Backup und Restore von ONTAP Daten

BlueXP backup and recovery

NetApp
June 11, 2025

Inhalt

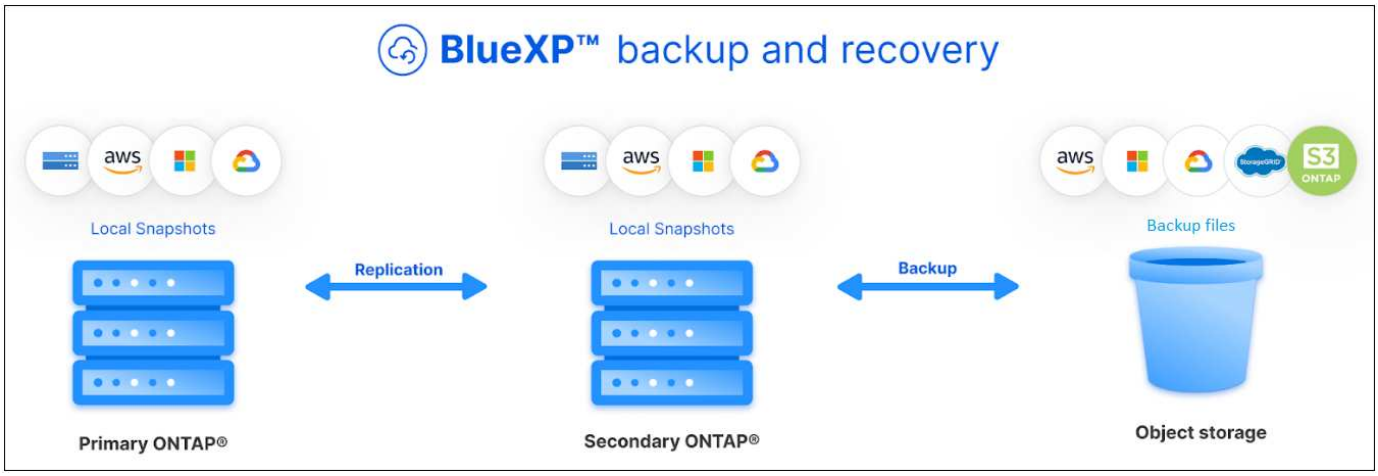
Backup und Restore von ONTAP Daten

Sichern Sie Ihre ONTAP Volume-Daten mit BlueXP Backup und Recovery

Der BlueXP Backup- und Recovery-Service bietet Backup- und Restore-Funktionen zum Schutz und zur langfristigen Archivierung Ihrer ONTAP Volume-Daten. Sie können eine 3-2-1-1-Strategie implementieren, bei der Sie 3 Kopien Ihrer Quelldaten auf 2 verschiedenen Storage-Systemen und 1 Kopie in der Cloud haben.

Nach Aktivierung werden mit Backup und Recovery dauerhaft inkrementelle Backups auf Block-Level erstellt, die auf einem anderen ONTAP Cluster und im Objekt-Storage in der Cloud gespeichert sind. Zusätzlich zu Ihrem Quell-Volume stehen Ihnen folgende Funktionen zur Verfügung:

- Snapshot Kopie des Volumes auf dem Quellsystem
- Repliziertes Volume auf einem anderen Storage-System
- Backup des Volumes im Objektspeicher



BlueXP Backup und Recovery nutzt die Datenreplizierungstechnologie SnapMirror von NetApp. So wird sichergestellt, dass alle Backups vollständig synchronisiert werden, indem Snapshot Kopien erstellt und an den Backup-Speicherort übertragen werden.

Der 3-2-1-5-Ansatz bietet unter anderem folgende Vorteile:

- Mehrere Datenkopien bieten mehrschichtigen Schutz vor internen (internen) und externen Cybersicherheitsbedrohungen.
- Mehrere Medientypen gewährleisten die Failover-Möglichkeit bei einem physischen oder logischen Ausfall eines Medientyps.
- Die vor-Ort-Kopie ermöglicht eine schnelle Wiederherstellung, da die externen Kopien bereit sind, nur für den Fall, dass die vor-Ort-Kopie beeinträchtigt wird.

Bei Bedarf können Sie ein ganzes *Volume*, einen *Ordner* oder eine oder mehrere *Dateien* von einer beliebigen Sicherungskopie in dieselbe oder eine andere Arbeitsumgebung wiederherstellen.

Funktionen

Replikationsfunktionen:

- Replizierung von Daten zwischen ONTAP Storage-Systemen zur Unterstützung von Backup und Disaster Recovery
- Stellen Sie die Zuverlässigkeit Ihrer DR-Umgebung mit Hochverfügbarkeit sicher.
- Die native ONTAP-Verschlüsselung während der Übertragung wird über einen Pre-Shared Key (PSK) zwischen den beiden Systemen eingerichtet.
- Kopierte Daten sind unveränderlich, bis sie beschreibbar und einsatzbereit sind.
- Die Replikation ist selbstheilend bei einem Übertragungsfehler.
- Im Vergleich zum "BlueXP Replizierungsservice", Die Replizierung in BlueXP Backup und Recovery umfasst folgende Features:
  - Replizierung mehrerer FlexVol Volumes zu einem Zeitpunkt auf ein sekundäres System
  - Wiederherstellung eines replizierten Volumes auf dem Quellsystem oder auf einem anderen System über die Benutzeroberfläche.

Siehe "Einschränkungen bei der Replizierung" Sie erhalten eine Liste mit Replizierungsfunktionen, die bei BlueXP Backup und Recovery nicht verfügbar sind.

Backup-to-Object-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.
- Unveränderliche Backup-Dateien werden so gesperrt und über den Aufbewahrungszeitraum geschützt.
- 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.
- 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:

- Stellen Sie Daten von einem bestimmten Zeitpunkt aus lokalen Snapshot Kopien, replizierten Volumes oder Backup von Volumes im Objekt-Storage wieder her.
- 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.
- Durchführung einer *schnellen Wiederherstellung* eines Volumes aus dem Cloud Storage auf ein Cloud Volumes ONTAP-System oder auf ein On-Premises-System; perfekt für Disaster-Recovery-Situationen, in denen möglichst bald Zugriff auf ein Volume ermöglicht werden muss.
- Stellen Sie Daten auf Blockebene wieder her, indem Sie die Daten direkt an dem von Ihnen angegebenen Speicherort platzieren, wobei die ursprünglichen ACLs erhalten bleiben.
- Durchsuchen und Suchen von Dateikatalogen zur einfachen Auswahl einzelner Ordner und Dateien für die Wiederherstellung einzelner Dateien.

Unterstützte Arbeitsumgebungen für Backup- und Wiederherstellungsvorgänge

BlueXP Backup und Recovery unterstützt ONTAP Arbeitsumgebungen sowie Public- und Private-Cloud-Provider.

Unterstützte Regionen

BlueXP Backup und Recovery wird von Cloud Volumes ONTAP in vielen Regionen von Amazon Web Services, Microsoft Azure und Google Cloud unterstützt.

"Weitere Informationen finden Sie in der Karte der globalen Regionen"

Unterstützte Backup-Ziele

Mit BlueXP Backup und Recovery können Sie ONTAP Volumes von den folgenden Quell-Arbeitsumgebungen in den folgenden sekundären Arbeitsumgebungen und Objekt-Storage bei Public- und Private-Cloud-Providern sichern. Snapshot-Kopien befinden sich in der Quell-Arbeitsumgebung.

Quelle Arbeitsumgebung	Sekundäre Arbeitsumgebung (Replikation)	Zielobjektspeicher (Backup) Ifdef::aws[]
Cloud Volumes ONTAP in AWS	Cloud Volumes ONTAP in AWS Lokales ONTAP System	Amazon S3 endif::aws[] ifdef::Azure[]
Cloud Volumes ONTAP in Azure	Cloud Volumes ONTAP in Azure Lokales ONTAP System	Azure Blob endif::Azure[] ifdef::gcp[]
Cloud Volumes ONTAP in Google	Cloud Volumes ONTAP in Google Lokales ONTAP System	Google Cloud Storage endif::gcp[]

Lokales ONTAP System	Cloud Volumes ONTAP Lokales ONTAP System	Ifdef::aws[] Amazon S3 Endif::aws[] Ifdef::azurblau[] Azure Blob Endif::azurblau[] Ifdef::gcp[] Google Cloud Storage Endif::gcp[] NetApp StorageGRID ONTAP S3

Unterstützte Wiederherstellungsziele

Sie können ONTAP-Daten aus einer Backup-Datei in einer sekundären Arbeitsumgebung (einem replizierten Volume) oder im Objektspeicher (einer Backup-Datei) in den folgenden Arbeitsumgebungen wiederherstellen. Snapshot Kopien befinden sich in der Quell-Arbeitsumgebung, sie können nur auf demselben System wiederhergestellt werden.

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

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

Unterstützte Volumes

BlueXP Backup und Recovery unterstützt folgende Volume-Typen:

- FlexVol Volumes für Lese- und Schreibvorgänge
- FlexGroup Volumes (erfordert ONTAP 9.12.1 oder höher)
- SnapLock Enterprise Volumes (erfordert ONTAP 9.11.1 oder höher)
- SnapLock Compliance für On-Premises Volumes (ONTAP 9 14 oder höher erforderlich)
- SnapMirror Data Protection (DP) Ziel-Volumes

BlueXP Backup und Recovery unterstützt keine Backups von FlexCache Volumes.

Siehe die Abschnitte unter "Einschränkungen bei Backup und Restore" Für zusätzliche Anforderungen und Einschränkungen.

Kosten

Für die Nutzung von BlueXP Backup und Recovery für ONTAP Systeme gibt es zwei Arten von Kosten: Ressourcengebühren und Servicegebühren. Beide Gebühren gelten für den Backup-to-Object-Teil des Service.

Es ist kostenfrei, Snapshot Kopien oder replizierte Volumes zu erstellen. Dabei fällt außer dem für die Speicherung der Snapshot Kopien und replizierten Volumes erforderlichen Festplattenspeicher an.

Ressourcengebühren

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

- Für Backups in Objekt-Storage bezahlen Sie bei Ihrem Cloud-Provider die Kosten für Objekt-Storage.

  Da BlueXP Backup und Recovery die Storage-Effizienz des Quell-Volumes erhalten behält, zahlen Sie für die Daten die Objekt-Storage-Kosten des Cloud-Providers – d. h. Effizienz nach_ ONTAP (für die kleineren Datenmengen nach Deduplizierung und Komprimierung).

- 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.
  - In Azure, an "Azure Synapse Workspace" Und "Azure Data Lake Storage" Werden in Ihrem Storage-Konto bereitgestellt, um Ihre Daten zu speichern und zu analysieren.
- In Google wird ein neuer Bucket implementiert, und der "Google Cloud BigQuery Services" Werden auf Konto-/Projektebene bereitgestellt.
- Wenn Sie Volume-Daten von einer Backup-Datei wiederherstellen möchten, die in einen Archiv-Objektspeicher verschoben wurde, fällt eine zusätzliche Abrufgebühr pro gib und eine Gebühr auf Anfrage des Cloud-Providers an.
- Wenn Sie während der Wiederherstellung von Volume-Daten eine Backup-Datei auf Ransomware überprüfen möchten (wenn Sie DataLock und Ransomware-Schutz für Ihre Cloud-Backups aktiviert haben), fallen zusätzliche Kosten für den ausgehenden Datenverkehr von Ihrem Cloud-Provider an.

Servicegebühren

Servicegebühren werden an NetApp gezahlt und decken sowohl die Kosten für die Erstellung von Backups im Objekt-Storage als auch für die Wiederherstellung von Volumes oder Dateien aus diesen Backups ab. Sie bezahlen nur für die geschützten Daten im Objekt-Storage. Berechnet wird aus der verwendeten logischen Quellkapazität (*vor* ONTAP-Effizienzen) von 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

BlueXP Backup und Recovery ist in den folgenden Nutzungsmodellen verfügbar:

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

Eine Backup-Lizenz ist nur für Backup und Restore aus dem Objektspeicher erforderlich. Die Erstellung von Snapshot Kopien und replizierten Volumes erfordert keine Lizenz.

Mit Ihrer eigenen Lizenz

Byol ist längerfristig (1, 2 oder 3 Jahre) und kapazitätsbasiert in 1-tib-Schritten. 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 BlueXP Digital Wallet-Seite eingeben, um den Service zu aktivieren. Wenn eine der beiden Limits erreicht ist, müssen Sie die Lizenz erneuern. Die BYOL-Lizenz für Backup gilt für alle Quellsysteme, die mit Ihrer-Organisation oder Ihrem BlueXP -Konto verbunden sind.

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

Pay-as-you-go-Abonnement

BlueXP Backup und Recovery bietet eine nutzungsbasierte Lizenzierung in einem Pay-as-you-go-Modell. Wenn Sie den Markt Ihres Cloud-Providers abonniert haben, bezahlen Sie pro gib für Daten, die gesichert werden. Es erfolgt 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 sind zwei Jahresverträge mit Laufzeiten von 1, 2 oder 3 Jahren erhältlich:

- 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 Backup und Recovery von Cloud Volumes ONTAP und BlueXP 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).

Bei Nutzung von Azure stehen zwei Jahresverträge mit Laufzeiten von 1, 2 oder 3 Jahren 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 Backup und Recovery von Cloud Volumes ONTAP und BlueXP 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).

Wenn Sie GCP nutzen, können Sie ein privates Angebot von NetApp anfordern und anschließend den Plan auswählen, wenn Sie während der Aktivierung von BlueXP für Backup und Recovery im Google Cloud Marketplace abonnieren.

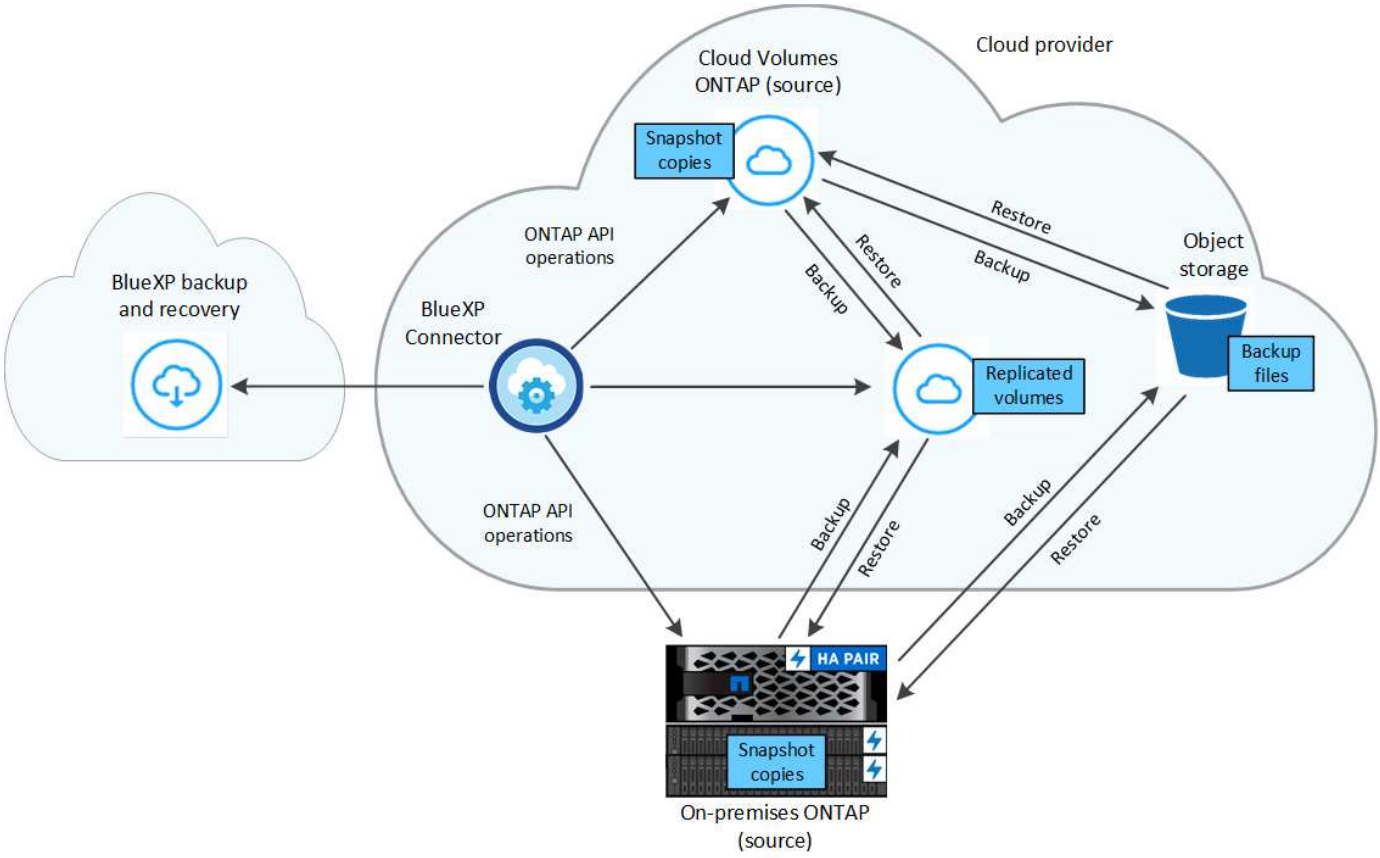
"Hier erfahren Sie, wie Sie Jahresverträge einrichten können".

Funktionsweise von BlueXP Backup und Recovery

Wenn Sie das Backup und Recovery von BlueXP auf einem Cloud Volumes ONTAP oder einem lokalen ONTAP System aktivieren, führt der Service ein vollständiges Backup Ihrer Daten durch. 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. Backup-to-Objekt-Storage basiert auf dem "NetApp SnapMirror Cloud Technologie".

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

Die folgende Abbildung zeigt die Beziehung zwischen den einzelnen Komponenten:



In diesem Diagramm werden Volumes angezeigt, die auf ein Cloud Volumes ONTAP System repliziert werden. Allerdings können auch Volumes auf ein lokales ONTAP System repliziert werden.

Speicherort von Backups

Backups befinden sich je nach Backup-Typ an verschiedenen Orten:

- *Snapshot Copies* befinden sich auf dem Quell-Volume in der Quell-Arbeitsumgebung.
- *Replizierte Volumes* befinden sich auf dem sekundären Storage-System – einem Cloud Volumes ONTAP- oder On-Premises-ONTAP-System.
- *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 Azure verwendet BlueXP eine neue oder vorhandene Ressourcengruppe mit einem Storage-Konto für den Blob-Container. BlueXP "Blockiert den öffentlichen Zugriff auf Ihre BLOB-Daten" Standardmäßig.
  - In GCP verwendet BlueXP ein neues oder bestehendes Projekt mit einem Storage-Konto für den Google Cloud Storage Bucket.
  - In StorageGRID verwendet BlueXP ein vorhandenes Mandantenkonto für den S3-Bucket.
  - In ONTAP S3 verwendet BlueXP ein vorhandenes Benutzerkonto für den S3-Bucket.

Wenn Sie künftig den Zielobjektspeicher für ein Cluster ändern möchten, müssen Sie unbedingt fortfahren "Heben Sie die Registrierung von BlueXP Backup und Recovery für die Arbeitsumgebung auf"Außerdem können Sie BlueXP Backup und Recovery mithilfe der Informationen eines neuen Cloud-Providers aktivieren.

Anpassbare Backup-Planungs- und Aufbewahrungseinstellungen

Wenn Sie BlueXP Backup und Recovery für eine funktionierende Umgebung aktivieren, werden alle Volumes, die Sie ursprünglich ausgewählt haben, über die von Ihnen ausgewählten Richtlinien gesichert. Sie können separate Richtlinien für Snapshot-Kopien, replizierte Volumes und Backup-Dateien auswählen. Wenn Sie verschiedenen Backup-Richtlinien bestimmten Volumes mit unterschiedlichen Recovery-Zeitpunkten (Recovery Point Objectives, RPO) zuweisen möchten, können Sie zusätzliche Richtlinien für diesen Cluster erstellen und diese Richtlinien nach der Aktivierung von BlueXP Backup und Recovery anderen Volumes zuweisen.

Es steht eine Kombination aus stündlichen, täglichen, wöchentlichen, monatlichen und jährlichen Backups aller Volumes zur Verfügung. Für Backups auf Objektspeicher können Sie auch eine der systemdefinierten Richtlinien auswählen, die Backup und Aufbewahrung für 3 Monate, 1 Jahr und 7 Jahre vorsehen. 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.

> Die auf das Volume angewendete Snapshot-Richtlinie muss über eine der Etiketten verfügen, die Sie in Ihrer Replizierungsrichtlinie und für das Backup in der Objektrichtlinie verwenden. Wenn keine übereinstimmenden Etiketten gefunden werden, werden keine Sicherungsdateien erstellt. Wenn Sie beispielsweise „wöchentliche“ replizierte Volumes und Backup-Dateien erstellen möchten, müssen Sie eine Snapshot-Richtlinie verwenden, die „wöchentliche“ Snapshot-Kopien erstellt.

Sobald Sie die maximale Anzahl von Backups für eine Kategorie oder ein Intervall erreicht haben, werden ältere Backups entfernt, sodass Sie immer die aktuellsten Backups haben (und so nehmen veraltete Backups nicht mehr Speicherplatz in Anspruch).

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 in Objekt-Storage vor 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.

Geplante Scans zum Schutz vor Ransomware sind standardmäßig aktiviert. Die Standardeinstellung für die Scanfrequenz beträgt 7 Tage. Der Scan wird nur auf der letzten Snapshot Kopie durchgeführt. Die geplanten Scans können deaktiviert werden, um Ihre Kosten zu senken. Sie können geplante Ransomware-Scans für die

neueste Snapshot Kopie über die Option auf der Seite „Erweiterte Einstellungen“ aktivieren oder deaktivieren. Wenn Sie diese Option aktivieren, werden standardmäßig wöchentliche Scans durchgeführt. Sie können diesen Zeitplan auf Tage oder Wochen ändern oder deaktivieren, um Kosten zu sparen.

Die Backup-Aufbewahrungsfrist entspricht dem Aufbewahrungszeitraum des Backup-Plans plus einem Puffer von maximal 31 Tagen. 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.

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

Weitere Informationen finden Sie unter:

- "Funktionsweise von DataLock und Ransomware-Schutz".
- "So aktualisieren Sie Ransomware-Schutzoptionen auf der Seite Erweiterte Einstellungen".

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. Sie haben auch die Möglichkeit, die Backup-Dateien sofort in den Archiv-Storage zu senden, ohne dafür in standardmäßigen Cloud-Storage geschrieben zu werden. 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 für weitere Kostenoptimierung entweder in *S3 Glacier* oder *S3 Glacier Deep Archive* Storage in der BlueXP Backup- und Recovery-UI verschieben. "Weitere Informationen zu AWS Archiv-Storage".

- In Azure werden Backups im Zusammenhang mit der *Cool* Zugriffsebene durchgeführt.

  Wenn Ihr Cluster ONTAP 9.10.1 oder höher verwendet, haben Sie nach einer bestimmten Anzahl von Tagen die Möglichkeit, ältere Backups in der Backup- und Recovery-UI von BlueXP auf den Storage *Azure Archive* zu verschieben, um weitere Kosten zu optimieren. "Erfahren Sie mehr über Azure Archiv-Storage".

- In GCP werden Backups der Klasse *Standard* Storage zugeordnet.

  Wenn Ihr Cluster ONTAP 9.12.1 oder höher verwendet, haben Sie nach einer bestimmten Anzahl von Tagen die Möglichkeit, ältere Backups in der BlueXP Backup- und Recovery-UI auf den *Archiv* Storage zu verschieben, um weitere Kosten zu optimieren. "Erfahren Sie mehr über Google Archivspeicher".

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

  Wenn Ihr On-Premises-Cluster ONTAP 9.12.1 oder höher verwendet und Ihr StorageGRID System mindestens 11.4 nutzt, können Sie ältere Backup-Dateien nach einer bestimmten Anzahl von Tagen in den Public-Cloud-Archiv-Storage archivieren. Aktuell werden weitere Support für AWS S3 Glacier/S3 Glacier Deep Archive oder Azure Archive Storage Tiers unterstützt. "Weitere Informationen zur Archivierung von Backup-Dateien aus StorageGRID".

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 Volumen, das Sie sichern, auf einem FabricPool-Aggregat liegt und es eine andere Tiering-Richtlinie als zugewiesen hat `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 verschoben werden, liest BlueXP Backup und Recovery Daten aus der Cloud-Tier und nicht aus der lokalen Tier ein. 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.

Planen Sie Ihren Schutz mit BlueXP Backup und Recovery

Der BlueXP Backup- und Recovery-Service ermöglicht das Erstellen von bis zu drei Kopien Ihrer Quell-Volumes zum Schutz Ihrer Daten. Es gibt viele Optionen, die Sie auswählen können, wenn Sie diesen Service auf Ihren Volumes aktivieren. Daher sollten Sie Ihre Auswahl überprüfen, um vorbereitet zu sein.

Wir gehen auf die folgenden Optionen ein:

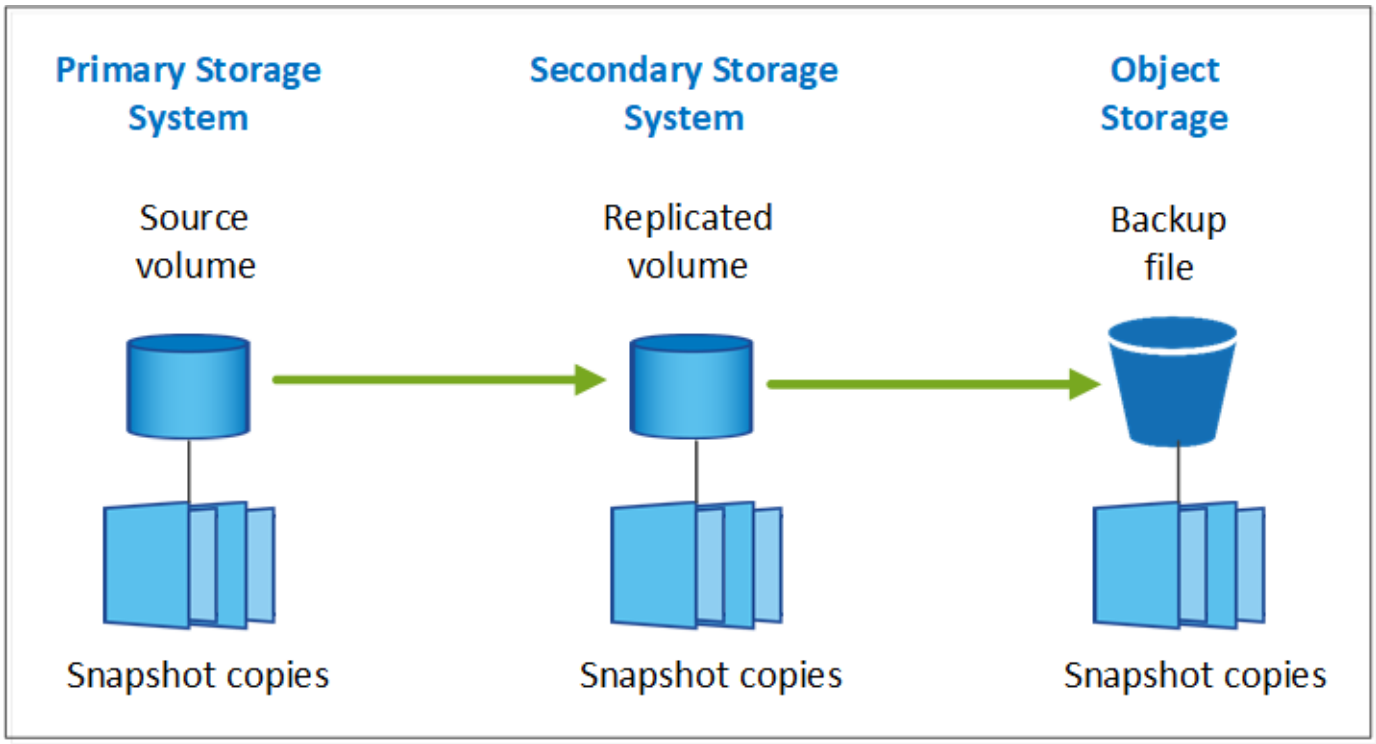
- Welche Sicherungsfunktionen kommen für Sie zum Einsatz: snapshot Kopien, replizierte Volumes und/oder Backup in der Cloud
- Welche Backup-Architektur verwenden Sie? Ein Kaskadierungs- oder Fan-out-Backup Ihrer Volumes
- Werden die standardmäßigen Backup-Richtlinien verwendet oder müssen Sie benutzerdefinierte Richtlinien erstellen
- Soll der Service die Cloud-Buckets für Sie erstellen oder sollen Sie vor dem Start eine Objekt-Storage-Container erstellen
- Welchen BlueXP Connector-Implementierungsmodus verwenden Sie (Standard, eingeschränkter oder privater Modus)?

Welche Schutzfunktionen werden Sie verwenden

Bevor Sie die Funktionen auswählen, die Sie verwenden werden, finden Sie hier eine kurze Erklärung, was die einzelnen Funktionen tun und welche Art von Schutz es bietet.

Backup-Typ	Beschreibung
Snapshot	Erstellt ein schreibgeschütztes, zeitpunktgenaues Image eines Volumes innerhalb des Quell-Volumes als Snapshot-Kopie. Sie können die Snapshot-Kopie verwenden, um einzelne Dateien wiederherzustellen oder den gesamten Inhalt eines Volumes wiederherzustellen.
Replizierung	Erstellt eine sekundäre Kopie der Daten auf einem anderen ONTAP Storage-System und aktualisiert die sekundären Daten kontinuierlich. Ihre Daten bleiben aktuell und verfügbar.
Cloud-Backup	Erstellt Backups Ihrer Daten in der Cloud für den Schutz und für die langfristige Archivierung. Bei Bedarf können Sie ein Volume, einen Ordner oder einzelne Dateien aus dem Backup in derselben oder einer anderen Arbeitsumgebung wiederherstellen.

Snapshots bilden die Grundlage aller Backup-Methoden. Sie müssen den Backup- und Recovery-Service verwenden. Eine Snapshot-Kopie ist ein schreibgeschütztes, zeitpunktgenaues Image eines Volumes. Das Image verbraucht nur minimalen Speicherplatz und verursacht keinen nennenswerten Performance-Overhead, da es seit der letzten Snapshot-Kopie nur Änderungen an Dateien aufzeichnet. Die auf Ihrem Volume erstellte Snapshot Kopie wird verwendet, um das replizierte Volume und die Backup-Datei mit den Änderungen am Quell-Volume synchronisiert zu halten, wie in der Abbildung gezeigt.



Sie können sowohl replizierte Volumes auf einem anderen ONTAP Storage-System als auch Backup-Dateien in der Cloud erstellen. Oder Sie haben die Wahl, ob Sie nur replizierte Volumes oder Backup-Dateien erstellen möchten.

Zusammengefasst sind dies die gültigen Sicherheitsflüsse, die Sie für Volumes in Ihrer ONTAP Arbeitsumgebung erstellen können:

- Quellvolume → Snapshot copy → repliziertes Volume → Sicherungsdatei
- Quellvolume → Snapshot copy → Sicherungsdatei

- Quell-Volume → Snapshot Kopie → repliziertes Volume

> Die anfängliche Erstellung eines replizierten Volumes oder einer Backup-Datei beinhaltet eine vollständige Kopie der Quelldaten – dies wird als *Baseline Transfer* bezeichnet. Nachfolgende Transfers enthalten nur differenzielle Kopien der Quelldaten (der Snapshot).

Vergleich der verschiedenen Backup-Methoden

Die folgende Tabelle zeigt einen generalisierten Vergleich der drei Backup-Methoden. Obwohl Objektspeicher in der Regel kostengünstiger ist als Ihr lokaler Festplatten-Storage, wenn Sie denken, dass Sie Daten häufig aus der Cloud wiederherstellen könnten, können die Kosten für ausgehenden Datenverkehr von Cloud-Providern einige Einsparungen reduzieren. Sie müssen ermitteln, wie oft Sie Daten aus den Backup-Dateien in der Cloud wiederherstellen müssen.

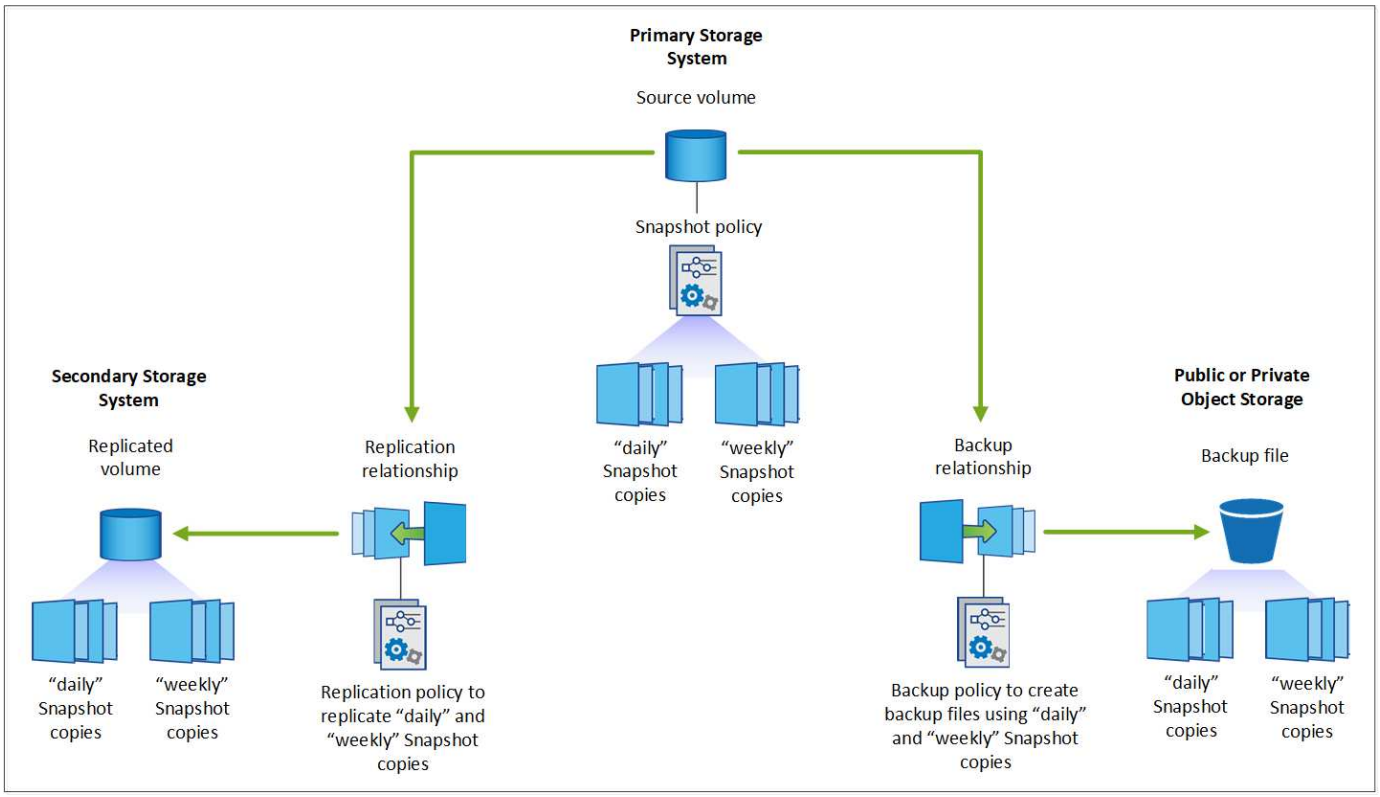
Zusätzlich zu diesem Kriterium bietet Cloud Storage zusätzliche Sicherheitsoptionen, wenn Sie die DataLock- und Ransomware-Schutzfunktion verwenden. Außerdem werden durch Auswahl von Archiv-Storage-Klassen für ältere Backup-Dateien zusätzliche Kosteneinsparungen erzielt. "Erfahren Sie mehr über DataLock und Ransomware-Schutz" Und "Einstellungen für Archiv-Storage".

Backup-Typ	Backup-Geschwindigkeit	Backup-Kosten	Restore-Geschwindigkeit	Wiederherstellungskosten
Snapshot	Hoch	Niedrig (Festplattenspeicher)	Hoch	Niedrig
Replikation	Mittel	Mittel (Festplattenspeicherplatz)	Mittel	Mittel (Netzwerk)
Cloud-Backup	Niedrig	Niedrig (Objektraum)	Niedrig	Hoch (Provider-Gebühren)

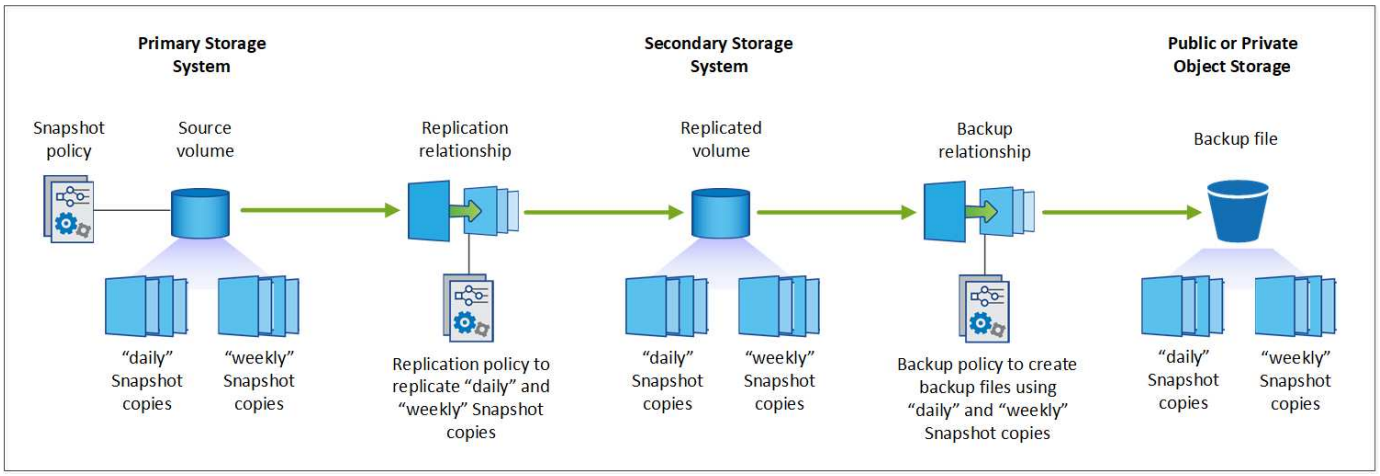
Welche Backup-Architektur werden Sie verwenden

Wenn Sie sowohl replizierte Volumes als auch Backup-Dateien erstellen, können Sie eine Fan-out- oder Kaskadenarchitektur wählen, um Backups Ihrer Volumes zu erstellen.

Eine **Fan-out**-Architektur überträgt die Snapshot-Kopie unabhängig sowohl auf das Ziel-Storage-System als auch auf das Backup-Objekt in der Cloud.



Eine **Kaskadenarchitektur** überträgt die Snapshot-Kopie zuerst an das Ziel-Storage-System. Anschließend überträgt dieses System die Kopie an das Backup-Objekt in der Cloud.



Vergleich der verschiedenen Architekturwahlen

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

Fan-out	Kaskadierung
Geringe Auswirkungen auf die Performance des Quellsystems, da Snapshot Kopien an 2 unterschiedliche Systeme gesendet werden	Geringere Auswirkungen auf die Performance des Quell-Storage-Systems, da die Snapshot Kopie nur einmal gesendet wird
Einfachere Einrichtung, da alle Richtlinien, Netzwerk- und ONTAP-Konfigurationen auf dem Quellsystem ausgeführt werden	Erfordert, dass auch vom sekundären System aus eine gewisse Netzwerk- und ONTAP-Konfiguration durchgeführt werden muss.

Werden die Standardrichtlinien für Snapshots, Replikationen und Backups verwendet

Sie können Ihre Backups entweder über die von NetApp bereitgestellten Standardrichtlinien oder über benutzerdefinierte Richtlinien erstellen. Wenn Sie den Backup- und Recovery-Service für Ihre Volumes mit dem Aktivierungsassistenten aktivieren, können Sie aus den Standardrichtlinien und anderen Richtlinien auswählen, die bereits in der Arbeitsumgebung (Cloud Volumes ONTAP oder On-Premises ONTAP System) vorhanden sind. Wenn Sie eine andere Richtlinie als die vorhandenen Richtlinien verwenden möchten, können Sie die Richtlinie vor dem Starten oder während der Verwendung des Aktivierungsassistenten erstellen.

- Die Standard-Snapshot-Richtlinie erstellt stündliche, tägliche und wöchentliche Snapshot-Kopien und behält 6 stündliche, 2 tägliche und 2 wöchentliche Snapshot-Kopien bei.
- Die Standardreplizierungsrichtlinie repliziert tägliche und wöchentliche Snapshot-Kopien und behält 7 tägliche und 52 wöchentliche Snapshot-Kopien bei.
- Die Standard-Backup-Richtlinie repliziert tägliche und wöchentliche Snapshot-Kopien und behält 7 tägliche und 52 wöchentliche Snapshot-Kopien bei.

Wenn Sie benutzerdefinierte Richtlinien für Replizierung oder Backup erstellen, müssen die Richtlinienbeschriftungen (z. B. „täglich“ oder „wöchentlich“) mit den Bezeichnungen übereinstimmen, die in Ihren Snapshot-Richtlinien oder replizierten Volumes vorhanden sind, und Backup-Dateien werden nicht erstellt.

Sie können in der BlueXP Backup- und Recovery-UI Snapshot-, Replizierungs- und Backup-to-Objekt-Storage-Richtlinien erstellen. Weitere Informationen finden Sie im Abschnitt"Hinzufügen einer neuen Backup-Richtlinie".

Zusätzlich zum Erstellen benutzerdefinierter Richtlinien mithilfe von BlueXP Backup und Recovery können Sie System Manager oder die ONTAP Befehlszeilenschnittstelle (CLI) verwenden:

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

Hinweis: Wenn Sie System Manager verwenden, wählen Sie **Asynchronous** als Richtlinientyp für Replikationsrichtlinien aus, und wählen Sie **Asynchronous** und **Backup in der Cloud** für Backup in Objektrichtlinien aus.

Hier sind einige Beispiele für ONTAP CLI-Befehle, die hilfreich sein könnten, wenn Sie benutzerdefinierte Richtlinien erstellen. Beachten Sie, dass Sie in diesen Befehlen den Befehl „*admin* vServer“ (Storage VM) verwenden müssen `<vserver_name>`.

Richtlinienbeschreibung	Befehl
Einfache Snapshot-Richtlinie	`snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly`
Einfaches Backup in die Cloud	`snapmirror policy create -policy <policy_name> -transfer -priority normal -vserver <vserver_name> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

Richtlinienbeschreibung	Befehl
Backup in der Cloud mit DataLock und Ransomware-Schutz	`snapmirror policy create -policy CloudBackupService-Enterprise -snapshot-lock-mode enterprise -vserver <vserver_name>` `snapmirror policy add-rule -policy CloudBackupService-Enterprise -retention-period 30days`
Backup in die Cloud mit Archiv-Storage-Klasse	`snapmirror policy create -vserver <vserver_name> -policy <policy_name> -archive-after-days <days> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`
Einfache Replizierung auf ein anderes Storage-System	`snapmirror policy create -policy <policy_name> -type async-mirror -vserver <vserver_name>` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

Für Backups in der Cloud können nur Vault-Richtlinien verwendet werden.

Wo befinden sich meine Richtlinien?

Backup-Richtlinien befinden sich an verschiedenen Standorten, je nachdem, welche Backup-Architektur Sie verwenden möchten: Fan-out oder Kaskadierung. Replikationsrichtlinien und Backup-Richtlinien sind nicht auf dieselbe Weise ausgelegt, da Replikationen zwei ONTAP-Speichersysteme verbinden und Backup to Object einen Speicheranbieter als Ziel verwendet.

- Snapshot-Richtlinien befinden sich immer auf dem primären Storage-System.
- Replizierungsrichtlinien befinden sich immer auf dem sekundären Storage-System.
- Richtlinien für Backups auf Objekten werden auf dem System erstellt, auf dem sich das Quell-Volume befindet. Dies ist der primäre Cluster für Fan-out-Konfigurationen und der sekundäre Cluster für Kaskadenkonfigurationen.

Diese Unterschiede sind in der Tabelle aufgeführt.

Der Netapp Architektur Sind	Snapshot-Richtlinie	Replizierungsrichtlinie	Backup-Richtlinie
Fan-out	Primär	Sekundär	Primär
Kaskade	Primär	Sekundär	Sekundär

Wenn Sie also planen, bei der Nutzung der Kaskadenarchitektur benutzerdefinierte Richtlinien zu erstellen, müssen Sie auf dem sekundären System, auf dem die replizierten Volumes erstellt werden, Replizierungs- und Backup-to-Object-Richtlinien erstellen. Wenn Sie planen, bei der Nutzung der Fan-out-Architektur benutzerdefinierte Richtlinien zu erstellen, müssen Sie auf dem sekundären System, auf dem die replizierten Volumes erstellt werden, die Replizierungsrichtlinien für Backups in Objekten auf dem primären System erstellen.

Wenn Sie die Standardrichtlinien verwenden, die auf allen ONTAP Systemen vorhanden sind, sind alle fertig.

Möchten Sie Ihren eigenen Objekt-Storage-Container erstellen

Wenn Sie Backup-Dateien im Objektspeicher für eine Arbeitsumgebung erstellen, erstellt der Backup- und Recovery-Service standardmäßig den Container (Bucket oder Storage-Konto) für die Backup-Dateien im von Ihnen konfigurierten Objekt-Storage-Konto. Der AWS- oder GCP-Bucket hat standardmäßig den Namen „netapp-Backup-<uuid>“. Das Azure Blob Storage-Konto trägt die Bezeichnung „netappsausw <uuid>“.

Sie können den Container selbst im Objekt-Provider-Konto erstellen, wenn Sie ein bestimmtes Präfix verwenden oder besondere Eigenschaften zuweisen möchten. Wenn Sie einen eigenen Container erstellen möchten, müssen Sie ihn erstellen, bevor Sie den Aktivierungsassistenten starten. Für BlueXP Backup und Recovery können beliebige Buckets und Share Buckets verwendet werden. Der Assistent für die Backup-Aktivierung erkennt automatisch die bereitgestellten Container für das ausgewählte Konto und die Anmeldeinformationen, sodass Sie das gewünschte Konto auswählen können.

Sie können den Bucket von BlueXP oder von Ihrem Cloud-Provider erstellen.

- "Amazon S3 Buckets aus BlueXP erstellen"
- "Azure Blob-Storage-Konten aus BlueXP erstellen"
- "Google Cloud Storage Buckets aus BlueXP erstellen"

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

Erweiterte Bucket-Einstellungen

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

- Archiv-Storage auf Ihren eigenen Buckets wird derzeit im AWS S3 Storage unterstützt, wenn die Software ONTAP 9.10.1 oder höher auf Ihren Clustern verwendet wird. Standardmäßig werden Backups in der Speicherklasse S3 *Standard* gestartet. Stellen Sie sicher, dass Sie den Bucket mit den entsprechenden Lebenszyklusregeln erstellen:
  - Verschieben Sie die Objekte im gesamten Bucket nach 30 Tagen nach S3 *Standard-IA*.
  - Verschieben Sie die Objekte mit dem Tag "smc_Push_to_Archive: True" nach *Glacier Flexible Retrieval* (ehemals S3 Glacier)
- DataLock- und Ransomware-Schutz werden im AWS-Speicher unterstützt, wenn Sie auf Ihren Clustern die Software ONTAP 9.11.1 oder höher verwenden, und im Azure-Speicher, wenn Sie die Software ONTAP 9.12.1 oder höher verwenden.
  - Bei AWS müssen Sie die Objektsperrung auf dem Bucket aktivieren, indem Sie eine 30-Tage-Aufbewahrungsfrist verwenden.
  - Bei Azure müssen Sie die Storage-Klasse mit der Unveränderlichkeit von Versionslevel errichten.

Welchen BlueXP Connector-Implementierungsmodus verwenden Sie

Wenn Sie Ihren Storage bereits mit BlueXP managen, wurde bereits ein BlueXP Connector installiert. Wenn Sie denselben Connector mit BlueXP Backup und Recovery nutzen möchten, steht Ihnen alles bereit. Wenn Sie einen anderen Connector verwenden müssen, müssen Sie ihn installieren, bevor Sie mit der Backup- und Recovery-Implementierung beginnen.

BlueXP bietet mehrere Implementierungsmodi, die es Ihnen ermöglichen, BlueXP entsprechend Ihren Geschäfts- und Sicherheitsanforderungen zu nutzen. *Standard Mode* nutzt die BlueXP SaaS-Ebene für die

volle Funktionalität. *Restricted Mode* und *Private Mode* stehen Unternehmen mit Konnektivitätsbeschränkungen zur Verfügung.

"Weitere Informationen zu den BlueXP Implementierungsmodi".

Unterstützung für Websites mit voller Internetverbindung

Wenn BlueXP Backup und Recovery an einem Standort mit vollständiger Internetverbindung verwendet wird (auch als *Standard-Modus* oder *SaaS-Modus* bekannt), können Sie replizierte Volumes auf jedem beliebigen lokalen ONTAP oder Cloud Volumes ONTAP System erstellen, das von BlueXP gemanagt wird. Sie können darüber hinaus Backup-Dateien auf Objekt-Storage von einem der unterstützten Cloud-Provider erstellen. "Sehen Sie sich die vollständige Liste der unterstützten Backup-Ziele an".

Eine Liste der gültigen Connector-Standorte finden Sie in einem der folgenden Backup-Verfahren für den Cloud-Provider, bei dem Sie Sicherungsdateien erstellen möchten. Es gibt einige Einschränkungen, wenn der Connector manuell auf einem Linux-Rechner installiert oder bei einem bestimmten Cloud-Anbieter bereitgestellt werden muss.

- "Backup von Cloud Volumes ONTAP Daten in Amazon S3"
- "Sichern Sie On-Premises-ONTAP-Daten in Amazon S3"
- "Backup von Cloud Volumes ONTAP Daten in Azure Blob"
- "Sichern Sie On-Premises-ONTAP-Daten in Azure Blob"
- "Backup von Cloud Volumes ONTAP Daten in Google Cloud"
- "Backup von On-Premises-ONTAP-Daten in Google Cloud"
- "Sichern Sie On-Premises-ONTAP-Daten in StorageGRID"
- "Sichern Sie On-Premises-ONTAP auf ONTAP S3"

Unterstützung für Websites mit begrenzter Internetverbindung

BlueXP Backup und Recovery können an einem Standort mit eingeschränkter Internet-Konnektivität (auch als *eingeschränkter Modus* bezeichnet) verwendet werden, um Volume-Daten zu sichern. In diesem Fall müssen Sie den BlueXP Connector in der Ziel-Cloud-Region implementieren.

- Sie können Daten von lokalen ONTAP Systemen oder Cloud Volumes ONTAP Systemen in AWS Geschäftsregionen in Amazon S3 sichern. "Backup von Cloud Volumes ONTAP Daten in Amazon S3".
- Sie können Daten aus lokalen ONTAP Systemen oder Cloud Volumes ONTAP Systemen in Azure kommerzielle Regionen in Azure Blob sichern. "Backup von Cloud Volumes ONTAP Daten in Azure Blob".

Unterstützung für Websites ohne Internetverbindung

BlueXP Backup und Recovery kann an einem Standort ohne Internetverbindung (auch als *Private-Modus* oder *Dark* Sites bezeichnet) verwendet werden, um Volume-Daten zu sichern. In diesem Fall müssen Sie den BlueXP Connector auf einem Linux-Host am selben Standort implementieren.

- Sie können Daten von lokalen ONTAP Systemen auf lokalen NetApp StorageGRID Systemen sichern. "Sichern Sie On-Premises-ONTAP-Daten in StorageGRID".
- Daten können von lokalen ONTAP Systemen auf lokalen ONTAP Systemen oder auf Cloud Volumes ONTAP Systemen gesichert werden, die für S3 Objekt-Storage konfiguriert sind. "Sichern Sie On-Premises-ONTAP-Daten in ONTAP S3".
  Ifdef::aws[]

Verwalten Sie Sicherungsrichtlinien für ONTAP-Volumes mit BlueXP Backup und Recovery

Verwenden Sie mit BlueXP Backup und Recovery die von NetApp bereitgestellten Standard-Backup-Richtlinien zum Erstellen Ihrer Backups oder erstellen Sie benutzerdefinierte Richtlinien. Richtlinien regeln die Sicherungshäufigkeit, die Dauer der Sicherung und die Anzahl der Sicherungsdateien, die aufbewahrt werden.

Wenn Sie den Backup- und Recovery-Service für Ihre Volumes mit dem Aktivierungsassistenten aktivieren, können Sie aus den Standardrichtlinien und anderen Richtlinien auswählen, die bereits in der Arbeitsumgebung (Cloud Volumes ONTAP oder On-Premises ONTAP System) vorhanden sind. Wenn Sie eine andere Richtlinie als die vorhandenen Richtlinien verwenden möchten, können Sie die Richtlinie vor oder während der Verwendung des Aktivierungsassistenten erstellen.

Weitere Informationen zu den standardmäßigen Backup-Richtlinien finden Sie unter "Planen Sie Ihren Weg zum Schutz".

BlueXP Backup und Recovery bietet drei Arten von Backups von ONTAP Daten: Snapshots, Replizierungen und Backups in Objekt-Storage. Ihre Richtlinien befinden sich an verschiedenen Orten, basierend auf der von Ihnen verwendeten Architektur und der Art des Backups:

Der Netapp Architektur Sind	Speicherort der Snapshot-Richtlinie	Speicherort der Replizierungsrichtlinie	Speicherort für Backup in Objektrichtlinie
Fan-out	Primär	Sekundär	Primär
Kaskade	Primär	Sekundär	Sekundär

Erstellen Sie anhand der folgenden Tools Backup-Richtlinien, je nach Ihrer Umgebung, Ihren Einstellungen und dem Schutztyp:

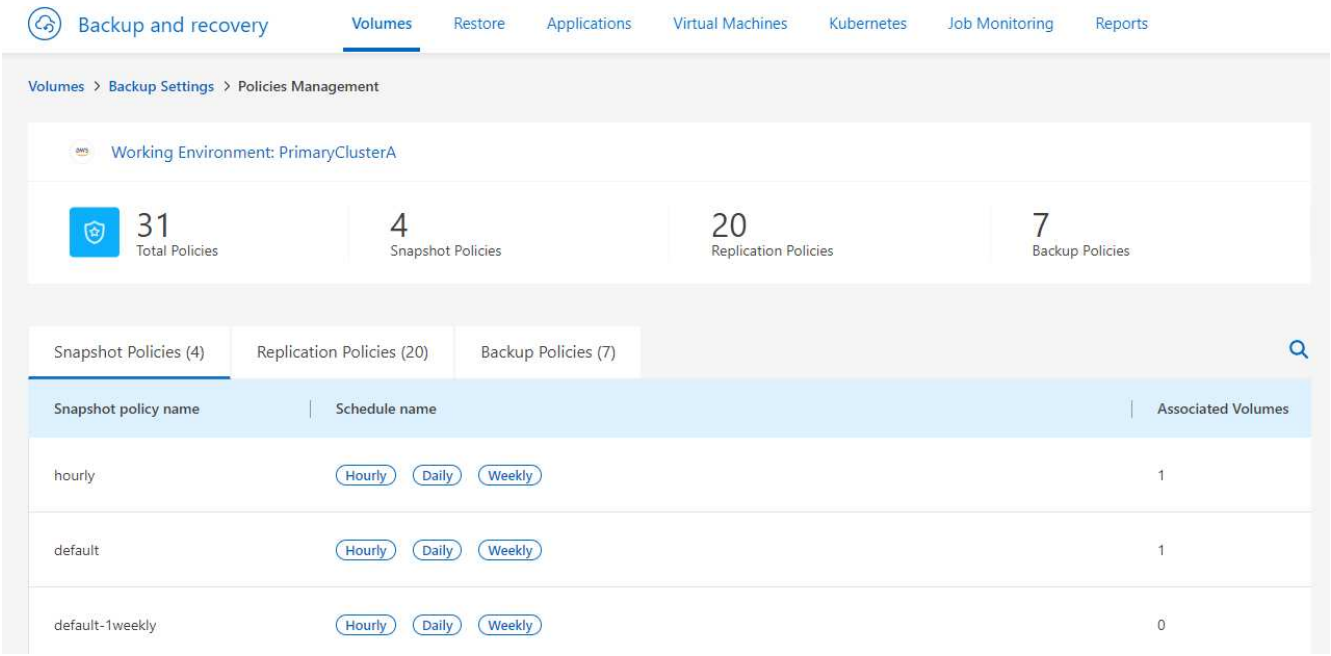
- BlueXP UI
- System Manager-UI
- CLI VON ONTAP

Wenn Sie System Manager verwenden, wählen Sie **Asynchronous** als Richtlinientyp für Replikationsrichtlinien aus, und wählen Sie **Asynchronous** und **Back up to Cloud** für Backup to object Policies aus.

Richtlinien für eine Arbeitsumgebung anzeigen

1. Wählen Sie in der BlueXP-Benutzeroberfläche **Volumes** > **Backup-Einstellungen** aus.
2. Wählen Sie auf der Seite Backup Settings die Arbeitsumgebung aus und wählen Sie die Option **actions** ••• Und wählen Sie **Richtlinienverwaltung** aus.

   Die Seite Richtlinienverwaltung wird angezeigt.



Snapshot-Richtlinien werden standardmäßig angezeigt.

3. Um andere Richtlinien anzuzeigen, die in der Arbeitsumgebung vorhanden sind, wählen Sie entweder **Replikationsrichtlinien** oder **Backup-Richtlinien** aus. Wenn die bestehenden Richtlinien für Ihre Backup-Pläne verwendet werden können, sind Sie alle bereit. Wenn Sie eine Richtlinie mit unterschiedlichen Merkmalen benötigen, können Sie auf dieser Seite neue Richtlinien erstellen.

Erstellen von Richtlinien

Sie können Richtlinien erstellen, die Ihre Snapshot Kopien, Replizierungen und Backups in Objekt-Storage regeln:

- bevor Sie den Snapshot initiieren
- bevor Sie die Replikation starten
- Erstellen Sie vor dem Initiieren des Backups eine Richtlinie für Backup-to-Object-Storage

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

Ein Teil Ihrer 3-2-1-5-Strategie umfasst die Erstellung einer Snapshot Kopie des Volumes auf dem **primären** Storage-System.

Während des Richtlinienerstellungsprozesses werden Snapshot- und SnapMirror-Labels identifiziert, die auf Zeitplan und Aufbewahrung hinweisen. Sie können vordefinierte Beschriftungen verwenden oder eigene erstellen.

Schritte

1. Wählen Sie in der BlueXP-Benutzeroberfläche **Volumes** > **Backup-Einstellungen** aus.
2. Wählen Sie auf der Seite Backup Settings die Arbeitsumgebung aus und wählen Sie die Option **actions** ••• Und wählen Sie **Richtlinienverwaltung** aus.

   Die Seite Richtlinienverwaltung wird angezeigt.

3. Wählen Sie auf der Seite Policies **Create Policy** > **Create Snapshot Policy** aus.

4. Geben Sie den Richtliniennamen an.
5. Wählen Sie den Snapshot Zeitplan oder die Zeitpläne aus. Sie können maximal 5 Etiketten haben. Oder erstellen Sie einen Zeitplan.
6. Wenn Sie einen Zeitplan erstellen möchten:
   a. Wählen Sie die Häufigkeit von stündlich, täglich, wöchentlich, monatlich oder jährlich aus.
   b. Geben Sie die Snapshot-Labels an, die den Zeitplan und die Aufbewahrung kennzeichnen.
   c. Geben Sie ein, wann und wie oft der Snapshot erstellt wird.
   d. Aufbewahrung: Geben Sie die Anzahl der zu haltenden Snapshots ein.
7. Wählen Sie **Erstellen**.

Snapshot Policy Beispiel mit Kaskadenarchitektur

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

1. Cluster 1:
   a. Wählen Sie Cluster 1 auf der Richtlinienseite aus.
   b. Ignorieren Sie die Richtlinienabschnitte „Replikation“ und „Backup to Object“.
   c. Erstellen Sie die Snapshot-Richtlinie.
2. Cluster 2:
   a. Wählen Sie Cluster 2 auf der Seite Policy aus.
   b. Ignorieren Sie den Abschnitt zu Snapshot-Richtlinien.
   c. Konfigurieren Sie die Richtlinien für Replikation und Backup auf Objekt.

Erstellen Sie eine Replikationsrichtlinie, bevor Sie die Replikation starten

Ihre Strategie für 3-2-1-1 kann auch die Replizierung eines Volumes auf einem anderen Storage-System umfassen. Die Replikationsrichtlinie befindet sich auf dem **sekundären** Speichersystem.

Schritte

1. Wählen Sie auf der Seite Policies **Create Policy** > **Create Replication Policy** aus.
2. Geben Sie im Abschnitt Richtliniendetails den Richtliniennamen an.
3. Geben Sie die SnapMirror-Labels (maximal 5) an, die die Aufbewahrung für jedes Label kennzeichnen.
4. Geben Sie den Übertragungszeitplan an.
5. Wählen Sie **Erstellen**.

Erstellen Sie vor dem Initiieren des Backups eine Richtlinie für Backup-to-Object-Storage

Ihre 3-2-1-1-Strategie umfasst unter Umständen auch Backups von Volumes auf Objekt-Storage.

Diese Storage-Richtlinie befindet sich abhängig von der Backup-Architektur an verschiedenen Speicherorten des Storage-Systems:

- Fan-out: Primäres Storage-System
- Kaskadierung: Sekundäres Storage-System

Schritte

1. Wählen Sie auf der Seite Policy Management **Create Policy** > **Create Backup Policy** aus.
2. Geben Sie im Abschnitt Richtliniendetails den Richtliniennamen an.
3. Geben Sie die SnapMirror-Labels (maximal 5) an, die die Aufbewahrung für jedes Label kennzeichnen.
4. Geben Sie die Einstellungen an, einschließlich des Übertragungszeitplans und des Zeitplans für die Archivierung von Backups.
5. (Optional) um ältere Sicherungsdateien nach einer bestimmten Anzahl von Tagen in eine kostengünstigere Speicherklasse oder Zugriffsebene zu verschieben, wählen Sie die Option **Archiv** aus und geben die Anzahl der Tage an, die vergehen sollen, bevor die Daten archiviert werden. Geben Sie **0** als „Archiv nach Tagen“ ein, um Ihre Sicherungsdatei direkt an den Archivspeicher zu senden.

   "Erfahren Sie mehr über die Storage-Einstellungen für Archive".

6. (Optional) Wählen Sie die Option **DataLock & Ransomware Protection** aus, um Ihre Backups vor Änderungen oder Löschungen zu schützen.

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

   "Erfahren Sie mehr über die verfügbaren DataLock-Einstellungen".

7. Wählen Sie **Erstellen**.

Bearbeiten Sie eine Richtlinie

Sie können benutzerdefinierte Snapshot-, Replizierungs- oder Backup-Richtlinien bearbeiten.

Eine Änderung der Backup-Richtlinie wirkt sich auf alle Volumes aus, die diese Richtlinie verwenden.

Schritte

1. Wählen Sie auf der Seite Richtlinienverwaltung die Richtlinie aus, und wählen Sie die Option **actions** aus ••• Und wählen Sie **Richtlinie bearbeiten**.

   Für Replizierungs- und Backup-Richtlinien ist der gleiche Prozess.

2. Nehmen Sie auf der Seite Richtlinie bearbeiten die Änderungen vor.
3. Wählen Sie **Speichern**.

Löschen Sie eine Richtlinie

Sie können Richtlinien löschen, die keinem Volume zugeordnet sind.

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

Schritte

1. Wählen Sie auf der Seite Richtlinienverwaltung die Richtlinie aus, und wählen Sie die Option **actions** aus ••• Und wählen Sie **Snapshot-Richtlinie löschen**.
2. Wählen Sie **Löschen**.

Weitere Informationen

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

"Erstellen Sie mit System Manager eine Snapshot-Richtlinie"
"Erstellen Sie eine Snapshot-Richtlinie über die ONTAP CLI"
"Erstellen Sie mit System Manager eine Replikationsrichtlinie"
"Erstellen Sie eine Replizierungsrichtlinie mithilfe der ONTAP-CLI"
"Erstellen Sie mit System Manager eine Richtlinie für das Backup auf Objekt-Storage"
"Erstellen Sie mithilfe der ONTAP CLI eine Richtlinie für das Backup in Objekt-Storage"

Backup-to-Object-Richtlinienoptionen in BlueXP Backup und Recovery

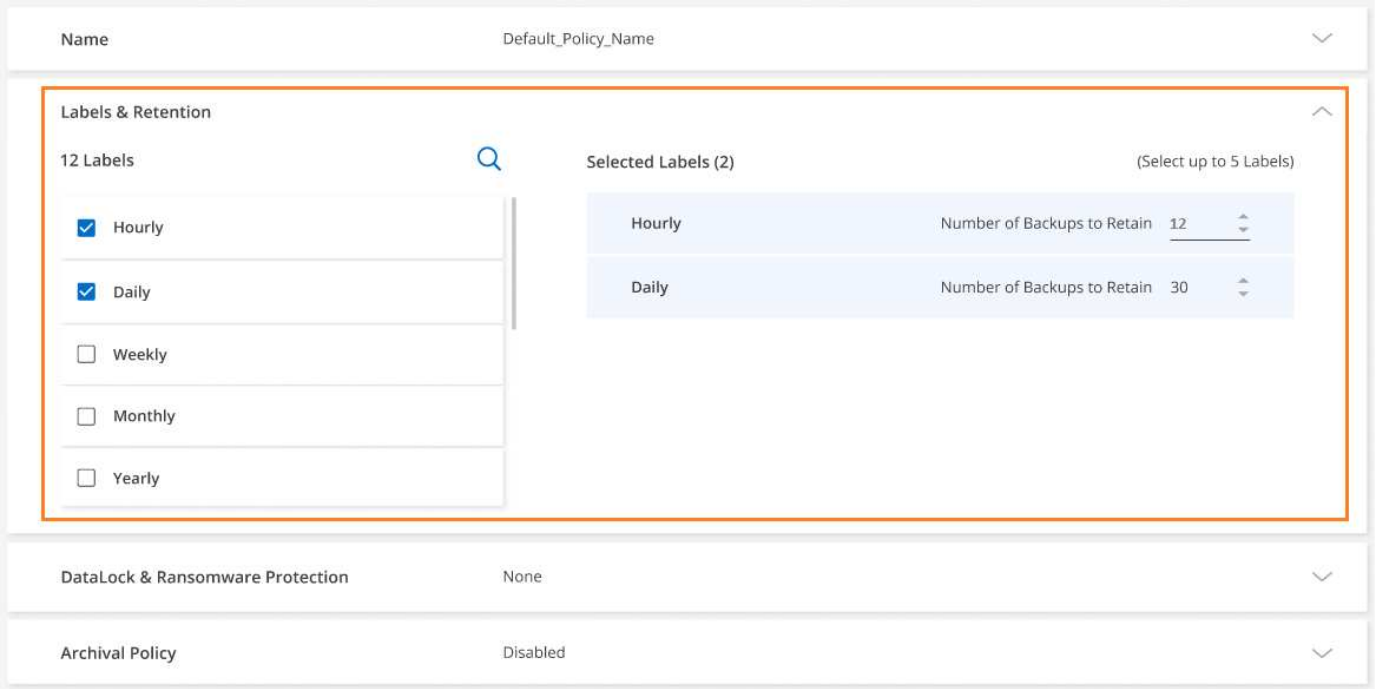
Mit BlueXP Backup und Recovery können Sie Backup-Richtlinien mit einer Vielzahl von Einstellungen für Ihre lokalen ONTAP und Cloud Volumes ONTAP Systeme erstellen.

Diese Richtlinieneinstellungen sind nur für den Objekt-Storage relevant. Keine dieser Einstellungen wirkt sich auf Ihre Snapshot- oder Replikationsrichtlinien aus. Ähnliche Richtlinieneinstellungen für Snapshots und Replikationen werden in Zukunft hinzugefügt.

Optionen für den Backup-Zeitplan

Mit BlueXP Backup und Recovery können Sie mehrere Backup-Richtlinien mit eindeutigen Zeitplänen für jede Arbeitsumgebung (Cluster) erstellen. Sie können Volumes mit unterschiedlichen Recovery-Punkten (RPO) unterschiedliche Backup-Richtlinien zuweisen.

Jede Sicherungsrichtlinie enthält einen Abschnitt für *Labels & Retention*, den Sie auf Ihre Sicherungsdateien anwenden können. Die auf das Volume angewendete Snapshot-Richtlinie muss eine der Richtlinien sein, die von BlueXP Backup- und Recovery- oder Backup-Dateien erkannt werden. Sie wird dann nicht erstellt.



Es gibt zwei Teile des Zeitplans: Das Etikett und der Aufbewahrungswert:

- Die **Bezeichnung** definiert, wie oft eine Sicherungsdatei aus dem Volume erstellt (oder aktualisiert) wird. Sie können eine der folgenden Beschriftungstypen auswählen:
  - Sie können eine oder eine Kombination aus, **stündlich**, **täglich**, **wöchentlich**, **monatlich**, Und **jährliche** Zeitrahmen.
  - Sie können eine der vom System definierten Richtlinien auswählen, die Backup und Aufbewahrung für 3 Monate, 1 Jahr oder 7 Jahre bieten.
  - Wenn Sie im Cluster benutzerdefinierte Backup-Sicherungsrichtlinien mit ONTAP System Manager oder der ONTAP CLI erstellt haben, können Sie eine dieser Richtlinien auswählen.
- Der Wert **Retention** definiert, wie viele Sicherungsdateien für jedes Etikett (Zeitrahmen) aufbewahrt werden. Sobald die maximale Anzahl von Backups in einer Kategorie oder Intervall erreicht wurde, werden ältere Backups entfernt, sodass Sie immer über die aktuellsten Backups verfügen. Dies spart auch Storage-Kosten, da veraltete Backups nicht mehr Speicherplatz in der Cloud belegen.

Beispiel: Erstellen Sie eine Backup Policy, die 7 **wöchentlich** und 12 **monatlich** Backups erstellt:

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

Beachten Sie, dass die jährlichen Backups nach der Übertragung in den Objektspeicher automatisch aus dem Quellsystem gelöscht werden. Dieses Standardverhalten kann geändert werden "Klicken Sie auf der Seite Erweiterte Einstellungen auf" Für die Arbeitsumgebung.

DataLock- und Ransomware-Schutzoptionen

BlueXP Backup und Recovery bietet Unterstützung für DataLock und Ransomware-Schutz für Ihre Volume-Backups. Mit diesen Funktionen sperren Sie Ihre Backup-Dateien und scannen sie, um mögliche Ransomware auf den Backup-Dateien zu erkennen. Dies ist eine optionale Einstellung, die Sie in Ihren Backup-Richtlinien definieren können, wenn Sie zusätzliche Sicherheit für Ihre Volume-Backups für ein Cluster wünschen.

Beide Funktionen schützen Ihre Backup-Dateien, sodass Sie bei einem Ransomware-Angriff auf Ihre Backups immer über eine gültige Backup-Datei verfügen, von der Sie Daten wiederherstellen können. Darüber hinaus hilft es bei der Einhaltung bestimmter gesetzlicher Vorgaben, bei denen Backups für einen bestimmten Zeitraum gesperrt und aufbewahrt werden müssen. Wenn die Option DataLock und Ransomware-Schutz aktiviert ist, sind für den Cloud-Bucket, der als Teil der Backup- und Recovery-Aktivierung von BlueXP bereitgestellt wird, Objektsperrung und Objektversionierung aktiviert.

