# Dokumentation für Cloud-Backup

## Cloud Backup

NetApp
December 06, 2022

This PDF was generated from https://docs.netapp.com/de-de/cloud-manager-backup-restore/gcp/index.html on December 06, 2022. Always check docs.netapp.com for the latest.

# Inhaltsverzeichnis


Dokumentation für Cloud-Backup . . . 1
Was ist neu bei Cloud Backup . . . 2
Bis 6. Dezember 2022 . . . 2
November 2022 . . . 2
28. September 2022 . . . 4
19. September 2022 . . . 4
18. August 2022 . . . 5
13 Juli 2022 . . . 6
14. Juni 2022 . . . 7
Mai 2022 . . . 8
4. April 2022 . . . 9
3 März 2022 . . . 9
14 Februar 2022 . . . 10
Januar 2022 . . . 10
28. November 2021 . . . 11
5. November 2021 . . . 11
Oktober 4 2021 . . . 11
Los geht’s . . . 13
Weitere Informationen zu Cloud Backup . . . 13
Lizenzierung für Cloud Backup einrichten . . . 15
Überwachen des Status von Backup- und Restore-Jobs . . . 20
Backup und Restore von ONTAP Daten . . . 23
ONTAP-Cluster-Daten mit Cloud Backup schützen . . . 23
Sichern von Cloud Volumes ONTAP Daten auf Google Cloud Storage – . . . 31
Sichern von lokalen ONTAP-Daten auf Google Cloud Storage . . . 38
Sichern von lokalen ONTAP Daten in StorageGRID . . . 48
Verwalten von Backups für Ihre ONTAP Systeme . . . 57
Verwalten von Backup-Einstellungen auf Cluster-Ebene . . . 76
Wiederherstellen von ONTAP Daten aus Backup-Dateien . . . 81
Backup und Wiederherstellung von Kubernetes-Daten . . . 101
Kubernetes-Cluster-Daten mit Cloud Backup schützen . . . 101
Sichern Sie persistente Kubernetes-Volume-Daten auf Google Cloud Storage . . . 105
Das Backup-Management für Kubernetes-Systeme . . . 110
Wiederherstellung von Kubernetes-Daten aus Backup-Dateien . . . 121
Backup und Restore von Applikationsdaten . . . 124
Backup und Restore von On-Premises-Applikationsdaten . . . 124
Backup und Restore von Cloud-nativen Applikationsdaten . . . 137
Daten von Virtual Machines sichern und wiederherstellen . . . 150
Sichern Sie Ihre Daten von Virtual Machines . . . 150
Registrieren Sie das SnapCenter Plug-in für VMware vSphere . . . 151
Erstellen einer Richtlinie zum Backup von Virtual Machines . . . 152
Sichern Sie Datenspeicher in StorageGRID . . . 152
Management der Sicherung von Virtual Machines . . . 153

Wiederherstellung von Virtual Machines aus der Cloud . . . 155
Cloud-Backup-APIs . . . 156
Erste Schritte . . . 156
Beispiel mit den APIs . . . 158
API-Referenz . . . 160
Referenz . . . 162
Konfigurationseinstellungen für Cloud-Backup-Richtlinien . . . 162
AWS S3-Archiv-Storage-Klassen und Restore Abrufzeiten . . . 167
Azure-Archivierungsebenen und Wiederherstellungszeiten . . . 168
Google Archivspeicherklassen und Abrufzeiten wiederherstellen . . . 169
Backup für Multi-Account-Zugriff in Azure konfigurieren . . . 170
Wissen und Support . . . 178
Für den Support anmelden . . . 178
Holen Sie sich Hilfe . . . 182
Rechtliche Hinweise . . . 186
Urheberrecht . . . 186
Marken . . . 186
Patente . . . 186
Datenschutzrichtlinie . . . 186
Open Source . . . 186

# Dokumentation für Cloud-Backup

# Was ist neu bei Cloud Backup

Alles zum Thema Cloud Backup:

## Bis 6. Dezember 2022

### Support der Google Archivspeicher

Sicherungsdateien werden zunächst in der Speicherklasse Google Standard erstellt. Jetzt können Sie ältere Backups nach einer bestimmten Anzahl von Tagen auf Google Archivspeicher verschieben, um die Kosten weiter zu optimieren.

Diese Funktion wird derzeit für ONTAP-Cluster vor Ort mit ONTAP 9.12.1 oder höher unterstützt. Dieses Angebot ist derzeit nicht für Cloud Volumes ONTAP Systeme verfügbar.

### Unterstützung für FlexGroup Volumes

Cloud Backup unterstützt jetzt FlexGroup Volumes. Bei Verwendung von ONTAP 9.12.1 oder neuer können Sie FlexGroup Volumes in Public- und Private-Cloud-Storage sichern. Wenn Sie über funktionierende Umgebungen mit FlexVol- und FlexGroup-Volumes verfügen, können Sie nach der Aktualisierung der ONTAP Software jedes der FlexGroup-Volumes auf diesen Systemen sichern.

"Die vollständige Liste der unterstützten Volume-Typen finden Sie unter".

### Möglichkeit zur Wiederherstellung von Daten aus Backups in einem bestimmten Aggregat auf Cloud Volumes ONTAP Systemen

In älteren Versionen könnten Sie das Aggregat nur auswählen, wenn Sie Daten in On-Premises-ONTAP-Systemen wiederherstellen. Diese Funktion ist jetzt auch für die Wiederherstellung von Daten auf Cloud Volumes ONTAP Systemen geeignet.

## November 2022

### Möglichkeit, ältere Snapshot Kopien in die Basis-Backup-Dateien zu exportieren

Wenn es lokale Snapshot-Kopien für Volumes in Ihrer Arbeitsumgebung gibt, die Ihren Backup-Schedule-Etiketten (z. B. täglich, wöchentlich usw.) entsprechen, können Sie diese historischen Snapshots als Backup-Dateien in den Objekt-Storage exportieren. Damit können Sie Ihre Backups in die Cloud initialisieren, indem Sie ältere Snapshot-Kopien in die Basis-Backup-Kopie verschieben.

Diese Option ist bei der Aktivierung von Cloud Backup für Ihre Arbeitsumgebungen verfügbar. Sie können diese Einstellung auch später im ändern "Seite „Erweiterte Einstellungen“".

### Cloud Backup kann nun für die Archivierung von Volumes verwendet werden, die Sie nicht mehr auf dem Quellsystem benötigen

Nun können Sie die Backup-Beziehung für ein Volume löschen. Auf diese Weise erhalten Sie einen Archivierungsmechanismus, wenn Sie die Erstellung neuer Backup-Dateien beenden und das Quell-Volume löschen möchten, aber alle vorhandenen 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. "Erfahren Sie, wie".

## Unterstützung wurde hinzugefügt, um Cloud Backup-Benachrichtigungen per E-Mail und im Notification Center zu erhalten

Cloud Backup wurde in den BlueXP Notification Service integriert. Sie können Cloud-Backup-Benachrichtigungen anzeigen, indem Sie in der Menüleiste von BlueXP auf die Benachrichtigungsglocke klicken. Sie können BlueXP auch so konfigurieren, dass Benachrichtigungen per E-Mail als Benachrichtigungen gesendet werden, damit Sie auch dann über wichtige Systemaktivitäten informiert werden können, wenn Sie nicht im System angemeldet sind. Die E-Mail kann an alle Empfänger gesendet werden, die auf Backup- und Wiederherstellungsaktivitäten achten müssen. "Erfahren Sie, wie".

## Mit der neuen Seite „Erweiterte Einstellungen“ können Sie Backup-Einstellungen auf Cluster-Ebene ändern

Auf dieser neuen Seite können Sie viele Backup-Einstellungen auf Cluster-Ebene ändern, die Sie bei der Aktivierung von Cloud Backup für jedes ONTAP System festgelegt haben. Sie können auch einige Einstellungen ändern, die als „Standard“-Backup-Einstellungen angewendet werden. Die vollständigen Backup-Einstellungen, die Sie ändern können, umfassen:

- Die Storage-Schlüssel, die Ihrem ONTAP System Zugriff auf Objekt-Storage gewähren
- Die Netzwerkbandbreite, die dem Hochladen von Backups in den Objektspeicher zugewiesen ist
- Die automatische Backup-Einstellung (und -Richtlinie) für zukünftige Volumes
- Die Archiv-Storage-Klasse (nur AWS)
- Gibt an, ob historische Snapshot-Kopien in den ersten Basis-Backup-Dateien enthalten sind
- Gibt an, ob „jährliche“ Snapshots aus dem Quellsystem entfernt werden
- ONTAP-IPspace, der mit dem Objekt-Storage verbunden ist (bei falscher Auswahl während der Aktivierung)

"Weitere Informationen zum Managen von Backup-Einstellungen auf Cluster-Ebene".

## Sie können jetzt Backup-Dateien mithilfe von Search & Restore wiederherstellen, wenn Sie einen On-Premises Connector verwenden

In der vorherigen Version wurde beim Einsatz des Connectors in Ihrer Umgebung Unterstützung beim Erstellen von Backup-Dateien in der Public Cloud erhalten. In dieser Version wurde mithilfe von Search & Restore weiterhin Unterstützung für die Wiederherstellung von Backups von Amazon S3 oder Azure Blob ermöglicht, wenn der Connector in Ihrer lokalen Umgebung implementiert wird. Search & Restore unterstützt jetzt auch die Wiederherstellung von Backups aus StorageGRID Systemen in ONTAP Systemen vor Ort.

Derzeit muss der Connector in der Google Cloud Platform bereitgestellt werden, wenn Sie Search & Restore verwenden, um Backups von Google Cloud Storage wiederherzustellen.

## Die Seite Job-Überwachung wurde aktualisiert

Die folgenden Aktualisierungen wurden an der vorgenommen "Seite Job-Überwachung":

- Es steht eine Spalte für „Workload“ zur Verfügung, damit Sie die Seite filtern können, um Jobs für die folgenden Backup-Services anzuzeigen: Volumes, Applikationen, Virtual Machines und Kubernetes.
- Sie können neue Spalten für „Benutzername“ und „Jobtyp“ hinzufügen, wenn Sie diese Details für einen bestimmten Backup-Job anzeigen möchten.
- Auf der Seite Jobdetails werden alle untergeordneten Jobs angezeigt, die ausgeführt werden, um den

Hauptjob abzuschließen.

- Die Seite wird automatisch alle 15 Minuten aktualisiert, so dass Sie immer die aktuellsten Ergebnisse des Jobstatus sehen. Und Sie können auf die Schaltfläche **Aktualisieren** klicken, um die Seite sofort zu aktualisieren.

### Kontoübergreifende Backup-Verbesserungen für AWS

Wenn Sie ein anderes AWS Konto für Ihre Cloud Volumes ONTAP-Backups verwenden möchten als für die Quell-Volumes, müssen Sie die Zielanmeldeinformationen für AWS-Konto in BlueXP hinzufügen, und Sie müssen die Berechtigungen "s3:PutBucketPolicy" und "s3:PutBucketEigentümershipControls" zur IAM-Rolle hinzufügen, die BlueXP mit Berechtigungen versorgt. In der Vergangenheit mussten Sie zahlreiche Einstellungen in der AWS Console konfigurieren – dieser Wunsch brauchen Sie nicht mehr.

## 28. September 2022

### Erweiterungen für Cloud Backup für Applikationen

- Unterstützt Google Cloud Platform (GCP) und StorageGRID, um applikationskonsistente Snapshots zu erstellen
- Erstellen benutzerdefinierter Richtlinien
- Unterstützung von Archiv-Storage
- SAP HANA-Applikationen sichern
- Sichern Sie Oracle und SQL Applikationen auf VMware Umgebungen
- Backup von Applikationen aus lokalem Sekundär-Storage
- Backups deaktivieren
- SnapCenter-Server nicht registrieren

### Verbesserungen bei Cloud Backup für Virtual Machines

- Unterstützt StorageGRID für das Backup von einem oder mehreren Datastores
- Erstellen benutzerdefinierter Richtlinien

## 19. September 2022

### DataLock und Ransomware-Schutz können für Backup-Dateien in StorageGRID Systemen konfiguriert werden

In der letzten Version wurden *DataLock und Ransomware Protection* für Backups eingeführt, die in Amazon S3 Buckets gespeichert sind. Diese Version erweitert den Support für Backup-Dateien, die in StorageGRID Systemen gespeichert sind. Wenn Ihr Cluster ONTAP 9.11.1 oder höher verwendet und auf Ihrem StorageGRID System Version 11.6.0.3 oder höher ausgeführt wird, ist diese neue Backup-Policy-Option verfügbar. "Erfahren Sie mehr darüber, wie Sie mit DataLock- und Ransomware-Schutz Ihre Backups schützen können".

Beachten Sie, dass Sie einen Connector mit Version 3.9.22 oder neuer verwenden müssen. Der Connector muss in Ihrem Haus installiert werden und kann auf einer Website mit oder ohne Internetzugang installiert werden.

### Die Wiederherstellung auf Ordnerebene ist jetzt über Ihre Sicherungsdateien verfügbar

Jetzt können Sie einen Ordner aus einer Sicherungsdatei wiederherstellen, wenn Sie Zugriff auf alle Dateien in diesem Ordner benötigen (Verzeichnis oder Freigabe). Das Wiederherstellen eines Ordners ist wesentlich effizienter als das Wiederherstellen eines gesamten Volumes. Diese Funktion steht für Wiederherstellungsvorgänge mit der Methode „Durchsuchen und Wiederherstellen“ und der Methode „Suchen und Wiederherstellen“ bei Verwendung von ONTAP 9.11.1 oder höher zur Verfügung. Zu diesem Zeitpunkt können Sie nur einen einzigen Ordner auswählen und wiederherstellen, und nur Dateien aus diesem Ordner werden wiederhergestellt - keine Unterordner oder Dateien in Unterordnern, wiederhergestellt.

### Restores auf Dateiebene stehen nun für Backups zur Verfügung, die in Archiv-Storage verschoben wurden

Früher war es möglich, Volumes nur von Backup-Dateien wiederherzustellen, die in Archiv-Storage verschoben wurden (nur AWS und Azure). Sie können nun einzelne Dateien aus diesen archivierten Backup-Dateien wiederherstellen. Diese Funktion steht für Wiederherstellungsvorgänge mit der Methode „Durchsuchen und Wiederherstellen“ und der Methode „Suchen und Wiederherstellen“ bei Verwendung von ONTAP 9.11.1 oder höher zur Verfügung.

### Wiederherstellung auf Dateiebene bietet jetzt die Möglichkeit, die ursprüngliche Quelldatei zu überschreiben

In der Vergangenheit wurde eine auf das ursprüngliche Volume wiederhergestellte Datei immer als neue Datei mit dem Präfix "Restore_<file_Name>" wiederhergestellt. Nun können Sie die ursprüngliche Quelldatei überschreiben, wenn Sie die Datei an den ursprünglichen Speicherort auf dem Volume wiederherstellen. Diese Funktion steht für Wiederherstellungsvorgänge sowohl mit der Methode Durchsuchen und Wiederherstellen als auch mit der Methode Suchen und Wiederherstellen zur Verfügung.

### Per Drag-and-Drop können Sie Cloud-Backups in StorageGRID-Systemen aktivieren

Wenn der "StorageGRID" Ziel für Ihre Backups ist als Arbeitsumgebung auf dem Canvas vorhanden, Sie können Ihre On-Prem ONTAP Arbeitsumgebung auf das Ziel ziehen, um den Cloud Backup-Setup-Assistenten zu starten.

## 18. August 2022

### Der Schutz von Cloud-nativen Applikationsdaten wurde durch zusätzliche Unterstützung hinzugefügt

Cloud Backup für Applikationen ist ein SaaS-basierter Service mit Datensicherungsfunktionen für Applikationen, die auf NetApp Cloud Storage ausgeführt werden. Cloud Backup für Applikationen in BlueXP ermöglicht effizientes, applikationskonsistentes, richtlinienbasiertes Backup und Restore von Oracle Datenbanken in Amazon FSX für NetApp ONTAP.https://docs.netapp.com/us-en/cloud-manager-backup-restore/concept-protect-cloud-app-data-to-cloud.html["Weitere Informationen ."^].

### Die Suche & Wiederherstellung wird jetzt auch für Backup-Dateien in Azure Blob unterstützt

Die Suchmethode zur Wiederherstellung von Volumes und Dateien steht jetzt für Benutzer zur Verfügung, die ihre Backup-Dateien in Azure Blob Storage speichern. "Erfahren Sie, wie Sie Ihre Volumes und Dateien

mithilfe von Search Restore wiederherstellen wiederherstellen wiederherstellen wiederherstellen".

Beachten Sie, dass in der Rolle Connector zusätzliche Berechtigungen erforderlich sind, um diese Funktion nutzen zu können. Ein Connector, der mit Software der Version 3.9.21 (August 2022) bereitgestellt wird, umfasst diese Berechtigungen. Wenn Sie den Connector mit einer früheren Version bereitgestellt haben, müssen Sie die Berechtigungen manuell hinzufügen. "Lesen Sie, wie Sie diese Berechtigungen hinzufügen, falls erforderlich".

### Wir haben die Möglichkeit hinzugefügt, Ihre Backup-Dateien vor Löschungen und Ransomware-Angriffen zu schützen

Cloud Backup unterstützt jetzt Objekt-Lock-Support für Ransomware-sichere Backups. Wenn Ihr Cluster ONTAP 9.11.1 oder höher verwendet und Ihr Backup-Ziel Amazon S3 ist, steht jetzt eine neue Backup-Policy-Option namens *DataLock und Ransomware Protection* zur Verfügung. DataLock schützt Ihre Backup-Dateien vor Änderungen oder Löschung. Ransomware-Schutz scannt Ihre Backup-Dateien, um nach einem Ransomware-Angriff auf Ihre Backup-Dateien zu suchen. "Erfahren Sie mehr darüber, wie Sie mit DataLock- und Ransomware-Schutz Ihre Backups schützen können".

Beachten Sie, dass in der Rolle Connector zusätzliche Berechtigungen erforderlich sind, um diese Funktion nutzen zu können. Ein Connector, der mit der Software Version 3.9.21 bereitgestellt wird, enthält diese Berechtigungen. Wenn Sie den Connector mit einer früheren Version bereitgestellt haben, müssen Sie die Berechtigungen manuell hinzufügen. "Lesen Sie, wie Sie diese Berechtigungen hinzufügen, falls erforderlich".

### Cloud Backup unterstützt jetzt Richtlinien, die mithilfe benutzerdefinierter SnapMirror Labels erstellt werden

Zuvor unterstützte Cloud Backup nur vordefinierte SnapMirror Labels wie stündlich, täglich, wöchentlich, stündlich oder jährlich. Jetzt kann Cloud Backup SnapMirror Richtlinien erkennen, die über individuelle SnapMirror-Labels verfügen, die Sie mit System Manager oder der CLI erstellt haben. Diese neuen Bezeichnungen werden der Cloud Backup-UI ausgesetzt. Damit können Sie Volumes mit dem SnapMirror Label Ihrer Wahl in der Cloud sichern.

### Zusätzliche Verbesserung der Backup-Richtlinien für ONTAP Systeme

Einige Seiten der Backup-Richtlinien wurden neu gestaltet, um alle für Volumes in jedem ONTAP Cluster verfügbaren Backup-Richtlinien einfacher anzuzeigen. Dadurch sind die Details der verfügbaren Richtlinien einfacher abrufbar, damit Sie die besten Richtlinien auf Ihren Volumes anwenden können.

### Aktivieren Sie Cloud Backup per Drag-and-Drop in Azure Blob und Google Cloud Storage

Wenn der "Azure Blob" Oder "Google Cloud Storage" Ziel für Ihre Backups ist als Arbeitsumgebung auf dem Canvas vorhanden. Sie können Ihre On-Prem ONTAP oder Cloud Volumes ONTAP Arbeitsumgebung (installiert in Azure oder GCP) auf das Ziel ziehen, um den Backup-Setup-Assistenten zu starten.

Für Amazon S3 Buckets ist diese Funktion bereits vorhanden.

## 13 Juli 2022

### SnapLock Enterprise Volumes werden jetzt zusätzlich unterstützt

Mit Cloud Backup lassen sich jetzt SnapLock Enterprise Volumes in Public und Private Clouds sichern. Für diese Funktion muss auf Ihrem ONTAP System ONTAP 9.11.1 oder höher ausgeführt werden. SnapLock-

Compliance-Volumes werden derzeit jedoch nicht unterstützt.

### Bei Verwendung eines On-Premises-Connectors können Sie jetzt Backup-Dateien in der Public Cloud erstellen

Früher mussten Sie den Connector im selben Cloud-Provider implementieren, als wo Sie Backup-Dateien erstellt haben. Mit einem Connector, der in Ihrem Standort implementiert ist, können Sie jetzt Backup-Dateien von On-Premises-ONTAP-Systemen über Amazon S3, Azure Blob und Google Cloud Storage erstellen. (Bei der Erstellung von Sicherungsdateien auf StorageGRID Systemen war immer ein On-Prem-Connector erforderlich.)

### Wenn Backup-Richtlinien für ONTAP Systeme erstellt werden, sind zusätzliche Funktionen verfügbar

- Das Backup steht nun gemäß jährlicher Planung zur Verfügung. Der Standardwert für die Aufbewahrung ist 1 für jährliche Backups. Sie können diesen Wert jedoch ändern, wenn Sie auf die Backup-Dateien vieler Jahre zugreifen möchten.
- Sie können Ihre Backup-Richtlinien benennen, damit Sie Ihre Richtlinien mit beschreibenden Text identifizieren können.

## 14. Juni 2022

### Es wurde Unterstützung für das Backup von On-Premises-ONTAP-Cluster-Daten an Standorten ohne Internetzugang hinzugefügt

Wenn Ihr ONTAP-Cluster vor Ort an einem Standort ohne Internetzugang – auch als „Dark Site“ oder „Offline“ bezeichnet – gespeichert ist, können Sie mit Cloud Backup Volumes-Daten auf einem NetApp StorageGRID-System am selben Standort sichern. Für diese Funktionalität muss auch der BlueXP Connector (Version 3.9.19 oder höher) auf der Offline-Website bereitgestellt werden.

"Lesen Sie, wie Sie den Connector in Ihrer Offline-Website installieren".https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-backup-onprem-private-cloud.html["Erfahren Sie, wie Sie ONTAP Daten in StorageGRID auf Ihrer Offline-Website sichern"].

### Cloud Backup für Virtual Machines 1.1.0 ist jetzt allgemein verfügbar

Durch die Integration des SnapCenter Plug-ins für VMware vSphere in BlueXP können Sie Daten auf Ihren virtuellen Maschinen schützen. Sie können Datastores in der Cloud sichern und Virtual Machines problemlos im lokalen SnapCenter Plug-in für VMware vSphere wiederherstellen.

"Erfahren Sie mehr über die Sicherung von Virtual Machines in der Cloud".

### Für die ONTAP Browse & Restore-Funktion ist keine Cloud Restore-Instanz erforderlich

Für Suchvorgänge und Restores auf Dateiebene von S3 und Blob-Storage wurde eine separate Cloud Restore-Instanz/Virtual Machine benötigt. Diese Instanz wurde heruntergefahren, wenn sie nicht verwendet wird — aber es hat immer noch Zeit und Kosten für die Wiederherstellung von Dateien hinzugefügt. Diese Funktion wurde durch einen kostenfrei bereitgestellten Container ersetzt, der bei Bedarf auf dem Connector bereitgestellt wird. Es bietet folgende Vorteile:

- Keine zusätzlichen Kosten für Restore-Vorgänge auf Dateiebene

- Schnellere Restore-Vorgänge auf Dateiebene
- Unterstützung für Browse & Restore-Vorgänge für Dateien aus der Cloud, wenn der Connector vor Ort installiert ist

Beachten Sie, dass die Cloud Restore-Instanz/VM automatisch entfernt wird, wenn Sie sie zuvor verwendet haben. Ein Cloud-Backup-Prozess wird einmal am Tag ausgeführt, um alle alten Cloud Restore-Instanzen zu löschen. Diese Änderung ist völlig transparent - es gibt keine Auswirkungen auf Ihre Daten, und Sie werden keine Änderungen an Ihren Backup- oder Restore-Jobs bemerken.

### Unterstützung für Dateien aus Google Cloud- und StorageGRID-Storage finden Sie unter Durchsuchen und Wiederherstellen

Durch Hinzufügen des Containers für Browse & Restore (wie oben beschrieben) lassen sich nun Dateiwiederherstellungsvorgänge aus Backup-Dateien durchführen, die in Google Cloud- und StorageGRID-Systemen gespeichert sind. Mit Browse & Restore können Dateien jetzt bei allen Public-Cloud-Providern und von StorageGRID wiederhergestellt werden. "Erfahren Sie, wie Sie „Browse Restore“ verwenden, um Volumes und Dateien aus Ihren ONTAP-Backups wiederherzustellen".

