgekehrt, damit Sie den Fortschritt des Wiederherstellungsvorgangs überprüfen können.

Ergebnis

Cloud Backup erstellt auf Basis des ausgewählten Backups ein neues Volume. Das können Sie "Verwalten Sie die Backup-Einstellungen für dieses neue Volume" Nach Bedarf.

Beachten Sie, dass die Wiederherstellung eines Volumes aus einer Backup-Datei im Archiv-Storage je nach Archivebene und Restore-Priorität viele Minuten oder Stunden in Anspruch nehmen kann. Sie können auf die Registerkarte **Job Monitoring** klicken, um den Wiederherstellungsfortschritt anzuzeigen.

Wiederherstellen von Ordnern und Dateien mit Durchsuchen und Wiederherstellen

Wenn Sie nur einige Dateien aus einem ONTAP Volume-Backup wiederherstellen müssen, können Sie einen Ordner oder einzelne Dateien wiederherstellen, anstatt das gesamte Volume wiederherzustellen. Sie können Ordner und Dateien in einem vorhandenen Volume in der ursprünglichen Arbeitsumgebung oder in einer anderen Arbeitsumgebung wiederherstellen, die dasselbe Cloud-Konto verwendet. Ordner und Dateien können auch auf einem Volume auf einem lokalen ONTAP System wiederhergestellt werden.

Wenn Sie mehrere Dateien auswählen, werden alle Dateien auf dem gleichen Ziellaufwerk wiederhergestellt, das Sie auswählen. Wenn Sie also Dateien auf unterschiedlichen Volumes wiederherstellen möchten, müssen Sie den Wiederherstellungsprozess mehrmals ausführen.

Derzeit können Sie nur einen einzigen Ordner auswählen und wiederherstellen. Und nur Dateien aus diesem Ordner werden wiederhergestellt - keine Unterordner oder Dateien in Unterordnern werden wiederhergestellt.

- Sie können 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 anschließend auf die von Ihnen benötigten Dateien zugreifen.
- Die Wiederherstellung auf Ordnerebene wird derzeit nicht unterstützt, wenn sich die Sicherungsdatei im Archiv-Speicher befindet. In diesem Fall können Sie den Ordner aus einer neueren Sicherungsdatei wiederherstellen, die nicht archiviert wurde, oder Sie können das gesamte Volume aus dem archivierten Backup wiederherstellen und dann auf den gewünschten Ordner und die Dateien zugreifen.

Voraussetzungen

- Die ONTAP-Version muss mindestens 9.6 sein, um *File* Restore-Vorgänge durchzuführen.
- Die ONTAP-Version muss mindestens 9.11.1 sein, um Vorgänge *folder* wiederherstellen zu können. Ifdef::aws[]

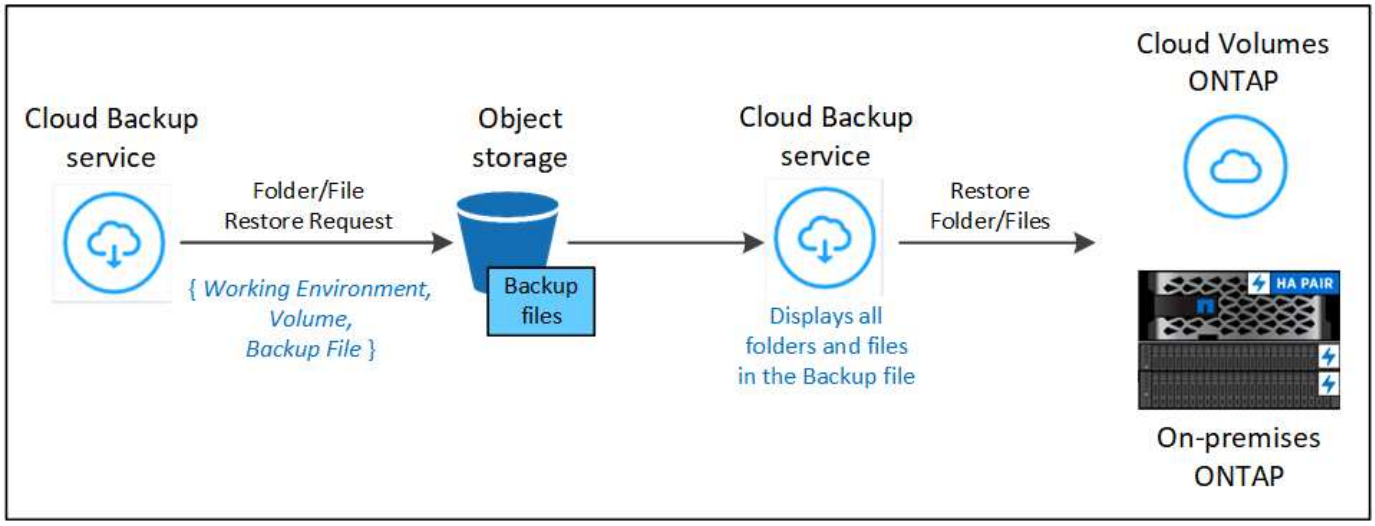
Wiederherstellung von Ordnern und Dateien

Der Prozess geht wie folgt vor:

1. Wenn Sie einen Ordner oder eine oder mehrere Dateien aus einem Volume-Backup wiederherstellen möchten, klicken Sie auf die Registerkarte **Wiederherstellen** und klicken Sie unter *Durchsuchen & Wiederherstellen* auf **Dateien oder Ordner**.
2. Wählen Sie die Arbeitsumgebung, das Volume und die Sicherungsdatei aus, in der sich der Ordner oder die Datei(en) befinden.
3. Cloud Backup zeigt die Ordner und Dateien an, die in der ausgewählten Sicherungsdatei vorhanden sind.
4. Wählen Sie den Ordner oder die Datei(en) aus, die Sie aus diesem Backup wiederherstellen möchten.
5. Wählen Sie den Zielspeicherort aus, an dem der Ordner oder die Dateien wiederhergestellt werden sollen

(Arbeitsumgebung, Volume und Ordner), und klicken Sie auf **Wiederherstellen**.