"Weitere Informationen finden Sie im Blog zum Schutz von DataLock und Ransomware".

Diese Funktion bietet keinen Schutz für Ihre Quell-Volumes, sondern nur für die Backups dieser Quell-Volumes. Verwenden Sie einige der "Ransomware-Schutz durch ONTAP" um Ihre Quellvolumes zu schützen.

- Wenn Sie DataLock- und Ransomware-Schutz verwenden möchten, können Sie diese beim Erstellen Ihrer ersten Backup-Richtlinie und beim Aktivieren von BlueXP Backup und Recovery für diesen Cluster aktivieren. Sie können Ransomware-Scans später mithilfe der erweiterten Einstellungen für BlueXP Backup und Recovery aktivieren oder deaktivieren.
- Wenn BlueXP beim Wiederherstellen von Volume-Daten eine Backup-Datei auf Ransomware scannt, fallen für den Zugriff auf die Inhalte der Backup-Datei zusätzliche Kosten von Ihrem Cloud-Provider an.

Was ist DataLock

DataLock schützt Ihre Sicherungsdateien vor einer bestimmten Zeit, die auch *unveränderlicher Speicher* genannt wird. Diese Funktionalität nutzt Technologie des Objekt-Storage-Providers zur „Objektsperrung“. Der Zeitraum, in dem die Sicherungsdatei gesperrt (und aufbewahrt) ist, wird als Aufbewahrungszeitraum für DataLock bezeichnet. Er basiert auf dem von Ihnen definierten Zeitplan für die Backup-Richtlinie und der Aufbewahrungseinstellung sowie auf einem Puffer von maximal 31 Tagen. Jede DataLock-Aufbewahrungsrichtlinie, die weniger als 31 Tage beträgt, wird auf mindestens 31 Tage aufgerundet.

Beachten Sie, dass alte Backups nach Ablauf des Aufbewahrungszeitraums von DataLock gelöscht werden, nicht nach Ablauf der Aufbewahrungsfrist für Backups.

Sehen wir uns einige Beispiele an, wie das funktioniert:

- Wenn Sie einen monatlichen Backup-Zeitplan mit 12 Retentions erstellen, wird jedes Backup für 12 Monate (plus einen maximalen 31-Tage-Puffer) gesperrt, bevor es gelöscht wird.
- Wenn Sie eine Sicherungsrichtlinie erstellen, die 30 tägliche, 7 wöchentliche, 12 monatliche Backups erstellt, gibt es drei Aufbewahrungsfristen. Die „30 täglichen“ Backups würden für 44 Tage (30 Tage plus einen maximalen 31-Tage-Puffer) aufbewahrt, die „7 wöchentlichen“ Backups für 9 Wochen (7 Wochen plus einen maximalen 31-Tage-Puffer) aufbewahrt und die „12 monatlichen“ Backups für 12 Monate (plus einen maximalen 31-Tage-Puffer) aufbewahrt werden.
- Wenn Sie einen stündlichen Backup-Zeitplan mit 24 Aufbewahrung erstellen, könnten Sie denken, dass Backups für 24 Stunden gesperrt sind. Da dies jedoch weniger als 30 Tage beträgt, wird jedes Backup gesperrt und 44 Tage lang aufbewahrt (30 Tage plus maximal 31 Tage Puffer).

  Sie können in diesem letzten Fall sehen, dass, wenn jede Backup-Datei für 30 Tage gesperrt ist (plus einen maximalen 31-Tage-Puffer), Sie mit viel mehr Backup-Dateien enden, als in der Regel mit einer stündlichen/24 Retentions Policy beibehalten würde. Wenn BlueXP Backup und Recovery die 25. Backup-Datei erstellt, würde es normalerweise das älteste Backup löschen, um die maximalen Retentions bei 24 zu behalten (basierend auf der Richtlinie). Die DataLock-Aufbewahrungseinstellung überschreibt in diesem Fall die Richtlinienaufbewahrung von Ihrer Backup-Richtlinie. Dies könnte sich auf Ihre Storage-Kosten auswirken, da Backup-Dateien über einen längeren Zeitraum im Objektspeicher gespeichert werden.

Was ist Ransomware-Schutz

Ransomware-Schutz scannt Ihre Backup-Dateien, um einen Ransomware-Angriff auf einen Nachweis zu untersuchen. Die Erkennung von Ransomware-Angriffen erfolgt über einen Prüfsummenvergleich. Wenn potenzielle Ransomware-Angriffe in einer neuen Backup-Datei oder in einer vorherigen Backup-Datei erkannt werden, wird diese neuere Backup-Datei durch die neueste Backup-Datei ersetzt, die keine Anzeichen eines Ransomware-Angriffs zeigt. (Die Datei, die als Ransomware-Angriff gekennzeichnet ist, wird 1 Tag nach ihrer Ersetzung gelöscht.)

Ransomware-Scans finden an den folgenden Punkten des Backup- und Wiederherstellungsprozesses statt:

- Wenn eine Sicherungsdatei erstellt wird.

  Sie können Ransomware-Scans optional aktivieren oder deaktivieren.

  Der Scan wird nicht auf der Sicherungsdatei durchgeführt, wenn er zum ersten Mal in den Cloud-Speicher geschrieben wird, sondern wenn die **nächste** Sicherungsdatei geschrieben wird. Wenn Sie beispielsweise einen wöchentlichen Backup-Zeitplan für Dienstag eingestellt haben, wird am Dienstag den 14. Ein Backup erstellt. Dann am Dienstag der 21. Eine weitere Sicherung erstellt wird. Der Ransomware-Scan wird derzeit auf der Backup-Datei vom 14. Juni durchgeführt.

- Wenn Sie versuchen, Daten aus einer Sicherungsdatei wiederherzustellen

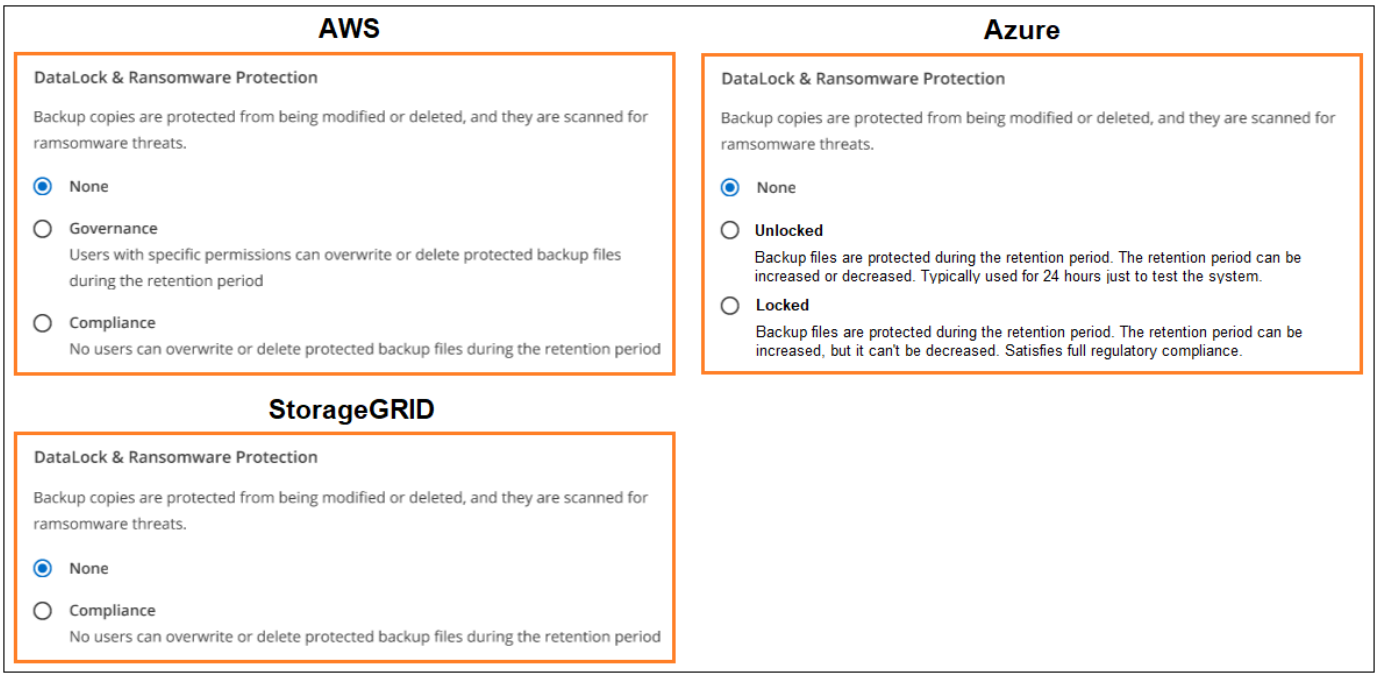
  Sie können einen Scan ausführen, bevor Sie Daten aus einer Sicherungsdatei wiederherstellen, oder diesen Scan überspringen.

- Manuell

  Sie können jederzeit einen Ransomware-Sicherheitsscan bei Bedarf ausführen und den Zustand einer spezifischen Backup-Datei überprüfen. Die Folgen sind besonders dann hilfreich, wenn Ransomware-Probleme auf einem bestimmten Volume gehabt haben und man überprüfen möchte, dass die Backups für das Volume nicht beeinträchtigt sind.

DataLock- und Ransomware-Schutzoptionen

Jede Sicherungsrichtlinie enthält einen Abschnitt für *DataLock und Ransomware-Schutz*, den Sie auf Ihre Backup-Dateien anwenden können.



Scans nach Ransomware-Schutz sind standardmäßig aktiviert. Die Standardeinstellung für die Scanfrequenz beträgt 7 Tage. Der Scan wird nur auf der letzten Snapshot Kopie durchgeführt. Sie können Ransomware-Scans auf der letzten Snapshot Kopie mit der Option auf der Seite „Erweiterte Einstellungen“ aktivieren oder deaktivieren. Wenn Sie diese Option aktivieren, werden standardmäßig alle 7 Tage gescannt.

Sie können diesen Zeitplan auf Tage oder Wochen ändern oder deaktivieren, um Kosten zu sparen.

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

Für jede Backup-Richtlinie stehen folgende Einstellungen zur Verfügung:

AWS

- **Keine** (Standard)

  DataLock-Schutz und Ransomware-Schutz sind deaktiviert.

- * Governance*

  DataLock ist auf *Governance*-Modus eingestellt, bei dem Benutzer mit `s3:BypassGovernanceRetention` Berechtigung ("Siehe unten") Können Sicherungsdateien während der Aufbewahrungsfrist überschreiben oder löschen. Ransomware-Schutz ist aktiviert.

- * Compliance*

  DataLock ist auf den *Compliance*-Modus eingestellt, in dem während der Aufbewahrungszeit keine Benutzer Sicherungsdateien überschreiben oder löschen können. Ransomware-Schutz ist aktiviert.

Azure

- **Keine** (Standard)

  DataLock-Schutz und Ransomware-Schutz sind deaktiviert.

- **Entsperrt**

  Backup-Dateien werden während der Aufbewahrungsfrist geschützt. Die Aufbewahrungsfrist kann erhöht oder verkürzt werden. Wurde normalerweise 24 Stunden für das Testen des Systems verwendet. Ransomware-Schutz ist aktiviert.

- **Gesperrt**

  Backup-Dateien werden während der Aufbewahrungsfrist geschützt. Der Aufbewahrungszeitraum kann erhöht werden, kann aber nicht verkürzt werden. Erfüllt vollständige Einhaltung gesetzlicher Vorschriften Ransomware-Schutz ist aktiviert.

StorageGRID

- **Keine** (Standard)

  DataLock-Schutz und Ransomware-Schutz sind deaktiviert.

- * Compliance*

  DataLock ist auf den *Compliance*-Modus eingestellt, in dem während der Aufbewahrungszeit keine Benutzer Sicherungsdateien überschreiben oder löschen können. Ransomware-Schutz ist aktiviert.

Unterstützte Arbeitsumgebungen und Objekt-Storage-Anbieter

Bei Verwendung von Objekt-Storage bei den folgenden Public- und Private-Cloud-Providern können Sie die DataLock- und Ransomware-Sicherung auf ONTAP Volumes aus den folgenden Arbeitsumgebungen aktivieren. Weitere Cloud-Provider werden in zukünftigen Versionen hinzugefügt.

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[] endif::gcp[]
Lokales ONTAP System	Ifdef::aws[] Amazon S3 endif::aws[] ifdef::azurAzure[] Azure Blob endif::Azure[] ifdef::gcp[] endif::gcp[] NetApp StorageGRID

Anforderungen

- Für AWS:
  - Ihre Cluster müssen ONTAP 9.11.1 oder höher ausführen
  - Der Connector kann in der Cloud oder vor Ort bereitgestellt werden
  - Die folgenden S3-Berechtigungen müssen Teil der IAM-Rolle sein, die dem Connector Berechtigungen erteilt. Sie befinden sich im Abschnitt „BackupS3Policy“ für die Ressource „arn:aws:s3::netapp-Backup-*“:

AWS S3 Berechtigungen

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAkl
- s3:PuttObjectTagging
- s3:DeleteObject
- s3:DeleteObjectTagging
- s3:GetObjectRetention
- s3:DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleKonfiguration
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBucketVersions
- s3:ListBucket
- s3:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketVersionierung
- s3:PuttObjectVersionTagging
- s3:GetBucketVersionierung
- s3:GetBucketAcl
- s3:BypassGovernanceAufbewahrung
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

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

- Für Azure:
  - Ihre Cluster müssen ONTAP 9.12.1 oder höher ausführen
  - Der Connector kann in der Cloud oder vor Ort bereitgestellt werden
- Für StorageGRID:
  - Ihre Cluster müssen ONTAP 9.11.1 oder höher ausführen
  - Auf Ihren StorageGRID Systemen muss 11.6.0.3 oder höher ausgeführt werden
  - Der Connector muss auf Ihrem Gelände bereitgestellt werden (er kann auf einer Website mit oder ohne

Internetzugang installiert werden).

- Die folgenden S3-Berechtigungen müssen Teil der IAM-Rolle sein, die dem Connector Berechtigungen bereitstellt:

  StorageGRID S3 Berechtigungen

  - s3:GetObjectVersionTagging
  - s3:GetBucketObjectLockConfiguration
  - s3:GetObjectVersionAkl
  - s3:PuttObjectTagging
  - s3:DeleteObject
  - s3:DeleteObjectTagging
  - s3:GetObjectRetention
  - s3:DeleteObjectVersionTagging
  - s3:PutObject
  - s3:GetObject
  - s3:PutBucketObjectLockConfiguration
  - s3:GetLifecycleKonfiguration
  - s3:GetBucketTagging
  - s3:DeleteObjectVersion
  - s3:ListBucketVersions
  - s3:ListBucket
  - s3:PutBucketTagging
  - s3:GetObjectTagging
  - s3:PutBucketVersionierung
  - s3:PuttObjectVersionTagging
  - s3:GetBucketVersionierung
  - s3:GetBucketAcl
  - s3:PutObjectRetention
  - s3:GetBucketLocation
  - s3:GetObjectVersion

Einschränkungen

- Die Data Lock- und Ransomware-Schutzfunktion ist nicht verfügbar, wenn Sie in der Backup-Richtlinie Archivspeicher konfiguriert haben.
- Die bei der Aktivierung von BlueXP ausgewählte DataLock Option für Backup und Recovery muss für alle Backup-Richtlinien für dieses Cluster verwendet werden.
- Sie können nicht mehrere DataLock-Modi auf einem einzelnen Cluster verwenden.
- Wenn Sie DataLock aktivieren, werden alle Volume-Backups gesperrt. Es können keine gesperrten und

nicht gesperrten Volume-Backups für einen einzelnen Cluster kombiniert werden.

- DataLock- und Ransomware-Schutz ist für neue Volume-Backups mit einer Backup-Richtlinie mit aktiviertem DataLock und Ransomware-Schutz anwendbar. Sie können diese Funktionen später über die Option Erweiterte Einstellungen aktivieren oder deaktivieren.
- FlexGroup Volumes können DataLock- und Ransomware-Schutz nur verwenden, wenn ONTAP 9.13.1 oder höher verwendet wird.

Tipps zur Senkung von DataLock-Kosten

Sie können die Ransomware-Scan-Funktion aktivieren oder deaktivieren, während die DataLock-Funktion aktiv bleibt. Um zusätzliche Kosten zu vermeiden, können Sie geplante Ransomware-Scans deaktivieren. Auf diese Weise können Sie Ihre Sicherheitseinstellungen anpassen und Kosten durch den Cloud-Provider vermeiden.

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

Sie können verschiedene Schutzstufen wählen:

- **DataLock *ohne* Ransomware-Scans**: Bietet Schutz für Backup-Daten im Zielspeicher, die sich entweder im Governance- oder im Compliance-Modus befinden können.
  - **Governance-Modus**: Bietet Administratoren Flexibilität, geschützte Daten zu überschreiben oder zu löschen.
  - **Compliance-Modus**: Bietet vollständige Unlöschbarkeit bis zum Ablauf der Aufbewahrungsfrist. So lassen sich auch die strengsten Datensicherheitsanforderungen hochgradig regulierter Umgebungen erfüllen. Die Daten können während ihres Lebenszyklus nicht überschrieben oder geändert werden. Dies bietet den bestmöglichen Schutz für Ihre Backup-Kopien.

    Microsoft Azure verwendet stattdessen einen Sperrmodus und einen Entsperrmodus.

- **DataLock *mit* Ransomware-Scans**: Bietet eine zusätzliche Sicherheitsschicht für Ihre Daten. Diese Funktion hilft bei der Erkennung von Versuchen, Sicherungskopien zu ändern. Bei einem Versuch wird diskret eine neue Version der Daten erstellt. Die Scanfrequenz kann in 1, 2, 3, 4, 5 geändert werden. 6 oder 7 Tage. Werden Scans alle 7 Tage eingestellt, sinken die Kosten deutlich.

Weitere Tipps zur Senkung der DataLock-Kosten finden Sie unter https://community.netapp.com/t5/Tech-ONTAP-Blogs/Understanding-BlueXP-Backup-and-Recovery-DataLock-and-Ransomware-Feature-TCO/ba-p/453475

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

Storage-Optionen für die Archivierung

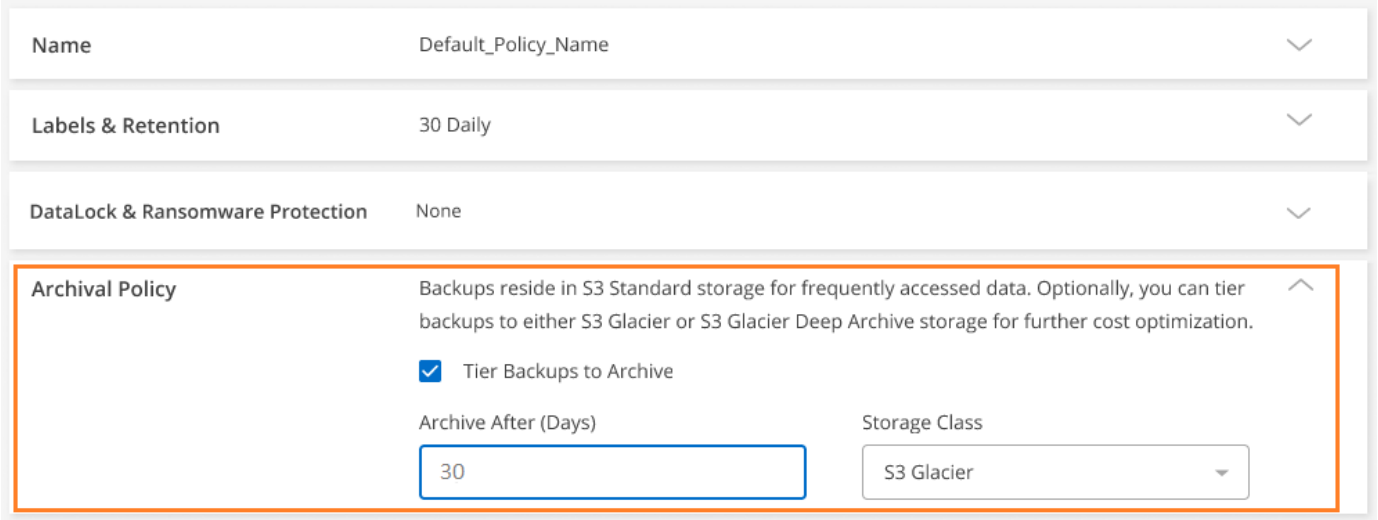
Beim Einsatz von AWS, Azure oder Google Cloud Storage können Sie ältere Backup-Dateien nach einer bestimmten Anzahl von Tagen auf eine kostengünstigere Archiv-Storage-Klasse oder auf eine Zugriffs-Tier verschieben. Sie haben auch die Möglichkeit, die Backup-Dateien sofort in den Archiv-Storage zu senden, ohne dafür in standardmäßigen Cloud-Storage geschrieben zu werden. Geben Sie einfach **0** als "Archiv nach Tagen" ein, um Ihre Sicherungsdatei direkt an den Archivspeicher zu senden. Dies kann insbesondere für Benutzer nützlich sein, die selten auf Daten aus Cloud-Backups zugreifen müssen oder Benutzer, die eine Tape-Backup-Lösung ersetzen.

Auf Daten auf Archiv-Tiers kann bei Bedarf nicht sofort zugegriffen werden und die Abrufkosten sind höher.

Daher müssen Sie berücksichtigen, wie häufig Daten aus Backup-Dateien wiederhergestellt werden müssen, bevor Sie sich für die Archivierung Ihrer Backup-Dateien entscheiden.

- Selbst wenn Sie „0“ wählen, um alle Datenblöcke an Cloud-Archiv-Storage zu senden, werden Metadaten-Blöcke immer in Standard-Cloud-Storage geschrieben.
- Archivspeicher kann nicht verwendet werden, wenn Sie DataLock aktiviert haben.
- Sie können die Archivierungsrichtlinie nicht ändern, nachdem Sie **0** Tage (sofort archivieren) ausgewählt haben.

Jede Backup-Richtlinie enthält einen Abschnitt zur „ *Archivierungsrichtlinie*“, den Sie auf Ihre Backup-Dateien anwenden können.



- 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 entweder auf *S3 Glacier* oder *S3 Glacier Deep Archive* Storage Tiering. "Weitere Informationen zu AWS Archiv-Storage".

  - Wenn Sie bei der Aktivierung von BlueXP Backup und Recovery in Ihrer ersten Backup-Richtlinie keinen Archiv-Tier auswählen, wird *S3 Glacier* Ihre einzige Archivierungsoption für zukünftige Richtlinien sein.
  - Wenn Sie in Ihrer ersten Backup-Richtlinie *S3 Glacier* auswählen, können Sie für zukünftige Backup-Richtlinien für diesen Cluster in die *S3 Glacier Deep Archive*-Ebene wechseln.
  - Wenn Sie in Ihrer ersten Backup-Richtlinie *S3 Glacier Deep Archive* auswählen, ist diese Tier die einzige Archiv-Tier, die für zukünftige Backup-Richtlinien für diesen Cluster verfügbar ist.
- In Azure werden Backups im Zusammenhang mit der *Cool* Zugriffsebene durchgeführt.

  Wenn Ihr Cluster ONTAP 9.10.1 oder höher verwendet, können Sie ältere Backups auf *Azure Archive* Storage Tiering. "Erfahren Sie mehr über Azure Archiv-Storage".

- In GCP werden Backups der Klasse *Standard* Storage zugeordnet.

  Wenn Ihr On-Premises-Cluster ONTAP 9.12.1 oder höher verwendet, haben Sie nach einer bestimmten Anzahl von Tagen die Möglichkeit, ältere Backups in der Backup- und Recovery-UI von BlueXP auf den *Archiv* Storage zu verschieben, um weitere Kosten zu optimieren. "Erfahren Sie mehr über Google Archivspeicher".

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

  Wenn Ihr On-Premises-Cluster ONTAP 9.12.1 oder höher verwendet und Ihr StorageGRID System mindestens 11.4 nutzt, können Sie ältere Backup-Dateien im Public-Cloud-Archiv-Storage archivieren.

+ ** bei AWS, können Sie Backups in AWS *S3 Glacier* oder *S3 Glacier Deep Archive* Storage Tiering. "Weitere Informationen zu AWS Archiv-Storage".

+ ** bei Azure, können Sie ältere Backups in *Azure Archive* Storage Tiering. "Erfahren Sie mehr über Azure Archiv-Storage".

+
"Weitere Informationen zur Archivierung von Backup-Dateien aus StorageGRID".

Verwalten Sie die Optionen für die Sicherung auf Objektspeicher auf der Seite „Erweiterte Einstellungen“ von BlueXP Backup and Recovery

Über die Seite „Erweiterte Einstellungen“ können Sie Einstellungen für Storage auf Cluster-Ebene und Backup-to-Objekt-Storage ändern, die Sie bei der Aktivierung von BlueXP Backup und Recovery für jedes ONTAP System festlegen. Sie können auch einige Einstellungen ändern, die als „Standard“-Backup-Einstellungen angewendet werden. Dazu gehört auch die Änderung der Übertragungsrate von Backups in Objekt-Storage, unabhängig davon, ob historische Snapshot Kopien als Backup-Dateien exportiert werden, und die Aktivierung oder Deaktivierung von Ransomware-Scans für eine Arbeitsumgebung.

Diese Einstellungen sind nur für Backup-to-Object-Speicher verfügbar. Keine dieser Einstellungen wirkt sich auf Ihre Snapshot- oder Replikationseinstellungen aus. Ähnliche Einstellungen für die Replikation auf Cluster-Ebene für Snapshots und Replikationen werden in Zukunft hinzugefügt.

Auf der Seite Erweiterte Einstellungen können Sie die folgenden Optionen ändern:

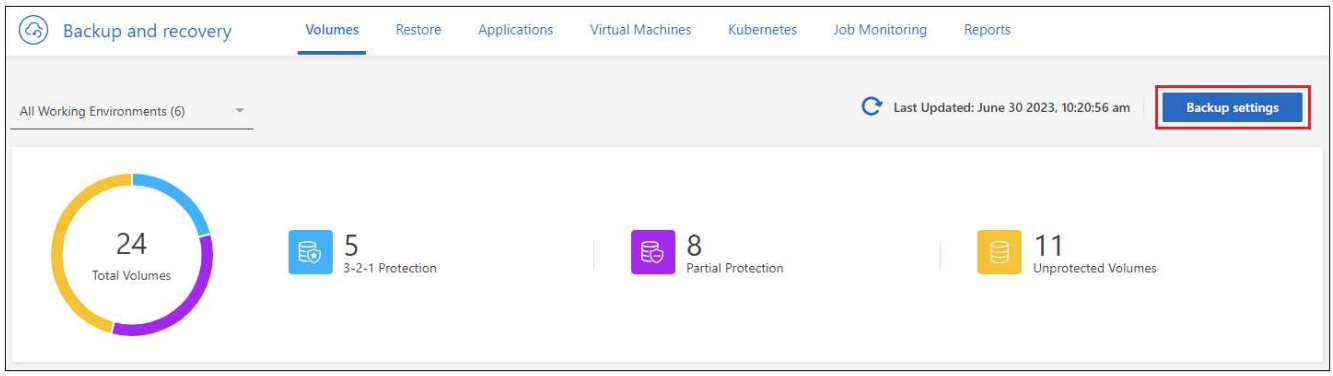
- Ändern der zum Hochladen von Backups auf den Objektspeicher zugewiesenen Netzwerkbandbreite mit der Option Max. Übertragungsrate
  Ifdef::aws[]
- Es ändert sich, ob historische Snapshot Kopien als Backup-Dateien exportiert und in den ersten Basis-Backup-Dateien für zukünftige Volumes enthalten sind
- Es wird geändert, ob „jährliche“ Snapshots aus dem Quellsystem entfernt werden
- Aktivieren oder Deaktivieren von Ransomware-Scans für eine Arbeitsumgebung, einschließlich geplanter Scans

Zeigen Sie Backup-Einstellungen auf Cluster-Ebene an

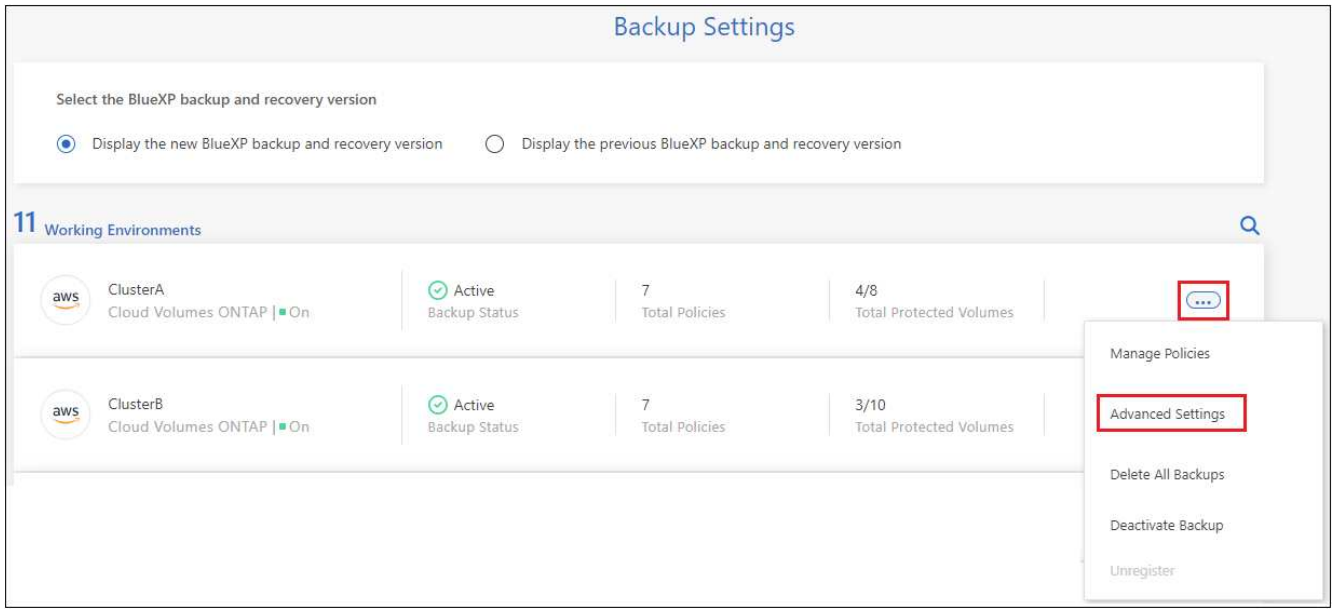
Sie können die Backup-Einstellungen auf Clusterebene für jede Arbeitsumgebung anzeigen.

Schritte

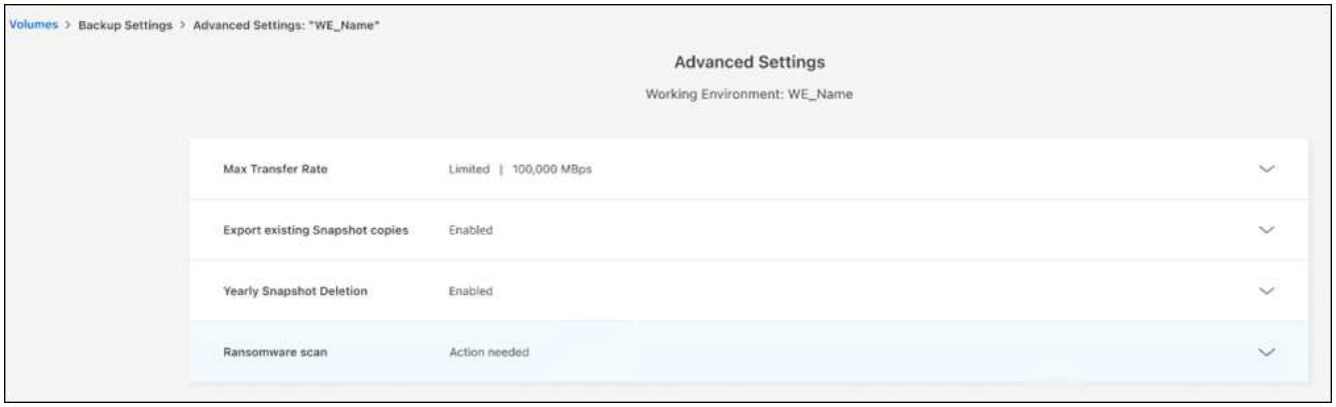
1. Wählen Sie im Menü BlueXP die Option **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.



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.



4. Erweitern Sie die Option, und nehmen Sie die Änderung vor.

Alle Backup-Vorgänge nach der Änderung verwenden die neuen Werte.

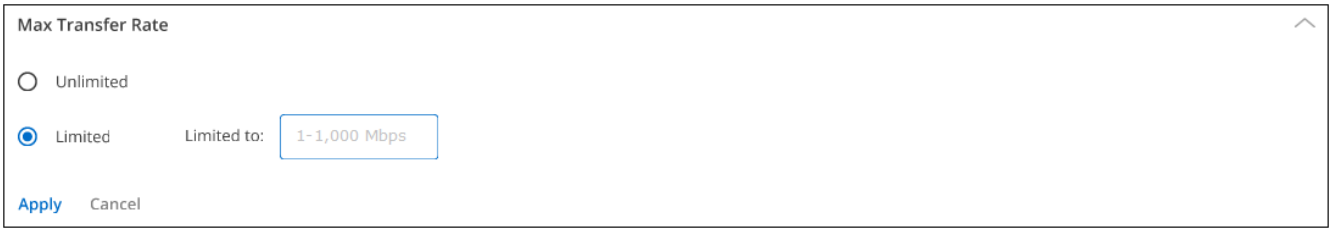
Beachten Sie, dass einige Optionen basierend auf der Version von ONTAP auf dem Quell-Cluster nicht verfügbar sind und auf dem Ziel des Cloud-Providers, in dem sich die Backups befinden, basieren.

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

Wenn Sie BlueXP Backup und Recovery für eine funktionierende Umgebung aktivieren, kann ONTAP standardmäßig eine unbegrenzte Bandbreite verwenden, um die Backup-Daten von den Volumes in der Arbeitsumgebung in den Objekt-Storage zu übertragen. Wenn Sie feststellen, dass der Backup-Verkehr normale Benutzer-Workloads beeinträchtigt, können Sie die während der Übertragung verwendete Netzwerkbandbreite mithilfe der Option maximale Übertragungsrate auf der Seite Erweiterte Einstellungen drosseln.

Schritte

1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.
2. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Wählen Sie für die Arbeitsumgebung die Option **Erweiterte Einstellungen** aus.
3. Erweitern Sie auf der Seite Erweiterte Einstellungen den Abschnitt **Max. Übertragungsrate**.



4. Wählen Sie einen Wert zwischen 1 und 1,000 Mbit/s als maximale Übertragungsrate.
5. 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.
6. Wählen Sie **Anwenden**.

Diese Einstellung wirkt sich nicht auf die Bandbreite aus, die anderen Replikationsbeziehungen zugewiesen ist, die für Volumes in der Arbeitsumgebung konfiguriert werden können.

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

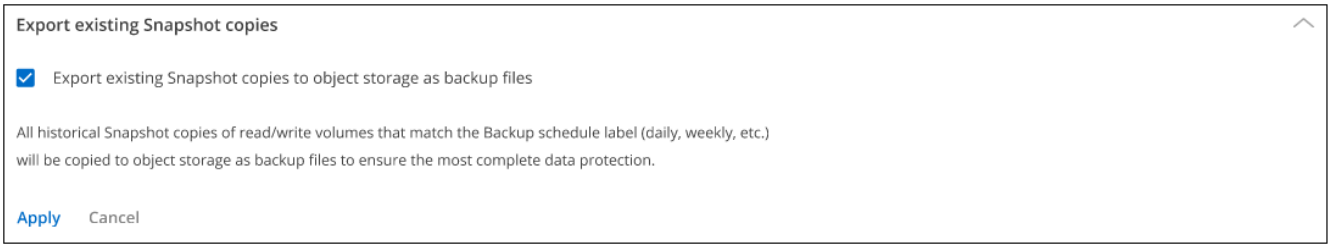
Wenn es lokale Snapshot-Kopien für Volumes gibt, die mit dem Backup-Schedule-Label übereinstimmen, das Sie in dieser Arbeitsumgebung verwenden (z. B. täglich, wöchentlich usw.), können Sie diese historischen Snapshots als Backup-Dateien in Objekt-Storage exportieren. Damit können Sie Ihre Backups in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

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 die Option **Erweiterte Einstellungen** aus.

3. Erweitern Sie auf der Seite Erweiterte Einstellungen den Abschnitt **vorhandene Snapshot-Kopien exportieren**.



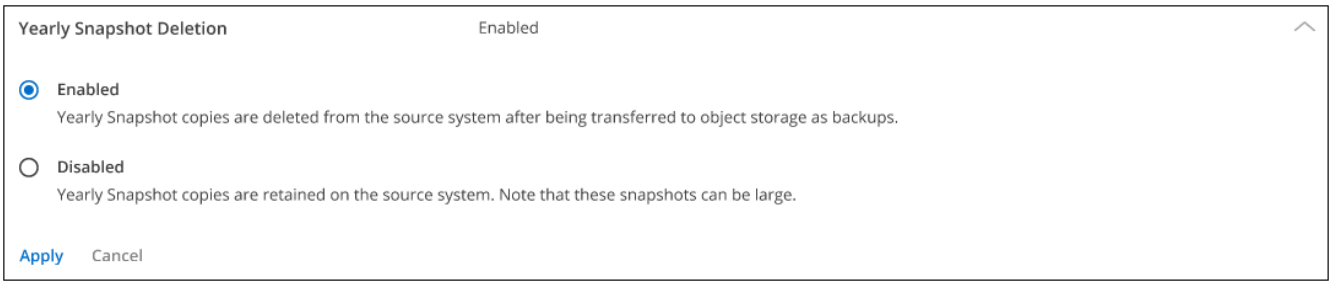
4. Wählen Sie, ob vorhandene Snapshot Kopien exportiert werden sollen.
5. Wählen Sie **Anwenden**.

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

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

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 die Option **Erweiterte Einstellungen** aus.
3. Erweitern Sie auf der Seite Erweiterte Einstellungen den Abschnitt **jährliches Löschen von Snapshots**.



4. Wählen Sie **disabled** aus, um die jährlichen Snapshots auf dem Quellsystem beizubehalten.
5. Wählen Sie **Anwenden**.

Aktivieren oder deaktivieren Sie Ransomware-Scans

Scans nach Ransomware-Schutz sind standardmäßig aktiviert. Die Standardeinstellung für die Scanfrequenz beträgt 7 Tage. Der Scan wird nur auf der letzten Snapshot Kopie durchgeführt. Sie können Ransomware-Scans auf der letzten Snapshot Kopie mit der Option auf der Seite „Erweiterte Einstellungen“ aktivieren oder deaktivieren. Wenn Sie diese Option aktivieren, werden standardmäßig alle 7 Tage gescannt.

Sie können diesen Zeitplan auf Tage oder Wochen ändern oder deaktivieren, um Kosten zu sparen.

Bei der Aktivierung von Ransomware-Scans können je nach Cloud-Provider zusätzliche Gebühren anfallen.

Geplante Ransomware-Scans werden nur mit der neuesten Snapshot Kopie ausgeführt.

Wenn die geplanten Ransomware-Scans deaktiviert sind, können Sie dennoch On-Demand-Scans durchführen und während der Wiederherstellung einen Scan durchführen.

Siehe "Management von Richtlinien" Finden Sie Details zum Management von Richtlinien, die Ransomware-Erkennung implementieren.

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 die Option **Erweiterte Einstellungen** aus.
3. Erweitern Sie auf der Seite Erweiterte Einstellungen den Abschnitt **Ransomware-Scan**.
4. Aktivieren oder deaktivieren Sie **Ransomware Scan**.
5. Wählen Sie * geplante Ransomware-Scan*.
6. Ändern Sie optional den Standardscan jede Woche in Tage oder Wochen.
7. Legen Sie fest, wie oft der Scan in Tagen oder Wochen ausgeführt werden soll.
8. Wählen Sie **Anwenden**.

Sichern Sie Cloud Volumes ONTAP-Daten mit BlueXP Backup und Recovery auf Amazon S3

Führen Sie einige Schritte zur Sicherung und Wiederherstellung mit BlueXP durch, um mit der Sicherung von Volume-Daten von Ihren Cloud Volumes ONTAP-Systemen auf 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.

Überprüfen Sie die Unterstützung Ihrer Konfiguration

- Sie verwenden Cloud Volumes ONTAP 9.8 oder höher in AWS (ONTAP 9.8P13 und höher wird empfohlen).
- 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 BYOL-Lizenz für BlueXP Backup und Recovery von NetApp.
- Sie haben einen Connector in AWS installiert:
  - Der Connector kann auf einer Website mit vollem Internetzugang ("Standard-Modus") oder mit eingeschränkter Internetverbindung ("eingeschränkter Modus") installiert werden.
  - Die IAM-Rolle, die den BlueXP Connector mit Berechtigungen bereitstellt, umfasst die neuesten S3-Berechtigungen "BlueXP-Richtlinie".

Bereiten Sie Ihren BlueXP Connector vor

Wenn Sie bereits einen Connector in einer AWS-Region implementiert haben, dann sind Sie fertig. Falls nicht, müssen Sie einen BlueXP Connector in AWS installieren, um Cloud Volumes ONTAP Daten in AWS zu sichern. Der Connector kann auf einer Website mit vollem Internetzugang ("Standard-Modus") oder mit eingeschränkter Internetverbindung ("eingeschränkter Modus") installiert werden.

Lizenzanforderungen prüfen

Sie müssen die Lizenzanforderungen sowohl für AWS als auch für BlueXP prüfen.

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes

Stellen Sie sicher, dass die primären und sekundären Storage-Systeme die Anforderungen der ONTAP Version und des Netzwerks erfüllen.

BlueXP Backup und Recovery ermöglichen

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

Aktivieren Sie Backups auf Ihren ONTAP Volumes

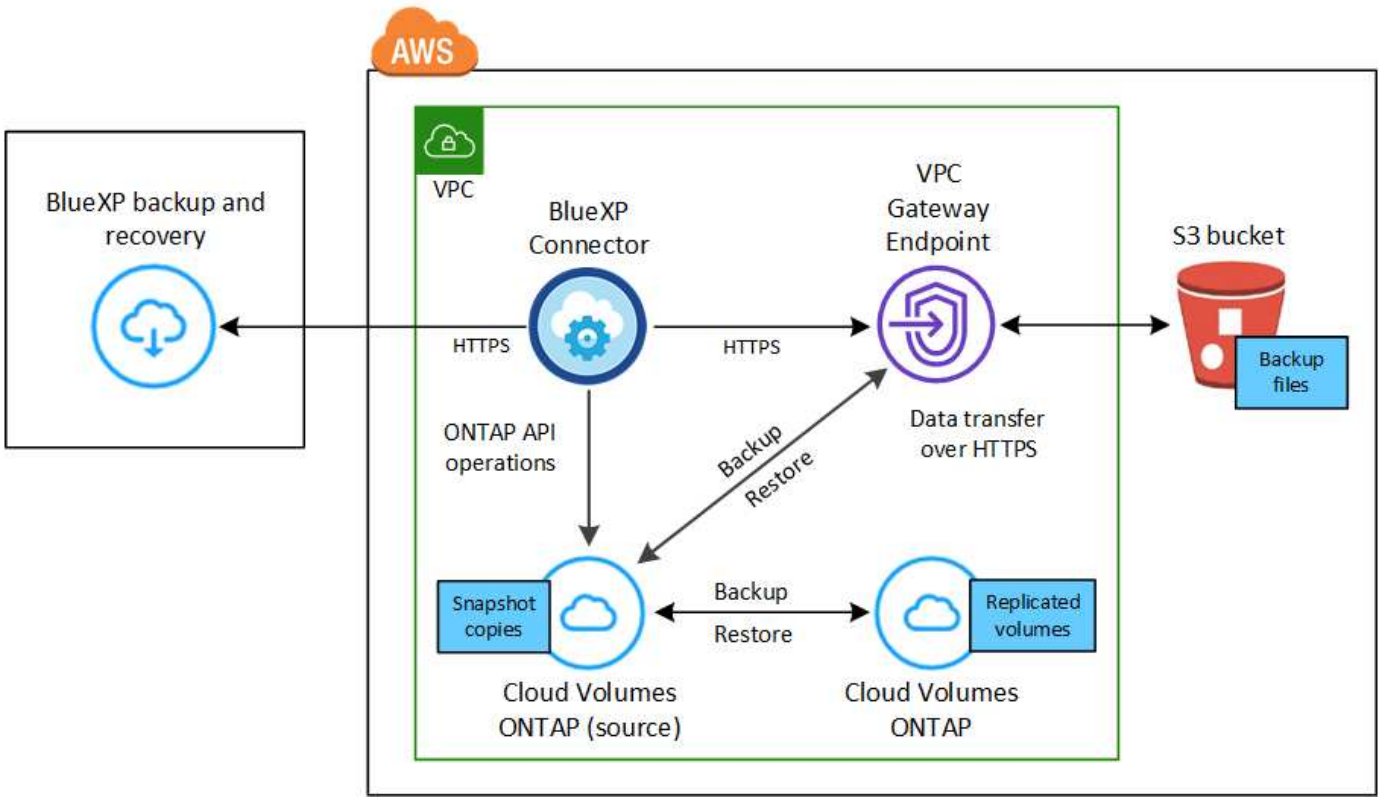
Folgen Sie dem Setup-Assistenten, um die Replikations- und Backup-Richtlinien auszuwählen, die Sie verwenden möchten, sowie die Volumes, die Sie sichern möchten.

Überprüfen Sie die Unterstützung Ihrer Konfiguration

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 jede Komponente und die Verbindungen, die Sie zwischen ihnen vorbereiten müssen.

Optional können Sie für replizierte Volumes auch eine Verbindung zu einem sekundären ONTAP-System über eine öffentliche oder private Verbindung herstellen.



Der VPC-Gateway-Endpunkt muss bereits in der VPC vorhanden sein. "Weitere Informationen zu Gateway-Endpunkten".

Unterstützte ONTAP-Versionen

Mindestens ONTAP 9.8; ONTAP 9.8P13 und höher wird empfohlen.

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".

Lizenzanforderungen prüfen

Für die PAYGO-Lizenzierung für BlueXP Backup und Recovery ist im AWS Marketplace ein BlueXP Abonnement verfügbar, das die Implementierung von Cloud Volumes ONTAP und BlueXP Backup und Recovery ermöglicht. Sie müssen "Melden Sie sich für dieses BlueXP-Abonnement an" Bevor Sie BlueXP Backup und Recovery aktivieren, Die Abrechnung für BlueXP Backup und Recovery 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".

Wenn Sie eine Cloud Volumes ONTAP Arbeitsumgebung erstellen, müssen Sie bei einem Jahresvertrag für die Bündelung von Backup und Recovery von Cloud Volumes ONTAP und BlueXP ein Jahresvertrag abschließen. Mit dieser Option können Sie Backups von Daten vor Ort nicht erstellen.

Für die BYOL-Lizenzierung für BlueXP Backup und Recovery benötigen Sie die Seriennummer von NetApp, anhand derer Sie den Service für die Dauer und Kapazität der Lizenz nutzen können. "Erfahren Sie, wie Sie Ihre BYOL-Lizenzen managen". Sie müssen eine BYOL-Lizenz verwenden, wenn der Connector und das Cloud Volumes ONTAP-System an einem dunklen Standort bereitgestellt werden.

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

Bereiten Sie Ihren BlueXP Connector vor

Der Connector muss in einer AWS Region mit vollem oder eingeschränktem Internetzugang installiert sein („Standard“ oder „eingeschränkter“ Modus). "Einzelheiten finden Sie in den BlueXP Implementierungsmodi".

- "Erfahren Sie mehr über Steckverbinder"
- "Implementieren eines Connectors in AWS im Standardmodus (vollständiger Internetzugang)"
- "Installieren Sie den Connector im eingeschränkten Modus (eingeschränkter Zugriff für ausgehende Verbindungen)."

Überprüfen oder Hinzufügen von Berechtigungen zum Konnektor

Die IAM-Rolle, die BlueXP Berechtigungen bereitstellt, muss die neuesten S3-Berechtigungen enthalten "BlueXP-Richtlinie". Wenn die Richtlinie nicht alle diese Berechtigungen enthält, finden Sie weitere Informationen unter "AWS Dokumentation: Bearbeiten der IAM-Richtlinien".

Hier sind die spezifischen Berechtigungen aus der Richtlinie:

```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutBucketOwnershipControls"
                "s3:PutBucketPublicAccessBlock",
                "s3:PutEncryptionConfiguration",
                "s3:GetObjectVersionTagging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectVersionAcl",
                "s3:PutObjectTagging",
                "s3:DeleteObjectTagging",
                "s3:GetObjectRetention",
                "s3:DeleteObjectVersionTagging",
                "s3:PutBucketObjectLockConfiguration",
                "s3:DeleteObjectVersion",
                "s3:GetObjectTagging",
                "s3:PutBucketVersioning",
                "s3:PutObjectVersionTagging",
                "s3:GetBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:PutObjectRetention",
                "s3:GetObjectVersion",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
```

```
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
                "glue:BatchDeletePartition"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

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

Erforderliche AWS Cloud Volumes ONTAP Berechtigungen

Wenn auf Ihrem Cloud Volumes ONTAP System ONTAP 9.12.1 oder eine höhere Software ausgeführt wird, muss die IAM-Rolle, die diese Arbeitsumgebung mit Berechtigungen bereitstellt, einen neuen Satz von S3-Berechtigungen enthalten, speziell für BlueXP-Backup und -Recovery von aktuellen Versionen "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.

Unterstützte AWS-Regionen

BlueXP-Sicherung und -Wiederherstellung wird in allen AWS-Regionen unterstützt, einschließlich der AWS GovCloud-Regionen.

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:

- Stellen Sie sicher, dass die Berechtigungen „s3:PutBucketPolicy“ und „s3:PutBucketOwnershipControls“ Teil der IAM-Rolle sind, die dem BlueXP Connector Berechtigungen erteilt.
- Fügen Sie die Anmeldeinformationen für das AWS Zielkonto in BlueXP hinzu. "So geht's".
- Fügen Sie die folgenden Berechtigungen in den Benutzeranmeldeinformationen im zweiten Konto hinzu:

```
"athena:StartQueryExecution",
"athena:GetQueryResults",
"athena:GetQueryExecution",
"glue:GetDatabase",
"glue:GetTable",
"glue:CreateTable",
"glue:CreateDatabase",
"glue:GetPartitions",
"glue:BatchCreatePartition",
"glue:BatchDeletePartition"
```

Erstellen Sie Ihre eigenen Buckets

Standardmäßig erstellt der Service Buckets für Sie. Wenn Sie Ihre eigenen Buckets verwenden möchten, können Sie diese erstellen, bevor Sie den Assistenten für die Backup-Aktivierung starten und diese Buckets dann im Assistenten auswählen.

"Erfahren Sie mehr über das Erstellen eigener Buckets".

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes

Wenn Sie planen, mithilfe von BlueXP Backup und Recovery replizierte Volumes auf einem sekundären ONTAP System zu erstellen, stellen Sie sicher, dass die Quell- und Zielsysteme die folgenden Netzwerkanforderungen erfüllen.

Netzwerkanforderungen für On-Premises-ONTAP

- Wenn sich der Cluster an Ihrem Standort befindet, sollten Sie über eine Verbindung zwischen Ihrem Unternehmensnetzwerk und Ihrem virtuellen Netzwerk des Cloud-Providers verfügen. Hierbei handelt es sich in der Regel um eine VPN-Verbindung.
- ONTAP Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Cluster-Anforderungen erfüllen.

  Da Sie Daten auf Cloud Volumes ONTAP oder auf lokale Systeme replizieren können, prüfen Sie Peering-Anforderungen für lokale ONTAP Systeme. "Anzeigen von Voraussetzungen für Cluster-Peering in der ONTAP-Dokumentation".

Netzwerkanforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen ein- und ausgehenden Regeln enthalten: Speziell Regeln für ICMP und die Ports 11104 und 11105. Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.
- Um Daten zwischen zwei Cloud Volumes ONTAP Systemen in verschiedenen Subnetzen zu replizieren, müssen die Subnetze gemeinsam geroutet werden (dies ist die Standardeinstellung).

BlueXP Backup und Recovery auf Cloud Volumes ONTAP ermöglichen

Die Aktivierung von BlueXP Backup und Recovery ist einfach. Die Schritte unterscheiden sich leicht, je nachdem, ob Sie ein bestehendes oder ein neues Cloud Volumes ONTAP-System besitzen.

BlueXP Backup und Recovery auf einem neuen System aktivieren

BlueXP Backup und Recovery sind 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. Wählen Sie im BlueXP-Bildschirm **Arbeitsumgebung hinzufügen**, wählen Sie den Cloud-Provider aus und wählen Sie **Neu hinzufügen**. Wählen Sie **Cloud Volumes ONTAP erstellen**.
2. Wählen Sie **Amazon Web Services** als Cloud-Provider aus und wählen Sie dann einen einzelnen Knoten oder ein HA-System aus.
3. Füllen Sie die Seite „Details & Credentials“ aus.
4. Lassen Sie den Dienst auf der Seite Dienste aktiviert, und wählen Sie **Weiter**.

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

Ergebnis

BlueXP Backup und Recovery ist auf dem System aktiviert. Wenn Sie Volumes auf diesen Cloud Volumes ONTAP Systemen erstellt haben, starten Sie BlueXP Backup und Recovery sowie "Aktivieren Sie die Sicherung auf jedem Volume, das Sie schützen möchten".

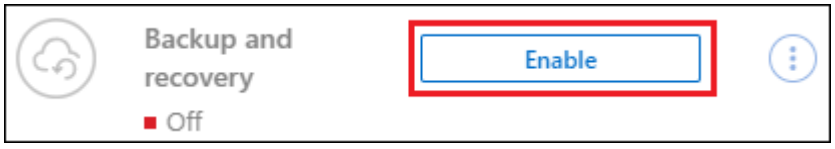
BlueXP Backup und Recovery auf einem vorhandenen System aktivieren

Ermöglichen Sie jederzeit BlueXP Backup und Recovery auf einem vorhandenen System direkt aus der Betriebsumgebung.

Schritte

1. Wählen Sie auf dem BlueXP-Bildschirm die Arbeitsumgebung aus und wählen Sie im rechten Bereich neben dem Backup- und Recovery-Dienst **Enable** aus.

   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.



Informationen zum Ändern von Backup-Einstellungen oder Hinzufügen von Replikationen finden Sie unter "ONTAP-Backups managen".

Aktivieren Sie Backups auf Ihren ONTAP Volumes

Sie können Backups jederzeit direkt aus Ihrer On-Premises-Arbeitsumgebung heraus aktivieren.

Ein Assistent führt Sie durch die folgenden wichtigen Schritte:

- die Sie sichern möchten
- Backup-Strategie definieren
- Überprüfen Sie Ihre Auswahl

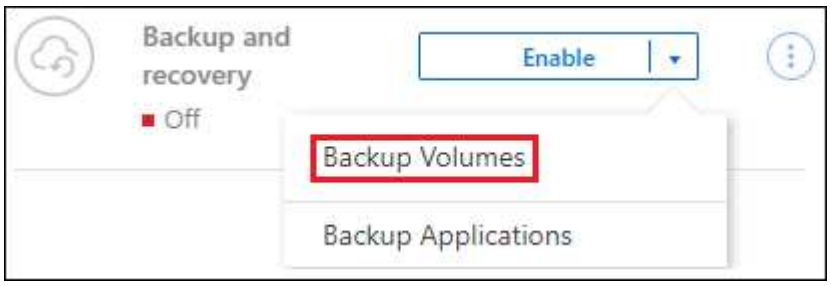
Das können Sie auch Zeigt die API-Befehle an Kopieren Sie im Überprüfungsschritt den Code, um die Backup-Aktivierung für zukünftige Arbeitsumgebungen zu automatisieren.

Starten Sie den Assistenten

Schritte

1. Greifen Sie auf eine der folgenden Arten auf den Assistenten zur Aktivierung von Backup und Recovery zu:

   - Wählen Sie auf dem BlueXP-Bildschirm die Arbeitsumgebung aus, und wählen Sie im rechten Bereich neben dem Sicherungs- und Wiederherstellungsdienst die Option **Enable > Backup Volumes** aus.



     Wenn das AWS Ziel für Ihre Backups als Arbeitsumgebung auf dem Canvas vorhanden ist, können Sie das ONTAP-Cluster auf den AWS Objekt-Storage ziehen.

   - Wählen Sie in der Sicherungs- und Wiederherstellungsleiste **Volumes** aus. Wählen Sie auf der Registerkarte Volumes die Option **actions** aus ••• Icon-Option und wählen Sie **Activate Backup** für ein einzelnes Volume (das noch nicht über Replikation oder Backup auf Objektspeicher bereits aktiviert ist).

   Auf der Seite Einführung des Assistenten werden die Schutzoptionen einschließlich lokaler Snapshots, Replikation und Backups angezeigt. Wenn Sie die zweite Option in diesem Schritt gewählt haben, wird die Seite „Backup-Strategie definieren“ mit einem ausgewählten Volume angezeigt.

2. Fahren Sie mit den folgenden Optionen fort:

   - Wenn Sie bereits einen BlueXP Connector haben, sind Sie fertig. Wählen Sie einfach **Weiter**.
   - Wenn Sie noch keinen BlueXP Connector haben, wird die Option **Connector hinzufügen** angezeigt. Siehe Bereiten Sie Ihren BlueXP Connector vor.

Wählen Sie die Volumes aus, die Sie sichern möchten

Wählen Sie die Volumes aus, die Sie schützen möchten. Ein geschütztes Volume verfügt über eine oder mehrere der folgenden Elemente: Snapshot-Richtlinie, Replizierungsrichtlinie und Richtlinie für das Backup in ein Objekt.

Sie können FlexVol- oder FlexGroup-Volumes schützen. Sie können jedoch keine Kombination dieser Volumes auswählen, wenn Sie Backups für eine funktionierende Umgebung aktivieren. Informieren Sie sich darüber "Aktivieren Sie das Backup für zusätzliche Volumes in der Arbeitsumgebung" (FlexVol oder FlexGroup), nachdem Sie das Backup für die ersten Volumes konfiguriert haben.

- Sie können ein Backup nur auf einem einzelnen FlexGroup Volume gleichzeitig aktivieren.
- Die ausgewählten Volumes müssen dieselbe SnapLock-Einstellung aufweisen. Auf allen Volumes muss SnapLock Enterprise aktiviert oder SnapLock deaktiviert sein.

Schritte

Beachten Sie, dass die Richtlinien, die Sie später auswählen, diese vorhandenen Richtlinien überschreiben, wenn die von Ihnen ausgewählten Volumes bereits Snapshot- oder Replikationsrichtlinien angewendet haben.

1. Wählen Sie auf der Seite Volumes auswählen das Volume oder die Volumes aus, die Sie schützen möchten.
   - Optional können Sie die Zeilen so filtern, dass nur Volumes mit bestimmten Volumentypen, Stilen und mehr angezeigt werden, um die Auswahl zu erleichtern.
   - Nachdem Sie das erste Volume ausgewählt haben, können Sie alle FlexVol Volumes auswählen (FlexGroup Volumes können nur einzeln ausgewählt werden). Um alle vorhandenen FlexVol-Volumes zu sichern, aktivieren Sie zuerst ein Volume und dann das Kontrollkästchen in der Titelzeile. (

).
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume (

).
2. Wählen Sie **Weiter**.

Backup-Strategie definieren

Zur Definition der Backup-Strategie gehören die folgenden Optionen:

- Unabhängig davon, ob Sie eine oder alle Backup-Optionen: Lokale Snapshots, Replikation und Backup-to-Object-Storage möchten
- Der Netapp Architektur Sind
- Lokale Snapshot-Richtlinie
- Replikationsziel und -Richtlinie

Wenn die ausgewählten Volumes andere Snapshot- und Replikationsrichtlinien haben als die in diesem Schritt ausgewählten Richtlinien, werden die vorhandenen Richtlinien überschrieben.

- Backup von Objekt-Storage-Informationen (Provider-, Verschlüsselungs-, Netzwerk-, Backup-Richtlinien- und Exportoptionen)

Schritte

1. Wählen Sie auf der Seite Backup-Strategie definieren eine oder alle der folgenden Optionen aus. Alle drei sind standardmäßig ausgewählt:
   - **Lokale Snapshots**: Wenn Sie eine Replikation oder Sicherung auf Objektspeicher durchführen, müssen lokale Snapshots erstellt werden.
   - **Replikation**: Erstellt replizierte Volumes auf einem anderen ONTAP-Speichersystem.

- **Backup**: Sichert Volumes auf Objektspeicher.

2. **Architektur**: Wenn Sie Replikation und Backup gewählt haben, wählen Sie einen der folgenden Informationsflüsse:
   - **Kaskadierung**: Informationsflüsse vom primären Speichersystem zum sekundären und vom sekundären zum Objektspeicher.
   - **Fan out**: Der Informationsfluss vom primären zum sekundären *und* vom primären zum Objektspeicher.

     Einzelheiten zu diesen Architekturen finden Sie unter "Planen Sie Ihren Weg zum Schutz".

3. **Lokaler Snapshot**: Wählen Sie eine vorhandene Snapshot-Richtlinie aus oder erstellen Sie eine neue.

   Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung des Snapshots finden Sie unter "Erstellen einer Richtlinie".

   Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

   - Geben Sie den Namen der Richtlinie ein.
   - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
   - Wählen Sie **Erstellen**.

4. **Replikation**: Stellen Sie die folgenden Optionen ein:
   - **Replikationsziel**: Wählen Sie die Zielarbeitsumgebung und SVM aus. Wählen Sie optional das Zielaggregat oder die Aggregate und das Präfix oder Suffix aus, die dem Namen des replizierten Volumes hinzugefügt werden sollen.
   - **Replikationsrichtlinie**: Wählen Sie eine vorhandene Replikationsrichtlinie oder erstellen Sie eine.

     Informationen zum Erstellen einer benutzerdefinierten Richtlinie finden Sie unter "Erstellen einer Richtlinie"..

     Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

     - Geben Sie den Namen der Richtlinie ein.
     - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
     - Wählen Sie **Erstellen**.

5. **Backup auf Objekt**: Wenn Sie **Backup** ausgewählt haben, stellen Sie die folgenden Optionen ein:
   - **Anbieter**: Wählen Sie **Amazon Web Services**.
   - **Provider-Einstellungen**: Geben Sie die Provider-Details und die Region ein, in der die Backups gespeichert werden sollen.

     Geben Sie das AWS-Konto ein, das zum Speichern der Backups verwendet wird. 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.

Wählen Sie die Region aus, in der die Backups gespeichert werden sollen. Dies kann eine andere Region sein als der Speicherort des Cloud Volumes ONTAP Systems.

Erstellen Sie entweder einen neuen Bucket, oder wählen Sie einen vorhandenen Bucket aus.

- **Verschlüsselungsschlüssel**: Wenn Sie einen neuen Bucket erstellt haben, geben Sie die Verschlüsselungsschlüsselinformationen ein, die Sie vom Provider erhalten haben. Entscheiden Sie, ob Sie die AWS Standardschlüssel verwenden oder Ihre eigenen vom Kunden gemanagten Schlüssel in Ihrem AWS-Konto auswählen werden, um die Verschlüsselung Ihrer Daten zu managen. ("Nutzen Sie Ihre eigenen Schlüssel").

  Wenn Sie Ihre eigenen vom Kunden verwalteten Schlüssel verwenden möchten, geben Sie den Schlüsselspeicher und die Schlüsselinformationen ein.

  Wenn Sie einen vorhandenen Bucket ausgewählt haben, sind Verschlüsselungsinformationen bereits verfügbar, sodass Sie ihn jetzt nicht mehr eingeben müssen.

- **Backup-Richtlinie**: Wählen Sie eine vorhandene Richtlinie für Backup-to-Object-Storage aus oder erstellen Sie eine.

  Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Sicherung finden Sie unter "Erstellen einer Richtlinie".

  Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

  - Geben Sie den Namen der Richtlinie ein.
  - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
  - Legen Sie für Backup-to-Object-Richtlinien die Einstellungen für DataLock und Ransomware-Schutz fest. Weitere Informationen zu DataLock und Ransomware-Schutz finden Sie unter "Richtlinieneinstellungen für Backup-to-Object".
  - Wählen Sie **Erstellen**.

- **Exportieren vorhandener Snapshot-Kopien als Backup-Kopien in den Objektspeicher**: Wenn es lokale Snapshot-Kopien für Volumes in dieser Arbeitsumgebung gibt, die mit dem Backup-Zeitplan-Label übereinstimmen, das Sie gerade für diese Arbeitsumgebung ausgewählt haben (z. B. täglich, wöchentlich usw.), wird diese zusätzliche Eingabeaufforderung angezeigt. Aktivieren Sie dieses Kontrollkästchen, damit alle historischen Snapshots als Backup-Dateien in den Objektspeicher kopiert werden, um einen möglichst vollständigen Schutz für Ihre Volumes zu gewährleisten.

6. Wählen Sie **Weiter**.

Überprüfen Sie Ihre Auswahl

Dies ist die Möglichkeit, Ihre Auswahl zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

Schritte

1. Überprüfen Sie auf der Seite „Überprüfen“ Ihre Auswahl.
2. Aktivieren Sie optional das Kontrollkästchen, um * die Snapshot-Policy-Labels automatisch mit den Label der Replikations- und Backup-Policy* zu synchronisieren. Dadurch werden Snapshots mit einem Label erstellt, das den Labels in den Replizierungs- und Backup-Richtlinien entspricht.

3. Wählen Sie **Sicherung Aktivieren**.

Ergebnis

Mit BlueXP Backup und Recovery werden erste Backups Ihrer Volumes erstellt. Der Basistransfer des replizierten Volumes und der Backup-Datei beinhaltet eine vollständige Kopie der Daten des primären Storage-Systems. Nachfolgende Transfers enthalten differenzielle Kopien der primären Storage-System-Daten in Snapshot Kopien.

Ein repliziertes Volume wird im Zielcluster erstellt, das mit dem primären Storage Volume synchronisiert wird.

Ein S3-Bucket wird in dem Servicekonto erstellt, das durch den eingegebenen S3-Zugriffsschlüssel und geheimen Schlüssel angegeben ist, und die Backup-Dateien werden dort gespeichert.

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".

Zeigt die API-Befehle an

Möglicherweise möchten Sie die API-Befehle anzeigen und optional kopieren, die im Assistenten Sicherung und Wiederherstellung aktivieren verwendet werden. Dies ist möglicherweise sinnvoll, um die Backup-Aktivierung in zukünftigen Arbeitsumgebungen zu automatisieren.

Schritte

1. Wählen Sie im Assistenten Backup und Recovery aktivieren **API-Anforderung anzeigen** aus.
2. Um die Befehle in die Zwischenablage zu kopieren, wählen Sie das Symbol **Kopieren**.

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 Sie Cloud Volumes ONTAP-Daten mit BlueXP Backup und Recovery im Azure Blob-Speicher

Führen Sie einige Schritte zur Sicherung und Wiederherstellung mit BlueXP durch, um mit der Sicherung von Volumedaten von Ihren Cloud Volumes ONTAP-Systemen in den Azure Blob-Speicher 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 verwenden Cloud Volumes ONTAP 9.8 oder höher in Azure (ONTAP 9.8P13 und höher wird empfohlen).
- 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", Oder Sie haben gekauft "Und aktiviert" Eine BYOL-Lizenz für BlueXP Backup und Recovery von NetApp.

2 **Bereiten Sie Ihren BlueXP Connector vor**

Wenn Sie bereits einen Connector in einer Azure-Region implementiert haben, sind Sie fertig. Falls nicht, müssen Sie einen BlueXP Connector in Azure installieren, um Cloud Volumes ONTAP Daten in Azure Blob Storage zu sichern. Der Connector kann auf einer Website mit vollem Internetzugang ("Standard-Modus") oder mit eingeschränkter Internetverbindung ("eingeschränkter Modus") installiert werden.

Bereiten Sie Ihren BlueXP Connector vor

3 **Lizenzanforderungen prüfen**

Sie müssen die Lizenzanforderungen sowohl für Azure als auch für BlueXP prüfen.

Siehe Lizenzanforderungen prüfen.

4 **Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes**

Stellen Sie sicher, dass die Quell- und Zielsysteme die Anforderungen der ONTAP Version und des Netzwerks erfüllen.

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes.

5 **BlueXP Backup und Recovery ermöglichen**

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

BlueXP Backup und Recovery auf Cloud Volumes ONTAP ermöglichen.

6 **Aktivieren Sie Backups auf Ihren ONTAP Volumes**

Folgen Sie dem Setup-Assistenten, um die Replikations- und Backup-Richtlinien auszuwählen, die Sie verwenden möchten, sowie die Volumes, die Sie sichern möchten.

Aktivieren Sie Backups auf Ihren ONTAP Volumes.

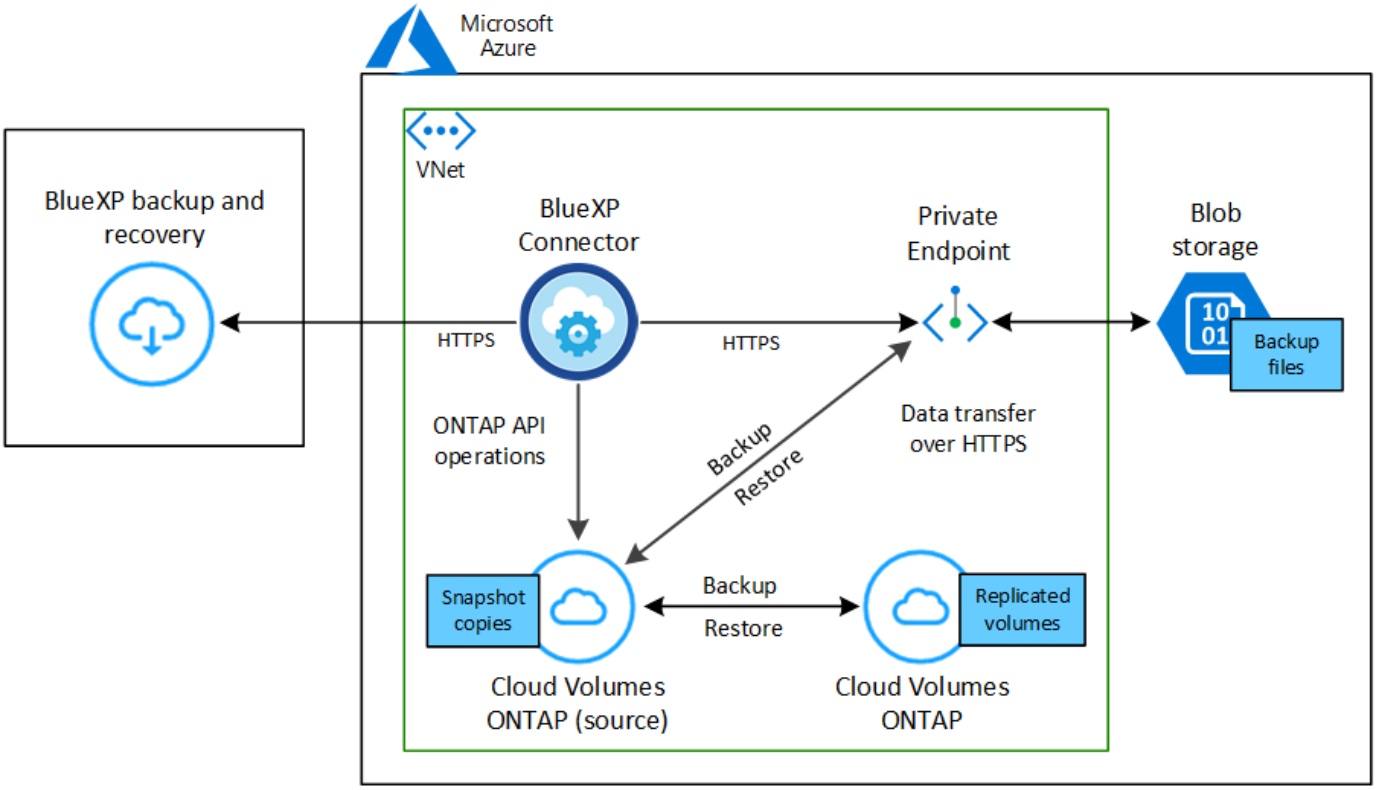
Überprüfen Sie die Unterstützung Ihrer Konfiguration

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration

verfügen, bevor Sie mit dem Backup von Volumes in Azure Blob Storage beginnen.

Die folgende Abbildung zeigt jede Komponente und die Verbindungen, die Sie zwischen ihnen vorbereiten müssen.

Optional können Sie für replizierte Volumes auch eine Verbindung zu einem sekundären ONTAP-System über eine öffentliche oder private Verbindung herstellen.



Unterstützte ONTAP-Versionen

Mindestens ONTAP 9.8; ONTAP 9.8P13 und höher wird empfohlen.

Unterstützte Azure Regionen

Die Sicherung und Wiederherstellung von BlueXP wird in allen Azure-Regionen unterstützt, einschließlich der Azure Government-Regionen.

BlueXP Backup und Recovery stellt den Blob-Container standardmäßig mit lokaler Redundanz (LRS) zur Kostenoptimierung bereit. Sie können diese Einstellung auf Zonenredundanz (ZRS) ändern, nachdem BlueXP Backup und Recovery aktiviert wurde, wenn Sie sicherstellen möchten, dass Ihre Daten zwischen verschiedenen Zonen repliziert werden. Siehe Microsoft-Anweisungen für "Ändern der Replizierung Ihres Storage-Kontos".

Erforderliche Einrichtung zum Erstellen von Backups in einem anderen Azure Abonnement

Standardmäßig werden Backups mit demselben Abonnement erstellt wie das für Ihr Cloud Volumes ONTAP-System verwendete. Wenn Sie ein anderes Azure Abonnement für Ihre Backups verwenden möchten, müssen Sie dies tun "Melden Sie sich beim Azure-Portal an und verlinken Sie die beiden Abonnements".

Lizenzanforderungen prüfen

Für die PAYGO-Lizenzierung für BlueXP Backup und Recovery ist vor der Aktivierung von BlueXP Backup und

Recovery ein Abonnement über den Azure Marketplace erforderlich. Die Abrechnung für BlueXP Backup und Recovery erfolgt über dieses Abonnement. "Sie können sich auf der Seite Details Credentials des Assistenten für die Arbeitsumgebung anmelden".

Für die BYOL-Lizenzierung für BlueXP Backup und Recovery benötigen Sie die Seriennummer von NetApp, anhand derer Sie den Service für die Dauer und Kapazität der Lizenz nutzen können. "Erfahren Sie, wie Sie Ihre BYOL-Lizenzen managen". Sie müssen eine BYOL-Lizenz verwenden, wenn der Connector und das Cloud Volumes ONTAP-System an einem Dark Site („Private Mode“) bereitgestellt werden.

Darüber hinaus benötigen Sie ein Microsoft Azure-Abonnement für den Speicherplatz, auf dem sich Ihre Backups befinden.

Bereiten Sie Ihren BlueXP Connector vor

Der Connector kann in einer Azure-Region mit vollem oder eingeschränktem Internetzugang (Standard- oder eingeschränkter Modus) installiert werden. "Einzelheiten finden Sie in den BlueXP Implementierungsmodi".

- "Erfahren Sie mehr über Steckverbinder"
- "Implementieren eines Connectors in Azure im Standardmodus (vollständiger Internetzugang)"
- "Installieren Sie den Connector im eingeschränkten Modus (eingeschränkter Zugriff für ausgehende Verbindungen)."

Überprüfen oder Hinzufügen von Berechtigungen zum Konnektor

Um die Such- und Wiederherstellungsfunktion für BlueXP Backup und Recovery verwenden zu können, müssen Sie in der Rolle für den Connector über bestimmte Berechtigungen verfügen, damit dieser auf den Azure Synapse Workspace und das Data Lake Storage Account zugreifen kann. Lesen Sie die unten stehenden Berechtigungen, und befolgen Sie die Schritte, wenn Sie die Richtlinie ändern müssen.

Bevor Sie beginnen

- Sie müssen den Azure Synapse Analytics Resource Provider (genannt „Microsoft.Synapse“) im Abonnement registrieren. "Erfahren Sie, wie Sie diesen Ressourcenanbieter für Ihr Abonnement registrieren". Sie müssen der Subscription **Owner** oder **Contributor** sein, um den Ressourcenanbieter zu registrieren.
- Port 1433 muss für die Kommunikation zwischen dem Connector und den Azure Synapse SQL-Diensten offen sein.

Schritte

1. Identifizieren Sie die Rolle, die der virtuellen Konnektor-Maschine zugewiesen ist:
   a. Öffnen Sie im Azure-Portal den Service für Virtual Machines.
   b. Wählen Sie die virtuelle Verbindungsmaschine aus.
   c. Wählen Sie unter Einstellungen **Identität** aus.
   d. Wählen Sie **Azure-Rollenzuweisungen** aus.
   e. Notieren Sie sich die benutzerdefinierte Rolle, die der virtuellen Connector-Maschine zugewiesen ist.
2. Aktualisieren der benutzerdefinierten Rolle:
   a. Öffnen Sie im Azure-Portal Ihr Azure-Abonnement.
   b. Wählen Sie **Zugriffskontrolle (IAM) > Rollen**.
   c. Wählen Sie die Auslassungspunkte (**…**) für die benutzerdefinierte Rolle aus und wählen Sie dann **Bearbeiten**.

d. Wählen Sie **JSON** und fügen Sie die folgenden Berechtigungen hinzu:

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"Zeigen Sie das vollständige JSON-Format für die Richtlinie an"

e. Klicken Sie auf **Review + Update** und dann auf **Update**.

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

Sie können im Aktivierungsassistenten Ihre eigenen, vom Kunden gemanagten Schlüssel für die Datenverschlüsselung verwenden, anstatt die von Microsoft verwalteten Standardschlüssel zu verwenden. In diesem Fall benötigen Sie das Azure-Abonnement, den Key Vault-Namen und den Key. "Sehen Sie, wie Sie Ihre eigenen Schlüssel verwenden".

BlueXP Backup und Recovery unterstützt *Azure Access Policies*, das *Azure Role-Based Access Control* (Azure RBAC) Berechtigungsmodell und das *Managed Hardware Security Model* (HSM) (siehe "Was ist ein von Azure Key Vault gemanagter HSM?").

Erstellen Sie Ihr Azure Blob Storage-Konto

Standardmäßig erstellt der Service Storage-Konten für Sie. Wenn Sie Ihre eigenen Speicherkonten verwenden möchten, können Sie diese erstellen, bevor Sie den Assistenten für die Backup-Aktivierung starten und dann diese Speicherkonten im Assistenten auswählen.

"Erfahren Sie mehr über das Erstellen Ihrer eigenen Storage-Konten".

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes

Wenn Sie planen, mithilfe von BlueXP Backup und Recovery replizierte Volumes auf einem sekundären ONTAP System zu erstellen, stellen Sie sicher, dass die Quell- und Zielsysteme die folgenden Netzwerkanforderungen erfüllen.

Netzwerkanforderungen für On-Premises-ONTAP

- Wenn sich der Cluster an Ihrem Standort befindet, sollten Sie über eine Verbindung zwischen Ihrem Unternehmensnetzwerk und Ihrem virtuellen Netzwerk des Cloud-Providers verfügen. Hierbei handelt es sich in der Regel um eine VPN-Verbindung.
- ONTAP Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Cluster-Anforderungen erfüllen.

  Da Sie Daten auf Cloud Volumes ONTAP oder auf lokale Systeme replizieren können, prüfen Sie Peering-Anforderungen für lokale ONTAP Systeme. "Anzeigen von Voraussetzungen für Cluster-Peering in der ONTAP-Dokumentation".

Netzwerkanforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen ein- und ausgehenden Regeln enthalten: Speziell Regeln für ICMP und die Ports 11104 und 11105. Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.
- Um Daten zwischen zwei Cloud Volumes ONTAP Systemen in verschiedenen Subnetzen zu replizieren, müssen die Subnetze gemeinsam geroutet werden (dies ist die Standardeinstellung).

BlueXP Backup und Recovery auf Cloud Volumes ONTAP ermöglichen

Die Aktivierung von BlueXP Backup und Recovery ist einfach. Die Schritte unterscheiden sich leicht, je nachdem, ob Sie ein bestehendes oder ein neues Cloud Volumes ONTAP-System besitzen.

BlueXP Backup und Recovery auf einem neuen System aktivieren

BlueXP Backup und Recovery sind standardmäßig im Assistenten für die Arbeitsumgebung aktiviert. Achten Sie darauf, dass die Option aktiviert bleibt.

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

> Wenn Sie den Namen der Ressourcengruppe auswählen möchten, deaktivieren Sie bei der Bereitstellung von Cloud Volumes ONTAP BlueXP Backup und Recovery. Befolgen Sie die Schritte für Aktivieren von BlueXP Backup und Recovery auf einem vorhandenen System Um das Backup und Recovery von BlueXP zu aktivieren und die Ressourcengruppe auszuwählen.

Schritte

1. Wählen Sie im BlueXP-Bildschirm **Arbeitsumgebung hinzufügen**, wählen Sie den Cloud-Provider aus und wählen Sie **Neu hinzufügen**. Wählen Sie **Cloud Volumes ONTAP erstellen**.
2. Wählen Sie **Microsoft Azure** als Cloud-Provider aus und wählen Sie dann einen einzelnen Knoten oder ein HA-System aus.
3. Geben Sie auf der Seite Azure Credentials definieren den Namen, die Client-ID, den Clientschlüssel und die Verzeichnis-ID ein, und klicken Sie auf **Weiter**.
4. Füllen Sie die Seite „Details & Zugangsdaten“ aus und stellen Sie sicher, dass ein Azure Marketplace-Abonnement besteht, und klicken Sie auf **Weiter**.
5. Lassen Sie auf der Seite Dienste den Dienst aktiviert, und klicken Sie auf **Weiter**.

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

Ergebnis

BlueXP Backup und Recovery ist auf dem System aktiviert. Wenn Sie Volumes auf diesen Cloud Volumes ONTAP Systemen erstellt haben, starten Sie BlueXP Backup und Recovery sowie "Aktivieren Sie die Sicherung auf jedem Volume, das Sie schützen möchten".

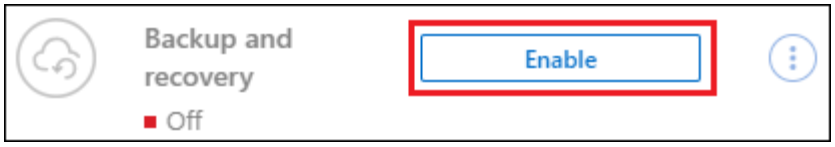
BlueXP Backup und Recovery auf einem vorhandenen System aktivieren

BlueXP Backup und Recovery sind jederzeit möglich – direkt aus der Arbeitsumgebung.

Schritte

1. Wählen Sie auf dem BlueXP-Bildschirm die Arbeitsumgebung aus und wählen Sie im rechten Bereich neben dem Backup- und Recovery-Dienst **Enable** aus.

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



2. Füllen Sie die Seiten im Assistenten zur Implementierung von BlueXP Backup und Recovery aus.
3. Wenn Sie Backups initiieren möchten, fahren Sie mit fort Aktivieren Sie Backups auf Ihren ONTAP Volumes.

Aktivieren Sie Backups auf Ihren ONTAP Volumes

Sie können Backups jederzeit direkt aus Ihrer On-Premises-Arbeitsumgebung heraus aktivieren.

Ein Assistent führt Sie durch die folgenden wichtigen Schritte:

- die Sie sichern möchten
- Backup-Strategie definieren
- Überprüfen Sie Ihre Auswahl

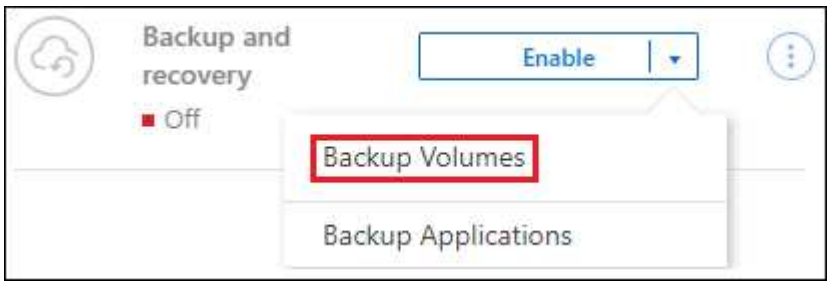
Das können Sie auch Zeigt die API-Befehle an Kopieren Sie im Überprüfungsschritt den Code, um die Backup-Aktivierung für zukünftige Arbeitsumgebungen zu automatisieren.

Starten Sie den Assistenten

Schritte

1. Greifen Sie auf eine der folgenden Arten auf den Assistenten zur Aktivierung von Backup und Recovery zu:

   - Wählen Sie auf dem BlueXP-Bildschirm die Arbeitsumgebung aus, und wählen Sie im rechten Bereich neben dem Sicherungs- und Wiederherstellungsdienst die Option **Enable > Backup Volumes** aus.



     Wenn das Azure-Ziel für Ihre Backups als Arbeitsumgebung auf dem Canvas vorhanden ist, können Sie das ONTAP-Cluster auf den Azure Blob-Objekt-Storage ziehen.

   - Wählen Sie in der Sicherungs- und Wiederherstellungsleiste **Volumes** aus. Wählen Sie auf der Registerkarte Volumes die Option **actions** aus ••• Und wählen Sie **Backup aktivieren** für ein einzelnes Volume (das noch nicht über Replikation oder Backup auf Objektspeicher verfügt).

   Auf der Seite Einführung des Assistenten werden die Schutzoptionen einschließlich lokaler Snapshots, Replikation und Backups angezeigt. Wenn Sie die zweite Option in diesem Schritt gewählt haben, wird die Seite „Backup-Strategie definieren“ mit einem ausgewählten Volume angezeigt.

2. Fahren Sie mit den folgenden Optionen fort:

   - Wenn Sie bereits einen BlueXP Connector haben, sind Sie fertig. Wählen Sie einfach **Weiter**.

- Wenn Sie noch keinen BlueXP Connector haben, wird die Option **Connector hinzufügen** angezeigt. Siehe Bereiten Sie Ihren BlueXP Connector vor.

Wählen Sie die Volumes aus, die Sie sichern möchten

Wählen Sie die Volumes aus, die Sie schützen möchten. Ein geschütztes Volume verfügt über eine oder mehrere der folgenden Elemente: Snapshot-Richtlinie, Replizierungsrichtlinie und Backup-to-Object-Richtlinie.

Sie können FlexVol- oder FlexGroup-Volumes schützen. Sie können jedoch keine Kombination dieser Volumes auswählen, wenn Sie Backups für eine funktionierende Umgebung aktivieren. Informieren Sie sich darüber "Aktivieren Sie das Backup für zusätzliche Volumes in der Arbeitsumgebung" (FlexVol oder FlexGroup), nachdem Sie das Backup für die ersten Volumes konfiguriert haben.

- Sie können ein Backup nur auf einem einzelnen FlexGroup Volume gleichzeitig aktivieren.
- Die ausgewählten Volumes müssen dieselbe SnapLock-Einstellung aufweisen. Auf allen Volumes muss SnapLock Enterprise aktiviert oder SnapLock deaktiviert sein.

Schritte

Beachten Sie, dass die Richtlinien, die Sie später auswählen, diese vorhandenen Richtlinien überschreiben, wenn die von Ihnen ausgewählten Volumes bereits Snapshot- oder Replikationsrichtlinien angewendet haben.

1. Wählen Sie auf der Seite Volumes auswählen das Volume oder die Volumes aus, die Sie schützen möchten.
   - Optional können Sie die Zeilen so filtern, dass nur Volumes mit bestimmten Volumentypen, Stilen und mehr angezeigt werden, um die Auswahl zu erleichtern.
   - Nachdem Sie das erste Volume ausgewählt haben, können Sie alle FlexVol-Volumes auswählen. (FlexGroup Volumes können nur einzeln ausgewählt werden.) Um alle vorhandenen FlexVol-Volumes zu sichern, aktivieren Sie zuerst ein Volume und dann das Kontrollkästchen in der Titelzeile. (

).
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume (

).
2. Wählen Sie **Weiter**.

Backup-Strategie definieren

Zur Definition der Backup-Strategie gehören die folgenden Optionen:

- Unabhängig davon, ob Sie eine oder alle Backup-Optionen: Lokale Snapshots, Replikation und Backup-to-Object-Storage möchten
- Der Netapp Architektur Sind
- Lokale Snapshot-Richtlinie
- Replikationsziel und -Richtlinie

Wenn die ausgewählten Volumes andere Snapshot- und Replikationsrichtlinien haben als die in diesem Schritt ausgewählten Richtlinien, werden die vorhandenen Richtlinien überschrieben.

- Backup von Objekt-Storage-Informationen (Provider-, Verschlüsselungs-, Netzwerk-, Backup-Richtlinien- und Exportoptionen)

Schritte

1. Wählen Sie auf der Seite Backup-Strategie definieren eine oder alle der folgenden Optionen aus. Alle drei sind standardmäßig ausgewählt:
   - **Lokale Snapshots**: Wenn Sie eine Replikation oder Sicherung auf Objektspeicher durchführen, müssen lokale Snapshots erstellt werden.
   - **Replikation**: Erstellt replizierte Volumes auf einem anderen ONTAP-Speichersystem.
   - **Backup**: Sichert Volumes auf Objektspeicher.
2. **Architektur**: Wenn Sie Replikation und Backup gewählt haben, wählen Sie einen der folgenden Informationsflüsse:
   - **Kaskadierung**: Informationsflüsse vom primären Speichersystem zum sekundären und vom sekundären zum Objektspeicher.
   - **Fan out**: Der Informationsfluss vom primären zum sekundären *und* vom primären zum Objektspeicher.

     Einzelheiten zu diesen Architekturen finden Sie unter "Planen Sie Ihren Weg zum Schutz".
3. **Lokaler Snapshot**: Wählen Sie eine vorhandene Snapshot-Richtlinie aus oder erstellen Sie eine.

   Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung des Snapshots finden Sie unter "Erstellen einer Richtlinie".

   Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:
   - Geben Sie den Namen der Richtlinie ein.
   - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
   - Wählen Sie **Erstellen**.
4. **Replikation**: Stellen Sie die folgenden Optionen ein:
   - **Replikationsziel**: Wählen Sie die Zielarbeitsumgebung und SVM aus. Wählen Sie optional das Zielaggregat oder die Aggregate und das Präfix oder Suffix aus, die dem Namen des replizierten Volumes hinzugefügt werden sollen.
   - **Replikationsrichtlinie**: Wählen Sie eine vorhandene Replikationsrichtlinie oder erstellen Sie eine.

     Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Replikation finden Sie unter "Erstellen einer Richtlinie".

     Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:
     - Geben Sie den Namen der Richtlinie ein.
     - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
     - Wählen Sie **Erstellen**.
5. **Backup auf Objekt**: Wenn Sie **Backup** ausgewählt haben, stellen Sie die folgenden Optionen ein:
   - **Provider**: Wählen Sie **Microsoft Azure**.
   - **Provider-Einstellungen**: Geben Sie die Provider-Details ein.

     Geben Sie den Bereich ein, in dem die Backups gespeichert werden sollen. Dies kann eine andere

Region sein als der Speicherort des Cloud Volumes ONTAP Systems.

Erstellen Sie entweder ein neues Storage-Konto oder wählen Sie ein vorhandenes aus.

Geben Sie das zum Speichern der Backups verwendete Azure-Abonnement ein. Dabei kann es sich um ein anderes Abonnement als um das Cloud Volumes ONTAP-System handelt. Wenn Sie ein anderes Azure Abonnement für Ihre Backups verwenden möchten, müssen Sie dies tun "Melden Sie sich beim Azure-Portal an und verlinken Sie die beiden Abonnements".

Erstellen Sie entweder Ihre eigene Ressourcengruppe, die den Blob-Container verwaltet, oder wählen Sie den Typ und die Gruppe der Ressourcengruppe aus.

Wenn Sie Ihre Backup-Dateien vor Änderung oder Löschung schützen möchten, stellen Sie sicher, dass das Storage-Konto mit aktiviertem unveränderlichem Storage erstellt wurde und eine Aufbewahrungsfrist von 30 Tagen verwendet wird.

Wenn Sie zur weiteren Kostenoptimierung ältere Backup-Dateien in Azure Archivspeicher verschieben möchten, stellen Sie sicher, dass das Speicherkonto über die entsprechende Lebenszyklusregel verfügt.

- **Verschlüsselungsschlüssel**: Wenn Sie ein neues Azure-Speicherkonto erstellt haben, geben Sie die Schlüsselinformationen des Verschlüsselungsschlüssels ein, die Sie vom Provider erhalten haben. Wählen Sie aus, ob Sie die Azure Standardschlüssel verwenden oder Ihre eigenen vom Kunden verwalteten Schlüssel aus Ihrem Azure Konto auswählen werden, um die Verschlüsselung Ihrer Daten zu managen.

  Wenn Sie Ihre eigenen vom Kunden verwalteten Schlüssel verwenden möchten, geben Sie den Schlüsselspeicher und die Schlüsselinformationen ein. "Erfahren Sie, wie Sie Ihre eigenen Schlüssel verwenden".

  Wenn Sie ein vorhandenes Microsoft Storage-Konto ausgewählt haben, sind Verschlüsselungsinformationen bereits verfügbar. Sie müssen es daher jetzt nicht eingeben.

- **Netzwerk**: Wählen Sie den IPspace und ob Sie einen privaten Endpunkt verwenden. Der private Endpunkt ist standardmäßig deaktiviert.

  i. 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.

  ii. Wählen Sie optional aus, ob Sie einen zuvor konfigurierten privaten Azure-Endpunkt verwenden möchten. "Informieren Sie sich über die Verwendung eines privaten Azure Endpunkts".

- **Backup-Richtlinie**: Wählen Sie eine vorhandene Richtlinie für Backup-to-Object-Storage aus.

  Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Sicherung finden Sie unter "Erstellen einer Richtlinie".

  Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

  - Geben Sie den Namen der Richtlinie ein.
  - Legen Sie für Backup-to-Object-Richtlinien die Einstellungen für DataLock und Ransomware-Schutz fest. Weitere Informationen zu DataLock und Ransomware-Schutz finden Sie unter

"Richtlinieneinstellungen für Backup-to-Object".

- Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
- Wählen Sie **Erstellen**.

◦ **Exportieren vorhandener Snapshot-Kopien als Backup-Kopien in den Objektspeicher**: Wenn es lokale Snapshot-Kopien für Volumes in dieser Arbeitsumgebung gibt, die mit dem Backup-Zeitplan-Label übereinstimmen, das Sie gerade für diese Arbeitsumgebung ausgewählt haben (z. B. täglich, wöchentlich usw.), wird diese zusätzliche Eingabeaufforderung angezeigt. Aktivieren Sie dieses Kontrollkästchen, damit alle historischen Snapshots als Backup-Dateien in den Objektspeicher kopiert werden, um einen möglichst vollständigen Schutz für Ihre Volumes zu gewährleisten.

6. Wählen Sie **Weiter**.

Überprüfen Sie Ihre Auswahl

Dies ist die Möglichkeit, Ihre Auswahl zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

Schritte

1. Überprüfen Sie auf der Seite „Überprüfen“ Ihre Auswahl.
2. Aktivieren Sie optional das Kontrollkästchen, um * die Snapshot-Policy-Labels automatisch mit den Label der Replikations- und Backup-Policy* zu synchronisieren. Dadurch werden Snapshots mit einem Label erstellt, das den Labels in den Replizierungs- und Backup-Richtlinien entspricht.
3. Wählen Sie **Sicherung Aktivieren**.

Ergebnis

Mit BlueXP Backup und Recovery werden erste Backups Ihrer Volumes erstellt. Der Basistransfer des replizierten Volumes und der Backup-Datei beinhaltet eine vollständige Kopie der Daten des primären Storage-Systems. Nachfolgende Transfers enthalten differenzielle Kopien der primären Storage-Daten, die in Snapshot Kopien enthalten sind.

Ein repliziertes Volume wird im Zielcluster erstellt, das mit dem primären Volume synchronisiert wird.

In der von Ihnen eingegebenen Ressourcengruppe wird ein Blob-Speicher-Container erstellt und die Backup-Dateien dort gespeichert.

BlueXP Backup und Recovery stellt den Blob-Container standardmäßig mit lokaler Redundanz (LRS) zur Kostenoptimierung bereit. Sie können diese Einstellung auf Zoneredundanz (ZRS) ändern, wenn Sie sicherstellen möchten, dass Ihre Daten zwischen verschiedenen Zonen repliziert werden. Siehe Microsoft-Anweisungen für "Ändern der Replizierung Ihres Storage-Kontos".

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".

Zeigt die API-Befehle an

Möglicherweise möchten Sie die API-Befehle anzeigen und optional kopieren, die im Assistenten Sicherung und Wiederherstellung aktivieren verwendet werden. Dies ist möglicherweise sinnvoll, um die Backup-Aktivierung in zukünftigen Arbeitsumgebungen zu automatisieren.

Schritte

1. Wählen Sie im Assistenten Backup und Recovery aktivieren **API-Anforderung anzeigen** aus.

2. Um die Befehle in die Zwischenablage zu kopieren, wählen Sie das Symbol **Kopieren**.

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 unter anderem die Änderung der verfügbaren Netzwerkbandbreite für das Hochladen von Backups in den Objekt-Storage, die Änderung der automatischen Backup-Einstellung für zukünftige Volumes.
- Das können Sie auch "Wiederherstellung von Volumes, Ordnern oder einzelnen Dateien aus einer Sicherungsdatei" Zu einem Cloud Volumes ONTAP System in Azure oder zu einem ONTAP System vor Ort.

Sichern Sie Cloud Volumes ONTAP-Daten mit BlueXP Backup und Recovery in Google Cloud Storage

Führen Sie einige Schritte zur Sicherung und Wiederherstellung mit BlueXP durch, um mit der Sicherung von Volume-Daten von Ihren Cloud Volumes ONTAP-Systemen in Google Cloud Storage 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 verwenden Cloud Volumes ONTAP 9.8 oder höher in GCP (ONTAP 9.8P13 und höher wird empfohlen).
- Sie verfügen über ein gültiges GCP-Abonnement für den Speicherplatz, in dem sich Ihre Backups befinden.
- Sie haben ein Servicekonto in Ihrem Google Cloud Project, das eine benutzerdefinierte Rolle mit reduzierten Berechtigungen hat.

  Die Storage-Administratorrolle ist für das Servicekonto nicht mehr erforderlich, über das BlueXP Backup und Recovery für den Zugriff auf Google Cloud Storage Buckets ermöglicht werden.

- Sie haben sich für das angemeldet "BlueXP Marketplace Backup-Angebot", Oder Sie haben gekauft "Und aktiviert" Eine BYOL-Lizenz für BlueXP Backup und Recovery von NetApp.

2 Bereiten Sie Ihren BlueXP Connector vor

Wenn Sie bereits einen Connector in einer GCP-Region bereitgestellt haben, sind Sie fertig. Falls nicht, müssen Sie einen BlueXP Connector in GCP installieren, um Cloud Volumes ONTAP Daten in Google Cloud Storage zu sichern. Der Connector kann auf einer Website mit vollem Internetzugang ("Standard-Modus") oder mit eingeschränkter Internetverbindung ("eingeschränkter Modus") installiert werden.

3 Lizenzanforderungen prüfen

Prüfen Sie die Lizenzanforderungen sowohl für Google Cloud als auch für BlueXP.

4 Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes

Stellen Sie sicher, dass die Quell- und Zielsysteme die Anforderungen der ONTAP Version und des Netzwerks erfüllen.

5 BlueXP Backup und Recovery ermöglichen

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

6 Google Cloud als Backup-Ziel vorbereiten

Richten Sie Berechtigungen für den Connector ein, um den Google Cloud-Bucket zu erstellen und zu managen.

Optional können Sie für die Datenverschlüsselung eigene benutzerdefinierte gemanagte Schlüssel einrichten, ohne die Standardschlüssel von Google Cloud zu verwenden. Erfahren Sie, wie Sie Ihre Google Cloud-Umgebung für ONTAP-Backups vorbereiten.

7 Aktivieren Sie Backups auf Ihren ONTAP Volumes

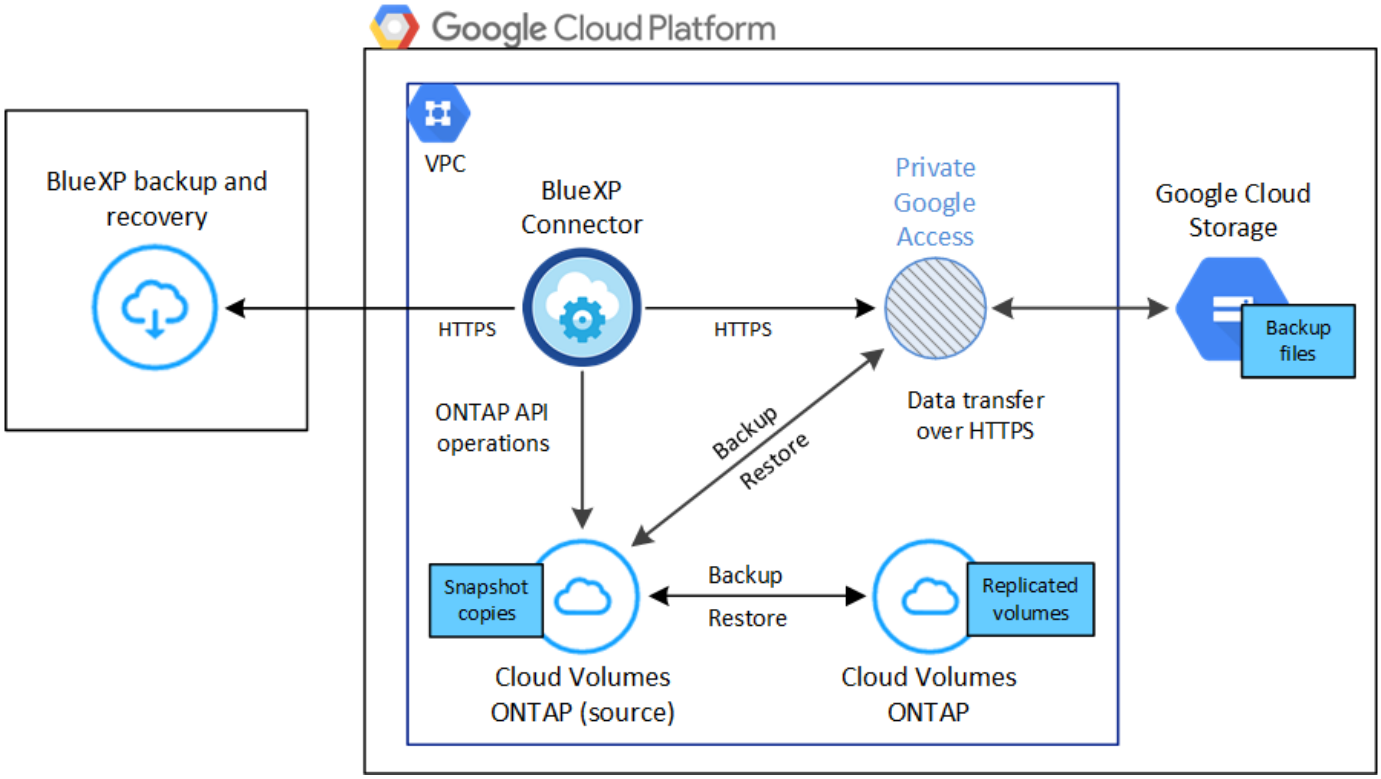
Folgen Sie dem Setup-Assistenten, um die Replikations- und Backup-Richtlinien auszuwählen, die Sie verwenden möchten, sowie die Volumes, die Sie sichern möchten.

Überprüfen Sie die Unterstützung Ihrer Konfiguration

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass eine unterstützte Konfiguration vorhanden ist, bevor Sie Volumes in Google Cloud Storage sichern.

Die folgende Abbildung zeigt jede Komponente und die Verbindungen, die Sie zwischen ihnen vorbereiten müssen.

Optional können Sie für replizierte Volumes auch eine Verbindung zu einem sekundären ONTAP-System über eine öffentliche oder private Verbindung herstellen.



Unterstützte ONTAP-Versionen

Mindestens ONTAP 9.8; ONTAP 9.8P13 und höher wird empfohlen.

Unterstützte GCP-Regionen

BlueXP-Sicherung und -Wiederherstellung wird in allen GCP-Regionen unterstützt.

GCP-Service-Konto

Sie benötigen ein Servicekonto in Ihrem Google Cloud Project, das die benutzerdefinierte Rolle hat. "Erfahren Sie, wie Sie ein Servicekonto erstellen"

Die Storage-Administratorrolle ist für das Servicekonto nicht mehr erforderlich, über das BlueXP Backup und Recovery für den Zugriff auf Google Cloud Storage Buckets ermöglicht werden.

Lizenzanforderungen prüfen

Für die PAYGO-Lizenzierung für BlueXP Backup und Recovery ist im Google Marketplace ein BlueXP Abonnement verfügbar, das die Implementierung von Cloud Volumes ONTAP und BlueXP Backup und Recovery ermöglicht. Sie müssen "Melden Sie sich für dieses BlueXP-Abonnement an" Bevor Sie BlueXP Backup und Recovery aktivieren, Die Abrechnung für BlueXP Backup und Recovery erfolgt über dieses Abonnement. "Sie können sich auf der Seite Details Credentials des Assistenten für die Arbeitsumgebung anmelden".

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

Und Sie benötigen ein Google-Abonnement für den Speicherplatz, in dem Ihre Backups zu finden sind.

Bereiten Sie Ihren BlueXP Connector vor

Der Connector muss in einer Google-Region mit Internetzugang installiert werden.

- "Erfahren Sie mehr über Steckverbinder"
- "Implementieren Sie einen Connector in Google Cloud"

Überprüfen oder Hinzufügen von Berechtigungen zum Konnektor

Um die „Suchen & Wiederherstellen“-Funktion von BlueXP für Backup und Recovery nutzen zu können, müssen Sie in der Rolle für den Connector bestimmte Berechtigungen besitzen, damit dieser auf den Google Cloud BigQuery Service zugreifen kann. Lesen Sie die unten stehenden Berechtigungen, und befolgen Sie die Schritte, wenn Sie die Richtlinie ändern müssen.

Schritte

1. Im "Google Cloud Console", Gehen Sie zur Seite **Rollen**.
2. Wählen Sie in der Dropdown-Liste oben auf der Seite das Projekt oder die Organisation aus, das die Rolle enthält, die Sie bearbeiten möchten.
3. Wählen Sie eine benutzerdefinierte Rolle aus.
4. Wählen Sie **Rolle bearbeiten**, um die Berechtigungen der Rolle zu aktualisieren.
5. Wählen Sie **Berechtigungen hinzufügen**, um der Rolle die folgenden neuen Berechtigungen hinzuzufügen.

```
bigquery.jobs.get
bigquery.jobs.list
bigquery.jobs.listAll
bigquery.datasets.create
bigquery.datasets.get
bigquery.jobs.create
bigquery.tables.get
bigquery.tables.getData
bigquery.tables.list
bigquery.tables.create
```

6. Wählen Sie **Update**, um die bearbeitete Rolle zu speichern.

Erforderliche Informationen zur Nutzung von vom Kunden gemanagten Verschlüsselungsschlüsseln (CMEK)

Sie können Ihre eigenen, von Kunden gemanagten Schlüssel zur Datenverschlüsselung verwenden, statt die von Google standardmäßig gemanagten Verschlüsselungsschlüssel zu verwenden. Sowohl regionsübergreifende als auch projektübergreifende Schlüssel werden unterstützt, sodass Sie ein Projekt für einen Bucket auswählen können, der sich vom Projekt des CMEK-Schlüssels unterscheidet. Wenn Sie planen, Ihre eigenen kundenverwalteten Schlüssel zu verwenden:

- Sie benötigen den Schlüsselring und den Schlüsselnamen, damit Sie diese Informationen im Aktivierungsassistenten hinzufügen können. "Erfahren Sie mehr über vom Kunden verwaltete Verschlüsselungsschlüssel".

- Sie müssen überprüfen, ob diese erforderlichen Berechtigungen in der Rolle für den Connector enthalten sind:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Sie müssen überprüfen, ob die Google API „Cloud Key Management Service (KMS)“ in Ihrem Projekt aktiviert ist. Siehe "Google Cloud-Dokumentation: Aktivieren von APIs" Entsprechende Details.

CMEK-Überlegungen:

- Sowohl HSM (Hardware-unterstützt) als auch Software-generierte Schlüssel werden unterstützt.
- Es werden sowohl neu erstellte als auch importierte Cloud KMS-Schlüssel unterstützt.
- Es werden nur regionale Schlüssel unterstützt, globale Schlüssel werden nicht unterstützt.
- Derzeit wird nur der Zweck „symmetrische Verschlüsselung/Entschlüsselung“ unterstützt.
- Der dem Storage-Konto zugeordnete Service-Agent wird der IAM-Rolle „CryptoKey Encrypter/Decrypter (Rollen/Cloudkms.cryptoKeyEncrypterDecrypter)“ von BlueXP Backup und Recovery zugewiesen.

Erstellen Sie Ihre eigenen Buckets

Standardmäßig erstellt der Service Buckets für Sie. Wenn Sie Ihre eigenen Buckets verwenden möchten, können Sie diese erstellen, bevor Sie den Assistenten für die Backup-Aktivierung starten und diese Buckets dann im Assistenten auswählen.

"Erfahren Sie mehr über das Erstellen eigener Buckets".

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes

Wenn Sie planen, mithilfe von BlueXP Backup und Recovery replizierte Volumes auf einem sekundären ONTAP System zu erstellen, stellen Sie sicher, dass die Quell- und Zielsysteme die folgenden Netzwerkanforderungen erfüllen.

Netzwerkanforderungen für On-Premises-ONTAP

- Wenn sich der Cluster an Ihrem Standort befindet, sollten Sie über eine Verbindung zwischen Ihrem Unternehmensnetzwerk und Ihrem virtuellen Netzwerk des Cloud-Providers verfügen. Hierbei handelt es sich in der Regel um eine VPN-Verbindung.
- ONTAP Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Cluster-Anforderungen erfüllen.

  Da Sie Daten auf Cloud Volumes ONTAP oder auf lokale Systeme replizieren können, prüfen Sie Peering-Anforderungen für lokale ONTAP Systeme. "Anzeigen von Voraussetzungen für Cluster-Peering in der ONTAP-Dokumentation".

- Die Sicherheitsgruppe der Instanz muss die erforderlichen ein- und ausgehenden Regeln enthalten: Speziell Regeln für ICMP und die Ports 11104 und 11105. Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.
- Um Daten zwischen zwei Cloud Volumes ONTAP Systemen in verschiedenen Subnetzen zu replizieren, müssen die Subnetze gemeinsam geroutet werden (dies ist die Standardeinstellung).

BlueXP Backup und Recovery auf Cloud Volumes ONTAP ermöglichen

Die Aktivierung von BlueXP Backup und Recovery ist einfach. Die Schritte unterscheiden sich leicht, je nachdem, ob Sie ein bestehendes oder ein neues Cloud Volumes ONTAP-System besitzen.

BlueXP Backup und Recovery auf einem neuen System aktivieren

BlueXP Backup und Recovery können aktiviert werden, sobald Sie den Arbeitsumgebungs-Assistenten abgeschlossen haben, um ein neues Cloud Volumes ONTAP System zu erstellen.

Sie müssen bereits ein Servicekonto konfiguriert haben. Wenn Sie beim Erstellen des Cloud Volumes ONTAP Systems kein Service-Konto auswählen, müssen Sie das System deaktivieren und das Service-Konto über die GCP-Konsole zu Cloud Volumes ONTAP hinzufügen.

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

Schritte

1. Wählen Sie im BlueXP-Bildschirm **Arbeitsumgebung hinzufügen**, wählen Sie den Cloud-Provider aus und wählen Sie **Neu hinzufügen**. Wählen Sie **Cloud Volumes ONTAP erstellen**.
2. **Wählen Sie einen Standort**: Wählen Sie **Google Cloud Platform**.
3. **Typ** wählen: Wählen Sie **Cloud Volumes ONTAP** (entweder Single-Node oder Hochverfügbarkeit).
4. **Details & Anmeldeinformationen**: Geben Sie die folgenden Informationen ein:

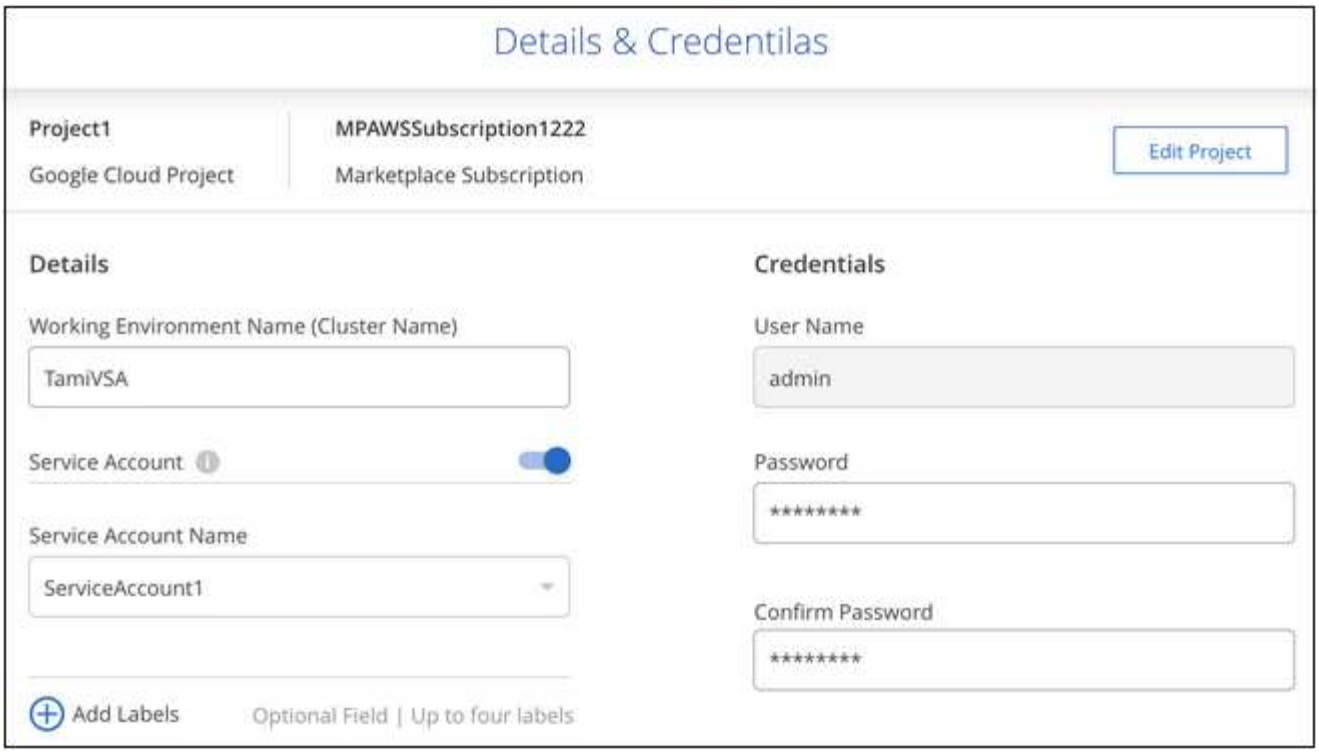
    a. Klicken Sie auf **Projekt bearbeiten** und wählen Sie ein neues Projekt aus, wenn sich das Projekt, das Sie verwenden möchten, von dem Standardprojekt unterscheidet (in dem sich der Connector befindet).

    b. Geben Sie den Cluster-Namen an.

    c. Aktivieren Sie den Schalter **Service Account** und wählen Sie das Servicekonto aus, das über die vordefinierte Rolle Storage Admin verfügt. Dies ist für die Aktivierung von Backups und Tiering erforderlich.

    d. Geben Sie die Anmeldeinformationen an.

    Stellen Sie sicher, dass ein GCP Marketplace Abonnement besteht.



5. **Services**: Lassen Sie den BlueXP Backup- und Recovery-Service aktiviert und klicken Sie auf **Weiter**.

6. Führen Sie die Seiten im Assistenten aus, um das System bereitzustellen, wie in beschrieben "Einführung von Cloud Volumes ONTAP in GCP".

Informationen zum Ändern von Backup-Einstellungen oder Hinzufügen von Replikationen finden Sie unter "ONTAP-Backups managen".

Ergebnis

BlueXP Backup und Recovery ist auf dem System aktiviert. Wenn Sie Volumes auf diesen Cloud Volumes ONTAP Systemen erstellt haben, starten Sie BlueXP Backup und Recovery sowie "Aktivieren Sie die Sicherung auf jedem Volume, das Sie schützen möchten".

BlueXP Backup und Recovery auf einem vorhandenen System aktivieren

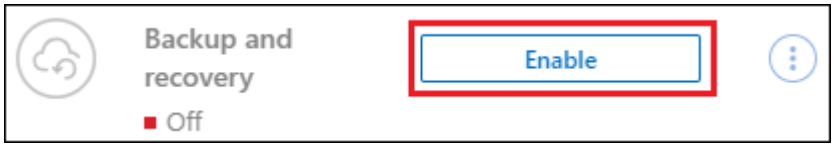
Backup und Recovery von BlueXP können jederzeit direkt aus der Arbeitsumgebung heraus aktiviert werden.

Schritte

1. Wählen Sie auf dem BlueXP-Bildschirm die Arbeitsumgebung aus und wählen Sie im rechten Bereich neben dem Backup- und Recovery-Dienst **Enable** aus.

   Wenn das Ziel von Google Cloud Storage für Ihre Backups als Arbeitsumgebung auf dem Canvas existiert, können Sie den Cluster auf die Google Cloud Storage Arbeitsumgebung ziehen, um den Setup-

Assistenten zu starten.



Informationen zum Ändern von Backup-Einstellungen oder Hinzufügen von Replikationen finden Sie unter "ONTAP-Backups managen".

Google Cloud Storage als Backup-Ziel vorbereiten

Die Vorbereitung von Google Cloud Storage als Backup-Ziel beinhaltet folgende Schritte:

- Richten Sie Berechtigungen ein.
- (Optional) Erstellen Sie Ihre eigenen Buckets. (Der Service erstellt Buckets für Sie, wenn Sie möchten.)
- (Optional) Einrichten von vom Kunden gemanagten Schlüsseln für die Datenverschlüsselung

Berechtigungen einrichten

Sie müssen Speicherzugriffsschlüssel für ein Dienstkonto bereitstellen, das über bestimmte Berechtigungen mit einer benutzerdefinierten Rolle verfügt. Ein Servicekonto ermöglicht BlueXP Backup und Recovery für Authentifizierung und Zugriff auf Cloud Storage Buckets, die für das Speichern von Backups verwendet werden. Die Schlüssel sind erforderlich, damit Google Cloud Storage weiß, wer die Anfrage stellt.

Schritte

1. Im "Google Cloud Console", Gehen Sie zur Seite **Rollen**.
2. "Erstellen Sie eine neue Rolle" Mit folgenden Berechtigungen:

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. In der Google Cloud Konsole "Rufen Sie die Seite Servicekonten auf".
4. Wählen Sie Ihr Cloud-Projekt aus.
5. Wählen Sie **Service-Konto erstellen** und geben Sie die erforderlichen Informationen ein:
   a. **Service Account Details**: Geben Sie einen Namen und eine Beschreibung ein.

b. **Bewilligung dieses Servicekontos Zugriff auf Projekt**: Wählen Sie die benutzerdefinierte Rolle aus, die Sie gerade erstellt haben.

c. Wählen Sie * Fertig*.

6. Gehen Sie zu "GCP-Speichereinstellungen" Außerdem Zugriffsschlüssel für das Servicekonto erstellen:

a. Wählen Sie ein Projekt aus, und wählen Sie **Interoperabilität**. Wenn Sie dies noch nicht getan haben, wählen Sie **Zugriff auf Interoperabilität aktivieren**.

b. Wählen Sie unter **Zugriffsschlüssel für Dienstkonten Schlüssel für ein Dienstkonto erstellen** aus, wählen Sie das soeben erstellte Dienstkonto aus und klicken Sie auf **Schlüssel erstellen**.

Beim Konfigurieren des Backup-Service müssen Sie die Schlüssel zu einem späteren Zeitpunkt in BlueXP Backup und Recovery eingeben.

Erstellen Sie Ihre eigenen Buckets

Standardmäßig erstellt der Service Buckets für Sie. Wenn Sie Ihre eigenen Buckets verwenden möchten, können Sie diese auch erstellen, bevor Sie den Assistenten zur Backup-Aktivierung starten und diese Buckets im Assistenten auswählen.

"Erfahren Sie mehr über das Erstellen eigener Buckets".

Einrichtung von CMEK (Customer Managed Encryption Keys) für die Datenverschlüsselung

Sie können Ihre eigenen, von Kunden gemanagten Schlüssel zur Datenverschlüsselung verwenden, statt die von Google standardmäßig gemanagten Verschlüsselungsschlüssel zu verwenden. Sowohl regionsübergreifende als auch projektübergreifende Schlüssel werden unterstützt, sodass Sie ein Projekt für einen Bucket auswählen können, der sich vom Projekt des CMEK-Schlüssels unterscheidet.

Wenn Sie planen, Ihre eigenen kundenverwalteten Schlüssel zu verwenden:

- Sie benötigen den Schlüsselring und den Schlüsselnamen, damit Sie diese Informationen im Aktivierungsassistenten hinzufügen können. "Erfahren Sie mehr über vom Kunden verwaltete Verschlüsselungsschlüssel".
- Sie müssen überprüfen, ob diese erforderlichen Berechtigungen in der Rolle für den Connector enthalten sind:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Sie müssen überprüfen, ob die Google API „Cloud Key Management Service (KMS)“ in Ihrem Projekt aktiviert ist. Siehe "Google Cloud-Dokumentation: Aktivieren von APIs" Entsprechende Details.

CMEK-Überlegungen:

- Sowohl HSM (Hardware-Backed) als auch Software-generierte Schlüssel werden unterstützt.
- Es werden sowohl neu erstellte als auch importierte Cloud KMS-Schlüssel unterstützt.
- Es werden nur regionale Schlüssel unterstützt, globale Schlüssel werden nicht unterstützt.
- Derzeit wird nur der Zweck „symmetrische Verschlüsselung/Entschlüsselung“ unterstützt.
- Der dem Storage-Konto zugeordnete Service-Agent wird der IAM-Rolle „CryptoKey Encrypter/Decrypter (Rollen/Cloudkms.cryptoKeyEncrypterDecrypter)“ von BlueXP Backup und Recovery zugewiesen.

Aktivieren Sie Backups auf Ihren ONTAP Volumes

Sie können Backups jederzeit direkt aus Ihrer On-Premises-Arbeitsumgebung heraus aktivieren.

Ein Assistent führt Sie durch die folgenden wichtigen Schritte:

- die Sie sichern möchten
- Backup-Strategie definieren
- Überprüfen Sie Ihre Auswahl

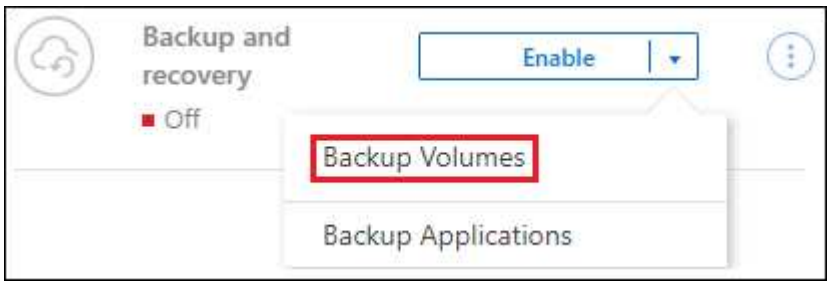
Das können Sie auch Zeigt die API-Befehle an Kopieren Sie im Überprüfungsschritt den Code, um die Backup-Aktivierung für zukünftige Arbeitsumgebungen zu automatisieren.

Starten Sie den Assistenten

Schritte

1. Greifen Sie auf eine der folgenden Arten auf den Assistenten zur Aktivierung von Backup und Recovery zu:

   - Wählen Sie auf dem BlueXP-Bildschirm die Arbeitsumgebung aus, und wählen Sie im rechten Bereich neben dem Sicherungs- und Wiederherstellungsdienst die Option **Enable > Backup Volumes** aus.

     Wenn das GCP-Ziel für Ihre Backups als Arbeitsumgebung auf dem Bildschirm vorhanden ist, können Sie das ONTAP-Cluster auf den GCP-Objektspeicher ziehen.

   - Wählen Sie in der Sicherungs- und Wiederherstellungsleiste **Volumes** aus. Wählen Sie auf der Registerkarte Volumes die Option **actions** aus ••• Und wählen Sie **Backup aktivieren** für ein einzelnes Volume (das noch nicht über Replikation oder Backup auf Objektspeicher verfügt).

   Auf der Seite Einführung des Assistenten werden die Schutzoptionen einschließlich lokaler Snapshots, Replikation und Backups angezeigt. Wenn Sie die zweite Option in diesem Schritt gewählt haben, wird die Seite „Backup-Strategie definieren“ mit einem ausgewählten Volume angezeigt.

2. Fahren Sie mit den folgenden Optionen fort:

   - Wenn Sie bereits einen BlueXP Connector haben, sind Sie fertig. Wählen Sie einfach **Weiter**.
   - Wenn Sie noch keinen BlueXP Connector haben, wird die Option **Connector hinzufügen** angezeigt.

Siehe Bereiten Sie Ihren BlueXP Connector vor.

Wählen Sie die Volumes aus, die Sie sichern möchten

Wählen Sie die Volumes aus, die Sie schützen möchten. Ein geschütztes Volume verfügt über eine oder mehrere der folgenden Elemente: Snapshot-Richtlinie, Replizierungsrichtlinie und Richtlinie für das Backup in ein Objekt.

Sie können FlexVol- oder FlexGroup-Volumes schützen. Sie können jedoch keine Kombination dieser Volumes auswählen, wenn Sie Backups für eine funktionierende Umgebung aktivieren. Informieren Sie sich darüber "Aktivieren Sie das Backup für zusätzliche Volumes in der Arbeitsumgebung" (FlexVol oder FlexGroup), nachdem Sie das Backup für die ersten Volumes konfiguriert haben.

- Sie können ein Backup nur auf einem einzelnen FlexGroup Volume gleichzeitig aktivieren.
- Die ausgewählten Volumes müssen dieselbe SnapLock-Einstellung aufweisen. Auf allen Volumes muss SnapLock Enterprise aktiviert oder SnapLock deaktiviert sein.

Schritte

Beachten Sie, dass die Richtlinien, die Sie später auswählen, diese vorhandenen Richtlinien überschreiben, wenn die von Ihnen ausgewählten Volumes bereits Snapshot- oder Replikationsrichtlinien angewendet haben.

1. Wählen Sie auf der Seite Volumes auswählen das Volume oder die Volumes aus, die Sie schützen möchten.
   - Optional können Sie die Zeilen so filtern, dass nur Volumes mit bestimmten Volumentypen, Stilen und mehr angezeigt werden, um die Auswahl zu erleichtern.
   - Nachdem Sie das erste Volume ausgewählt haben, können Sie alle FlexVol Volumes auswählen (FlexGroup Volumes können nur einzeln ausgewählt werden). Um alle vorhandenen FlexVol-Volumes zu sichern, aktivieren Sie zuerst ein Volume und dann das Kontrollkästchen in der Titelzeile. (

).
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume (

).
2. Wählen Sie **Weiter**.

Backup-Strategie definieren

Zur Definition der Backup-Strategie gehören die folgenden Optionen:

- Unabhängig davon, ob Sie eine oder alle Backup-Optionen: Lokale Snapshots, Replikation und Backup-to-Object-Storage möchten
- Der Netapp Architektur Sind
- Lokale Snapshot-Richtlinie
- Replikationsziel und -Richtlinie

Wenn die ausgewählten Volumes andere Snapshot- und Replikationsrichtlinien haben als die in diesem Schritt ausgewählten Richtlinien, werden die vorhandenen Richtlinien überschrieben.

- Backup von Objekt-Storage-Informationen (Provider-, Verschlüsselungs-, Netzwerk-, Backup-Richtlinien- und Exportoptionen)

Schritte

1. Wählen Sie auf der Seite Backup-Strategie definieren eine oder alle der folgenden Optionen aus. Alle drei sind standardmäßig ausgewählt:
   - **Lokale Snapshots**: Wenn Sie eine Replikation oder Sicherung auf Objektspeicher durchführen, müssen lokale Snapshots erstellt werden.
   - **Replikation**: Erstellt replizierte Volumes auf einem anderen ONTAP-Speichersystem.
   - **Backup**: Sichert Volumes auf Objektspeicher.
2. **Architektur**: Wenn Sie Replikation und Backup gewählt haben, wählen Sie einen der folgenden Informationsflüsse:
   - **Kaskadierung**: Informationsflüsse vom primären Speichersystem zum sekundären und vom sekundären zum Objektspeicher.
   - **Fan out**: Der Informationsfluss vom primären zum sekundären *und* vom primären zum Objektspeicher.

     Einzelheiten zu diesen Architekturen finden Sie unter "Planen Sie Ihren Weg zum Schutz".
3. **Lokaler Snapshot**: Wählen Sie eine vorhandene Snapshot-Richtlinie aus oder erstellen Sie eine.

   Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Sicherung finden Sie unter "Erstellen einer Richtlinie".

   Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:
   - Geben Sie den Namen der Richtlinie ein.
   - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
   - Wählen Sie **Erstellen**.
4. **Replikation**: Stellen Sie die folgenden Optionen ein:
   - **Replikationsziel**: Wählen Sie die Zielarbeitsumgebung und SVM aus. Wählen Sie optional das Zielaggregat oder die Aggregate und das Präfix oder Suffix aus, die dem Namen des replizierten Volumes hinzugefügt werden sollen.
   - **Replikationsrichtlinie**: Wählen Sie eine vorhandene Replikationsrichtlinie oder erstellen Sie eine.

     Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Replikation finden Sie unter "Erstellen einer Richtlinie".

     Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:
     - Geben Sie den Namen der Richtlinie ein.
     - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
     - Wählen Sie **Erstellen**.
5. **Backup auf Objekt**: Wenn Sie **Backup** ausgewählt haben, stellen Sie die folgenden Optionen ein:
   - **Provider**: Wählen Sie **Google Cloud**.
   - **Provider-Einstellungen**: Geben Sie die Provider-Details und die Region ein, in der die Backups gespeichert werden sollen.

Erstellen Sie entweder einen neuen Bucket, oder wählen Sie einen vorhandenen Bucket aus.

- **Verschlüsselungsschlüssel**: Wenn Sie einen neuen Google-Bucket erstellt haben, geben Sie die Verschlüsselungsschlüsselinformationen ein, die Sie vom Anbieter erhalten haben. Wählen Sie aus, ob Sie die standardmäßige Google Cloud-Verschlüsselung verwenden oder Ihre eigenen vom Kunden verwalteten Schlüssel über Ihr Google-Konto auswählen, um die Verschlüsselung Ihrer Daten zu managen.

  Wenn Sie Ihre eigenen vom Kunden verwalteten Schlüssel verwenden möchten, geben Sie den Schlüsselspeicher und die Schlüsselinformationen ein.

  Wenn Sie einen vorhandenen Google Cloud-Bucket ausgewählt haben, sind bereits Verschlüsselungsinformationen verfügbar. Sie müssen sie daher jetzt nicht eingeben.

- **Backup-Richtlinie**: Wählen Sie eine vorhandene Richtlinie für Backup-to-Object-Storage aus oder erstellen Sie eine.

  Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Sicherung finden Sie unter "Erstellen einer Richtlinie".

  Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

  - Geben Sie den Namen der Richtlinie ein.
  - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
  - Wählen Sie **Erstellen**.

- **Exportieren vorhandener Snapshot-Kopien als Backup-Kopien in den Objektspeicher**: Wenn es lokale Snapshot-Kopien für Volumes in dieser Arbeitsumgebung gibt, die mit dem Backup-Zeitplan-Label übereinstimmen, das Sie gerade für diese Arbeitsumgebung ausgewählt haben (z. B. täglich, wöchentlich usw.), wird diese zusätzliche Eingabeaufforderung angezeigt. Aktivieren Sie dieses Kontrollkästchen, damit alle historischen Snapshots als Backup-Dateien in den Objektspeicher kopiert werden, um einen möglichst vollständigen Schutz für Ihre Volumes zu gewährleisten.

6. Wählen Sie **Weiter**.

Überprüfen Sie Ihre Auswahl

Dies ist die Möglichkeit, Ihre Auswahl zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

Schritte

1. Überprüfen Sie auf der Seite „Überprüfen“ Ihre Auswahl.
2. Aktivieren Sie optional das Kontrollkästchen, um * die Snapshot-Policy-Labels automatisch mit den Label der Replikations- und Backup-Policy* zu synchronisieren. Dadurch werden Snapshots mit einem Label erstellt, das den Labels in den Replizierungs- und Backup-Richtlinien entspricht.
3. Wählen Sie **Sicherung Aktivieren**.

Ergebnis

Mit BlueXP Backup und Recovery werden erste Backups Ihrer Volumes erstellt. Der Basistransfer des replizierten Volumes und der Backup-Datei beinhaltet eine vollständige Kopie der Daten des primären Storage-Systems. Nachfolgende Transfers enthalten differenzielle Kopien der primären Storage-System-Daten in Snapshot Kopien.

Ein repliziertes Volume wird im Zielcluster erstellt, das mit dem primären Storage-System-Volume synchronisiert wird.

Ein Google Cloud Storage-Bucket wird in dem Servicekonto erstellt, das durch den von Ihnen eingegebenen Google-Zugriffsschlüssel und geheimen Schlüssel angegeben ist, und die Backup-Dateien werden dort gespeichert.

Backups sind standardmäßig mit der Storage-Klasse *Standard* verknüpft. Sie können die preisgünstigeren Storage-Klassen *Nearline*, *Coldline* oder *Archive* verwenden. Sie konfigurieren die Storage-Klasse jedoch über Google, nicht über die BlueXP Backup- und Recovery-UI. Siehe das Thema Google "Ändern der Standard-Storage-Klasse eines Buckets" Entsprechende Details.

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".

Zeigt die API-Befehle an

Möglicherweise möchten Sie die API-Befehle anzeigen und optional kopieren, die im Assistenten Sicherung und Wiederherstellung aktivieren verwendet werden. Dies ist möglicherweise sinnvoll, um die Backup-Aktivierung in zukünftigen Arbeitsumgebungen zu automatisieren.

Schritte

1. Wählen Sie im Assistenten Backup und Recovery aktivieren **API-Anforderung anzeigen** aus.
2. Um die Befehle in die Zwischenablage zu kopieren, wählen Sie das Symbol **Kopieren**.

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 unter anderem die Änderung der verfügbaren Netzwerkbandbreite für das Hochladen von Backups in den Objekt-Storage, die Änderung der automatischen Backup-Einstellung für zukünftige Volumes.
- Das können Sie auch "Wiederherstellung von Volumes, Ordnern oder einzelnen Dateien aus einer Sicherungsdatei" Einem Cloud Volumes ONTAP System in Google oder einem lokalen ONTAP System übertragen.

Sichern Sie lokale ONTAP-Daten auf Amazon S3 mit BlueXP Backup und Recovery

Führen Sie einige Schritte in der Sicherung und Wiederherstellung von BlueXP durch, um mit der Sicherung von Volumedaten von Ihren lokalen ONTAP-Systemen auf einem sekundären Speichersystem und im Amazon S3-Cloud-Speicher zu beginnen.

„On-Premises ONTAP Systeme“ umfassen FAS, AFF und ONTAP Select Systeme.

Schnellstart

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

1 Identifizieren Sie die Verbindungsmethode, die Sie verwenden werden

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.

Identifizieren Sie die Verbindungsmethode.

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. Falls nicht, müssen Sie einen BlueXP Connector erstellen, um ONTAP Daten auf AWS S3 Storage zu sichern. Außerdem müssen Sie die Netzwerkeinstellungen für den Connector anpassen, damit er eine Verbindung zu AWS S3 herstellen kann.

Erfahren Sie, wie Sie einen Connector erstellen und die erforderlichen Netzwerkeinstellungen definieren.

3 Lizenzanforderungen prüfen

Sie müssen die Lizenzanforderungen sowohl für AWS als auch für BlueXP prüfen.

Siehe Lizenzanforderungen prüfen.

4 Bereiten Sie Ihre ONTAP-Cluster vor

Erkennen Sie Ihre ONTAP-Cluster in BlueXP, überprüfen Sie, ob die Cluster Mindestanforderungen erfüllen, und passen Sie Netzwerkeinstellungen für die Verbindung der Cluster mit AWS S3 an.

Informieren Sie sich, wie Sie Ihre ONTAP Cluster vorbereiten.

5 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 ONTAP Backups vorbereiten.

6 Aktivieren Sie Backups auf Ihren ONTAP Volumes

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

Backup-Richtlinien auszuwählen, die Sie verwenden werden, und die Volumes, die Sie sichern möchten.

Aktivieren Sie Backups auf Ihren ONTAP Volumes.

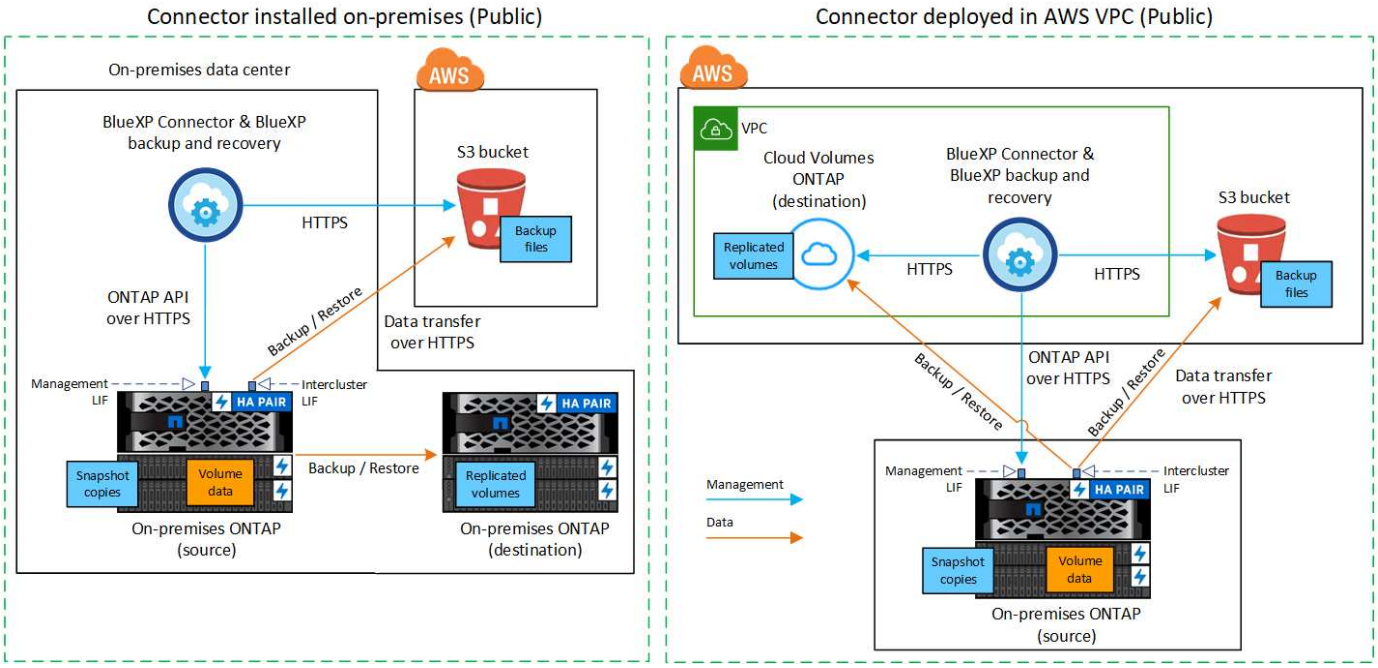
Identifizieren Sie die Verbindungsmethode

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

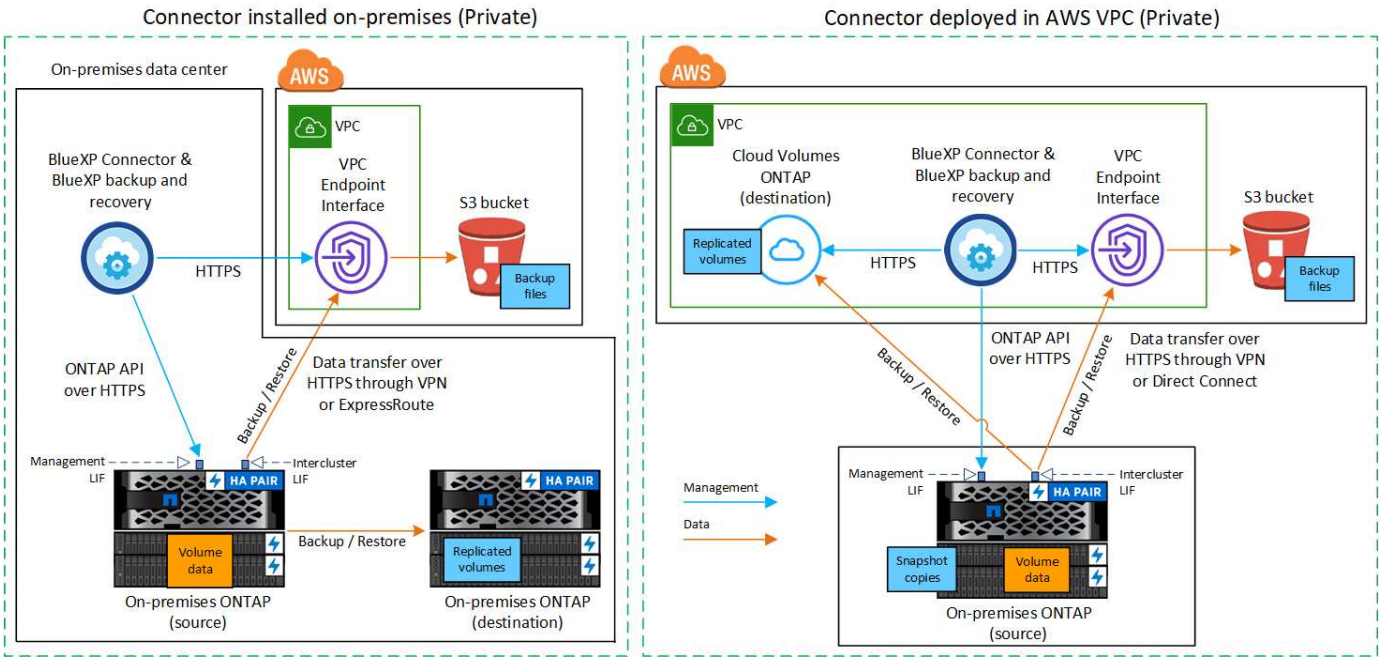
- **Öffentliche Verbindung** - direkte Verbindung des ONTAP-Systems mit AWS S3 über einen öffentlichen S3-Endpunkt.
- **Private Verbindung** - Verwenden Sie ein VPN oder AWS Direct Connect und leiten Sie den Verkehr über eine VPC Endpoint Schnittstelle, die eine private IP-Adresse verwendet.

Optional können Sie für replizierte Volumes auch eine Verbindung zu einem sekundären ONTAP-System über eine öffentliche oder private Verbindung herstellen.

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 Ihren BlueXP Connector vor

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

Erstellen oder Schalten 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 auf AWS S3 Storage zu sichern. Sie können keinen Connector verwenden, der bei einem anderen Cloud-Provider bereitgestellt wird.

- "Erfahren Sie mehr über Steckverbinder"
- "Installieren Sie einen Connector in AWS"
- "Installieren Sie einen Connector in Ihren Räumlichkeiten"
- "Installieren Sie einen Connector in einer AWS GovCloud Region"

  BlueXP Backup und Recovery werden in GovCloud Regionen unterstützt, wenn Connector in der Cloud bereitgestellt wird – und nicht dann, wenn sie an Ihrem Standort installiert sind. Darüber hinaus müssen Sie den Connector über AWS Marketplace implementieren. Sie können den Connector nicht von der BlueXP SaaS-Website in einer Regierungsregion implementieren.

Bereiten Sie die Netzwerkanforderungen für den Connector vor

Stellen Sie sicher, dass die folgenden Netzwerkanforderungen erfüllt sind:

- Stellen Sie sicher, dass das Netzwerk, in dem der Connector installiert ist, folgende Verbindungen ermöglicht:
  - Eine HTTPS-Verbindung über Port 443 zum BlueXP Backup- und Recovery-Service und zu Ihrem 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.

Lizenzanforderungen prüfen

Sie müssen die Lizenzanforderungen sowohl für AWS als auch für BlueXP überprüfen:

- Bevor Sie BlueXP Backup und Recovery für Ihr Cluster aktivieren können, müssen Sie entweder ein PAYGO-Angebot (Pay-as-you-go) für BlueXP Marketplace von AWS abonnieren oder eine BYOL-Lizenz für BlueXP Backup und Recovery von NetApp erwerben und aktivieren. Diese Lizenzen sind für Ihr Konto und können für mehrere Systeme verwendet werden.
  - Für die BlueXP PAYGO-Lizenzierung für Backup und Recovery benötigen Sie ein Abonnement des "NetApp BlueXP Angebot über den AWS Marketplace". Die Abrechnung für BlueXP Backup und Recovery erfolgt über dieses Abonnement.
  - Für die BYOL-Lizenzierung für BlueXP Backup und Recovery benötigen Sie die Seriennummer von NetApp, anhand derer Sie den Service für die Dauer und 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.

Unterstützte Regionen

Sie können in allen Regionen, einschließlich der AWS GovCloud-Regionen, Backups von lokalen Systemen auf Amazon S3 erstellen. Sie geben die Region an, in der Backups beim Einrichten des Dienstes gespeichert werden sollen.

Bereiten Sie Ihre ONTAP-Cluster vor

Sie müssen Ihr On-Premises-Quell-ONTAP-System und alle sekundären lokalen ONTAP oder Cloud Volumes ONTAP Systeme vorbereiten.

Zur Vorbereitung Ihrer ONTAP-Cluster sind folgende Schritte erforderlich:

- Ihre ONTAP-Systeme in BlueXP erkennen
- Überprüfen Sie die Systemanforderungen für ONTAP
- ONTAP Netzwerkanforderungen für Daten-Backups im Objekt-Storage prüfen
- Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes

Ihre ONTAP-Systeme in BlueXP erkennen

Sowohl das On-Premises-Quell-ONTAP-System als auch alle sekundären ONTAP- oder Cloud Volumes ONTAP-Systeme vor Ort müssen auf der BlueXP Leinwand verfügbar sein.

Sie müssen die Cluster-Management-IP-Adresse und das Passwort kennen, mit dem das Admin-Benutzerkonto den Cluster hinzufügen kann.

"Entdecken Sie ein Cluster".

Überprüfen Sie die Systemanforderungen für ONTAP

Stellen Sie sicher, dass die folgenden ONTAP-Anforderungen erfüllt sind:

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

  Hinweis: das „Hybrid Cloud Bundle“ ist bei Backup und Recovery von BlueXP nicht erforderlich.

  Erfahren Sie, wie Sie "Management Ihrer Cluster-Lizenzen".

- Zeit und Zeitzone sind korrekt eingestellt. Erfahren Sie, wie Sie "Konfigurieren Sie die Cluster-Zeit".
- Wenn Sie Daten replizieren möchten, sollten Sie vor der Replizierung von Daten überprüfen, ob auf den Quell- und Zielsystemen kompatible ONTAP-Versionen ausgeführt werden.

  "Zeigen Sie kompatible ONTAP Versionen für SnapMirror Beziehungen an".

ONTAP Netzwerkanforderungen für Daten-Backups im Objekt-Storage prüfen

Sie müssen die folgenden Anforderungen auf dem System konfigurieren, das eine Verbindung zu Objekt-Storage herstellt.

- Konfigurieren Sie für eine Fan-out-Backup-Architektur die folgenden Einstellungen auf dem *primary* -System.
- Konfigurieren Sie für eine kaskadierte Backup-Architektur die folgenden Einstellungen auf dem *Secondary* -System.

Die folgenden Netzwerkanforderungen für ONTAP-Cluster sind erforderlich:

- 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 BlueXP Backup und Recovery einrichten, werden Sie aufgefordert, den IPspace 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. die Firewall-Regeln, um BlueXP Backup- und Recovery-Verbindungen von ONTAP zum Objekt-Storage über Port 443 und Datenverkehr der 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".

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes

Wenn Sie planen, mithilfe von BlueXP Backup und Recovery replizierte Volumes auf einem sekundären ONTAP System zu erstellen, stellen Sie sicher, dass die Quell- und Zielsysteme die folgenden Netzwerkanforderungen erfüllen.

Netzwerkanforderungen für On-Premises-ONTAP

- Wenn sich der Cluster an Ihrem Standort befindet, sollten Sie über eine Verbindung zwischen Ihrem Unternehmensnetzwerk und Ihrem virtuellen Netzwerk des Cloud-Providers verfügen. Hierbei handelt es sich in der Regel um eine VPN-Verbindung.
- ONTAP Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Cluster-Anforderungen erfüllen.

  Da Sie Daten auf Cloud Volumes ONTAP oder auf lokale Systeme replizieren können, prüfen Sie Peering-Anforderungen für lokale ONTAP Systeme. "Anzeigen von Voraussetzungen für Cluster-Peering in der ONTAP-Dokumentation".

Netzwerkanforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen ein- und ausgehenden Regeln enthalten: Speziell Regeln für ICMP und die Ports 11104 und 11105. Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.

Amazon S3 als Backup-Ziel vorbereiten

Zur Vorbereitung von Amazon S3 als Backup-Ziel gehören die folgenden Schritte:

- S3-Berechtigungen einrichten.
- (Optional) Erstellen Sie Ihre eigenen S3 Buckets. (Der Service erstellt Buckets für Sie, wenn Sie möchten.)
- (Optional) Einrichten von vom Kunden gemanagten AWS-Schlüsseln für die Datenverschlüsselung
- (Optional) Konfigurieren Sie Ihr System für eine private Verbindung über eine VPC-Endpunktschnittstelle.

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. Stellen Sie sicher, dass der Connector über die erforderlichen Berechtigungen verfügt. Weitere Informationen finden Sie unter "Berechtigungen für BlueXP -Richtlinien".

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

2. Wenn Sie den Dienst aktivieren, werden Sie vom Backup-Assistenten aufgefordert, einen Zugriffsschlüssel und einen geheimen Schlüssel einzugeben. Diese 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.

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

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

Erstellen Sie Ihre eigenen Buckets

Standardmäßig erstellt der Service Buckets für Sie. Wenn Sie Ihre eigenen Buckets verwenden möchten, können Sie diese auch erstellen, bevor Sie den Assistenten zur Backup-Aktivierung starten und diese Buckets im Assistenten auswählen.

"Erfahren Sie mehr über das Erstellen eigener Buckets".

Wenn Sie eigene Buckets erstellen, sollten Sie den Bucket-Namen „netapp-Backup“ verwenden. Wenn Sie einen benutzerdefinierten Namen verwenden möchten, bearbeiten Sie das `ontapcloud-instance-policy-netapp-backup` IAMRole für die vorhandenen CVOs und fügen Sie die folgende Liste zu den S3-Berechtigungen hinzu. Sie müssen angeben `"Resource": "arn:aws:s3:::*"` Und weisen Sie alle erforderlichen Berechtigungen zu, die mit dem Bucket verknüpft werden müssen.

„Aktion“: [
„S3:ListBucket“
„S3:GetBucketLocation“
]
„Ressource“: „arn:aws:s3::*“,
„Effekt“: „Zulassen“
},
{
„Aktion“: [
„S3:GetObject“,
„S3:PutObject“,
„S3:DeleteObject“,
„S3:ListAllMyBuckets“,
„S3:PutObjectTagging“,
„S3:GetObjectTagging“,
„S3:RestoreObject“,
„S3:GetBucketObjectLockConfiguration“,
„S3:GetObjectRetention“,
„S3:PutBucketObjectLockConfiguration“,
„S3:PutObjectRetention“
]
„Ressource“: „arn:aws:s3::*“,

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 stattdessen Ihre eigenen von Kunden gemanagten Schlüssel zur Datenverschlüsselung verwenden möchten, statt die Standardschlüssel zu verwenden, müssen Sie die für die Verschlüsselung gemanagten Schlüssel bereits einrichten, bevor Sie den BlueXP Backup- und Recovery-Assistenten starten.

"Weitere Informationen zur Verwendung Ihrer eigenen Amazon-Verschlüsselungen mit Cloud Volumes ONTAP finden Sie unter".

"Erfahren Sie, wie Sie Ihre eigenen Amazon Verschlüsselungsschlüssel für BlueXP Backup und Recovery verwenden".

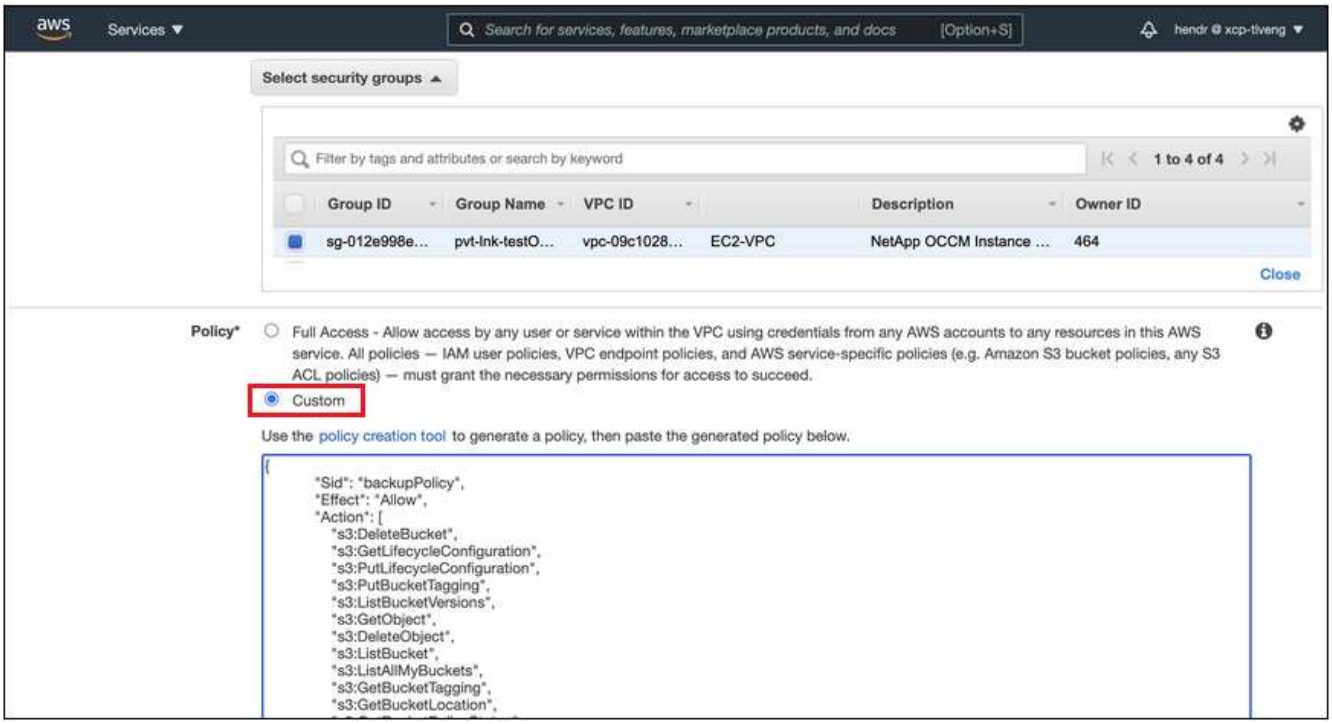
Konfigurieren Sie Ihr System für eine private Verbindung mithilfe einer VPC-Endpunktschnittstelle

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".

Schritte

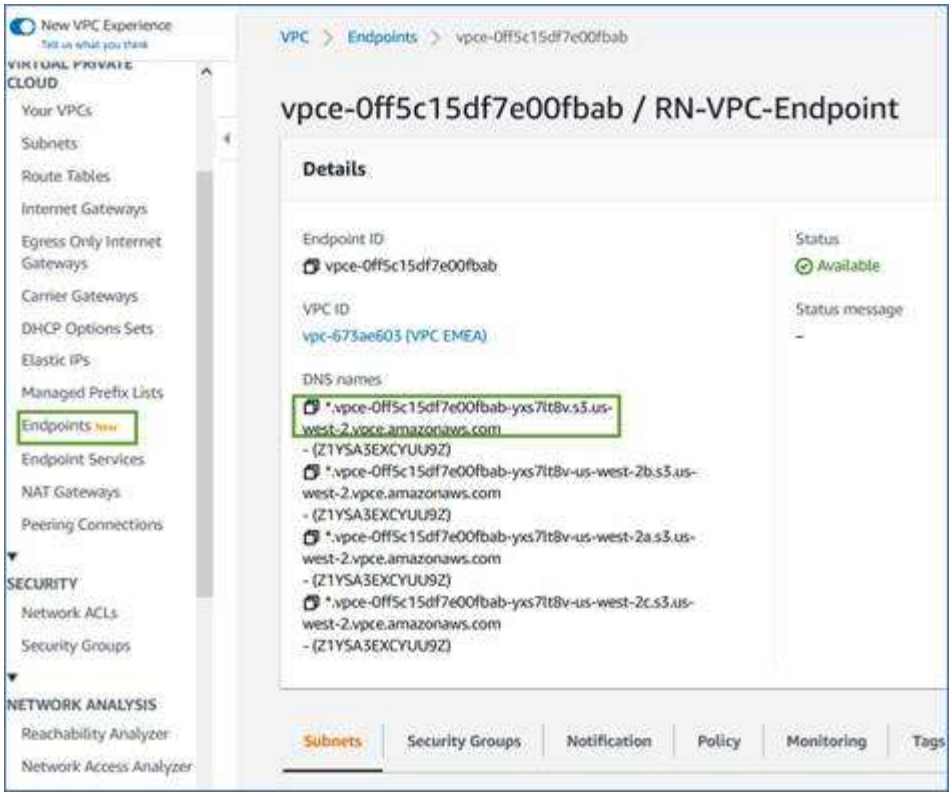
1. Konfiguration eines Schnittstellenendpunkts über die Amazon VPC Konsole oder die Befehlszeile erstellen. "Weitere Informationen zur Verwendung von AWS PrivateLink für Amazon S3 finden Sie unter".
2. Ändern Sie die Konfiguration der Sicherheitsgruppe, die dem BlueXP Connector zugeordnet ist. Sie müssen 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 das Backup und Recovery von BlueXP im 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
```