### Per Drag-and-Drop ist Cloud-Backup im S3-Storage möglich

Wenn das Amazon S3 Ziel für Ihre Backups als Arbeitsumgebung auf dem Canvas existiert, können Sie Ihr On-Prem ONTAP-Cluster oder Cloud Volumes ONTAP-System (installiert in AWS) auf die Amazon S3-Arbeitsumgebung ziehen, um den Setup-Assistenten zu initiieren.

### Automatische Anwendung einer Backup-Richtlinie auf neu erstellte Volumes in Kubernetes Clustern

Falls Sie nach Aktivierung von Cloud Backup neue persistente Volumes zu Ihren Kubernetes Clustern hinzugefügt haben, mussten Sie in der Vergangenheit auch daran denken, Backups für diese Volumes zu konfigurieren. Sie können nun eine Richtlinie auswählen, die automatisch auf neu erstellte Volumes angewendet wird "Klicken Sie auf der Seite „*Backup Settings*“ auf „" Für Cluster, die bereits Cloud Backup aktiviert haben.

### Cloud Backup APIs sind jetzt für das Management von Backup- und Restore-Vorgängen verfügbar

Die APIs sind unter verfügbar https://docs.netapp.com/us-en/cloud-manager-automation/cbs/overview.html. Siehe "Auf dieser Seite" Für eine Übersicht der APIs.

## Mai 2022

### Search & Restore wird jetzt mit Sicherungsdateien in Google Cloud Storage unterstützt

Im April wurde die Such- & Restore-Methode zur Wiederherstellung von Volumes und Dateien für Benutzer eingeführt, die ihre Backup-Dateien in AWS speichern. Jetzt ist die Funktion für Anwender verfügbar, die ihre Backup-Dateien in Google Cloud Storage speichern. "Erfahren Sie, wie Sie Ihre Volumes und Dateien mithilfe von Search Restore wiederherstellen wiederherstellen wiederherstellen wiederherstellen".

### Backup-Richtlinie konfigurieren, die automatisch auf neu erstellte Volumes in Kubernetes Clustern angewendet wird

Falls Sie nach Aktivierung von Cloud Backup neue persistente Volumes zu Ihren Kubernetes Clustern hinzugefügt haben, mussten Sie in der Vergangenheit auch daran denken, Backups für diese Volumes zu konfigurieren. Sie können nun eine Richtlinie auswählen, die automatisch auf neu erstellte Volumes angewendet wird. Diese Option ist im Setup-Assistenten verfügbar, wenn Sie Cloud Backup für ein neues Kubernetes-Cluster aktivieren.

### Cloud Backup erfordert jetzt eine Lizenz, bevor sie für eine Arbeitsumgebung aktiviert wird

Die Implementierung der Lizenzierung mit Cloud Backup hat einige Änderungen:

- Sie müssen sich für ein PAYGO Marketplace Abonnement bei Ihrem Cloud-Provider anmelden oder eine BYOL-Lizenz von NetApp erwerben, bevor Sie Cloud Backup aktivieren können.
- Die 30-Tage-kostenlose Testversion steht nur bei Nutzung eines PAYGO Abonnements von Ihrem Cloud-Provider zur Verfügung. Diese ist bei Verwendung der BYOL-Lizenz nicht verfügbar.
- Die kostenlose Testversion startet den Tag, an dem das Marketplace-Abonnement beginnt. Wenn Sie beispielsweise die kostenlose Testversion aktivieren, nachdem Sie 30 Tage lang ein Marketplace-Abonnement für ein Cloud Volumes ONTAP-System verwendet haben, steht die Cloud Backup-Testversion nicht zur Verfügung.

"Erfahren Sie mehr über die verfügbaren Lizenzmodelle".

## 4. April 2022

### Cloud Backup für Applikationen 1.1.0 (unterstützt von SnapCenter) ist jetzt allgemein verfügbar

Mit der neuen Cloud Backup für Applikationen können Sie vorhandene applikationskonsistente Snapshots (Backups) für Oracle und Microsoft SQL vom primären Storage vor Ort in den Cloud-Objekt-Storage in Amazon S3 oder Azure Blob auslagern.

Bei Bedarf können diese Daten aus der Cloud in On-Premises-Umgebungen wiederhergestellt werden.

"Weitere Informationen zum Schutz von On-Premises-Applikationsdaten in der Cloud".

### Neue Such- und Wiederherstellungsfunktion zur Suche nach Volumes oder Dateien in allen ONTAP Backup-Dateien

Jetzt können Sie nach einem Volume oder einer Datei über **alle ONTAP Backup-Dateien** nach einem Teil- oder Volldateinamen, einem partiellen oder vollständigen Dateinamen, einem Größenbereich und zusätzlichen Suchfiltern suchen. Dies ist eine großartige neue Möglichkeit, die wiederherzustellenden Daten zu finden, falls Sie nicht sicher sind, welches Cluster oder Volume die Quelle für die Daten war. "Erfahren Sie, wie Sie suchen Restore verwenden".

## 3 März 2022

### Möglichkeit für das Backup persistenter Volumes von den GKE Kubernetes-Clustern auf Google Cloud Storage

Wenn im GKE-Cluster NetApp Astra Trident installiert ist und Cloud Volumes ONTAP für GCP als Backend-Storage für den Cluster verwendet wird, können Sie Ihre persistenten Volumes in und aus dem Google Cloud Storage sichern und wiederherstellen. "Weitere Informationen finden Sie hier".

### Die Beta-Funktion zur Verwendung von Cloud Data Sense zum Scannen Ihrer Cloud Backup-Dateien wurde in dieser Version eingestellt

## 14 Februar 2022

### Nun können Sie Backup-Richtlinien einzelnen Volumes in einem einzigen Cluster zuweisen

Früher konnten alle Volumes in einem Cluster nur eine einzelne Backup-Richtlinie zugewiesen werden. Sie können nun mehrere Backup-Richtlinien für ein einzelnes Cluster erstellen und unterschiedliche Richtlinien auf verschiedene Volumes anwenden. "Hier erfahren Sie, wie Sie neue Backup-Richtlinien für ein Cluster erstellen und diesen ausgewählten Volumes zuweisen".

### Über eine neue Option können Sie automatisch eine standardmäßige Backup-Richtlinie auf neu erstellte Volumes anwenden

In der Vergangenheit mussten Sie neue Volumes, die nach Aktivierung von Cloud Backup in einer Arbeitsumgebung erstellt wurden, manuell eine Backup-Richtlinie anwenden. Unabhängig davon, ob das Volume in BlueXP, System Manager, der CLI oder mithilfe von APIs erstellt wurde, entdeckt Cloud Backup das Volume und wendet die als Standardrichtlinie ausgewählte Backup-Richtlinie an.

Diese Option steht zur Verfügung, wenn Sie das Backup in einer neuen Arbeitsumgebung aktivieren oder über die Seite „ *Volumes* verwalten“ für vorhandene Arbeitsumgebungen.

### Neuer Job Monitor ist verfügbar, um den Prozessstatus aller Backup- und Wiederherstellungsaufträge anzuzeigen

Der Job Monitor kann sehr hilfreich sein, wenn Sie eine Operation gegen mehrere Volumes eingeleitet haben, z. B. das Ändern der Backup-Richtlinie oder das Löschen von Backups, so dass Sie sehen können, wann der Vorgang auf allen Volumes abgeschlossen ist. "Lesen Sie, wie Sie den Job Monitor verwenden".

## Januar 2022

### Möglichkeit zur Sicherung persistenter Volumes von AKS Kubernetes-Clustern auf Azure Blob Storage

Wenn in Ihrem AKS Cluster NetApp Astra Trident installiert ist und Cloud Volumes ONTAP für Azure als Back-End-Storage für den Cluster genutzt wird, können Sie Volumes mit Backups und Restores von und aus dem Azure Blob-Storage durchführen. "Weitere Informationen finden Sie hier".

### In dieser Version wurden die Cloud Backup Service-Gebühren geändert, um sich stärker an die Branchenstandards anzupassen

Anstatt NetApp für die Kapazität auf Basis der Größe der Backup-Dateien zu bezahlen, zahlen Sie jetzt nur für die gesicherten Daten, berechnet anhand der verwendeten logischen Kapazität (vor der ONTAP-Effizienz) der zu sichernden ONTAP Quell-Volumes. Diese Kapazität wird auch als Front-End Terabyte (FETB) bezeichnet.

## 28. November 2021

### Möglichkeit zur Sicherung persistenter Volumes von EKS Kubernetes-Clustern in Amazon S3

Wenn in Ihrem EKS Cluster NetApp Astra Trident installiert ist und Cloud Volumes ONTAP für AWS als Backend-Storage für den Cluster genutzt wird, können Sie Volumes in und aus Amazon S3 sichern und wiederherstellen. "Weitere Informationen finden Sie hier".

### Verbesserte Funktionalität für das Backup von DP Volumes

Cloud Backup unterstützt jetzt die Erstellung von Backups von DP-Volumes, die auf dem ONTAP Zielsystem in einer SVM-DR-Beziehung vorhanden sind. Es gibt einige Einschränkungen, siehe "Einschränkungen zu nutzen" Entsprechende Details.

## 5. November 2021

### Möglichkeit zur Auswahl eines privaten Endpunkts bei der Wiederherstellung eines Volumes auf ein lokales ONTAP System

Bei der Wiederherstellung eines Volumes in einem ONTAP On-Premises-System über eine Backup-Datei in Amazon S3 oder Azure Blob können Sie jetzt einen privaten Endpunkt auswählen, der eine Verbindung zu Ihrem lokalen System privat und sicher herstellt.

### Jetzt können Sie ältere Backup-Dateien nach einigen Tagen in Archiv-Storage verschieben, um Kosten zu sparen

Wenn in Ihrem Cluster ONTAP 9.10.1 oder höher ausgeführt wird und Sie AWS oder Azure Cloud-Storage verwenden, können Sie Tiering von Backups in den Archiv-Storage aktivieren. Weitere Informationen zu "AWS S3 Archiv-Storage-Klassen" Und "Archiv-Zugriffs-Tiers für Azure Blob".

### Byol-Lizenzen für Cloud Backup sind in der Registerkarte Datendienste-Lizenzen im Digital Wallet eingezogen

Byol-Lizenzierung für Cloud Backup hat sich von der Registerkarte Cloud Backup Licenses auf die Registerkarte Data Services Licenses im BlueXP Digital Wallet verlagert.

## Oktober 4 2021

### Die Größe der Sicherungsdatei ist jetzt auf der Seite Backup verfügbar, wenn Sie eine Volume- oder Dateiwiederherstellung durchführen

Dies ist nützlich, wenn Sie große Sicherungsdateien löschen möchten, die unnötig sind, oder so können Sie

Backup-Dateien Größen vergleichen, um alle anormalen Backup-Dateien zu identifizieren, die das Ergebnis eines bösartigen Software-Angriffs sein könnten.

## Mit dem TCO-Rechner können Sie die Kosten für Cloud-Backups vergleichen

Der TCO-Rechner hilft Ihnen, die TCO für Cloud Backup zu verstehen, und diese Kosten mit herkömmlichen Backup-Lösungen zu vergleichen, um mögliche Einsparungen abzuschätzen. Zur Verfügunghttps://cloud.netapp.com/cloud-backup-service-tco-calculator["Hier"^].

## Möglichkeit der Registrierung von Cloud Backup für eine Arbeitsumgebung

Das ist jetzt ganz einfach "Unregister für Cloud Backup für eine Arbeitsumgebung" Wenn Sie keine Backup-Funktion mehr für diese Arbeitsumgebung verwenden möchten (oder berechnet werden).

# Los geht’s

## Weitere Informationen zu Cloud Backup

Cloud Backup ist ein Service für BlueXP (früher Cloud Manager) Arbeitsumgebungen, die Backup- und Restore-Funktionen zum Schutz und zur langfristigen Archivierung Ihrer Daten bieten. Backups werden automatisch erstellt und in einem Objektspeicher in Ihrem Public oder Private Cloud-Konto gespeichert.

Bei Bedarf können Sie ein ganzes *Volume* von einem Backup in dieselbe oder andere Arbeitsumgebung wiederherstellen. Beim Backup von ONTAP-Daten können Sie auch auswählen, eine oder mehrere *Dateien* von einem Backup in dieselbe oder andere Arbeitsumgebung wiederherzustellen.

"Weitere Informationen zu Cloud Backup".

Mit Backup & Restore können folgende Aufgaben ausgeführt werden:

- Erstellen Sie Backups und Restores von ONTAP Volumes von Cloud Volumes ONTAP und lokalen ONTAP Systemen. "Detaillierte Funktionen finden Sie hier".
- Sichern und Wiederherstellen persistenter Kubernetes-Volumes "Detaillierte Funktionen finden Sie hier".
- Erstellen Sie mithilfe von Cloud-Backup für Applikationen Backups konsistenter Snapshots aus lokalen ONTAP-Systemen in die Cloud. "Detaillierte Funktionen finden Sie hier".
- Erstellen Sie Backups von Datastores in der Cloud und stellen Sie Virtual Machines mithilfe von Cloud Backup für VMware zurück in das lokale vCenter. "Detaillierte Funktionen finden Sie hier".

"Sehen Sie sich eine kurze Demo an"

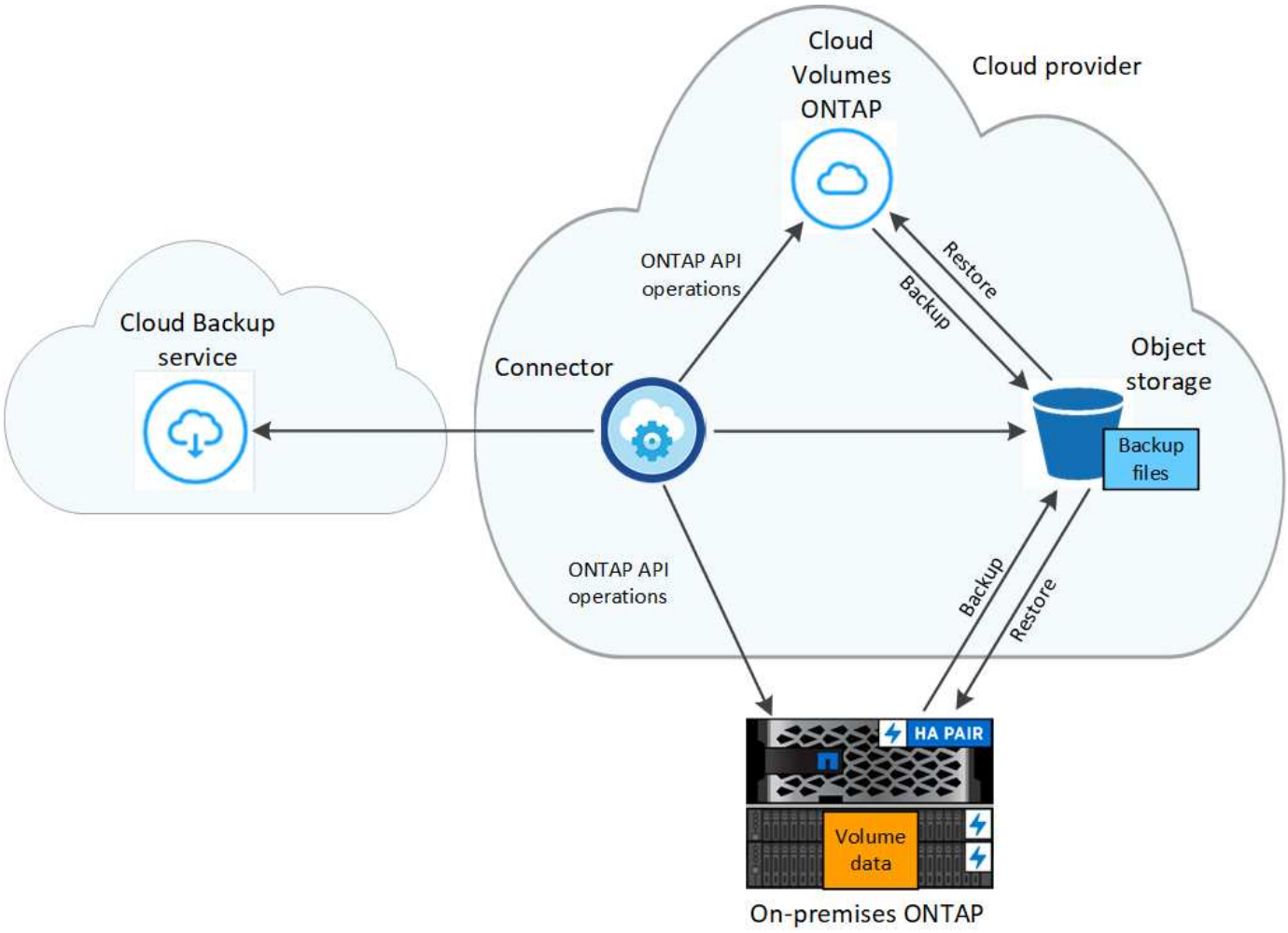
> Wenn der BlueXP Connector in einer Regierungsregion in der Cloud oder an einer Website ohne Internetzugang (eine dunkle Site) bereitgestellt wird, unterstützt Cloud Backup nur Backup- und Restore-Vorgänge von ONTAP Systemen. Bei der Verwendung dieser alternativen Implementierungsmethoden unterstützt Cloud Backup keine Backup- und Restore-Vorgänge von Kubernetes-Clustern, Applikationen oder Virtual Machines.

### Funktionsweise von Cloud Backup

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

In den meisten Fällen verwenden Sie die BlueXP-Benutzeroberfläche für alle Backup-Vorgänge. Ab ONTAP 9.9.1 können Sie jedoch mit ONTAP System Manager Volume-Backup-Vorgänge Ihrer lokalen ONTAP Cluster initiieren. "Mit System Manager erstellen Sie mit Cloud Backup Backups Ihrer Volumes in der Cloud."

Die folgende Abbildung zeigt die Beziehung zwischen den einzelnen Komponenten:




### Speicherort von Backups

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

- In GCP nutzt BlueXP ein neues oder bereits bestehendes Projekt mit einem Storage-Konto für den Google Cloud Storage Bucket.
- In StorageGRID verwendet BlueXP ein vorhandenes Storage-Konto für den Objektspeicher-Bucket.

### Backups werden um Mitternacht erstellt

- Stündliche Backups beginnen 5 Minuten nach der Stunde, jede Stunde.
- Tägliche Backups beginnen jeden Tag kurz nach Mitternacht.
- Wöchentliche Backups beginnen direkt nach Mitternacht am Sonntagmorgen.
- Monatliche Backups beginnen knapp nach Mitternacht am ersten Tag eines jeden Monats.
- Jährliche Backups beginnen knapp nach Mitternacht am ersten Tag des Jahres.

Die Startzeit ist auf der Zeitzone basiert, die auf jedem ONTAP Quell-System eingestellt ist. Sie können keine Backup-Vorgänge zu einem vom Benutzer bestimmten Zeitpunkt von der UI planen. Weitere Informationen erhalten Sie von Ihrem System Engineer.

**Backup-Kopien sind mit Ihrem NetApp Konto verknüpft**

Backup-Kopien sind dem zugewiesen "NetApp Konto" In dem sich der Konnektor befindet.

Wenn Sie mehrere Connectors auf demselben NetApp Konto haben, zeigt jeder Connector dieselbe Liste von Backups an. Dazu gehören auch die Backups, die mit Cloud Volumes ONTAP und lokalen ONTAP-Instanzen von anderen Connectors verbunden sind.

# Lizenzierung für Cloud Backup einrichten

Sie können Cloud Backup lizenzieren, indem Sie bei Ihrem Cloud-Provider ein Pay-as-you-go- (PAYGO) oder ein jährliches Marketplace-Abonnement erwerben oder eine Bring-Your-Own-License-Lizenz (BYOL) von NetApp erwerben. Es ist eine gültige Lizenz erforderlich, um Cloud Backup in einer Arbeitsumgebung zu aktivieren, Backups Ihrer Produktionsdaten zu erstellen und Backup-Daten auf einem Produktionssystem wiederherzustellen.

Ein paar Notizen, bevor Sie weitere lesen:

- Wenn Sie bereits das Pay-as-you-go-Abonnement (PAYGO) in Ihrem Cloud-Provider-Markt für ein Cloud Volumes ONTAP-System abonniert haben, sind Sie auch automatisch bei Cloud Backup angemeldet. Sie müssen sich nicht erneut anmelden.
- Die Bring-Your-Own-License (BYOL) von Cloud Backup ist eine Floating-Lizenz, die Sie auf allen Systemen Ihres BlueXP Kontos verwenden können. Wenn also über ausreichende Backup-Kapazität mit einer bestehenden BYOL-Lizenz verfügen, müssen Sie keine weitere BYOL-Lizenz erwerben.
- Wenn Sie eine BYOL-Lizenz verwenden, empfehlen wir Ihnen, auch ein PAYGO Abonnement zu abonnieren. Wenn Sie mehr Daten als von Ihrer BYOL-Lizenz zulässig sichern, wird das Backup über Ihr Pay-as-you-go-Abonnement fortgesetzt – es tritt keine Serviceunterbrechung auf.
- Beim Backup von lokalen ONTAP-Daten in StorageGRID ist eine BYOL-Lizenz erforderlich. Es entstehen jedoch keine Kosten für Cloud-Provider-Storage.

"Weitere Informationen zu den Kosten für den Einsatz von Cloud Backup."

## 30 Tage kostenlos testen mit unserer

Eine kostenlose 30-Tage-Testversion von Cloud Backup erhalten Sie über das Pay-as-you-go-Abonnement auf dem Markt Ihres Cloud-Providers. Die kostenlose Testversion beginnt zu dem Zeitpunkt, zu dem Sie die Marketplace-Liste abonnieren. Wenn Sie für das Marketplace-Abonnement bei der Bereitstellung eines Cloud Volumes ONTAP Systems bezahlen und dann 10 Tage später die kostenlose Testversion von Cloud Backup starten, haben Sie 20 Tage Zeit, die kostenlose Testversion zu nutzen.

Wenn die kostenlose Testversion endet, werden Sie ohne Unterbrechung automatisch auf das PAYGO-Abonnement umgeschaltet. Wenn Sie sich entscheiden, Cloud Backup nicht weiterhin zu verwenden, einfach "Cloud Backup aus der Arbeitsumgebung ablösen" Vor Ablauf der Testversion wird Ihnen keine Rechnung erhoben.

## Nutzen Sie ein Cloud-Backup-PAYGO-Abonnement

Beim nutzungsbasierten Modell bezahlen Sie Ihren Cloud-Provider für Objekt-Storage-Kosten und für NetApp Backup-Lizenzen auf Stundenbasis in einem einzigen Abonnement. Sie sollten sich auch dann abonnieren, wenn Sie eine kostenlose Testversion haben oder Ihre eigene Lizenz mitbringen (BYOL):

- Das Abonnieren sorgt dafür, dass es keine Serviceunterbrechung gibt, nachdem Ihre kostenlose Testversion endet. Wenn die Studie endet, werden Sie stündlich nach der Menge der Daten, die Sie sichern berechnet.
- Wenn Sie mehr Daten als mit Ihrer BYOL-Lizenz zulässig sichern, wird das Daten-Backup über Ihr Pay-as-you-go-Abonnement fortgesetzt. Wenn Sie beispielsweise eine 10-tib-BYOL-Lizenz haben, wird die gesamte Kapazität über den 10 tib Speicherplatz durch das PAYGO-Abonnement berechnet.

Sie werden nicht von Ihrem Pay-as-you-go-Abonnement während der kostenlosen Testversion oder wenn Sie nicht überschritten haben Ihre Byol-Lizenz.

Es gibt einige PAYGO-Pläne für Cloud-Backup:

- Paket „Cloud Backup“, mit dem Sie Cloud Volumes ONTAP Daten und ONTAP Daten vor Ort sichern können
- Ein Paket „CVO Professional“, mit dem Sie Cloud Volumes ONTAP und Cloud-Backup bündeln können. Dazu zählen unbegrenzte Backups für das Cloud Volumes ONTAP-System mit der Lizenz (die Backup-Kapazität wird nicht von der lizenzierten Kapazität erfasst). Diese Option ermöglicht es Ihnen nicht, Backups von On-Premises ONTAP-Daten.