6. Die Datei(en) wird(n) wiederhergestellt.

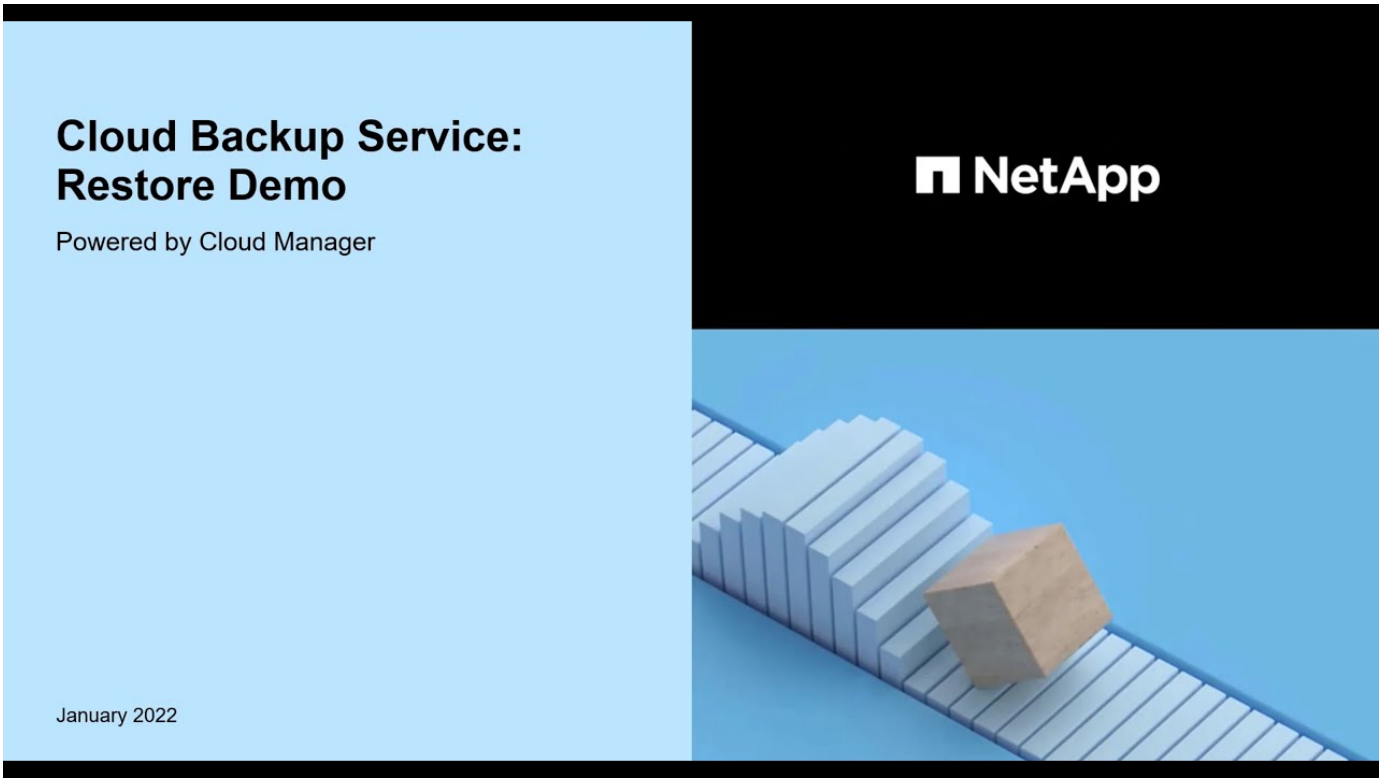


Wie Sie sehen, müssen Sie den Namen der Arbeitsumgebung, den Namen des Volumes, das Datum der Sicherungsdatei und den Ordner-/Dateinamen kennen, um einen Ordner oder eine Dateiwiederherstellung durchzuführen.

Ordner und Dateien werden wiederhergestellt

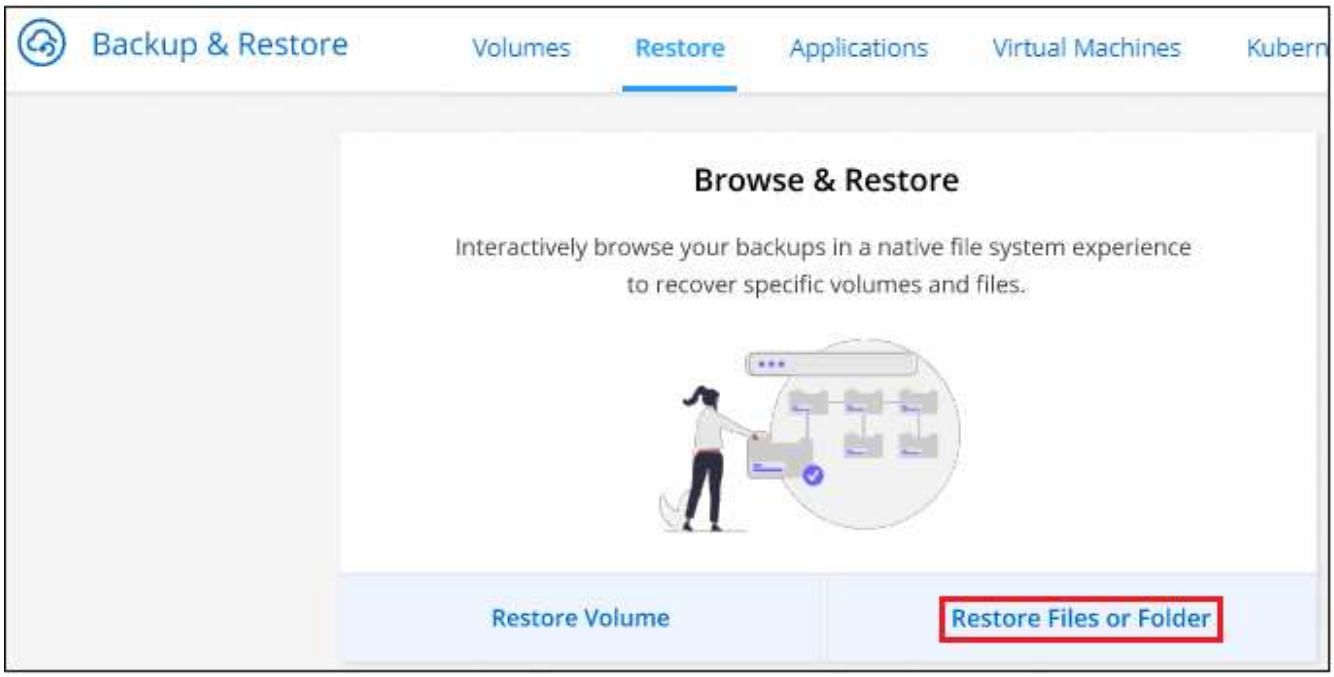
Führen Sie diese Schritte aus, um Ordner oder Dateien auf einem Volume von einem ONTAP Volume-Backup wiederherzustellen. Sie sollten den Namen des Volumes und das Datum der Sicherungsdatei kennen, die Sie zum Wiederherstellen des Ordners oder der Datei(en) verwenden möchten. Diese Funktion verwendet Live Browsing, so dass Sie die Liste der Verzeichnisse und Dateien innerhalb jeder Backup-Datei anzeigen können.