Aktivieren Sie Backups auf Ihren ONTAP Volumes

Sie können Backups jederzeit direkt aus Ihrer On-Premises-Arbeitsumgebung heraus aktivieren.

Ein Assistent führt Sie durch die folgenden wichtigen Schritte:

- die Sie sichern möchten
- Backup-Strategie definieren
- Überprüfen Sie Ihre Auswahl

Das können Sie auch Zeigt die API-Befehle an Kopieren Sie im Überprüfungsschritt den Code, um die Backup-Aktivierung für zukünftige Arbeitsumgebungen zu automatisieren.

Starten Sie den Assistenten

Schritte

1. Greifen Sie auf eine der folgenden Arten auf den Assistenten zur Aktivierung von Backup und Recovery zu:

   - Wählen Sie auf dem BlueXP-Bildschirm die Arbeitsumgebung aus, und wählen Sie im rechten Bereich neben dem Sicherungs- und Wiederherstellungsdienst die Option **Enable > Backup Volumes** aus.

     Wenn das Amazon S3-Ziel für Ihre Backups als Arbeitsumgebung auf dem Bildschirm vorhanden ist, können Sie das ONTAP-Cluster auf den Amazon S3-Objektspeicher ziehen.

   - Wählen Sie in der Sicherungs- und Wiederherstellungsleiste **Volumes** aus. Wählen Sie auf der Registerkarte Volumes die Option **actions** aus ••• Und wählen Sie **Backup aktivieren** für ein einzelnes Volume (das noch nicht über Replikation oder Backup auf Objektspeicher verfügt).

   Auf der Seite Einführung des Assistenten werden die Schutzoptionen einschließlich lokaler Snapshots, Replikation und Backups angezeigt. Wenn Sie die zweite Option in diesem Schritt gewählt haben, wird die Seite „Backup-Strategie definieren“ mit einem ausgewählten Volume angezeigt.

2. Fahren Sie mit den folgenden Optionen fort:

   - Wenn Sie bereits einen BlueXP Connector haben, sind Sie fertig. Wählen Sie einfach **Weiter**.
   - Wenn Sie noch keinen BlueXP Connector haben, wird die Option **Connector hinzufügen** angezeigt. Siehe Bereiten Sie Ihren BlueXP Connector vor.

Wählen Sie die Volumes aus, die Sie sichern möchten

Wählen Sie die Volumes aus, die Sie schützen möchten. Ein geschütztes Volume verfügt über eine oder mehrere der folgenden Elemente: Snapshot-Richtlinie, Replizierungsrichtlinie und Richtlinie für das Backup in ein Objekt.

Sie können FlexVol- oder FlexGroup-Volumes schützen. Sie können jedoch keine Kombination dieser Volumes auswählen, wenn Sie Backups für eine funktionierende Umgebung aktivieren. Informieren Sie sich darüber "Aktivieren Sie das Backup für zusätzliche Volumes in der Arbeitsumgebung" (FlexVol oder FlexGroup),

nachdem Sie das Backup für die ersten Volumes konfiguriert haben.

- Sie können ein Backup nur auf einem einzelnen FlexGroup Volume gleichzeitig aktivieren.
- Die ausgewählten Volumes müssen dieselbe SnapLock-Einstellung aufweisen. Auf allen Volumes muss SnapLock Enterprise aktiviert oder SnapLock deaktiviert sein.

Schritte

Beachten Sie, dass die Richtlinien, die Sie später auswählen, diese vorhandenen Richtlinien überschreiben, wenn die von Ihnen ausgewählten Volumes bereits Snapshot- oder Replikationsrichtlinien angewendet haben.

1. Wählen Sie auf der Seite Volumes auswählen das Volume oder die Volumes aus, die Sie schützen möchten.
   - Optional können Sie die Zeilen so filtern, dass nur Volumes mit bestimmten Volumentypen, Stilen und mehr angezeigt werden, um die Auswahl zu erleichtern.
   - Nachdem Sie das erste Volume ausgewählt haben, können Sie alle FlexVol Volumes auswählen (FlexGroup Volumes können nur einzeln ausgewählt werden). Um alle vorhandenen FlexVol-Volumes zu sichern, aktivieren Sie zuerst ein Volume und dann das Kontrollkästchen in der Titelzeile. (

).
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume (

).
2. Wählen Sie **Weiter**.

Backup-Strategie definieren

Zur Definition der Backup-Strategie gehören die folgenden Optionen:

- Unabhängig davon, ob Sie eine oder alle Backup-Optionen: Lokale Snapshots, Replikation und Backup-to-Object-Storage möchten
- Der Netapp Architektur Sind
- Lokale Snapshot-Richtlinie
- Replikationsziel und -Richtlinie

Wenn die ausgewählten Volumes andere Snapshot- und Replikationsrichtlinien haben als die in diesem Schritt ausgewählten Richtlinien, werden die vorhandenen Richtlinien überschrieben.

- Backup von Objekt-Storage-Informationen (Provider-, Verschlüsselungs-, Netzwerk-, Backup-Richtlinien- und Exportoptionen)

Schritte

1. Wählen Sie auf der Seite Backup-Strategie definieren eine oder alle der folgenden Optionen aus. Alle drei sind standardmäßig ausgewählt:
   - **Lokale Snapshots**: Wenn Sie eine Replikation oder Sicherung auf Objektspeicher durchführen, müssen lokale Snapshots erstellt werden.
   - **Replikation**: Erstellt replizierte Volumes auf einem anderen ONTAP-Speichersystem.
   - **Backup**: Sichert Volumes auf Objektspeicher.
2. **Architektur**: Wenn Sie Replikation und Backup gewählt haben, wählen Sie einen der folgenden Informationsflüsse:

- **Kaskadierung**: Informationsflüsse vom primären zum sekundären zum Objektspeicher und vom sekundären zum Objektspeicher.
- **Fan Out**: Informationen fließen vom primären zum sekundären *und* vom primären zum Objektspeicher.

  Einzelheiten zu diesen Architekturen finden Sie unter "Planen Sie Ihren Weg zum Schutz".

3. **Lokaler Snapshot**: Wählen Sie eine vorhandene Snapshot-Richtlinie aus oder erstellen Sie eine Policy.

   Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung des Snapshots finden Sie unter "Erstellen einer Richtlinie".

4. Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:
   - Geben Sie den Namen der Richtlinie ein.
   - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
     - Legen Sie für Backup-to-Object-Richtlinien die Einstellungen für DataLock und Ransomware-Schutz fest. Weitere Informationen zu DataLock und Ransomware-Schutz finden Sie unter "Richtlinieneinstellungen für Backup-to-Object".
   - Wählen Sie **Erstellen**.
5. **Replikation**: Stellen Sie die folgenden Optionen ein:
   - **Replikationsziel**: Wählen Sie die Zielarbeitsumgebung und SVM aus. Wählen Sie optional das Zielaggregat oder die Aggregate und das Präfix oder Suffix aus, die dem Namen des replizierten Volumes hinzugefügt werden sollen.
   - **Replikationsrichtlinie**: Wählen Sie eine vorhandene Replikationsrichtlinie oder erstellen Sie eine Policy.

     Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Replikation finden Sie unter "Erstellen einer Richtlinie".

     Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

     - Geben Sie den Namen der Richtlinie ein.
     - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
     - Wählen Sie **Erstellen**.
6. **Backup auf Objekt**: Wenn Sie **Backup** ausgewählt haben, stellen Sie die folgenden Optionen ein:
   - **Anbieter**: Wählen Sie **Amazon Web Services**.
   - **Provider-Einstellungen**: Geben Sie die Provider-Details und die AWS-Region ein, in der die Backups gespeichert werden sollen.

     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.

   - **Bucket**: Wählen Sie entweder einen vorhandenen S3-Bucket aus oder erstellen Sie einen neuen. Siehe "S3-Buckets hinzufügen".
   - **Verschlüsselungsschlüssel**: Wenn Sie einen neuen S3-Bucket erstellt haben, geben Sie die Verschlüsselungsschlüsselinformationen ein, die Sie vom Provider erhalten haben. Entscheiden Sie,

ob Sie für das Management der Verschlüsselung Ihrer Daten die standardmäßigen Verschlüsselungsschlüssel von Amazon S3 oder Ihre eigenen von Kunden gemanagten Schlüssel in Ihrem AWS-Konto verwenden werden.

Wenn Sie einen vorhandenen Bucket ausgewählt haben, sind Verschlüsselungsinformationen bereits verfügbar, sodass Sie ihn jetzt nicht mehr eingeben müssen.

- **Netzwerk**: Wählen Sie den IPspace und ob Sie einen privaten Endpunkt verwenden. Der private Endpunkt ist standardmäßig deaktiviert.
  i. 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.
  ii. 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".
- **Backup Policy**: Wählen Sie eine vorhandene Backup Policy aus oder erstellen Sie eine Policy.

  Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Sicherung finden Sie unter "Erstellen einer Richtlinie".

  Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

  - Geben Sie den Namen der Richtlinie ein.
  - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
  - Wählen Sie **Erstellen**.
- **Exportieren vorhandener Snapshot-Kopien als Backup-Kopien in den Objektspeicher**: Wenn es lokale Snapshot-Kopien für Volumes in dieser Arbeitsumgebung gibt, die mit dem Backup-Zeitplan-Label übereinstimmen, das Sie gerade für diese Arbeitsumgebung ausgewählt haben (z. B. täglich, wöchentlich usw.), wird diese zusätzliche Eingabeaufforderung angezeigt. Aktivieren Sie dieses Kontrollkästchen, damit alle historischen Snapshots als Backup-Dateien in den Objektspeicher kopiert werden, um einen möglichst vollständigen Schutz für Ihre Volumes zu gewährleisten.

7. Wählen Sie **Weiter**.

Überprüfen Sie Ihre Auswahl

Dies ist die Möglichkeit, Ihre Auswahl zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

Schritte

1. Überprüfen Sie auf der Seite „Überprüfen“ Ihre Auswahl.
2. Aktivieren Sie optional das Kontrollkästchen, um * die Snapshot-Policy-Labels automatisch mit den Label der Replikations- und Backup-Policy* zu synchronisieren. Dadurch werden Snapshots mit einem Label erstellt, das den Labels in den Replizierungs- und Backup-Richtlinien entspricht.
3. Wählen Sie **Sicherung Aktivieren**.

Ergebnis

Mit BlueXP Backup und Recovery werden erste Backups Ihrer Volumes erstellt. Der Basistransfer des replizierten Volumes und der Backup-Datei beinhaltet eine vollständige Kopie der Daten des primären Storage-Systems. Nachfolgende Transfers enthalten differenzielle Kopien der Primärdaten, die in Snapshot Kopien

enthalten sind.

Ein repliziertes Volume wird im Zielcluster erstellt, das mit dem primären Storage Volume synchronisiert wird.

Der S3-Bucket wird in dem Servicekonto erstellt, das durch den eingegebenen S3-Zugriffsschlüssel und geheimen Schlüssel angegeben ist, und die Backup-Dateien werden dort gespeichert. 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".

Zeigt die API-Befehle an

Möglicherweise möchten Sie die API-Befehle anzeigen und optional kopieren, die im Assistenten Sicherung und Wiederherstellung aktivieren verwendet werden. Dies ist möglicherweise sinnvoll, um die Backup-Aktivierung in zukünftigen Arbeitsumgebungen zu automatisieren.

Schritte

1. Wählen Sie im Assistenten Backup und Recovery aktivieren **API-Anforderung anzeigen** aus.
2. Um die Befehle in die Zwischenablage zu kopieren, wählen Sie das Symbol **Kopieren**.

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 Sie lokale ONTAP-Daten mit BlueXP Backup und Recovery im Azure Blob Storage

Führen Sie einige Schritte in der Sicherung und Wiederherstellung von BlueXP durch, um mit der Sicherung von Volumedaten von Ihren lokalen ONTAP-Systemen auf einem sekundären Speichersystem und im Azure Blob-Speicher zu beginnen.

„On-Premises ONTAP Systeme“ umfassen FAS, AFF und ONTAP Select Systeme.

Schnellstart

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

Identifizieren Sie die Verbindungsmethode, die Sie verwenden werden

Sie haben die Wahl, ob Sie Ihr lokales ONTAP-Cluster über das öffentliche Internet direkt mit Azure verbinden oder ob Sie ein VPN oder Azure ExpressRoute verwenden und den Datenverkehr über eine private VPC-Endpunktschnittstelle zu Azure weiterleiten möchten.

Identifizieren Sie die Verbindungsmethode.

Bereiten Sie Ihren BlueXP Connector vor

Falls Sie bereits einen Connector in Ihrem Azure vnet oder Ihrem Standort implementiert haben, sind Sie alle bereit. Falls nicht, müssen Sie einen BlueXP Connector erstellen, um ONTAP Daten in Azure Blob Storage zu sichern. Außerdem müssen Sie die Netzwerkeinstellungen für den Connector anpassen, damit eine Verbindung zu Azure hergestellt werden kann.

Erfahren Sie, wie Sie einen Connector erstellen und die erforderlichen Netzwerkeinstellungen definieren.

Lizenzanforderungen prüfen

Sie müssen die Lizenzanforderungen sowohl für Azure als auch für BlueXP prüfen.

Siehe Lizenzanforderungen prüfen.

Bereiten Sie Ihre ONTAP-Cluster vor

Erkennen Sie Ihre ONTAP Cluster in BlueXP, überprüfen Sie, ob die Cluster Mindestanforderungen erfüllen, und passen Sie die Netzwerkeinstellungen für die Verbindung der Cluster mit Azure an.

Informieren Sie sich, wie Sie Ihre ONTAP Cluster vorbereiten.

Azure Blob als Backup-Ziel vorbereiten

Richten Sie Berechtigungen für den Connector ein, um den Azure Bucket zu erstellen und zu managen. Außerdem müssen Sie Berechtigungen für den lokalen ONTAP-Cluster einrichten, damit er Daten in den Azure-Bucket lesen und schreiben kann.

Optional können Sie auch Ihre eigenen benutzerdefinierten Schlüssel für die Datenverschlüsselung einrichten, ohne die standardmäßigen Azure Verschlüsselungsschlüssel verwenden zu müssen. Erfahren Sie, wie Sie Ihre Azure-Umgebung für ONTAP-Backups vorbereiten.

Aktivieren Sie Backups auf Ihren ONTAP Volumes

Wählen Sie die Arbeitsumgebung aus und klicken Sie auf **Aktivieren > Backup Volumes** neben dem Backup- und Recovery-Dienst im rechten Fenster. Folgen Sie dann dem Setup-Assistenten, um die Replikations- und Backup-Richtlinien auszuwählen, die Sie verwenden werden, und die Volumes, die Sie sichern möchten.

Aktivieren Sie Backups auf Ihren ONTAP Volumes.

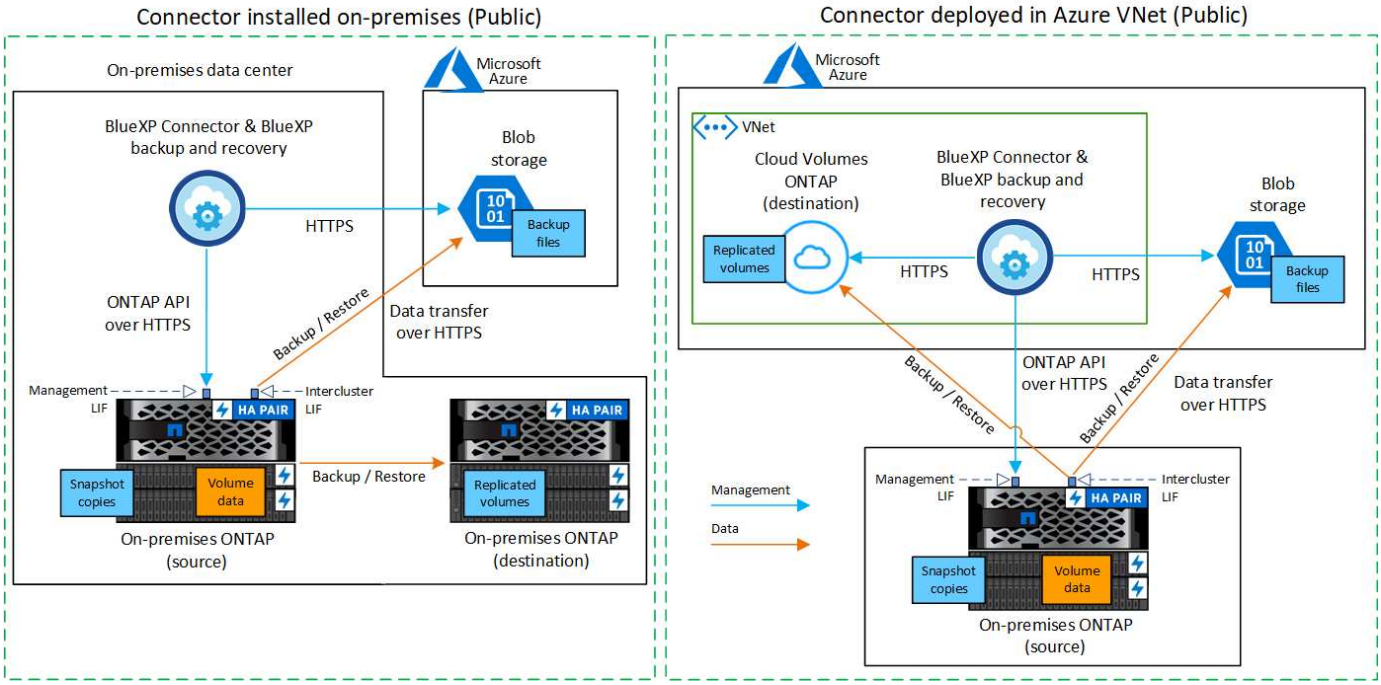
Identifizieren Sie die Verbindungsmethode

Wählen Sie aus, welche der beiden Verbindungsmethoden Sie zur Konfiguration von Backups von On-Premises-ONTAP-Systemen zu Azure Blob verwenden möchten.

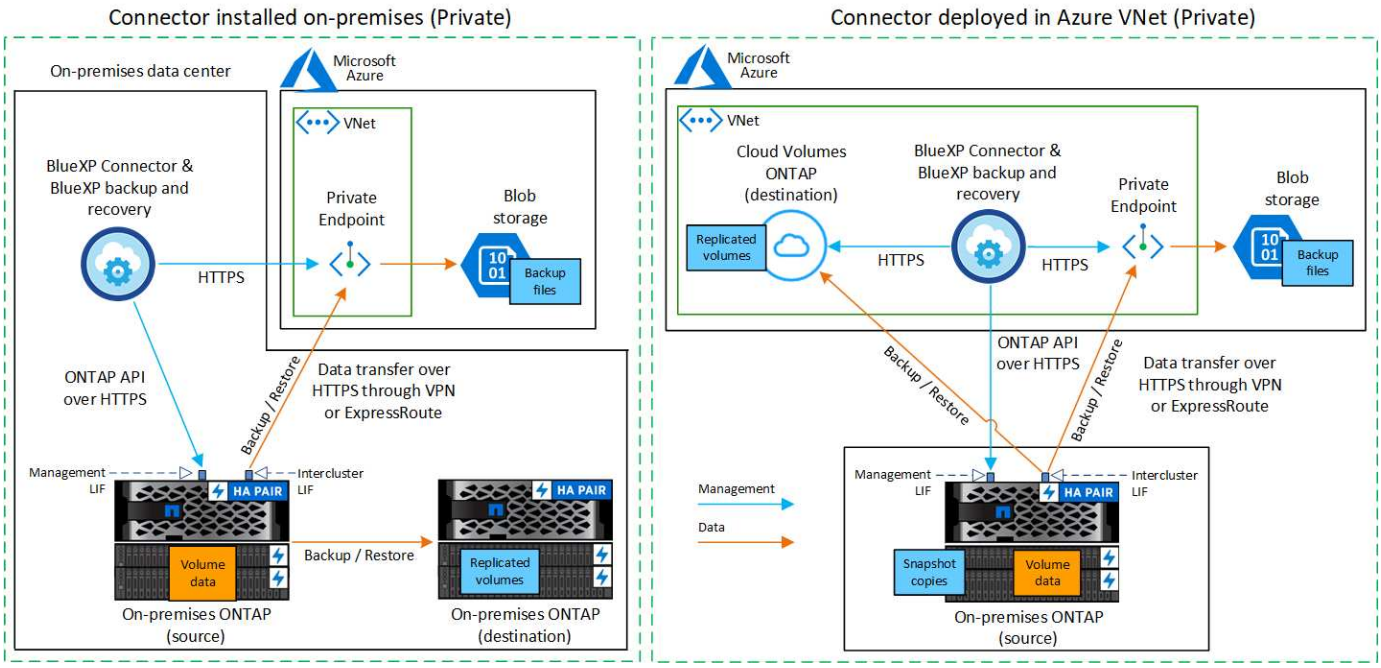
- **Öffentliche Verbindung** - direkte Verbindung des ONTAP-Systems mit Azure Blob-Speicher über einen öffentlichen Azure-Endpunkt.
- **Private Verbindung** - Verwenden Sie ein VPN oder ExpressRoute und leiten Sie den Verkehr über einen privaten vnet Endpunkt, der eine private IP-Adresse verwendet.

Optional können Sie für replizierte Volumes auch eine Verbindung zu einem sekundären ONTAP-System über eine öffentliche oder private Verbindung herstellen.

Das folgende Diagramm zeigt die Methode **Public Connection** und die Verbindungen, die Sie zwischen den Komponenten vorbereiten müssen. Verwenden Sie entweder einen Connector, den Sie an Ihrem Standort installiert haben, oder einen Connector, den Sie in Azure vnet implementiert haben.



Das folgende Diagramm zeigt die Methode **private Verbindung** und die Verbindungen, die Sie zwischen den Komponenten vorbereiten müssen. Verwenden Sie entweder einen Connector, den Sie an Ihrem Standort installiert haben, oder einen Connector, den Sie in Azure vnet implementiert haben.



Bereiten Sie Ihren BlueXP Connector vor

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

Erstellen oder Schalten von Anschlüssen

Falls Sie bereits einen Connector in Ihrem Azure vnet oder Ihrem Standort implementiert haben, sind Sie alle bereit.

Falls nicht, müssen Sie an einem dieser Standorte einen Connector erstellen, um ONTAP-Daten in Azure Blob Storage zu sichern. Sie können keinen Connector verwenden, der bei einem anderen Cloud-Provider bereitgestellt wird.

- "Erfahren Sie mehr über Steckverbinder"
- "Installieren Sie einen Connector in Azure"
- "Installieren Sie einen Connector in Ihren Räumlichkeiten"
- "Installieren Sie einen Connector in einer Azure Government-Region"

  BlueXP Backup und Recovery werden in Azure Government Regionen unterstützt, wenn der Connector in der Cloud bereitgestellt wird – und nicht dann, wenn er an Ihrem Standort installiert ist. Darüber hinaus müssen Sie den Connector über den Azure Marketplace implementieren. Sie können den Connector nicht von der BlueXP SaaS-Website in einer Regierungsregion implementieren.

Bereiten Sie die Vernetzung für den Connector vor

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 BlueXP Backup- und Recovery-Service und zu Ihrem Blob Objekt-Storage ("Siehe die Liste der Endpunkte")
- Eine HTTPS-Verbindung über Port 443 an Ihre ONTAP-Cluster-Management-LIF
- Damit die Such- und Restore-Funktion von BlueXP für Backup und Recovery funktioniert, muss Port 1433 für die Kommunikation zwischen dem Connector und den Azure Synapse SQL-Services offen sein.
- Für Implementierungen von Azure und Azure Government sind weitere Regeln für eingehende Sicherheitsgruppen erforderlich. Siehe "Regeln für den Connector in Azure" Entsprechende Details.

2. Aktivieren Sie einen privaten vnet Endpunkt zum Azure Storage. Dies ist erforderlich, wenn Sie über eine ExpressRoute oder VPN-Verbindung zwischen Ihrem ONTAP Cluster und dem vnet verfügen und Sie eine Kommunikation zwischen dem Connector und Blob Storage in Ihrem virtuellen privaten Netzwerk wünschen (eine **private**-Verbindung).

Überprüfen oder Hinzufügen von Berechtigungen zum Konnektor

Um die Such- und Wiederherstellungsfunktion für BlueXP Backup und Recovery verwenden zu können, müssen Sie in der Rolle für den Connector über bestimmte Berechtigungen verfügen, damit dieser auf den Azure Synapse Workspace und das Data Lake Storage Account zugreifen kann. Lesen Sie die unten stehenden Berechtigungen, und befolgen Sie die Schritte, wenn Sie die Richtlinie ändern müssen.

Bevor Sie beginnen

Sie müssen den Azure Synapse Analytics Resource Provider (genannt „Microsoft.Synapse“) im Abonnement registrieren. "Erfahren Sie, wie Sie diesen Ressourcenanbieter für Ihr Abonnement registrieren". Sie müssen der Subscription **Owner** oder **Contributor** sein, um den Ressourcenanbieter zu registrieren.

Schritte

1. Identifizieren Sie die Rolle, die der virtuellen Konnektor-Maschine zugewiesen ist:
   a. Öffnen Sie im Azure-Portal den Virtual Machines-Service.
   b. Wählen Sie die virtuelle Verbindungsmaschine aus.
   c. Wählen Sie unter **Einstellungen Identität**.
   d. Wählen Sie **Azure-Rollenzuweisungen** aus.
   e. Notieren Sie sich die benutzerdefinierte Rolle, die der virtuellen Connector-Maschine zugewiesen ist.
2. Aktualisieren der benutzerdefinierten Rolle:
   a. Öffnen Sie im Azure-Portal Ihr Azure-Abonnement.
   b. Wählen Sie **Zugriffskontrolle (IAM) > Rollen**.
   c. Wählen Sie die Auslassungspunkte (**…**) für die benutzerdefinierte Rolle aus und wählen Sie dann **Bearbeiten**.
   d. Wählen Sie **JSON** und fügen Sie die folgenden Berechtigungen hinzu:

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"Zeigen Sie das vollständige JSON-Format für die Richtlinie an"

e. Wählen Sie **Überprüfen + Aktualisieren** und dann **Aktualisieren**.

Lizenzanforderungen prüfen

Lizenzanforderungen müssen sowohl für Azure als auch für BlueXP geprüft werden:

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

Unterstützte Regionen

Sie können in allen Regionen, einschließlich Azure Government-Regionen, Sicherungen von lokalen Systemen in Azure Blob erstellen. Sie geben die Region an, in der die Backups beim Einrichten des Dienstes gespeichert werden sollen.

Bereiten Sie Ihre ONTAP-Cluster vor

Sie müssen Ihr On-Premises-Quell-ONTAP-System und alle sekundären lokalen ONTAP oder Cloud Volumes ONTAP Systeme vorbereiten.

Zur Vorbereitung Ihrer ONTAP-Cluster sind folgende Schritte erforderlich:

- Ihre ONTAP-Systeme in BlueXP erkennen
- Überprüfen Sie die Systemanforderungen für ONTAP
- ONTAP Netzwerkanforderungen für Daten-Backups im Objekt-Storage prüfen
- Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes

Ihre ONTAP-Systeme in BlueXP erkennen

Sowohl das On-Premises-Quell-ONTAP-System als auch alle sekundären ONTAP- oder Cloud Volumes ONTAP-Systeme vor Ort müssen auf der BlueXP Leinwand verfügbar sein.

Sie müssen die Cluster-Management-IP-Adresse und das Passwort kennen, mit dem das Admin-Benutzerkonto den Cluster hinzufügen kann.
"Entdecken Sie ein Cluster".

Überprüfen Sie die Systemanforderungen für ONTAP

Stellen Sie sicher, dass die folgenden ONTAP-Anforderungen erfüllt sind:

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

  Hinweis: das „Hybrid Cloud Bundle“ ist bei Backup und Recovery von BlueXP nicht erforderlich.

Erfahren Sie, wie Sie "Management Ihrer Cluster-Lizenzen".

- Zeit und Zeitzone sind korrekt eingestellt. Erfahren Sie, wie Sie "Konfigurieren Sie die Cluster-Zeit".
- Wenn Sie Daten replizieren möchten, sollten Sie vor der Replizierung von Daten überprüfen, ob auf den Quell- und Zielsystemen kompatible ONTAP-Versionen ausgeführt werden.

  "Zeigen Sie kompatible ONTAP Versionen für SnapMirror Beziehungen an".

ONTAP Netzwerkanforderungen für Daten-Backups im Objekt-Storage prüfen

Sie müssen die folgenden Anforderungen auf dem System konfigurieren, das eine Verbindung zu Objekt-Storage herstellt.

- Konfigurieren Sie für eine Fan-out-Backup-Architektur die folgenden Einstellungen auf dem *primary* -System.
- Konfigurieren Sie für eine kaskadierte Backup-Architektur die folgenden Einstellungen auf dem *Secondary* -System.

Die folgenden Netzwerkanforderungen für ONTAP-Cluster sind erforderlich:

- Das ONTAP Cluster initiiert eine HTTPS-Verbindung über Port 443 von der Intercluster-LIF zu Azure Blob Storage für Backup- und Restore-Vorgänge.

  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 Connector kann in einem Azure vnet residieren.
- 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 BlueXP Backup und Recovery einrichten, werden Sie aufgefordert, den IPspace 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 LIFs der Nodes und Intercluster können auf den Objektspeicher zugreifen.
- 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 Objektspeicher zu erhalten.
- Aktualisieren Sie bei Bedarf die Firewall-Regeln, um BlueXP Backup- und Recovery-Serviceverbindungen von ONTAP zum Objekt-Storage über Port 443 und Datenverkehr der Namensauflösung von der Storage-VM zum DNS-Server über Port 53 (TCP/UDP) zu ermöglichen.

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes

Wenn Sie planen, mithilfe von BlueXP Backup und Recovery replizierte Volumes auf einem sekundären ONTAP System zu erstellen, stellen Sie sicher, dass die Quell- und Zielsysteme die folgenden Netzwerkanforderungen erfüllen.

Netzwerkanforderungen für On-Premises-ONTAP

- Wenn sich der Cluster an Ihrem Standort befindet, sollten Sie über eine Verbindung zwischen Ihrem Unternehmensnetzwerk und Ihrem virtuellen Netzwerk des Cloud-Providers verfügen. Hierbei handelt es sich in der Regel um eine VPN-Verbindung.
- ONTAP Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Cluster-Anforderungen erfüllen.

  Da Sie Daten auf Cloud Volumes ONTAP oder auf lokale Systeme replizieren können, prüfen Sie Peering-Anforderungen für lokale ONTAP Systeme. "Anzeigen von Voraussetzungen für Cluster-Peering in der ONTAP-Dokumentation".

Netzwerkanforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen ein- und ausgehenden Regeln enthalten: Speziell Regeln für ICMP und die Ports 11104 und 11105. Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.

Azure Blob als Backup-Ziel vorbereiten

1. Sie können Ihre eigenen, von Ihnen gemanagten Schlüssel zur Datenverschlüsselung im Aktivierungsassistenten verwenden und nicht die von Microsoft verwalteten Standardschlüssel verwenden. In diesem Fall müssen Sie über das Azure-Abonnement, den Namen von Key Vault und den Schlüssel verfügen. "Erfahren Sie, wie Sie Ihre eigenen Schlüssel verwenden".

   Beachten Sie, dass Backup und Recovery *Azure-Zugriffsrichtlinien* als Berechtigungsmodell unterstützt. Das rollenbasierte Berechtigungsmodell *Azure RBAC (Role-Based Access Control*) wird derzeit nicht unterstützt.

2. Wenn Sie eine sicherere Verbindung über das öffentliche Internet von Ihrem On-Prem-Datacenter zum vnet haben möchten, besteht die Möglichkeit, einen Azure Private Endpunkt im Aktivierungs-Assistenten zu konfigurieren. In diesem Fall müssen Sie vnet und Subnetz für diese Verbindung kennen. "Weitere Informationen zur Verwendung eines privaten Endpunkts finden Sie unter".

Erstellen Sie Ihr Azure Blob Storage-Konto

Standardmäßig erstellt der Service Storage-Konten für Sie. Wenn Sie Ihre eigenen Speicherkonten verwenden möchten, können Sie diese erstellen, bevor Sie den Assistenten für die Backup-Aktivierung starten und dann diese Speicherkonten im Assistenten auswählen.

"Erfahren Sie mehr über das Erstellen Ihrer eigenen Storage-Konten".

Aktivieren Sie Backups auf Ihren ONTAP Volumes

Sie können Backups jederzeit direkt aus Ihrer On-Premises-Arbeitsumgebung heraus aktivieren.

Ein Assistent führt Sie durch die folgenden wichtigen Schritte:

- die Sie sichern möchten
- Backup-Strategie definieren
- Überprüfen Sie Ihre Auswahl

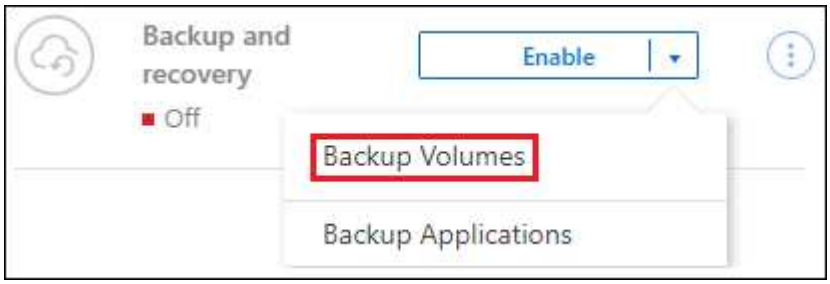
Das können Sie auch Zeigt die API-Befehle an Kopieren Sie im Überprüfungsschritt den Code, um die Backup-Aktivierung für zukünftige Arbeitsumgebungen zu automatisieren.

Starten Sie den Assistenten

Schritte

1. Greifen Sie auf eine der folgenden Arten auf den Assistenten zur Aktivierung von Backup und Recovery zu:

   - Wählen Sie auf dem BlueXP-Bildschirm die Arbeitsumgebung aus, und wählen Sie im rechten Bereich neben dem Sicherungs- und Wiederherstellungsdienst die Option **Enable > Backup Volumes** aus.



     Wenn das Azure-Ziel für Ihre Backups als Arbeitsumgebung auf dem Canvas vorhanden ist, können Sie das ONTAP-Cluster auf den Azure Blob-Objekt-Storage ziehen.

   - Wählen Sie in der Sicherungs- und Wiederherstellungsleiste **Volumes** aus. Wählen Sie auf der Registerkarte Volumes die Option **actions** aus ••• Und wählen Sie **Backup aktivieren** für ein einzelnes Volume (das noch nicht über Replikation oder Backup auf Objektspeicher verfügt).

   Auf der Seite Einführung des Assistenten werden die Schutzoptionen einschließlich lokaler Snapshots, Replikation und Backups angezeigt. Wenn Sie die zweite Option in diesem Schritt gewählt haben, wird die Seite „Backup-Strategie definieren“ mit einem ausgewählten Volume angezeigt.

2. Fahren Sie mit den folgenden Optionen fort:

   - Wenn Sie bereits einen BlueXP Connector haben, sind Sie fertig. Wählen Sie einfach **Weiter**.
   - Wenn Sie noch keinen BlueXP Connector haben, wird die Option **Connector hinzufügen** angezeigt. Siehe Bereiten Sie Ihren BlueXP Connector vor.

Wählen Sie die Volumes aus, die Sie sichern möchten

Wählen Sie die Volumes aus, die Sie schützen möchten. Ein geschütztes Volume verfügt über eine oder mehrere der folgenden Elemente: Snapshot-Richtlinie, Replizierungsrichtlinie und Richtlinie für das Backup in ein Objekt.

Sie können FlexVol- oder FlexGroup-Volumes schützen. Sie können jedoch keine Kombination dieser Volumes auswählen, wenn Sie Backups für eine funktionierende Umgebung aktivieren. Informieren Sie sich darüber "Aktivieren Sie das Backup für zusätzliche Volumes in der Arbeitsumgebung" (FlexVol oder FlexGroup), nachdem Sie das Backup für die ersten Volumes konfiguriert haben.

- Sie können ein Backup nur auf einem einzelnen FlexGroup Volume gleichzeitig aktivieren.
- Die ausgewählten Volumes müssen dieselbe SnapLock-Einstellung aufweisen. Auf allen Volumes muss SnapLock Enterprise aktiviert oder SnapLock deaktiviert sein.

Schritte

Beachten Sie, dass die Richtlinien, die Sie später auswählen, diese vorhandenen Richtlinien überschreiben, wenn die von Ihnen ausgewählten Volumes bereits Snapshot- oder Replikationsrichtlinien angewendet haben.

1. Wählen Sie auf der Seite Volumes auswählen das Volume oder die Volumes aus, die Sie schützen

möchten.

- Optional können Sie die Zeilen so filtern, dass nur Volumes mit bestimmten Volumentypen, Stilen und mehr angezeigt werden, um die Auswahl zu erleichtern.
- Nachdem Sie das erste Volume ausgewählt haben, können Sie alle FlexVol Volumes auswählen (FlexGroup Volumes können nur einzeln ausgewählt werden). Um alle vorhandenen FlexVol-Volumes zu sichern, aktivieren Sie zuerst ein Volume und dann das Kontrollkästchen in der Titelzeile. (

).
- Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume (

).

2. Wählen Sie **Weiter**.

Backup-Strategie definieren

Zur Definition der Backup-Strategie gehören die folgenden Optionen:

- Unabhängig davon, ob Sie eine oder alle Backup-Optionen: Lokale Snapshots, Replikation und Backup-to-Object-Storage möchten
- Der Netapp Architektur Sind
- Lokale Snapshot-Richtlinie
- Replikationsziel und -Richtlinie

> Wenn die ausgewählten Volumes andere Snapshot- und Replikationsrichtlinien haben als die in diesem Schritt ausgewählten Richtlinien, werden die vorhandenen Richtlinien überschrieben.

- Backup von Objekt-Storage-Informationen (Provider-, Verschlüsselungs-, Netzwerk-, Backup-Richtlinien- und Exportoptionen)

Schritte

1. Wählen Sie auf der Seite Backup-Strategie definieren eine oder alle der folgenden Optionen aus. Alle drei sind standardmäßig ausgewählt:
   - **Lokale Snapshots**: Wenn Sie eine Replikation oder Sicherung auf Objektspeicher durchführen, müssen lokale Snapshots erstellt werden.
   - **Replikation**: Erstellt replizierte Volumes auf einem anderen ONTAP-Speichersystem.
   - **Backup**: Sichert Volumes auf Objektspeicher.
2. **Architektur**: Wenn Sie Replikation und Backup gewählt haben, wählen Sie einen der folgenden Informationsflüsse:
   - **Kaskadierung**: Informationsflüsse vom primären zum sekundären und vom sekundären zum Objektspeicher.
   - **Fan Out**: Informationen fließen vom primären zum sekundären *und* vom primären zum Objektspeicher.

   Einzelheiten zu diesen Architekturen finden Sie unter "Planen Sie Ihren Weg zum Schutz".
3. **Lokaler Snapshot**: Wählen Sie eine vorhandene Snapshot-Richtlinie aus oder erstellen Sie eine neue.

> Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung des Snapshots finden Sie unter "Erstellen einer Richtlinie".

Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

- Geben Sie den Namen der Richtlinie ein.
- Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
- Wählen Sie **Erstellen**.

4. **Replikation**: Stellen Sie die folgenden Optionen ein:
   - **Replikationsziel**: Wählen Sie die Zielarbeitsumgebung und SVM aus. Wählen Sie optional das Zielaggregat oder die Aggregate und das Präfix oder Suffix aus, die dem Namen des replizierten Volumes hinzugefügt werden sollen.
   - **Replikationsrichtlinie**: Wählen Sie eine vorhandene Replikationsrichtlinie oder erstellen Sie eine neue.

     Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Replikation finden Sie unter "Erstellen einer Richtlinie".

     Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

     - Geben Sie den Namen der Richtlinie ein.
     - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
     - Wählen Sie **Erstellen**.
5. **Backup auf Objekt**: Wenn Sie **Backup** ausgewählt haben, stellen Sie die folgenden Optionen ein:
   - **Provider**: Wählen Sie **Microsoft Azure**.
   - **Provider-Einstellungen**: Geben Sie die Provider-Details und die Region ein, in der die Backups gespeichert werden sollen.

     Erstellen Sie entweder ein neues Storage-Konto oder wählen Sie ein vorhandenes aus.

     Erstellen Sie entweder Ihre eigene Ressourcengruppe, die den Blob-Container verwaltet, oder wählen Sie den Typ und die Gruppe der Ressourcengruppe aus.

     Wenn Sie Ihre Backup-Dateien vor Änderung oder Löschung schützen möchten, stellen Sie sicher, dass das Storage-Konto mit aktiviertem unveränderlichem Storage erstellt wurde und eine Aufbewahrungsfrist von 30 Tagen verwendet wird.

     Wenn Sie zur weiteren Kostenoptimierung ältere Backup-Dateien in Azure Archivspeicher verschieben möchten, stellen Sie sicher, dass das Speicherkonto über die entsprechende Lebenszyklusregel verfügt.
   - **Verschlüsselungsschlüssel**: Wenn Sie ein neues Azure-Speicherkonto erstellt haben, geben Sie die Schlüsselinformationen des Verschlüsselungsschlüssels ein, die Sie vom Provider erhalten haben. Wählen Sie aus, ob Sie die Azure Standardschlüssel verwenden oder Ihre eigenen vom Kunden verwalteten Schlüssel aus Ihrem Azure Konto auswählen werden, um die Verschlüsselung Ihrer Daten zu managen.

     Wenn Sie Ihre eigenen vom Kunden verwalteten Schlüssel verwenden möchten, geben Sie den Schlüsselspeicher und die Schlüsselinformationen ein.

Wenn Sie ein vorhandenes Microsoft Storage-Konto ausgewählt haben, sind Verschlüsselungsinformationen bereits verfügbar. Sie müssen es daher jetzt nicht eingeben.

- **Netzwerk**: Wählen Sie den IPspace und ob Sie einen privaten Endpunkt verwenden. Der private Endpunkt ist standardmäßig deaktiviert.
  i. 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.
  ii. Wählen Sie optional aus, ob Sie einen zuvor konfigurierten privaten Azure-Endpunkt verwenden möchten. "Informieren Sie sich über die Verwendung eines privaten Azure Endpunkts".
- **Backup Policy**: Wählen Sie eine vorhandene Richtlinie für das Objekt-Storage-Backup aus oder erstellen Sie eine neue.

  Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Sicherung finden Sie unter "Erstellen einer Richtlinie".

  Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

  - Geben Sie den Namen der Richtlinie ein.
  - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
  - Legen Sie für Backup-to-Object-Richtlinien die Einstellungen für DataLock und Ransomware-Schutz fest. Weitere Informationen zu DataLock und Ransomware-Schutz finden Sie unter "Richtlinieneinstellungen für Backup-to-Object".
  - Wählen Sie **Erstellen**.
- **Exportieren vorhandener Snapshot-Kopien als Backup-Kopien in den Objektspeicher**: Wenn es lokale Snapshot-Kopien für Volumes in dieser Arbeitsumgebung gibt, die mit dem Backup-Zeitplan-Label übereinstimmen, das Sie gerade für diese Arbeitsumgebung ausgewählt haben (z. B. täglich, wöchentlich usw.), wird diese zusätzliche Eingabeaufforderung angezeigt. Aktivieren Sie dieses Kontrollkästchen, damit alle historischen Snapshots als Backup-Dateien in den Objektspeicher kopiert werden, um einen möglichst vollständigen Schutz für Ihre Volumes zu gewährleisten.

6. Wählen Sie **Weiter**.

Überprüfen Sie Ihre Auswahl

Dies ist die Möglichkeit, Ihre Auswahl zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

Schritte

1. Überprüfen Sie auf der Seite „Überprüfen“ Ihre Auswahl.
2. Aktivieren Sie optional das Kontrollkästchen, um * die Snapshot-Policy-Labels automatisch mit den Label der Replikations- und Backup-Policy* zu synchronisieren. Dadurch werden Snapshots mit einem Label erstellt, das den Labels in den Replizierungs- und Backup-Richtlinien entspricht.
3. Wählen Sie **Sicherung Aktivieren**.

Ergebnis

Mit BlueXP Backup und Recovery werden erste Backups Ihrer Volumes erstellt. Der Basistransfer des replizierten Volumes und der Backup-Datei beinhaltet eine vollständige Kopie der Daten des primären Storage-Systems. Nachfolgende Transfers enthalten differenzielle Kopien der primären Storage-System-Daten in

Snapshot Kopien.

Ein repliziertes Volume wird im Zielcluster erstellt, das mit dem primären Volume synchronisiert wird.

In der von Ihnen eingegebenen Ressourcengruppe wird ein Blob-Speicherkonto erstellt und die Backup-Dateien dort gespeichert. 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".

Zeigt die API-Befehle an

Möglicherweise möchten Sie die API-Befehle anzeigen und optional kopieren, die im Assistenten Sicherung und Wiederherstellung aktivieren verwendet werden. Dies ist möglicherweise sinnvoll, um die Backup-Aktivierung in zukünftigen Arbeitsumgebungen zu automatisieren.

Schritte

1. Wählen Sie im Assistenten Backup und Recovery aktivieren **API-Anforderung anzeigen** aus.
2. Um die Befehle in die Zwischenablage zu kopieren, wählen Sie das Symbol **Kopieren**.

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 unter anderem die Änderung der verfügbaren Netzwerkbandbreite für das Hochladen von Backups in den Objekt-Storage, die Änderung der automatischen Backup-Einstellung für zukünftige Volumes.
- Das können Sie auch "Wiederherstellung von Volumes, Ordnern oder einzelnen Dateien aus einer Sicherungsdatei" Zu einem Cloud Volumes ONTAP System in Azure oder zu einem ONTAP System vor Ort.

Sichern Sie lokale ONTAP-Daten mit BlueXP Backup und Recovery in Google Cloud Storage

Führen Sie einige Schritte in der Sicherung und Wiederherstellung von BlueXP durch, um mit der Sicherung von Volume-Daten von Ihren primären ONTAP-Systemen vor Ort auf ein sekundäres Speichersystem und in Google Cloud Storage zu beginnen.

„On-Premises ONTAP Systeme“ umfassen FAS, AFF und ONTAP Select Systeme.

Schnellstart

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

Identifizieren Sie die Verbindungsmethode, die Sie verwenden werden

Sie können entscheiden, ob Sie Ihren lokalen ONTAP Cluster über das öffentliche Internet direkt mit Google Cloud Storage verbinden oder ob Sie ein VPN oder Google Cloud Interconnect verwenden und den Datenverkehr über eine private Google Access-Schnittstelle leiten werden, die eine private IP-Adresse verwendet.

Bereiten Sie Ihren BlueXP Connector vor

Wenn Sie bereits einen Connector in Ihrer Google Cloud Platform VPC implementiert haben, sind Sie alle festgelegt. Falls nicht, müssen Sie einen BlueXP Connector erstellen, um ONTAP Daten auf Google Cloud Storage zu sichern. Außerdem müssen Sie die Netzwerkeinstellungen für den Connector anpassen, damit eine Verbindung zu Google Cloud hergestellt werden kann.

Bereiten Sie die Vernetzung für den Connector vor

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

Überprüfen Sie die Lizenzanforderungen

Prüfen Sie die Lizenzanforderungen sowohl für Google Cloud als auch für BlueXP.

Bereiten Sie Ihre ONTAP-Cluster vor

Erkennen Sie Ihre ONTAP Cluster in BlueXP, überprüfen Sie, ob die Cluster Mindestanforderungen erfüllen, und passen Sie Netzwerkeinstellungen für die Verbindung der Cluster mit Google Cloud an.

Google Cloud als Backup-Ziel vorbereiten

Richten Sie Berechtigungen für den Connector ein, um den Google Cloud-Bucket zu erstellen und zu managen. Sie müssen außerdem Berechtigungen für den lokalen ONTAP-Cluster einrichten, damit dieser Daten in den Google Cloud-Bucket lesen und schreiben kann.

Optional können Sie für die Datenverschlüsselung eigene benutzerdefinierte gemanagte Schlüssel einrichten, ohne die Standardschlüssel von Google Cloud zu verwenden.

Aktivieren Sie Backups auf Ihren ONTAP Volumes

Wählen Sie die Arbeitsumgebung aus und klicken Sie auf **Aktivieren > Backup Volumes** neben dem Backup- und Recovery-Dienst im rechten Fenster. Folgen Sie dann dem Setup-Assistenten, um die Replikations- und Backup-Richtlinien auszuwählen, die Sie verwenden werden, und die Volumes, die Sie sichern möchten.

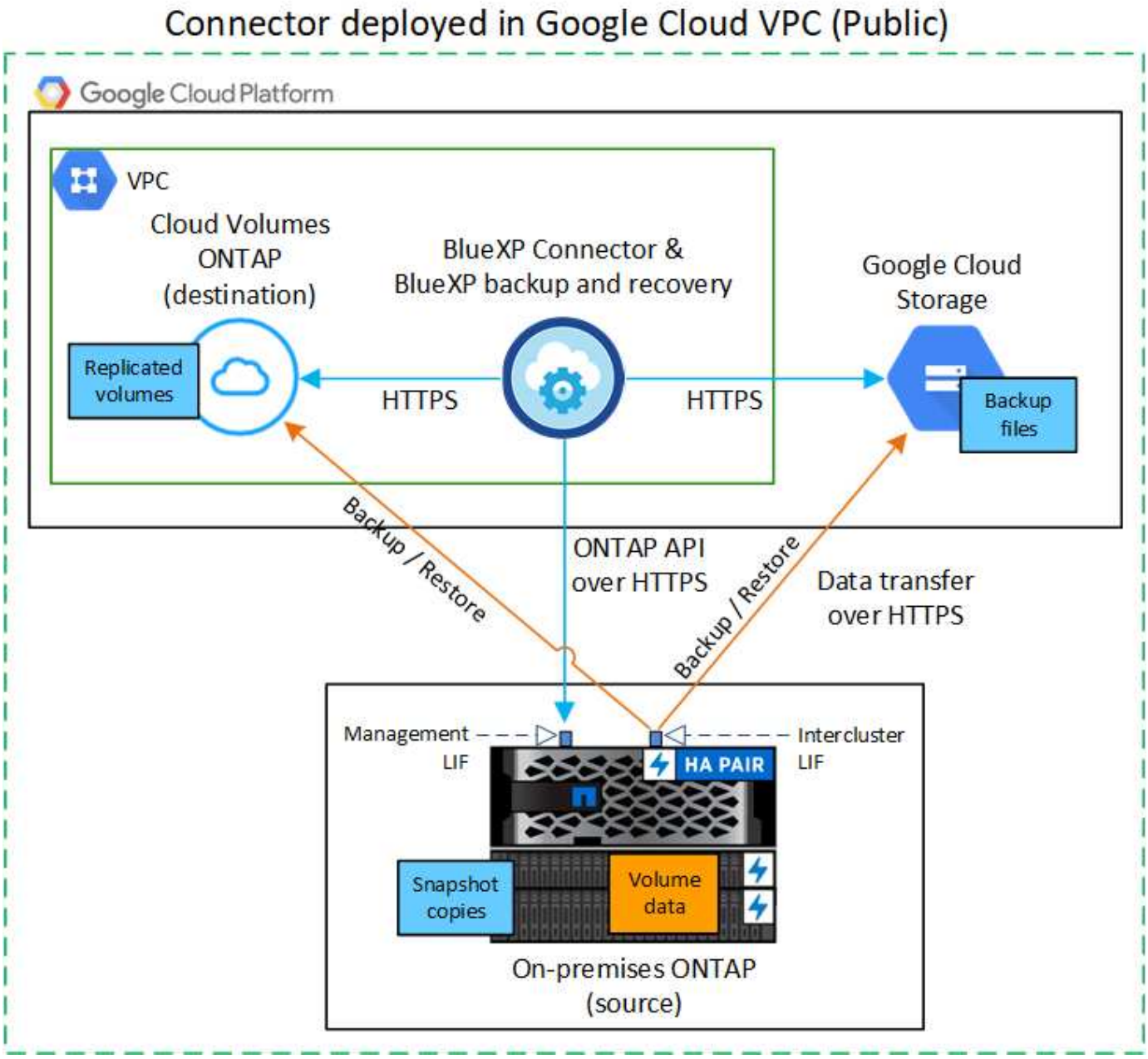
Identifizieren Sie die Verbindungsmethode

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

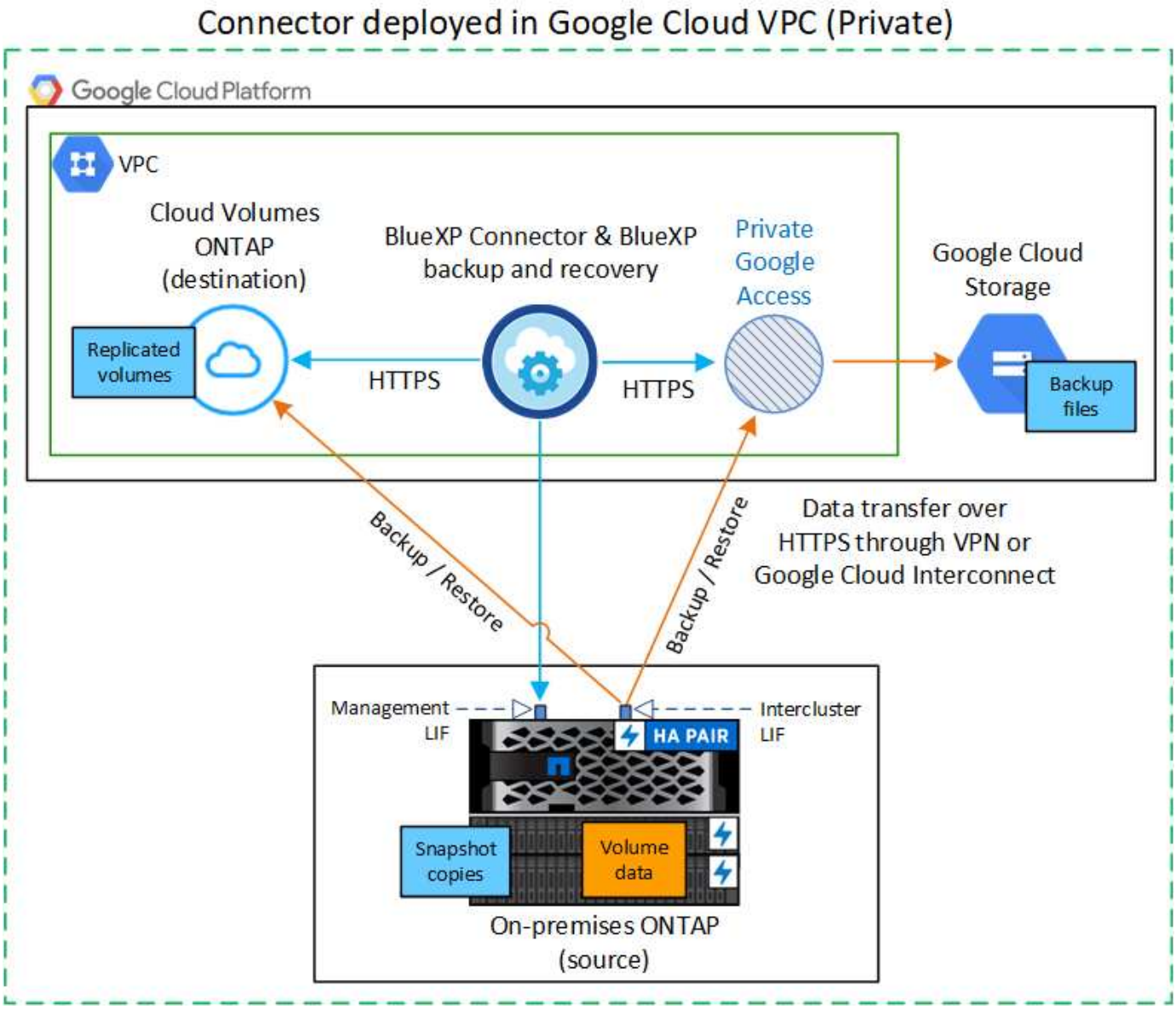
- **Öffentliche Verbindung** - direkte Verbindung des ONTAP-Systems mit Google Cloud-Speicher über einen öffentlichen Google-Endpunkt.
- **Private Verbindung** - Verwenden Sie ein VPN oder Google Cloud Interconnect und leiten Sie den Datenverkehr über eine private Google Access-Schnittstelle, die eine private IP-Adresse verwendet.