"Erfahren Sie mehr über diese kapazitätsbasierten Lizenzpakete".

Über diese Links können Sie Cloud Backup über Ihren Cloud-Provider-Marketplace abonnieren:

- GCP: "Weitere Informationen zu Preisen finden Sie im BlueXP Marketplace Angebot".

## Verwenden Sie einen Jahresvertrag

Bezahlen Sie jedes Jahr für Cloud Backup mit einem Jahresvertrag.

Bei der Nutzung von GCP können Sie Ihren NetApp Vertriebsmitarbeiter kontaktieren, um einen Jahresvertrag zu erwerben. Der Vertrag ist als Privatangebot im Google Cloud Marketplace erhältlich. Nachdem NetApp das private Angebot mit Ihnen geteilt hat, können Sie den Jahresplan auch während der Cloud Backup-Aktivierung über den Google Cloud Marketplace beziehen.

## Verwenden einer Cloud Backup-BYOL-Lizenz

Mit den Bring-Your-Own-License-Lizenzen von NetApp erhalten Sie Vertragsbedingungen mit 1, 2 oder 3 Jahren. Sie bezahlen nur für die Daten, die Sie sichern, berechnet sich anhand der genutzten logischen Kapazität (*before* any Effizienzfunktionen) der zu sichernden ONTAP Quell-Volumes. Diese Kapazität wird auch als Front-End Terabyte (FETB) bezeichnet.

Die BYOL Cloud Backup-Lizenz ist eine Floating-Lizenz, bei der die Gesamtkapazität über alle Systeme hinweg genutzt wird, die mit Ihrem BlueXP-Konto verknüpft sind. Bei ONTAP Systemen wird die erforderliche Kapazität durch Ausführen des CLI-Befehls grob geschätzt `volume show -fields logical-used-by-afs` Für die Volumes, die Sie sichern möchten.

Wenn Sie keine Cloud Backup-BYOL-Lizenz haben, klicken Sie auf das Chat-Symbol rechts unten von BlueXP, um eine Lizenz zu erwerben.

Wenn Sie optional eine nicht zugewiesene Node-basierte Lizenz für Cloud Volumes ONTAP haben, die Sie nicht verwenden werden, können Sie diese in eine Cloud Backup Lizenz mit derselben Dollaräquivalenz und demselben Ablaufdatum konvertieren. "Weitere Informationen finden Sie hier".

Sie verwenden die Seite „Digital Wallet“ in BlueXP, um BYOL-Lizenzen zu verwalten. Sie können neue

Lizenzen hinzufügen, vorhandene Lizenzen aktualisieren und den Lizenzstatus über das Digital Wallet anzeigen.

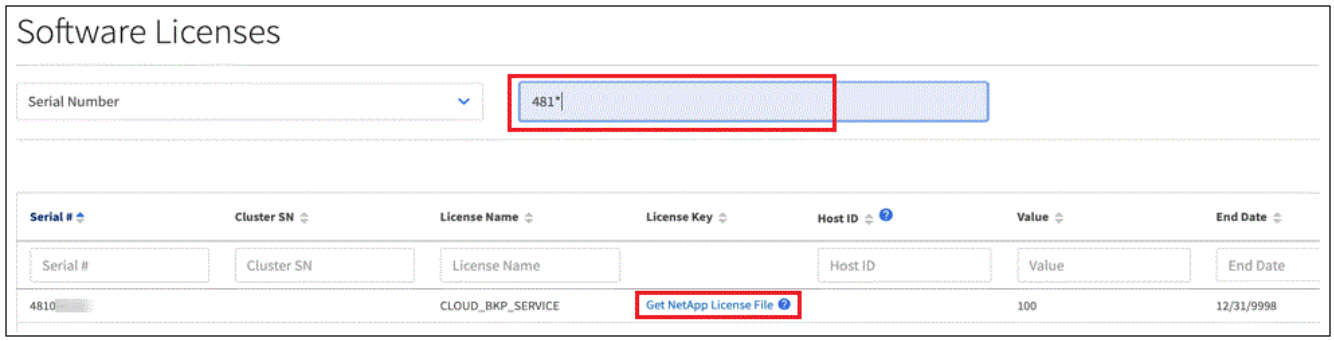
### Holen Sie Ihre Cloud Backup-Lizenzdatei

Nachdem Sie Ihre Cloud Backup-Lizenz erworben haben, aktivieren Sie die Lizenz in BlueXP entweder durch Eingabe der Seriennummer und des NSS-Kontos oder durch Hochladen der NLF-Lizenzdatei. Die folgenden Schritte zeigen, wie Sie die Lizenzdatei NLF abrufen können, wenn Sie diese Methode verwenden möchten.

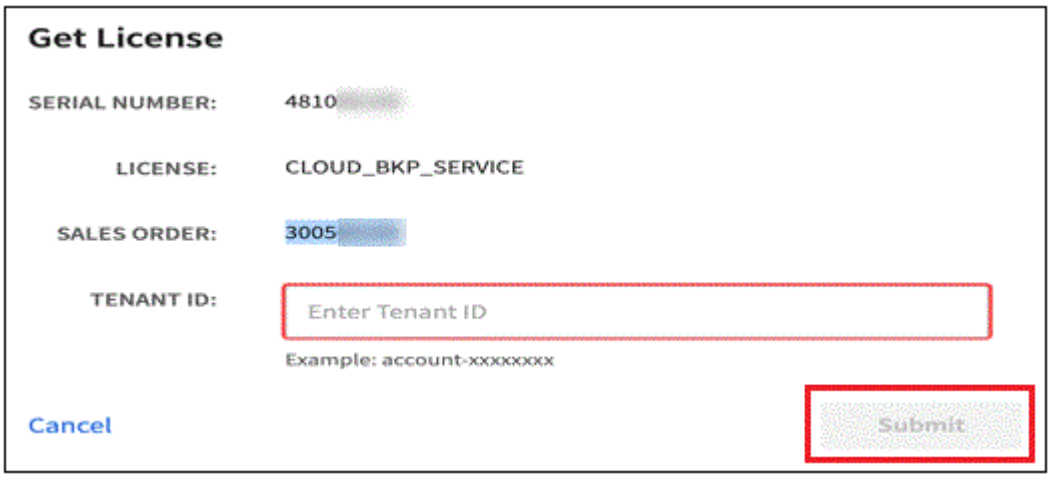
Wenn Sie Cloud Backup in einer On-Premises-Website, die keinen Internetzugang hat, was bedeutet, dass Sie den BlueXP Connector auf einem Host in der Offline-On-Premises-Website bereitgestellt haben, müssen Sie die Lizenzdatei von einem Internet-verbundenen System erhalten. Die Aktivierung der Lizenz unter Verwendung der Seriennummer und des NSS-Kontos ist für Offline-Installationen (Dark Site) nicht verfügbar.

#### Schritte

1. Melden Sie sich beim an "NetApp Support Website" Klicken Sie anschließend auf **Systeme > Softwarelizenzen**.
2. Geben Sie die Seriennummer Ihrer Cloud Backup-Lizenz ein.




3. Klicken Sie in der Spalte **Lizenzschlüssel** auf **NetApp Lizenzdatei abrufen**.
4. Geben Sie Ihre BlueXP-Konto-ID ein (dies wird als Mandanten-ID auf der Support-Website bezeichnet) und klicken Sie auf **Absenden**, um die Lizenzdatei herunterzuladen.




Sie können Ihre BlueXP-Konto-ID finden, indem Sie oben in BlueXP das Dropdown-Menü **Konto** auswählen und dann neben Ihrem Konto auf **Konto verwalten** klicken. Ihre Account-ID wird auf der Registerkarte „Übersicht“ angezeigt.

### Byol-Lizenzen für Cloud Backup werden Ihrem Konto hinzugefügt

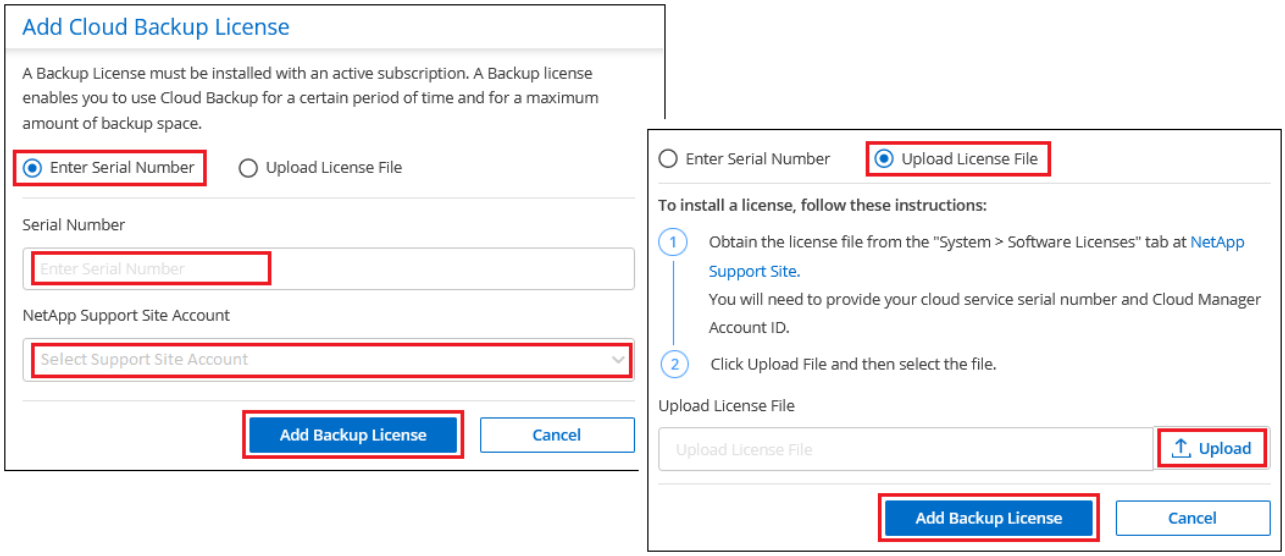
Nachdem Sie eine Cloud Backup Lizenz für Ihr NetApp Konto erworben haben, müssen Sie die Lizenz zu BlueXP hinzufügen.

#### Schritte

1. Klicken Sie im BlueXP-Menü auf **Governance > Digital Wallet** und wählen Sie dann die Registerkarte **Data Services Licenses** aus.
2. Klicken Sie Auf **Lizenz Hinzufügen**.
3. Geben Sie im Dialogfeld „*Lizenz hinzufügen*“ die Lizenzinformationen ein, und klicken Sie auf **Lizenz hinzufügen**:
   - Wenn Sie über die Seriennummer der Sicherungslizenz verfügen und Ihr NSS-Konto kennen, wählen Sie die Option **Seriennummer eingeben** aus, und geben Sie diese Informationen ein.

     Wenn Ihr NetApp Support Site Konto nicht in der Dropdown-Liste verfügbar ist, "Fügen Sie das NSS-Konto zu BlueXP hinzu".

   - Wenn Sie über die Sicherungslizenz verfügen (erforderlich, wenn Sie sie in einem dunklen Standort installieren), wählen Sie die Option **Lizenzdatei hochladen** aus und befolgen Sie die Anweisungen, um die Datei anzuhängen.

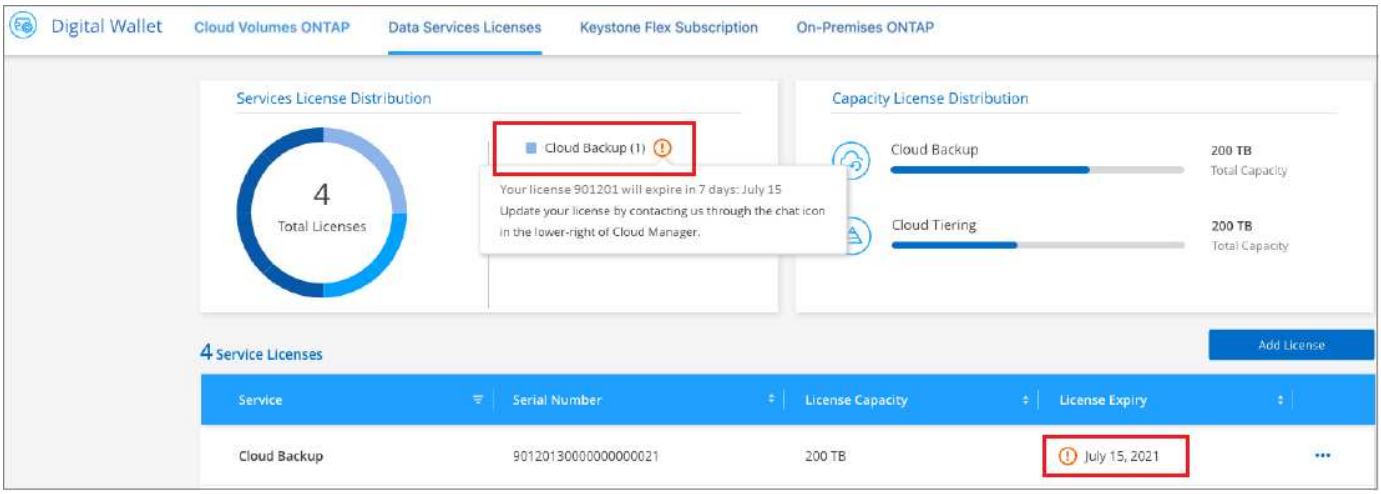



#### Ergebnis

BlueXP fügt die Lizenz hinzu, damit Cloud Backup aktiv ist.

### Byol-Lizenz für Cloud Backup aktualisieren

Wenn sich Ihre Lizenzlaufzeit dem Ablaufdatum nähert oder Ihre lizenzierte Kapazität die Grenze erreicht, werden Sie in der Backup-Benutzeroberfläche benachrichtigt. Dieser Status wird auch auf der Seite Digital Wallet und in angezeigt "Benachrichtigungen".




Sie können Ihre Cloud Backup-Lizenz vor Ablauf des Zeitraums aktualisieren, damit Ihre Daten nicht durch Backup und Restore gesichert werden können.

**Schritte**

1. Klicken Sie rechts unten auf das Chat-Symbol von BlueXP, oder wenden Sie sich an den Support, um eine Verlängerung Ihres Termins oder zusätzliche Kapazität Ihrer Cloud Backup-Lizenz für die jeweilige Seriennummer anzufordern.

   Nach der Zahlung für die Lizenz und der Registrierung auf der NetApp Support-Website aktualisiert BlueXP automatisch die Lizenz im Digital Wallet. Auf der Seite „Data Services Licenses“ wird die Änderung in 5 bis 10 Minuten dargestellt.

2. Wenn BlueXP die Lizenz nicht automatisch aktualisieren kann (zum Beispiel, wenn sie auf einer dunklen Seite installiert wird), müssen Sie die Lizenzdatei manuell hochladen.

   a. Das können Sie Beziehen Sie die Lizenzdatei über die NetApp Support-Website.

   b. Klicken Sie auf der Registerkarte Digital Wallet Page *Data Services Licenses* auf ••• Klicken Sie für die Serviceseriennummer, die Sie aktualisieren, auf **Lizenz aktualisieren**.

   c. Laden Sie auf der Seite *Update License* die Lizenzdatei hoch und klicken Sie auf **Update License**.

**Ergebnis**

BlueXP aktualisiert die Lizenz, sodass Cloud Backup weiterhin aktiv ist.

### Überlegungen zu BYOL-Lizenzen

Bei Verwendung einer Cloud Backup-BYOL-Lizenz zeigt BlueXP eine Warnung in der Benutzeroberfläche an, wenn sich die Größe aller Daten, die Sie sichern, dem Kapazitätslimit nähert oder dem Ablaufdatum der Lizenz

nähert. Sie erhalten folgende Warnungen:

- Wenn Backups 80 % der lizenzierten Kapazität erreicht haben, und noch einmal, wenn Sie die Obergrenze erreicht haben
- 30 Tage, bevor eine Lizenz abläuft, und wieder, wenn die Lizenz abläuft

Verwenden Sie das Chat-Symbol rechts unten in der BlueXP-Schnittstelle, um Ihre Lizenz zu verlängern, wenn diese Warnungen angezeigt werden.

Zwei Dinge können passieren, wenn Ihre Byol-Lizenz abläuft:

- Wenn das Konto, das Sie nutzen, über ein Marketplace-Konto verfügt, läuft der Backup-Service weiter, wird jedoch in ein PAYGO Lizenzmodell verschoben. Die Kapazität Ihrer Backups wird Ihnen in Rechnung gestellt.
- Wenn das Konto, das Sie verwenden, kein Marketplace-Konto hat, läuft der Backup-Service weiter, aber Sie werden weiterhin die Warnungen sehen.

Sobald Sie Ihr BYOL-Abonnement verlängert haben, aktualisiert BlueXP die Lizenz automatisch. Wenn BlueXP nicht über die sichere Internetverbindung auf die Lizenzdatei zugreifen kann (z. B. bei Installation in einer dunklen Site), können Sie die Datei selbst beziehen und sie manuell auf BlueXP hochladen. Anweisungen hierzu finden Sie unter "So aktualisieren Sie eine Cloud Backup-Lizenz".

Systeme, die auf eine PAYGO-Lizenz verschoben wurden, werden automatisch an die BYOL-Lizenz zurückgegeben. Bei Systemen, die ohne Lizenz ausgeführt wurden, werden die Warnungen nicht mehr angezeigt.

# Überwachen des Status von Backup- und Restore-Jobs

Sie können den Status von Backup- und Wiederherstellungsjobs überwachen, die Sie in Ihren Arbeitsumgebungen initiiert haben. Auf diese Weise können Sie die Aufträge sehen, die erfolgreich abgeschlossen wurden, die derzeit in Bearbeitung sind und die, die nicht erfolgreich abgeschlossen wurden, damit Sie Probleme diagnostizieren und beheben können. Sie können auch Benachrichtigungen so konfigurieren, dass sie per E-Mail versendet werden, dass Sie über wichtige Systemaktivitäten informiert werden können, auch wenn Sie nicht im System angemeldet sind.

## Verwenden Sie den Job Monitor, um den Status des Backup- und Wiederherstellungsjobs anzuzeigen

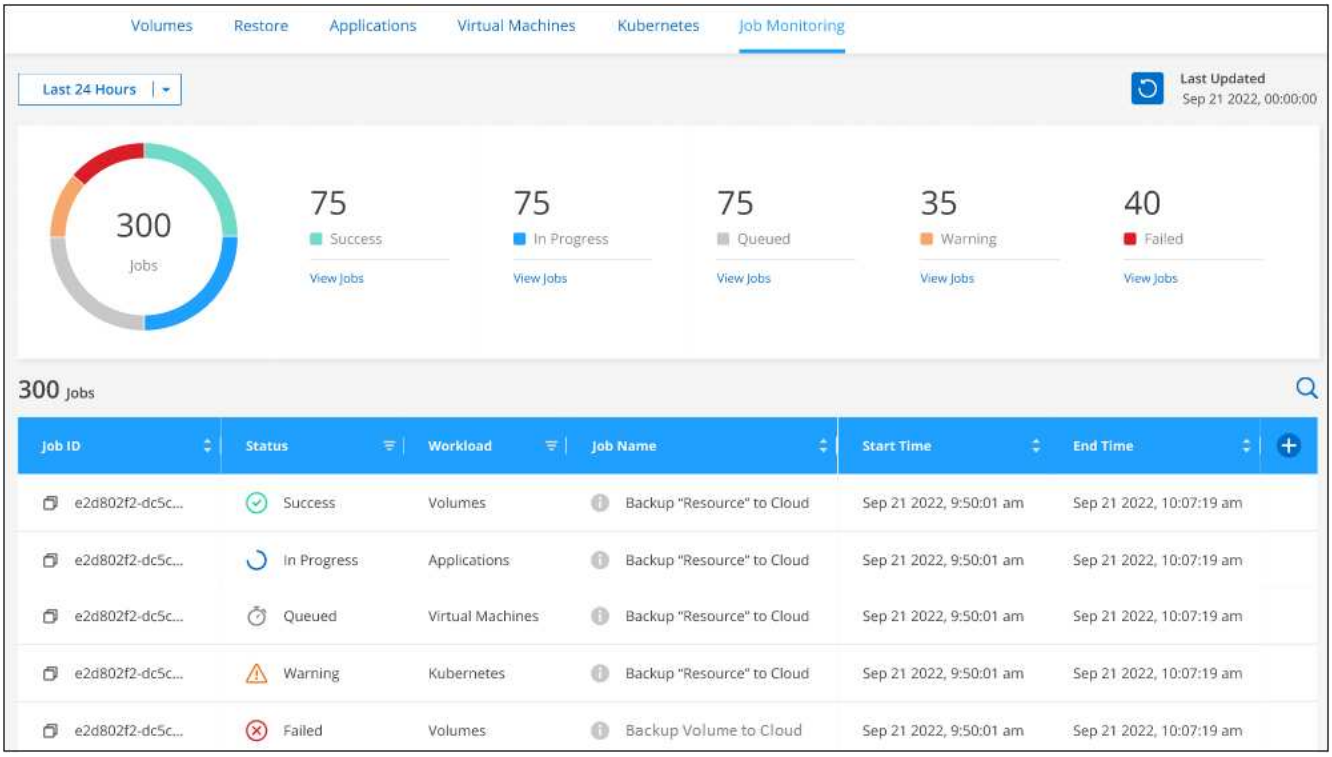
Auf der Registerkarte **Job Monitoring** können Sie eine Liste aller Backup- und Wiederherstellungsvorgänge und deren aktueller Status anzeigen. Dies umfasst auch Abläufe Ihrer Cloud Volumes ONTAP, lokalen ONTAP, Applikationen, Virtual Machines und Kubernetes-Systeme. Jeder Vorgang oder Job hat eine eindeutige ID und einen Status. Der Status kann lauten:

- Erfolg
- In Bearbeitung
- Warteschlange
- Warnung
- Fehlgeschlagen

Beachten Sie, dass systeminitiierte Jobs, wie laufende Backup-Vorgänge, nicht in der Registerkarte **Job Monitoring** — nur vom Benutzer initiierte Jobs angezeigt werden.

**Schritte**

1. Wählen Sie im Menü BlueXP die Option **Schutz > Sicherung und Wiederherstellung**.
2. Klicken Sie auf die Registerkarte **Job Monitoring**.



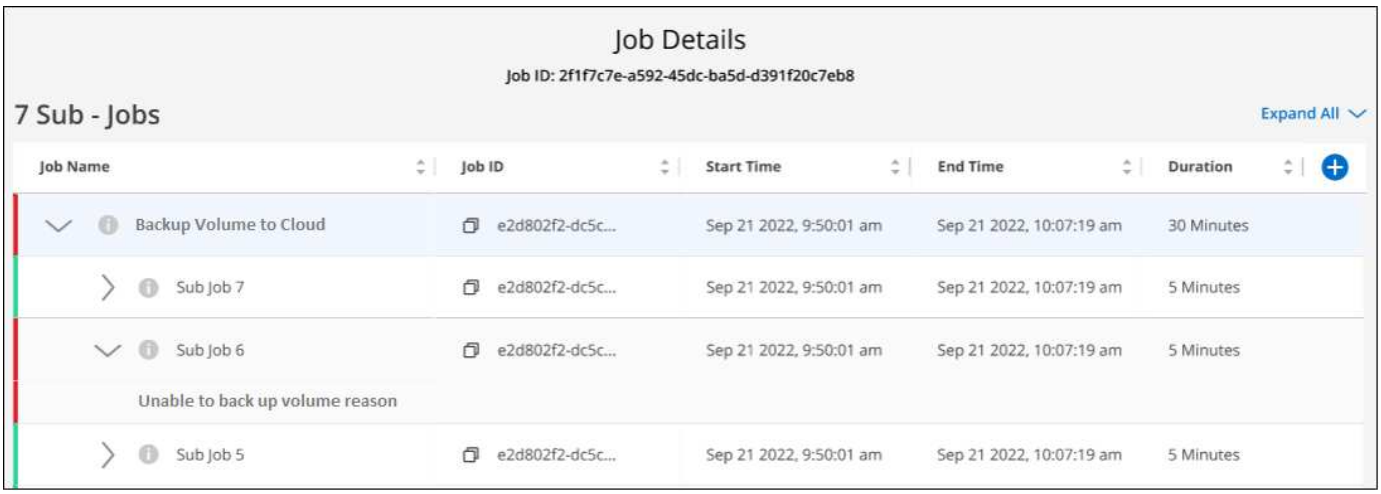

In diesem Screenshot werden die standardmäßigen Spalten-/Feldüberschriften angezeigt. Klicken Sie auf Um Spaltenüberschriften ein- und auszublenden, oder um zwei zusätzliche Überschriften für „Benutzername“ und „Typ“ hinzuzufügen.