Das folgende Video zeigt einen kurzen Rundgang durch die Wiederherstellung einer einzelnen Datei:

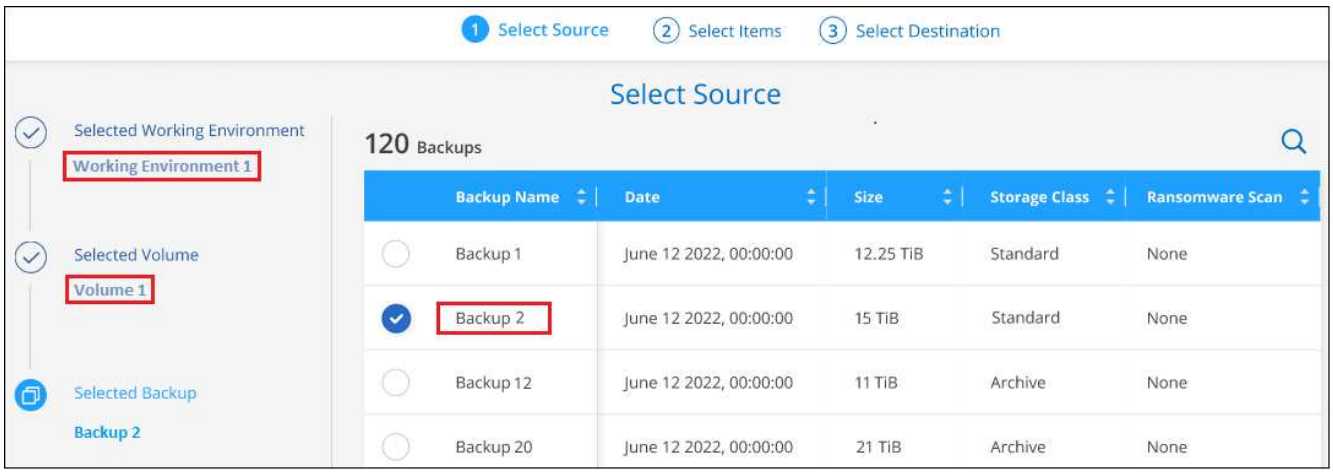


Schritte

1. Wählen Sie im Menü BlueXP die Option **Schutz > Sicherung und Wiederherstellung**.
2. Klicken Sie auf die Registerkarte **Wiederherstellen**, und das Dashboard wiederherstellen wird angezeigt.
3. Klicken Sie im Abschnitt *Durchsuchen & Wiederherstellen* auf **Dateien oder Ordner wiederherstellen**.



4. Navigieren Sie auf der Seite *Quelle auswählen* zur Sicherungsdatei für das Volume, das den Ordner oder die Dateien enthält, die wiederhergestellt werden sollen. Wählen Sie die **Arbeitsumgebung**, das **Volume** und den **Backup** aus, der den Datums-/Zeitstempel enthält, aus dem Sie Dateien wiederherstellen möchten.



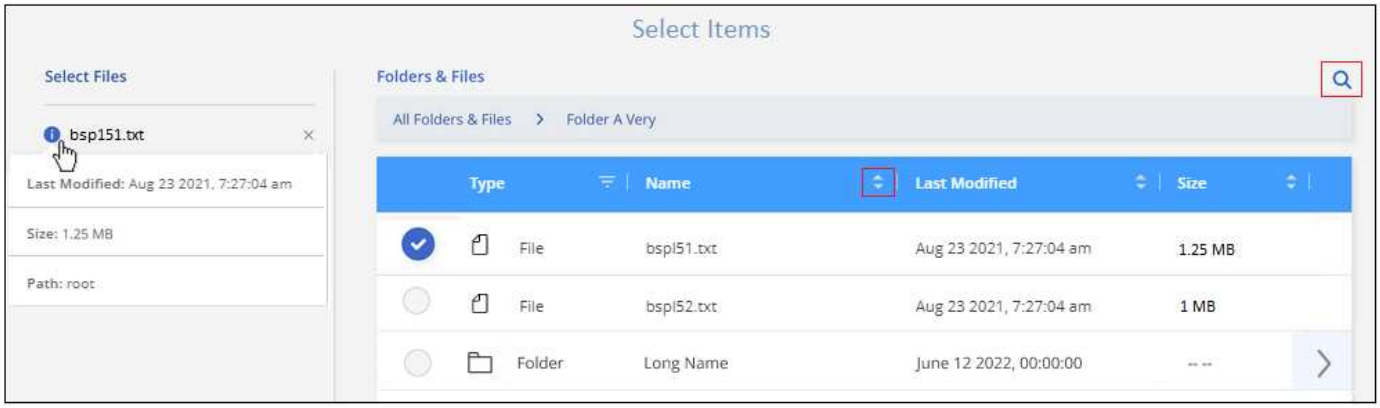
5. Klicken Sie auf **Weiter** und die Liste der Ordner und Dateien aus der Volume-Sicherung wird angezeigt.

   Wenn Sie Ordner oder Dateien aus einer Sicherungsdatei wiederherstellen, die sich in einer Archivspeicherebene befindet (verfügbar ab ONTAP 9.10.1), können Sie die Priorität wiederherstellen auswählen.

"Erfahren Sie mehr über die Wiederherstellung aus AWS Archiv-Storage".

+ und falls Ransomware-Schutz für die Backup-Datei aktiv ist (wenn Sie DataLock und Ransomware-Schutz in der Backup-Policy aktiviert), dann werden Sie aufgefordert, einen zusätzlichen Ransomware-Scan auf der Backup-Datei vor der Wiederherstellung der Daten auszuführen. Wir empfehlen, die Backup-Datei nach Ransomware zu scannen.