Optional können Sie für replizierte Volumes auch eine Verbindung zu einem sekundären ONTAP-System über eine öffentliche oder private Verbindung herstellen.

Das folgende Diagramm zeigt die Methode **Public Connection** und die Verbindungen, die Sie zwischen den Komponenten vorbereiten müssen. Der Connector muss in der Google Cloud Platform VPC implementiert werden.



Das folgende Diagramm zeigt die Methode **private Verbindung** und die Verbindungen, die Sie zwischen den Komponenten vorbereiten müssen. Der Connector muss in der Google Cloud Platform VPC implementiert werden.



Bereiten Sie Ihren BlueXP Connector vor

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

Erstellen oder Schalten von Anschlüssen

Wenn Sie bereits einen Connector in Ihrer Google Cloud Platform VPC implementiert haben, sind Sie alle festgelegt.

Falls nicht, müssen Sie an diesem Speicherort einen Connector erstellen, um ONTAP-Daten in Google Cloud Storage zu sichern. Es kann kein Connector verwendet werden, der bei einem anderen Cloud-Provider oder vor Ort implementiert wird.

- "Erfahren Sie mehr über Steckverbinder"
- "Installieren Sie einen Connector in GCP"

Bereiten Sie die Vernetzung für den Connector vor

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 BlueXP Backup- und Recovery-Service und zu Ihrem Google Cloud Storage ("Siehe die Liste der Endpunkte")
   - Eine HTTPS-Verbindung über Port 443 an Ihre ONTAP-Cluster-Management-LIF
2. Aktivieren Sie den privaten Google-Zugang (oder Private Service Connect) im Subnetz, in dem Sie den Connector bereitstellen möchten. "Privater Zugriff Auf Google" Oder "Private Service Connect" Sind erforderlich, wenn Sie eine direkte Verbindung von Ihrem ONTAP Cluster zur VPC haben und Sie die Kommunikation zwischen dem Connector und Google Cloud Storage in Ihrem virtuellen privaten Netzwerk (eine **private** Verbindung) wünschen.

   Befolgen Sie die Anweisungen von Google, um diese privaten Zugangsoptionen einzurichten. Stellen Sie sicher, dass Ihre DNS-Server so konfiguriert wurden `www.googleapis.com` Und `storage.googleapis.com` An die korrekten internen (privaten) IP-Adressen.

Überprüfen oder Hinzufügen von Berechtigungen zum Konnektor

Um die „Suchen & Wiederherstellen“-Funktion von BlueXP für Backup und Recovery nutzen zu können, müssen Sie in der Rolle für den Connector bestimmte Berechtigungen besitzen, damit dieser auf den Google Cloud BigQuery Service zugreifen kann. Überprüfen Sie die unten aufgeführten Berechtigungen, und befolgen Sie die Schritte, wenn Sie die Richtlinie ändern müssen.

Schritte

1. Im "Google Cloud Console", Gehen Sie zur Seite **Rollen**.
2. Wählen Sie in der Dropdown-Liste oben auf der Seite das Projekt oder die Organisation aus, das die Rolle enthält, die Sie bearbeiten möchten.
3. Wählen Sie eine benutzerdefinierte Rolle aus.
4. Wählen Sie **Rolle bearbeiten**, um die Berechtigungen der Rolle zu aktualisieren.
5. Wählen Sie **Berechtigungen hinzufügen**, um der Rolle die folgenden neuen Berechtigungen hinzuzufügen.

```
bigquery.jobs.get
bigquery.jobs.list
bigquery.jobs.listAll
bigquery.datasets.create
bigquery.datasets.get
bigquery.jobs.create
bigquery.tables.get
bigquery.tables.getData
bigquery.tables.list
bigquery.tables.create
```

6. Wählen Sie **Update**, um die bearbeitete Rolle zu speichern.

Lizenzanforderungen prüfen

- Bevor Sie BlueXP Backup und Recovery für Ihr Cluster aktivieren können, müssen Sie entweder ein PAYGO-Angebot (Pay-as-you-go) für BlueXP Marketplace von Google abonnieren oder eine BYOL-Lizenz für BlueXP Backup und Recovery von NetApp erwerben und aktivieren. Diese Lizenzen sind für Ihr Konto und können für mehrere Systeme verwendet werden.
  - Für die BlueXP PAYGO-Lizenzierung für Backup und Recovery benötigen Sie ein Abonnement des "NetApp BlueXP Angebot über Google Marketplace". Die Abrechnung für BlueXP Backup und Recovery erfolgt über dieses Abonnement.
  - Für die BYOL-Lizenzierung für BlueXP Backup und Recovery benötigen Sie die Seriennummer von NetApp, anhand derer Sie den Service für die Dauer und Kapazität der Lizenz nutzen können. "Erfahren Sie, wie Sie Ihre BYOL-Lizenzen managen".
- Sie benötigen ein Google-Abonnement für den Objekt-Speicherplatz, in dem Ihre Backups gespeichert werden.

Unterstützte Regionen

Sie können in allen Regionen Backups von lokalen Systemen in Google Cloud Storage erstellen. Sie geben die Region an, in der Backups beim Einrichten des Dienstes gespeichert werden sollen.

Bereiten Sie Ihre ONTAP-Cluster vor

Sie müssen Ihr On-Premises-Quell-ONTAP-System und alle sekundären lokalen ONTAP oder Cloud Volumes ONTAP Systeme vorbereiten.

Zur Vorbereitung Ihrer ONTAP-Cluster sind folgende Schritte erforderlich:

- Ihre ONTAP-Systeme in BlueXP erkennen
- Überprüfen Sie die Systemanforderungen für ONTAP
- ONTAP Netzwerkanforderungen für Daten-Backups im Objekt-Storage prüfen
- Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes

Ihre ONTAP-Systeme in BlueXP erkennen

Sowohl das On-Premises-Quell-ONTAP-System als auch alle sekundären ONTAP- oder Cloud Volumes ONTAP-Systeme vor Ort müssen auf der BlueXP Leinwand verfügbar sein.

Sie müssen die Cluster-Management-IP-Adresse und das Passwort kennen, mit dem das Admin-Benutzerkonto den Cluster hinzufügen kann.
"Entdecken Sie ein Cluster".

Überprüfen Sie die Systemanforderungen für ONTAP

Stellen Sie sicher, dass die folgenden ONTAP-Anforderungen erfüllt sind:

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

  Hinweis: das „Hybrid Cloud Bundle“ ist bei Backup und Recovery von BlueXP nicht erforderlich.

Erfahren Sie, wie Sie "Management Ihrer Cluster-Lizenzen".

- Zeit und Zeitzone sind korrekt eingestellt. Erfahren Sie, wie Sie "Konfigurieren Sie die Cluster-Zeit".
- Wenn Sie Daten replizieren möchten, sollten Sie vor der Replizierung von Daten überprüfen, ob auf den Quell- und Zielsystemen kompatible ONTAP-Versionen ausgeführt werden.

  "Zeigen Sie kompatible ONTAP Versionen für SnapMirror Beziehungen an".

ONTAP Netzwerkanforderungen für Daten-Backups im Objekt-Storage prüfen

Sie müssen die folgenden Anforderungen auf dem System konfigurieren, das eine Verbindung zu Objekt-Storage herstellt.

- Konfigurieren Sie für eine Fan-out-Backup-Architektur die folgenden Einstellungen auf dem *primary* -System.
- Konfigurieren Sie für eine kaskadierte Backup-Architektur die folgenden Einstellungen auf dem *Secondary* -System.

Die folgenden Netzwerkanforderungen für ONTAP-Cluster sind erforderlich:

- Der ONTAP Cluster initiiert für Backup- und Restore-Vorgänge eine HTTPS-Verbindung über Port 443 von der Intercluster LIF zu Google Cloud Storage.

  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 Connector kann in einer Google Cloud Platform VPC residieren.
- 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 BlueXP Backup und Recovery einrichten, werden Sie aufgefordert, den IPspace 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.
- 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 privaten Google Access oder Private Service Connect verwenden, stellen Sie sicher, dass Ihre DNS-Server so konfiguriert wurden, dass sie Punkt `storage.googleapis.com` An die richtige interne (private) IP-Adresse.

- 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 ggf. die Firewall-Regeln, um BlueXP Backup- und Recovery-Verbindungen von ONTAP zu Objekt-Storage über Port 443 und Datenverkehr der Namensauflösung von der Storage-VM zum DNS-Server über Port 53 (TCP/UDP) zu ermöglichen.

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes

Wenn Sie planen, mithilfe von BlueXP Backup und Recovery replizierte Volumes auf einem sekundären ONTAP System zu erstellen, stellen Sie sicher, dass die Quell- und Zielsysteme die folgenden Netzwerkanforderungen erfüllen.

Netzwerkanforderungen für On-Premises-ONTAP

- Wenn sich der Cluster an Ihrem Standort befindet, sollten Sie über eine Verbindung zwischen Ihrem Unternehmensnetzwerk und Ihrem virtuellen Netzwerk des Cloud-Providers verfügen. Hierbei handelt es sich in der Regel um eine VPN-Verbindung.
- ONTAP Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Cluster-Anforderungen erfüllen.

  Da Sie Daten auf Cloud Volumes ONTAP oder auf lokale Systeme replizieren können, prüfen Sie Peering-Anforderungen für lokale ONTAP Systeme. "Anzeigen von Voraussetzungen für Cluster-Peering in der ONTAP-Dokumentation".

Netzwerkanforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen ein- und ausgehenden Regeln enthalten: Speziell Regeln für ICMP und die Ports 11104 und 11105. Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.

Google Cloud Storage als Backup-Ziel vorbereiten

Die Vorbereitung von Google Cloud Storage als Backup-Ziel beinhaltet folgende Schritte:

- Richten Sie Berechtigungen ein.
- (Optional) Erstellen Sie Ihre eigenen Buckets. (Der Service erstellt Buckets für Sie, wenn Sie möchten.)
- (Optional) Einrichten von vom Kunden gemanagten Schlüsseln für die Datenverschlüsselung

Berechtigungen einrichten

Sie müssen Speicherzugriffsschlüssel für ein Dienstkonto bereitstellen, das über bestimmte Berechtigungen mit einer benutzerdefinierten Rolle verfügt. Ein Servicekonto ermöglicht BlueXP Backup und Recovery für Authentifizierung und Zugriff auf Cloud Storage Buckets, die für das Speichern von Backups verwendet werden. Die Schlüssel sind erforderlich, damit Google Cloud Storage weiß, wer die Anfrage stellt.

Schritte

1. Im "Google Cloud Console", Gehen Sie zur Seite **Rollen**.
2. "Erstellen Sie eine neue Rolle" Mit folgenden Berechtigungen:

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. In der Google Cloud Konsole "Rufen Sie die Seite Servicekonten auf".
4. Wählen Sie Ihr Cloud-Projekt aus.
5. Wählen Sie **Service-Konto erstellen** und geben Sie die erforderlichen Informationen ein:
   a. **Service Account Details**: Geben Sie einen Namen und eine Beschreibung ein.
   b. **Bewilligung dieses Servicekontos Zugriff auf Projekt**: Wählen Sie die benutzerdefinierte Rolle aus, die Sie gerade erstellt haben.
   c. Wählen Sie * Fertig*.
6. Gehen Sie zu "GCP-Speichereinstellungen" Außerdem Zugriffsschlüssel für das Servicekonto erstellen:
   a. Wählen Sie ein Projekt aus, und wählen Sie **Interoperabilität**. Wenn Sie dies noch nicht getan haben, wählen Sie **Zugriff auf Interoperabilität aktivieren**.
   b. Wählen Sie unter **Zugriffsschlüssel für Dienstkonten Schlüssel für ein Dienstkonto erstellen** aus, wählen Sie das soeben erstellte Dienstkonto aus und klicken Sie auf **Schlüssel erstellen**.

      Beim Konfigurieren des Backup-Service müssen Sie die Schlüssel zu einem späteren Zeitpunkt in BlueXP Backup und Recovery eingeben.

Erstellen Sie Ihre eigenen Buckets

Standardmäßig erstellt der Service Buckets für Sie. Wenn Sie Ihre eigenen Buckets verwenden möchten, können Sie diese auch erstellen, bevor Sie den Assistenten zur Backup-Aktivierung starten und diese Buckets im Assistenten auswählen.

"Erfahren Sie mehr über das Erstellen eigener Buckets".

Einrichtung von CMEK (Customer Managed Encryption Keys) für die Datenverschlüsselung

Sie können Ihre eigenen, von Kunden gemanagten Schlüssel zur Datenverschlüsselung verwenden, statt die von Google standardmäßig gemanagten Verschlüsselungsschlüssel zu verwenden. Sowohl regionsübergreifende als auch projektübergreifende Schlüssel werden unterstützt, sodass Sie ein Projekt für einen Bucket auswählen können, der sich vom Projekt des CMEK-Schlüssels unterscheidet.

Wenn Sie planen, Ihre eigenen kundenverwalteten Schlüssel zu verwenden:

- Sie benötigen den Schlüsselring und den Schlüsselnamen, damit Sie diese Informationen im Aktivierungsassistenten hinzufügen können. "Erfahren Sie mehr über vom Kunden verwaltete Verschlüsselungsschlüssel".
- Sie müssen überprüfen, ob diese erforderlichen Berechtigungen in der Rolle für den Connector enthalten sind:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Sie müssen überprüfen, ob die Google API „Cloud Key Management Service (KMS)“ in Ihrem Projekt aktiviert ist. Siehe "Google Cloud-Dokumentation: Aktivieren von APIs" Entsprechende Details.

CMEK-Überlegungen:

- Sowohl HSM (Hardware-Backed) als auch Software-generierte Schlüssel werden unterstützt.
- Es werden sowohl neu erstellte als auch importierte Cloud KMS-Schlüssel unterstützt.
- Es werden nur regionale Schlüssel unterstützt, globale Schlüssel werden nicht unterstützt.
- Derzeit wird nur der Zweck „symmetrische Verschlüsselung/Entschlüsselung“ unterstützt.
- Der dem Storage-Konto zugeordnete Service-Agent wird der IAM-Rolle „CryptoKey Encrypter/Decrypter (Rollen/Cloudkms.cryptoKeyEncrypterDecrypter)“ von BlueXP Backup und Recovery zugewiesen.

Aktivieren Sie Backups auf Ihren ONTAP Volumes

Sie können Backups jederzeit direkt aus Ihrer On-Premises-Arbeitsumgebung heraus aktivieren.

Ein Assistent führt Sie durch die folgenden wichtigen Schritte:

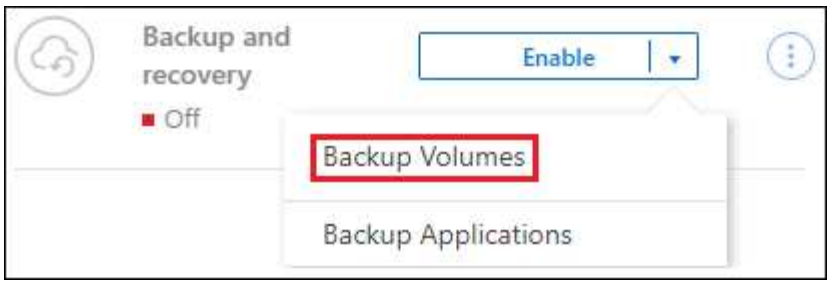
- die Sie sichern möchten
- Backup-Strategie definieren
- Überprüfen Sie Ihre Auswahl

Das können Sie auch Zeigt die API-Befehle an Kopieren Sie im Überprüfungsschritt den Code, um die Backup-Aktivierung für zukünftige Arbeitsumgebungen zu automatisieren.

Starten Sie den Assistenten

Schritte

1. Greifen Sie auf eine der folgenden Arten auf den Assistenten zur Aktivierung von Backup und Recovery zu:
    - Wählen Sie auf dem BlueXP-Bildschirm die Arbeitsumgebung aus, und wählen Sie im rechten Bereich neben dem Sicherungs- und Wiederherstellungsdienst die Option **Enable > Backup Volumes** aus.



Wenn das Google Cloud Storage-Ziel für Ihre Backups als Arbeitsumgebung auf dem Canvas vorhanden ist, können Sie das ONTAP-Cluster auf den Google Cloud-Objektspeicher ziehen.

- Wählen Sie in der Sicherungs- und Wiederherstellungsleiste **Volumes** aus. Wählen Sie auf der Registerkarte Volumes die Option **actions** aus ••• Und wählen Sie **Backup aktivieren** für ein einzelnes Volume (das noch nicht über Replikation oder Backup auf Objektspeicher verfügt). .

Auf der Seite Einführung des Assistenten werden die Schutzoptionen einschließlich lokaler Snapshots, Replikation und Backups angezeigt. Wenn Sie die zweite Option in diesem Schritt gewählt haben, wird die Seite „Backup-Strategie definieren“ mit einem ausgewählten Volume angezeigt.

2. Fahren Sie mit den folgenden Optionen fort:
   - Wenn Sie bereits einen BlueXP Connector haben, sind Sie fertig. Wählen Sie einfach **Weiter**.
   - Wenn Sie noch keinen BlueXP Connector haben, wird die Option **Connector hinzufügen** angezeigt. Siehe Bereiten Sie Ihren BlueXP Connector vor.

Wählen Sie die Volumes aus, die Sie sichern möchten

Wählen Sie die Volumes aus, die Sie schützen möchten. Ein geschütztes Volume verfügt über eine oder mehrere der folgenden Elemente: Snapshot-Richtlinie, Replizierungsrichtlinie und Richtlinie für das Backup in ein Objekt.

Sie können FlexVol- oder FlexGroup-Volumes schützen. Sie können jedoch keine Kombination dieser Volumes auswählen, wenn Sie Backups für eine funktionierende Umgebung aktivieren. Informieren Sie sich darüber "Aktivieren Sie das Backup für zusätzliche Volumes in der Arbeitsumgebung" (FlexVol oder FlexGroup), nachdem Sie das Backup für die ersten Volumes konfiguriert haben.

- Sie können ein Backup nur auf einem einzelnen FlexGroup Volume gleichzeitig aktivieren.
- Die ausgewählten Volumes müssen dieselbe SnapLock-Einstellung aufweisen. Auf allen Volumes muss SnapLock Enterprise aktiviert oder SnapLock deaktiviert sein.

Schritte

Beachten Sie, dass die Richtlinien, die Sie später auswählen, diese vorhandenen Richtlinien überschreiben, wenn die von Ihnen ausgewählten Volumes bereits Snapshot- oder Replikationsrichtlinien angewendet haben.

1. Wählen Sie auf der Seite Volumes auswählen das Volume oder die Volumes aus, die Sie schützen möchten.
   - Optional können Sie die Zeilen so filtern, dass nur Volumes mit bestimmten Volumentypen, Stilen und mehr angezeigt werden, um die Auswahl zu erleichtern.
   - Nachdem Sie das erste Volume ausgewählt haben, können Sie alle FlexVol Volumes auswählen (FlexGroup Volumes können nur einzeln ausgewählt werden). Um alle vorhandenen FlexVol-Volumes zu sichern, aktivieren Sie zuerst ein Volume und dann das Kontrollkästchen in der Titelzeile. (

).

- Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume (

).

2. Wählen Sie **Weiter**.

Backup-Strategie definieren

Zur Definition der Backup-Strategie gehören die folgenden Optionen:

- Unabhängig davon, ob Sie eine oder alle Backup-Optionen: Lokale Snapshots, Replikation und Backup-to-Object-Storage möchten
- Der Netapp Architektur Sind
- Lokale Snapshot-Richtlinie
- Replikationsziel und -Richtlinie

> Wenn die ausgewählten Volumes andere Snapshot- und Replikationsrichtlinien haben als die in diesem Schritt ausgewählten Richtlinien, werden die vorhandenen Richtlinien überschrieben.

- Backup von Objekt-Storage-Informationen (Provider-, Verschlüsselungs-, Netzwerk-, Backup-Richtlinien- und Exportoptionen)

Schritte

1. Wählen Sie auf der Seite Backup-Strategie definieren eine oder alle der folgenden Optionen aus. Alle drei sind standardmäßig ausgewählt:
   - **Lokale Snapshots**: Wenn Sie eine Replikation oder Sicherung auf Objektspeicher durchführen, müssen lokale Snapshots erstellt werden.
   - **Replikation**: Erstellt replizierte Volumes auf einem anderen ONTAP-Speichersystem.
   - **Backup**: Sichert Volumes auf Objektspeicher.
2. **Architektur**: Wenn Sie Replikation und Backup gewählt haben, wählen Sie einen der folgenden Informationsflüsse:
   - **Kaskadierung**: Informationsflüsse vom primären zum sekundären und vom sekundären zum Objektspeicher.
   - **Fan Out**: Informationen fließen vom primären zum sekundären *und* vom primären zum Objektspeicher.

   Einzelheiten zu diesen Architekturen finden Sie unter "Planen Sie Ihren Weg zum Schutz".
3. **Lokaler Snapshot**: Wählen Sie eine vorhandene Snapshot-Richtlinie aus oder erstellen Sie eine neue.

   > Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung des Snapshots finden Sie unter "Erstellen einer Richtlinie".

   Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:
   - Geben Sie den Namen der Richtlinie ein.
   - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
   - Wählen Sie **Erstellen**.
4. **Replikation**: Stellen Sie die folgenden Optionen ein:

- **Replikationsziel**: Wählen Sie die Zielarbeitsumgebung und SVM aus. Wählen Sie optional das Zielaggregat oder die Aggregate und das Präfix oder Suffix aus, die dem Namen des replizierten Volumes hinzugefügt werden sollen.
- **Replikationsrichtlinie**: Wählen Sie eine vorhandene Replikationsrichtlinie oder erstellen Sie eine neue.

  Informationen zum Erstellen einer benutzerdefinierten Richtlinie, bevor Sie die Replikation aktivieren, finden Sie unter "Erstellen einer Richtlinie".

  Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

  - Geben Sie den Namen der Richtlinie ein.
  - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
  - Wählen Sie **Erstellen**.

5. **Backup auf Objekt**: Wenn Sie **Backup** ausgewählt haben, stellen Sie die folgenden Optionen ein:
   - **Provider**: Wählen Sie **Google Cloud**.
   - **Provider-Einstellungen**: Geben Sie die Provider-Details und die Region ein, in der die Backups gespeichert werden sollen.

     Erstellen Sie entweder einen neuen Bucket, oder wählen Sie einen bereits erstellten Bucket aus.

     Wenn Sie ältere Backup-Dateien zur weiteren Kostenoptimierung in Google Cloud Archive Storage verschieben möchten, stellen Sie sicher, dass der Bucket die entsprechende Lifecycle-Regel hat.

     Geben Sie den Google Cloud-Zugriffsschlüssel und den geheimen Schlüssel ein.

   - **Verschlüsselungsschlüssel**: Wenn Sie ein neues Google Cloud-Speicherkonto erstellt haben, geben Sie die Ihnen vom Anbieter gegebenen Verschlüsselungsschlüsselinformationen ein. Sie haben die Wahl, ob Sie die standardmäßige Google Cloud-Verschlüsselung verwenden oder Ihre eigenen von Kunden gemanagten Schlüssel aus Ihrem Google Cloud-Konto auswählen werden, um die Verschlüsselung Ihrer Daten zu managen.

     Wenn Sie ein vorhandenes Google Cloud Storage-Konto ausgewählt haben, sind Verschlüsselungsinformationen bereits verfügbar. Sie müssen sie daher jetzt nicht eingeben.

     Wenn Sie Ihre eigenen vom Kunden verwalteten Schlüssel verwenden möchten, geben Sie den Schlüsselring und den Schlüsselnamen ein. "Erfahren Sie mehr über vom Kunden verwaltete Verschlüsselungsschlüssel".

   - **Netzwerk**: Wählen Sie den IPspace.

     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.

   - **Backup Policy**: Wählen Sie eine vorhandene Richtlinie für das Objekt-Storage-Backup aus oder erstellen Sie eine neue.

Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Sicherung finden Sie unter "Erstellen einer Richtlinie".

Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

- Geben Sie den Namen der Richtlinie ein.
- Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
- Wählen Sie **Erstellen**.

◦ **Exportieren vorhandener Snapshot-Kopien als Backup-Kopien in den Objektspeicher**: Wenn es lokale Snapshot-Kopien für Volumes in dieser Arbeitsumgebung gibt, die mit dem Backup-Zeitplan-Label übereinstimmen, das Sie gerade für diese Arbeitsumgebung ausgewählt haben (z. B. täglich, wöchentlich usw.), wird diese zusätzliche Eingabeaufforderung angezeigt. Aktivieren Sie dieses Kontrollkästchen, damit alle historischen Snapshots als Backup-Dateien in den Objektspeicher kopiert werden, um einen möglichst vollständigen Schutz für Ihre Volumes zu gewährleisten.

6. Wählen Sie **Weiter**.

Überprüfen Sie Ihre Auswahl

Dies ist die Möglichkeit, Ihre Auswahl zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

Schritte

1. Überprüfen Sie auf der Seite „Überprüfen“ Ihre Auswahl.
2. Aktivieren Sie optional das Kontrollkästchen, um * die Snapshot-Policy-Labels automatisch mit den Label der Replikations- und Backup-Policy* zu synchronisieren. Dadurch werden Snapshots mit einem Label erstellt, das den Labels in den Replizierungs- und Backup-Richtlinien entspricht.
3. Wählen Sie **Sicherung Aktivieren**.

Ergebnis

Mit BlueXP Backup und Recovery werden erste Backups Ihrer Volumes erstellt. Der Basistransfer des replizierten Volumes und der Backup-Datei beinhaltet eine vollständige Kopie der Daten des primären Storage-Systems. Nachfolgende Transfers enthalten differenzielle Kopien der primären Storage-System-Daten in Snapshot Kopien.

Ein repliziertes Volume wird im Zielcluster erstellt, das mit dem Quell-Volume synchronisiert wird.

Ein Google Cloud Storage-Bucket wird automatisch in dem Servicekonto erstellt, das durch den von Ihnen eingegebenen Zugriffsschlüssel und den geheimen Schlüssel von Google angegeben wird und die Backup-Dateien dort gespeichert sind. 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".

Zeigt die API-Befehle an

Möglicherweise möchten Sie die API-Befehle anzeigen und optional kopieren, die im Assistenten Sicherung und Wiederherstellung aktivieren verwendet werden. Dies ist möglicherweise sinnvoll, um die Backup-Aktivierung in zukünftigen Arbeitsumgebungen zu automatisieren.

Schritte

1. Wählen Sie im Assistenten Backup und Recovery aktivieren **API-Anforderung anzeigen** aus.
2. Um die Befehle in die Zwischenablage zu kopieren, wählen Sie das Symbol **Kopieren**.

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" Einem Cloud Volumes ONTAP System in Google oder einem lokalen ONTAP System übertragen.

Sichern Sie lokale ONTAP-Daten auf ONTAP S3 mit BlueXP Backup und Recovery

Führen Sie einige Schritte in der Sicherung und Wiederherstellung von BlueXP durch, um mit der Sicherung von Volumedaten von Ihren primären lokalen ONTAP-Systemen zu beginnen. Sie können Backups an ein sekundäres ONTAP Storage-System (ein repliziertes Volume) oder an einen Bucket auf einem ONTAP System senden, das als S3-Server (eine Backup-Datei) konfiguriert ist oder beides.

Das primäre lokale ONTAP System kann ein FAS, AFF oder ONTAP Select System sein. Das sekundäre ONTAP System kann ein On-Premises ONTAP oder Cloud Volumes ONTAP System sein. Der Objekt-Storage kann sich auf einem lokalen ONTAP System oder auf einem Cloud Volumes ONTAP System befinden, auf dem Sie einen S3-Objekt-Storage-Server (Simple Storage Service) aktiviert haben.

Schnellstart

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

Identifizieren Sie die Verbindungsmethode, die Sie verwenden werden

Informieren Sie sich darüber, wie Sie Ihren primären lokalen ONTAP-Cluster zur Replizierung mit dem sekundären ONTAP-Cluster und dem als S3-Server für Backups im Objekt-Storage konfigurierten ONTAP-Cluster verbinden.

Identifizieren Sie die Verbindungsmethode.

Bereiten Sie Ihren BlueXP Connector vor

Wenn Sie bereits einen BlueXP Connector implementiert haben, sind Sie fertig. Falls nicht, müssen Sie einen BlueXP Connector erstellen, um ONTAP Daten in ONTAP S3 zu sichern. Außerdem müssen Sie die Netzwerkeinstellungen für den Connector anpassen, damit eine Verbindung zu ONTAP S3 hergestellt werden

kann.

Erfahren Sie, wie Sie einen Connector erstellen und die erforderlichen Netzwerkeinstellungen definieren.

3 Lizenzanforderungen prüfen

Prüfen Sie dann die Lizenzanforderungen für Ihre ONTAP Systeme sowie für das Backup und Recovery von BlueXP.

Überprüfen Sie die Lizenzanforderungen.

4 Bereiten Sie Ihre ONTAP-Cluster vor

Primäre und sekundäre ONTAP Cluster in BlueXP erkennen, überprüfen, ob die Cluster Mindestanforderungen erfüllen, und Netzwerkeinstellungen anpassen, damit die Cluster eine Verbindung zum ONTAP S3 Objekt-Storage herstellen können.

Informieren Sie sich, wie Sie Ihre ONTAP Cluster vorbereiten.

5 ONTAP S3 als Backup-Ziel vorbereiten

Richten Sie Berechtigungen für den Connector ein, damit dieser den ONTAP S3-Bucket verwalten kann. Außerdem müssen Sie Berechtigungen für das lokale ONTAP-Quell-Cluster einrichten, damit es Daten in den ONTAP S3-Bucket lesen und schreiben kann.

Erfahren Sie, wie Sie Ihre ONTAP S3 Umgebung für ONTAP Backups vorbereiten.

6 Aktivieren Sie Backups auf Ihren ONTAP Volumes

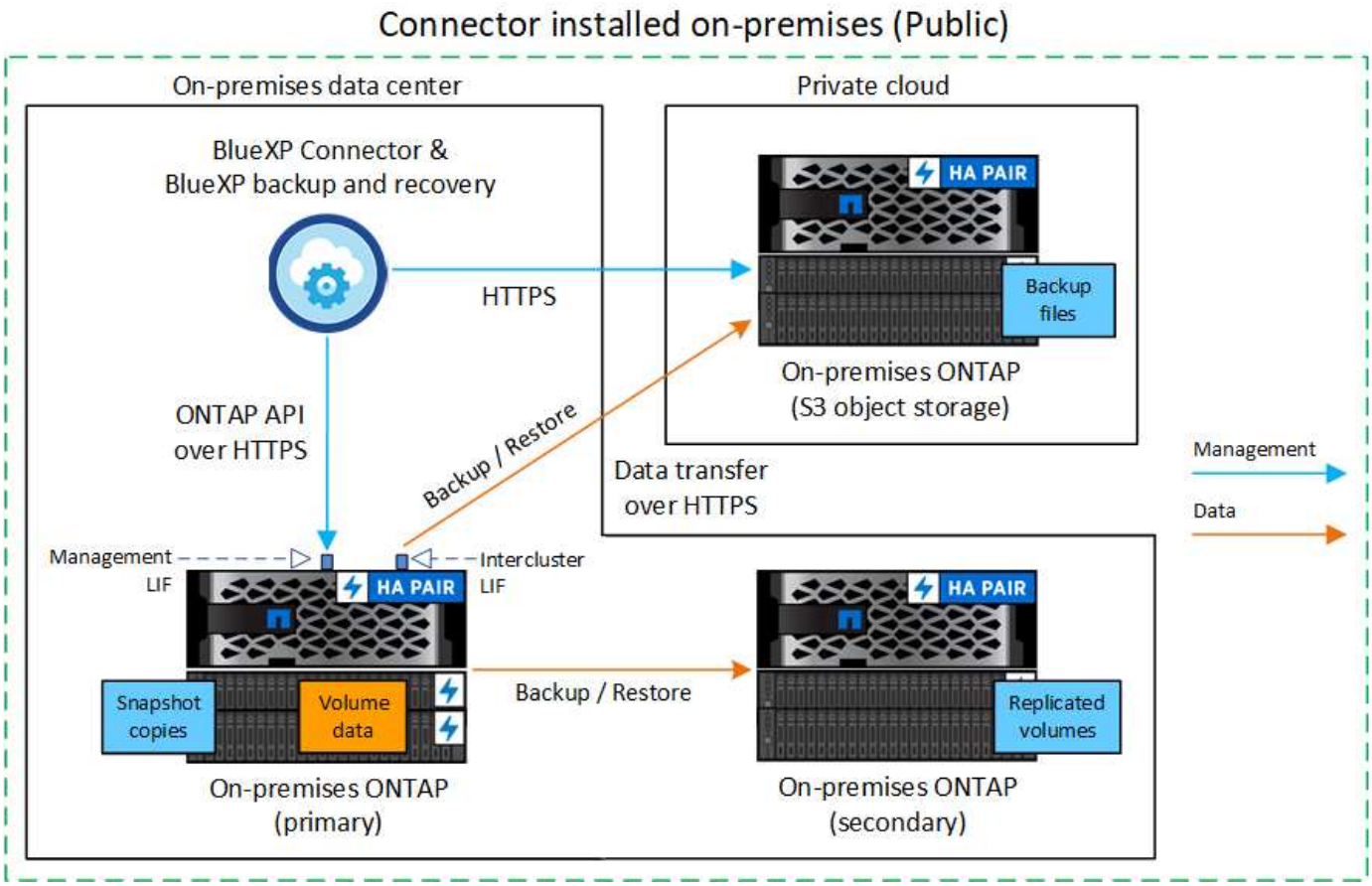
Wählen Sie die primäre Arbeitsumgebung aus und klicken Sie auf **Enable > Backup Volumes** neben dem Sicherungs- und Wiederherstellungsdienst im rechten Fensterbereich. Folgen Sie dann dem Setup-Assistenten, um die Volumes auszuwählen, die Sie sichern möchten, sowie die Richtlinien für Snapshot, Replizierung und Backup in einem Objekt, die Sie verwenden möchten.

Aktivieren Sie Backups auf Ihren ONTAP Volumes.

Identifizieren Sie die Verbindungsmethode

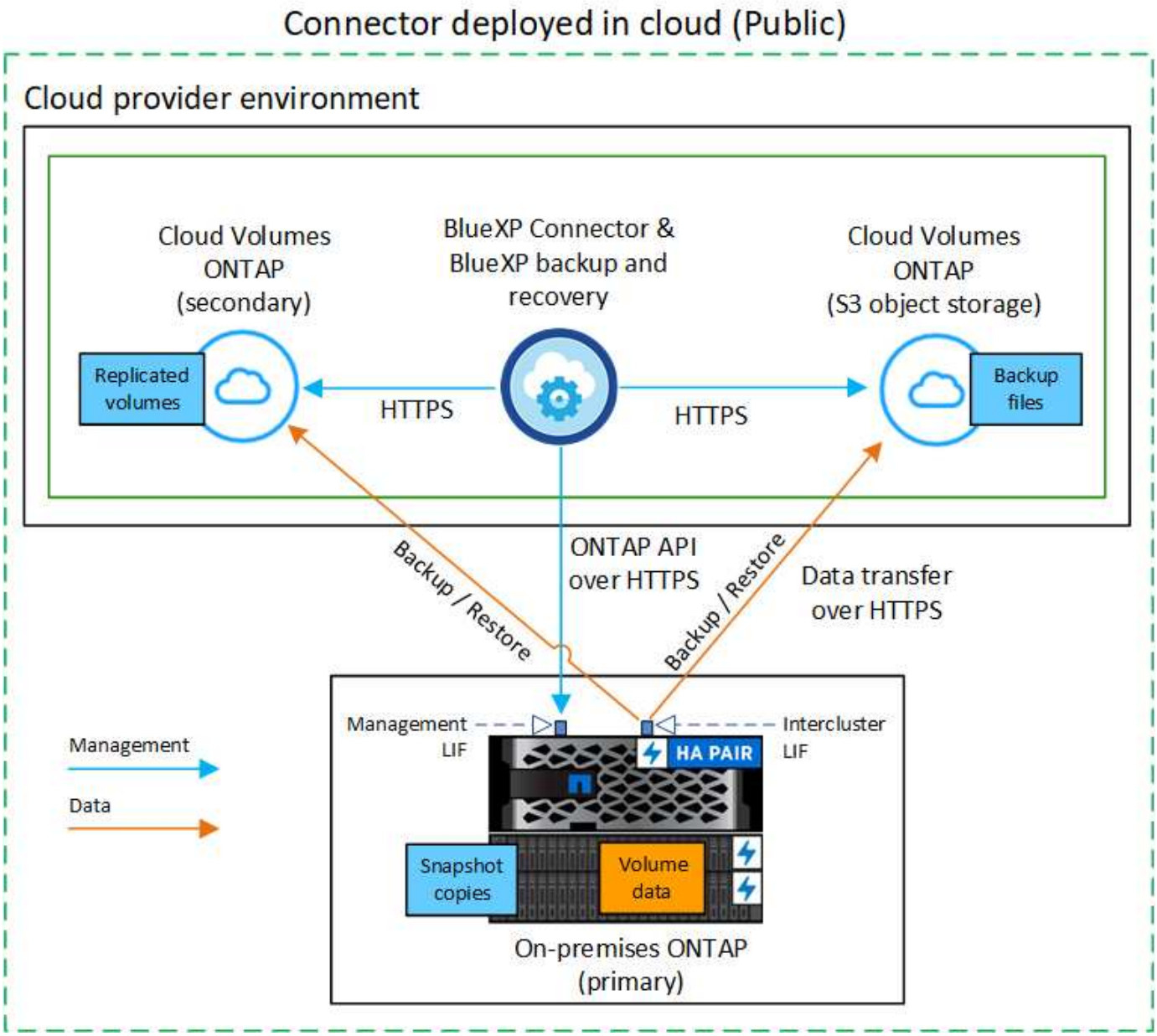
Es gibt viele Konfigurationen, in denen Sie Backups auf einem S3-Bucket auf einem ONTAP-System erstellen können. Im Folgenden werden zwei Szenarien dargestellt.

Die folgende Abbildung zeigt jede Komponente beim Backup eines primären On-Premises-ONTAP-Systems auf einem für S3 konfigurierten On-Premises-ONTAP-System sowie die Verbindungen, die Sie zwischen ihnen vorbereiten müssen. Sie zeigt außerdem eine Verbindung zu einem sekundären ONTAP-System am selben lokalen Standort, um Volumes zu replizieren.



Wenn der Connector und das primäre On-Premises-ONTAP-System an einem On-Premises-Standort ohne Internetzugang installiert sind (eine „private“ Mode-Implementierung), muss sich das ONTAP S3 System im selben On-Premises-Datacenter befinden.

Das folgende Bild zeigt jede Komponente beim Backup eines primären On-Premises-ONTAP-Systems auf einem für S3 konfigurierten Cloud Volumes ONTAP-System und die Verbindungen, die Sie zwischen ihnen vorbereiten müssen. Sie zeigt außerdem eine Verbindung zu einem sekundären Cloud Volumes ONTAP-System in derselben Cloud-Provider-Umgebung zur Replizierung von Volumes.



In diesem Szenario sollte der Connector in derselben Cloud-Provider-Umgebung eingesetzt werden, in der die Cloud Volumes ONTAP-Systeme eingesetzt werden.

Bereiten Sie Ihren BlueXP Connector vor

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

Erstellen oder Schalten von Anschlüssen

Bei Daten-Backups in ONTAP S3 muss ein BlueXP Connector vor Ort oder in der Cloud verfügbar sein. Sie müssen entweder einen neuen Connector installieren oder sicherstellen, dass sich der aktuell ausgewählte Connector an einem dieser Standorte befindet. Der On-Premise Connector kann an einem Standort mit oder ohne Internetzugang installiert werden.

- "Erfahren Sie mehr über Steckverbinder"

- "Installieren Sie den Connector in Ihrer Cloud-Umgebung"
- "Installieren des Connectors auf einem Linux-Host mit Internetzugang"
- "Installieren des Connectors auf einem Linux-Host ohne Internetzugang"
- "Wechseln zwischen den Anschlüssen"

Bereiten Sie die Netzwerkanforderungen für den Connector vor

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

- Eine HTTPS-Verbindung über Port 443 zum ONTAP S3-Server
- Eine HTTPS-Verbindung über Port 443 zur ONTAP Quell-Cluster-Management-LIF
- Eine Outbound-Internetverbindung über Port 443 zu BlueXP Backup und Recovery (nicht erforderlich, wenn der Connector an einer „dunklen“ Stelle installiert ist)

Überlegungen zum privaten Modus (dunkle Seite)

Die Backup- und Recovery-Funktionen von BlueXP sind in den BlueXP Connector integriert. Wenn die Connector-Software im privaten Modus installiert ist, müssen Sie sie regelmäßig aktualisieren, um auf neue Funktionen zugreifen zu können. Prüfen Sie die "BlueXP Backup und Recovery Was ist neu" Um die neuen Funktionen in jeder BlueXP Backup- und Recovery-Version anzuzeigen. Wenn Sie die neuen Funktionen verwenden möchten, führen Sie die Schritte bis aus "Aktualisieren Sie die Connector-Software".

Wenn Sie das Backup und Recovery von BlueXP in einer standardmäßigen SaaS-Umgebung nutzen, werden die Backup- und Recovery-Konfigurationsdaten von BlueXP in der Cloud gesichert. Wenn Sie BlueXP Backup und Recovery an einem Standort ohne Internetzugang nutzen, werden die Backup- und Recovery-Konfigurationsdaten von BlueXP auf den ONTAP S3 Bucket gesichert, auf dem die Backups gespeichert werden. Wenn Sie jemals einen Connector-Fehler in Ihrem privaten Modus Standort haben, können Sie dies tun "Wiederherstellung der Backup- und Recovery-Daten von BlueXP in einem neuen Connector".

Lizenzanforderungen prüfen

Bevor Sie das Backup und Recovery von BlueXP für Ihr Cluster aktivieren können, müssen Sie eine BYOL-Lizenz für BlueXP Backup und Recovery von NetApp erwerben und aktivieren. Die Lizenz gilt für Backup und Wiederherstellung im Objekt-Storage – zum Erstellen von Snapshot Kopien oder replizierten Volumes ist keine Lizenz erforderlich. 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 ONTAP S3 nicht unterstützt.

Bereiten Sie Ihre ONTAP-Cluster vor

Sie müssen Ihr On-Premises-Quell-ONTAP-System und alle sekundären lokalen ONTAP oder Cloud Volumes ONTAP Systeme vorbereiten.

Zur Vorbereitung Ihrer ONTAP-Cluster sind folgende Schritte erforderlich:

- Ihre ONTAP-Systeme in BlueXP erkennen
- Überprüfen Sie die Systemanforderungen für ONTAP

- ONTAP Netzwerkanforderungen für Daten-Backups im Objekt-Storage prüfen
- Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes

Ihre ONTAP-Systeme in BlueXP erkennen

Sowohl das On-Premises-Quell-ONTAP-System als auch alle sekundären ONTAP- oder Cloud Volumes ONTAP-Systeme vor Ort müssen auf der BlueXP Leinwand verfügbar sein.

Sie müssen die Cluster-Management-IP-Adresse und das Passwort kennen, mit dem das Admin-Benutzerkonto den Cluster hinzufügen kann.
"Entdecken Sie ein Cluster".

Überprüfen Sie die Systemanforderungen für ONTAP

Stellen Sie sicher, dass die folgenden ONTAP-Anforderungen erfüllt sind:

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

  Hinweis: das „Hybrid Cloud Bundle“ ist bei Backup und Recovery von BlueXP nicht erforderlich.

  Erfahren Sie, wie Sie "Management Ihrer Cluster-Lizenzen".

- Zeit und Zeitzone sind korrekt eingestellt. Erfahren Sie, wie Sie "Konfigurieren Sie die Cluster-Zeit".
- Wenn Sie Daten replizieren möchten, sollten Sie vor der Replizierung von Daten überprüfen, ob auf den Quell- und Zielsystemen kompatible ONTAP-Versionen ausgeführt werden.

  "Zeigen Sie kompatible ONTAP Versionen für SnapMirror Beziehungen an".

ONTAP Netzwerkanforderungen für Daten-Backups im Objekt-Storage prüfen

Sie müssen sicherstellen, dass die folgenden Anforderungen für das System erfüllt sind, das eine Verbindung zum Objekt-Storage herstellt.

- Wenn Sie eine Fan-out-Backup-Architektur verwenden, müssen die Einstellungen auf dem *primary*-Speichersystem konfiguriert werden.
- Wenn Sie eine kaskadierte Backup-Architektur verwenden, müssen die Einstellungen auf dem *Secondary*-Speichersystem konfiguriert werden.

  "Erfahren Sie mehr über die Arten der Backup-Architektur".

Die folgenden Netzwerkanforderungen für ONTAP-Cluster sind erforderlich:

- Das ONTAP Cluster initiiert für Backup- und Restore-Vorgänge eine HTTPS-Verbindung über einen benutzerdefinierten Port von der Intercluster LIF zum ONTAP S3 Server. 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.

- 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 BlueXP Backup und Recovery einrichten, werden Sie aufgefordert, den IPspace 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 Standard verwenden, müssen Sie möglicherweise eine statische Route erstellen, um Zugriff auf den Objektspeicher zu erhalten.
- Aktualisieren Sie bei Bedarf die Firewall-Regeln, um die Verbindungen des BlueXP Backup- und Recovery-Service von ONTAP zu dem Objekt-Storage über den angegebenen Port (normalerweise Port 443) und den Datenverkehr der Namensauflösung von der Storage-VM zum DNS-Server über Port 53 (TCP/UDP) zu ermöglichen.

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes

Wenn Sie planen, mithilfe von BlueXP Backup und Recovery replizierte Volumes auf einem sekundären ONTAP System zu erstellen, stellen Sie sicher, dass die Quell- und Zielsysteme die folgenden Netzwerkanforderungen erfüllen.

Netzwerkanforderungen für On-Premises-ONTAP

- Wenn sich der Cluster an Ihrem Standort befindet, sollten Sie über eine Verbindung zwischen Ihrem Unternehmensnetzwerk und Ihrem virtuellen Netzwerk des Cloud-Providers verfügen. Hierbei handelt es sich in der Regel um eine VPN-Verbindung.
- ONTAP Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Cluster-Anforderungen erfüllen.

  Da Sie Daten auf Cloud Volumes ONTAP oder auf lokale Systeme replizieren können, prüfen Sie Peering-Anforderungen für lokale ONTAP Systeme. "Anzeigen von Voraussetzungen für Cluster-Peering in der ONTAP-Dokumentation".

Netzwerkanforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen ein- und ausgehenden Regeln enthalten: Speziell Regeln für ICMP und die Ports 11104 und 11105. Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.

ONTAP S3 als Backup-Ziel vorbereiten

Sie müssen im ONTAP Cluster einen S3-Objekt-Storage-Server (Simple Storage Service) aktivieren, den Sie für Objekt-Storage-Backups verwenden möchten. Siehe "ONTAP S3 Dokumentation" Entsprechende Details.

Hinweis: Sie können diesen Cluster auf dem BlueXP Canvas erkennen, aber er wird nicht als S3-Objekt-Storage-Server identifiziert. Sie können keine Quell-Arbeitsumgebung per Drag & Drop in diese S3-Arbeitsumgebung ziehen, um eine Backup-Aktivierung zu initiieren.

Dieses ONTAP-System muss die folgenden Anforderungen erfüllen:

Unterstützte ONTAP-Versionen

Für lokale ONTAP Systeme ist ONTAP 9.8 oder eine höhere Version erforderlich.
Für Cloud Volumes ONTAP Systeme ist ONTAP 9.9.1 und höher erforderlich.

S3-Anmeldedaten

Sie müssen einen S3-Benutzer erstellt haben, um den Zugriff auf Ihren ONTAP S3-Storage zu steuern. "Weitere Informationen finden Sie in der Dokumentation zu ONTAP S3".

Wenn Sie ein Backup auf ONTAP S3 einrichten, werden Sie vom Backup-Assistenten zur Eingabe eines S3-Zugriffsschlüssels und eines geheimen Schlüssels für ein Benutzerkonto aufgefordert. Das Benutzerkonto ermöglicht BlueXP Backup und Recovery zur Authentifizierung und zum Zugriff auf die ONTAP S3 Buckets, die zum Speichern von Backups verwendet werden. Die Schlüssel sind erforderlich, damit ONTAP S3 weiß, wer die Anforderung stellt.

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

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

Aktivieren Sie Backups auf Ihren ONTAP Volumes

Sie können Backups jederzeit direkt aus Ihrer On-Premises-Arbeitsumgebung heraus aktivieren.

Ein Assistent führt Sie durch die folgenden wichtigen Schritte:

- Wählen Sie die Volumes aus, die Sie sichern möchten
- Backup-Strategie und -Richtlinien definieren
- Überprüfen Sie Ihre Auswahl

Das können Sie auch Zeigt die API-Befehle an Kopieren Sie im Überprüfungsschritt den Code, um die Backup-Aktivierung für zukünftige Arbeitsumgebungen zu automatisieren.

Starten Sie den Assistenten

Schritte

1. Greifen Sie auf eine der folgenden Arten auf den Assistenten zur Aktivierung von Backup und Recovery zu:
   - Wählen Sie auf dem BlueXP-Bildschirm die Arbeitsumgebung aus, und wählen Sie im rechten Bereich neben dem Sicherungs- und Wiederherstellungsdienst die Option **Enable > Backup Volumes** aus.
   - Wählen Sie in der Sicherungs- und Wiederherstellungsleiste **Volumes** aus. Wählen Sie auf der Registerkarte Volumes die Option **actions (…)** aus und wählen Sie **Activate Backup** für ein einzelnes Volume (das noch nicht über Replikation oder Backup auf Objektspeicher verfügt).

   Auf der Seite Einführung des Assistenten werden die Schutzoptionen einschließlich lokaler Snapshots, Replikationen und Backups angezeigt. Wenn Sie die zweite Option in diesem Schritt gewählt haben, wird die Seite „Backup-Strategie definieren“ mit einem ausgewählten Volume angezeigt.

2. Fahren Sie mit den folgenden Optionen fort:
   - Wenn Sie bereits einen BlueXP Connector haben, sind Sie fertig. Wählen Sie einfach **Weiter**.
   - Wenn Sie keinen BlueXP Connector haben, wird die Option **Connector hinzufügen** angezeigt. Siehe Bereiten Sie Ihren BlueXP Connector vor.

Wählen Sie die Volumes aus, die Sie sichern möchten

Wählen Sie die Volumes aus, die Sie schützen möchten. Ein geschütztes Volume verfügt über eine oder mehrere der folgenden Elemente: Snapshot-Richtlinie, Replizierungsrichtlinie und Richtlinie für das Backup in ein Objekt.

Sie können FlexVol- oder FlexGroup-Volumes schützen. Sie können jedoch keine Kombination dieser Volumes auswählen, wenn Sie Backups für eine funktionierende Umgebung aktivieren. Informieren Sie sich darüber "Aktivieren Sie das Backup für zusätzliche Volumes in der Arbeitsumgebung" (FlexVol oder FlexGroup), nachdem Sie das Backup für die ersten Volumes konfiguriert haben.

- Sie können ein Backup nur auf einem einzelnen FlexGroup Volume gleichzeitig aktivieren.
- Die ausgewählten Volumes müssen dieselbe SnapLock-Einstellung aufweisen. Auf allen Volumes muss SnapLock Enterprise aktiviert oder SnapLock deaktiviert sein.

Schritte

Beachten Sie, dass die Richtlinien, die Sie später auswählen, diese vorhandenen Richtlinien überschreiben, wenn die von Ihnen ausgewählten Volumes bereits Snapshot- oder Replikationsrichtlinien angewendet haben.

1. Wählen Sie auf der Seite Volumes auswählen das Volume oder die Volumes aus, die Sie schützen möchten.
   - Optional können Sie die Zeilen so filtern, dass nur Volumes mit bestimmten Volumentypen, Stilen und mehr angezeigt werden, um die Auswahl zu erleichtern.
   - Nachdem Sie das erste Volume ausgewählt haben, können Sie alle FlexVol Volumes auswählen (FlexGroup Volumes können nur einzeln ausgewählt werden). Um alle vorhandenen FlexVol-Volumes zu sichern, aktivieren Sie zuerst ein Volume und dann das Kontrollkästchen in der Titelzeile. (

).
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume (

).
2. Wählen Sie **Weiter**.

Backup-Strategie definieren

Die Definition der Backup-Strategie umfasst die Konfiguration der folgenden Optionen:

- Schutzoptionen: Ob Sie eine oder alle Backup-Optionen implementieren möchten: Lokale Snapshots, Replikation und Backup in Objektspeicher
- Architektur: Unabhängig davon, ob Sie eine Fan-out- oder kaskadierende Backup-Architektur nutzen möchten
- Lokale Snapshot-Richtlinie
- Replikationsziel und -Richtlinie
- Backup von Objekt-Storage-Informationen (Provider-, Verschlüsselungs-, Netzwerk-, Backup-Richtlinien- und Exportoptionen)

Schritte

1. Wählen Sie auf der Seite „Backup-Strategie definieren“ eine oder alle der folgenden Optionen aus. Alle drei sind standardmäßig ausgewählt:
   - **Lokale Snapshots**: Erstellt lokale Snapshot-Kopien.
   - **Replikation**: Erstellt replizierte Volumes auf einem anderen ONTAP-Speichersystem.
   - **Backup**: Sichert Volumes auf einem Bucket auf einem für S3 konfigurierten ONTAP-System.
2. **Architektur**: Wenn Sie sowohl Replikation als auch Backup gewählt haben, wählen Sie einen der folgenden Informationsflüsse:
   - **Kaskadierung**: Backup-Daten fließen vom primären zum sekundären System und dann vom sekundären zum Objektspeicher.
   - **Fan Out**: Backup-Daten werden vom primären zum sekundären System *und* vom primären zum Objekt-Storage geleitet.

     Einzelheiten zu diesen Architekturen finden Sie unter "Planen Sie Ihren Weg zum Schutz".
3. **Lokaler Snapshot**: Wählen Sie eine vorhandene Snapshot-Richtlinie aus oder erstellen Sie eine neue.

   Wenn Sie vor dem Aktivieren des Snapshots eine benutzerdefinierte Richtlinie erstellen möchten, können Sie System Manager oder die ONTAP CLI verwenden `snapmirror policy create` Befehl. Siehe.

   Informationen zum Erstellen einer benutzerdefinierten Richtlinie mit diesem Service vor dem Aktivieren des Snapshots finden Sie unter "Erstellen einer Richtlinie".

   Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

   - Geben Sie den Namen der Richtlinie ein.
   - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
   - Wählen Sie **Erstellen**.
4. **Replikation**: Wenn Sie **Replikation** ausgewählt haben, stellen Sie die folgenden Optionen ein:
   - **Replikationsziel**: Wählen Sie die Zielarbeitsumgebung und SVM aus. Wählen Sie optional das Zielaggregat (oder Aggregate für FlexGroup Volumes) und ein Präfix oder Suffix aus, das dem Namen des replizierten Volumes hinzugefügt wird.
   - **Replikationsrichtlinie**: Wählen Sie eine vorhandene Replikationsrichtlinie oder erstellen Sie eine neue.

     Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

     - Geben Sie den Namen der Richtlinie ein.
     - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
     - Wählen Sie **Erstellen**.
5. **Backup auf Objekt**: Wenn Sie **Backup** ausgewählt haben, stellen Sie die folgenden Optionen ein:
   - **Anbieter**: Wählen Sie **ONTAP S3**.
   - **Provider-Einstellungen**: Geben Sie die FQDN-Details des S3-Servers, den Port und den

Zugriffsschlüssel des Benutzers und den geheimen Schlüssel ein.

Der Zugriffsschlüssel und der geheime Schlüssel gelten für den Benutzer, den Sie erstellt haben, um dem ONTAP Cluster Zugriff auf den S3-Bucket zu geben.

- **Netzwerk**: Wählen Sie den IPspace im Quell-ONTAP-Cluster, wo 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 Auswahl des korrekten IPspaces wird sichergestellt, dass BlueXP Backup und Recovery eine Verbindung von ONTAP zu Ihrem ONTAP S3 Objekt-Storage einrichten können.

- **Backup Policy**: Wählen Sie eine vorhandene Backup Policy aus oder erstellen Sie eine neue.

  Sie können eine Richtlinie mit System Manager oder der ONTAP CLI erstellen. Zum Erstellen einer benutzerdefinierten Richtlinie mithilfe der ONTAP-CLI `snapmirror policy create` Befehl, siehe.

  Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Sicherung über die Benutzeroberfläche finden Sie unter "Erstellen einer Richtlinie".

  Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

  - Geben Sie den Namen der Richtlinie ein.
  - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
  - Legen Sie für Backup-to-Object-Richtlinien die Einstellungen für DataLock und Ransomware-Schutz fest. Weitere Informationen zu DataLock und Ransomware-Schutz finden Sie unter "Richtlinieneinstellungen für Backup-to-Object".
  - Wählen Sie **Erstellen**.

- **Bestehende Snapshot-Kopien als Backup-Dateien in den Objektspeicher exportieren**: Wenn es lokale Snapshot-Kopien für Volumes in dieser Arbeitsumgebung gibt, die mit dem gerade ausgewählten Backup-Zeitplan-Label übereinstimmen (z.B. täglich, wöchentlich, etc.), wird diese zusätzliche Eingabeaufforderung angezeigt. Aktivieren Sie dieses Kontrollkästchen, damit alle historischen Snapshots als Backup-Dateien in den Objektspeicher kopiert werden, um einen möglichst vollständigen Schutz für Ihre Volumes zu gewährleisten.

6. Wählen Sie **Weiter**.

Überprüfen Sie Ihre Auswahl

Dies ist die Möglichkeit, Ihre Auswahl zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

Schritte

1. Überprüfen Sie auf der Seite „Überprüfen“ Ihre Auswahl.
2. Aktivieren Sie optional das Kontrollkästchen, um * die Snapshot-Policy-Labels automatisch mit den Label der Replikations- und Backup-Policy* zu synchronisieren. Dadurch werden Snapshots mit einem Label erstellt, das den Labels in den Replizierungs- und Backup-Richtlinien entspricht. Wenn die Richtlinien nicht übereinstimmen, werden keine Backups erstellt.

3. Wählen Sie **Sicherung Aktivieren**.

Ergebnis

Mit BlueXP Backup und Recovery werden erste Backups Ihrer Volumes erstellt. Der Basistransfer des replizierten Volumes und der Backup-Datei beinhaltet eine vollständige Kopie der Quelldaten. Nachfolgende Transfers enthalten differenzielle Kopien der primären Storage-Daten, die in Snapshot Kopien enthalten sind.

Ein repliziertes Volume wird im Zielcluster erstellt, das mit dem primären Storage Volume synchronisiert wird.

Ein S3-Bucket wird in dem Servicekonto erstellt, das durch den eingegebenen S3-Zugriffsschlüssel und geheimen Schlüssel angegeben ist, und die Backup-Dateien werden dort gespeichert.

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".

Zeigt die API-Befehle an

Möglicherweise möchten Sie die API-Befehle anzeigen und optional kopieren, die im Assistenten Sicherung und Wiederherstellung aktivieren verwendet werden. Dies ist möglicherweise sinnvoll, um die Backup-Aktivierung in zukünftigen Arbeitsumgebungen zu automatisieren.

Schritte

1. Wählen Sie im Assistenten Backup und Recovery aktivieren **API-Anforderung anzeigen** aus.
2. Um die Befehle in die Zwischenablage zu kopieren, wählen Sie das Symbol **Kopieren**.

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 unter anderem die Änderung der verfügbaren Netzwerkbandbreite für das Hochladen von Backups in den Objekt-Storage, die Änderung der automatischen Backup-Einstellung für zukünftige Volumes.
- Das können Sie auch "Wiederherstellung von Volumes, Ordnern oder einzelnen Dateien aus einer Sicherungsdatei" Auf ein lokales ONTAP System zugreifen:

Sichern Sie lokale ONTAP-Daten mit BlueXP Backup und Recovery auf StorageGRID

Führen Sie einige Schritte in der Sicherung und Wiederherstellung von BlueXP durch, um mit der Sicherung von Volume-Daten von Ihren primären ONTAP-Systemen vor Ort auf ein sekundäres Speichersystem und auf Objektspeicher in Ihren NetApp StorageGRID-Systemen zu beginnen.

„On-Premises ONTAP Systeme“ umfassen FAS, AFF und ONTAP Select Systeme.

Schnellstart

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

1 Identifizieren Sie die Verbindungsmethode, die Sie verwenden werden

Prüfen Sie, wie Sie Ihr lokales ONTAP-Cluster über das öffentliche Internet direkt mit StorageGRID verbinden oder ob Sie ein VPN verwenden und den Datenverkehr über eine private VPC-Endpoint-Schnittstelle zu StorageGRID weiterleiten.

Identifizieren Sie die Verbindungsmethode.

2 Bereiten Sie Ihren BlueXP Connector vor

Wenn Sie bereits einen Connector in Ihren Räumlichkeiten installiert haben, sind Sie alle bereit. Falls nicht, müssen Sie einen BlueXP Connector erstellen, um ONTAP Daten in StorageGRID zu sichern. Außerdem müssen Sie die Netzwerkeinstellungen für den Connector anpassen, damit er eine Verbindung zu StorageGRID herstellen kann.

Erfahren Sie, wie Sie einen Connector erstellen und die erforderlichen Netzwerkeinstellungen definieren.

3 Lizenzanforderungen prüfen

Sie müssen die Lizenzanforderungen sowohl für StorageGRID als auch für BlueXP prüfen.

Siehe Lizenzanforderungen prüfen.

4 Bereiten Sie Ihre ONTAP-Cluster vor

Erkennen Sie Ihre ONTAP Cluster in BlueXP, überprüfen Sie, ob die Cluster Mindestanforderungen erfüllen, und passen Sie Netzwerkeinstellungen für die Verbindung der Cluster mit StorageGRID an.

Informieren Sie sich, wie Sie Ihre ONTAP Cluster vorbereiten.

5 StorageGRID als Backup-Ziel vorbereiten

Richten Sie Berechtigungen für den Connector ein, um den StorageGRID-Bucket zu erstellen und zu verwalten. Außerdem müssen Sie Berechtigungen für den lokalen ONTAP-Cluster einrichten, damit dieser Daten in den Bucket lesen und schreiben kann.

Optional können Sie auch Ihre eigenen benutzerdefinierten verwalteten Schlüssel für die Datenverschlüsselung einrichten, ohne die standardmäßigen StorageGRID-Verschlüsselungsschlüssel verwenden zu müssen. Erfahren Sie, wie Sie Ihre StorageGRID Umgebung für ONTAP Backups vorbereiten.

6 Aktivieren Sie Backups auf Ihren ONTAP Volumes

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

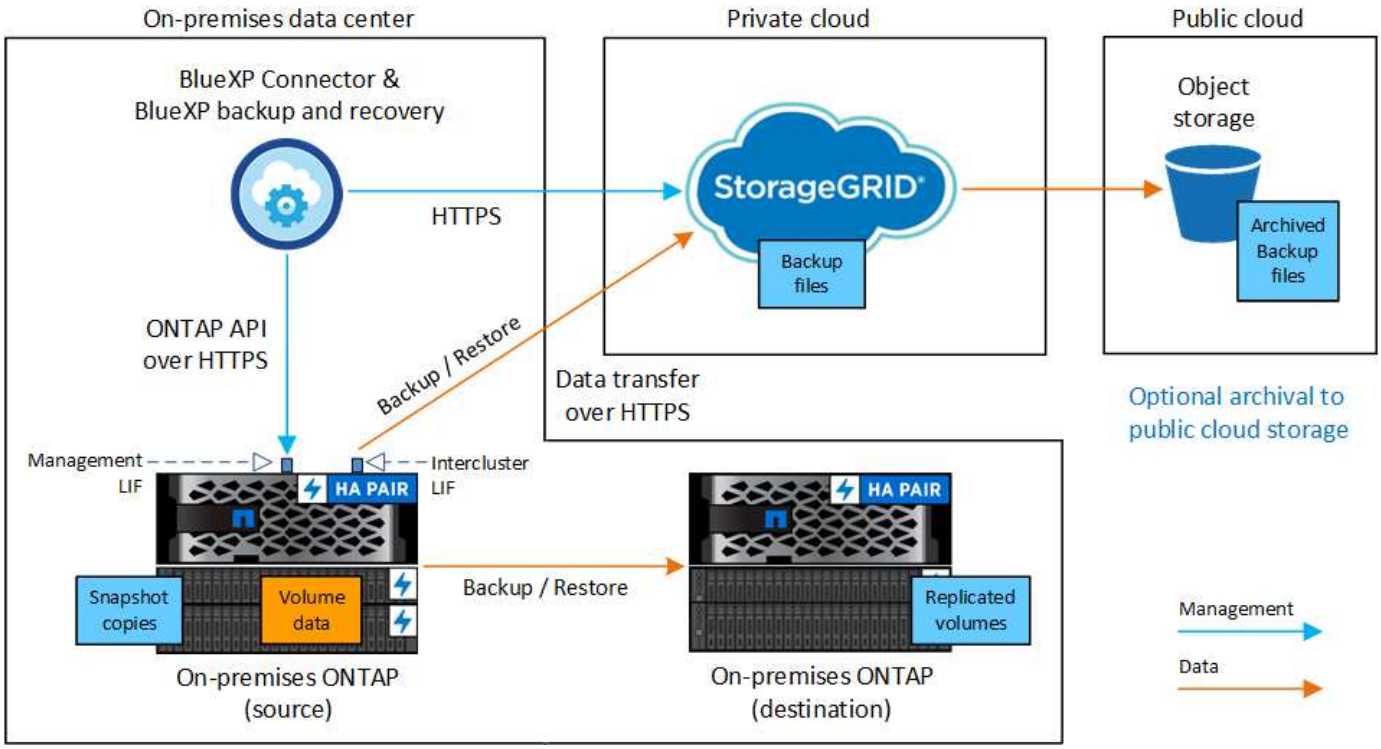
Backup-Richtlinien auszuwählen, die Sie verwenden werden, und die Volumes, die Sie sichern möchten.

Aktivieren Sie Backups auf Ihren ONTAP Volumes.

Identifizieren Sie die Verbindungsmethode

Die folgende Abbildung zeigt die einzelnen Komponenten beim Backup eines On-Premises-ONTAP-Systems auf StorageGRID sowie die Verbindungen, die Sie zwischen diesen Systemen vorbereiten müssen.

Optional können Sie eine Verbindung zu einem sekundären ONTAP-System am selben Standort herstellen, um Volumes zu replizieren.



Wenn der Connector und das On-Premises-ONTAP-System an einem On-Premises-Standort ohne Internetzugang (eine „Dark Site“) installiert werden, muss sich das StorageGRID System im selben On-Premises-Datacenter befinden. Die Archivierung älterer Backup-Dateien in der Public Cloud wird nicht in dunklen Site-Konfigurationen unterstützt.

Bereiten Sie Ihren BlueXP Connector vor

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

Erstellen oder Schalten von Anschlüssen

Wenn Sie Daten-Backups in StorageGRID erstellen, muss ein BlueXP Connector vor Ort verfügbar sein. Sie müssen entweder einen neuen Connector installieren oder sicherstellen, dass sich der aktuell ausgewählte Connector vor Ort 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"

Bereiten Sie die Netzwerkanforderungen für den Connector vor

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 Outbound-Internetverbindung über Port 443 zu BlueXP Backup und Recovery (nicht erforderlich, wenn der Connector an einer „dunklen“ Stelle installiert ist)

Überlegungen zum privaten Modus (dunkle Seite)

- Die Backup- und Recovery-Funktionen von BlueXP sind in den BlueXP Connector integriert. Wenn die Connector-Software im privaten Modus installiert ist, müssen Sie sie regelmäßig aktualisieren, um auf neue Funktionen zugreifen zu können. Prüfen Sie die "BlueXP Backup und Recovery Was ist neu" Um die neuen Funktionen in jeder BlueXP Backup- und Recovery-Version anzuzeigen. Wenn Sie die neuen Funktionen verwenden möchten, führen Sie die Schritte bis aus "Aktualisieren Sie die Connector-Software".

  Die neue Version von BlueXP Backup und Recovery mit der Möglichkeit, Snapshot Kopien und replizierte Volumes zu planen und zu erstellen sowie Backups in Objektspeicher zu erstellen, setzt voraus, dass Sie Version 3.9.31 oder höher des BlueXP Connector verwenden. Es wird daher empfohlen, dass Sie diese neueste Version erhalten, um alle Ihre Backups zu verwalten.

- Wenn Sie BlueXP Backup und Recovery in einer SaaS-Umgebung nutzen, werden die Backup- und Recovery-Konfigurationsdaten von BlueXP in der Cloud gesichert. Wenn Sie BlueXP Backup und Recovery an einem Standort ohne Internetzugang nutzen, werden die Backup- und Recovery-Konfigurationsdaten von BlueXP auf den StorageGRID Bucket gesichert, auf dem die Backups gespeichert werden. Wenn Sie jemals einen Connector-Fehler in Ihrem privaten Modus Standort haben, können Sie dies tun "Wiederherstellung der Backup- und Recovery-Daten von BlueXP in einem neuen Connector".

Lizenzanforderungen prüfen

Bevor Sie das Backup und Recovery von BlueXP für Ihr Cluster aktivieren können, müssen Sie eine BYOL-Lizenz für BlueXP Backup und Recovery 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.

Bereiten Sie Ihre ONTAP-Cluster vor

Sie müssen Ihr On-Premises-Quell-ONTAP-System und alle sekundären lokalen ONTAP oder Cloud Volumes ONTAP Systeme vorbereiten.

Zur Vorbereitung Ihrer ONTAP-Cluster sind folgende Schritte erforderlich:

- Ihre ONTAP-Systeme in BlueXP erkennen

- Überprüfen Sie die Systemanforderungen für ONTAP
- ONTAP Netzwerkanforderungen für Daten-Backups im Objekt-Storage prüfen
- Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes

Ihre ONTAP-Systeme in BlueXP erkennen

Sowohl das On-Premises-Quell-ONTAP-System als auch alle sekundären ONTAP- oder Cloud Volumes ONTAP-Systeme vor Ort müssen auf der BlueXP Leinwand verfügbar sein.

Sie müssen die Cluster-Management-IP-Adresse und das Passwort kennen, mit dem das Admin-Benutzerkonto den Cluster hinzufügen kann.
"Entdecken Sie ein Cluster".

Überprüfen Sie die Systemanforderungen für ONTAP

Stellen Sie sicher, dass die folgenden ONTAP-Anforderungen erfüllt sind:

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

  Hinweis: das „Hybrid Cloud Bundle“ ist bei Backup und Recovery von BlueXP nicht erforderlich.

  Erfahren Sie, wie Sie "Management Ihrer Cluster-Lizenzen".

- Zeit und Zeitzone sind korrekt eingestellt. Erfahren Sie, wie Sie "Konfigurieren Sie die Cluster-Zeit".
- Wenn Sie Daten replizieren möchten, sollten Sie vor der Replizierung von Daten überprüfen, ob auf den Quell- und Zielsystemen kompatible ONTAP-Versionen ausgeführt werden.