Wenn Sie nach bestimmten Jobs suchen, können Sie:

- Verwenden Sie die Zeitauswahl oben links auf der Seite, um Jobs für einen bestimmten Zeitraum anzuzeigen
- Geben Sie einen Teil des Jobnamens in das Suchfeld ein
- Klicken Sie auf **Jobs anzeigen** für einen bestimmten Status, z. B. unter „Fehlgeschlagen“, um nur fehlgeschlagene Jobs anzuzeigen
- Sortieren Sie die Ergebnisse mithilfe des Filters in jeder Spaltenüberschrift. Der Filter für die Spalte „Workloads“ ermöglicht Ihnen zum Beispiel, Jobs in den folgenden Kategorien anzuzeigen:
  - Volumes (Cloud Volumes ONTAP und lokale ONTAP Volumes)
  - Applikationen Unterstützt
  - Virtual Machines
  - Kubernetes

Diese Seite wird automatisch alle 15 Minuten aktualisiert, sodass Sie immer die aktuellsten Ergebnisse des Jobstatus sehen. Klicken Sie auf die Schaltfläche **Aktualisieren**, um die Seite sofort zu aktualisieren.

Um Details anzuzeigen, die einem bestimmten Job entsprechen, klicken Sie auf den Namen des Jobs. Auf der Seite „Jobdetails“ werden alle untergeordneten Jobs angezeigt, die ausgeführt werden, um den Hauptjob abzuschließen.




## Verwenden Sie das Notification Center, um Sicherungs- und Wiederherstellungswarnungen zu überprüfen

Das Notification Center verfolgt den Fortschritt von Backup- und Restore-Jobs, die Sie initiiert haben, damit Sie überprüfen können, ob der Vorgang erfolgreich war oder nicht. Sie können die Benachrichtigungen anzeigen, indem Sie auf die Schaltfläche ( klicken) In der BlueXP-Menüleiste. Außerdem können Sie BlueXP so konfigurieren, dass Benachrichtigungen per E-Mail als Warnungen gesendet werden, damit Sie auch dann über wichtige Systemaktivitäten informiert werden können, wenn Sie nicht im System angemeldet sind.

Derzeit gibt es vier Ereignisse, die E-Mail-Benachrichtigungen auslösen:

- Aktivierung von Cloud Backup in der Arbeitsumgebung fehlgeschlagen
- Wiederherstellung von Cloud-Backups fehlgeschlagen
- Ad-hoc-Backup (On-Demand) des Volumes ist fehlgeschlagen
- Potenzielle Ransomware-Angriffe auf Ihrem System erkannt

Standardmäßig erhalten BlueXP-Kontoadministratoren E-Mails für alle „kritischen“ und „Empfehlungsmeldungen“. Alle anderen Benutzer und Empfänger sind standardmäßig so konfiguriert, dass sie keine Benachrichtigungs-E-Mails erhalten. E-Mails können an alle BlueXP Benutzer, die Teil Ihres NetApp Cloud Kontos sind, oder an andere Empfänger gesendet werden, die Backup- und Wiederherstellungsaktivitäten kennen müssen.

Sie müssen die Benachrichtigungstypen „kritisch“ und „Fehler“ auswählen, um E-Mail-Benachrichtigungen zum Cloud Backup zu erhalten.

"Erfahren Sie mehr über das Notification Center und das Senden von Warn-E-Mails für Backup- und Wiederherstellungsaufträge".

# Backup und Restore von ONTAP Daten

## ONTAP-Cluster-Daten mit Cloud Backup schützen

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

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

### Funktionen

Backup-Funktionen:

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

Wiederherstellungsfunktionen:

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

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

## Unterstützte ONTAP-Arbeitsumgebungen und Objekt-Storage-Provider

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

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

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

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

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

### Unterstützung für Websites ohne Internetverbindung

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

## Unterstützte Volumes

Cloud Backup unterstützt die folgenden Volume-Typen:

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

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

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

## Kosten

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

### Ressourcengebühren

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

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

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

- Beim Wiederherstellen von Daten mithilfe von Suchen und Wiederherstellen werden bestimmte Ressourcen vom Cloud-Provider bereitgestellt. Die Datenmenge, die von Ihren Suchanfragen gescannt wird, kostet pro tib. (Diese Ressourcen sind für Durchsuchen und Wiederherstellen nicht erforderlich.)
- In Google wird ein neuer Bucket implementiert, und der "Google Cloud BigQuery Services" Werden auf Konto-/Projektebene bereitgestellt.
- Falls Sie Volume-Daten aus einer Backup-Datei wiederherstellen müssen, die in den Archiv-Storage verschoben wurde, erhalten Sie eine zusätzliche Gebühr für den pro gib-Abruf und die Gebühr pro Anfrage vom Cloud-Provider.

### Servicegebühren

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

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

## Lizenzierung

Cloud Backup ist mit den folgenden Nutzungsmodellen verfügbar:

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

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

### Mit Ihrer eigenen Lizenz

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

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

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

### Pay-as-you-go-Abonnement

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

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

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

### Jahresvertrag

- Bei der Verwendung von GCP können Sie ein privates Angebot von NetApp anfordern. Anschließend können Sie den Plan auswählen, wenn Sie während der Cloud Backup-Aktivierung über den Google Cloud Marketplace abonnieren.

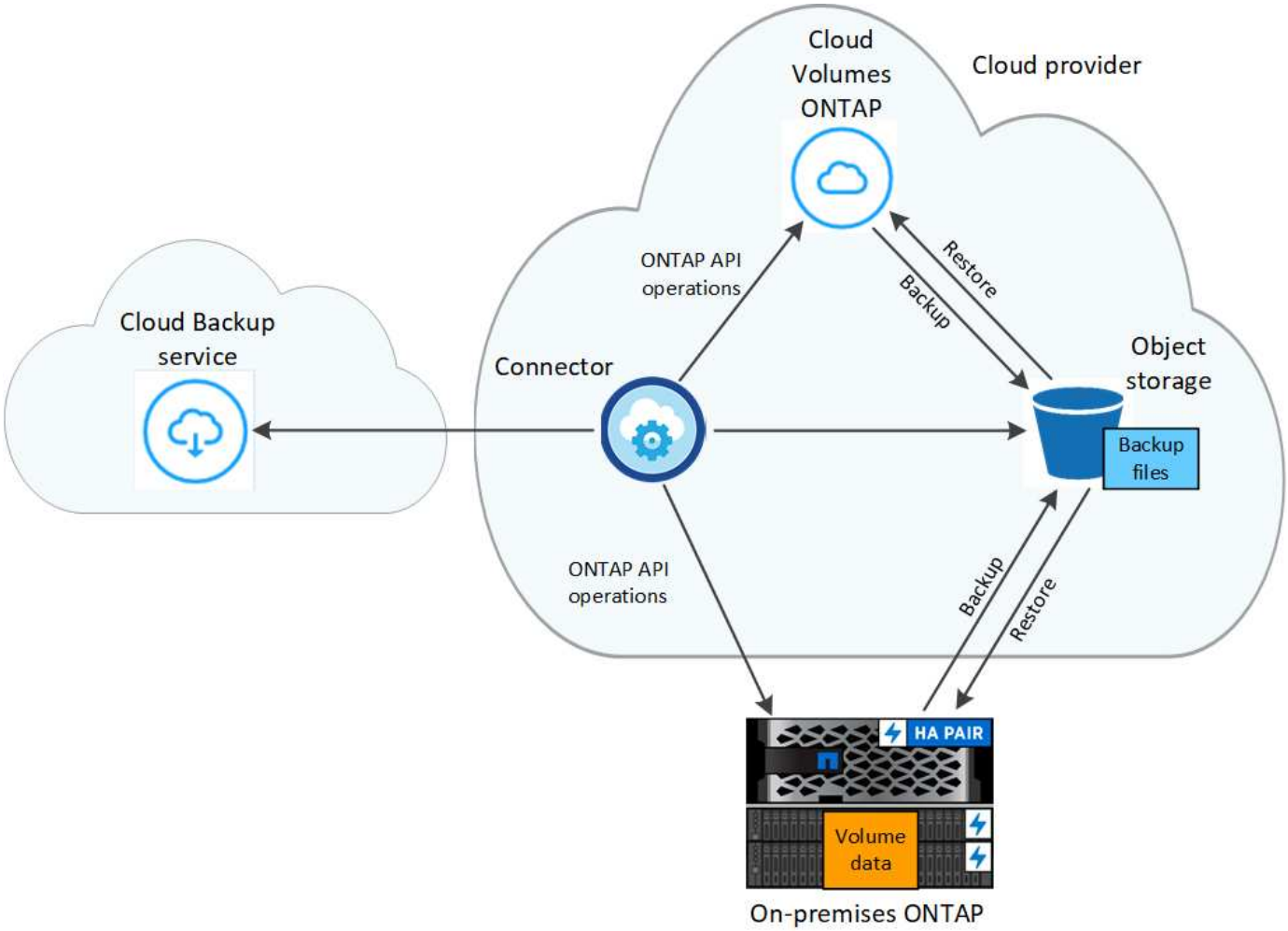
"Hier erfahren Sie, wie Sie Jahresverträge einrichten können".

## Funktionsweise von Cloud Backup

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

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

Die folgende Abbildung zeigt die Beziehung zwischen den einzelnen Komponenten:




### Speicherort von Backups

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

- In GCP nutzt BlueXP ein neues oder bereits bestehendes Projekt mit einem Storage-Konto für den Google Cloud Storage Bucket.
- In StorageGRID verwendet BlueXP ein vorhandenes Storage-Konto für den Objektspeicher-Bucket.

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

### Anpassbare Backup-Planungs- und Aufbewahrungseinstellungen

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

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

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

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

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

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

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

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

### Sicherungseinstellungen für Dateien sichern

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

Die Backup-Aufbewahrungsdauer ist identisch mit der Aufbewahrungsfrist des Backup-Zeitplans plus 14 Tage.

Beispielsweise werden bei *Weekly* Backups mit gespeicherten *5* Kopien jede Backup-Datei 5 Wochen lang gesperrt. *Monatliche* Backups mit *6* Kopien zurückbehaltenen Kopien werden jede Backup-Datei 6 Monate lang gesperrt.

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

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

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

**Archiv-Storage für ältere Backup-Dateien**

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

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

  Wenn Ihr On-Prem-Cluster ONTAP 9.12.1 oder höher verwendet, können Sie nach einer bestimmten Anzahl von Tagen ältere Backups als *Archive* Storage in der Cloud Backup UI verschieben, um die Kosten weiter zu optimieren. (Diese Funktion ist derzeit für Cloud Volumes ONTAP Systeme nicht verfügbar.) "Erfahren Sie mehr über Google Archivspeicher".

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

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

## Überlegungen zu den Tiering-Richtlinien von FabricPool

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

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

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

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

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

## Einschränkungen

Das folgende Problem ist bekannt, das in einer zukünftigen Version behoben wird:

- Wenn während eines Wiederherstellungsvorgangs auf einem System mit ONTAP Version 9.10.1 oder neuer ein Backup erstellt wurde und auf dem System, auf dem das Volume wiederhergestellt wird, ONTAP Version 9.10.0 oder eine frühere Version ausgeführt wird, schlägt die Wiederherstellung entweder durch Systemunterbrechung oder in manchen Fällen erfolgreich fehl. Aber das Volumen ist beschädigt.

### Backup-Einschränkungen

- Um ältere Backup-Dateien per Tiering in Archiv-Storage zu verschieben, muss der Cluster ONTAP 9.10.1 oder höher ausführen. Für die Wiederherstellung von Volumes aus Backup-Dateien, die sich im Archiv-Storage befinden, muss im Ziel-Cluster zudem ONTAP 9.10.1+ ausgeführt werden.
- Wenn eine Backup-Richtlinie erstellt oder bearbeitet wird, wenn dieser Richtlinie keine Volumes zugewiesen werden, kann die Anzahl der zurückbehaltenen Backups maximal 1018 sein. Als Workaround können Sie die Anzahl der Backups zur Erstellung der Richtlinie verringern. Anschließend können Sie die Richtlinie bearbeiten, um bis zu 4000 Backups zu erstellen, nachdem Sie der Richtlinie Volumes zugewiesen haben.
- Bei der Sicherung von Datensicherungs-Volumes (DP):
  - Beziehungen zu den SnapMirror-Labels `app_consistent` Und `all_source_snapshot` Wird nicht in der Cloud gesichert werden.
  - Wenn Sie lokale Kopien der Snapshots auf dem SnapMirror Ziel-Volume erstellen (unabhängig von den verwendeten SnapMirror Bezeichnungen), werden diese Snapshots nicht als Backups in die Cloud verschoben. Zu diesem Zeitpunkt müssen Sie eine Snapshot-Richtlinie mit den gewünschten Labels auf dem Quell-DP-Volume erstellen, um Cloud Backup zu sichern.
- SVM-DR-Volume-Backup wird unter den folgenden Einschränkungen unterstützt:
  - Backups werden nur von der sekundären ONTAP unterstützt.
  - Die auf das Volume angewandte Snapshot Richtlinie muss eine der vom Cloud Backup anerkannten Richtlinien sein, einschließlich täglich, wöchentlich, monatlich usw. die standardmäßige „SM_created“ Richtlinie (wird für **Spiegelung aller Snapshots** verwendet) Das DP-Volume wird nicht erkannt und in der Liste der Volumes, die gesichert werden können, nicht angezeigt.
- Das MetroCluster (MCC) Backup wird nur von ONTAP sekundär unterstützt: MCC > SnapMirror > ONTAP > Cloud Backup > Objekt-Storage.
- Ad-hoc-Volume-Backup mit der **Backup Now**-Taste wird auf Datensicherungs-Volumes nicht unterstützt.
- SM-BC-Konfigurationen werden nicht unterstützt.
- ONTAP unterstützt keine Fan-out-of-SnapMirror-Beziehungen von einem einzelnen Volume zu mehreren Objektspeicher. Daher wird diese Konfiguration nicht von Cloud Backup unterstützt.
- WORM-/Compliance-Modus auf einem Objektspeicher wird derzeit nur von Amazon S3 und StorageGRID unterstützt. Dies wird als DataLock-Funktion bezeichnet und muss mit Cloud Backup-Einstellungen verwaltet werden.

### Einschränkungen bei der Datei- und Ordnerwiederherstellung

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

- Browse & Restore kann bis zu 100 einzelne Dateien gleichzeitig wiederherstellen.
- Search & Restore kann 1 Datei gleichzeitig wiederherstellen.
- Suchen und Wiederherstellen und Suchen und Wiederherstellen können 1 Ordner gleichzeitig wiederherstellen.

- Die wiederherzustellende Datei muss die gleiche Sprache verwenden wie die Sprache auf dem Zielvolume. Wenn die Sprachen nicht identisch sind, wird eine Fehlermeldung angezeigt.
- Wiederherstellung auf Dateiebene wird nicht unterstützt, wenn Sie dasselbe Konto mit verschiedenen BlueXP-Systemen in unterschiedlichen Subnetzen verwenden.
- Sie können einzelne Ordner nicht wiederherstellen, wenn sich die Sicherungsdatei im Archiv-Speicher befindet.
- Wiederherstellung auf Dateiebene mithilfe von Suchen & Wiederherstellen wird nicht unterstützt, wenn der Connector auf einer Website ohne Internetzugang installiert wird (dunkle Seite).

# Sichern von Cloud Volumes ONTAP Daten auf Google Cloud Storage –

Führen Sie einige Schritte durch, um die Datensicherung von Cloud Volumes ONTAP auf Google Cloud Storage zu starten.

## Schnellstart

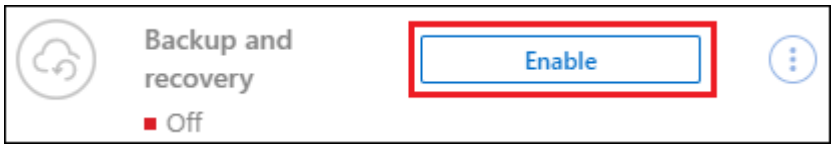
Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

1 **Überprüfen Sie die Unterstützung Ihrer Konfiguration**

- In GCP wird Cloud Volumes ONTAP 9.7P5 oder höher verwendet.
- Sie verfügen über ein gültiges GCP-Abonnement für den Speicherplatz, in dem sich Ihre Backups befinden.
- Sie verfügen über ein Service-Konto in Ihrem Google Cloud Projekt, das über die vordefinierte Rolle „Storage Admin“ verfügt.
- Sie haben sich für das angemeldet "BlueXP Marketplace Backup-Angebot", Oder Sie haben gekauft "Und aktiviert" Eine Cloud Backup BYOL-Lizenz von NetApp

2 **Cloud Backup auf Ihrem neuen oder vorhandenen System aktivieren**

- Neue Systeme: Cloud Backup kann aktiviert werden, wenn Sie den Assistenten für die neue Arbeitsumgebung abschließen.
- Bestehende Systeme: Wählen Sie die Arbeitsumgebung aus und klicken Sie auf **Aktivieren** neben dem Backup- und Recovery-Dienst im rechten Fenster, und folgen Sie dann dem Setup-Assistenten.

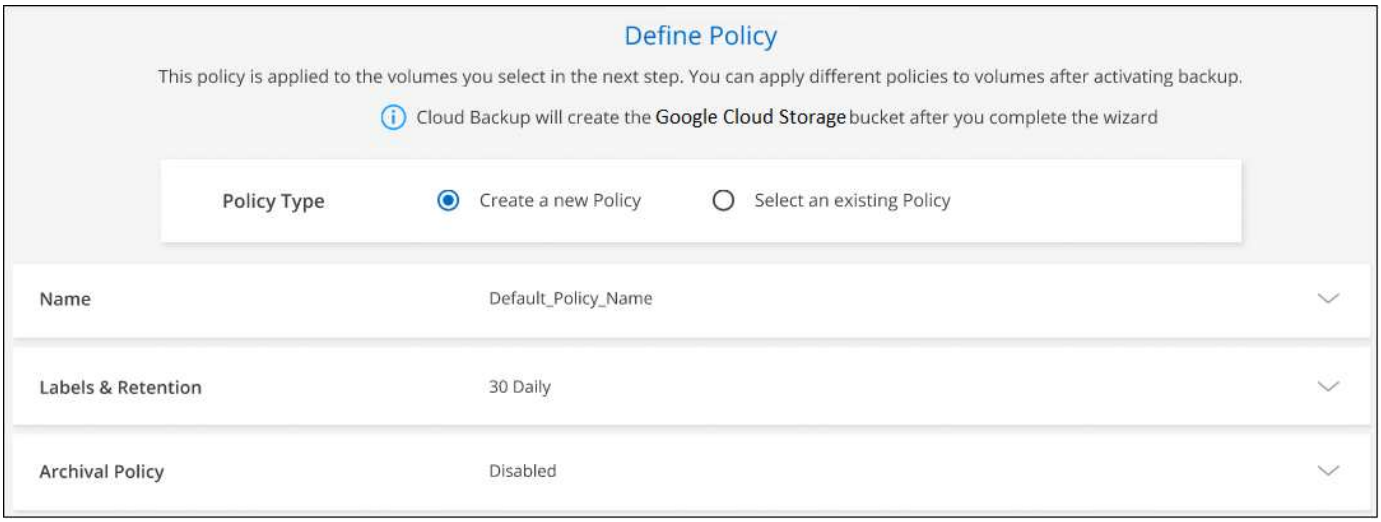



3 **Geben Sie die Anbieterdetails ein**

Wählen Sie das Google Cloud Projekt aus, in dem der Google Cloud Storage-Bucket für Backups erstellt werden soll.

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

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



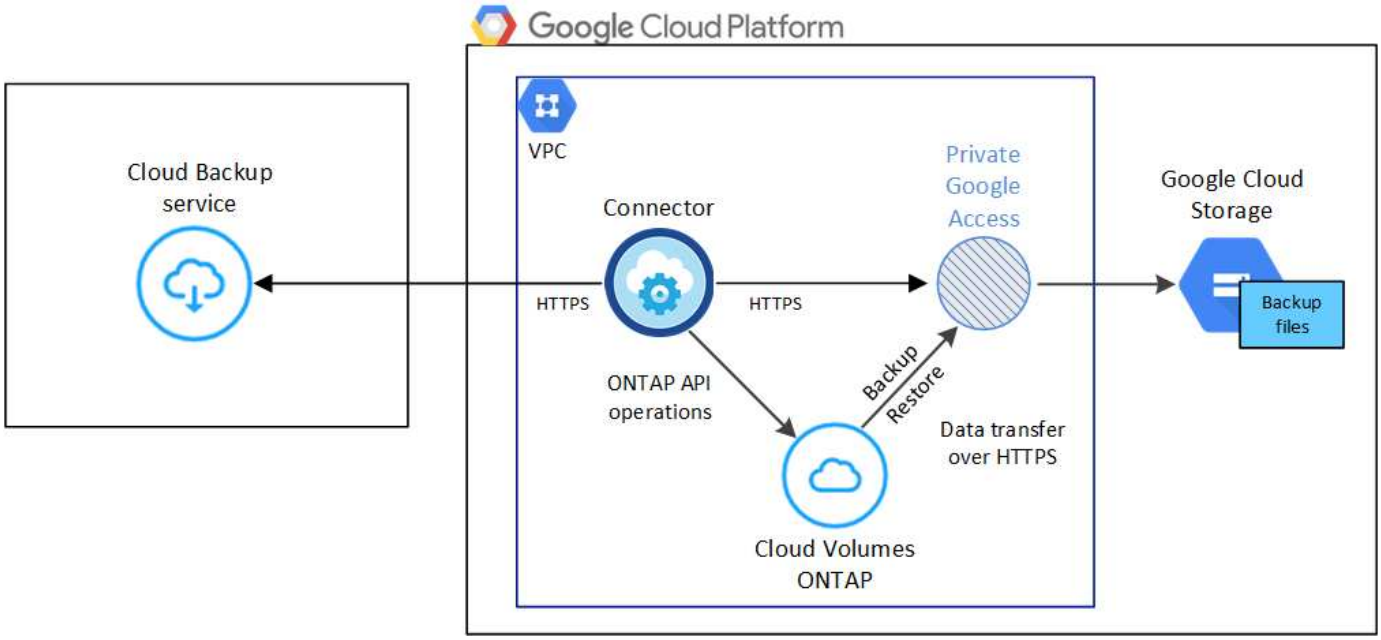

**5** **Wählen Sie die Volumes aus, die Sie sichern möchten**

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

## Anforderungen

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

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




### Unterstützte ONTAP-Versionen

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

### Lizenzanforderungen

Für Cloud Backup PAYGO-Lizenzen ist ein BlueXP-Abonnement über das verfügbar "GCP Marketplace" Ist erforderlich, bevor Sie Cloud Backup aktivieren. Die Abrechnung für Cloud Backup erfolgt über dieses Abonnement. "Sie können sich auf der Seite Details Credentials des Assistenten für die Arbeitsumgebung anmelden".

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

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

### Unterstützte GCP-Regionen

Cloud Backup wird in allen GCP-Regionen unterstützt "Wobei Cloud Volumes ONTAP unterstützt wird".

### GCP-Service-Konto

Sie benötigen ein Servicekonto in Ihrem Google Cloud Projekt, das über die vordefinierte Rolle „Storage Admin“ verfügt. "Erfahren Sie, wie Sie ein Servicekonto erstellen".

### Überprüfen oder Hinzufügen von Berechtigungen zum Konnektor

Um die Cloud Backup Funktion „Search & Restore“ nutzen zu können, benötigen Sie spezielle Berechtigungen in der Rolle für den Connector, damit er 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.

1. In "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. Klicken Sie auf eine benutzerdefinierte Rolle.
4. Klicken Sie auf **Rolle bearbeiten**, um die Berechtigungen der Rolle zu aktualisieren.

5. Klicken Sie auf **Berechtigungen hinzufügen**, um der Rolle folgende neue 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. Klicken Sie auf **Aktualisieren**, um die bearbeitete Rolle zu speichern.

## Aktivierung von Cloud Backup auf einem neuen System

Cloud Backup kann aktiviert werden, wenn Sie den Assistenten für die Arbeitsumgebung zur Erstellung eines neuen Cloud Volumes ONTAP Systems abschließen.