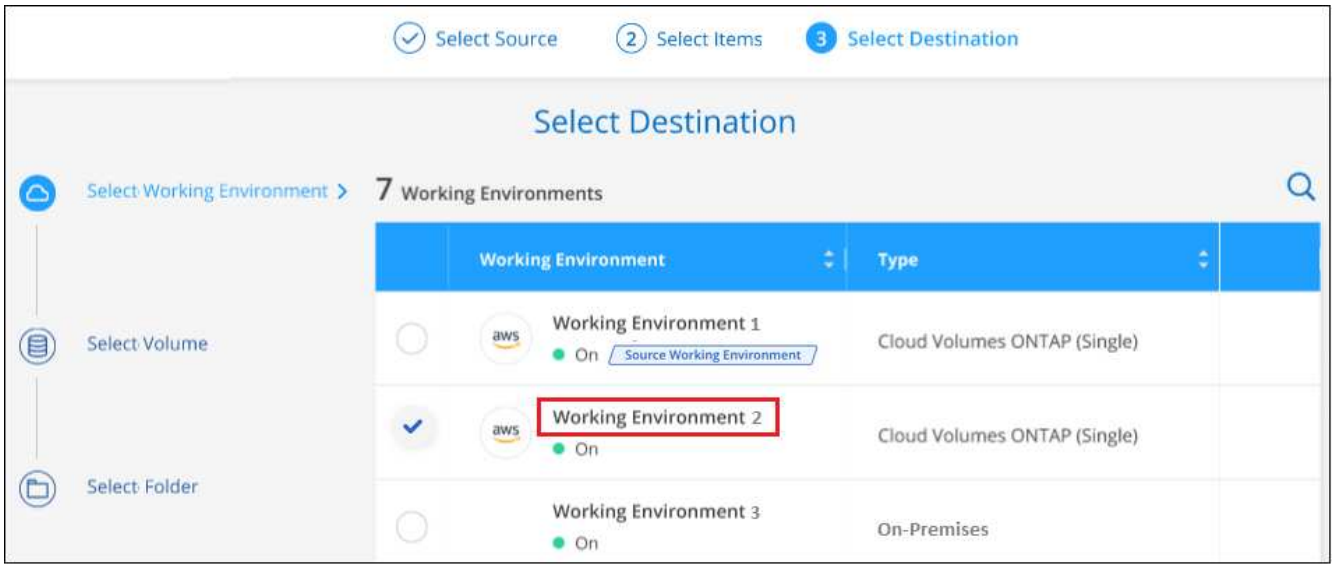
+



1. Wählen Sie auf der Seite „ Elemente auswählen_“ den Ordner oder die Datei(en) aus, die wiederhergestellt werden sollen, und klicken Sie auf **Weiter**. So finden Sie das Element:
   - Sie können auf den Ordner oder den Dateinamen klicken, wenn Sie ihn sehen.
   - Sie können auf das Suchsymbol klicken und den Namen des Ordners oder der Datei eingeben, um direkt zum Element zu navigieren.
   - Sie können Ebenen in Ordnern mithilfe des nach unten navigieren Schaltfläche am Ende der Zeile, um bestimmte Dateien zu finden.

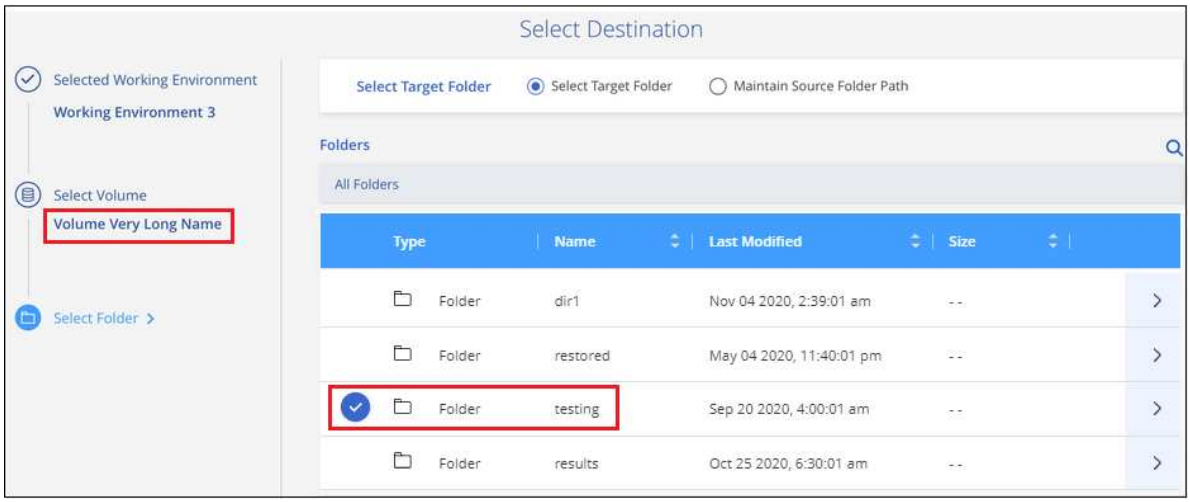
     Wenn Sie Dateien auswählen, werden sie auf der linken Seite der Seite hinzugefügt, damit Sie die Dateien sehen können, die Sie bereits ausgewählt haben. Sie können bei Bedarf eine Datei aus dieser Liste entfernen, indem Sie neben dem Dateinamen auf das **x** klicken.

2. Wählen Sie auf der Seite *Ziel auswählen* die Option **Arbeitsumgebung** aus, in der Sie die Elemente wiederherstellen möchten.



Wenn Sie ein On-Premises-Cluster auswählen und noch nicht die Cluster-Verbindung mit dem Objekt-Storage konfiguriert haben, werden zusätzliche Informationen benötigt:

- Bei der Wiederherstellung aus Amazon S3 geben Sie den IPspace im ONTAP Cluster ein, in dem sich das Ziel-Volume befindet, sowie den AWS Zugriffsschlüssel und den geheimen Schlüssel, die für den Zugriff auf den Objekt-Storage erforderlich sind. Sie können auch eine private Link-Konfiguration für die Verbindung zum Cluster auswählen.
  - Geben Sie beim Wiederherstellen aus StorageGRID den FQDN des StorageGRID-Servers und den Port ein, den ONTAP für die HTTPS-Kommunikation mit StorageGRID verwenden soll, geben Sie den Zugriffsschlüssel und den geheimen Schlüssel ein, der für den Zugriff auf den Objektspeicher erforderlich ist, sowie den IPspace im ONTAP-Cluster, in dem sich das Ziel-Volume befindet.
    a. Wählen Sie dann den **Volume** und den **Ordner** aus, in dem Sie den Ordner oder die Datei(en) wiederherstellen möchten.



Sie haben ein paar Optionen für den Speicherort beim Wiederherstellen von Ordnern und Dateien.