  "Zeigen Sie kompatible ONTAP Versionen für SnapMirror Beziehungen an".

ONTAP Netzwerkanforderungen für Daten-Backups im Objekt-Storage prüfen

Sie müssen die folgenden Anforderungen auf dem System konfigurieren, das eine Verbindung zu Objekt-Storage herstellt.

- Wenn Sie eine Fan-out-Backup-Architektur verwenden, müssen die folgenden Einstellungen auf dem *primary*-Speichersystem konfiguriert werden.
- Wenn Sie eine kaskadierte Backup-Architektur verwenden, müssen die folgenden Einstellungen auf dem *Secondary*-Speichersystem konfiguriert werden.

Die folgenden Netzwerkanforderungen für ONTAP-Cluster sind erforderlich:

- 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 BlueXP Backup und Recovery einrichten, werden Sie aufgefordert, den IPspace 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 Objektspeicher zu erhalten.
- Aktualisieren Sie bei Bedarf die Firewall-Regeln, um die Verbindungen des BlueXP Backup- und Recovery-Service von ONTAP zu dem Objekt-Storage über den angegebenen Port (normalerweise Port 443) und den Datenverkehr der Namensauflösung von der Storage-VM zum DNS-Server über Port 53 (TCP/UDP) zu ermöglichen.

Überprüfen Sie die ONTAP Netzwerkanforderungen für die Replizierung von Volumes

Wenn Sie planen, mithilfe von BlueXP Backup und Recovery replizierte Volumes auf einem sekundären ONTAP System zu erstellen, stellen Sie sicher, dass die Quell- und Zielsysteme die folgenden Netzwerkanforderungen erfüllen.

Netzwerkanforderungen für On-Premises-ONTAP

- Wenn sich der Cluster an Ihrem Standort befindet, sollten Sie über eine Verbindung zwischen Ihrem Unternehmensnetzwerk und Ihrem virtuellen Netzwerk des Cloud-Providers verfügen. Hierbei handelt es sich in der Regel um eine VPN-Verbindung.
- ONTAP Cluster müssen zusätzliche Subnetz-, Port-, Firewall- und Cluster-Anforderungen erfüllen.

  Da Sie Daten auf Cloud Volumes ONTAP oder auf lokale Systeme replizieren können, prüfen Sie Peering-Anforderungen für lokale ONTAP Systeme. "Anzeigen von Voraussetzungen für Cluster-Peering in der ONTAP-Dokumentation".

Netzwerkanforderungen für Cloud Volumes ONTAP

- Die Sicherheitsgruppe der Instanz muss die erforderlichen ein- und ausgehenden Regeln enthalten: Speziell Regeln für ICMP und die Ports 11104 und 11105. Diese Regeln sind in der vordefinierten Sicherheitsgruppe enthalten.

StorageGRID als Backup-Ziel vorbereiten

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

Weitere Informationen zu DataLock und Ransomware-Schutz-Anforderungen für StorageGRID, siehe "Richtlinienoptionen für das Backup an ein Objekt".

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.

Für das Tiering älterer Backups in einen Cloud-Archiv-Storage müssen Ihre StorageGRID Systeme Version 11.3 oder höher ausführen. Darüber hinaus müssen Ihre StorageGRID-Systeme im BlueXP Bildschirm erkannt werden.

Zur Nutzung des Archivspeichers ist ein IP-Zugriff auf den Admin-Knoten erforderlich.

Gateway-IP-Zugriff ist immer erforderlich.

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 BlueXP Backup und Recovery für Authentifizierung und 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.

Bereiten Sie die Archivierung älterer Backup-Dateien im Public-Cloud-Storage vor

Durch das Tiering älterer Backup-Dateien im Archiv-Storage sparen Sie Kosten, da Sie für Backups, die Sie möglicherweise nicht benötigen, eine kostengünstigere Storage-Klasse verwenden. StorageGRID ist eine lokale (Private Cloud) Lösung, die keinen Archiv-Storage bietet, aber ältere Backup-Dateien in einen Public Cloud-Archiv-Storage verschieben kann. Bei dieser Art werden Daten, die auf Cloud-Speicher verteilt sind oder aus dem Cloud-Speicher wiederhergestellt werden, zwischen StorageGRID und dem Cloud-Speicher verschoben. BlueXP ist an diesem Datentransfer nicht beteiligt.

Die aktuelle Unterstützung ermöglicht Ihnen die Archivierung von Backups in AWS *S3 Glacier*/*S3 Glacier Deep Archive* oder *Azure Archive* Storage.

ONTAP-Anforderungen

- Ihr Cluster muss ONTAP 9.12.1 oder höher verwenden.

StorageGRID-Anforderungen

- Ihr StorageGRID muss 11.4 oder höher verwenden.

- Ihr StorageGRID muss sein "Entdeckt und verfügbar im BlueXP Canvas".

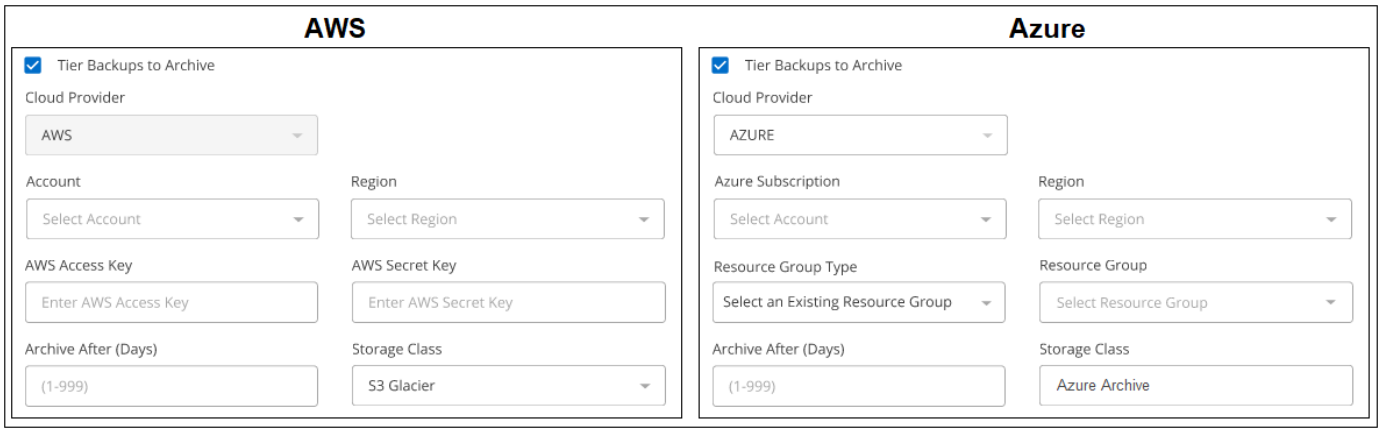
Amazon S3 Anforderungen

- Sie müssen sich für den Speicherplatz, auf dem sich Ihre archivierten Backups befinden, bei einem Amazon S3-Konto anmelden.
- Zudem stehen für das Tiering von Backups AWS S3 Glacier oder S3 Glacier Deep Archive Storage zur Verfügung. "Weitere Informationen zu AWS Archivierungs-Tiers".
- StorageGRID sollte über einen vollständigen Kontrollzugriff auf den Bucket verfügen (`s3:*`Ist dies jedoch nicht möglich, muss die Bucket-Richtlinie StorageGRID die folgenden S3-Berechtigungen erteilen:
  - `s3:AbortMultipartUpload`
  - `s3:DeleteObject`
  - `s3:GetObject`
  - `s3:ListBucket`
  - `s3:ListBucketMultipartUploads`
  - `s3:ListMultipartUploadParts`
  - `s3:PutObject`
  - `s3:RestoreObject`

Azure Blob Anforderungen

- Sie müssen sich für ein Azure-Abonnement anmelden, um den Speicherplatz zu erhalten, auf dem sich Ihre archivierten Backups befinden.
- Mit dem Aktivierungsassistenten können Sie eine vorhandene Ressourcengruppe zur Verwaltung des Blob-Containers verwenden, der die Backups speichert, oder eine neue Ressourcengruppe erstellen.

Wenn Sie die Archivierungseinstellungen für die Backup-Richtlinie für Ihren Cluster definieren, geben Sie Ihre Zugangsdaten für den Cloud-Provider ein und wählen die gewünschte Storage-Klasse aus. BlueXP Backup und Recovery erstellt den Cloud-Bucket, wenn Sie das Backup für das Cluster aktivieren. Nachfolgend sind die für AWS und Azure Archiv-Storage erforderlichen Informationen dargestellt.



Die von Ihnen ausgewählten Archivierungsrichtlinien-Einstellungen generieren eine Information Lifecycle Management (ILM)-Richtlinie in StorageGRID und fügen die Einstellungen als „Regeln“ ein.

- Wenn bereits eine aktive ILM-Richtlinie vorhanden ist, werden der ILM-Richtlinie neue Regeln hinzugefügt,

um die Daten auf die Archiv-Tier zu verschieben.

- Wenn eine ILM-Richtlinie bereits im Status „vorgeschlagen“ vorhanden ist, ist die Erstellung und Aktivierung einer neuen ILM-Richtlinie nicht möglich. "Erfahren Sie mehr über StorageGRID ILM-Richtlinien und -Regeln".

Aktivieren Sie Backups auf Ihren ONTAP Volumes

Sie können Backups jederzeit direkt aus Ihrer On-Premises-Arbeitsumgebung heraus aktivieren.

Ein Assistent führt Sie durch die folgenden wichtigen Schritte:

- die Sie sichern möchten
- Backup-Strategie definieren
- Überprüfen Sie Ihre Auswahl

Das können Sie auch Zeigt die API-Befehle an Kopieren Sie im Überprüfungsschritt den Code, um die Backup-Aktivierung für zukünftige Arbeitsumgebungen zu automatisieren.

Starten Sie den Assistenten

Schritte

1. Greifen Sie auf eine der folgenden Arten auf den Assistenten zur Aktivierung von Backup und Recovery zu:

   - Wählen Sie auf dem BlueXP-Bildschirm die Arbeitsumgebung aus, und wählen Sie im rechten Bereich neben dem Sicherungs- und Wiederherstellungsdienst die Option **Enable > Backup Volumes** aus.

     Wenn das Ziel für die Backups als Arbeitsumgebung auf dem Bildschirm vorhanden ist, können Sie das ONTAP-Cluster auf den Objektspeicher ziehen.

   - Wählen Sie in der Sicherungs- und Wiederherstellungsleiste **Volumes** aus. Wählen Sie auf der Registerkarte Volumes die Option **actions (…)** aus und wählen Sie **Activate Backup** für ein einzelnes Volume (das noch nicht über Replikation oder Backup auf Objektspeicher verfügt).

   Auf der Seite Einführung des Assistenten werden die Schutzoptionen einschließlich lokaler Snapshots, Replikation und Backups angezeigt. Wenn Sie die zweite Option in diesem Schritt gewählt haben, wird die Seite „Backup-Strategie definieren“ mit einem ausgewählten Volume angezeigt.

2. Fahren Sie mit den folgenden Optionen fort:

   - Wenn Sie bereits einen BlueXP Connector haben, sind Sie fertig. Wählen Sie einfach **Weiter**.
   - Wenn Sie noch keinen BlueXP Connector haben, wird die Option **Connector hinzufügen** angezeigt. Siehe Bereiten Sie Ihren BlueXP Connector vor.

Wählen Sie die Volumes aus, die Sie sichern möchten

Wählen Sie die Volumes aus, die Sie schützen möchten. Ein geschütztes Volume verfügt über eine oder mehrere der folgenden Elemente: Snapshot-Richtlinie, Replizierungsrichtlinie und Richtlinie für das Backup in ein Objekt.

Sie können FlexVol- oder FlexGroup-Volumes schützen. Sie können jedoch keine Kombination dieser Volumes auswählen, wenn Sie Backups für eine funktionierende Umgebung aktivieren. Informieren Sie sich darüber "Aktivieren Sie das Backup für zusätzliche Volumes in der Arbeitsumgebung" (FlexVol oder FlexGroup), nachdem Sie das Backup für die ersten Volumes konfiguriert haben.

- Sie können ein Backup nur auf einem einzelnen FlexGroup Volume gleichzeitig aktivieren.
- Die ausgewählten Volumes müssen dieselbe SnapLock-Einstellung aufweisen. Auf allen Volumes muss SnapLock Enterprise aktiviert oder SnapLock deaktiviert sein.

Schritte

Beachten Sie, dass die Richtlinien, die Sie später auswählen, diese vorhandenen Richtlinien überschreiben, wenn die von Ihnen ausgewählten Volumes bereits Snapshot- oder Replikationsrichtlinien angewendet haben.

1. Wählen Sie auf der Seite Volumes auswählen das Volume oder die Volumes aus, die Sie schützen möchten.
   - Optional können Sie die Zeilen so filtern, dass nur Volumes mit bestimmten Volumentypen, Stilen und mehr angezeigt werden, um die Auswahl zu erleichtern.
   - Nachdem Sie das erste Volume ausgewählt haben, können Sie alle FlexVol Volumes auswählen (FlexGroup Volumes können nur einzeln ausgewählt werden). Um alle vorhandenen FlexVol-Volumes zu sichern, aktivieren Sie zuerst ein Volume und dann das Kontrollkästchen in der Titelzeile. (

).
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume (

).
2. Wählen Sie **Weiter**.

Backup-Strategie definieren

Zur Definition der Backup-Strategie gehören die folgenden Optionen:

- Unabhängig davon, ob Sie eine oder alle Backup-Optionen: Lokale Snapshots, Replikation und Backup-to-Object-Storage möchten
- Der Netapp Architektur Sind
- Lokale Snapshot-Richtlinie
- Replikationsziel und -Richtlinie

Wenn die ausgewählten Volumes andere Snapshot- und Replikationsrichtlinien haben als die in diesem Schritt ausgewählten Richtlinien, werden die vorhandenen Richtlinien überschrieben.

- Backup von Objekt-Storage-Informationen (Provider-, Verschlüsselungs-, Netzwerk-, Backup-Richtlinien- und Exportoptionen)

Schritte

1. Wählen Sie auf der Seite Backup-Strategie definieren eine oder alle der folgenden Optionen aus. Alle drei sind standardmäßig ausgewählt:
   - **Lokale Snapshots**: Wenn Sie eine Replikation oder Sicherung auf Objektspeicher durchführen, müssen lokale Snapshots erstellt werden.
   - **Replikation**: Erstellt replizierte Volumes auf einem anderen ONTAP-Speichersystem.
   - **Backup**: Sichert Volumes auf Objektspeicher.
2. **Architektur**: Wenn Sie sowohl Replikation als auch Backup gewählt haben, wählen Sie einen der folgenden Informationsflüsse:
   - **Kaskadierung**: Informationen fließen vom primären zum sekundären und dann vom sekundären zum

Objektspeicher.

- **Fan Out**: Informationen fließen vom primären zum sekundären *und* vom primären zum Objektspeicher.

  Einzelheiten zu diesen Architekturen finden Sie unter "Planen Sie Ihren Weg zum Schutz".

3. **Lokaler Snapshot**: Wählen Sie eine vorhandene Snapshot-Richtlinie aus oder erstellen Sie eine neue.

   Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung des Snapshots finden Sie unter "Erstellen einer Richtlinie".

   Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

   - Geben Sie den Namen der Richtlinie ein.
   - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
   - Wählen Sie **Erstellen**.

4. **Replikation**: Stellen Sie die folgenden Optionen ein:

   - **Replikationsziel**: Wählen Sie die Zielarbeitsumgebung und SVM aus. Wählen Sie optional das Zielaggregat oder die Aggregate und das Präfix oder Suffix aus, die dem Namen des replizierten Volumes hinzugefügt werden sollen.
   - **Replikationsrichtlinie**: Wählen Sie eine vorhandene Replikationsrichtlinie oder erstellen Sie eine.

     Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Replikation finden Sie unter "Erstellen einer Richtlinie".

     Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

     - Geben Sie den Namen der Richtlinie ein.
     - Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
     - Wählen Sie **Erstellen**.

5. **Backup auf Objekt**: Wenn Sie **Backup** ausgewählt haben, stellen Sie die folgenden Optionen ein:

   - **Anbieter**: Wählen Sie **StorageGRID**.
   - **Provider-Einstellungen**: Geben Sie den Provider-Gateway-Knoten FQDN-Details, Port, Zugriffsschlüssel und geheimen Schlüssel ein.

     Der Zugriffsschlüssel und der geheime Schlüssel gelten für den IAM-Benutzer, den Sie erstellt haben, um dem ONTAP-Cluster Zugriff auf den Bucket zu geben.

   - **Netzwerk**: Wählen Sie den IPspace im ONTAP Cluster, wo 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 Auswahl des korrekten IPspaces wird sichergestellt, dass BlueXP Backup und Recovery eine Verbindung von ONTAP zu Ihrem StorageGRID Objekt-Storage einrichten können.

   - **Backup Policy**: Wählen Sie eine vorhandene Richtlinie für das Objekt-Storage-Backup aus oder

erstellen Sie eine.

Informationen zum Erstellen einer benutzerdefinierten Richtlinie vor der Aktivierung der Sicherung finden Sie unter "Erstellen einer Richtlinie".

Um eine Richtlinie zu erstellen, wählen Sie **Create New Policy** aus, und führen Sie die folgenden Schritte aus:

- Geben Sie den Namen der Richtlinie ein.
- Wählen Sie bis zu 5 Schichtpläne aus, die in der Regel unterschiedliche Frequenzen haben.
- Legen Sie für Backup-to-Object-Richtlinien die Einstellungen für DataLock und Ransomware-Schutz fest. Weitere Informationen zu DataLock und Ransomware-Schutz finden Sie unter "Richtlinieneinstellungen für Backup-to-Object".

  Wenn Ihr Cluster ONTAP 9.11.1 oder höher verwendet, können Sie Ihre Backups vor dem Löschen und Ransomware-Angriffen schützen, indem Sie *DataLock und Ransomware Protection* konfigurieren. *DataLock* schützt Ihre Backup-Dateien vor Änderung oder Löschung, und *Ransomware Protection* scannt Ihre Backup-Dateien, um Beweise für einen Ransomware-Angriff in Ihren Backup-Dateien zu suchen.

- Wählen Sie **Erstellen**.

Wenn in Ihrem Cluster ONTAP 9.12.1 oder höher verwendet wird und Ihr StorageGRID System Version 11.4 oder höher verwendet, können Sie ältere Backups nach einer bestimmten Anzahl von Tagen in Tiers aus Public-Cloud-Archiven verschieben. Aktuell werden weitere Support für AWS S3 Glacier/S3 Glacier Deep Archive oder Azure Archive Storage Tiers unterstützt. Lesen Sie, wie Sie Ihre Systeme für diese Funktion konfigurieren.

- **Tiering Backup in Public Cloud**: Wählen Sie den Cloud-Provider aus, zu dem Sie Backups verschieben möchten, und geben Sie die Provider-Details ein.

  Wählen Sie einen neuen StorageGRID-Cluster aus oder erstellen Sie ihn. Weitere Informationen zum Erstellen eines StorageGRID Clusters, damit BlueXP ihn erkennen kann, finden Sie unter "StorageGRID-Dokumentation".

- **Exportieren vorhandener Snapshot-Kopien als Backup-Kopien in den Objektspeicher**: Wenn es lokale Snapshot-Kopien für Volumes in dieser Arbeitsumgebung gibt, die mit dem Backup-Zeitplan-Label übereinstimmen, das Sie gerade für diese Arbeitsumgebung ausgewählt haben (z. B. täglich, wöchentlich usw.), wird diese zusätzliche Eingabeaufforderung angezeigt. Aktivieren Sie dieses Kontrollkästchen, damit alle historischen Snapshots als Backup-Dateien in den Objektspeicher kopiert werden, um einen möglichst vollständigen Schutz für Ihre Volumes zu gewährleisten.

6. Wählen Sie **Weiter**.

Überprüfen Sie Ihre Auswahl

Dies ist die Möglichkeit, Ihre Auswahl zu überprüfen und gegebenenfalls Anpassungen vorzunehmen.

Schritte

1. Überprüfen Sie auf der Seite „Überprüfen“ Ihre Auswahl.
2. Aktivieren Sie optional das Kontrollkästchen, um * die Snapshot-Policy-Labels automatisch mit den Label der Replikations- und Backup-Policy* zu synchronisieren. Dadurch werden Snapshots mit einem Label erstellt, das den Labels in den Replizierungs- und Backup-Richtlinien entspricht.

3. Wählen Sie **Sicherung Aktivieren**.

Ergebnis

Mit BlueXP Backup und Recovery werden erste Backups Ihrer Volumes erstellt. Der Basistransfer des replizierten Volumes und der Backup-Datei beinhaltet eine vollständige Kopie der Quelldaten. Nachfolgende Transfers enthalten differenzielle Kopien der primären Storage-Daten, die in Snapshot Kopien enthalten sind.

Ein repliziertes Volume wird im Zielcluster erstellt, das mit dem primären Storage Volume synchronisiert wird.

Ein S3-Bucket wird in dem Servicekonto erstellt, das durch den eingegebenen S3-Zugriffsschlüssel und geheimen Schlüssel angegeben ist, und die Backup-Dateien werden dort gespeichert.

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".

Zeigt die API-Befehle an

Möglicherweise möchten Sie die API-Befehle anzeigen und optional kopieren, die im Assistenten Sicherung und Wiederherstellung aktivieren verwendet werden. Dies ist möglicherweise sinnvoll, um die Backup-Aktivierung in zukünftigen Arbeitsumgebungen zu automatisieren.

Schritte

1. Wählen Sie im Assistenten Backup und Recovery aktivieren **API-Anforderung anzeigen** aus.
2. Um die Befehle in die Zwischenablage zu kopieren, wählen Sie das Symbol **Kopieren**.

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 unter anderem die Änderung der verfügbaren Netzwerkbandbreite für das Hochladen von Backups in den Objekt-Storage, die Änderung der automatischen Backup-Einstellung für zukünftige Volumes.
- Das können Sie auch "Wiederherstellung von Volumes, Ordnern oder einzelnen Dateien aus einer Sicherungsdatei" Auf ein lokales ONTAP System zugreifen:

Migrieren Sie Volumes mit SnapMirror zur Cloud. Synchronisieren Sie sie erneut mit BlueXP Backup und Recovery.

Die SnapMirror to Cloud Resync-Funktion in BlueXP Backup und Recovery optimiert den Datenschutz und die Kontinuität während Volumemigrationen in NetApp-Umgebungen. Bei der Migration eines Volumes mithilfe von SnapMirror Logical Replication (LRSE), von einer lokalen NetApp Implementierung zu einer anderen oder zu einer Cloud-basierten Lösung wie Cloud Volumes ONTAP oder Cloud Volumes Service sorgt SnapMirror zu Cloud Resync dafür, dass vorhandene Cloud-Backups intakt und betriebsbereit bleiben.

Durch diese Funktion wird ein zeitaufwendiger und ressourcenintensiver Neustart des Basisplans überflüssig,

sodass Backup-Vorgänge nach der Migration fortgesetzt werden können. Diese Funktion ist in Workload-Migrationsszenarien nützlich, da sie sowohl FlexVols als auch FlexGroups unterstützt. Sie ist ab ONTAP Version 9.16.1 verfügbar.

Durch die Aufrechterhaltung der Backup-Kontinuität über verschiedene Umgebungen hinweg verbessert SnapMirror to Cloud Resync die betriebliche Effizienz und verringert die Komplexität des Datenmanagements in der Hybrid Cloud und Multi Cloud.

BlueXP Backup und Recovery SnapMirror zu Cloud Resync funktioniert

Bei einer technischen Aktualisierung oder der Migration von Volumes von einem ONTAP Cluster zu einem anderen ist es wichtig, dass Ihre Backups weiterhin ohne Unterbrechung arbeiten. BlueXP SnapMirror für Backup und Recovery in die Cloud Resync hilft dabei, da Ihre Cloud-Backups auch nach einer Volume-Migration konsistent bleiben.

Hier ein Beispiel:

Stellen Sie sich vor, Sie haben ein lokales Volume namens Vol1a. Dieses Volume verfügt über drei Snapshots: S1, S2 und S3. Diese Snapshots sind wie Wiederherstellungspunkte. Vol1 wird bereits über SnapMirror to Cloud (SM-C) in einem Endpunkt eines Cloud-Objektspeichers gesichert. Bisher wurden jedoch nur S1 und S2 im Objektspeicher gesichert.

Jetzt möchten Sie Vol1 zu einem anderen ONTAP-Cluster migrieren. Hierzu erstellen Sie eine SnapMirror Logical Replication (LRSE)-Beziehung zu einem neuen Cloud-Volume namens Vol1b. Dadurch werden alle drei Snapshots – S1, S2 und S3 – von Vol1a nach Vol1b übertragen.

Nach Abschluss der Migration haben Sie die folgende Einrichtung:

- Die ursprüngliche SM-C-Beziehung (Vol1a → Object Store) wird gelöscht.
- Die LRSE-Beziehung (Vol1a → Vol1b) wird ebenfalls gelöscht.
- Vol1b ist jetzt Ihr aktives Volume.

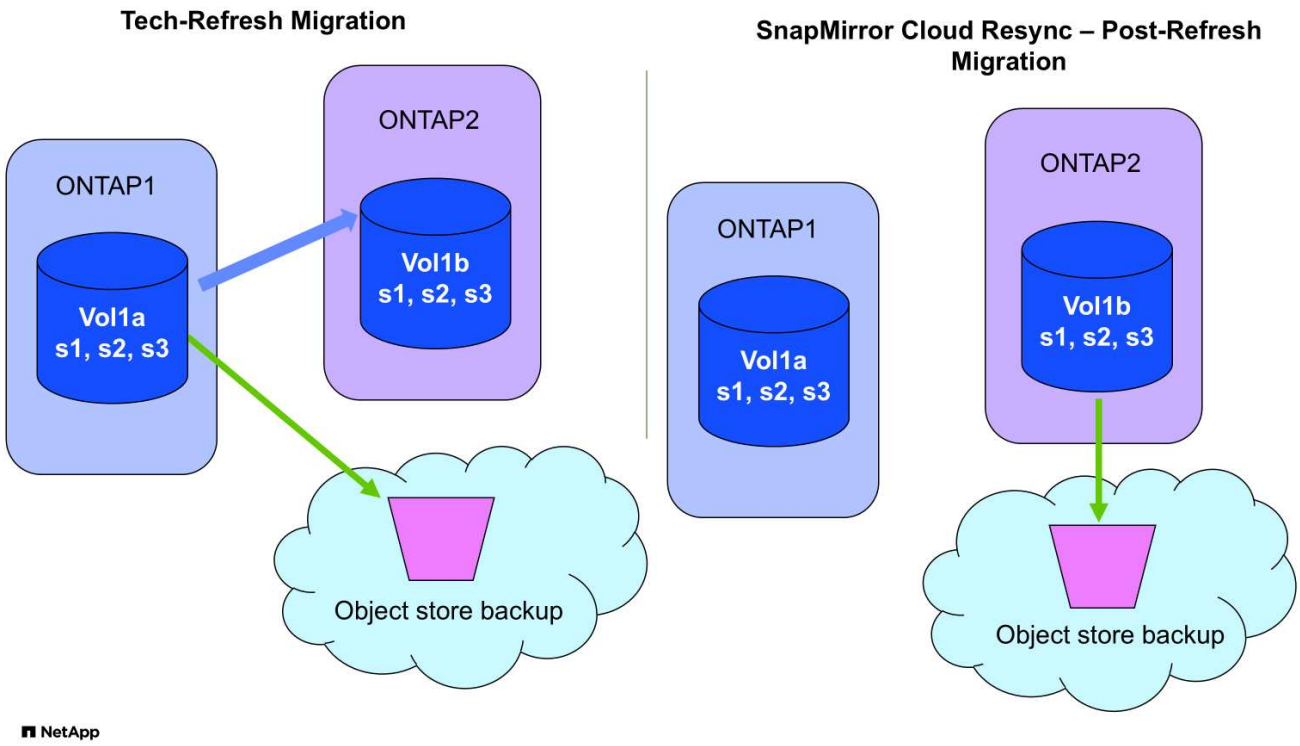
An diesem Punkt möchten Sie weiterhin das Backup von Vol1b am gleichen Cloud-Endpunkt fortsetzen. Aber anstatt ein vollständiges Backup von Grund auf neu zu starten (was Zeit und Ressourcen beanspruchen würde), verwenden Sie SnapMirror zu Cloud Resync.

So funktioniert die Resynchronisierung:

- Das System sucht nach einem gemeinsamen Snapshot zwischen Vol1a und Objektspeicher. In diesem Fall haben beide S2.
- Aufgrund dieses gemeinsamen Snapshots muss das System nur die inkrementellen Änderungen zwischen S2 und S3 übertragen.

Das bedeutet, dass nur die neuen Daten, die nach S2 hinzugefügt wurden, an den Objektspeicher gesendet werden, nicht an das gesamte Volume.

Dadurch wird verhindert, dass bereits gesicherte Daten erneut gesendet werden, Bandbreite eingespart wird und die Backup-Kette nach der Migration reibungslos weiterläuft.



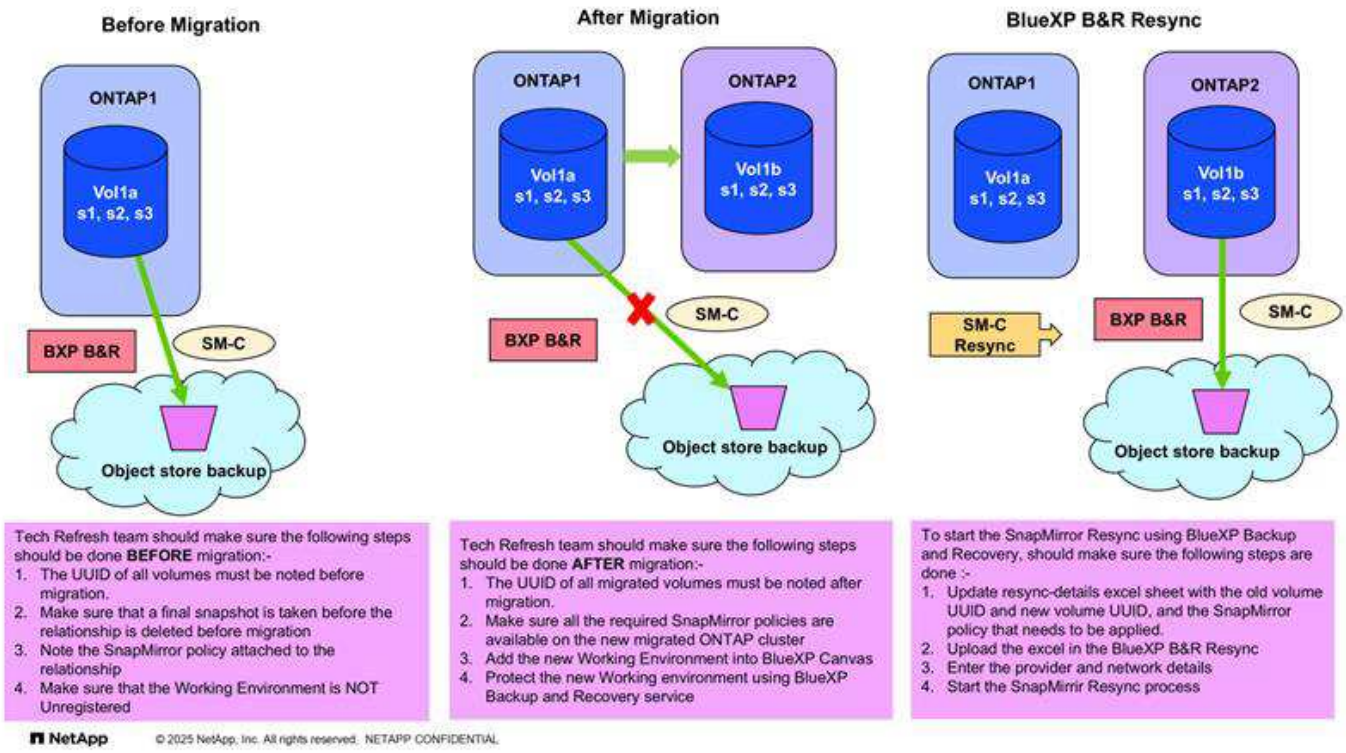
Verfahrenshinweise

- Auf dem Ziel-ONTAP-Cluster muss ONTAP Version 9.16.1 oder höher ausgeführt werden.
- Der alte Quell-ONTAP-Cluster muss mit BlueXP Backup und Recovery geschützt werden.
- Migrationen und technische Aktualisierungen werden nicht mit BlueXP Backup und Recovery durchgeführt. Sie sollten von einem Professional Services Team oder einem qualifizierten Storage-Administrator durchgeführt werden.
- Ein NetApp Migrationsteam ist zuständig für die Erstellung der SnapMirror Beziehung zwischen den ONTAP Quell- und Ziel-Clustern, um die Volume-Migration zu vereinfachen.
- Stellen Sie sicher, dass die Migration bei einer Technologieaktualisierung auf SnapMirror basiert.
- Resync von SnapMirror zu Cloud nach Migrationen mit SVM-Migrate-, SVM-DR- oder Head-Swap-Methoden werden derzeit nicht unterstützt.

Migration von Volumes mit SnapMirror zur Cloud-Neusynchronisierung

Die Migration von Volumes mit SnapMirror zu Cloud Resync umfasst die folgenden wichtigen Schritte, die im Folgenden genauer beschrieben werden:

- **Folgen Sie eine Checkliste vor der Migration**: Vor Beginn der Migration stellt ein NetApp-Team für die Technologieaktualisierung sicher, dass die folgenden Voraussetzungen erfüllt sind, um Datenverluste zu vermeiden und einen reibungslosen Migrationsprozess zu gewährleisten.
- **Folgen Sie eine Checkliste nach der Migration**: Nach der Migration stellt ein NetApp Tech Refresh Team sicher, dass die folgenden Schritte abgeschlossen sind, um den Schutz zu schaffen und die Resynchronisierung vorzubereiten.
- **SnapMirror zu Cloud Resync durchführen**: Nach der Migration führt ein NetApp Team für die Technologieaktualisierung einen SnapMirror zu Cloud Resync-Vorgang durch, um Cloud Backups von den neu migrierten Volumes fortzusetzen.



Checkliste vor der Migration befolgen

Vor Beginn der Migration stellt ein NetApp Team für Technologieaktualisierungen die folgenden Voraussetzungen sicher, um Datenverluste zu vermeiden und einen reibungslosen Migrationsprozess zu gewährleisten.

1. Sicherung aller zu migrierenden Volumes mittels BlueXP Backup und Recovery sicherstellen
2. Notieren Sie die UUIDs der Volume-Instanz. Notieren Sie sich die Instanz-UUIDs aller Volumes, bevor Sie die Migration starten. Diese Kennungen sind für das spätere Zuordnen und Neusynchronisieren von Bedeutung.
3. Erstellen Sie von jedem Volume einen endgültigen Snapshot, um den aktuellen Status beizubehalten, bevor Sie SnapMirror-Beziehungen löschen.
4. Dokumentieren der SnapMirror-Richtlinien. Notieren Sie die SnapMirror-Richtlinie, die derzeit der Beziehung jedes Volumes zugeordnet ist. Dies wird später während der SnapMirror-to-Cloud-Neusynchronisierung erforderlich sein.
5. Löschen Sie die SnapMirror-Cloud-Beziehungen mit dem Objektspeicher.
6. Erstellung einer standardmäßigen SnapMirror-Beziehung mit dem neuen ONTAP-Cluster zur Migration des Volumes auf den neuen Ziel-ONTAP-Cluster

Folgen Sie einer Checkliste nach der Migration

Nach der Migration stellt ein NetApp Team für Technologieaktualisierungen sicher, dass die folgenden Schritte durchgeführt werden, um den Schutz einzurichten und die Neusynchronisierung vorzubereiten.

1. Notieren Sie die UUIDs der neuen Volume-Instanz aller migrierten Volumes im ONTAP-Zielcluster.
2. Vergewissern Sie sich, dass alle erforderlichen SnapMirror-Richtlinien, die im alten ONTAP-Cluster verfügbar waren, im neuen ONTAP-Cluster richtig konfiguriert sind.

3. Fügen Sie das neue ONTAP-Cluster als Arbeitsumgebung im BlueXP -Bildschirm hinzu.

SnapMirror-zu-Cloud-Neusynchronisierung durchführen

Nach der Migration führt ein NetApp Team für Technologieaktualisierungen einen SnapMirror-zu-Cloud-Resynchronisierungsvorgang durch, um Cloud-Backups der neu migrierten Volumes wieder aufzunehmen.

1. Fügen Sie das neue ONTAP-Cluster als Arbeitsumgebung im BlueXP -Bildschirm hinzu.
2. Sehen Sie sich die Seite BlueXP Backup and Recovery Volumes an, um sicherzustellen, dass die Details der alten Arbeitsumgebung verfügbar sind.
3. Wählen Sie auf der Seite BlueXP Backup and Recovery Volumes die Option **Backup Settings** aus.
4. Wählen Sie im Menü **Resync Backup**.
5. Führen Sie auf der Seite Arbeitsumgebung neu synchronisieren die folgenden Schritte aus:
   a. **Neue Quellumgebung**: Geben Sie den neuen ONTAP-Cluster ein, wo die Volumes migriert wurden.
   b. **Existierender Target Object Store**: Wählen Sie den Zielobjektspeicher aus, der die Backups aus der alten Quell-Arbeitsumgebung enthält.
6. Wählen Sie **CSV-Vorlage herunterladen**, um die Excel-Tabelle Resync Details herunterzuladen. Geben Sie in diesem Datenblatt die Details der zu migrierenden Volumes ein. Geben Sie in der CSV-Datei die folgenden Details ein:
   - Die alte Volume-Instanz-UUID aus dem Quell-Cluster
   - Die neue Volume-Instanz-UUID aus dem Ziel-Cluster
   - Die SnapMirror-Richtlinie, die auf die neue Beziehung anzuwenden ist.
7. Wählen Sie **Upload** unter **Upload Volume Mapping Details** aus, um das fertige CSV-Blatt in die BlueXP Backup- und Recovery-Benutzeroberfläche hochzuladen.
8. Geben Sie die für die Resynchronisierung erforderlichen Provider- und Netzwerkkonfigurationsinformationen ein.
9. Wählen Sie **Absenden**, um den Validierungsprozess zu starten.

   Durch BlueXP Backup und Recovery wird gewährleistet, dass jedes für die Resynchronisierung ausgewählte Volume über mindestens einen gemeinsamen Snapshot verfügt. So wird sichergestellt, dass die Volumes für die Neusynchronisierung von SnapMirror zu Cloud bereit sind.

10. Überprüfen Sie die Validierungsergebnisse, einschließlich der neuen Quell-Volume-Namen und des Resync-Status für jedes Volume.
11. Prüfen Sie die Eignung von Volumes. Das System prüft, ob die Volumes für eine Neusynchronisierung geeignet sind. Wenn ein Volume nicht geeignet ist, bedeutet dies, dass kein gemeinsamer Snapshot gefunden wurde.

    Damit Volumes für den Resync-Vorgang zwischen SnapMirror und Cloud geeignet bleiben, erstellen Sie einen endgültigen Snapshot jedes Volumes, bevor Sie SnapMirror-Beziehungen vor der Migration löschen. Damit bleibt der aktuelle Zustand der Daten erhalten.

12. Wählen Sie **Resync**, um die Neusynchronisierung zu starten. Das System verwendet den gemeinsamen Snapshot, um nur die inkrementellen Änderungen zu übertragen, um die Kontinuität der Sicherung zu gewährleisten.
13. Überwachen Sie den Resyn-Prozess auf der Seite Job Monitor.

Verwalten Sie Backups für Ihre ONTAP-Systeme mit BlueXP Backup und Recovery

Verwalten Sie mit BlueXP Backup und Recovery Backups für Ihre Cloud Volumes ONTAP- und lokalen ONTAP-Systeme, indem Sie den Backup-Zeitplan ändern, Volume-Backups aktivieren/deaktivieren, Backups anhalten, Backups löschen und mehr. Dies umfasst alle Arten von Backups, einschließlich Snapshot Kopien, replizierte Volumes und Backup-Dateien im Objektspeicher.

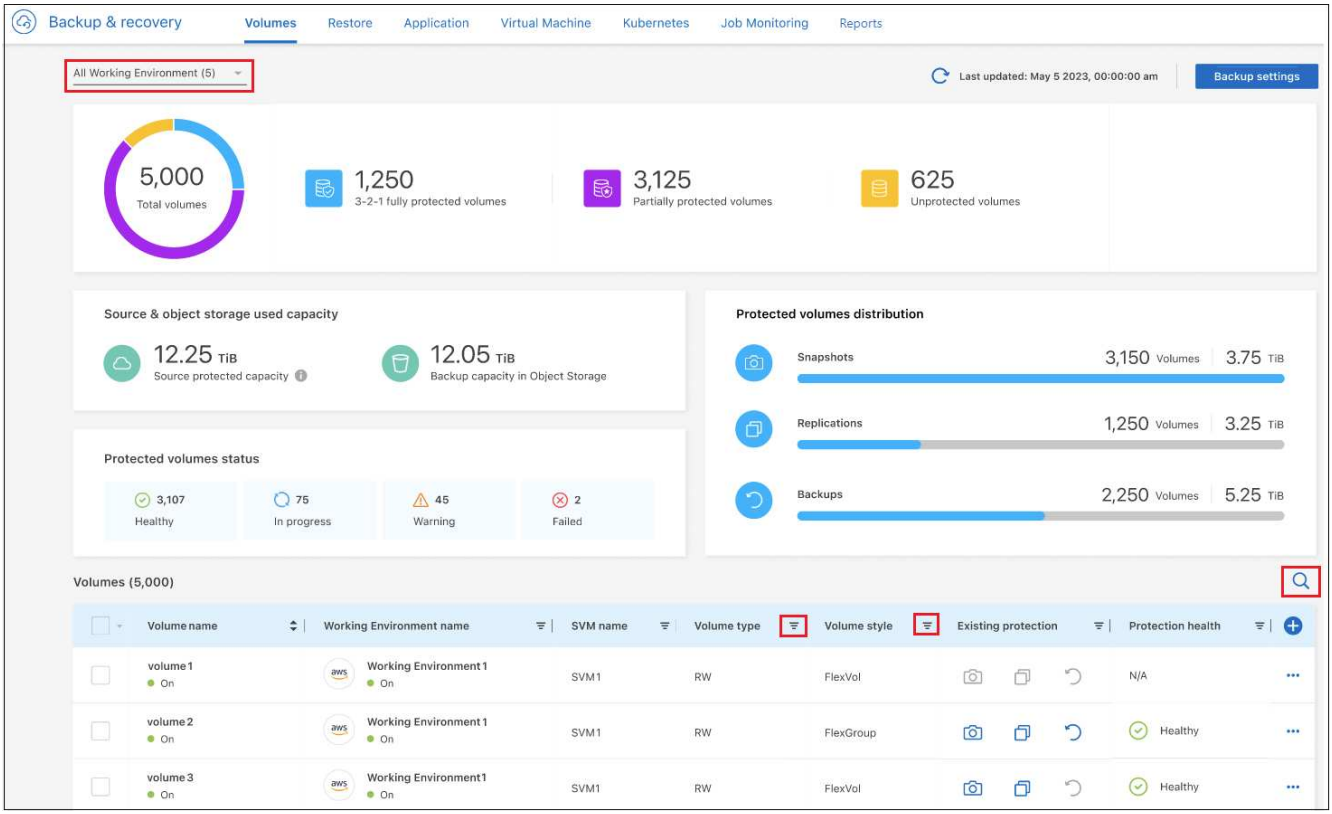
Backup-Dateien dürfen nicht direkt auf Ihren Storage-Systemen oder in Ihrer Cloud-Provider-Umgebung gemanagt oder geändert werden. Dies kann die Dateien beschädigen und zu einer nicht unterstützten Konfiguration führen.

Anzeigen des Backup-Status von Volumes in Ihren Arbeitsumgebungen

Sie können eine Liste aller Volumes anzeigen, die derzeit im Volume Backup Dashboard gesichert werden. Dies umfasst alle Arten von Backups, einschließlich Snapshot Kopien, replizierte Volumes und Backup-Dateien im Objektspeicher. Sie können auch die Volumes in den Arbeitsumgebungen anzeigen, die derzeit nicht gesichert werden.

Schritte

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



3. Wenn Sie nach bestimmten Volumes in bestimmten Arbeitsumgebungen suchen, können Sie die Liste

nach Arbeitsumgebung und Volumen verfeinern. Sie können auch den Suchfilter verwenden oder die Spalten nach Volume-Stil (FlexVol oder FlexGroup), Volume-Typ und mehr sortieren.

Wählen Sie aus, um zusätzliche Spalten (Aggregate, Sicherheitsstil (Windows oder UNIX), Snapshot-Richtlinie, Replikationsrichtlinie und Backup-Richtlinie) anzuzeigen .

4. Überprüfen Sie den Status der Schutzoptionen in der Spalte „bestehender Schutz“. Die 3 Symbole stehen für „Lokale Snapshot Kopien“, „replizierte Volumes“ und „Backups im Objektspeicher“.

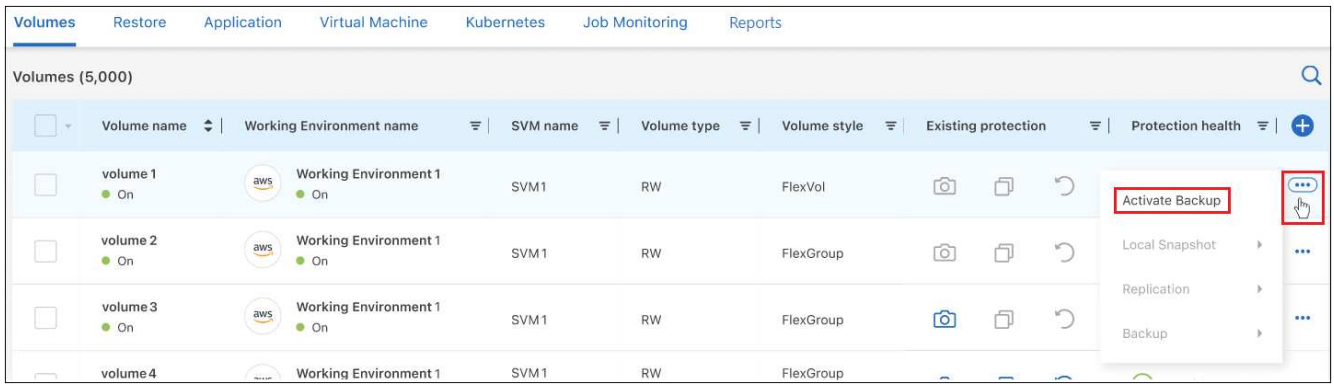
Jedes Symbol ist blau, wenn dieser Sicherungstyp aktiviert ist, und es ist grau, wenn der Sicherungstyp inaktiv ist. Sie können den Mauszeiger über jedes Symbol bewegen, um die verwendete Backup-Richtlinie sowie weitere relevante Informationen für jeden Backup-Typ anzuzeigen.

Aktivieren Sie Backups auf zusätzlichen Volumes in einer funktionierenden Umgebung

Wenn Sie bei der ersten Aktivierung von BlueXP Backup und Recovery nur auf einigen Volumes in einer Arbeitsumgebung das Backup aktiviert haben, können Sie Backups auf weiteren Volumes später aktivieren.

Schritte

1. Geben Sie auf der Registerkarte **Volumes** das Volume an, auf dem Sie Backups aktivieren möchten, und wählen Sie das Menü Aktionen aus ••• Am Ende der Zeile, und wählen Sie **Backup aktivieren**.



2. Wählen Sie auf der Seite *define Backup Strategy* die Backup-Architektur aus, und definieren Sie dann die Richtlinien und andere Details für lokale Snapshot-Kopien, replizierte Volumes und Backup-Dateien. Weitere Informationen zu Backup-Optionen der ersten Volumes, die Sie in dieser Arbeitsumgebung aktiviert haben, finden Sie unter. Klicken Sie anschließend auf **Weiter**.
3. Überprüfen Sie die Backup-Einstellungen für dieses Volume, und klicken Sie dann auf **Sicherung aktivieren**.

Wenn Sie die Sicherung auf mehreren Volumes gleichzeitig mit identischen Backup-Einstellungen aktivieren möchten, finden Sie weitere Informationen unter Bearbeiten Sie die Backup-Einstellungen auf mehreren Volumes Entsprechende Details.

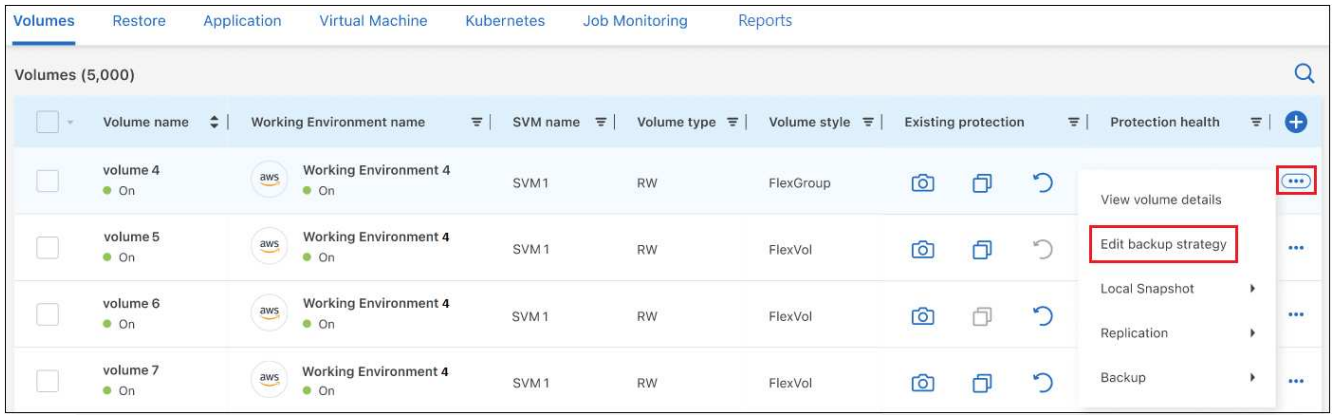
Ändern Sie die Backup-Einstellungen, die vorhandenen Volumes zugewiesen sind

Die Backup-Richtlinien, die Ihren vorhandenen Volumes mit zugewiesenen Richtlinien zugewiesen sind, können geändert werden. Sie können die Richtlinien für Ihre lokalen Snapshot-Kopien, replizierten Volumes und Backup-Dateien ändern. Alle neuen Snapshot-, Replizierungs- oder Backup-Richtlinien, die auf die Volumes angewendet werden sollen, müssen bereits vorhanden sein.

Bearbeiten Sie die Backup-Einstellungen auf einem einzelnen Volume

Schritte

1. Geben Sie auf der Registerkarte **Volumes** das Volume an, das Sie Richtlinienänderungen vornehmen möchten, und wählen Sie das Menü Aktionen aus ••• Am Ende der Zeile, und wählen Sie **Backup-Strategie bearbeiten**.



2. Nehmen Sie auf der Seite *Backup-Strategie bearbeiten* Änderungen an den bestehenden Backup-Richtlinien für lokale Snapshot-Kopien, replizierte Volumes und Sicherungsdateien vor, und klicken Sie auf **Weiter**.

   Wenn Sie bei der Aktivierung von BlueXP Backup und Recovery für diesen Cluster in der anfänglichen Backup-Richtlinie *DataLock und Ransomware-Schutz* für Cloud-Backups aktiviert haben, werden nur weitere Richtlinien angezeigt, die mit DataLock konfiguriert wurden. Und wenn Sie bei der Aktivierung von BlueXP Backup und Recovery *DataLock und Ransomware-Schutz* nicht aktiviert haben, werden Sie nur andere Cloud-Backup-Richtlinien sehen, für die DataLock nicht konfiguriert ist.

3. Überprüfen Sie die Backup-Einstellungen für dieses Volume, und klicken Sie dann auf **Sicherung aktivieren**.

Bearbeiten Sie die Backup-Einstellungen auf mehreren Volumes

Wenn Sie dieselben Backup-Einstellungen auf mehreren Volumes verwenden möchten, können Sie die Backup-Einstellungen auf mehreren Volumes gleichzeitig aktivieren oder bearbeiten. Sie können Volumes ohne Backup-Einstellungen, nur Snapshot-Einstellungen, nur Backups in Cloud-Einstellungen usw. auswählen und umfangreiche Änderungen über all diese Volumes mit unterschiedlichen Backup-Einstellungen vornehmen.

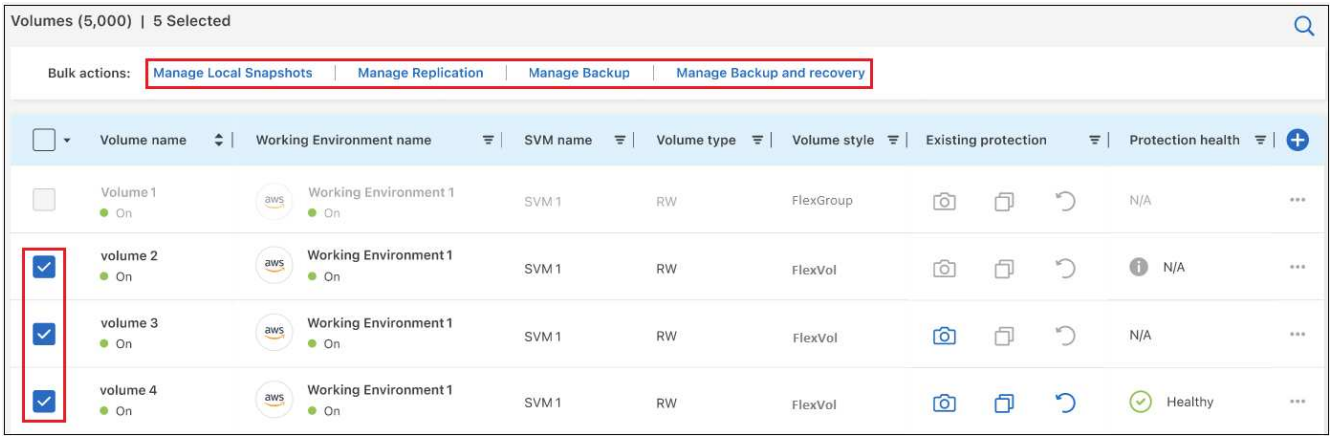
Bei der Arbeit mit mehreren Volumes müssen alle Volumes die folgenden gemeinsamen Merkmale aufweisen:

- Gleiche Arbeitsumgebung
- Gleicher Stil (FlexVol oder FlexGroup Volume)
- Gleicher Typ (Lese-/Schreibzugriff oder Data Protection Volume)

Wenn mehr als fünf Volumes für Backups aktiviert sind, werden mit BlueXP Backup und Recovery nur fünf Volumes gleichzeitig initialisiert. Wenn diese abgeschlossen sind, erstellt es den nächsten Stapel von fünf untergeordneten Jobs, um den nächsten Satz zu starten, und wird fortgesetzt, bis alle Volumes initialisiert werden.

Schritte

1. Filtern Sie auf der Registerkarte **Volumes** nach der Arbeitsumgebung, in der sich die Volumes befinden.
2. Wählen Sie alle Volumes aus, auf denen Sie die Backup-Einstellungen verwalten möchten.
3. Je nach Art der zu konfigurierenden Sicherungsaktion klicken Sie im Menü Massenaktionen auf die Schaltfläche:



Sicherungsaktion…	Klicken Sie auf diese Schaltfläche…
Verwalten der Snapshot Backup-Einstellungen	**Lokale Snapshots Verwalten**
Managen der Replikationsbackup-Einstellungen	**Replikation Verwalten**
Managen der Backup-Einstellungen in der Cloud	**Sicherung Verwalten**
Verwalten Sie mehrere Arten von Backup-Einstellungen. Mit dieser Option können Sie auch die Backup-Architektur ändern.	**Backup und Recovery verwalten**

4. Nehmen Sie auf der daraufhin angezeigten Backup-Seite Änderungen an den bestehenden Backup-Richtlinien für lokale Snapshot-Kopien, replizierte Volumes oder Sicherungsdateien vor, und klicken Sie auf **Speichern**.

   Wenn Sie bei der Aktivierung von BlueXP Backup und Recovery für diesen Cluster in der anfänglichen Backup-Richtlinie *DataLock und Ransomware-Schutz* für Cloud-Backups aktiviert haben, werden nur weitere Richtlinien angezeigt, die mit DataLock konfiguriert wurden. Und wenn Sie bei der Aktivierung von BlueXP Backup und Recovery *DataLock und Ransomware-Schutz* nicht aktiviert haben, werden Sie nur andere Cloud-Backup-Richtlinien sehen, für die DataLock nicht konfiguriert ist.

Erstellen Sie jederzeit eine manuelle Volume-Sicherung

Sie können jederzeit ein On-Demand-Backup erstellen, um den aktuellen Status des Volumes zu erfassen. Dies ist nützlich, wenn sehr wichtige Änderungen an einem Volume vorgenommen wurden und Sie nicht auf das nächste geplante Backup warten möchten, um diese Daten zu sichern. Sie können diese Funktion auch verwenden, um ein Backup für ein Volume zu erstellen, das derzeit nicht gesichert wird und den aktuellen Status erfassen soll.

Sie können eine Ad-hoc Snapshot Kopie oder ein Backup im Objekt eines Volume erstellen. Sie können kein ad-hoc repliziertes Volume erstellen.

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

Wenn Sie bei der Aktivierung von BlueXP Backup und Recovery für diesen Cluster *DataLock und Ransomware-Schutz* aktiviert haben, 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 **Backup** > **Ad-hoc-Backup erstellen**.

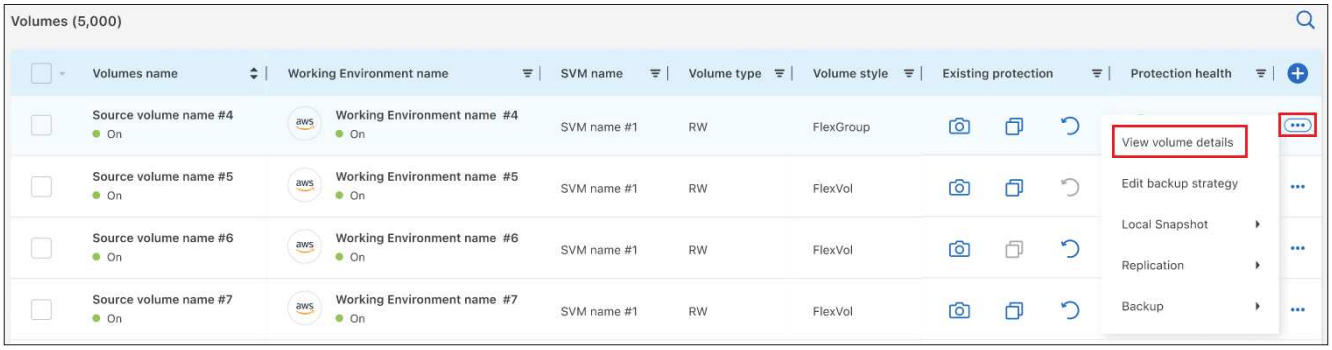
In der Spalte Backup Status für dieses Volume wird „in progress“ angezeigt, bis das Backup erstellt wird.

Sehen Sie sich die Liste der Backups für jedes Volume an

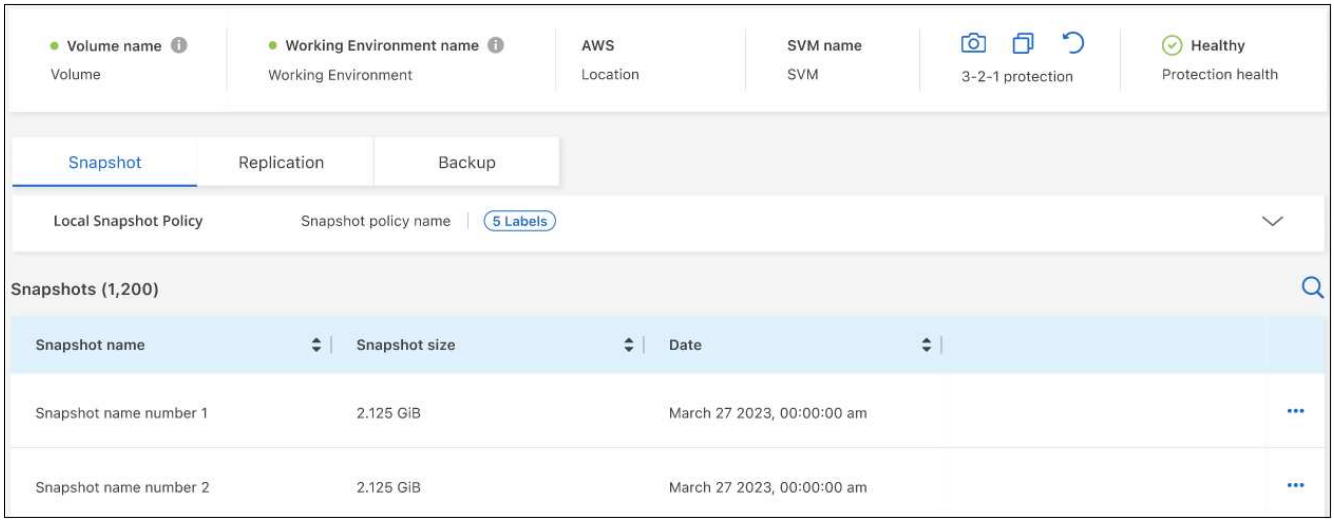
Sie können eine Liste aller Backup-Dateien anzeigen, die für jedes Volume vorhanden sind. Auf dieser Seite werden Details zum Quell-Volume, zum Zielort und zu Backup-Details wie zum Beispiel zum letzten Backup, zur aktuellen Backup-Richtlinie, zur Größe der Sicherungsdatei und mehr angezeigt.

Schritte

1. Klicken Sie auf der Registerkarte **Volumes** auf ••• Wählen Sie für das Quellvolume **View Volume Details**.



Die Details für das Volume und die Liste der Snapshot Kopien werden standardmäßig angezeigt.



2. Wählen Sie **Snapshot**, **Replication** oder **Backup**, um die Liste aller Sicherungsdateien für jeden Sicherungstyp anzuzeigen.

Führen Sie einen Ransomware-Scan bei einem Volume-Backup im Objekt-Storage durch

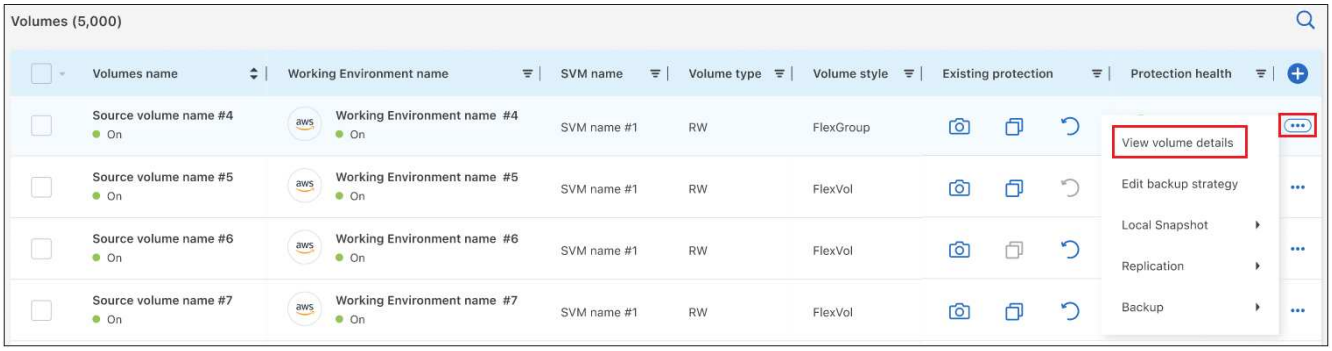
Die NetApp Software zum Schutz vor Ransomware überprüft Ihre Backup-Dateien, um nach Anzeichen eines Ransomware-Angriffs zu suchen, wenn eine Backup-to-Object-Datei erstellt wird und Daten aus einer Backup-Datei wiederhergestellt werden. Darüber hinaus können Sie jederzeit einen On-Demand-Scan zum Schutz vor Ransomware durchführen, um die Benutzerfreundlichkeit einer bestimmten Backup-Datei im Objekt-Storage zu 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 auf einem System mit ONTAP 9.11.1 oder höher erstellt wurde, und wenn Sie *DataLock und Ransomware-Schutz* in der Backup-to-Object-Richtlinie aktiviert

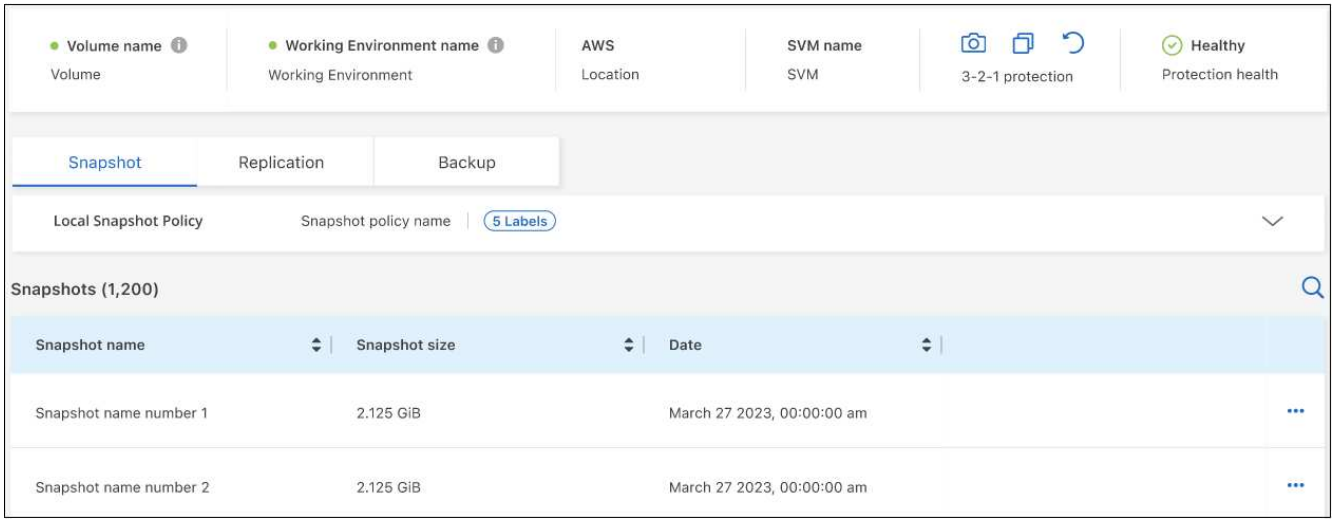
haben.

Schritte

1. Klicken Sie auf der Registerkarte **Volumes** auf ••• Wählen Sie für das Quellvolume **View Volume Details**.

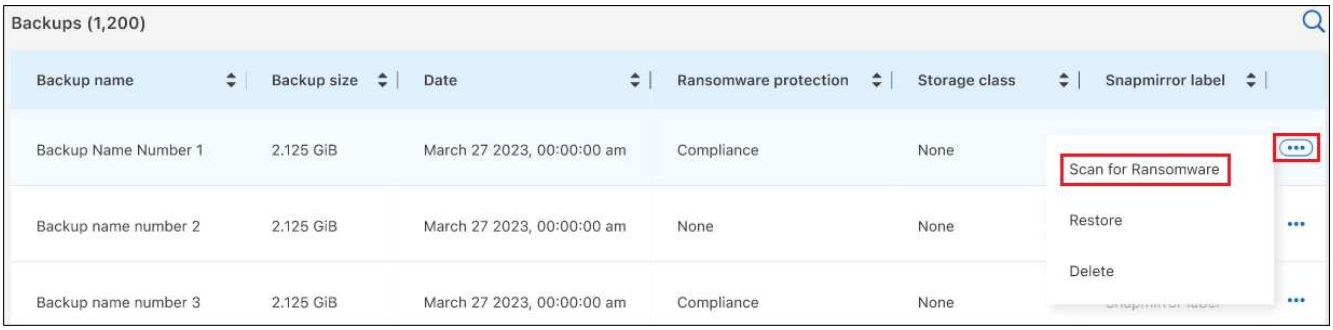


Die Details für das Volume werden angezeigt.



2. Wählen Sie **Backup**, um die Liste der Sicherungsdateien im Objektspeicher anzuzeigen.

3. Klicken Sie Auf ••• Für das Volumen Backup-Datei, die Sie für Ransomware scannen möchten und klicken Sie auf **Scan for Ransomware**.



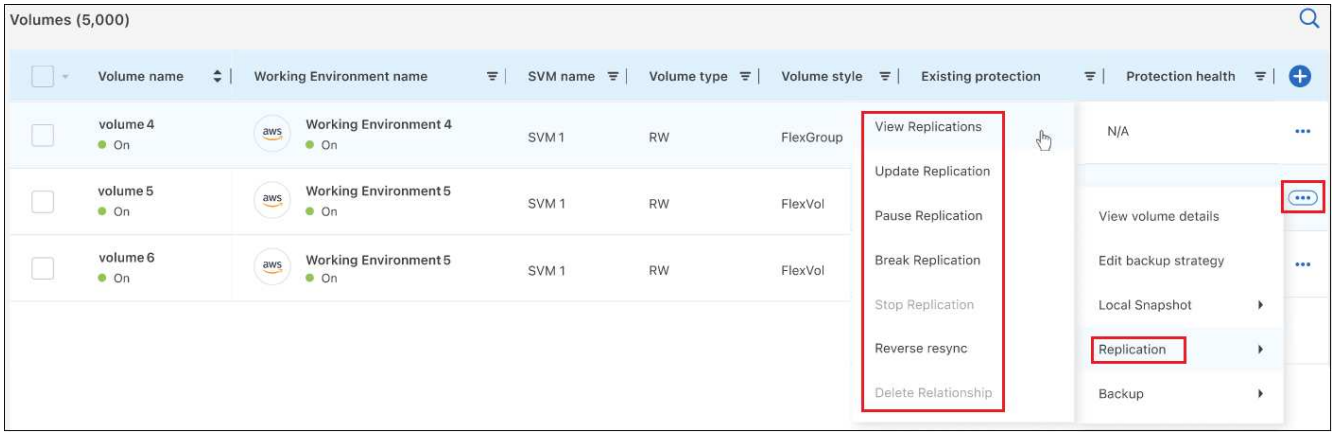
In der Spalte Ransomware Protection wird angezeigt, dass der Scan ausgeführt wird.

Verwalten der Replikationsbeziehung mit dem Quell-Volume

Nachdem Sie die Datenreplizierung zwischen zwei Systemen eingerichtet haben, können Sie die Datenreplikationsbeziehung verwalten.

Schritte

1. Klicken Sie auf der Registerkarte **Volumes** auf ••• Wählen Sie für das Quell-Volume die Option **Replikation**. Sie können alle verfügbaren Optionen sehen.
2. Wählen Sie die Replikationsaktion aus, die Sie durchführen möchten.



Die folgende Tabelle beschreibt die verfügbaren Aktionen:

Aktion	Beschreibung
Replikation Anzeigen	Zeigt Details zur Volume-Beziehung an: Übertragungsinformationen, Informationen zur letzten Übertragung, Details zum Volume und Informationen zur Schutzrichtlinie, die der Beziehung zugeordnet sind.
Replikation Aktualisieren	Startet eine inkrementelle Übertragung, um das Ziel-Volume zu aktualisieren, das mit dem Quell-Volume synchronisiert werden soll.
Replikation Anhalten	Unterbrechen Sie die inkrementelle Übertragung von Snapshot Kopien, um das Ziel-Volume zu aktualisieren. Wenn Sie die inkrementellen Aktualisierungen neu starten möchten, können Sie die Aktualisierung zu einem späteren Zeitpunkt fortsetzen.