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. Klicken Sie auf der Seite Arbeitsumgebungen auf **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen.
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:

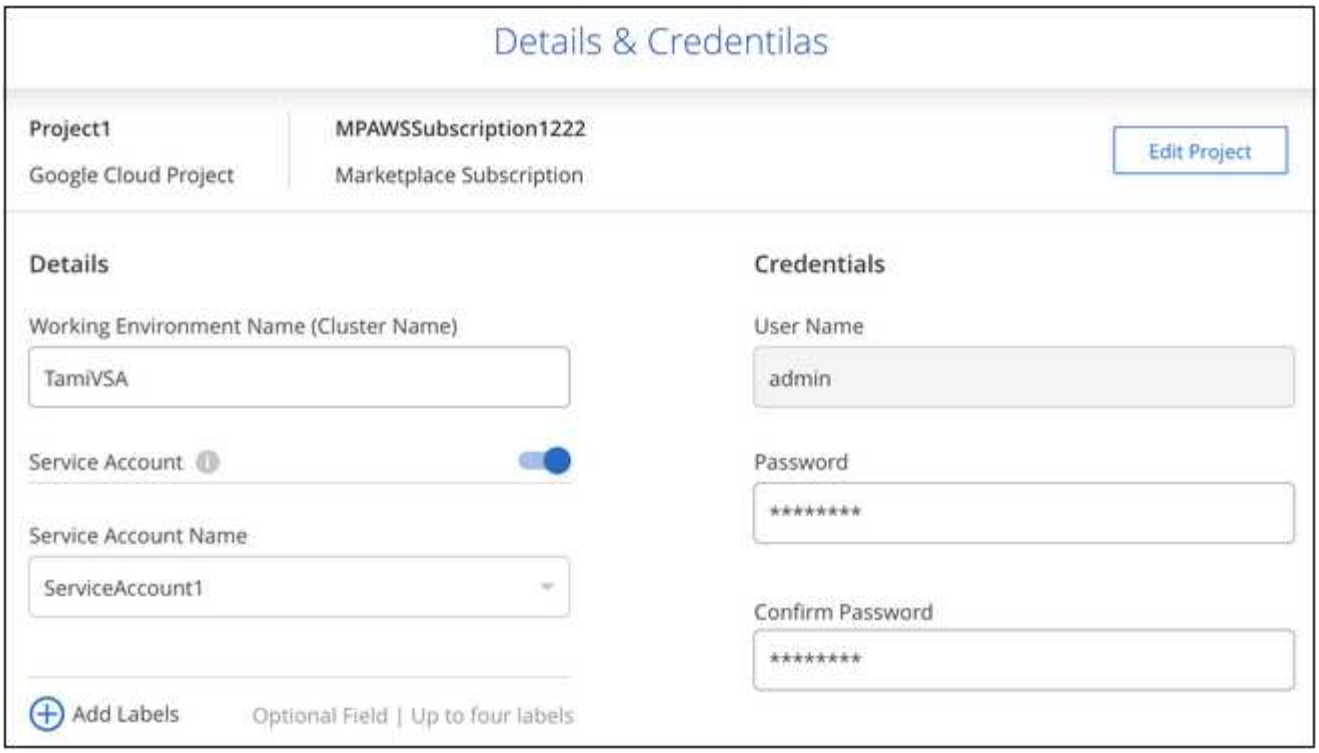
   a. Klicken Sie auf **Projekt bearbeiten** und wählen Sie ein neues Projekt aus, wenn sich das Projekt, das Sie verwenden möchten, von dem Standardprojekt unterscheidet (in dem sich der Connector befindet).

   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. **Leistungen**: Lassen Sie den Cloud Backup 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".

**Ergebnis**

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

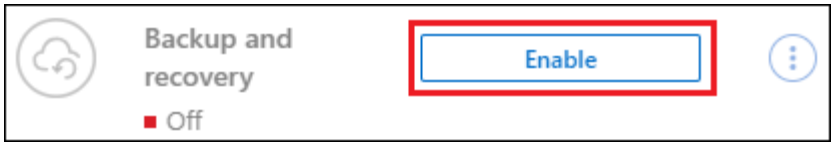
## Aktivierung von Cloud Backup auf einem vorhandenen System

Sie können Cloud Backup jederzeit direkt aus der Arbeitsumgebung aktivieren.

**Schritte**

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

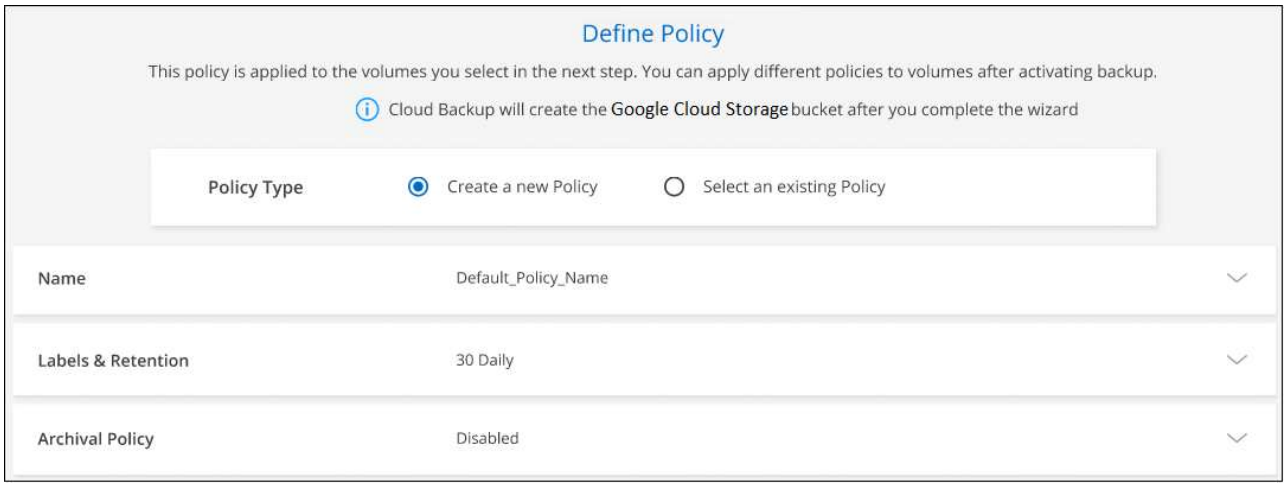
   Wenn das Ziel von Google Cloud Storage für Ihre Backups als Arbeitsumgebung auf dem Canvas existiert, können Sie den Cluster auf die Google Cloud Storage Arbeitsumgebung ziehen, um den Setup-Assistenten zu starten.




2. Wählen Sie das Google Cloud Projekt und die Region aus, in der der Google Cloud Storage Bucket für Backups erstellt werden soll, und klicken Sie auf **Weiter**.

Beachten Sie, dass das Projekt über ein Servicekonto verfügt, das über die vordefinierte Rolle „Speicheradministrator“ verfügt.

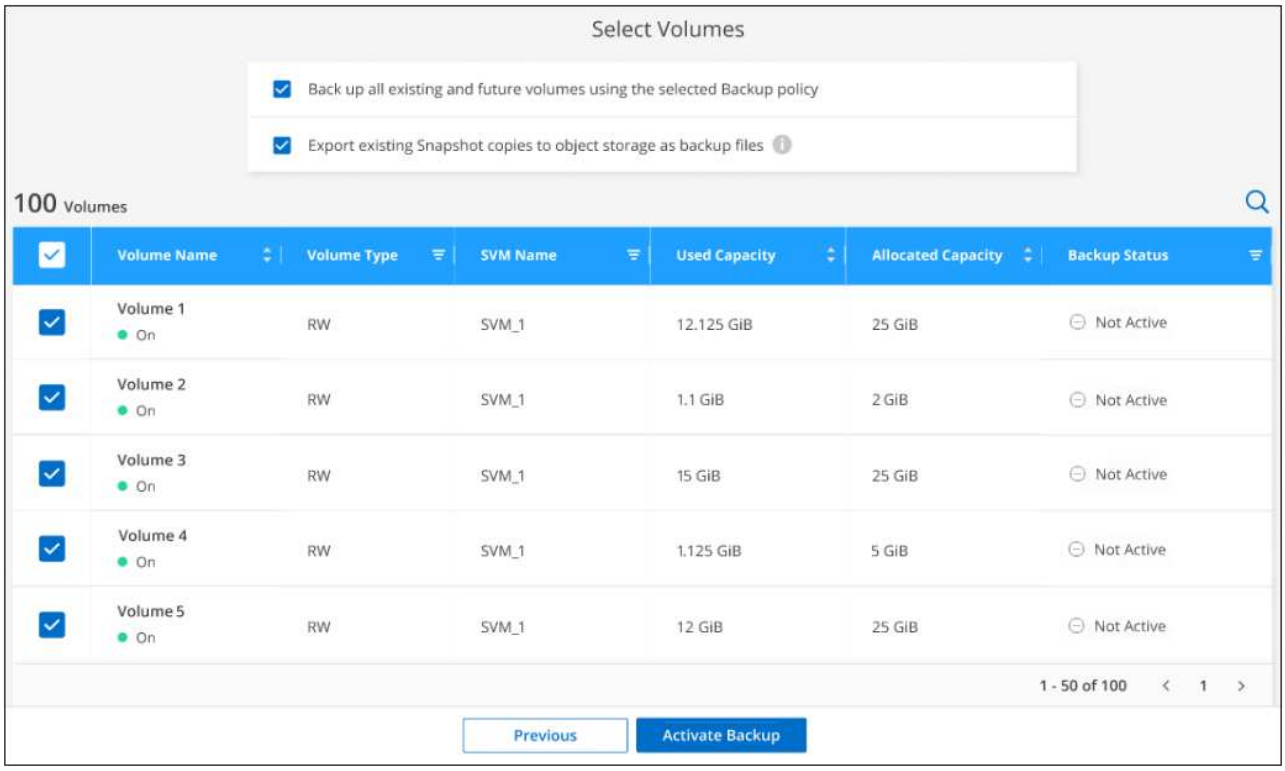
3. Geben Sie die Backup Policy Details ein, die für Ihre Standard Policy verwendet werden, und klicken Sie auf **Weiter**. Sie können eine vorhandene Richtlinie auswählen oder eine neue Richtlinie erstellen, indem Sie in den einzelnen Abschnitten Ihre Auswahl eingeben:
   a. Geben Sie den Namen für die Standardrichtlinie ein. Sie müssen den Namen nicht ändern.
   b. Legen Sie den Backup-Zeitplan fest und wählen Sie die Anzahl der zu behaltenden Backups aus. "Die Liste der vorhandenen Richtlinien, die Sie auswählen können, wird angezeigt".




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

( Volume Name ).

- Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume ( Volume_1 ).




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

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

**Ergebnis**

Ein 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".

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

## 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 von lokalen ONTAP-Daten auf Google Cloud Storage

Unternehmen Sie einige Schritte, um den Backup von Daten von lokalen ONTAP Systemen auf Google Cloud Storage zu starten.

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

## Schnellstart

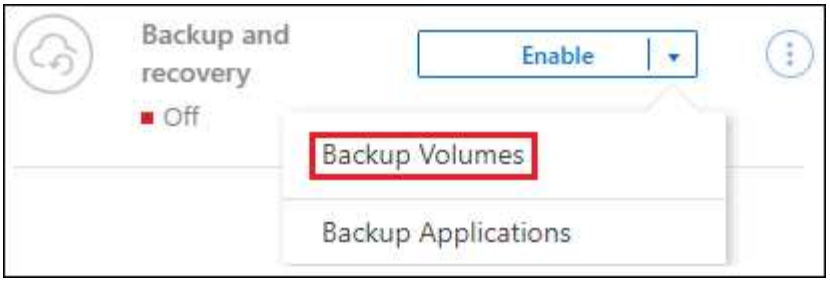
Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

**1 Überprüfen Sie die Unterstützung Ihrer Konfiguration**

- Sie haben den lokalen Cluster erkannt und zu einer Arbeitsumgebung in BlueXP hinzugefügt. Siehe "Erkennung von ONTAP Clustern" Entsprechende Details.
  - Auf dem Cluster läuft ONTAP 9.7P5 oder höher.
  - Das Cluster verfügt über eine SnapMirror Lizenz – es ist im Premium Bundle oder in der Datensicherungs-Bundle enthalten.
  - Der Cluster muss über die erforderlichen Netzwerkverbindungen zum Google-Speicher und zum Connector verfügen.
- Der Connector muss über die erforderlichen Netzwerkverbindungen zum Google-Speicher und zum Cluster verfügen.
- Sie haben ein gültiges Google-Abonnement für den Objektspeicherplatz, in dem sich Ihre Backups befinden.
- Sie verfügen über ein Google-Konto mit einem Zugriffsschlüssel und einem geheimen Schlüssel, damit der ONTAP-Cluster Daten sichern und wiederherstellen kann.

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

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



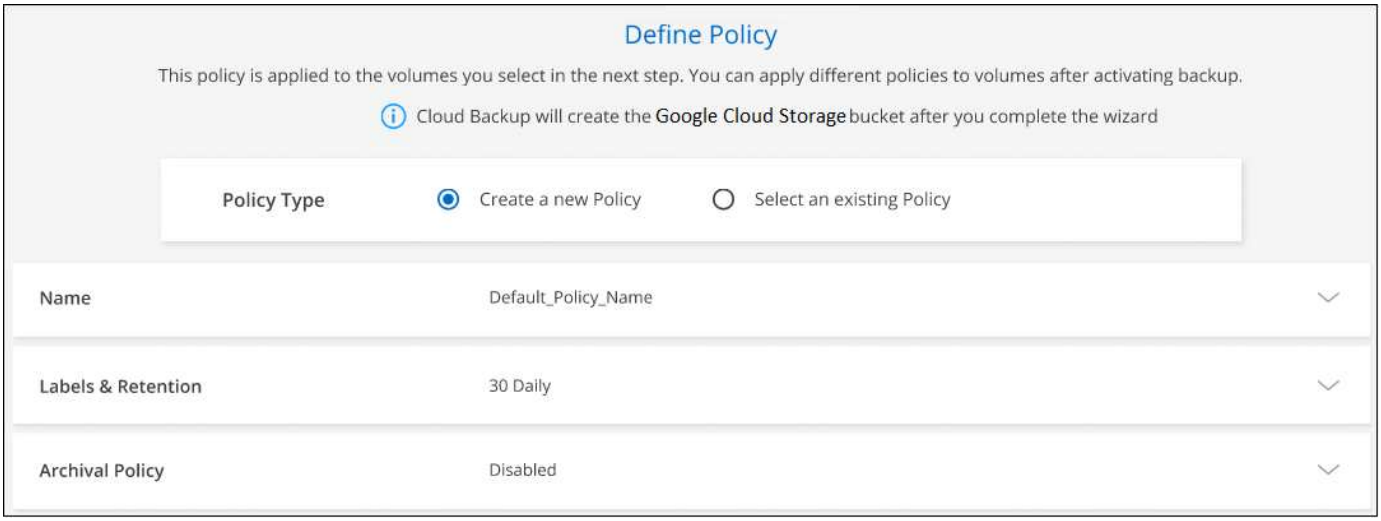

**3** **Wählen Sie den Cloud-Provider aus, und geben Sie die Provider-Details ein**

Wählen Sie Google Cloud als Anbieter aus, und geben Sie dann die Provider-Details ein. Sie müssen außerdem den IPspace im ONTAP Cluster angeben, auf dem sich die Volumes befinden.

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

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

Backups werden standardmäßig im Standard-Storage gespeichert. Falls in Ihrem Cluster ONTAP 9.12.1 oder höher verwendet wird, können Sie das Tiering von Backups nach einer bestimmten Anzahl von Tagen auf Google Archive Storage festlegen, um die Kosten weiter zu optimieren. "Weitere Informationen über die verfügbaren Konfigurationseinstellungen für Cloud Backup-Richtlinien".




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

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

## Anforderungen

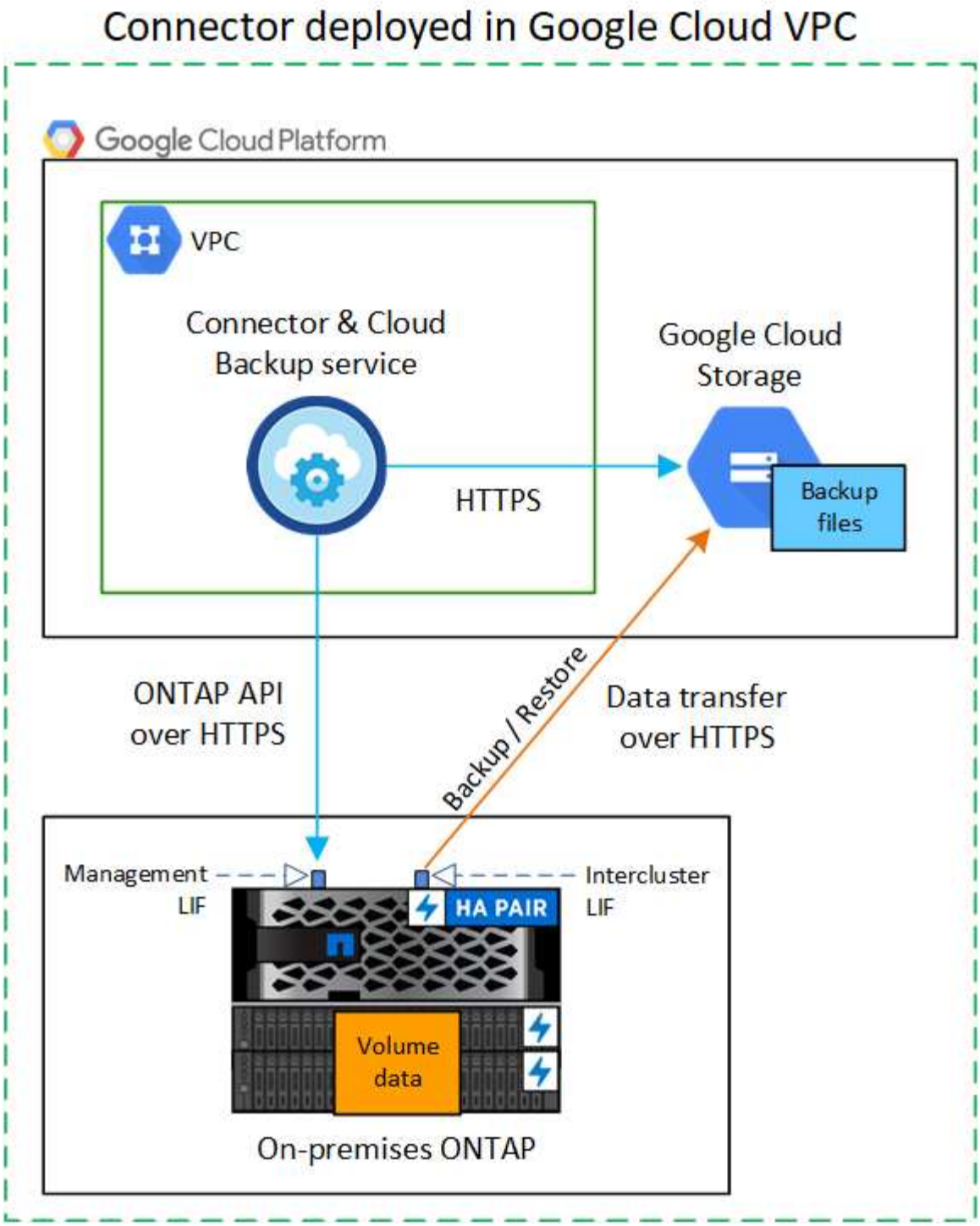
Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration

verfügen, bevor Sie mit dem Backup von On-Premises-Volumes in Google Cloud Storage beginnen.

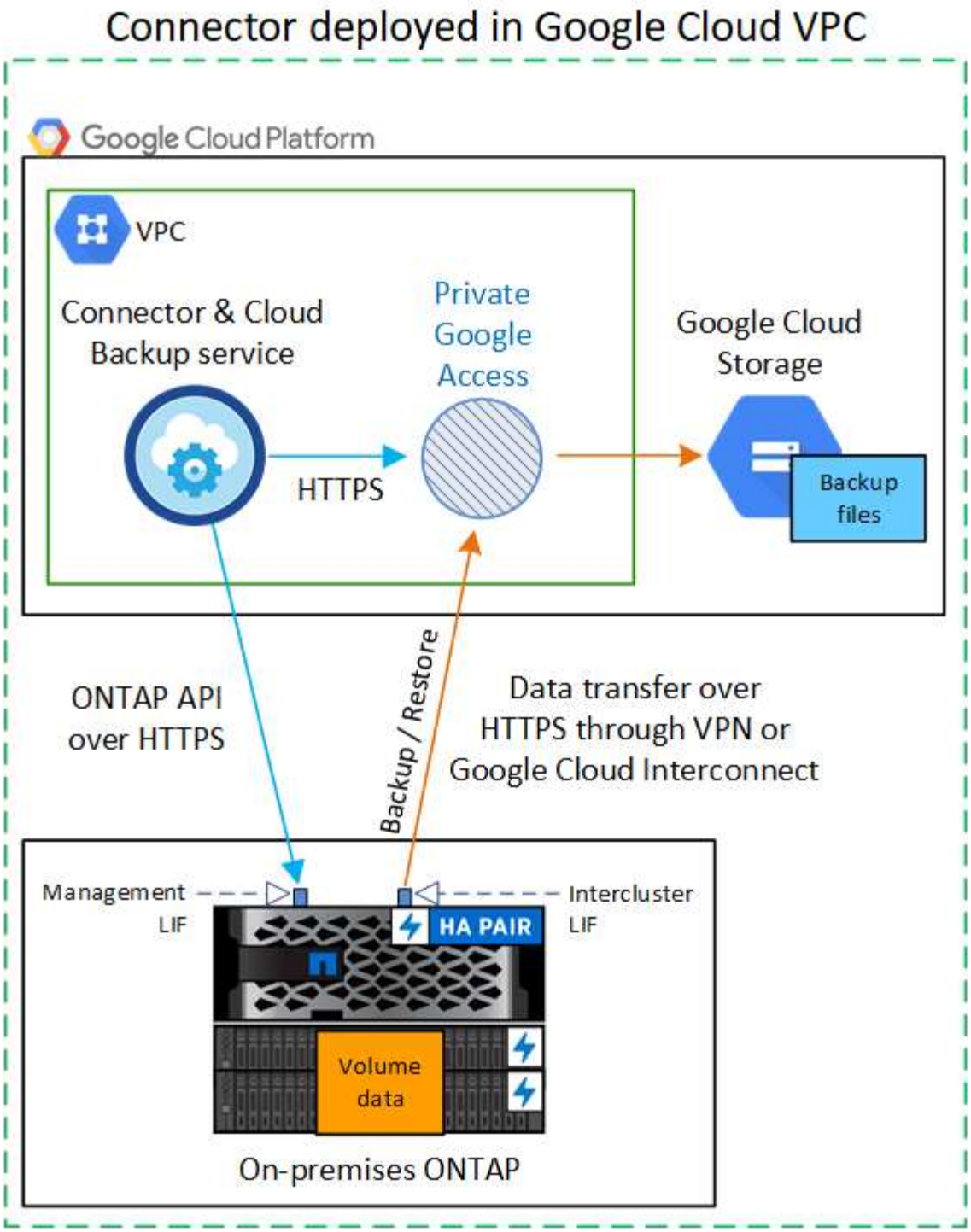
Bei der Konfiguration von Backups von lokalen ONTAP Systemen in Google Cloud Storage stehen zwei Verbindungsmethoden zur Verfügung.

- Öffentliche Verbindung: Über einen öffentlichen Google-Endpunkt wird das ONTAP-System direkt mit Google Cloud-Storage verbunden.
- 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.

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.




**Vorbereiten der ONTAP Cluster**

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

"Entdecken Sie ein Cluster".

**ONTAP-Anforderungen erfüllt**

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

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

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

- Zeit und Zeitzone sind korrekt eingestellt.

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

### Netzwerkanforderungen für Cluster

- Das ONTAP Cluster initiiert eine HTTPS-Verbindung über Port 443 von der Intercluster-LIF zu Google Cloud 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 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 Cloud Backup einrichten, werden Sie aufgefordert, den IP-Speicherplatz zu verwenden. Sie sollten den IPspace auswählen, dem jede LIF zugeordnet ist. Dies kann der „Standard“-IPspace oder ein benutzerdefinierter IPspace sein, den Sie erstellt haben.

- Die Intercluster-LIFs der Nodes können auf den Objektspeicher zugreifen.
- 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 auf Punkt storage.googleapis.com auf die richtige interne (private) IP-Adresse verweisen.

- 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. Firewall-Regeln, um Cloud Backup Service-Verbindungen von ONTAP zu Objektspeicher über Port 443 und Datenverkehr zur Namensauflösung von der Storage VM zum DNS-Server über Port 53 (TCP/UDP) zu ermöglichen.