- Wenn Sie **Zielordner auswählen**, wie oben gezeigt:
  - Sie können einen beliebigen Ordner auswählen.
  - Sie können den Mauszeiger auf einen Ordner bewegen und auf klicken Am Ende der Zeile, um in Unterordner zu bohren, und wählen Sie dann einen Ordner aus.
- Wenn Sie dieselbe Arbeitsumgebung und dasselbe Volume ausgewählt haben, als wo sich der Quellordner/die Datei befand, können Sie **Quellordner-Pfad verwalten** auswählen, um den Ordner oder die Datei(en) in demselben Ordner wiederherzustellen, in dem sie sich in der Quellstruktur befanden. Alle Ordner und Unterordner müssen bereits vorhanden sein; Ordner werden nicht erstellt. Beim Wiederherstellen der Dateien an ihrem ursprünglichen Speicherort können Sie die Quelldatei(en) überschreiben oder neue Dateien erstellen.
  a. Klicken Sie auf **Wiederherstellen** und Sie werden wieder zum Restore Dashboard zurückgekehrt, damit Sie den Fortschritt des Wiederherstellungsvorgangs überprüfen können. Sie können auch auf die Registerkarte **Job Monitoring** klicken, um den Wiederherstellungsfortschritt anzuzeigen.

Wiederherstellen von ONTAP-Daten mithilfe von Suche und Wiederherstellung

Sie können ein Volume, einen Ordner oder Dateien aus einer ONTAP-Sicherungsdatei mithilfe von Suchen und Wiederherstellen wiederherstellen wiederherstellen. Mit Search & Restore lassen sich anhand aller im Cloud Storage gespeicherten Backups nach einem bestimmten Volume, Ordner oder Datei suchen und anschließend eine Wiederherstellung durchführen. Sie müssen nicht den genauen Namen der Arbeitsumgebung oder den Namen des Volumes kennen - die Suche durchsucht alle Volume-Backup-Dateien.

Der Suchvorgang sieht auch alle lokalen Snapshot-Kopien aus, die auch für Ihre ONTAP Volumes vorhanden sind. Da das Wiederherstellen von Daten aus einer lokalen Snapshot-Kopie schneller und kostengünstiger ist als die Wiederherstellung aus einer Backup-Datei, möchten Sie möglicherweise Daten aus dem Snapshot wiederherstellen. Sie können den Snapshot als neues Volume von der Seite Volume Details auf dem Bildschirm wiederherstellen.

Wenn Sie ein Volume aus einer Backup-Datei wiederherstellen, erstellt Cloud Backup ein *neues* Volume, wobei die Daten aus dem Backup verwendet werden. Sie können die Daten als Volume in der ursprünglichen Arbeitsumgebung oder in einer anderen Arbeitsumgebung wiederherstellen, die sich in demselben Cloud-Konto wie die Arbeitsumgebung der Quelle befindet. Sie können Volumes auch in einem ONTAP System vor Ort wiederherstellen.

Sie können Ordner oder Dateien auf dem ursprünglichen Volume-Speicherort, auf einem anderen Volume in derselben Arbeitsumgebung oder in einer anderen Arbeitsumgebung wiederherstellen, die dasselbe Cloud-Konto verwendet. Ordner und Dateien können auch auf einem Volume auf einem lokalen ONTAP System wiederhergestellt werden.

Wenn die Backup-Datei für das wiederherzustellende Volume im Archiv-Storage (ab ONTAP 9.10.1 verfügbar) gespeichert ist, dauert der Restore-Vorgang länger und es entstehen zusätzliche Kosten. Beachten Sie, dass auf dem Ziel-Cluster ONTAP 9.10.1 oder höher für Volume-Wiederherstellung, 9.11.1 für Dateiwiederherstellung und 9.12.1 für Google Archive ausgeführt werden muss.

"Erfahren Sie mehr über die Wiederherstellung aus AWS Archiv-Storage".

- Sie können 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 anschließend auf die von Ihnen benötigten Dateien zugreifen.
- Die Wiederherstellung auf Ordnerebene wird derzeit nicht unterstützt, wenn sich die Sicherungsdatei im Archiv-Speicher befindet. In diesem Fall können Sie den Ordner aus einer neueren Sicherungsdatei wiederherstellen, die nicht archiviert wurde, oder Sie können das gesamte Volume aus dem archivierten Backup wiederherstellen und dann auf den gewünschten Ordner und die Dateien zugreifen.

Bevor Sie beginnen, sollten Sie eine Vorstellung von dem Namen oder Speicherort des Volumes oder der Datei haben, die Sie wiederherstellen möchten.

Das folgende Video zeigt einen kurzen Rundgang durch die Wiederherstellung einer einzelnen Datei:

Unterstützte Arbeitsumgebungen und Objektspeicheranbieter suchen und wiederherstellen

Sie können ein Volume, einen Ordner oder einzelne Dateien aus einer ONTAP-Sicherungsdatei in folgenden Arbeitsumgebungen wiederherstellen:

Speicherort Der Sicherungsdatei	Zielarbeitsumgebung ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP in AWS On-Premises ONTAP System endif::aws[] ifdef::azurAzure[]
Azure Blob	Cloud Volumes ONTAP in Azure On-Premises ONTAP System endif::Azure[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP in Google On-Premises ONTAP System endif::gcp[]
NetApp StorageGRID	Lokales ONTAP System

Für die Suche und Wiederherstellung kann der Connector an folgenden Orten installiert werden:

- Bei Amazon S3 kann der Connector in AWS oder lokal implementiert werden
- Für StorageGRID muss der Connector in Ihrem Haus bereitgestellt werden; mit Internetverbindung

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

Voraussetzungen

- Cluster-Anforderungen:
  - Die ONTAP-Version muss 9.8 oder höher sein.
  - Die Storage-VM (SVM), auf der sich das Volume befindet, muss über eine konfigurierte Daten-LIF

verfügen.

  - NFS muss auf dem Volume aktiviert sein.
  - Der SnapDiff RPC Server muss auf der SVM aktiviert sein. BlueXP führt diese Funktion automatisch aus, wenn Sie die Indexierung in der Arbeitsumgebung aktivieren.

- AWS-Anforderungen:
  - Spezifische Berechtigungen für Amazon Athena, AWS Glue und AWS S3 müssen der Benutzerrolle hinzugefügt werden, die BlueXP Berechtigungen bietet. "Stellen Sie sicher, dass alle Berechtigungen korrekt konfiguriert sind".

    Beachten Sie, dass wenn Sie Cloud Backup bereits mit einem zuvor konfigurierten Connector verwenden, Sie jetzt die Athena- und Glue-Berechtigungen zur BlueXP-Benutzerrolle hinzufügen müssen. Diese sind neu und für die Suche und Wiederherstellung erforderlich.