Aktion	Beschreibung
Replikation Unterbrechen	Bricht die Beziehung zwischen den Quell- und Ziel-Volumes und aktiviert das Ziel-Volume für den Datenzugriff - macht es Lese-und Schreibzugriff. Diese Option wird in der Regel verwendet, wenn das Quell-Volume aufgrund von Ereignissen wie Datenbeschädigung, versehentlichem Löschen oder einem Offline-Status keine Daten bereitstellen kann. "Erfahren Sie, wie Sie ein Ziel-Volume für Datenzugriff konfigurieren und ein Quell-Volume in der ONTAP Dokumentation neu aktivieren"
Replikation Abbrechen	Deaktiviert die Backups dieses Volumes auf dem Zielsystem und deaktiviert auch die Möglichkeit zur Wiederherstellung eines Volumes. Vorhandene Backups werden nicht gelöscht. Dadurch wird die Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes nicht gelöscht.
Reverse Resync	Kehrt die Rollen der Quell- und Ziel-Volumes um. Der Inhalt des ursprünglichen Quell-Volumes wird durch den Inhalt des Ziel-Volumes überschrieben. Dies ist hilfreich, wenn Sie ein Quell-Volume, das offline gegangen ist, reaktivieren möchten. Alle Daten, die zwischen der letzten Datenreplizierung und dem Zeitpunkt, zu dem das Quell-Volume deaktiviert wurde, auf das ursprüngliche Quell-Volume geschrieben wurden, bleiben nicht erhalten.
Beziehung Löschen	Löscht die Data-Protection-Beziehung zwischen Quell- und Ziel-Volumes, d. H., die Datenreplizierung findet nicht mehr zwischen den Volumes statt. Diese Aktion aktiviert nicht das Zielvolume für den Datenzugriff - das bedeutet, dass es nicht Lese- und Schreibvorgänge macht. Durch diese Aktion werden auch die Cluster-Peer-Beziehung und die SVM-Peer-Beziehung (Storage VM) gelöscht, falls keine anderen Datensicherungsbeziehungen zwischen den Systemen bestehen.

Ergebnis

Nachdem Sie eine Aktion ausgewählt haben, aktualisiert BlueXP die Beziehung.

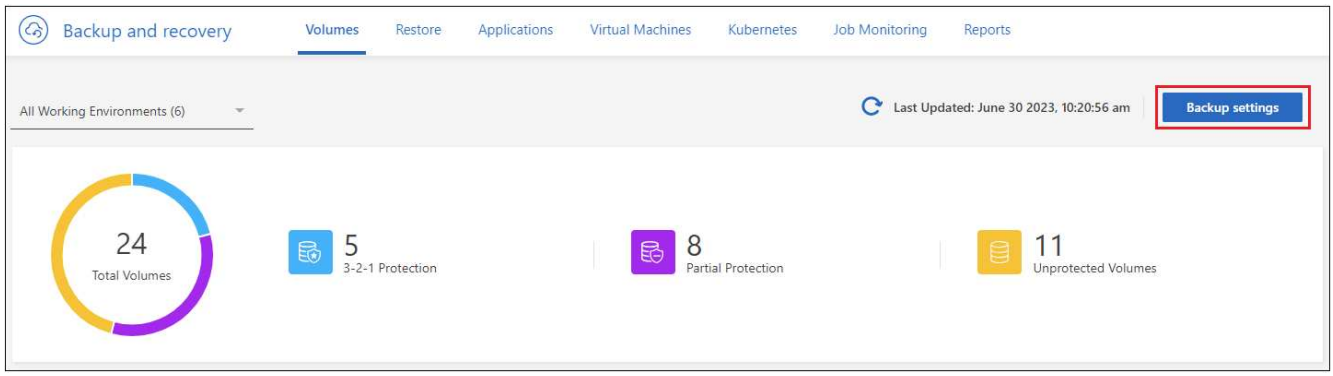
Bearbeiten Sie eine vorhandene Richtlinie für Backups in der Cloud

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.

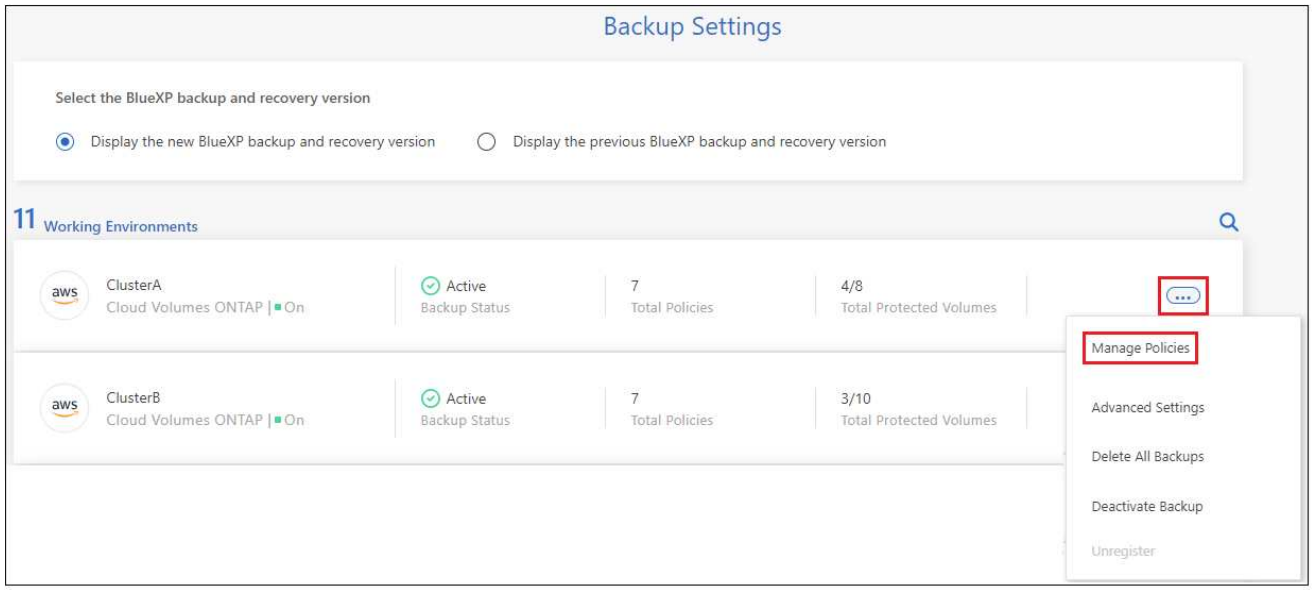
- Wenn Sie *DataLock und Ransomware-Schutz* in der ursprünglichen Richtlinie aktiviert haben, wenn BlueXP Backup und Recovery für diesen Cluster aktiviert wurde, müssen alle von Ihnen bearbeitenden Richtlinien mit derselben DataLock-Einstellung (Governance oder Compliance) konfiguriert werden. Und wenn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

Schritte

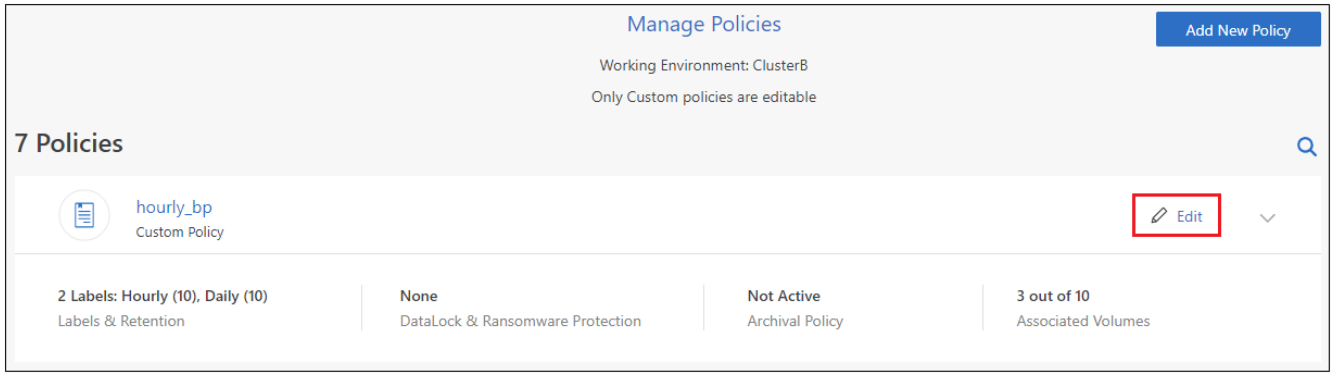
1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.



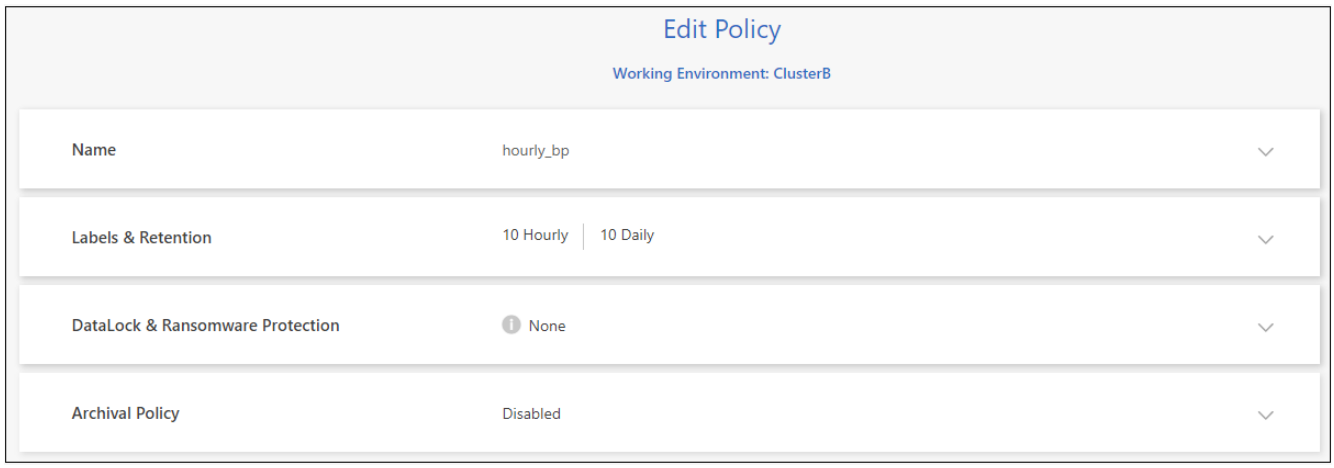
2. Klicken Sie auf der Seite „ Backup Settings_“ auf ••• Wählen Sie für die Arbeitsumgebung, in der Sie die Richtlinieneinstellungen ändern möchten, und wählen Sie **Richtlinien verwalten**.



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



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**.

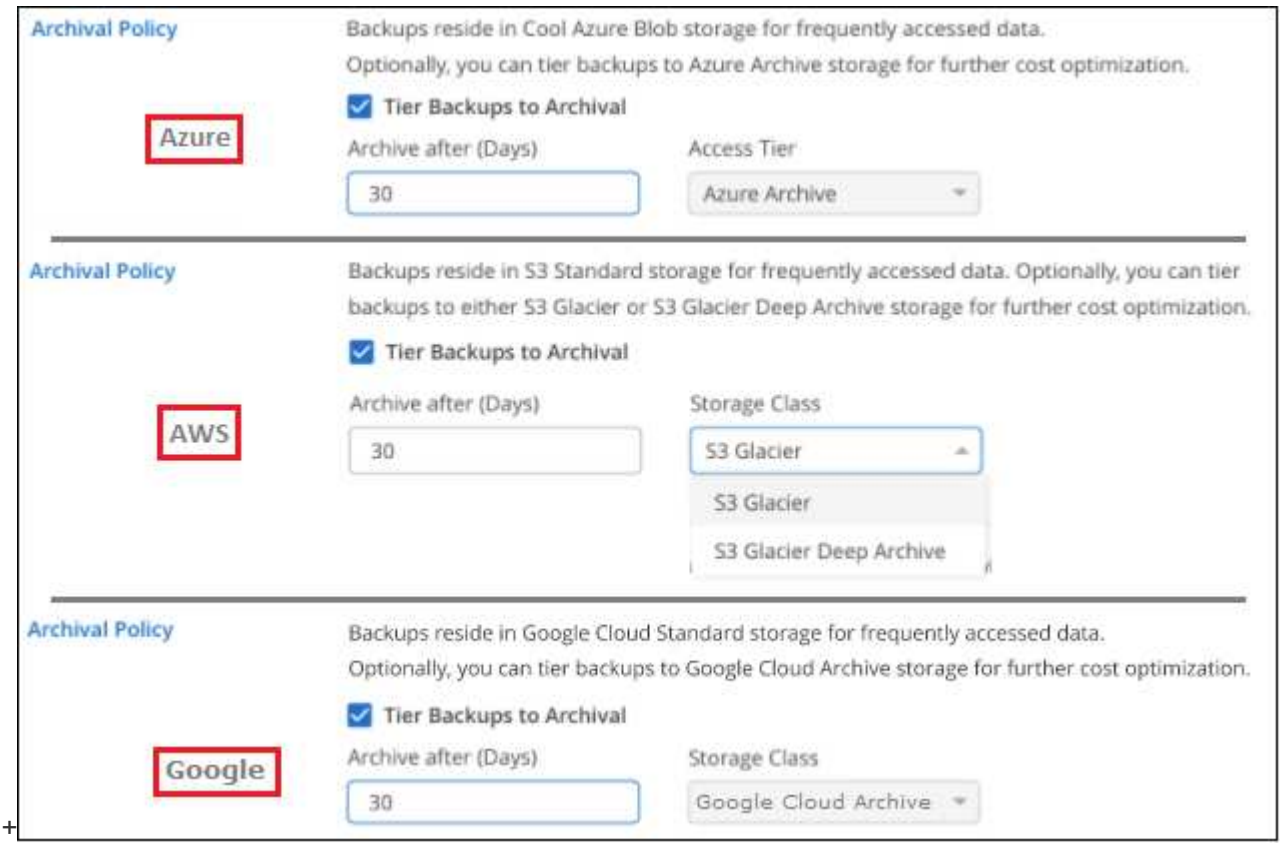


Wenn in Ihrem Cluster ONTAP 9.10.1 oder höher ausgeführt wird, haben Sie außerdem die Möglichkeit, das Tiering von Backups in Archiv-Storage nach einer bestimmten Anzahl von Tagen zu aktivieren oder zu deaktivieren.

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

"Erfahren Sie mehr über den Azure Archiv-Storage".

"Erfahren Sie mehr über die Verwendung von Google Archivspeicher". (ONTAP 9.12.1 erforderlich.)



+

+ 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.

Neue Richtlinie für das Backup in die Cloud hinzufügen

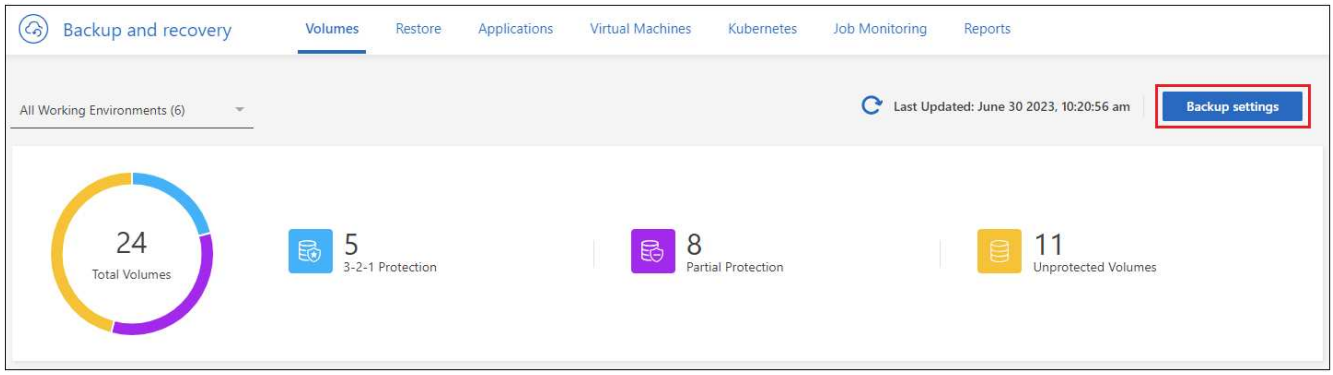
Wenn Sie BlueXP Backup und Recovery für eine funktionierende Umgebung aktivieren, werden alle Volumes, die Sie ursprünglich ausgewählt haben, mithilfe der von Ihnen definierten Standard-Backup-Richtlinie gesichert. Um bestimmten Volumes mit verschiedenen Recovery Point Objectives (RPOs) unterschiedliche 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 sind,Wenden Sie die Richtlinie auf Volumes in dieser Arbeitsumgebung an.

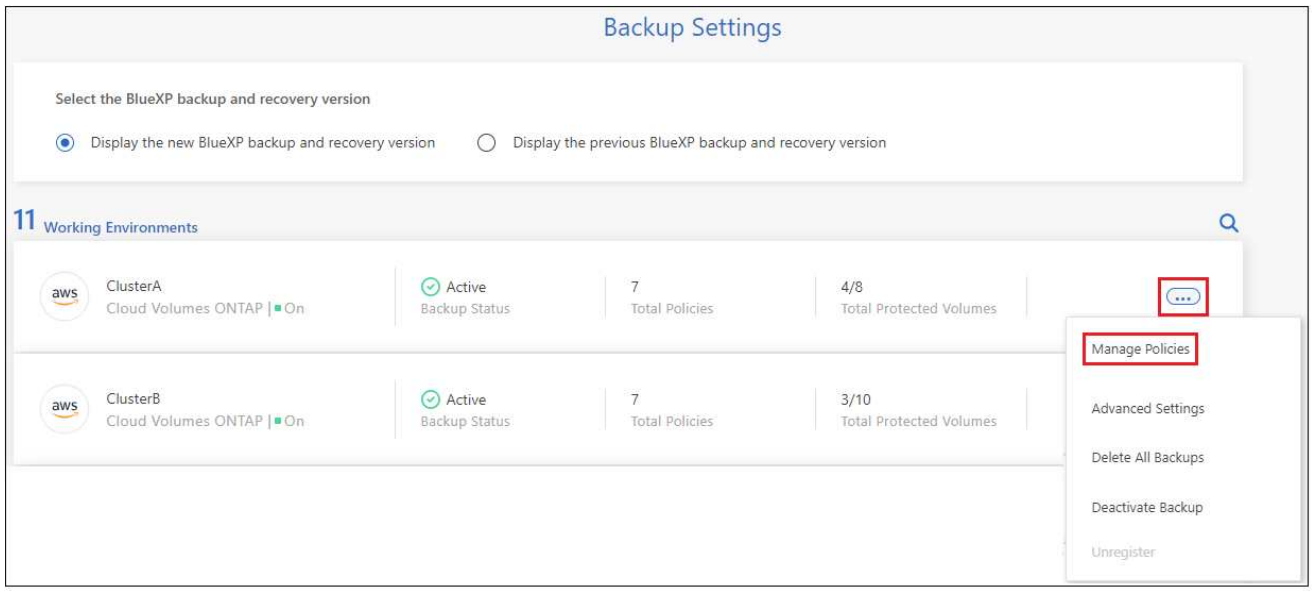
- Wenn Sie *DataLock und Ransomware Protection* in der ursprünglichen Richtlinie aktiviert haben, wenn BlueXP Backup und Recovery für diesen Cluster aktiviert wurde, müssen alle zusätzlich erstellten Richtlinien mit derselben DataLock-Einstellung (Governance oder Compliance) konfiguriert werden. Und wenn Sie bei der Aktivierung von BlueXP Backup und Recovery *DataLock und Ransomware-Schutz* nicht aktiviert haben, können Sie keine neuen Richtlinien erstellen, die DataLock verwenden.
- Wenn Sie bei der Erstellung von Backups auf AWS bei der ersten Backup-Richtlinie bei der Aktivierung von BlueXP Backup und Recovery *S3 Glacier* oder *S3 Glacier Deep Archive* ausgewählt haben, ist diese Tier die einzige Archiv-Tier, 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

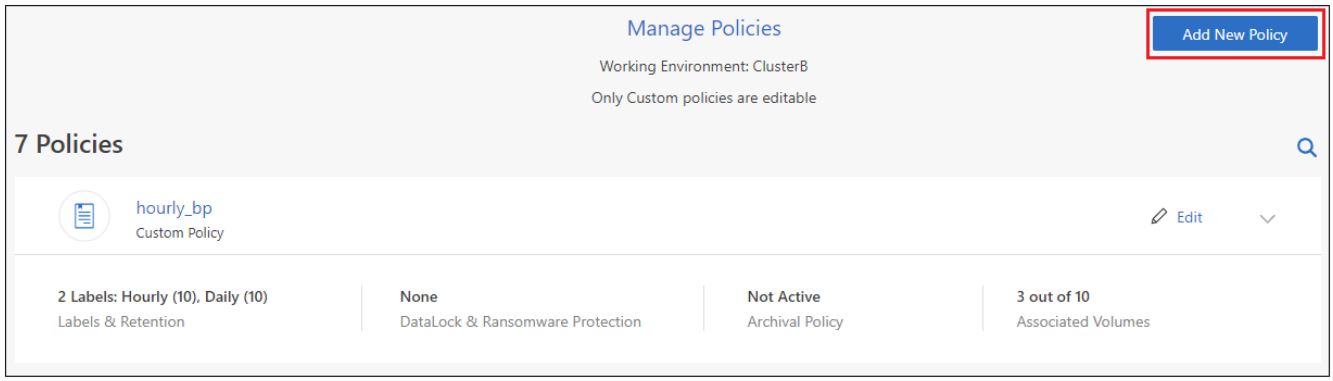
1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.



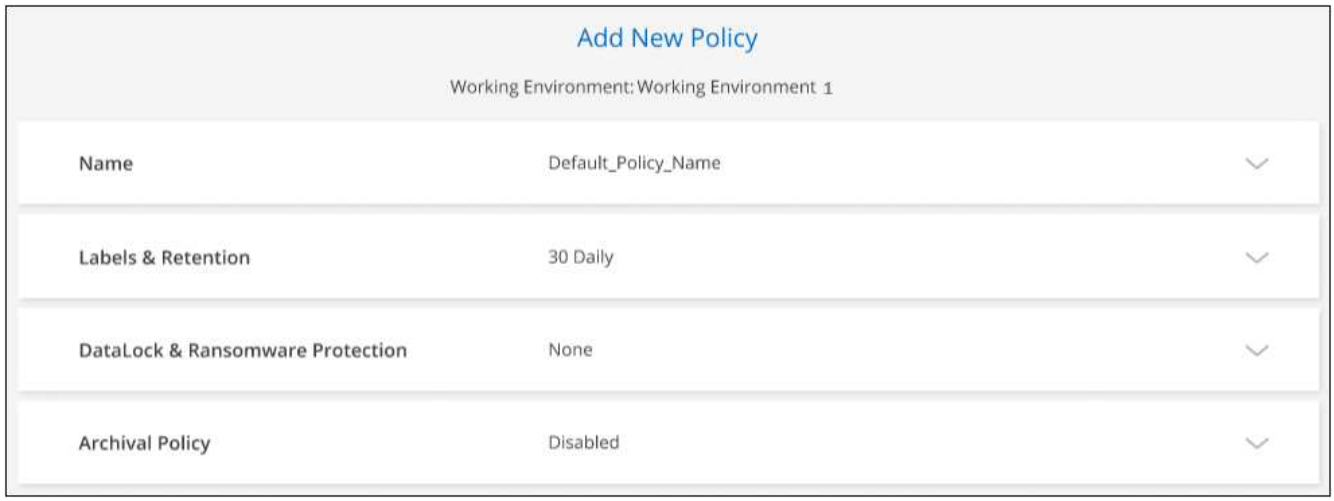
2. Klicken Sie auf der Seite „ Backup Settings_“ auf ••• Wählen Sie für die Arbeitsumgebung, in der Sie die neue Richtlinie hinzufügen möchten, und wählen Sie **Richtlinien verwalten**.



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**.

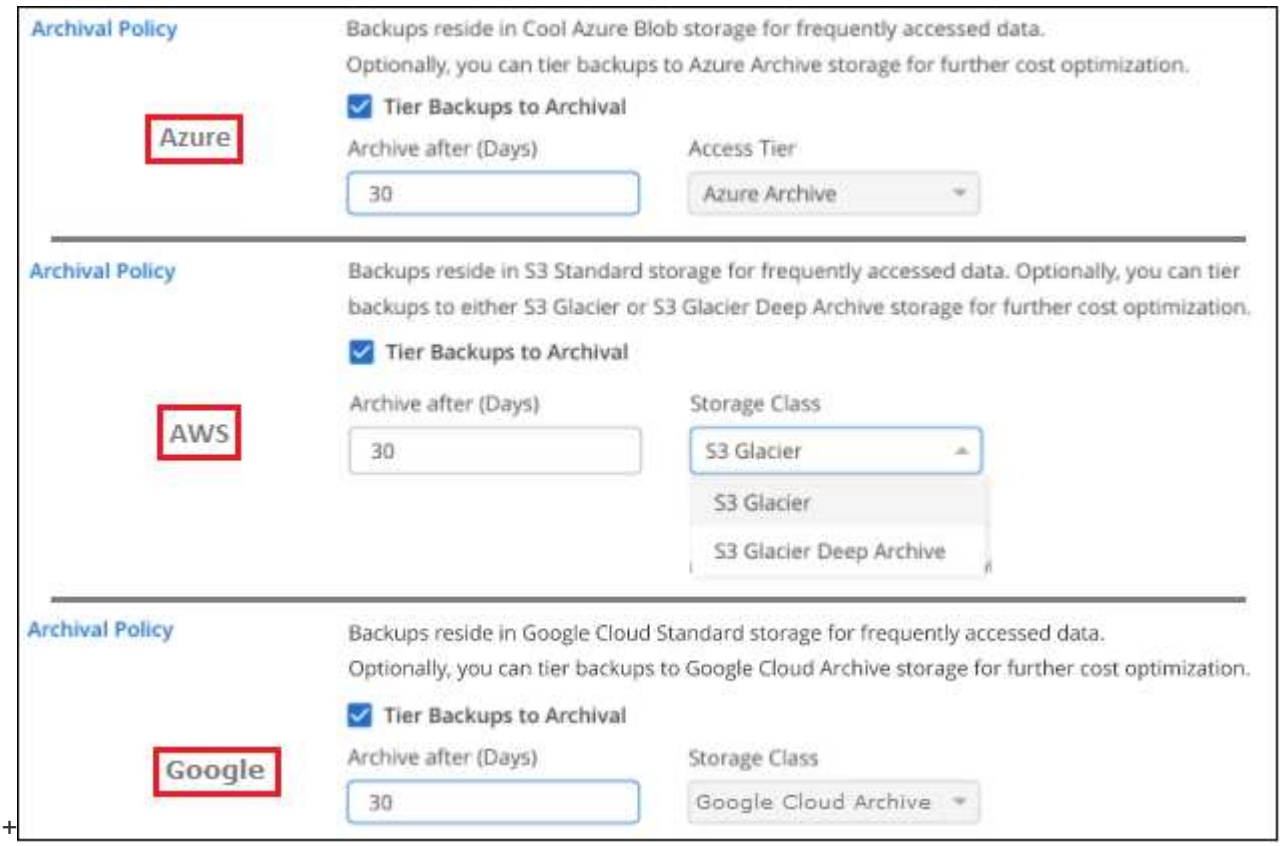


Wenn in Ihrem Cluster ONTAP 9.10.1 oder höher ausgeführt wird, haben Sie außerdem die Möglichkeit, das Tiering von Backups in Archiv-Storage nach einer bestimmten Anzahl von Tagen zu aktivieren oder zu deaktivieren.

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

"Erfahren Sie mehr über den Azure Archiv-Storage".

"Erfahren Sie mehr über die Verwendung von Google Archivspeicher". (ONTAP 9.12.1 erforderlich.)



Backups löschen

Mit BlueXP Backup und Recovery können Sie eine einzelne Backup-Datei löschen, alle Backups eines Volumes löschen oder alle Backups aller Volumes in einer funktionierenden Umgebung 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. BlueXP Backup und Recovery löscht Backups nicht automatisch, wenn Sie ein System löschen. Die Benutzeroberfläche bietet derzeit keine Unterstützung zum Löschen der Backups nach dem Löschen des Systems. Für alle verbleibenden Backups werden weiterhin die Kosten für Objekt-Storage in Rechnung gestellt.

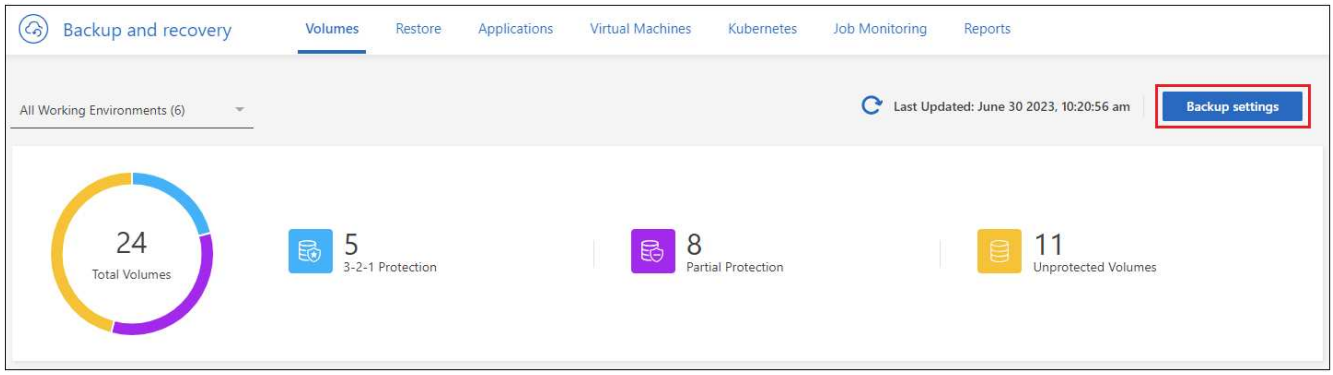
Löschen Sie alle Sicherungsdateien für eine funktionierende Umgebung

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

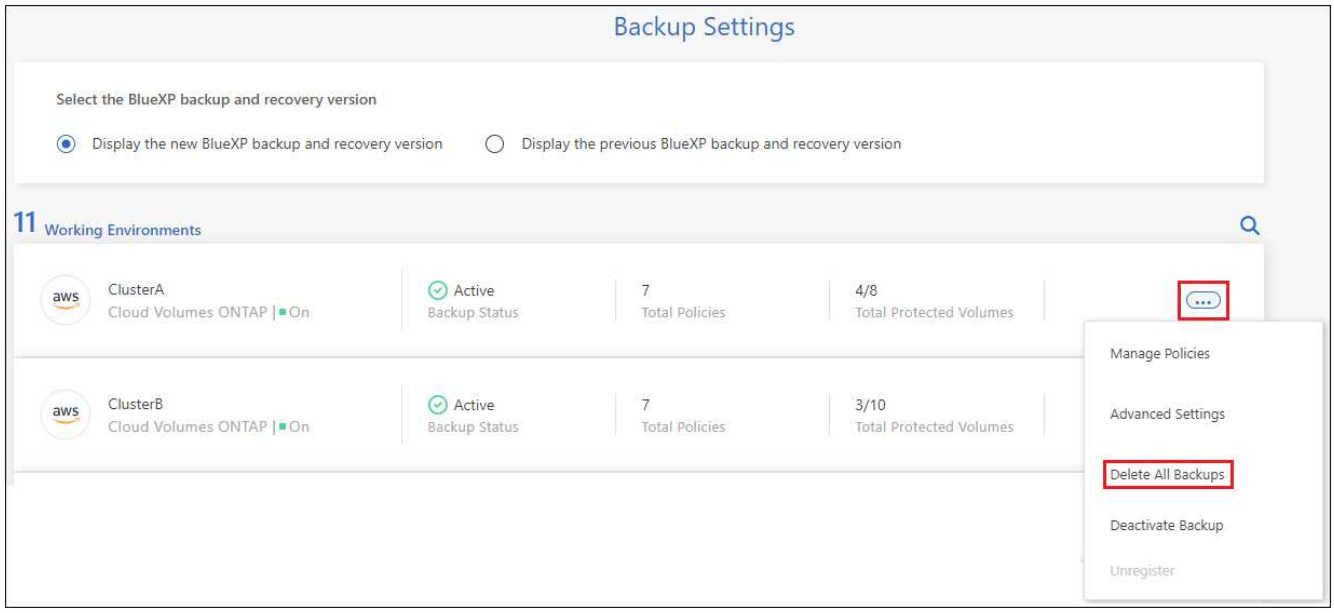
Beachten Sie, dass diese Aktion keine Auswirkungen auf Snapshot-Kopien oder replizierte Volumes hat. Diese Arten von Backup-Dateien werden nicht gelöscht.

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**.

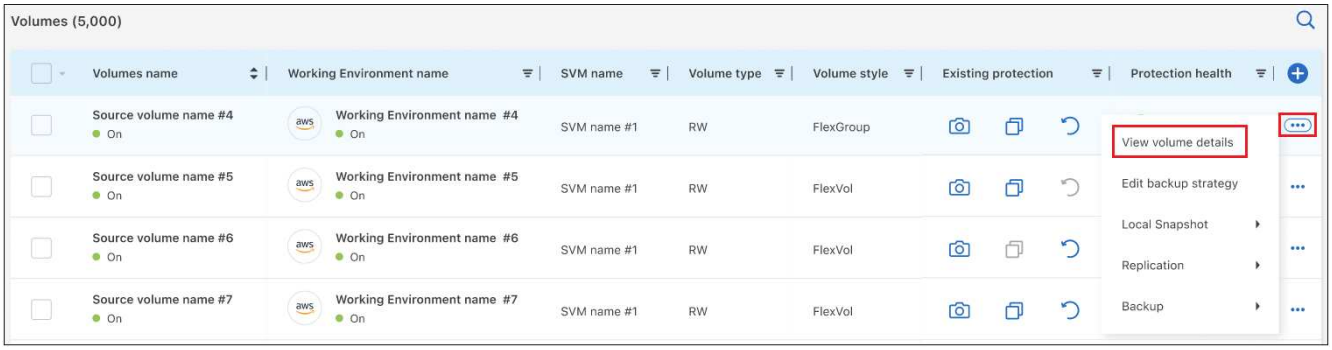
Eine einzelne Sicherungsdatei für ein Volume löschen

Sie können eine einzelne Sicherungsdatei löschen, wenn Sie sie nicht mehr benötigen. Dazu gehört auch das Löschen eines einzelnen Backups einer Volume-Snapshot-Kopie oder eines Backups im Objektspeicher.

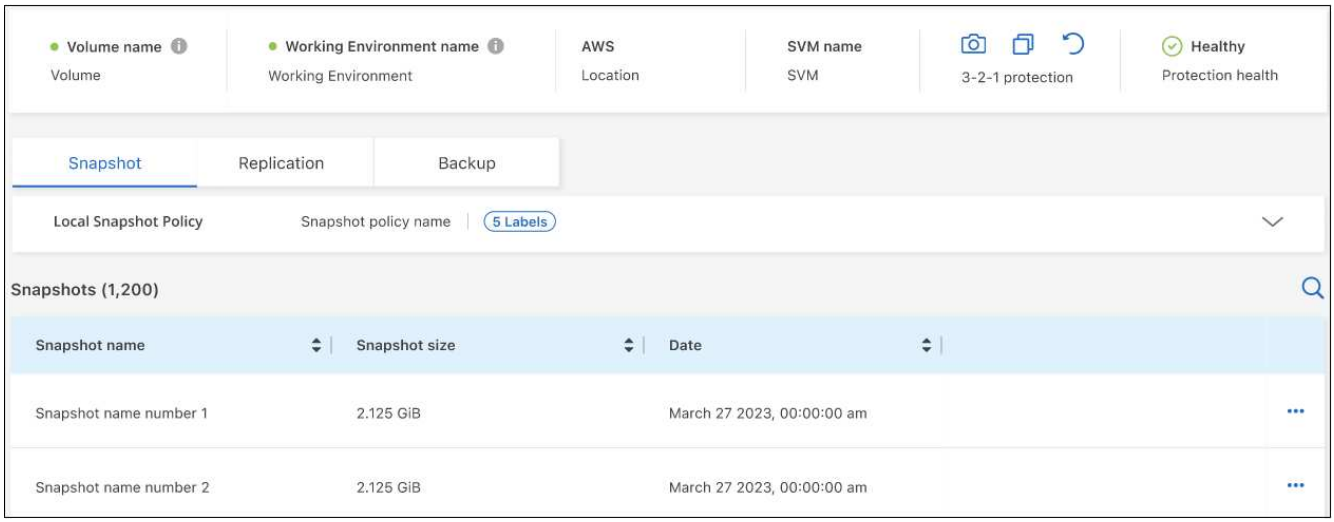
Replizierte Volumes (Data Protection Volumes) können nicht gelöscht werden.

Schritte

1. Klicken Sie auf der Registerkarte **Volumes** auf ••• Wählen Sie für das Quellvolume **View Volume Details**.

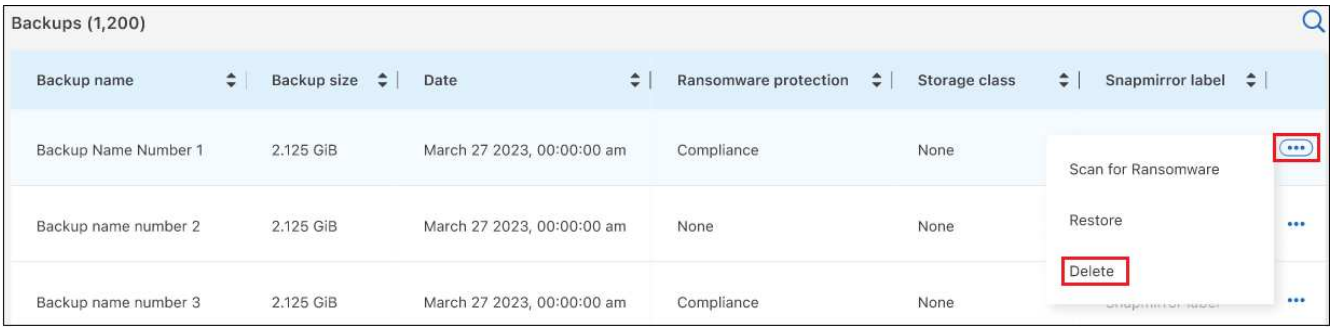


Die Details für das Volume werden angezeigt, und Sie können **Snapshot**, **Replication** oder **Backup** auswählen, um die Liste aller Sicherungsdateien für das Volume anzuzeigen. Standardmäßig werden die verfügbaren Snapshot Kopien angezeigt.



2. Wählen Sie **Snapshot** oder **Backup**, um den Typ der zu löschenden Sicherungsdateien anzuzeigen.

3. Klicken Sie Auf ••• Für die Sicherungsdatei des Datenträgers, die Sie löschen möchten, klicken Sie auf **Löschen**. Der Screenshot unten stammt von einer Backup-Datei im Objektspeicher.



4. 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.

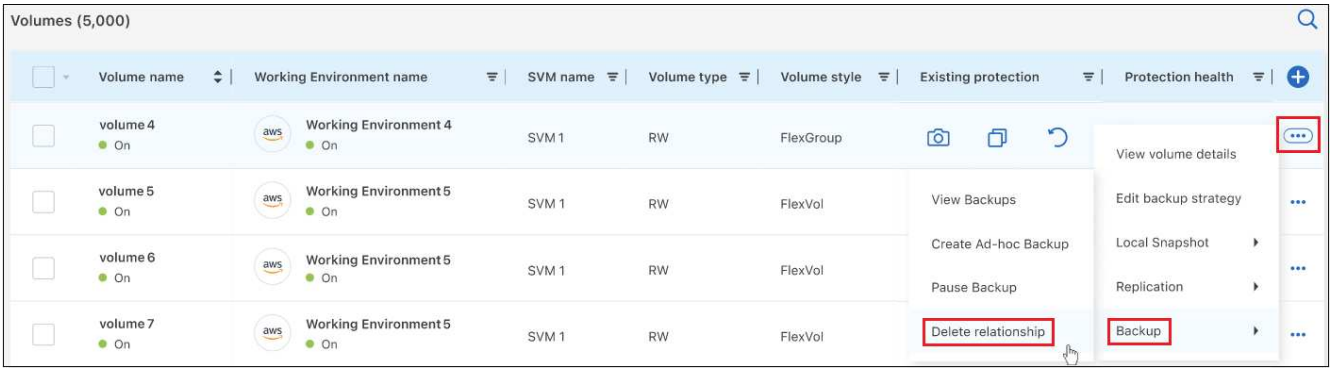
Diese Funktion ist nur verfügbar, wenn Ihr System ONTAP 9.12.1 oder höher ausführt.

Das Quell-Volume kann nicht von der BlueXP Backup- und Recovery-Benutzeroberfläche gelöscht werden. 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 jedoch alle Backups für das Volume löschen.

Schritte

1. Klicken Sie auf der Registerkarte **Volumes** auf ••• Wählen Sie für das Quellvolume **Backup** > **Beziehung löschen**.



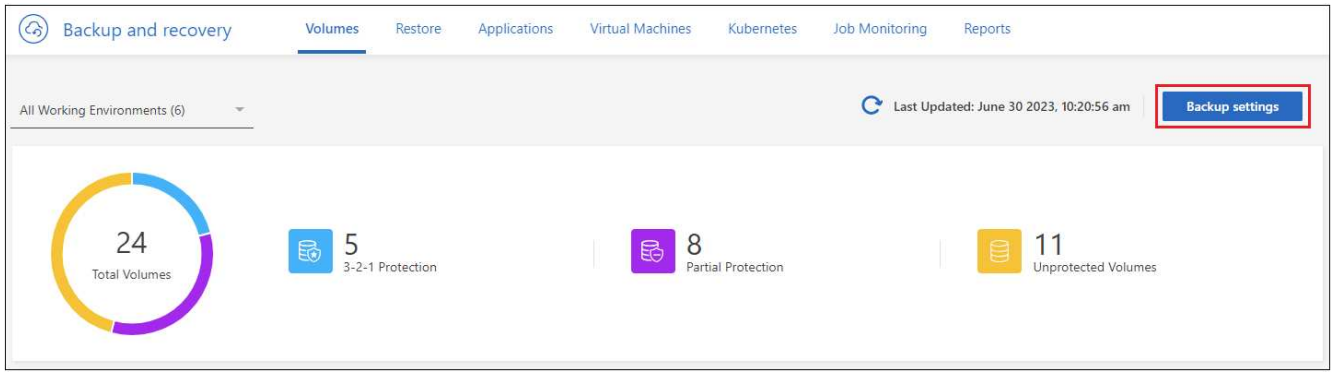
BlueXP Backup und Recovery für eine funktionierende Umgebung deaktivieren

Durch die Deaktivierung von BlueXP Backup- und Recovery-Funktionen für eine funktionierende Umgebung werden die Backups jedes Volumes auf dem System deaktiviert. Zudem wird 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.

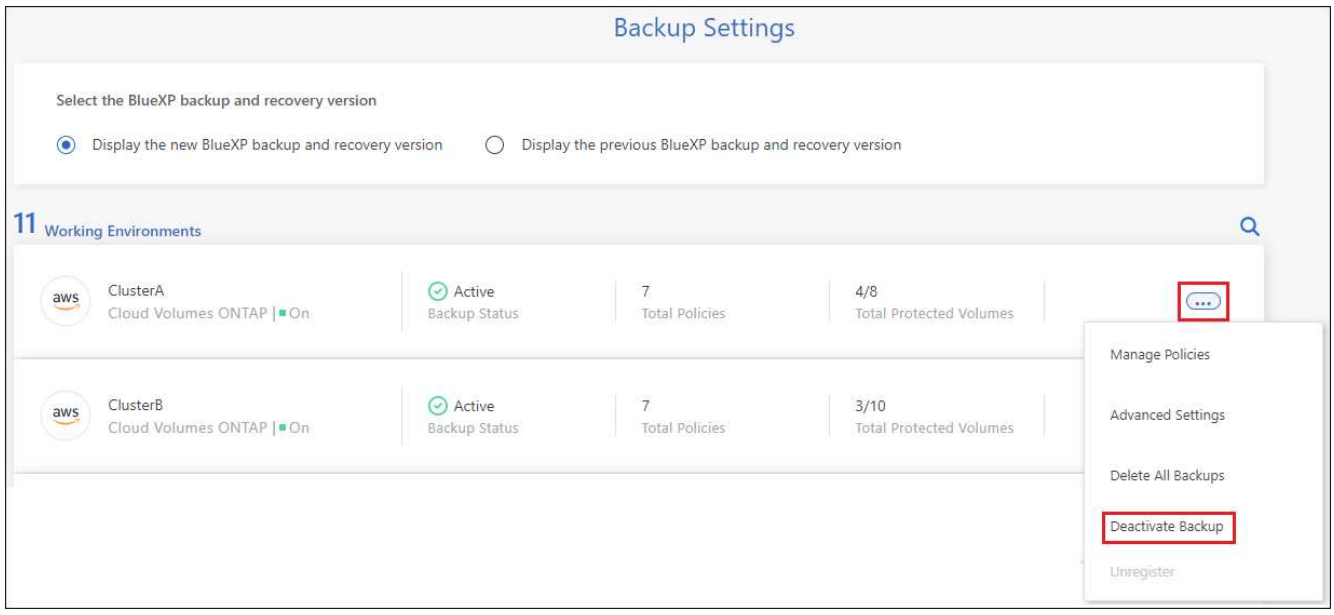
Beachten Sie, dass Cloud-Provider Ihnen weiterhin die Kosten für Objekt-Storage für die Kapazität in Ihrem Backup in Rechnung stellen, es sei denn, Sie sind erforderlich Löschen Sie die Backups.

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.

Heben Sie die Registrierung von BlueXP Backup und Recovery für eine funktionierende Umgebung auf

Wenn Sie die Backup-Funktionen nicht mehr nutzen möchten und Sie die Kosten für Backups in dieser Arbeitsumgebung abschaffen möchten, können Sie die Registrierung für das BlueXP Backup und Recovery für eine Arbeitsumgebung aufheben. 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 BlueXP Backup und Recovery für die Arbeitsumgebung entfernt haben, können Sie BlueXP Backup und Recovery für dieses Cluster mithilfe der Informationen des neuen Cloud-Providers aktivieren.

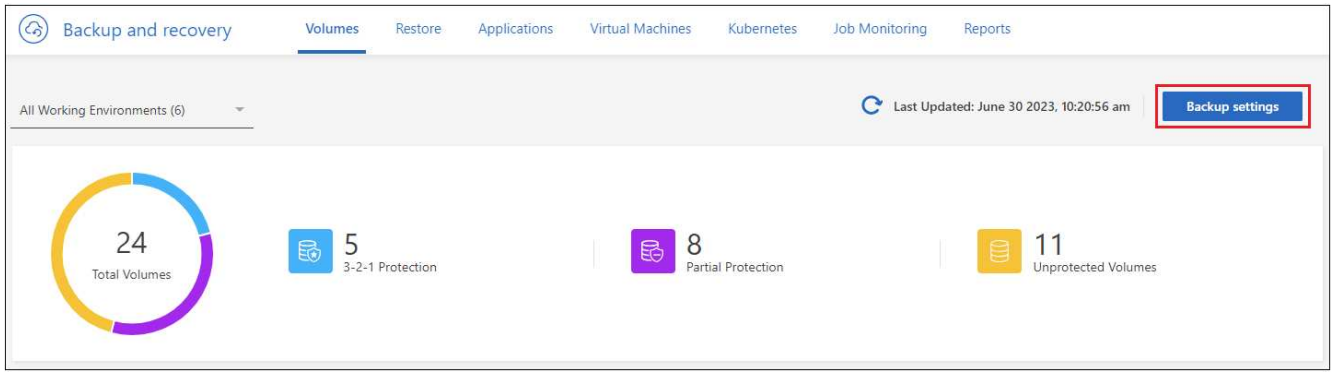
Bevor Sie das Backup- und Recovery-System von BlueXP aufheben können, müssen Sie in der folgenden Reihenfolge vorgehen:

- BlueXP Backup und Recovery für die Arbeitsumgebung deaktivieren
- Löschen Sie alle Backups für die Arbeitsumgebung

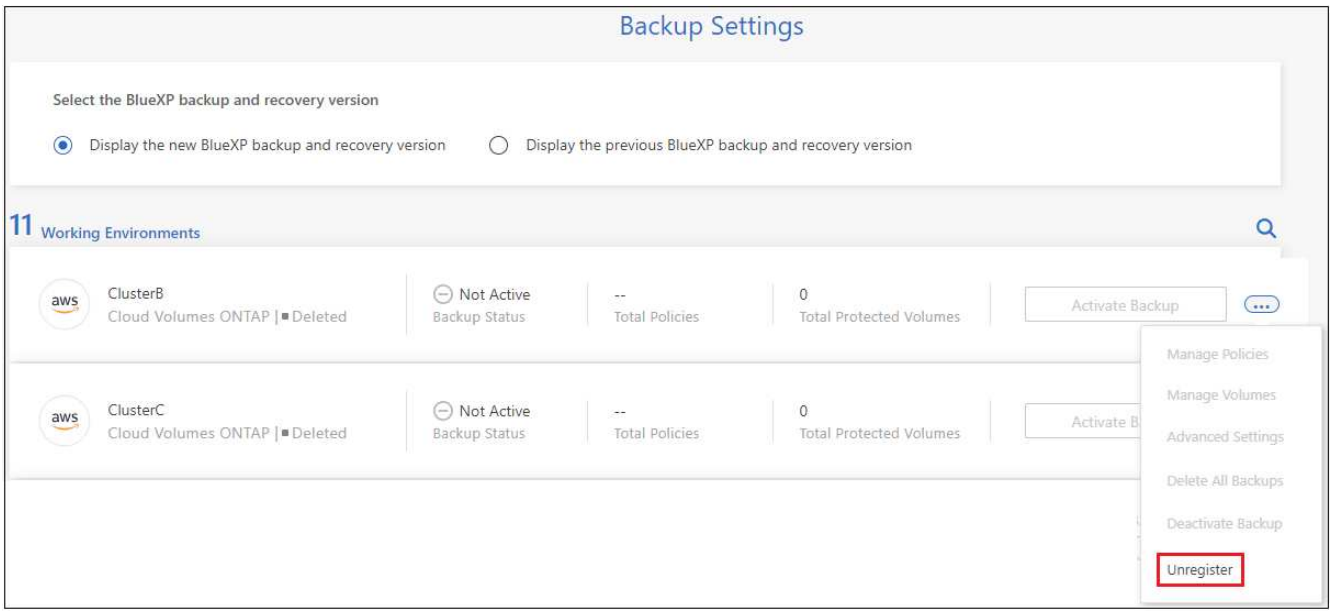
Die Option zum Aufheben der Registrierung ist erst verfügbar, wenn diese beiden Aktionen abgeschlossen sind.

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**.

Stellen Sie ONTAP-Daten aus Sicherungsdateien mit BlueXP Backup und Recovery wieder her

Backups Ihrer ONTAP Volume-Daten sind über die Standorte Ihrer Backups verfügbar: Snapshot Kopien, replizierte Volumes und im Objekt-Storage gespeicherte Backups. Sie können von jedem dieser Backup-Standorte aus Daten zu einem bestimmten Zeitpunkt wiederherstellen. Mit BlueXP Backup und Recovery können Sie ein komplettes ONTAP-Volume aus einer Sicherungsdatei wiederherstellen. Wenn Sie nur ein paar Dateien wiederherstellen müssen, können Sie einen Ordner oder einzelne Dateien 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 von Backup-Dateien auf ein Produktionssystem ist eine gültige BlueXP Backup- und Recovery-Lizenz erforderlich.

Zusammenfassend sind dies die gültigen Datenflüsse, die Sie verwenden können, um Volume-Daten in einer ONTAP Arbeitsumgebung wiederherzustellen:

- Sicherungsdatei → wiederhergestelltes Volume
- Repliziertes Volume → wiederhergestelltes Volume

- Snapshot Kopie → wiederhergestelltes Volume

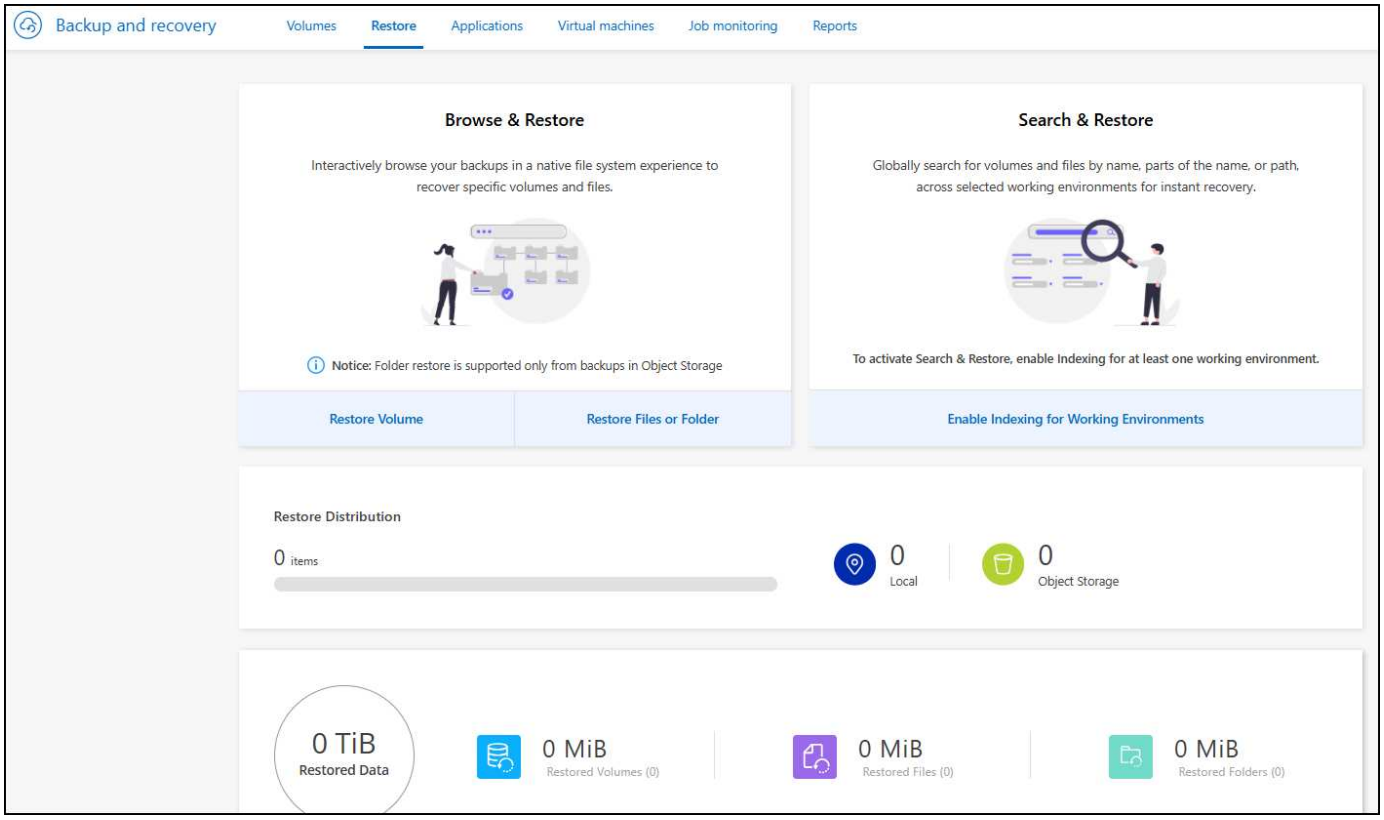
> Wenn der Wiederherstellungsvorgang nicht abgeschlossen ist, versuchen Sie den Wiederherstellungsvorgang erst dann erneut, wenn die Jobüberwachung anzeigt, dass der Wiederherstellungsvorgang fehlgeschlagen ist. Wenn Sie den Wiederherstellungsvorgang erneut versuchen, bevor der Job Monitor zeigt, dass der Wiederherstellungsvorgang fehlgeschlagen ist, schlägt der Wiederherstellungsvorgang erneut fehl. Wenn der Job-Monitor als „Fehlgeschlagen“ angezeigt wird, können Sie den Wiederherstellungsvorgang erneut versuchen.

> Einschränkungen im Zusammenhang mit der Wiederherstellung von ONTAP-Daten finden Sie unter "Einschränkungen bei Backup und Restore für ONTAP Volumes".

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.

> BlueXP Backup und Recovery müssen bereits für mindestens eine Arbeitsumgebung aktiviert sein und erste Backup-Dateien müssen vorhanden sein.



Wie Sie sehen, bietet das Wiederherstellungs-Dashboard zwei verschiedene Möglichkeiten zum Wiederherstellen von Daten aus Sicherungsdateien: **Durchsuchen und Wiederherstellen** und **Suchen und 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 können sich nicht an den genauen Namen oder das Volumen, in dem es sich befindet, oder an das Datum erinnern, an dem es zuletzt in gutem Zustand war.

Diese Tabelle bietet einen Funktionsvergleich der beiden Methoden.

Suchen Und Wiederherstellen	Suche Und Wiederherstellung
Durchsuchen Sie eine Ordnerstruktur, um das Volume, den Ordner oder die Datei in einer einzelnen Sicherungsdatei zu finden.	Suchen Sie nach einem Volume, Ordner oder einer Datei über **alle Sicherungsdateien** nach einem teilweisen oder vollständigen Datenträgernamen, einem teilweisen oder vollständigen Ordner-/Dateinamen, einem Größenbereich und zusätzlichen Suchfiltern.
Führt keine Dateiwiederherstellung durch, wenn die Datei gelöscht oder umbenannt wurde, und der Benutzer den ursprünglichen Dateinamen nicht kennt	Verarbeitet neu erstellte/gelöschte/umbenannte Verzeichnisse und neu erstellte/gelöschte/umbenannte Dateien
Es sind keine zusätzlichen Ressourcen für Cloud-Provider erforderlich	Beim Restore aus der Cloud werden pro Konto zusätzliche Bucket- und Public-Cloud-Provider-Ressourcen benötigt.
Es sind keine zusätzlichen Kosten für Cloud-Provider erforderlich	Wenn Sie Daten aus der Cloud wiederherstellen, sind zusätzliche Kosten erforderlich, wenn Sie Ihre Backups und Volumes zur Suche nach Suchergebnissen scannen.
Schnelle Wiederherstellung wird unterstützt.	Schnelle Wiederherstellung wird nicht unterstützt.

Diese Tabelle enthält eine Liste gültiger Wiederherstellungsvorgänge, die auf dem Speicherort der Sicherungsdateien basieren.

Backup-Typ	Suchen Und Wiederherstellen			Suche Und Wiederherstellung		
	Lautstärke wiederherstellen	* Dateien wiederherstellen*	**Ordner wiederherstellen**	**Lautstärke wiederherstellen**	* Dateien wiederherstellen*	**Ordner wiederherstellen**
Snapshot Kopie	Ja.	Nein	Nein	Ja.	Ja.	Ja.
Repliziertes Volume	Ja.	Nein	Nein	Ja.	Ja.	Ja.
Sicherungsdatei	Ja.	Ja.	Ja.	Ja.	Ja.	Ja.

Bevor Sie eine der beiden Wiederherstellungsmethoden 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:

- <<Stellen Sie Volumes mithilfe von Browse Restore wieder her,Stellen Sie Volumes mithilfe von Browse Restore wieder her
- <<Wiederherstellen von Ordnern und Dateien mit Durchsuchen Restore,Wiederherstellen von Ordnern und Dateien mit Durchsuchen Restore
- <<restore-ontap-data-using-search-restore,Stellen Sie Volumes, Ordner und Dateien mithilfe von Search Restore wieder her

Stellen Sie ONTAP-Daten mithilfe von Durchsuchen und Wiederherstellen wieder her

Bevor Sie mit der Wiederherstellung eines Volumes, Ordners oder einer Datei beginnen, sollten Sie den Namen des Volumes, von dem aus Sie wiederherstellen möchten, den Namen der Arbeitsumgebung und SVM, auf dem sich das Volume befindet, sowie das ungefähre Datum der Sicherungsdatei, aus der Sie wiederherstellen möchten, kennen. Sie können ONTAP Daten von einer Snapshot Kopie, einem replizierten Volume oder von Backups im Objektspeicher wiederherstellen.

Hinweis: Wenn sich die Sicherungsdatei mit den Daten, die Sie wiederherstellen möchten, im Archiv-Cloud-Speicher befindet (beginnend mit ONTAP 9.10.1), dauert der Wiederherstellungsvorgang länger und verursacht Kosten. Zusätzlich muss auf dem Ziel-Cluster für die Volume-Wiederherstellung ONTAP 9.10.1 oder höher, 9.11.1 für die Wiederherstellung von Dateien, 9.12.1 für Google Archive und StorageGRID und 9.13.1 für die Wiederherstellung von Ordnern ausgeführt werden.

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

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

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

Die hohe Priorität wird nicht unterstützt, wenn Daten aus dem Azure Archiv-Storage auf StorageGRID Systeme wiederhergestellt werden.

Unterstützte Arbeitsumgebungen und Objekt-Storage-Anbieter durchsuchen und wiederherstellen

Sie können ONTAP-Daten aus einer Backup-Datei in einer sekundären Arbeitsumgebung (einem replizierten Volume) oder im Objektspeicher (einer Backup-Datei) in den folgenden Arbeitsumgebungen wiederherstellen. Snapshot Kopien befinden sich in der Quell-Arbeitsumgebung, sie können nur auf demselben System wiederhergestellt werden.

Hinweis: Sie können ein Volume von jeder Art von Sicherungsdatei wiederherstellen, aber Sie können einen Ordner oder einzelne Dateien nur aus einer Sicherungsdatei im Objektspeicher wiederherstellen.

Aus Objektspeicher (Backup)	**Von Primär (Snapshot)**	**Vom Sekundären System (Replikation)**	Zum Ziel Der Arbeitsumgebung Ifdef::aws[]

Amazon S3	Cloud Volumes ONTAP in AWS Lokales ONTAP System	Cloud Volumes ONTAP in AWS Lokales ONTAP System Endif::aws[] Ifdef::azurblau[]	Azure Blob
Cloud Volumes ONTAP in Azure Lokales ONTAP System	Cloud Volumes ONTAP in Azure Lokales ONTAP System Endif::azurblau[] Ifdef::gcp[]	Google Cloud Storage	Cloud Volumes ONTAP in Google Lokales ONTAP System
Cloud Volumes ONTAP in Google On-Premises ONTAP System endif::gcp[]	NetApp StorageGRID	Lokales ONTAP System	Lokales ONTAP System Cloud Volumes ONTAP
Zum lokalen ONTAP System	ONTAP S3	Lokales ONTAP System	Lokales ONTAP System Cloud Volumes ONTAP

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

- Bei Amazon S3 kann der Connector in AWS oder lokal implementiert werden
- Für Azure Blob kann der Connector in Azure oder in Ihrem Standort implementiert werden
- Für Google Cloud Storage muss der Connector in Ihrer Google Cloud Platform VPC implementiert werden
- Für StorageGRID muss der Connector in Ihrem Betrieb mit oder ohne Internetzugang bereitgestellt werden
- Bei ONTAP S3 kann der Connector (mit oder ohne Internetzugang) vor Ort oder in einer Cloud-Provider-Umgebung implementiert werden

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

Wenn die ONTAP-Version auf Ihrem System kleiner als 9.13.1 ist, können Sie keine Ordner oder Dateien wiederherstellen, wenn die Sicherungsdatei mit DataLock & Ransomware konfiguriert wurde. In diesem Fall können Sie das gesamte Volume aus der Sicherungsdatei wiederherstellen und anschließend auf die von Ihnen benötigten Dateien zugreifen.

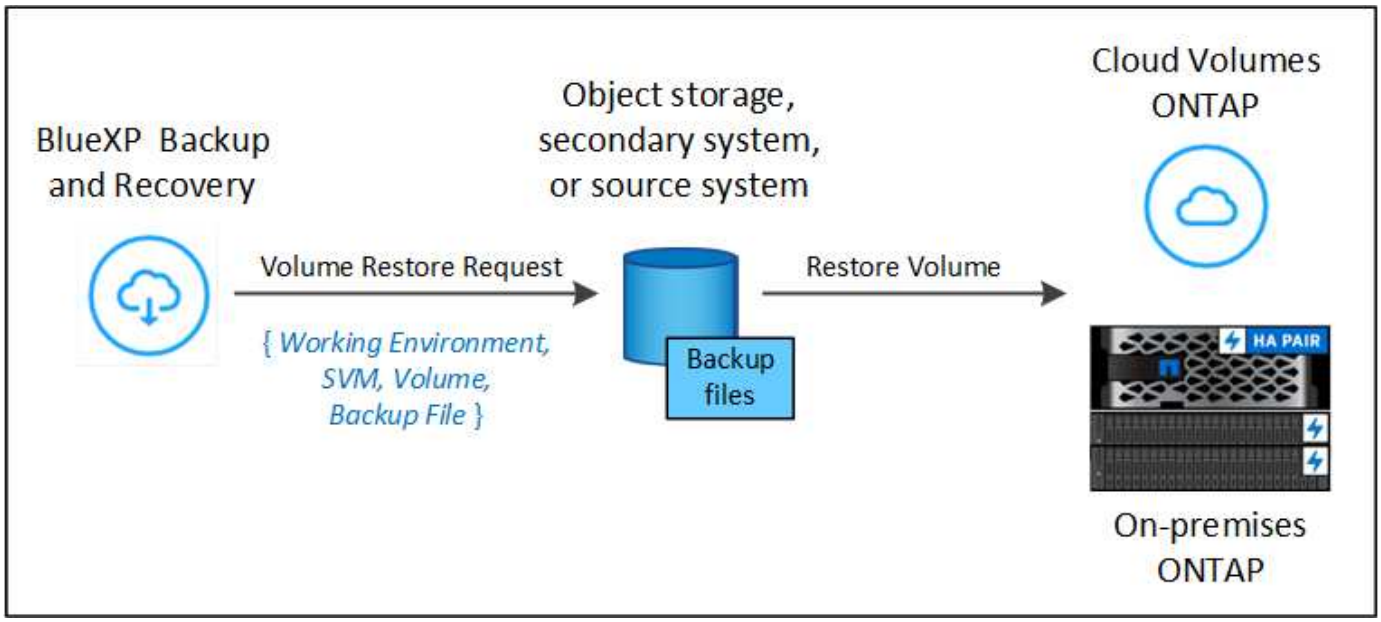
Stellen Sie Volumes mithilfe von Browse & Restore wieder her

Wenn Sie ein Volume aus einer Backup-Datei wiederherstellen, erstellt BlueXP Backup und Recovery mithilfe der Daten aus dem Backup ein *New* Volume. Wenn Sie ein Backup aus dem Objekt-Storage verwenden, können Sie die Daten auf einem Volume in der ursprünglichen Arbeitsumgebung wiederherstellen, in einer anderen Arbeitsumgebung, die sich in demselben Cloud-Konto wie die ursprüngliche Arbeitsumgebung befindet, oder auf einem lokalen ONTAP System.

Bei der Wiederherstellung eines Cloud-Backups auf einem Cloud Volumes ONTAP-System mit ONTAP 9.13.0 oder höher oder auf einem lokalen ONTAP-System mit ONTAP 9.14.1 haben Sie die Möglichkeit, eine schnelle Wiederherstellung durchzuführen. Die schnelle Wiederherstellung ist ideal für Disaster Recovery-Situationen, in denen Sie so schnell wie möglich Zugriff auf ein Volume gewährleisten müssen. Bei einer schnellen Wiederherstellung werden die Metadaten aus der Backup-Datei auf einem Volume wiederhergestellt, anstatt die gesamte Backup-Datei wiederherzustellen. Die schnelle Wiederherstellung ist weder für Performance- noch für latenzkritische Applikationen empfehlenswert und wird bei Backups in archiviertem Storage nicht unterstützt.

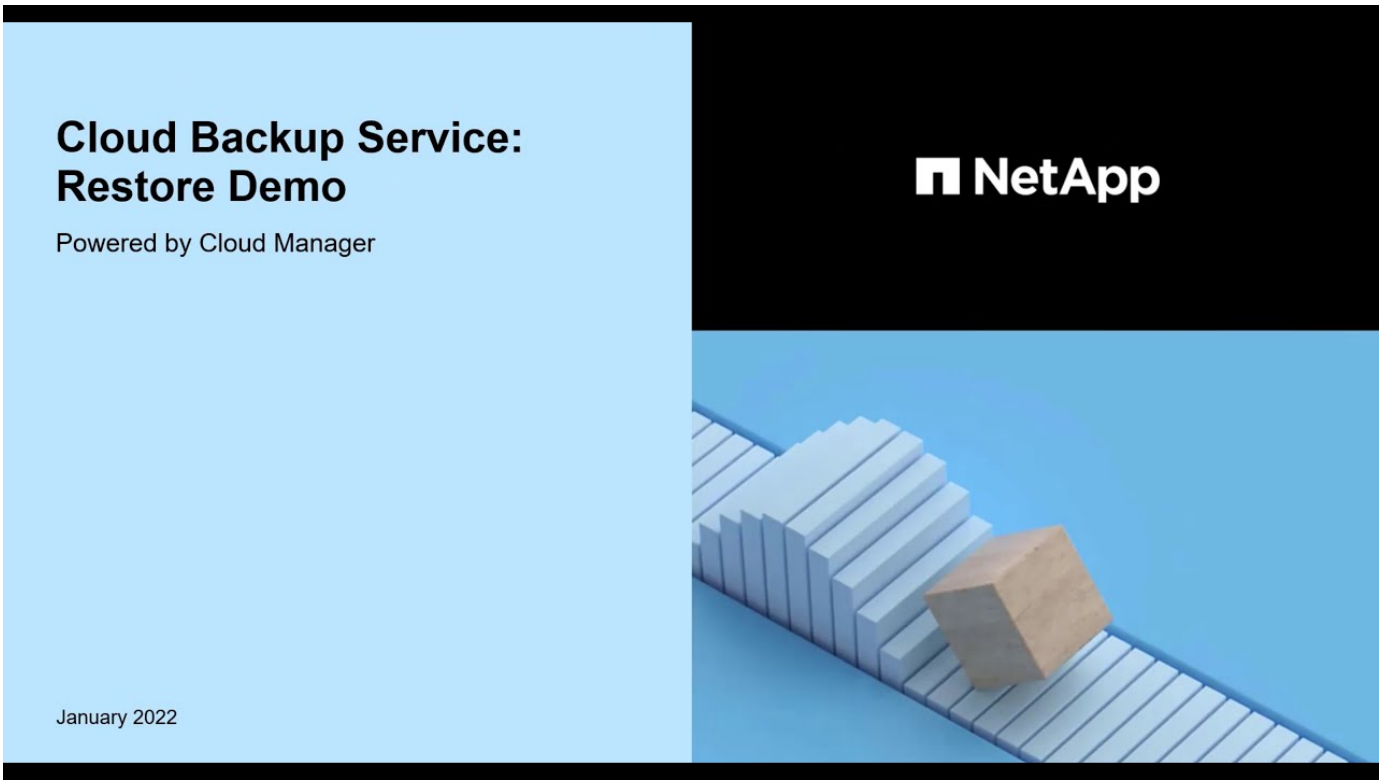
Die schnelle Wiederherstellung wird für FlexGroup Volumes nur dann unterstützt, wenn das Quellsystem, auf dem das Cloud-Backup erstellt wurde, ONTAP 9.12.1 oder höher ausgeführt wurde. Sie wird nur für SnapLock Volumes unterstützt, wenn auf dem Quellsystem ONTAP 9.11.0 oder höher ausgeführt wurde.