### Erstellen oder Umschalten 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 Standort 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"
- "Erste Schritte mit den Anschlüssen"
- "Installieren eines Steckers in GCP"

### Vorbereiten der Vernetzung für den Connector

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

#### Schritte

1. Stellen Sie sicher, dass das Netzwerk, in dem der Connector installiert ist, folgende Verbindungen ermöglicht:
   - Eine ausgehende Internetverbindung zum Cloud Backup Service über Port 443 (HTTPS)
   - Eine HTTPS-Verbindung über Port 443 zu Ihrem Google Cloud-Speicher
   - 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, dass sie Punkt www.googleapis.com und storage.googleapis.com auf die korrekten internen (privaten) IP-Adressen verweisen.

### Überprüfen oder Hinzufügen von Berechtigungen zum Konnektor

Um die Cloud Backup Funktion „Search & Restore“ nutzen zu können, benötigen Sie spezielle Berechtigungen in der Rolle für den Connector, damit er 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. In "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. Klicken Sie auf eine benutzerdefinierte Rolle.
4. Klicken Sie auf **Rolle bearbeiten**, um die Berechtigungen der Rolle zu aktualisieren.
5. Klicken Sie auf **Berechtigungen hinzufügen**, um der Rolle folgende neue 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. Klicken Sie auf **Aktualisieren**, um die bearbeitete Rolle zu speichern.

### Lizenzanforderungen prüfen

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

  Backups von On-Premises-Systemen in Google Cloud Storage lassen sich in allen Regionen erstellen "Wobei Cloud Volumes ONTAP unterstützt wird". Sie geben die Region an, in der Backups beim Einrichten des Dienstes gespeichert werden sollen.

### Google Cloud Storage wird für Backups vorbereitet

Wenn Sie ein Backup einrichten, müssen Sie Speicherzugriffsschlüssel für ein Servicekonto mit Storage Admin-Berechtigungen bereitstellen. Mithilfe eines Service-Kontos kann Cloud Backup zum Speichern von Backups Cloud-Storage-Buckets authentifizieren und auf diese zugreifen. Die Schlüssel sind erforderlich, damit Google Cloud Storage weiß, wer die Anfrage stellt.

#### Schritte

1. "Erstellen Sie ein Servicekonto mit der vordefinierten Rolle „Storage Admin“".
2. Gehen Sie zu "GCP-Speichereinstellungen" Außerdem Zugriffsschlüssel für das Servicekonto erstellen:
   a. Wählen Sie ein Projekt aus, und klicken Sie auf **Interoperabilität**. Falls Sie dies noch nicht getan haben, klicken Sie auf **Interoperabilitätszugriff aktivieren**.
   b. Klicken Sie unter **Zugriffsschlüssel für Servicekonten** auf **Schlüssel für ein Servicekonto erstellen**, wählen Sie das gerade erstellte Servicekonto aus und klicken Sie auf **Schlüssel erstellen**.

      Wenn Sie den Backup-Service konfigurieren, müssen Sie die Schlüssel später in Cloud Backup eingeben.

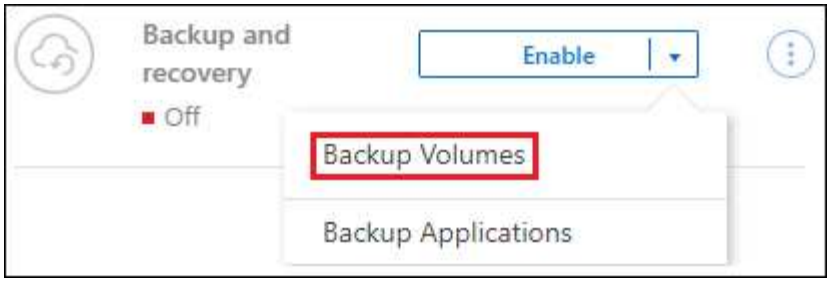
## Unterstützung Von Cloud Backup

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

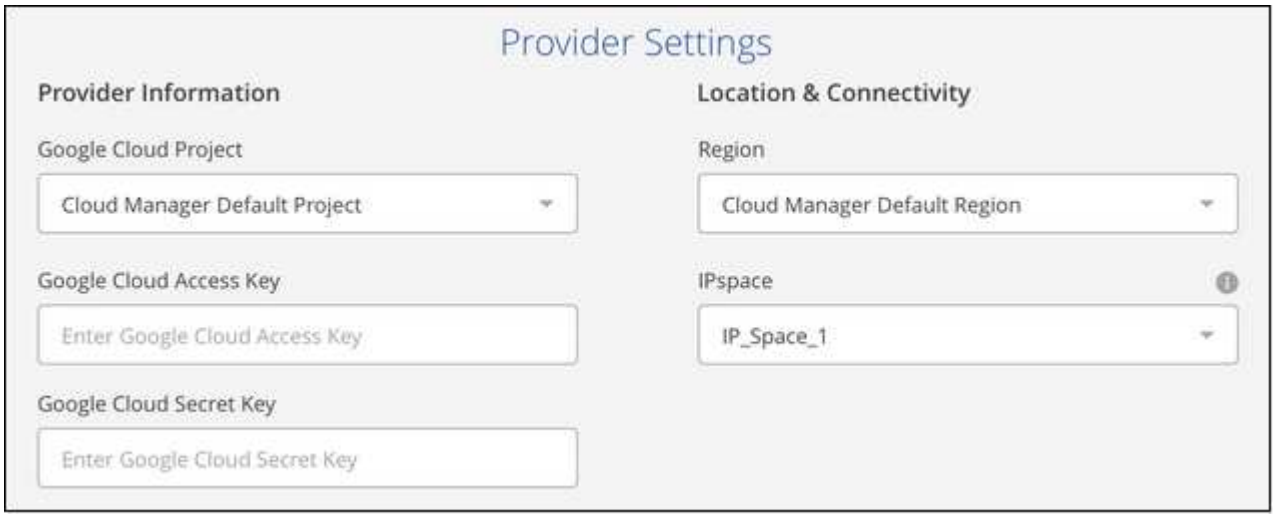
#### Schritte

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

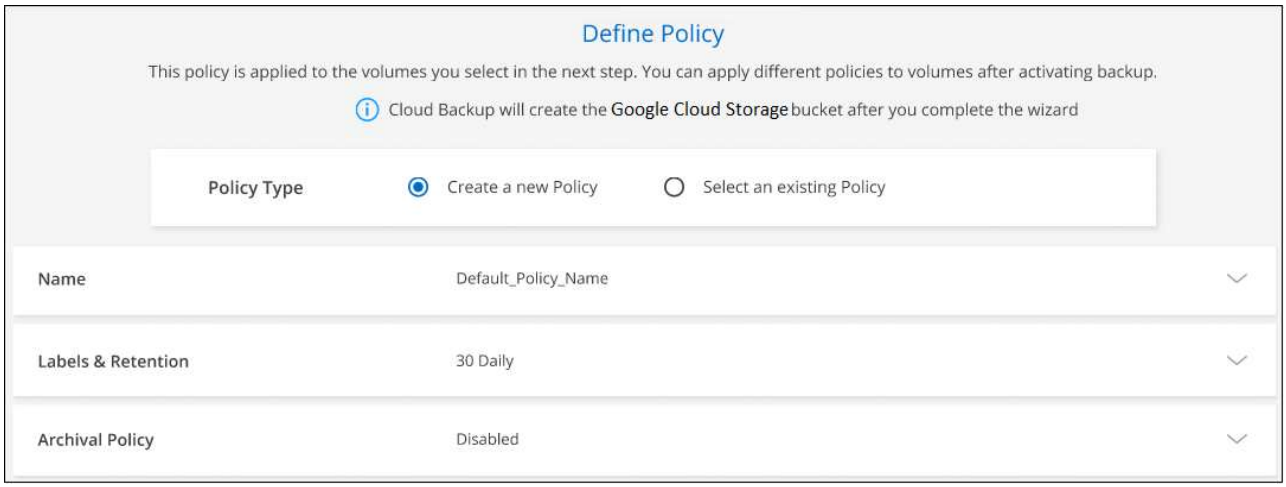
   Wenn das Ziel von Google Cloud Storage für Ihre Backups als Arbeitsumgebung auf dem Canvas existiert, können Sie den Cluster auf die Google Cloud Storage Arbeitsumgebung ziehen, um den Setup-Assistenten zu starten.



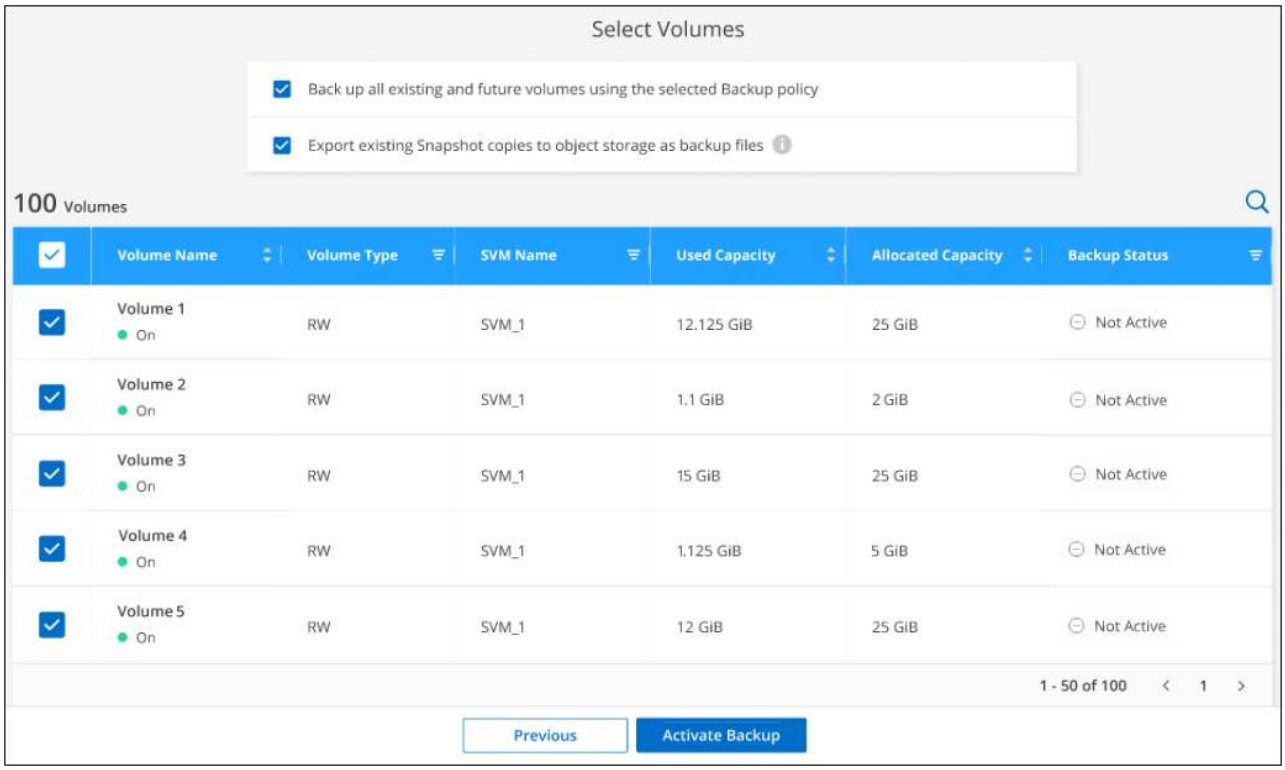

2. Wählen Sie Google Cloud als Anbieter und klicken Sie auf **Weiter**.
3. Geben Sie die Provider-Daten ein und klicken Sie auf **Weiter**.
   a. Das Google Cloud Projekt, an dem der Google Cloud Storage Bucket für Backups erstellt werden soll. (Das Projekt muss über ein Service-Konto verfügen, das über die vordefinierte Rolle „Storage Admin“ verfügt.)
   b. Der Google-Zugriffsschlüssel und der geheime Schlüssel zum Speichern der Backups.
   c. Der Google-Bereich, in dem die Backups gespeichert werden.
   d. Der IPspace im ONTAP Cluster, in dem sich die Volumes, die Sie sichern möchten, befinden. Die Intercluster-LIFs für diesen IPspace müssen über Outbound-Internetzugang verfügen.




4. Wenn Sie für Ihr Konto keine Lizenz für Cloud Backup besitzen, werden Sie zu diesem Zeitpunkt aufgefordert, die gewünschte Gebührenart auszuwählen. Sie können ein Pay-as-you-go (PAYGO) Marketplace-Angebot von BlueXP bei Google abonnieren (oder bei mehreren Abonnements eine auswählen) oder eine Cloud Backup BYOL-Lizenz von NetApp erwerben und aktivieren. "Erfahren Sie, wie Sie Cloud Backup-Lizenzen einrichten."
5. Geben Sie die Backup Policy Details ein, die für Ihre Standard Policy verwendet werden, und klicken Sie auf **Weiter**. Sie können eine vorhandene Richtlinie auswählen oder eine neue Richtlinie erstellen, indem Sie in den einzelnen Abschnitten Ihre Auswahl eingeben:
   a. Geben Sie den Namen für die Standardrichtlinie ein. Sie müssen den Namen nicht ändern.
   b. Legen Sie den Backup-Zeitplan fest und wählen Sie die Anzahl der zu behaltenden Backups aus. "Die Liste der vorhandenen Richtlinien, die Sie auswählen können, wird angezeigt".
   c. Bei Verwendung von ONTAP 9.12.1 oder neuer können Sie Backups nach einer bestimmten Anzahl von Tagen im Archiv-Storage Tiering zuweisen, um die Kosten weiter zu optimieren. "Weitere Informationen über die verfügbaren Konfigurationseinstellungen für Cloud Backup-Richtlinien".




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




   - Wenn es lokale Snapshot-Kopien für Lese-/Schreib-Volumes in dieser Arbeitsumgebung gibt, die dem Backup-Schedule-Label entsprechen, das Sie gerade für diese Arbeitsumgebung ausgewählt haben (z. B. täglich, wöchentlich usw.), wird eine zusätzliche Eingabeaufforderung angezeigt: „Export

vorhandener Snapshot Kopien in Objekt-Storage als Backup-Kopien“. Aktivieren Sie dieses Kontrollkästchen, wenn alle historischen Snapshots als Backup-Dateien in Objekt-Storage kopiert werden sollen, um sicherzustellen, dass die umfassendste Sicherung für Ihre Volumes gewährleistet ist.

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

**Ergebnis**

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".

## 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 von lokalen ONTAP Daten in StorageGRID

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

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

## Schnellstart

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

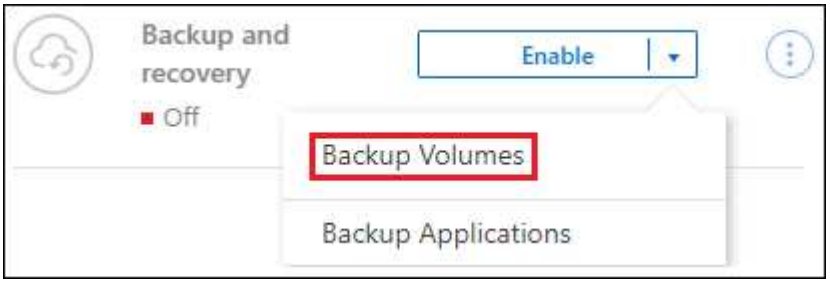
### 1 Überprüfen Sie die Unterstützung Ihrer Konfiguration

- Sie haben den lokalen Cluster erkannt und zu einer Arbeitsumgebung in BlueXP hinzugefügt. Siehe "Erkennung von ONTAP Clustern" Entsprechende Details.
  - Auf dem Cluster läuft ONTAP 9.7P5 oder höher.
  - Das Cluster verfügt über eine SnapMirror Lizenz – es ist im Premium Bundle oder in der Datensicherungs-Bundle enthalten.
  - Der Cluster muss über die erforderlichen Netzwerkverbindungen zu StorageGRID und zum Connector verfügen.

- Sie haben einen Connector auf Ihrem Gelände installiert.
  - Der Connector kann auf einer Website mit oder ohne Internetzugang installiert werden.
  - Das Networking für den Connector ermöglicht eine ausgehende HTTPS-Verbindung zum ONTAP-Cluster und zu StorageGRID.
- Sie haben gekauft "Und aktiviert" Eine Cloud Backup BYOL-Lizenz von NetApp
- Ihre StorageGRID hat Version 10.3 oder höher mit Zugriffsschlüsseln, die S3-Berechtigungen aufweisen.

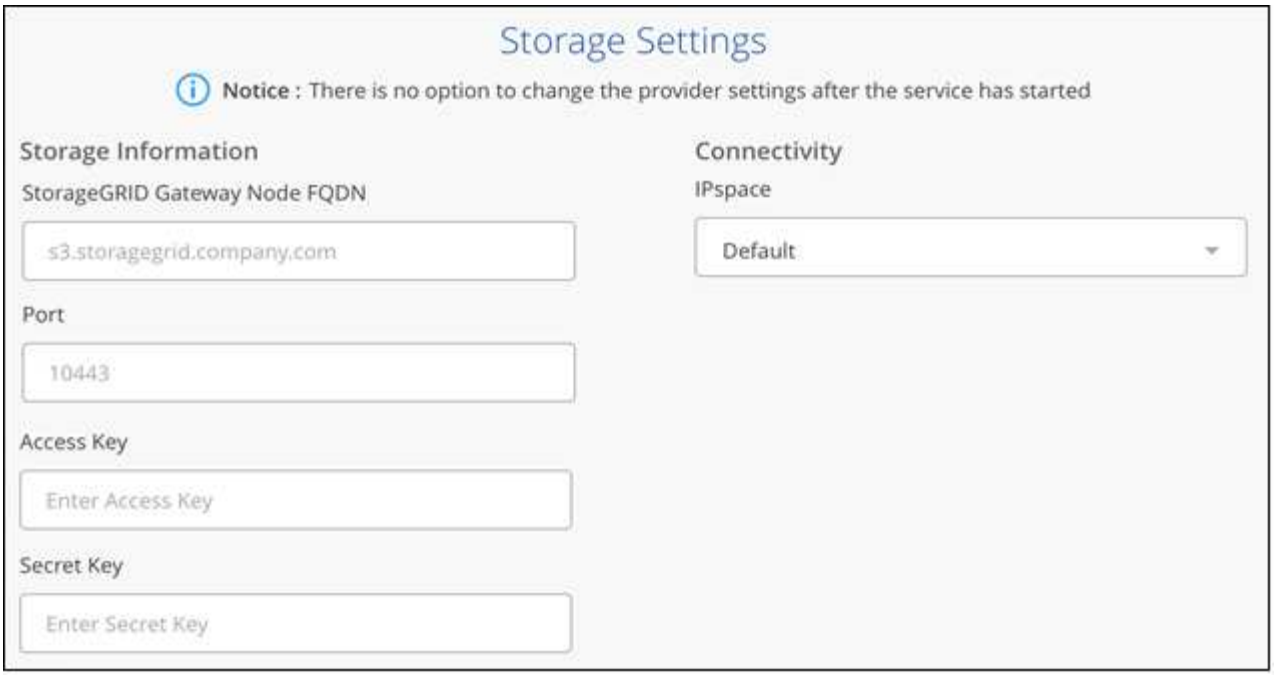
**2** **Aktivieren Sie Cloud Backup auf dem System**

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




**3** **Geben Sie die Details zum StorageGRID ein**

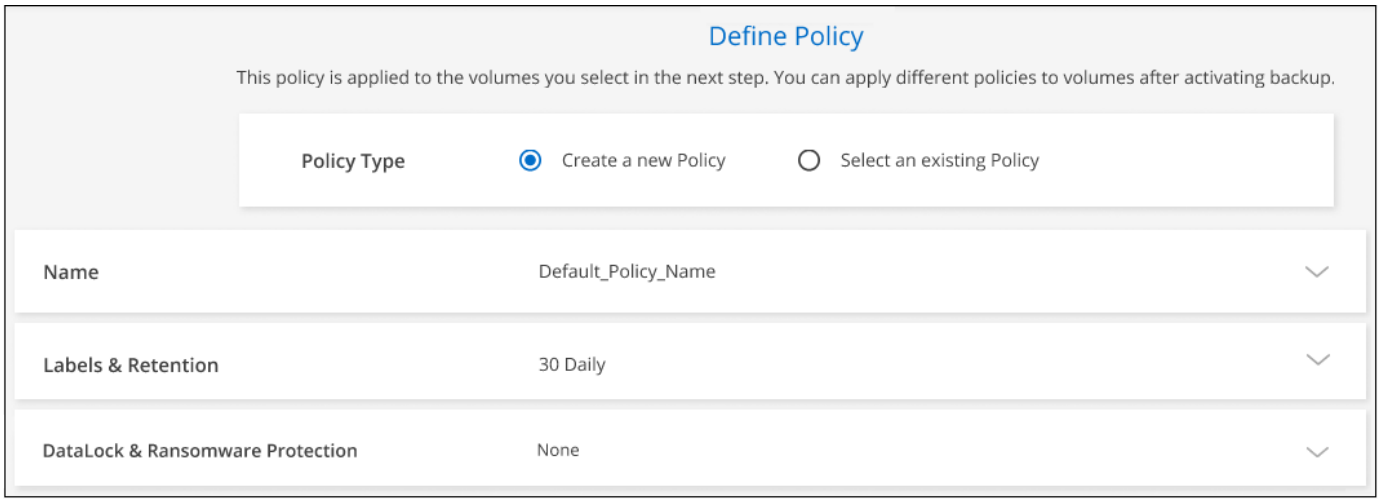
Wählen Sie als Provider StorageGRID aus, und geben Sie dann die Details zum StorageGRID-Server und dem S3-Mandantenkonto ein. Sie müssen außerdem den IPspace im ONTAP Cluster angeben, auf dem sich die Volumes befinden.




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

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

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




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

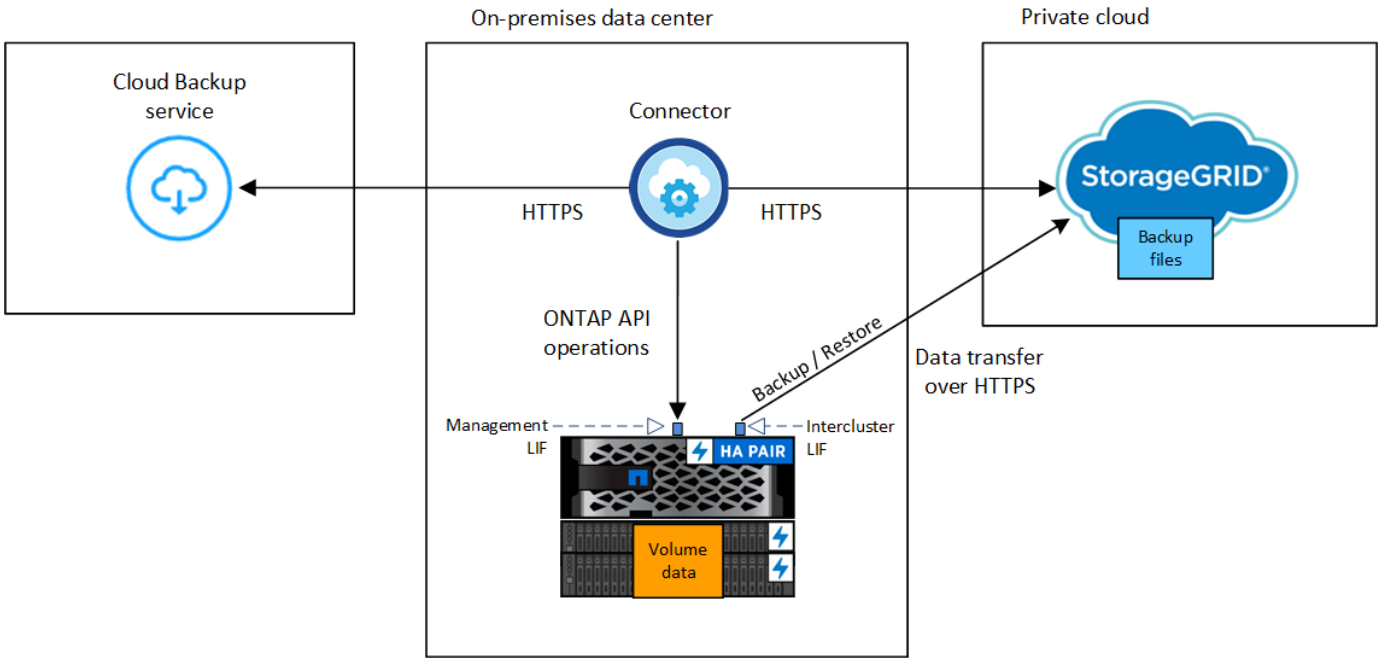
Legen Sie auf der Seite Volumes auswählen fest, welche Volumes gesichert werden sollen. Verwenden Sie dazu die Standard-Backup-Richtlinie. Um bestimmten Volumes unterschiedliche Backup-Richtlinien zuzuweisen, können Sie weitere Richtlinien erstellen und diese später auf Volumes anwenden.