- StorageGRID-Anforderungen:

  Je nach Konfiguration gibt es zwei Möglichkeiten, die Suche und Wiederherstellung zu implementieren:

  - Wenn Ihr Konto keine Anmeldedaten für Cloud-Provider enthält, werden die Informationen zum indexierten Katalog auf dem Connector gespeichert.
  - Wenn Sie haben "AWS Zugangsdaten" Oder "Azure Zugangsdaten" Im Konto wird der indizierte Katalog wie bei einem in der Cloud implementierten Connector beim Cloud-Provider gespeichert. (Bei beiden Anmeldedaten ist standardmäßig AWS ausgewählt.)

    Obwohl Sie einen On-Premises-Connector nutzen, müssen die Anforderungen an einen Cloud-Provider sowohl im Hinblick auf die Berechtigungen von Connector als auch auf Ressourcen von Cloud-Providern erfüllt werden. AWS und Azure Anforderungen können Sie sich bei der Verwendung dieser Implementierung oben anzeigen lassen.

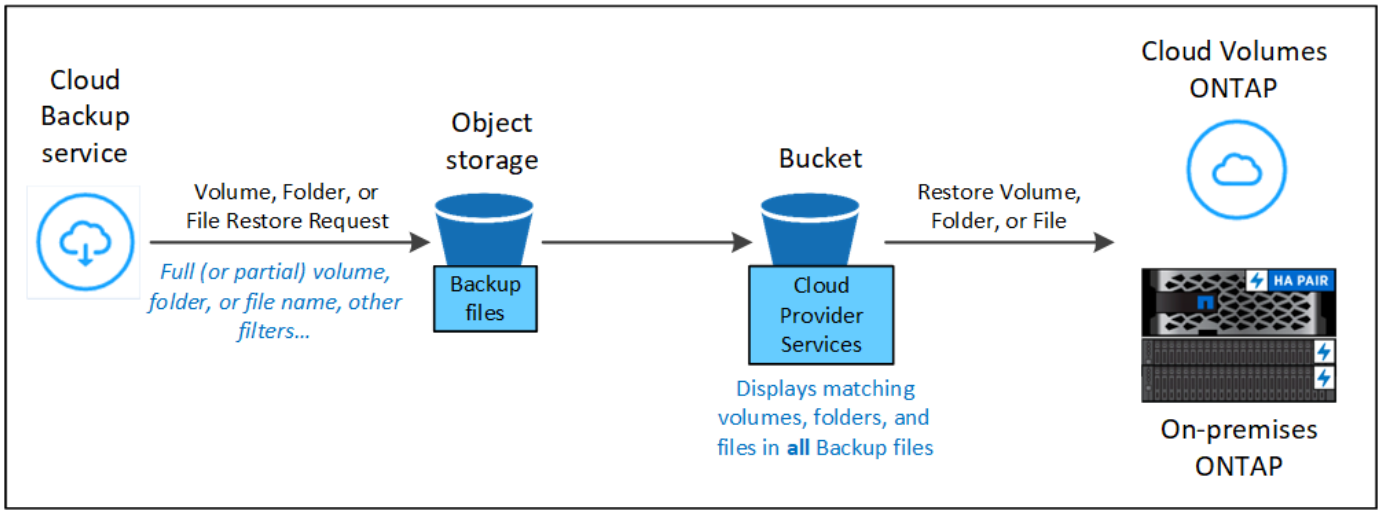
Such- und Wiederherstellungsvorgang

Der Prozess geht wie folgt vor:

1. Bevor Sie Suche und Wiederherstellung verwenden können, müssen Sie „Indizierung“ in jeder Arbeitsumgebung aktivieren, aus der Sie Volume-Daten wiederherstellen möchten. So kann der indizierte Katalog die Backup-Dateien für jedes Volume nachverfolgen.
2. Wenn Sie ein Volume oder Dateien aus einem Volume-Backup wiederherstellen möchten, klicken Sie unter *Search & Restore* auf **Suchen & Wiederherstellen**.
3. Geben Sie die Suchkriterien für ein Volume, einen Ordner oder eine Datei nach einem Teil- oder Volldatumnamen, einem partiellen oder vollständigen Dateinamen, einem Größenbereich, einem Erstellungsdatumbereich und anderen Suchfiltern ein, und klicken Sie auf **Suchen**.

   Auf der Seite Suchergebnisse werden alle Standorte angezeigt, die eine Datei oder ein Volume haben, die Ihren Suchkriterien entsprechen.

4. Klicken Sie auf **Alle Backups** für den Speicherort, den Sie verwenden möchten, um den Datenträger oder die Datei wiederherzustellen, und klicken Sie dann auf **Wiederherstellen** für die eigentliche Sicherungsdatei, die Sie verwenden möchten.
5. Wählen Sie den Speicherort aus, an dem die Volume-, Ordner- oder Datei(en) wiederhergestellt werden sollen, und klicken Sie auf **Wiederherstellen**.
6. Volume, Ordner oder Datei(en) werden wiederhergestellt.



Wie Sie sehen können, müssen Sie wirklich nur einen Teilnamen kennen und Cloud Backup sucht durch alle Backup-Dateien, die zu Ihrer Suche passen.

Aktivierung des indizierten Katalogs für jede Arbeitsumgebung

Bevor Sie Search & Restore verwenden können, müssen Sie „Indizierung“ in jeder Arbeitsumgebung aktivieren, aus der Sie Volumes oder Dateien wiederherstellen möchten. So kann der indexierte Katalog jedes Volume und jede Backup-Datei nachverfolgen, was Ihre Suchvorgänge sehr schnell und effizient macht.

Wenn Sie diese Funktion aktivieren, aktiviert Cloud Backup SnapDiff v3 auf der SVM für Ihre Volumes und führt folgende Aktionen durch:

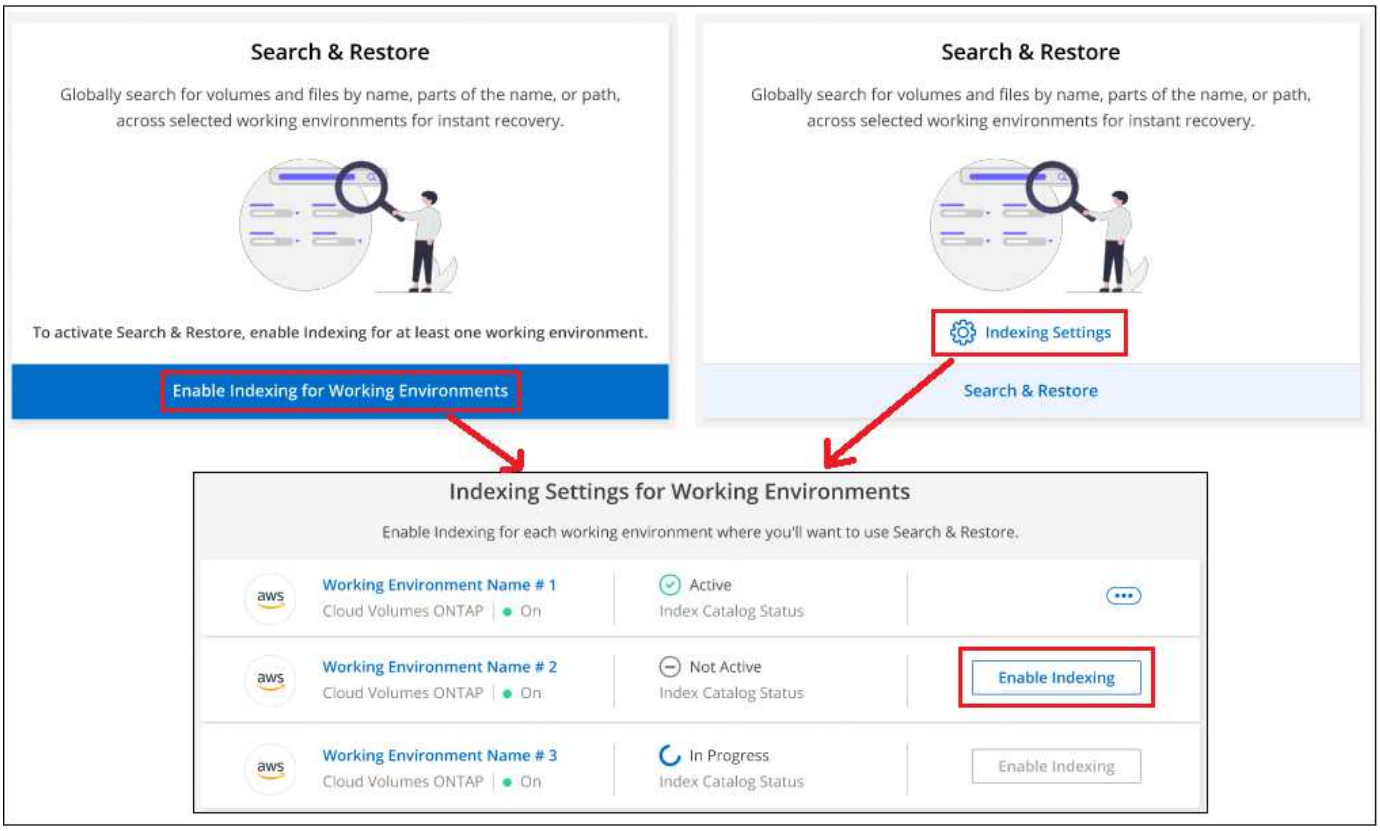
- Für Backups, die in AWS gespeichert werden, stellt die Software einen neuen S3-Bucket und den bereit "Interaktive Abfrage-Service von Amazon Athena" Und "AWS Glue serverloser Datenintegrations-Service".
- Für Backups, die in StorageGRID gespeichert sind, stellt das Unternehmen Speicherplatz auf dem Connector oder der Cloud-Provider-Umgebung bereit.

Wenn die Indexierung bereits für Ihre Arbeitsumgebung aktiviert wurde, rufen Sie den nächsten Abschnitt auf, um Ihre Daten wiederherzustellen.

So aktivieren Sie die Indizierung für eine Arbeitsumgebung:

- Wenn keine Arbeitsumgebungen indiziert wurden, klicken Sie im Restore Dashboard unter *Search & Restore* auf **Indizierung für Arbeitsumgebungen aktivieren** und klicken Sie für die Arbeitsumgebung auf **Indizierung aktivieren**.
- Wenn mindestens eine Arbeitsumgebung indiziert wurde, klicken Sie auf dem Restore Dashboard unter *Search & Restore* auf **Indexing Settings** und klicken Sie für die Arbeitsumgebung auf **Indizierung aktivieren**.

Nachdem alle Services bereitgestellt und der indizierte Katalog aktiviert wurde, wird die Arbeitsumgebung als „aktiv“ angezeigt.



In Abhängigkeit von der Größe der Volumes in der Arbeitsumgebung und der Anzahl der Backup-Dateien in der Cloud kann die Erstindizierung bis zu eine Stunde in Anspruch nehmen. Danach wird es stündlich transparent mit inkrementellen Änderungen aktualisiert, um auf dem Laufenden zu bleiben.

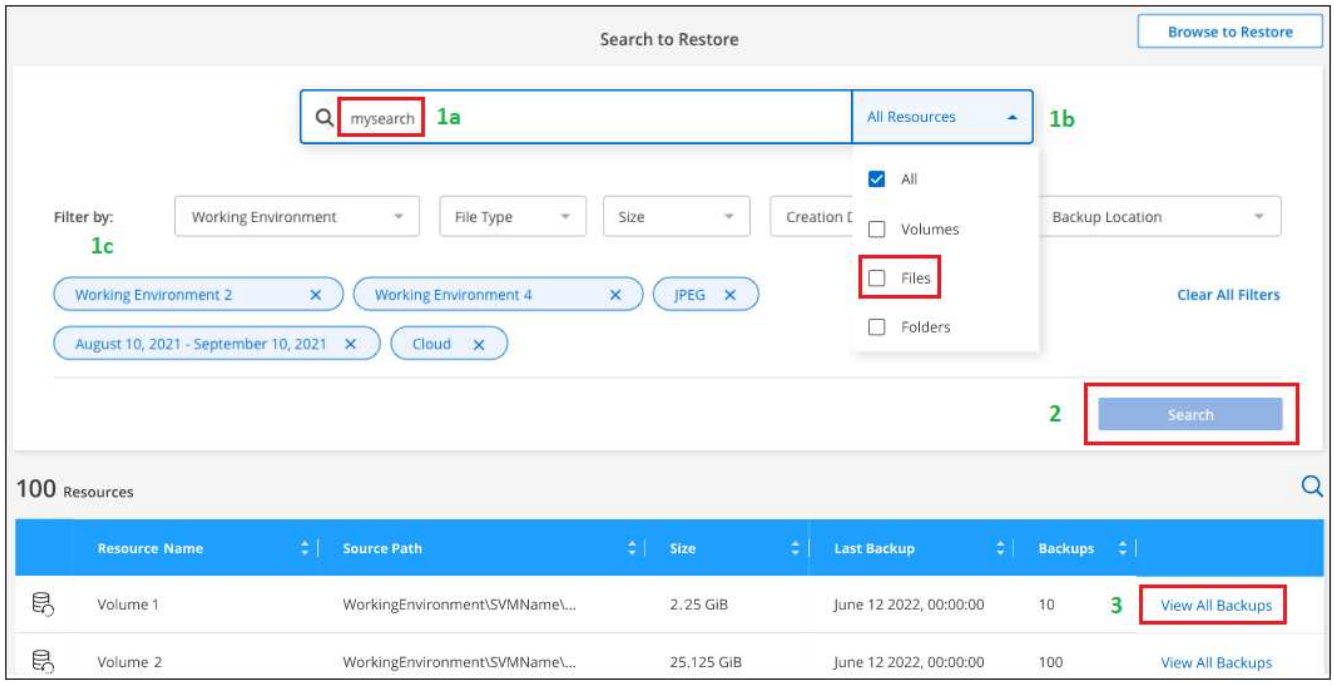
Wiederherstellen von Volumes, Ordnern und Dateien mithilfe von Search & Restore