Bei der Wiederherstellung von einem replizierten Volume können Sie das Volume in der ursprünglichen Arbeitsumgebung oder in einem Cloud Volumes ONTAP oder einem lokalen ONTAP System wiederherstellen.



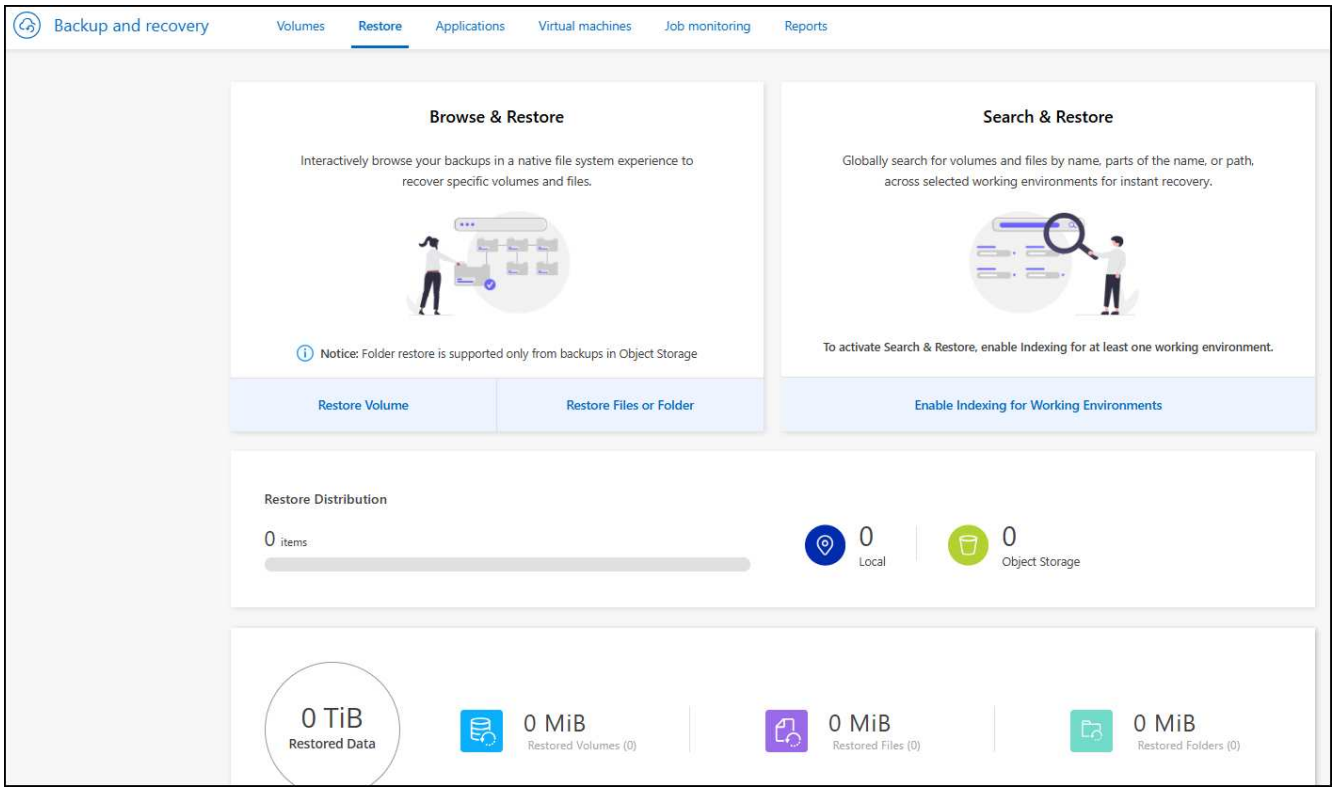
Wie Sie sehen können, müssen Sie den Namen der Quellarbeitsumgebung, die Storage-VM, den Volume-Namen und das Datum der Backup-Datei kennen, um eine Volume-Wiederherstellung durchzuführen.

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



Schritte

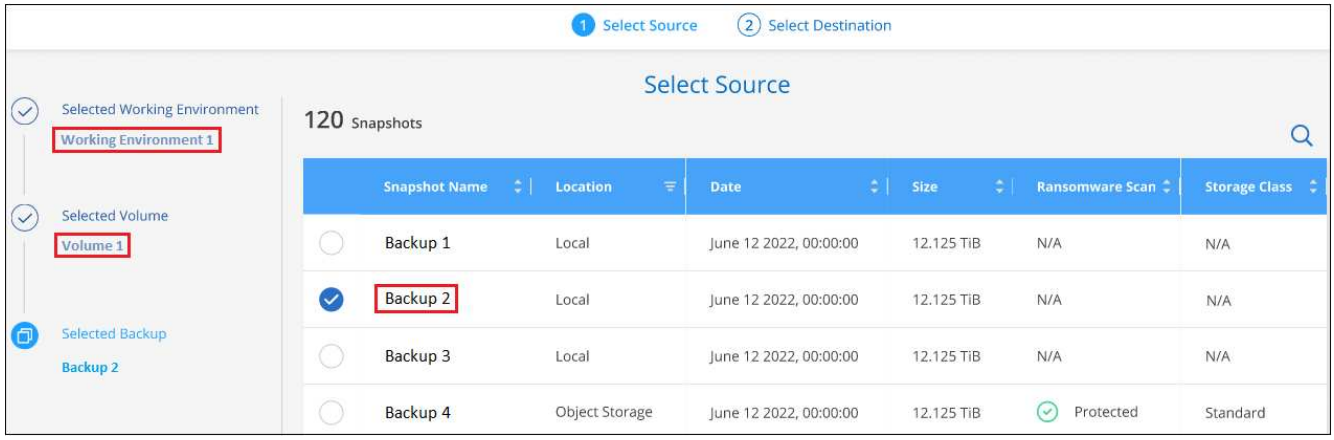
1. Wählen Sie im Menü BlueXP die Option **Schutz > Sicherung und Wiederherstellung**.
2. Klicken Sie auf die Registerkarte **Wiederherstellen**, und das Dashboard wiederherstellen wird angezeigt.
3. Klicken Sie im Abschnitt „*Browse & Restore*“ auf **Volume wiederherstellen**.



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.

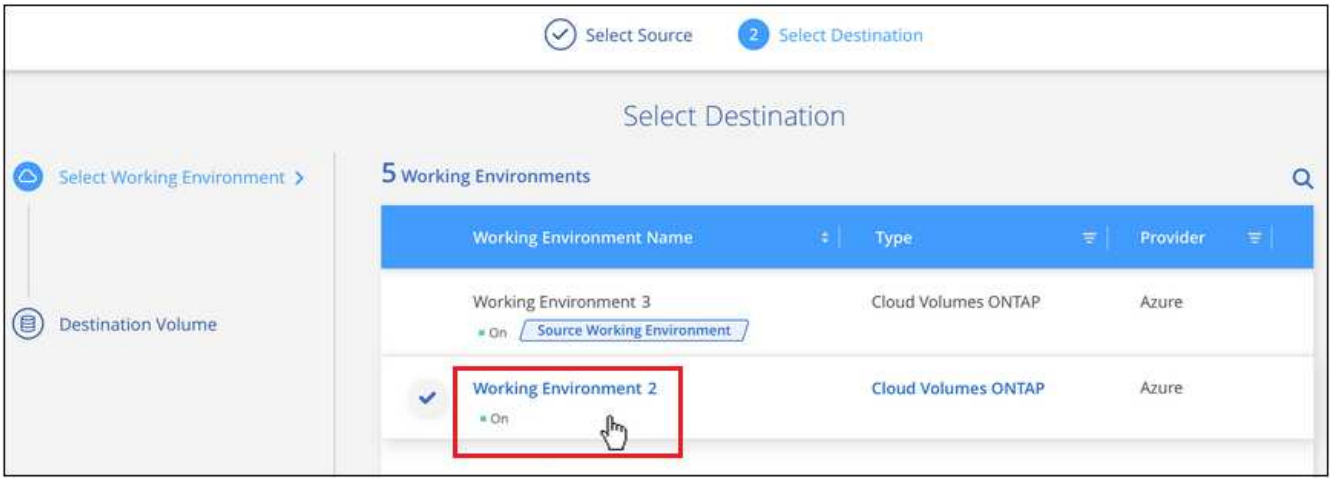
Die Spalte **Location** zeigt an, ob die Sicherungsdatei (Snapshot) **lokal** (eine Snapshot-Kopie auf dem Quellsystem), **sekundär** (ein repliziertes Volume auf einem sekundären ONTAP-System) oder **Objektspeicher** (eine Sicherungsdatei im Objektspeicher) ist. Wählen Sie die Datei aus, die Sie wiederherstellen möchten.



5. Klicken Sie Auf **Weiter**.

   Wenn Sie eine Backup-Datei im Objekt-Storage auswählen und für dieses Backup der Ransomware-Schutz aktiv ist (wenn Sie DataLock und Ransomware-Schutz in der Backup-Richtlinie aktiviert haben), werden Sie vor der Wiederherstellung der Daten aufgefordert, einen zusätzlichen Ransomware-Scan für die Backup-Datei auszuführen. Wir empfehlen, die Backup-Datei nach Ransomware zu scannen. (Für den Zugriff auf die Inhalte der Backup-Datei entstehen zusätzliche Kosten durch Ihren Cloud-Provider.)

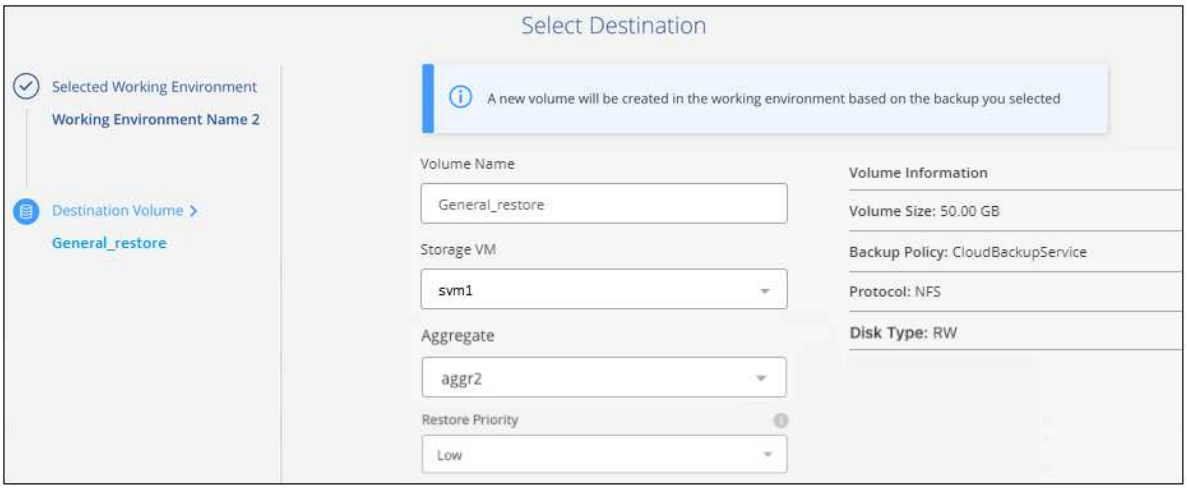
6. Wählen Sie auf der Seite *Ziel auswählen* die Option **Arbeitsumgebung** aus, in der Sie das Volume wiederherstellen möchten.



7. Wenn Sie beim Wiederherstellen einer Backup-Datei aus dem Objekt-Storage ein lokales ONTAP-System auswählen und noch nicht die Cluster-Verbindung zum Objekt-Storage konfiguriert haben, werden Sie zur Eingabe weiterer Informationen aufgefordert:
   - 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.

- Wählen Sie beim Wiederherstellen aus Azure Blob den IPspace im ONTAP Cluster aus, wo sich das Ziel-Volume befinden soll, wählen Sie Azure Abonnement für den Zugriff auf den Objekt-Storage aus. Wählen Sie optional einen privaten Endpunkt für den sicheren Datentransfer aus, indem Sie vnet und Subnetz auswählen.
- Wählen Sie bei der Wiederherstellung aus Google Cloud Storage das Google Cloud-Projekt sowie den Zugriffsschlüssel und den geheimen Schlüssel für den Zugriff auf den Objektspeicher, die Region, in der die Backups gespeichert sind, und den IPspace im ONTAP-Cluster, in dem sich das Ziel-Volume befindet.
- 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.
- Geben Sie beim Wiederherstellen aus ONTAP S3 den FQDN des ONTAP S3-Servers und den Port ein, den ONTAP für die HTTPS-Kommunikation mit ONTAP S3 verwenden soll, wählen Sie den Zugriffsschlüssel und den geheimen Schlüssel aus, die für den Zugriff auf den Objektspeicher erforderlich sind. und den IPspace im ONTAP Cluster, wo sich das Ziel-Volume befinden soll.

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. Bei der Wiederherstellung eines FlexGroup Volumes müssen Sie mehrere Aggregate auswählen. Standardmäßig wird **<source_Volume_Name>_restore** als Volume-Name verwendet.



Bei der Wiederherstellung eines Backups vom Objektspeicher auf ein Cloud Volumes ONTAP System mit ONTAP 9.13.0 oder neuer oder auf ein lokales ONTAP System mit ONTAP 9.14.1 haben Sie die Möglichkeit, eine *Quick Restore* -Operation durchzuführen.

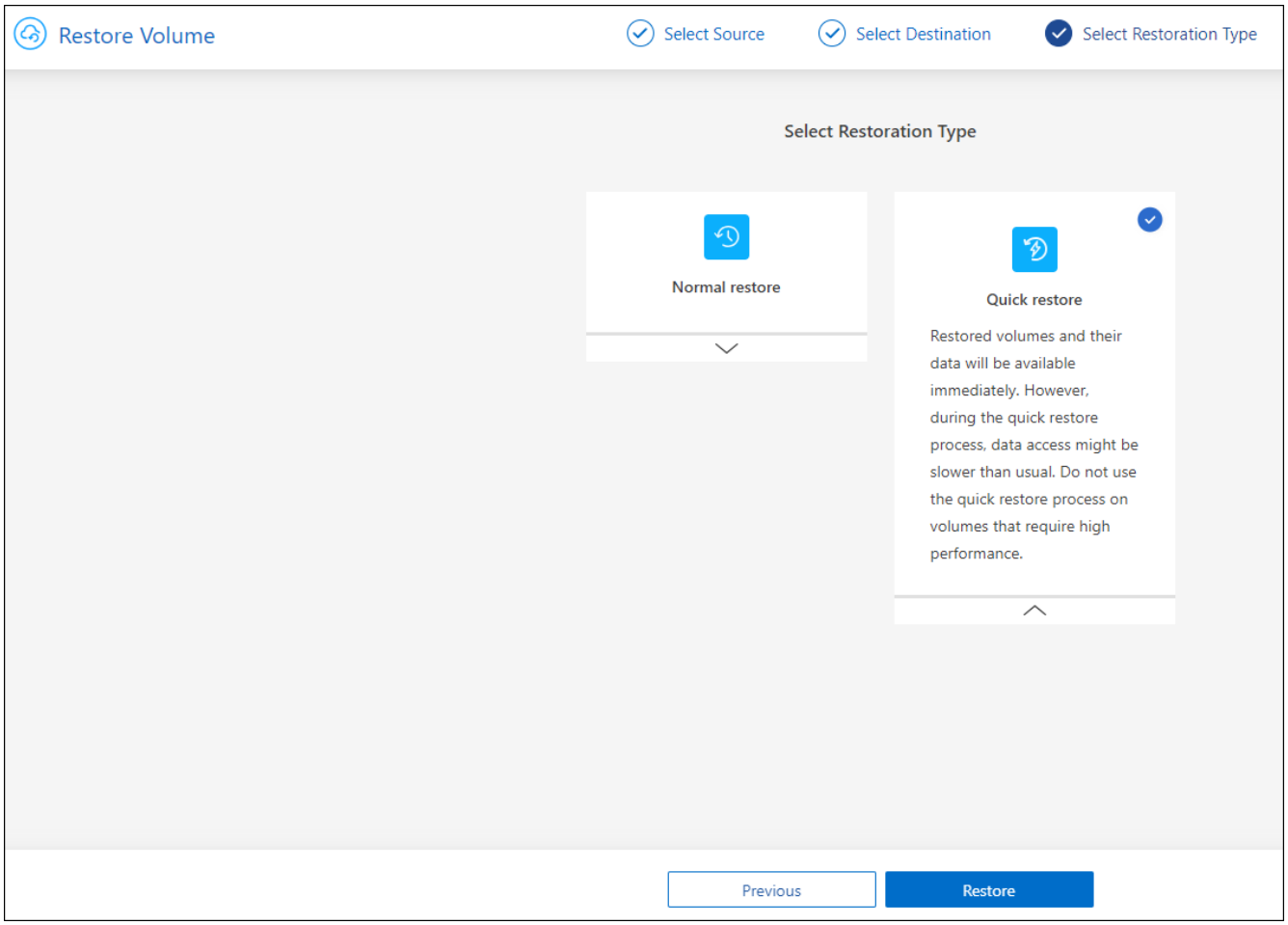
Wenn Sie das Volume aus einer Sicherungsdatei wiederherstellen, die sich in einer Archiv-Storage-Ebene befindet (verfügbar ab ONTAP 9.10.1), können Sie die Restore-Priorität auswählen.

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

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

"Erfahren Sie mehr über die Wiederherstellung aus Google Archiv-Storage". Backup-Dateien werden auf der Google Archiv Storage Tier nahezu sofort wiederhergestellt und müssen keine Restore-Priorität erhalten.

1. Klicken Sie auf **Weiter**, um auszuwählen, ob Sie eine normale Wiederherstellung oder einen Schnellwiederherstellungsprozess durchführen möchten:



   - **Normale Wiederherstellung**: Verwenden Sie normale Wiederherstellung auf Volumes, die hohe Leistung erfordern. Volumes sind erst verfügbar, wenn der Wiederherstellungsvorgang abgeschlossen ist.
   - **Quick Restore**: Wiederhergestellte Volumes und Daten werden sofort verfügbar sein. Verwenden Sie dies nicht auf Volumes, die eine hohe Performance erfordern, da der Zugriff auf die Daten während der schnellen Wiederherstellung möglicherweise langsamer als gewöhnlich sein kann.
2. Klicken Sie auf **Wiederherstellen** und Sie werden wieder zum Restore Dashboard zurückgekehrt, damit Sie den Fortschritt des Wiederherstellungsvorgangs überprüfen können.

Ergebnis

Mit BlueXP Backup und Recovery wird auf Basis des von Ihnen ausgewählten Backups ein neues Volume erstellt.

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 & Restore

Wenn Sie nur einige wenige 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.

> Sie können einen Ordner oder einzelne Dateien derzeit nur aus einer Sicherungsdatei im Objektspeicher wiederherstellen. Das Wiederherstellen von Dateien und Ordnern aus einer lokalen Snapshot-Kopie oder aus einer Sicherungsdatei, die sich in einer sekundären Arbeitsumgebung (einem replizierten Volume) befindet, wird derzeit nicht unterstützt.

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.

Wenn Sie ONTAP 9.13.0 oder höher verwenden, können Sie einen Ordner zusammen mit allen darin enthaltenen Dateien und Unterordnern wiederherstellen. Wenn Sie eine Version von ONTAP vor 9.13.0 verwenden, werden nur Dateien aus diesem Ordner wiederhergestellt - keine Unterordner oder Dateien in Unterordnern werden wiederhergestellt.

> - Wenn die Sicherungsdatei mit DataLock & Ransomware-Schutz konfiguriert wurde, wird die Wiederherstellung auf Ordnerebene nur unterstützt, wenn die ONTAP-Version 9.13.1 oder höher ist. Wenn Sie eine frühere Version von ONTAP verwenden, können Sie das gesamte Volume aus der Sicherungsdatei wiederherstellen und dann auf den gewünschten Ordner und die benötigten Dateien zugreifen.
> - Wenn sich die Backup-Datei im Archiv-Storage befindet, wird die Wiederherstellung auf Ordnerebene nur unterstützt, wenn die ONTAP-Version 9.13.1 oder höher ist. Wenn Sie eine frühere Version von ONTAP verwenden, können Sie den Ordner aus einer neueren Sicherungsdatei wiederherstellen, die nicht archiviert wurde, oder Sie können das gesamte Volume aus dem archivierten Backup wiederherstellen und dann auf den Ordner und die Dateien zugreifen, die Sie benötigen.
> - Mit ONTAP 9.15.1 können Sie FlexGroup-Ordner mit der Option "Durchsuchen und Wiederherstellen" wiederherstellen. Diese Funktion befindet sich in einem Technology Preview-Modus.
>
> Sie können es mit einem speziellen Flag testen, das in beschrieben "BlueXP Backup und Recovery – Release-Blog vom 2024. Juli"ist.

Voraussetzungen

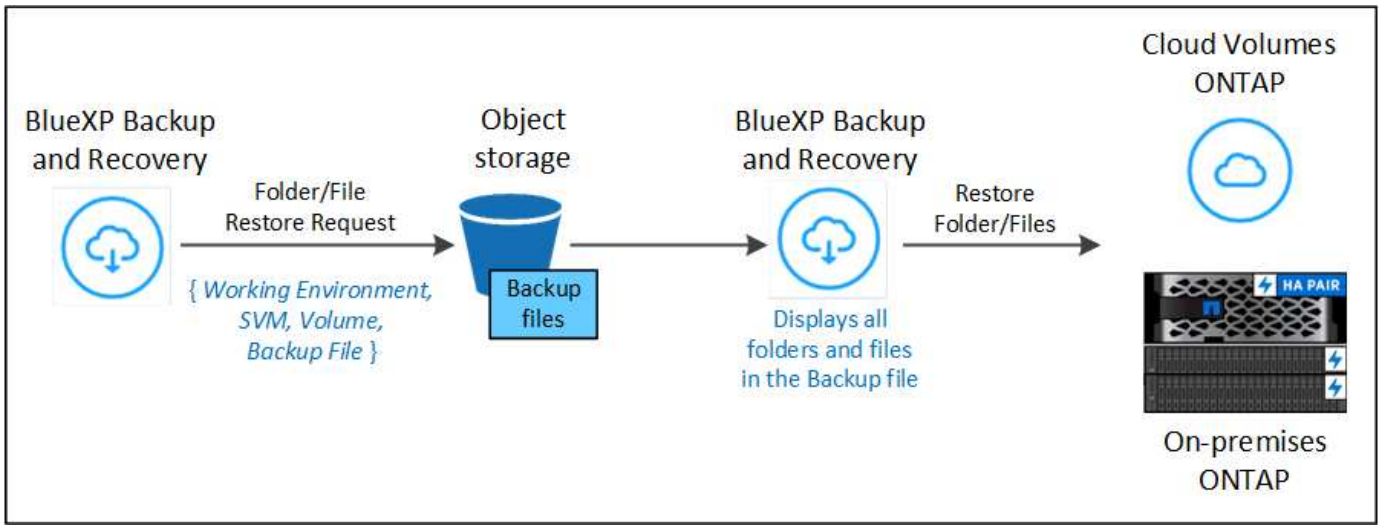
- Die ONTAP-Version muss mindestens 9.6 sein, um *File* Restore-Vorgänge durchzuführen.
- Die ONTAP-Version muss mindestens 9.11.1 sein, um Vorgänge *folder* wiederherstellen zu können. ONTAP Version 9.13.1 ist erforderlich, wenn sich die Daten im Archiv-Storage befinden oder wenn die Backup-Datei DataLock- und Ransomware-Schutz verwendet.
- Die ONTAP-Version muss 9.15.1 p2 oder höher sein, um FlexGroup-Verzeichnisse mithilfe der Option „Durchsuchen und Wiederherstellen“ wiederherzustellen.

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. Bei BlueXP Backup und Recovery werden die Ordner und Dateien angezeigt, die in der ausgewählten Backup-Datei 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.

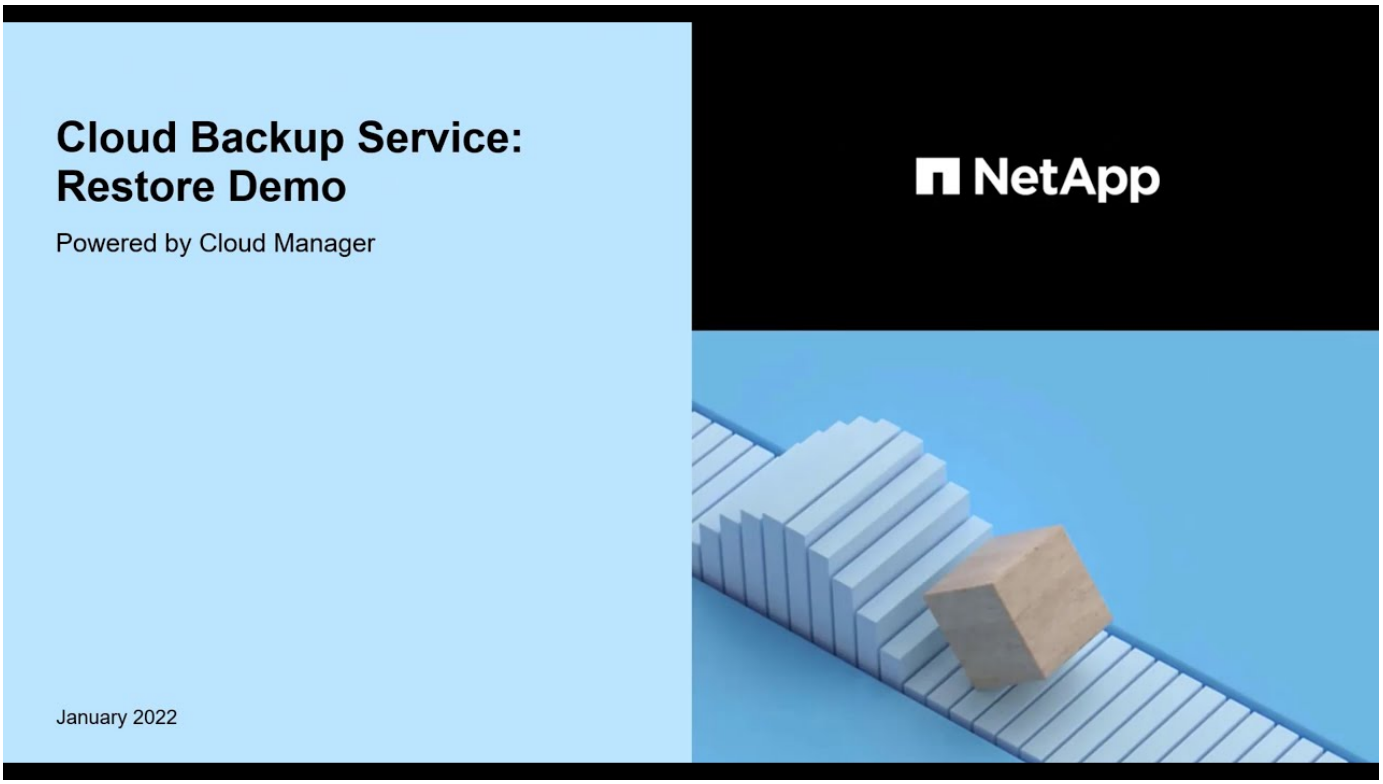


Wie Sie sehen, müssen Sie den Namen der Arbeitsumgebung, den Namen des Volumes, das Datum der Sicherungsdatei und den Ordner-/Dateinamen kennen, um einen Ordner oder eine Dateiwiederherstellung durchzuführen.

Wiederherstellung von Ordnern und Dateien

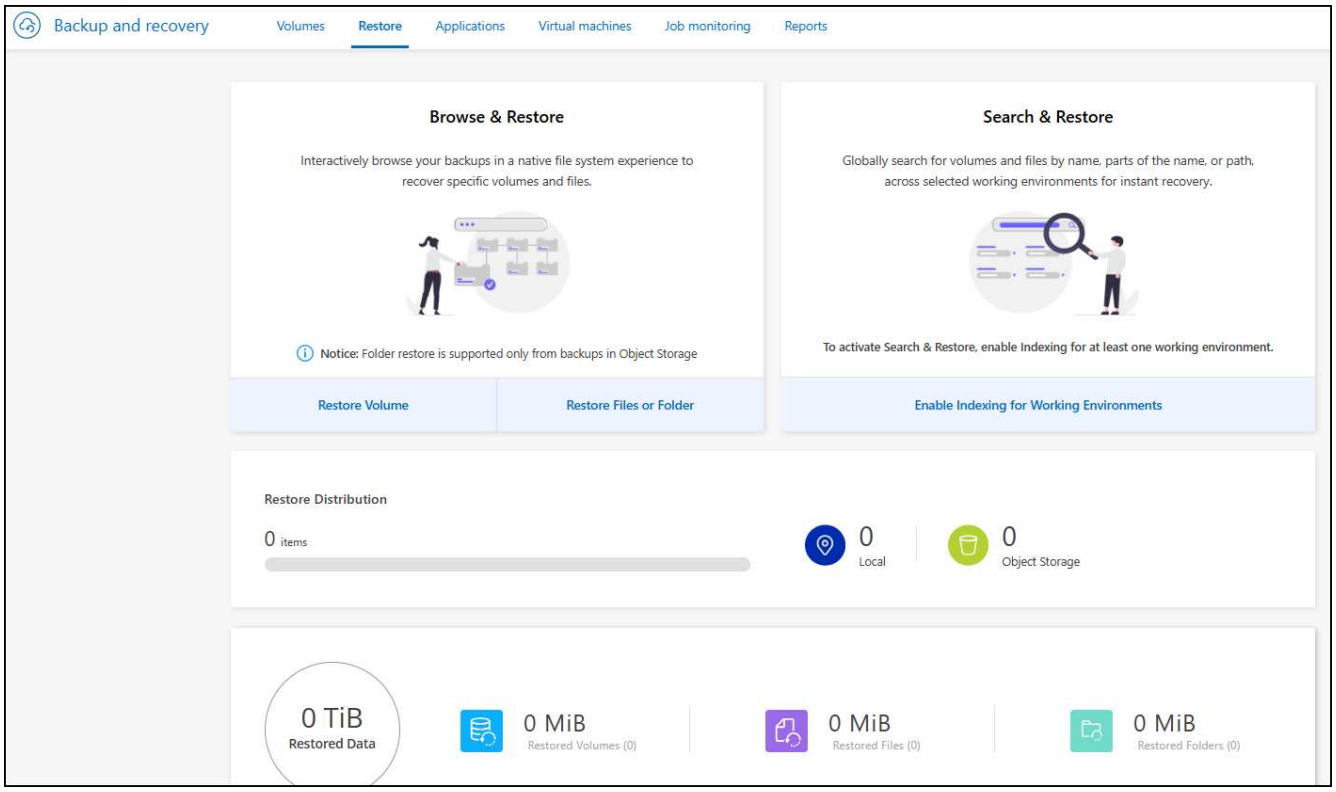
Führen Sie diese Schritte aus, um Ordner oder Dateien auf einem Volume von einem ONTAP Volume-Backup wiederherzustellen. Sie sollten den Namen des Volumes und das Datum der Sicherungsdatei kennen, die Sie zum Wiederherstellen des Ordners oder der Datei(en) verwenden möchten. Diese Funktion verwendet 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:



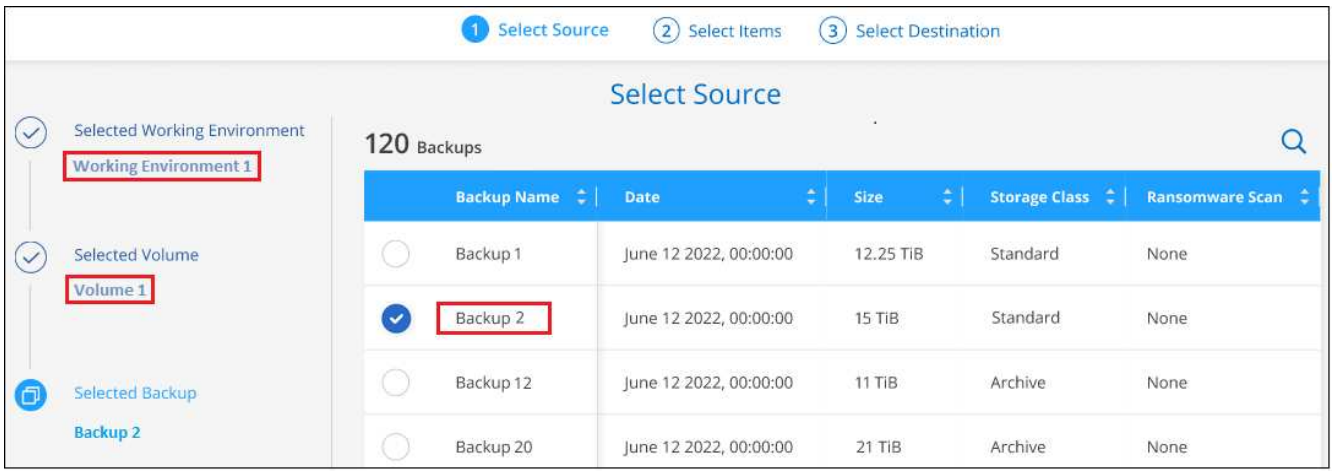
Schritte

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 einem Archiv-Storage-Tier befindet, können Sie die Wiederherstellungspriorität auswählen.

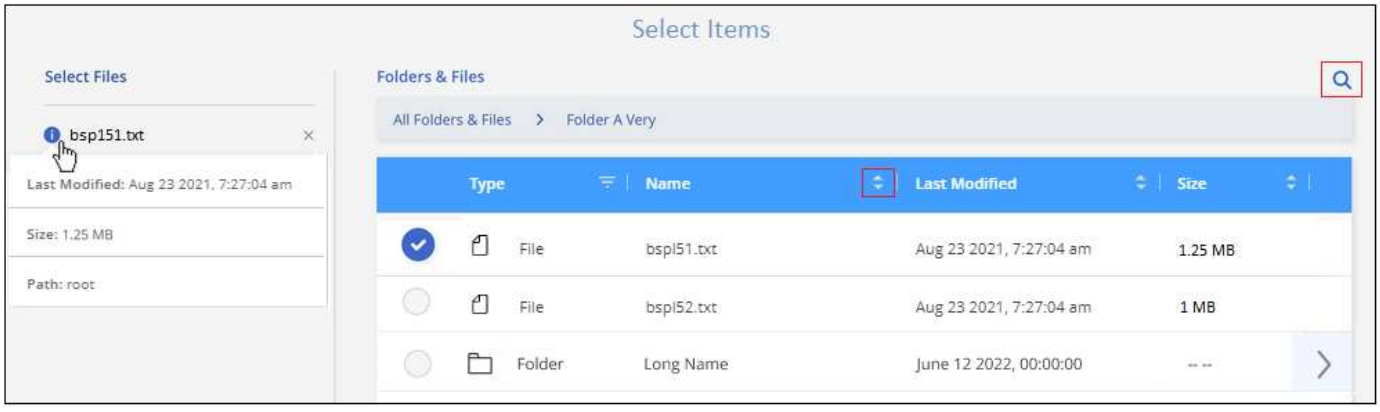
"Erfahren Sie mehr über die Wiederherstellung aus AWS Archiv-Storage".

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

"Erfahren Sie mehr über die Wiederherstellung aus Google Archiv-Storage". Backup-Dateien werden auf der Google Archiv Storage Tier nahezu sofort wiederhergestellt und müssen keine Restore-Priorität erhalten.

+
Und wenn für die Backup-Datei ein Ransomware-Schutz aktiv ist (wenn Sie in der Backup-Richtlinie DataLock und Ransomware-Schutz aktiviert haben), werden Sie vor dem Wiederherstellen der Daten aufgefordert, einen zusätzlichen Ransomware-Scan der Backup-Datei auszuführen. Wir empfehlen, die Backup-Datei nach Ransomware zu scannen. (Für den Zugriff auf die Inhalte der Backup-Datei entstehen zusätzliche Kosten durch Ihren Cloud-Provider.)

+

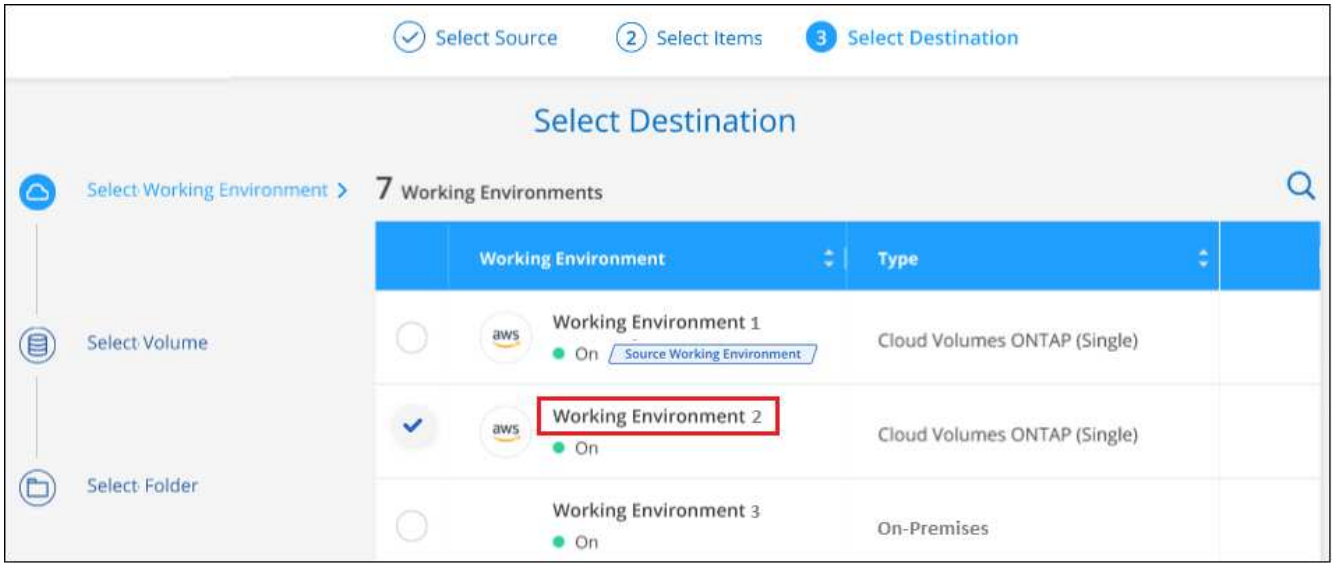


1. Wählen Sie auf der Seite „ Elemente auswählen_“ den Ordner oder die Datei(en) aus, die wiederhergestellt werden sollen, und klicken Sie auf **Weiter**. So finden Sie das Element:

- 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.

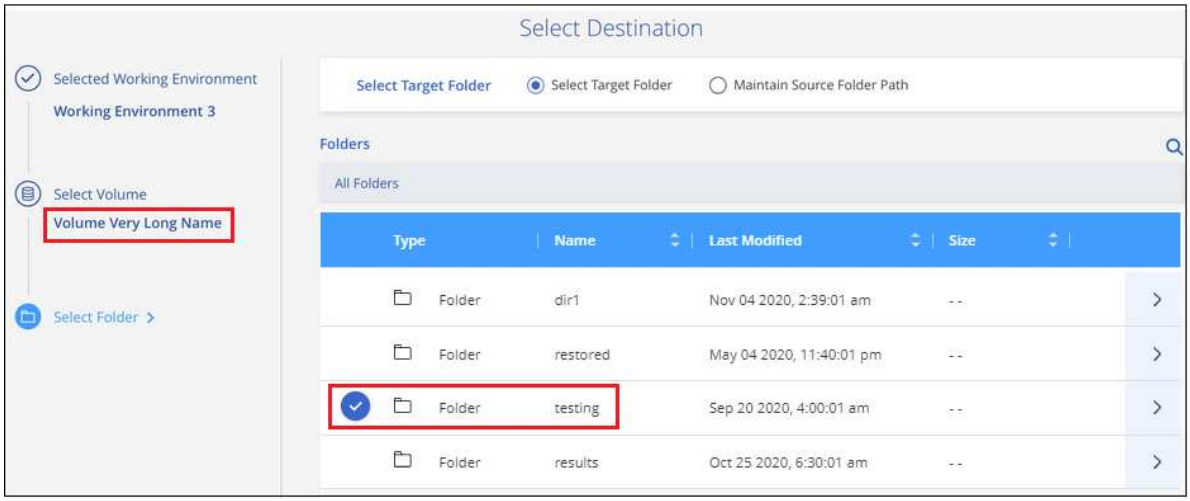
2. Wählen Sie auf der Seite *Ziel auswählen* die Option **Arbeitsumgebung** aus, in der Sie die Elemente wiederherstellen möchten.



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 bei der Wiederherstellung aus Azure Blob den IPspace im ONTAP Cluster ein, wo sich das Ziel-Volume befindet. Sie können auch eine Private Endpoint-Konfiguration für die Verbindung zum Cluster auswählen.
  - Geben Sie bei der Wiederherstellung aus Google Cloud Storage den IPspace im ONTAP Cluster ein, in dem sich die Ziel-Volumes befinden, sowie den Zugriffsschlüssel und den geheimen Schlüssel, die für den Zugriff auf den Objekt-Storage erforderlich sind.
  - 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.

Stellen Sie ONTAP-Daten mithilfe von Suchen und Wiederherstellen wieder her

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

Bei diesem Suchvorgang werden alle lokalen Snapshot Kopien für Ihre ONTAP Volumes, alle replizierten Volumes auf sekundären Storage-Systemen und alle Backup-Dateien im Objekt-Storage angezeigt. Da das Wiederherstellen von Daten von einer lokalen Snapshot Kopie oder einem replizierten Volume schneller und kostengünstiger sein kann als die Wiederherstellung von einer Backup-Datei im Objektspeicher, sollten Sie Daten von diesen anderen Standorten wiederherstellen.

Wenn Sie ein *vollständiges Volume* aus einer Backup-Datei wiederherstellen, erstellt BlueXP Backup und Recovery unter Verwendung der Daten aus dem Backup ein *neues* Volume. Sie können Daten als Volume in der ursprünglichen Arbeitsumgebung, in einer anderen Arbeitsumgebung, die sich in demselben Cloud-Konto wie die ursprüngliche Arbeitsumgebung befindet, oder auf einem lokalen ONTAP System wiederherstellen.

Sie können *Ordner oder Dateien* am ursprünglichen Speicherort des Volumes, auf einem anderen Volume in derselben Arbeitsumgebung, in einer anderen Arbeitsumgebung, die dasselbe Cloud-Konto verwendet, oder

auf einem Volume auf einem lokalen ONTAP-System wiederherstellen.

Wenn Sie ONTAP 9.13.0 oder höher verwenden, können Sie einen Ordner zusammen mit allen darin enthaltenen Dateien und Unterordnern wiederherstellen. Wenn Sie eine Version von ONTAP vor 9.13.0 verwenden, werden nur Dateien aus diesem Ordner wiederhergestellt - keine Unterordner oder Dateien in Unterordnern werden wiederhergestellt.

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 für die Volume-Wiederherstellung auch ONTAP 9.10.1 oder höher, 9.11.1 für die Dateiwiederherstellung, 9.12.1 für Google Archive und StorageGRID und 9.13.1 für die Wiederherstellung von Ordnern ausgeführt werden muss.

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

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

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

- Wenn die Backup-Datei im Objektspeicher mit DataLock & Ransomware-Schutz konfiguriert wurde, wird die Wiederherstellung auf Ordnerebene nur unterstützt, wenn die ONTAP-Version 9.13.1 oder höher ist. Wenn Sie eine frühere Version von ONTAP verwenden, können Sie das gesamte Volume aus der Sicherungsdatei wiederherstellen und dann auf den gewünschten Ordner und die benötigten Dateien zugreifen.
- Wenn sich die Backup-Datei im Objektspeicher im Archiv-Storage befindet, wird die Wiederherstellung auf Ordnerebene nur unterstützt, wenn die ONTAP Version 9.13.1 oder höher ist. Wenn Sie eine frühere Version von ONTAP verwenden, können Sie den Ordner aus einer neueren Sicherungsdatei wiederherstellen, die nicht archiviert wurde, oder Sie können das gesamte Volume aus dem archivierten Backup wiederherstellen und dann auf den Ordner und die Dateien zugreifen, die Sie benötigen.
- Die Priorität bei der Wiederherstellung „hoch“ wird beim Wiederherstellen von Daten aus dem Azure Archiv-Storage auf StorageGRID Systeme nicht unterstützt.
- Das Wiederherstellen von Ordnern wird derzeit nicht von Volumes in ONTAP S3 Objekt-Storage unterstützt.

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 ONTAP-Daten aus einer Backup-Datei in einer sekundären Arbeitsumgebung (einem replizierten Volume) oder im Objektspeicher (einer Backup-Datei) in den folgenden Arbeitsumgebungen wiederherstellen. Snapshot Kopien befinden sich in der Quell-Arbeitsumgebung, sie können nur auf demselben System wiederhergestellt werden.

Hinweis: Sie können Volumes und Dateien von jeder Art von Sicherungsdatei wiederherstellen, aber Sie können einen Ordner nur von Sicherungsdateien im Objektspeicher zu diesem Zeitpunkt wiederherstellen.

Speicherort Der Sicherungsdatei		**Zielarbeitsumgebung**
Objektspeicher (Sicherung)	**Sekundärsystem (Replikation)**	ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP in AWS Lokales ONTAP System	Cloud Volumes ONTAP in AWS On-Premises ONTAP System endif::aws[] ifdef::azurAzure[]
Azure Blob	Cloud Volumes ONTAP in Azure Lokales ONTAP System	Cloud Volumes ONTAP in Azure On-Premises ONTAP System endif::Azure[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP in Google Lokales ONTAP System	Cloud Volumes ONTAP in Google On-Premises ONTAP System endif::gcp[]
NetApp StorageGRID	Lokales ONTAP System Cloud Volumes ONTAP	Lokales ONTAP System
ONTAP S3	Lokales ONTAP System Cloud Volumes ONTAP	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 Azure Blob kann der Connector in Azure oder in Ihrem Standort implementiert werden
- Für Google Cloud Storage muss der Connector in Ihrer Google Cloud Platform VPC implementiert werden
- Für StorageGRID muss der Connector in Ihrem Betrieb mit oder ohne Internetzugang bereitgestellt werden
- Bei ONTAP S3 kann der Connector (mit oder ohne Internetzugang) vor Ort oder in einer Cloud-Provider-Umgebung implementiert werden

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 (NFS und SMB/CIFS Volumes werden unterstützt).
  - Der SnapDiff RPC Server muss auf der SVM aktiviert sein. BlueXP führt diese Funktion automatisch aus, wenn Sie die Indexierung in der Arbeitsumgebung aktivieren. (SnapDiff ist die Technologie, die die Datei- und Verzeichnisunterschiede zwischen Snapshot Kopien schnell identifiziert.)
- 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".

    Wenn Sie bereits BlueXP Backup und Recovery mit einem Connector genutzt haben, den Sie in der Vergangenheit konfiguriert haben, müssen Sie jetzt die Berechtigungen Athena und Glue zur BlueXP Benutzerrolle hinzufügen. Sie sind für Search & Restore erforderlich.
- Azure-Anforderungen:
  - Sie müssen den Azure Synapse Analytics Resource Provider (genannt „Microsoft.Synapse“) im Abonnement registrieren. "Erfahren Sie, wie Sie diesen Ressourcenanbieter für Ihr Abonnement registrieren". Sie müssen der Subscription **Owner** oder **Contributor** sein, um den Ressourcenanbieter zu registrieren.
  - Spezifische Berechtigungen für Azure Synapse Workspace- und Data Lake-Speicherkonto müssen der Benutzerrolle hinzugefügt werden, die BlueXP mit Berechtigungen versorgt. "Stellen Sie sicher, dass alle Berechtigungen korrekt konfiguriert sind".

    Wenn Sie bereits BlueXP Backup und Recovery mit einem Connector genutzt haben, den Sie in der Vergangenheit konfiguriert haben, müssen Sie der BlueXP Benutzerrolle jetzt die Berechtigungen für Azure Synapse Workspace und Data Lake Storage Account hinzufügen. Sie sind für Search & Restore erforderlich.
  - Der Connector muss **ohne** einen Proxy-Server für die HTTP-Kommunikation mit dem Internet konfiguriert werden. Wenn Sie einen HTTP-Proxyserver für Ihren Connector konfiguriert haben, können Sie die Such- und Wiederherstellungsfunktion nicht verwenden.
- Google Cloud-Anforderungen:
  - Spezifische Google BigQuery-Berechtigungen müssen der Benutzerrolle hinzugefügt werden, die

BlueXP Berechtigungen bereitstellt. "Stellen Sie sicher, dass alle Berechtigungen korrekt konfiguriert sind".

Wenn Sie bereits BlueXP Backup und Recovery mit einem Connector genutzt haben, den Sie in der Vergangenheit konfiguriert haben, müssen Sie jetzt die BigQuery-Berechtigungen zur BlueXP Benutzerrolle hinzufügen. Sie sind für Search & Restore erforderlich.

- StorageGRID- und ONTAP S3-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.

    Informationen zum indizierten Katalog v2 finden Sie im folgenden Abschnitt zum Aktivieren des indizierten Katalogs.

  - Wenn Sie einen Connector auf einer privaten (dunklen) Site verwenden, werden die indizierten Kataloginformationen auf dem Connector gespeichert (erfordert Connector Version 3.9.25 oder höher).
  - 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.

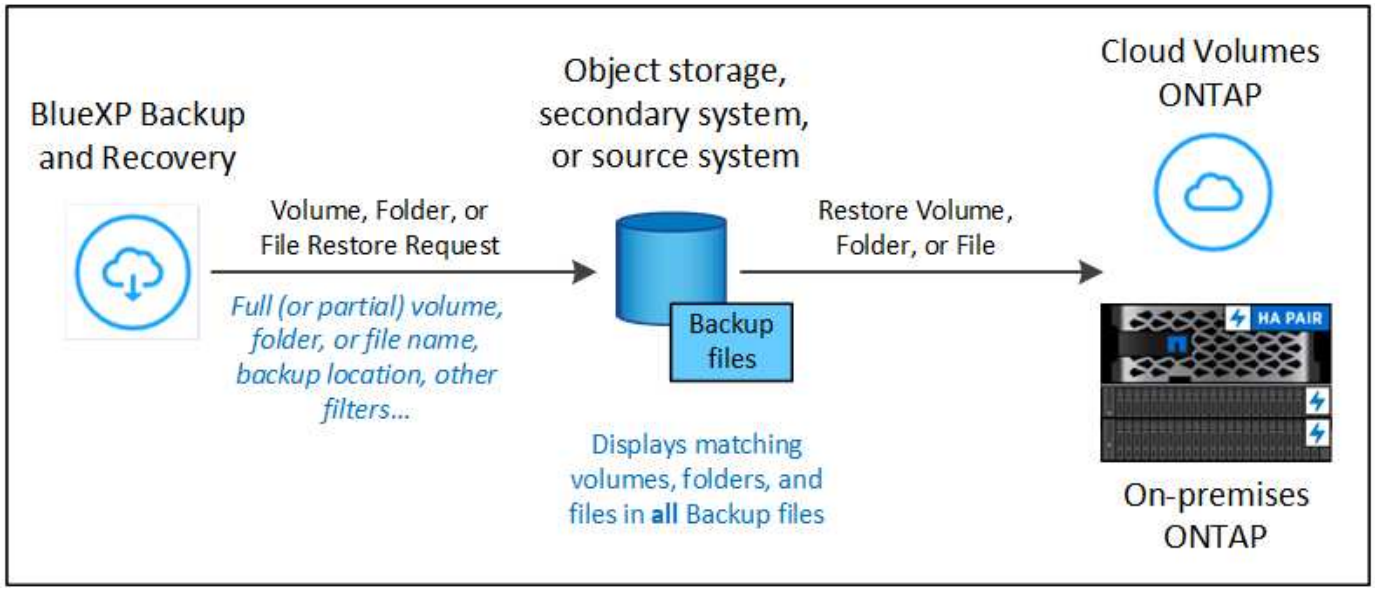
Such- und Wiederherstellungsvorgang

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 teilweisen oder vollständigen Datenträgernamen, einem teilweisen oder vollständigen Dateinamen, einem Sicherungsverzeichnis, einem Größenbereich, einem Erstellungsdatumbereich, anderen Suchfiltern ein. Und klicken Sie auf **Suche**.

   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, müssen Sie wirklich nur einen Teil des Namens kennen und BlueXP Backup- und Recovery-Suchen in allen Backup-Dateien durchführen, die Ihrer Suche entsprechen.

Aktivieren Sie den indizierten Katalog 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.

Der indizierte Katalog ist eine Datenbank, in der Metadaten zu allen Volumes und Backup-Dateien in Ihrer Arbeitsumgebung gespeichert werden. Es wird von der Such- und Wiederherstellungsfunktion verwendet, um schnell die Sicherungsdateien zu finden, die die wiederherzustellenden Daten enthalten.

Merkmale des indizierten Katalogs v2

Der im Februar 2025 veröffentlichte und im Juni 2025 aktualisierte Indexed Catalog v2 enthält Funktionen, die ihn effizienter und benutzerfreundlicher machen. Diese Version hat eine erhebliche Leistungssteigerung und ist standardmäßig für alle neuen Kunden aktiviert.

Lesen Sie die folgenden Überlegungen zu v2:

- Der indizierte Katalog v2 ist im Vorschaumodus verfügbar.
- Wenn Sie bereits Kunde sind und den Catalog v2 verwenden möchten, müssen Sie Ihre Umgebung vollständig neu indizieren.
- Der Catalog v2 indiziert nur die Snapshots, die eine Snapshot-Beschriftung haben.
- BlueXP Backup und Recovery indexiert Snapshots nicht mit „stündlichen“ SnapMirror-Etiketten. Wenn Sie Schnappschüsse mit dem „stündlichen“ SnapMirror-Label indexieren möchten, müssen Sie es manuell aktivieren, während sich der v2 im Vorschaumodus befindet.
- BlueXP Backup und Recovery indiziert Volumes und Snapshots, die mit Arbeitsumgebungen verbunden sind, die durch BlueXP Backup und Recovery geschützt sind, nur mit dem Katalog v2. Andere auf der BlueXP -Plattform erkannte Arbeitsumgebungen werden nicht indiziert.
- Die Datenindizierung mit Catalog v2 erfolgt in lokalen Umgebungen sowie in Amazon Web Services-, Microsoft Azure- und Google Cloud Platform (GCP)-Umgebungen.

Der indizierte Katalog v2 unterstützt Folgendes:

- Globale Sucheffizienz in weniger als 3 Minuten
- Bis zu 5 Milliarden Dateien
- Bis zu 5000 Volumes pro Cluster
- Bis zu 100.000 Snapshots pro Volume
- Die maximale Zeit für die Indizierung der Basislinie beträgt weniger als 7 Tage. Die tatsächliche Zeit variiert je nach Umgebung.

Aktivieren des indizierten Katalogs für eine Arbeitsumgebung

Der Dienst stellt keinen separaten Bucket bereit, wenn Sie den Indexed Catalog v2 verwenden. Stattdessen stellt der Dienst für Backups, die in AWS, Azure, Google Cloud Platform, StorageGRID oder ONTAP S3 gespeichert sind, Speicherplatz auf dem Connector oder in der Umgebung des Cloud-Anbieters bereit.

Wenn Sie den indizierten Katalog vor der Version 2 aktiviert haben, geschieht Folgendes mit Arbeitsumgebungen:

- 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 Azure gespeichert sind, stellt sie einen Azure Synapse Workspace und ein Data Lake Dateisystem als Container bereit, in dem die Workspace-Daten gespeichert werden.
- Für Backups, die in Google Cloud gespeichert sind, stellt die IT einen neuen Bucket bereit und "Google Cloud BigQuery Services" Werden auf Konto-/Projektebene bereitgestellt.
- Für in StorageGRID oder ONTAP S3 gespeicherte Backups stellt er Speicherplatz auf dem Connector oder in der Cloud-Provider-Umgebung bereit.

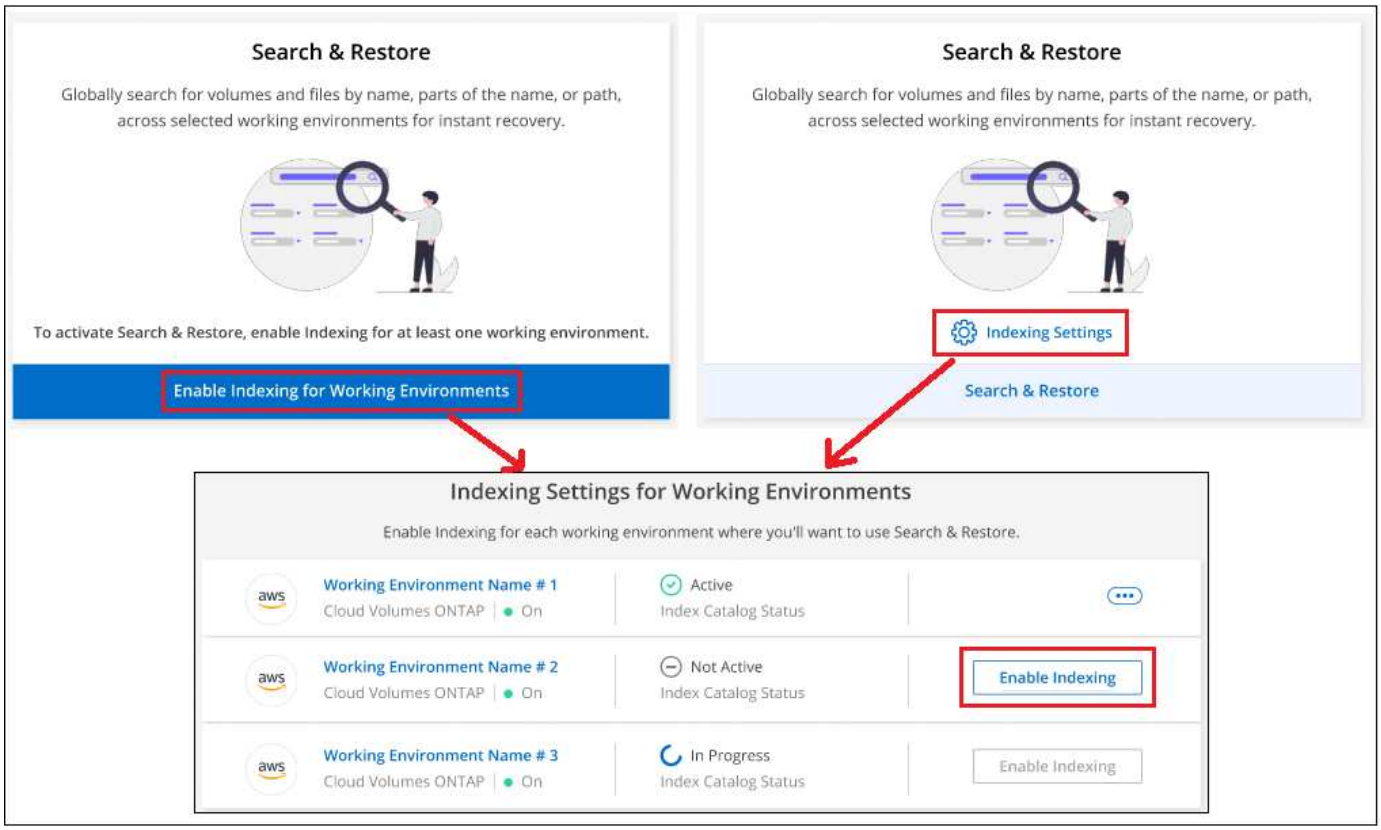
Wenn die Indexierung bereits für Ihre Arbeitsumgebung aktiviert wurde, rufen Sie den nächsten Abschnitt auf, um Ihre Daten wiederherzustellen.

Schritte zum Aktivieren der Indizierung für eine Arbeitsumgebung:

1. Führen Sie einen der folgenden Schritte aus:
    - Wenn keine Arbeitsumgebungen indiziert wurden, wählen Sie im Restore Dashboard unter *Search & Restore* **Enable Indexing for working Environments** aus.
    - Wenn mindestens eine Arbeitsumgebung bereits indiziert wurde, klicken Sie im Restore Dashboard unter *Suchen & Wiederherstellen* auf **Indexierungseinstellungen**.
2. Wählen Sie **Indizierung aktivieren** für die Arbeitsumgebung aus.

Ergebnis

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



Abhängig von der Größe der Volumes in der Arbeitsumgebung und der Anzahl der Backup-Dateien an allen 3 Backup-Standorten kann die anfängliche Indizierung bis zu einer Stunde dauern. Danach wird es stündlich transparent mit inkrementellen Änderungen aktualisiert, um auf dem Laufenden zu bleiben.

Stellen Sie Volumes, Ordner und Dateien mithilfe von Search & Restore wieder her

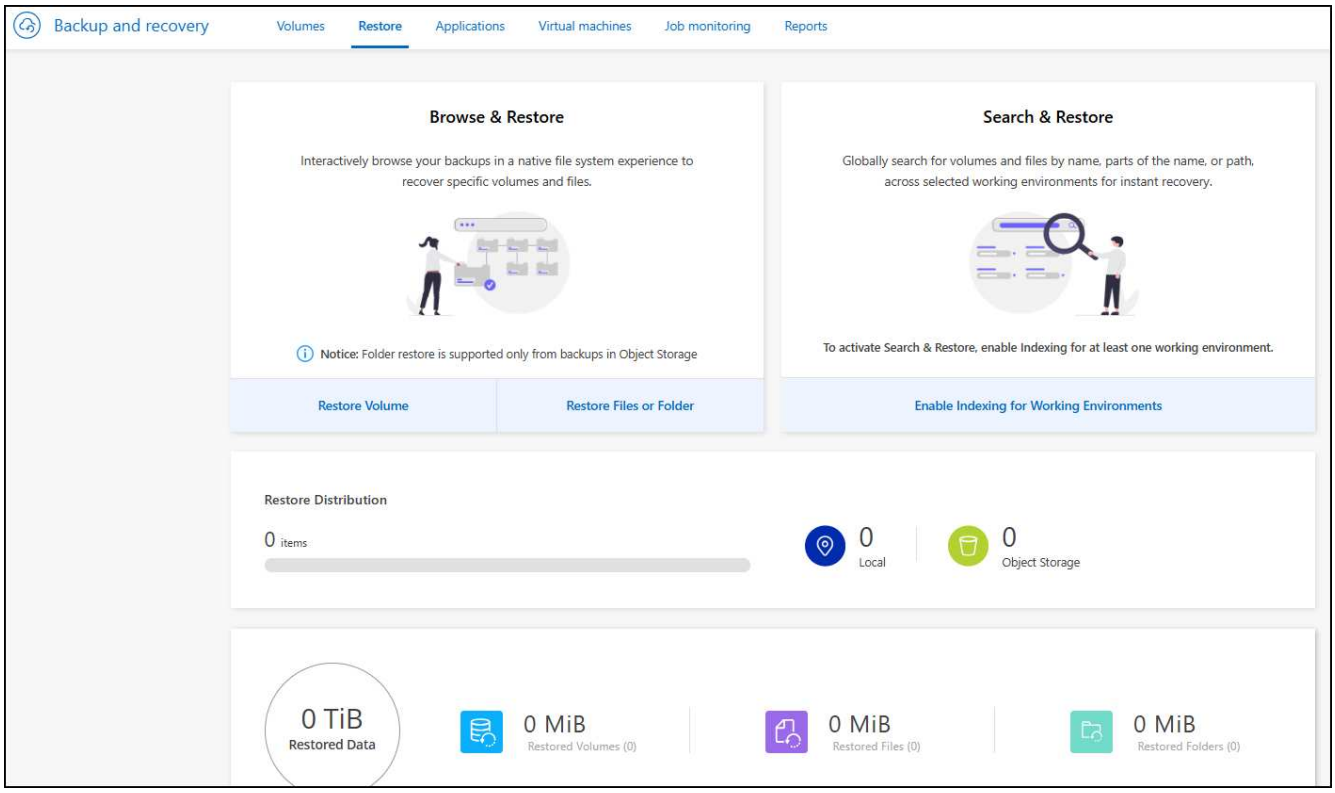
Nachdem Sie den haben Indexierung für Ihre Arbeitsumgebung aktiviert, Sie können Volumes, Ordner und Dateien mit Search & Restore wiederherstellen. So können Sie mithilfe verschiedener Filter genau die Datei oder das Volume finden, die Sie aus allen Backup-Dateien wiederherstellen möchten.

Schritte

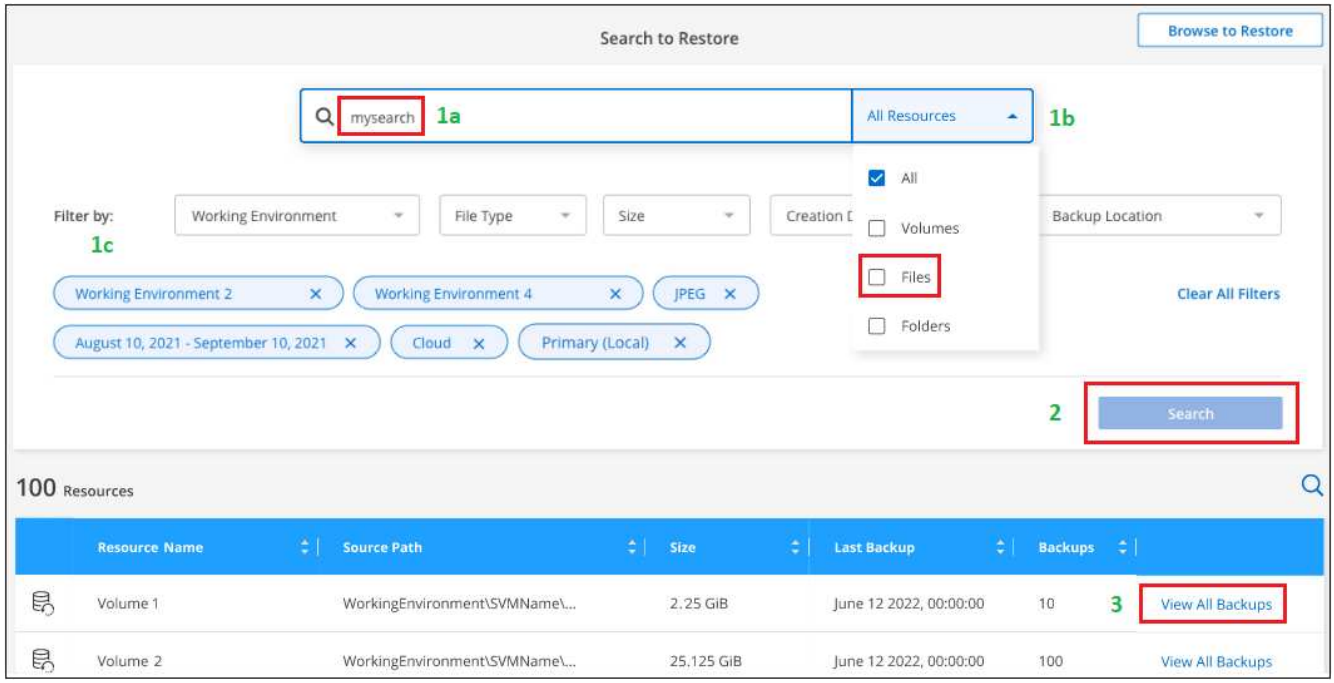
1. Wählen Sie im Menü BlueXP die Option **Schutz > Sicherung und Wiederherstellung**.
2. Klicken Sie auf die Registerkarte **Wiederherstellen**.

   Das Wiederherstellungs-Dashboard wird angezeigt.

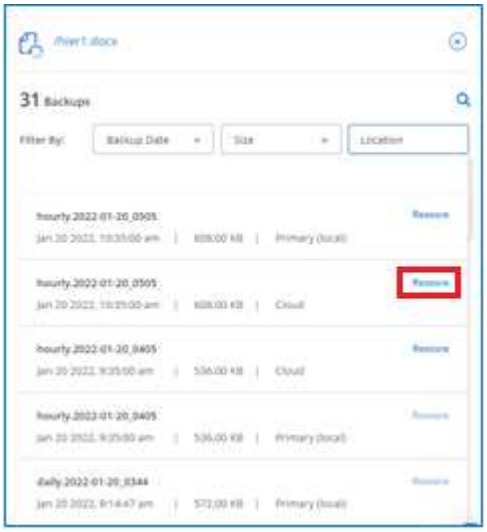
3. Wählen Sie im Abschnitt *Suchen und Wiederherstellen* die Option **Suchen und Wiederherstellen** aus.



4. Auf der Seite „Suchen und Wiederherstellen“:
   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. Sie können auch den Typ des Backup-Speicherorts auswählen, wenn Sie nur innerhalb der verfügbaren Snapshot-Kopien oder Backup-Dateien im Objektspeicher nach Ergebnissen suchen möchten.
5. Wählen Sie **Suchen** und im Bereich „Suchergebnisse“ werden alle Ressourcen angezeigt, die über eine Datei, einen Ordner oder ein Volume verfügen, das Ihrer Suche entspricht.



6. Suchen Sie die Ressource mit den Daten, die Sie wiederherstellen möchten, und wählen Sie **Alle Sicherungen anzeigen** aus, um alle Sicherungsdateien anzuzeigen, die das entsprechende Volume, den entsprechenden Ordner oder die entsprechende Datei enthalten.



7. Suchen Sie die Sicherungsdatei, die Sie zum Wiederherstellen der Daten verwenden möchten, und wählen Sie **Wiederherstellen**.

   Die Ergebnisse identifizieren lokale Snapshot-Kopien des Volumes und replizierte Remote-Volumes, die die Datei in Ihrer Suche enthalten. Sie können zwischen der Backup-Datei in der Cloud, der Snapshot Kopie oder dem replizierten Volume auswählen.

8. Wählen Sie den Zielspeicherort aus, an dem das Volume, der Ordner oder die Datei(en) wiederhergestellt werden sollen, und wählen Sie **Wiederherstellen**.
   - Für Volumes können Sie die ursprüngliche Ziel-Arbeitsumgebung auswählen oder eine andere Arbeitsumgebung auswählen. Bei der Wiederherstellung eines FlexGroup Volumes müssen Sie mehrere Aggregate 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".
    - Wählen Sie beim Wiederherstellen aus Azure Blob den IPspace im ONTAP Cluster aus, an dem sich das Ziel-Volume befindet, und wählen Sie optional einen privaten Endpunkt für den sicheren Datentransfer aus, indem Sie vnet und Subnetz auswählen. "Siehe Details zu diesen Anforderungen".
    - Wählen Sie bei der Wiederherstellung aus Google Cloud Storage den IP-Speicherplatz im ONTAP-Cluster aus, auf dem sich das Ziel-Volume befinden soll, und den Zugriffsschlüssel und den geheimen Schlüssel für den Zugriff auf den Objekt-Storage. "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".
    - Geben Sie beim Wiederherstellen aus ONTAP S3 den FQDN des ONTAP S3-Servers und den Port ein, den ONTAP für die HTTPS-Kommunikation mit ONTAP S3 verwenden soll, wählen Sie den Zugriffsschlüssel und den geheimen Schlüssel aus, die für den Zugriff auf den Objektspeicher erforderlich sind. und den IPspace im ONTAP Cluster, wo sich das Ziel-Volume befinden soll. "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 die Registerkarte **Jobüberwachung** auswählen, um den Wiederherstellungsfortschritt anzuzeigen.

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