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

## Anforderungen

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

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




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

### Vorbereiten der ONTAP Cluster

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

"Entdecken Sie ein Cluster".

### ONTAP-Anforderungen erfüllt

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

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

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

- Zeit und Zeitzone sind korrekt eingestellt.

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

### Netzwerkanforderungen für Cluster

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

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

- ONTAP erfordert eine eingehende Verbindung vom Connector zur Cluster-Management-LIF. Der Stecker muss sich in Ihrem Haus befinden.
- Auf jedem ONTAP Node ist eine Intercluster-LIF erforderlich, die die Volumes hostet, die Sie sichern

möchten. Die LIF muss dem *IPspace* zugewiesen sein, den ONTAP zur Verbindung mit Objekt-Storage verwenden sollte. "Erfahren Sie mehr über IPspaces".

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

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

### StorageGRID wird vorbereitet

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

#### Unterstützte StorageGRID-Versionen

StorageGRID 10.3 und höher wird unterstützt.

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

#### S3-Anmeldedaten

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

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

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

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

#### Objektversionierung

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

### Erstellen oder Umschalten von Anschlüssen

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

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

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

### Vorbereiten der Vernetzung für den Connector

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

#### Schritte

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

### Lizenzanforderungen

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

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

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

## Unterstützung von Cloud Backup für StorageGRID

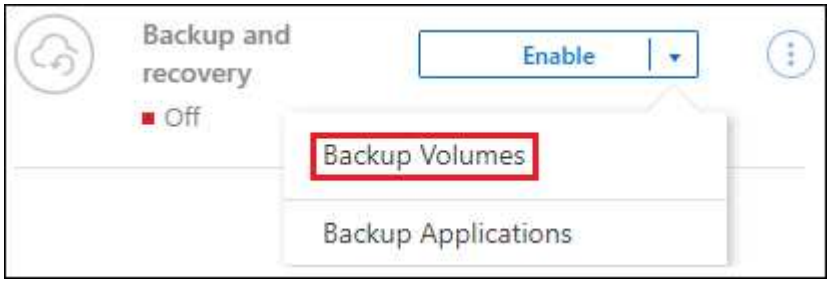
Cloud Backup kann jederzeit direkt aus der lokalen Arbeitsumgebung aktiviert werden.

#### Schritte

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

   Wenn das StorageGRID Ziel für Ihre Backups als eine Arbeitsumgebung auf dem Canvas existiert, können

Sie den Cluster auf die StorageGRID Arbeitsumgebung ziehen, um den Setup-Assistenten zu starten.




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

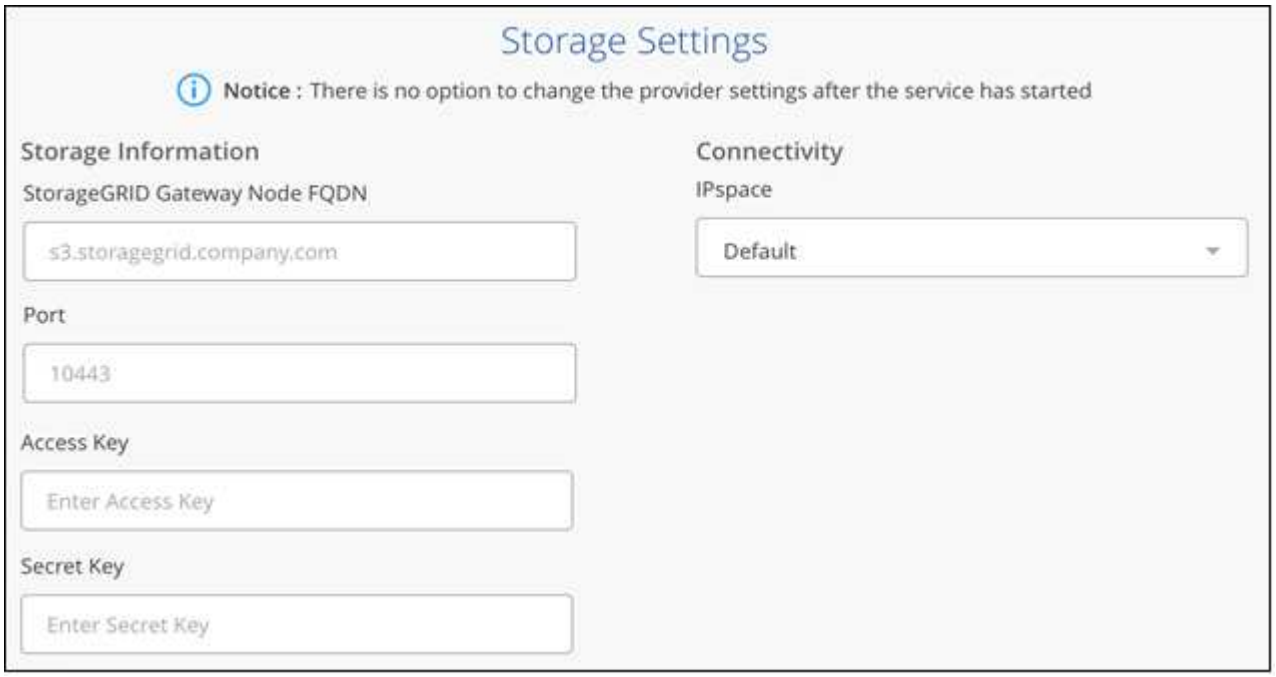
   a. Der FQDN des StorageGRID-Gateway-Knotens.

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

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

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

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

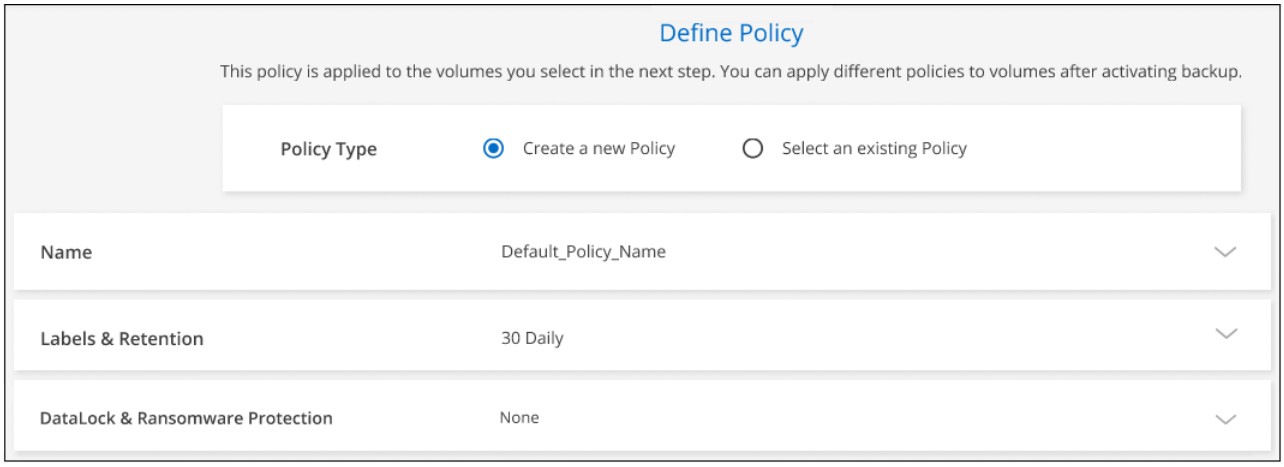



3. Geben Sie die Backup Policy Details ein, die für Ihre Standard Policy verwendet werden, und klicken Sie auf **Weiter**. Sie können eine vorhandene Richtlinie auswählen oder eine neue Richtlinie erstellen, indem Sie in den einzelnen Abschnitten Ihre Auswahl eingeben:

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

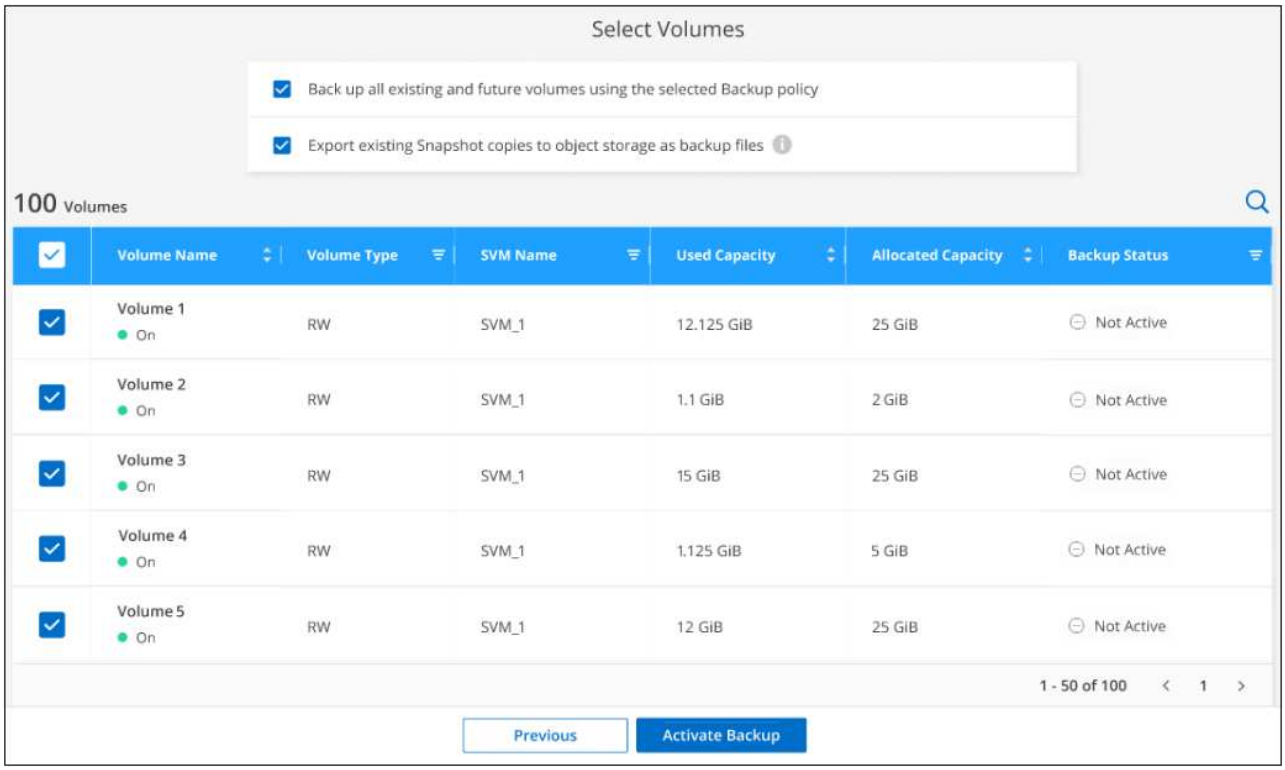
   b. Legen Sie den Backup-Zeitplan fest und wählen Sie die Anzahl der zu behaltenden Backups aus. "Die Liste der vorhandenen Richtlinien, die Sie auswählen können, wird angezeigt".

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




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

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




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

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

**Ergebnis**

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

## Was kommt als Nächstes?

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

# Verwalten von Backups für Ihre ONTAP Systeme

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

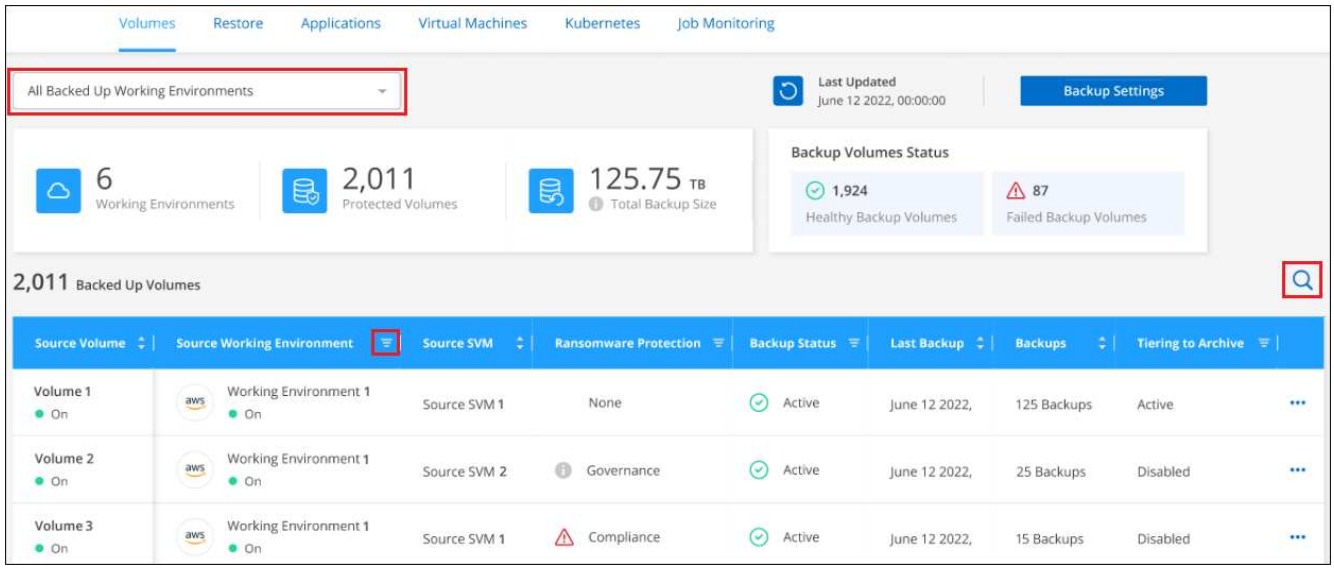
> Backup-Dateien lassen sich nicht direkt in der Umgebung Ihrer Cloud-Provider managen oder ändern. Dies kann die Dateien beschädigen und zu einer nicht unterstützten Konfiguration führen.

## Anzeigen der Volumes, die gesichert werden

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

**Schritte**

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




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

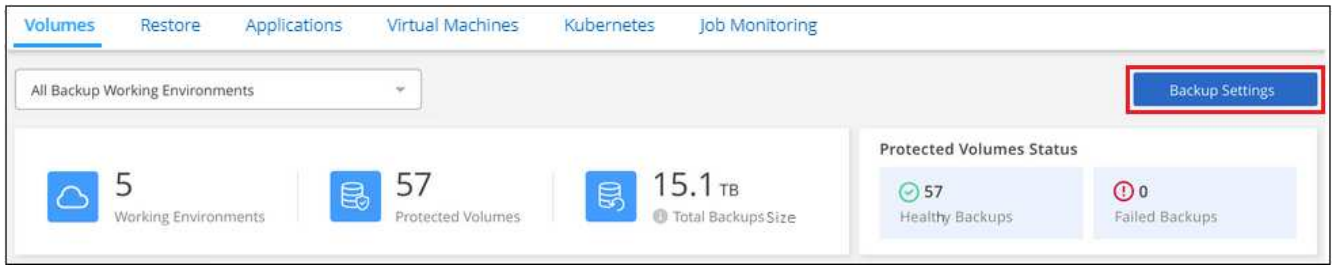
## Aktivieren und Deaktivieren von Backups von Volumes

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

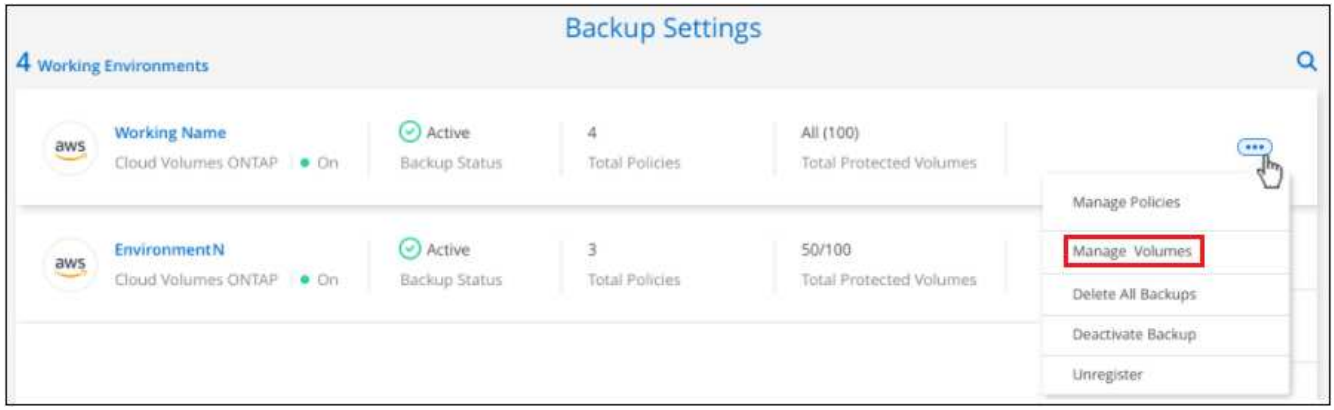
Sie können Backups für Volumes deaktivieren, sodass keine weiteren Backups erstellt werden. Dadurch wird auch die Möglichkeit deaktiviert, Volume-Daten aus einer Sicherungsdatei wiederherzustellen. So können Sie im Prinzip alle Backup- und Wiederherstellungsaktivitäten für einen bestimmten Zeitraum anhalten.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

**Schritte**

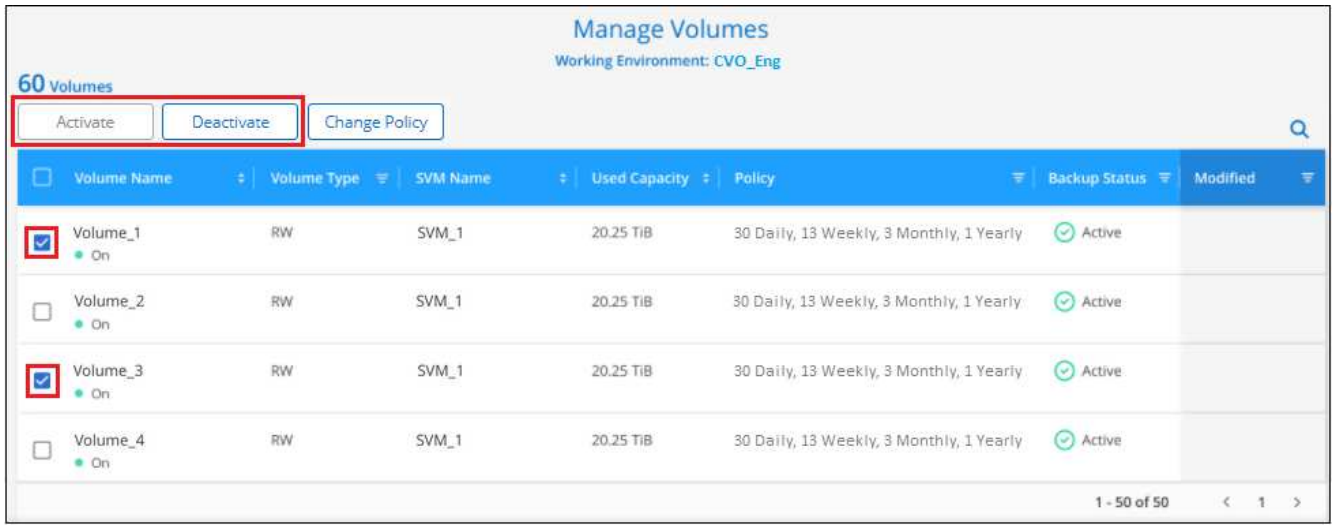
1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.




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




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




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

## Bearbeiten einer vorhandenen Backup-Richtlinie

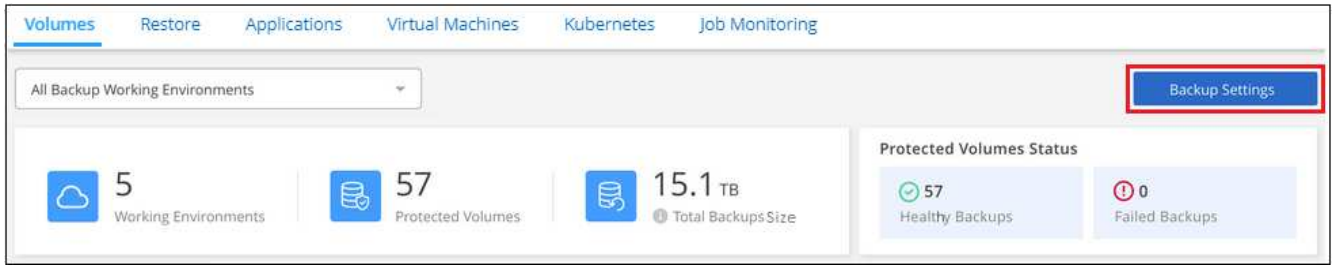
Sie können die Attribute für eine Backup-Richtlinie ändern, die derzeit auf Volumes in einer Arbeitsumgebung angewendet wird. Die Änderung der Backup-Richtlinie wirkt sich auf alle vorhandenen Volumes aus, die diese

Richtlinie verwenden.

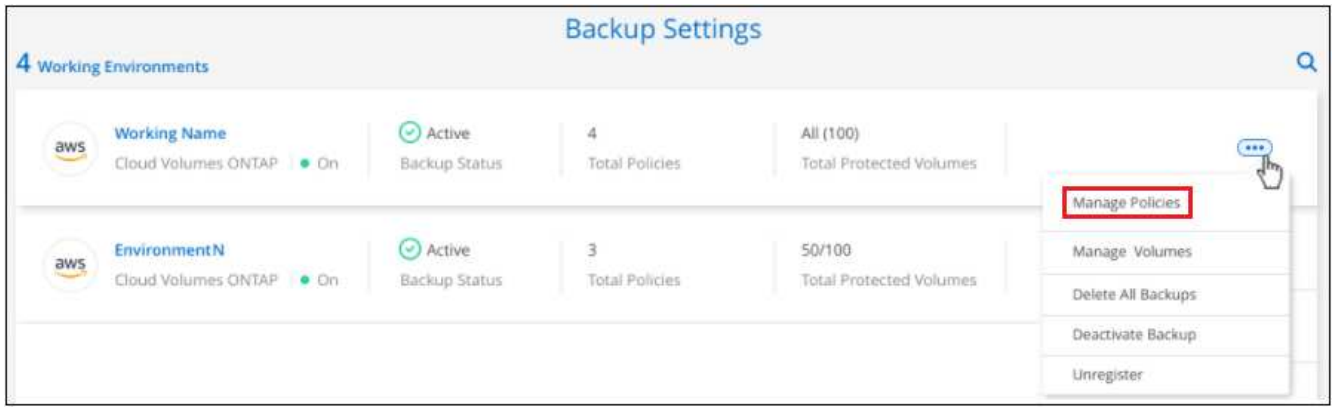
- Wenn Sie bei der Aktivierung von Cloud Backup für diesen Cluster *DataLock und Ransomware Protection* aktiviert haben, müssen alle Richtlinien, die Sie bearbeiten, mit derselben DataLock-Einstellung (Governance oder Compliance) konfiguriert werden. Und wenn Sie *DataLock und Ransomware Protection*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

**Schritte**

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

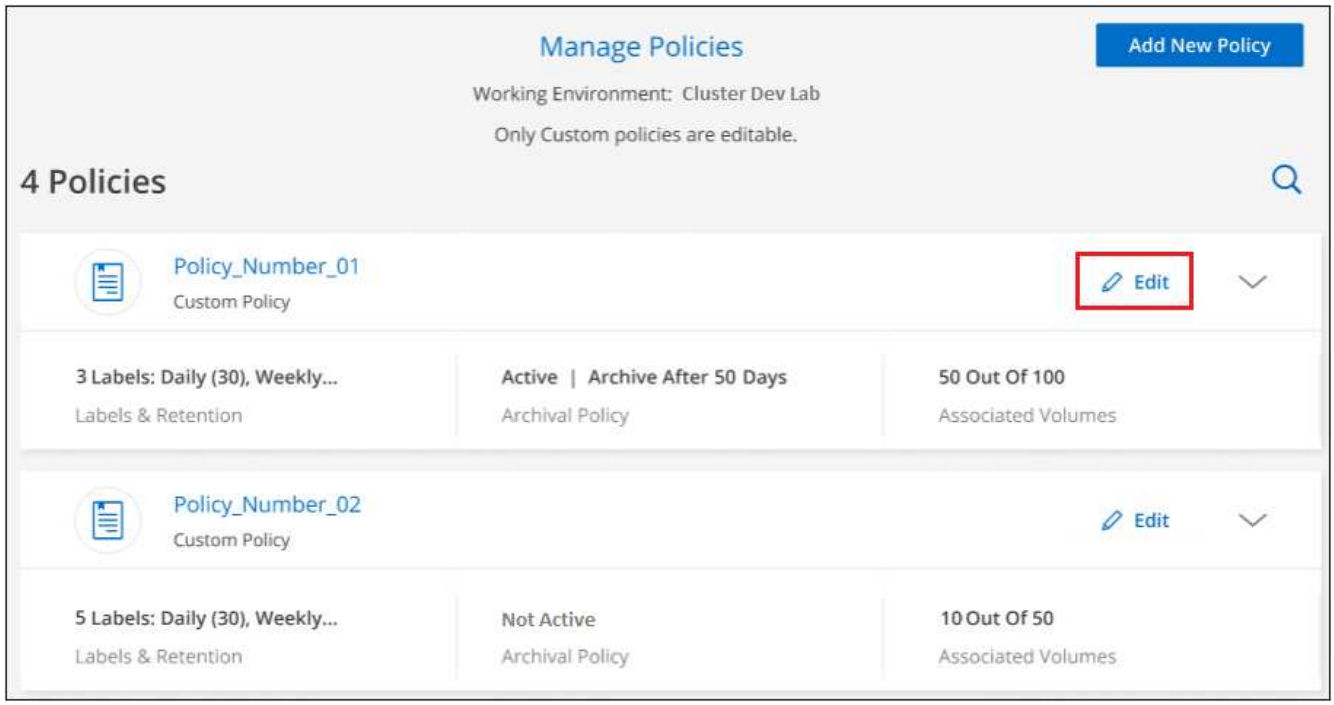



2. Klicken Sie auf der Seite „ Backup Settings_“ auf ••• Wählen Sie für die Arbeitsumgebung, in der Sie die Richtlinieneinstellungen ändern möchten, und wählen Sie **Richtlinien verwalten**.