Nachdem Sie den haben Indexierung für Ihre Arbeitsumgebung aktiviert, Sie können Volumes, Ordner und Dateien mit Search & Restore wiederherstellen. So können Sie mithilfe verschiedener Filter genau die Datei oder das Volume finden, die Sie aus allen Backup-Dateien wiederherstellen möchten.

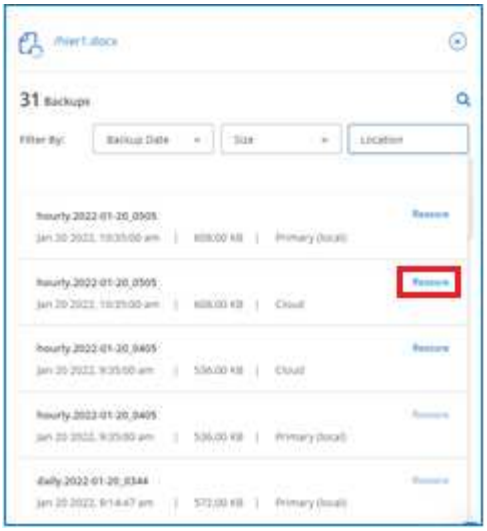
Schritte

1. Wählen Sie im Menü BlueXP die Option **Schutz > Sicherung und Wiederherstellung**.
2. Klicken Sie auf die Registerkarte **Wiederherstellen**, und das Dashboard wiederherstellen wird angezeigt.
3. Klicken Sie im Abschnitt *Suchen & Wiederherstellen* auf **Suchen & Wiederherstellen**.

4. Auf der Seite „Suche nach Wiederherstellung“:
   a. Geben Sie in der *Suchleiste* einen vollständigen oder teilweisen Volumennamen, Ordnernamen oder Dateinamen ein.
   b. Wählen Sie den Ressourcentyp aus: **Volumes**, **Dateien**, **Ordner** oder **Alle**.
   c. Wählen Sie im Bereich *Filter by* die Filterkriterien aus. Sie können beispielsweise die Arbeitsumgebung auswählen, in der sich die Daten befinden, und den Dateityp, z. B. eine JPEG-Datei.
5. Klicken Sie auf **Suchen** und im Bereich Suchergebnisse werden alle Ressourcen angezeigt, die eine Datei, einen Ordner oder ein Volume haben, das Ihrer Suche entspricht.



6. Klicken Sie auf **Alle Backups anzeigen** für die Ressource, die die wiederherzustellenden Daten enthält, um alle Sicherungsdateien anzuzeigen, die das entsprechende Volume, den Ordner oder die entsprechende Datei enthalten.



7. Klicken Sie auf **Wiederherstellen** für die Sicherungsdatei, die Sie verwenden möchten, um das Objekt aus der Cloud wiederherzustellen.

   Beachten Sie, dass die Ergebnisse auch lokale Volume-Snapshot-Kopien identifizieren, die die Datei in Ihrer Suche enthalten. Die **Restore** Taste funktioniert derzeit nicht für Snapshots, aber wenn Sie die Daten aus der Snapshot-Kopie anstelle der Backup-Datei wiederherstellen möchten, schreiben Sie den Namen und den Ort des Volumes auf, öffnen Sie die Seite Volume Details auf dem Bildschirm, Und verwenden Sie die Option **Wiederherstellen aus Snapshot Kopie**.

8. Wählen Sie den Zielspeicherort aus, an dem die Volumes, Ordner oder Dateien wiederhergestellt werden sollen, und klicken Sie auf **Wiederherstellen**.
   - Für Volumes können Sie die ursprüngliche Ziel-Arbeitsumgebung auswählen oder eine andere Arbeitsumgebung auswählen.
   - Für Ordner können Sie den ursprünglichen Speicherort wiederherstellen oder einen alternativen Speicherort auswählen, einschließlich der Arbeitsumgebung, des Volumes und des Ordners.
   - Bei Dateien können Sie sie am ursprünglichen Speicherort wiederherstellen oder einen alternativen Speicherort auswählen, einschließlich Arbeitsumgebung, Volume und Ordner. Wenn Sie den ursprünglichen Speicherort auswählen, können Sie die Quelldatei(en) überschreiben oder neue(n) Dateien erstellen.

     Wenn Sie ein lokales ONTAP System auswählen und die Cluster-Verbindung mit dem Objekt-Storage nicht bereits konfiguriert haben, werden zusätzliche Informationen benötigt:

     - Wählen Sie bei der Wiederherstellung aus Amazon S3 den IPspace im ONTAP Cluster aus, auf dem sich das Ziel-Volume befindet, und 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 geben. Wählen Sie optional einen privaten VPC-Endpunkt für den sicheren Datentransfer aus. "Siehe Details zu diesen Anforderungen".
       - Geben Sie beim Wiederherstellen aus StorageGRID den FQDN des StorageGRID-Servers und den Port ein, den ONTAP für die HTTPS-Kommunikation mit StorageGRID verwenden soll, geben Sie den Zugriffsschlüssel und den geheimen Schlüssel ein, der für den Zugriff auf den Objektspeicher erforderlich ist, sowie den IPspace im ONTAP-Cluster, in dem sich das Ziel-Volume befindet. "Siehe Details zu diesen Anforderungen".

Ergebnisse

Die Volume-, Ordner- oder Datei(en) werden wiederhergestellt und Sie werden zum Restore Dashboard

zurückgebracht, damit Sie den Fortschritt des Wiederherstellungsvorgangs überprüfen können. Sie können auch auf die Registerkarte **Job Monitoring** klicken, um den Wiederherstellungsfortschritt anzuzeigen.

Für wiederhergestellte Volumes ist möglich "Verwalten Sie die Backup-Einstellungen für dieses neue Volume" Nach Bedarf.

Copyright-Informationen

Copyright © 2022 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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