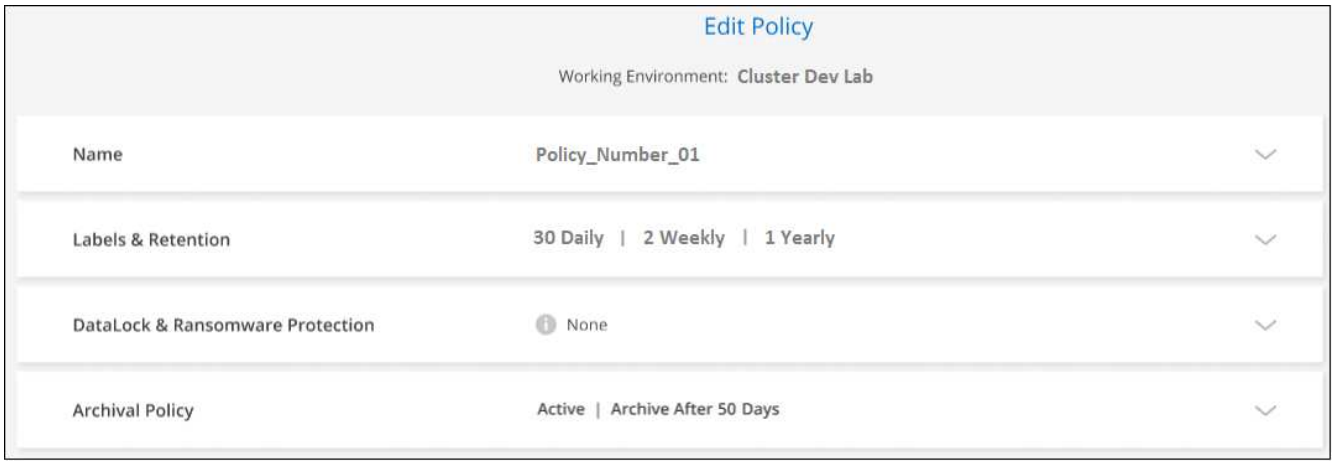



3. Klicken Sie auf der Seite *Policies verwalten* auf **Bearbeiten** für die Backup-Policy, die Sie in dieser Arbeitsumgebung ändern möchten.

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

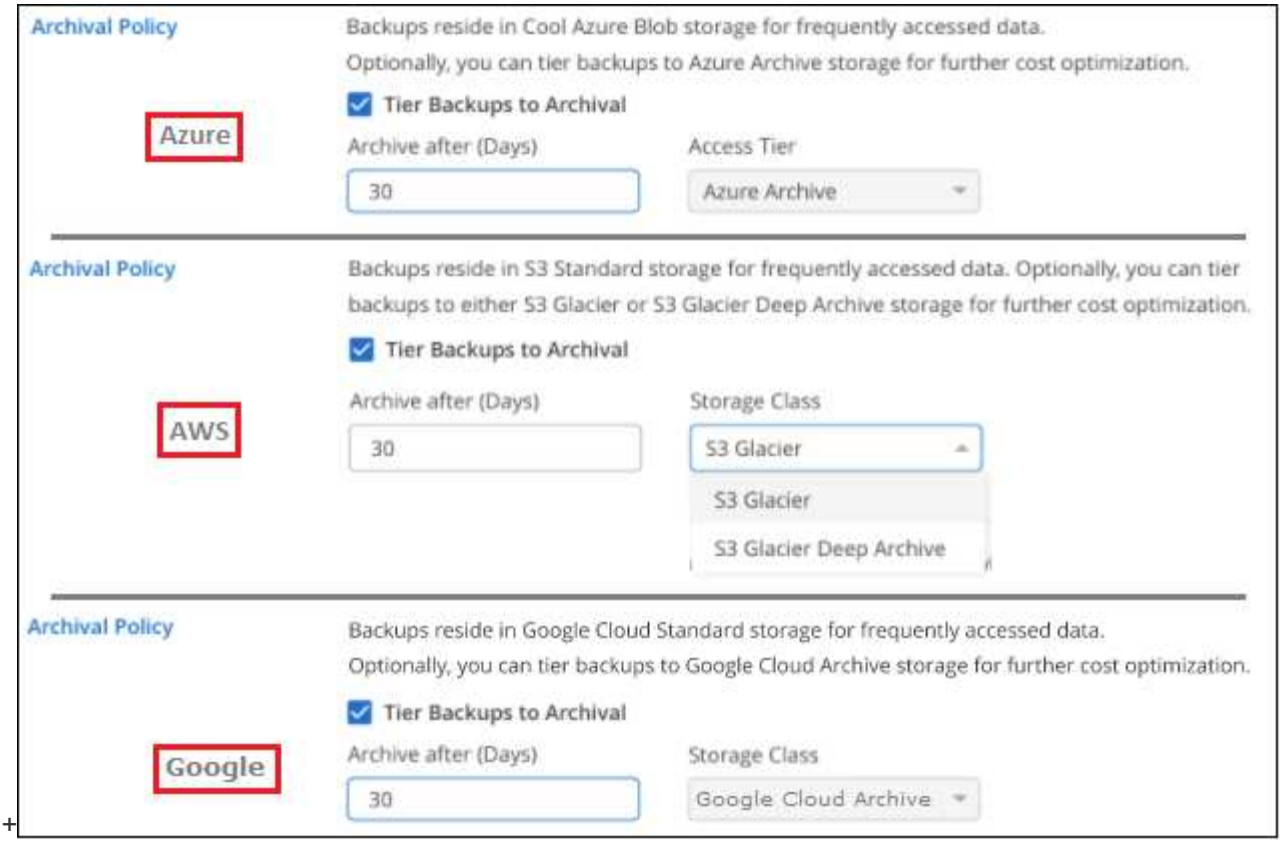



4. Klicken Sie auf der Seite *Edit Policy* auf ⌄ Erweitern Sie den Abschnitt *Labels & Retention*, um den Zeitplan und/oder die Backup-Aufbewahrung zu ändern, und klicken Sie auf **Speichern**.




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

"Erfahren Sie mehr über die Verwendung von 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.

## Hinzufügen einer neuen Backup-Richtlinie

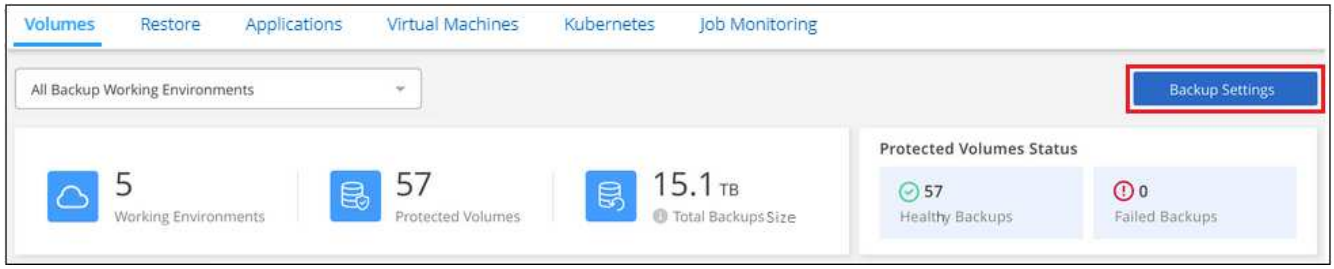
Wenn Sie Cloud-Backup für eine Arbeitsumgebung aktivieren, werden alle ausgewählten Volumes mit der von Ihnen definierten Standard-Backup-Richtlinie gesichert. Um bestimmten Volumes mit verschiedenen Recovery Point Objectives (RPOs) unterschiedliche Backup-Richtlinien zuzuweisen, können Sie zusätzliche Richtlinien für diesen Cluster erstellen und diese Richtlinien anderen Volumes zuweisen.

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

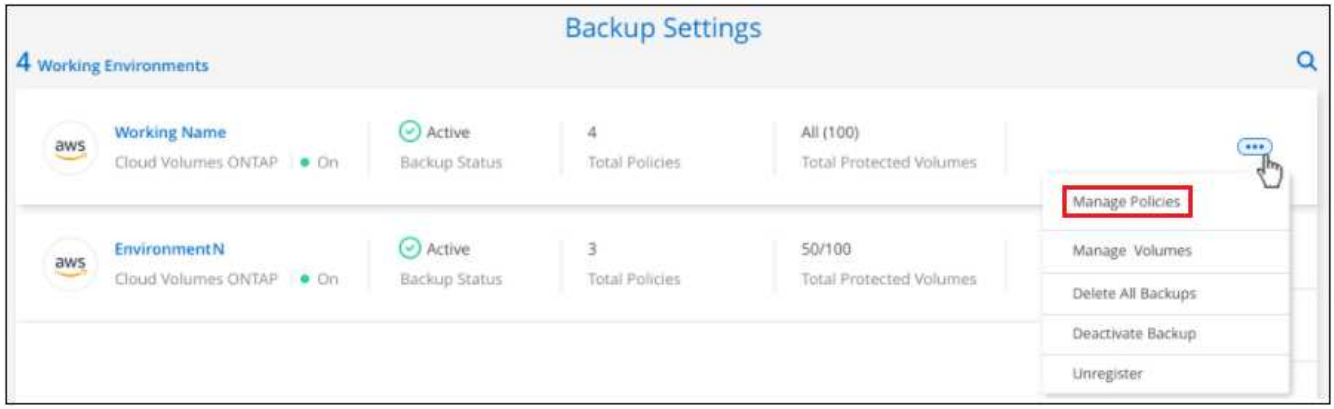
- Wenn Sie bei der Aktivierung von Cloud Backup für diesen Cluster *DataLock und Ransomware Protection* aktiviert haben, müssen alle von Ihnen erstellten zusätzlichen Richtlinien mit derselben DataLock-Einstellung (Governance oder Compliance) konfiguriert werden. Und wenn Sie bei der Aktivierung von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

**Schritte**

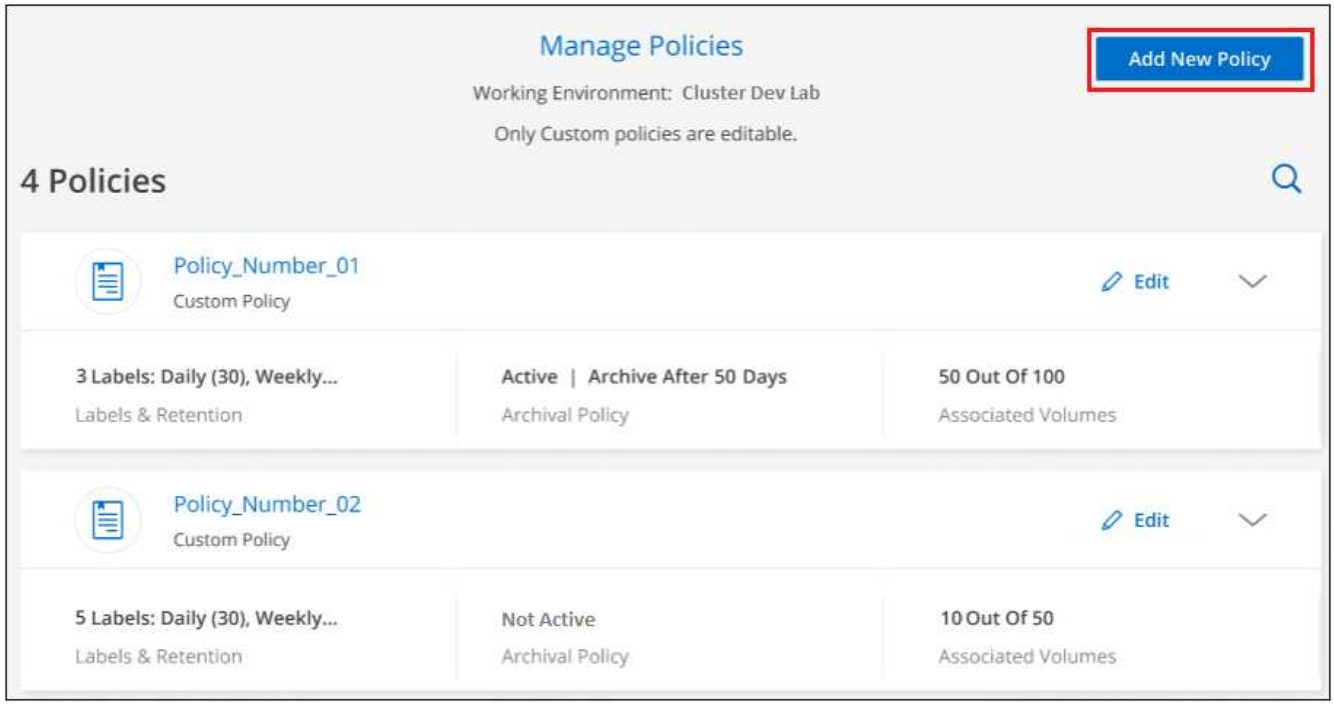
1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.



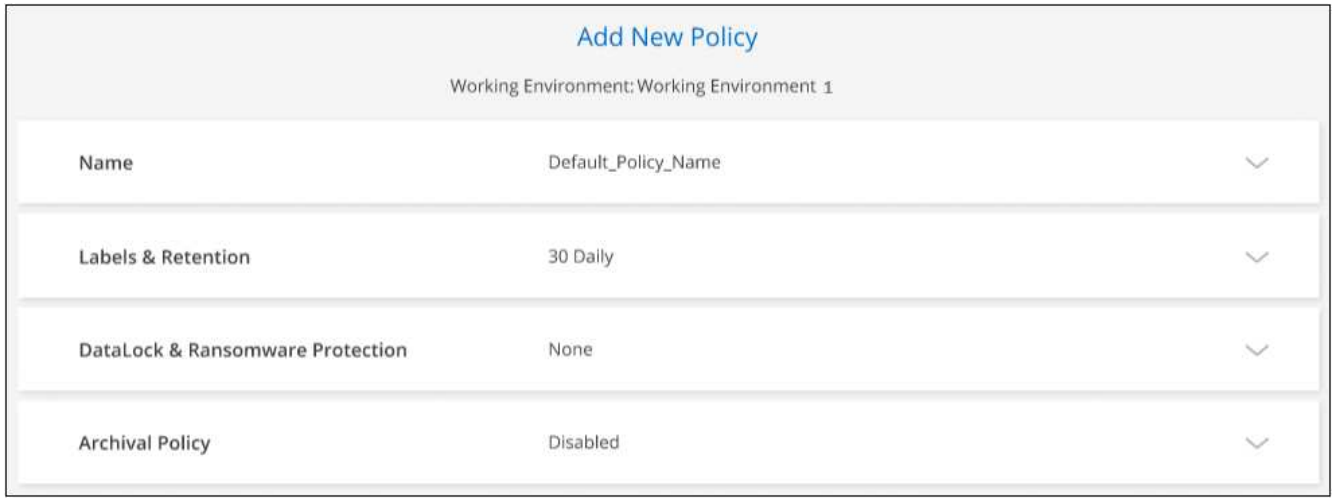

2. Klicken Sie auf der Seite „ Backup Settings_“ auf ••• Wählen Sie für die Arbeitsumgebung, in der Sie die neue Richtlinie hinzufügen möchten, und wählen Sie **Richtlinien verwalten**.




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

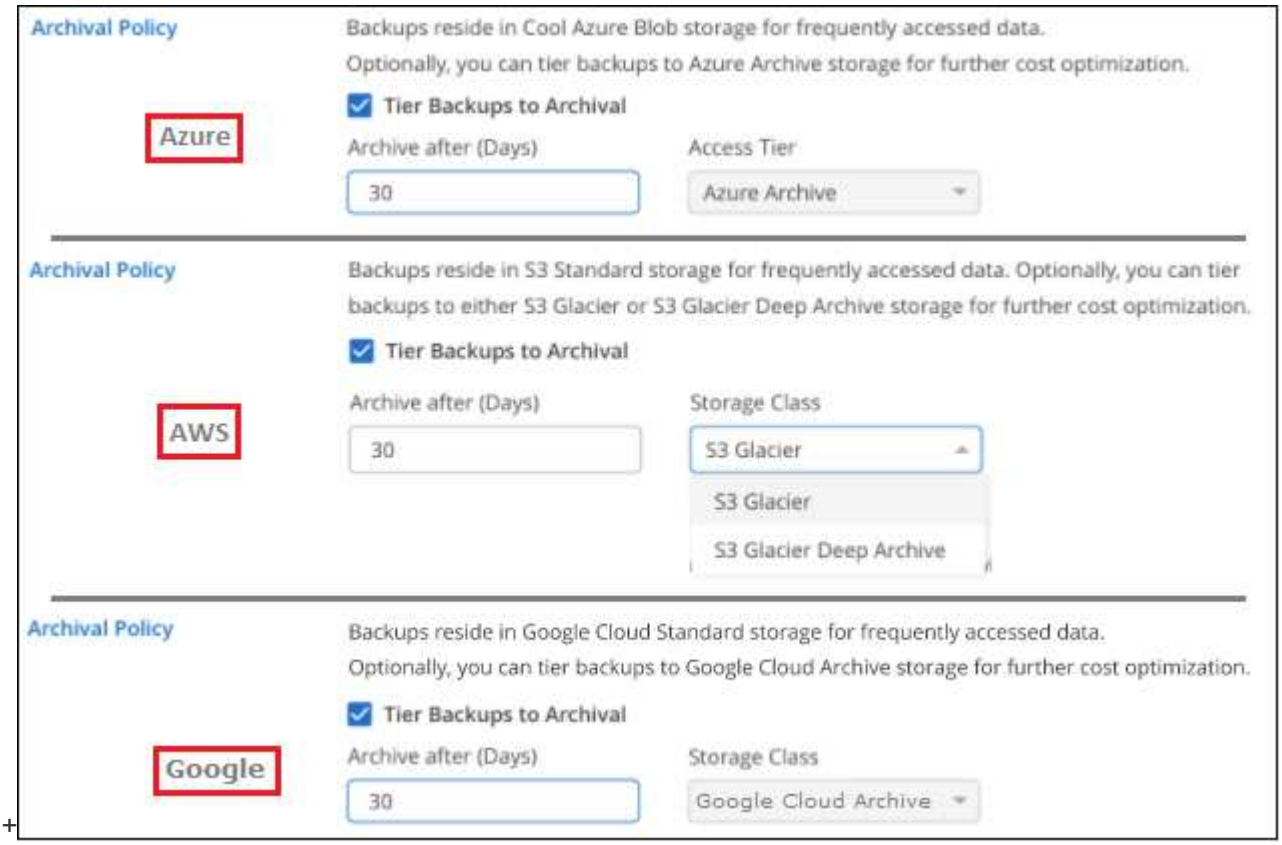



4. Klicken Sie auf der Seite „ Neue Richtlinie hinzufügen_“ auf ⌄ Erweitern Sie den Abschnitt *Labels & Retention*, um den Zeitplan und die Backup-Aufbewahrung zu definieren, und klicken Sie auf **Speichern**.




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

"Erfahren Sie mehr über die Verwendung von Google Archivspeicher". (ONTAP 9.12.1 erforderlich.)



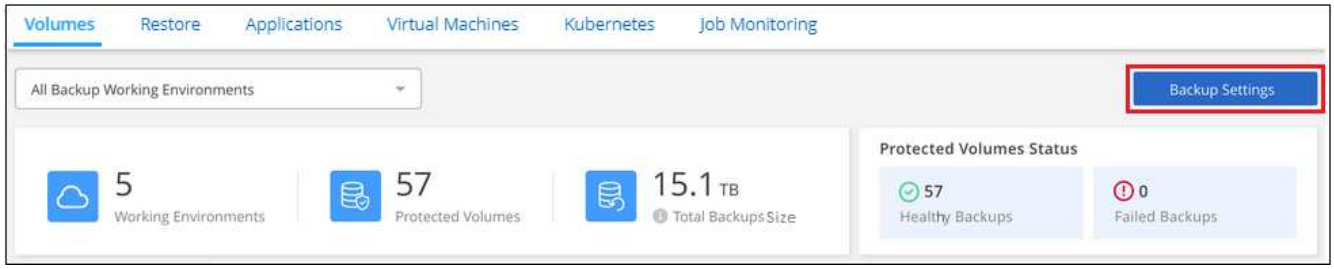

## Ändern der Richtlinie, die vorhandenen Volumes zugewiesen ist

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

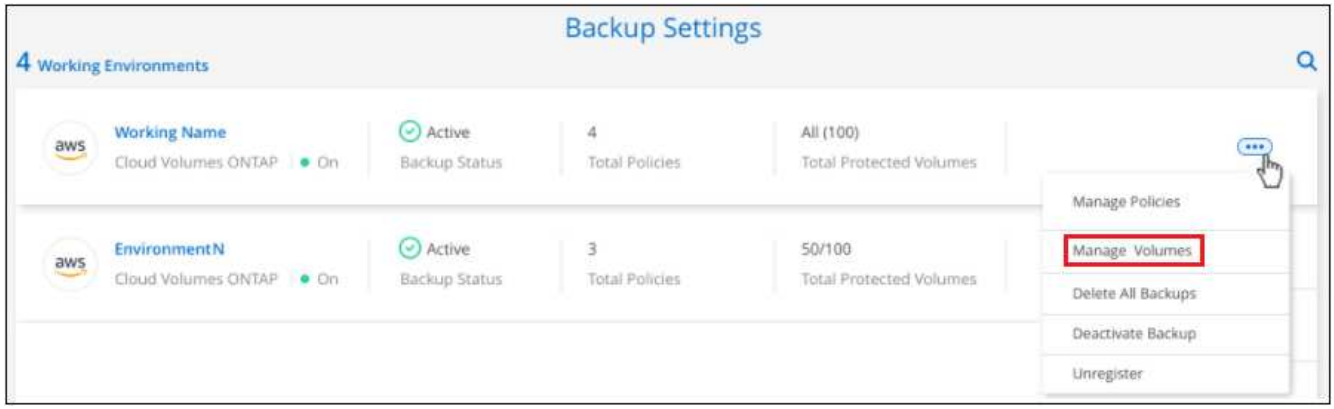
Beachten Sie, dass die Richtlinie, die Sie auf die Volumes anwenden möchten, bereits vorhanden sein muss. Erfahren Sie, wie Sie eine neue Backup-Richtlinie für eine Arbeitsumgebung hinzufügen.

**Schritte**

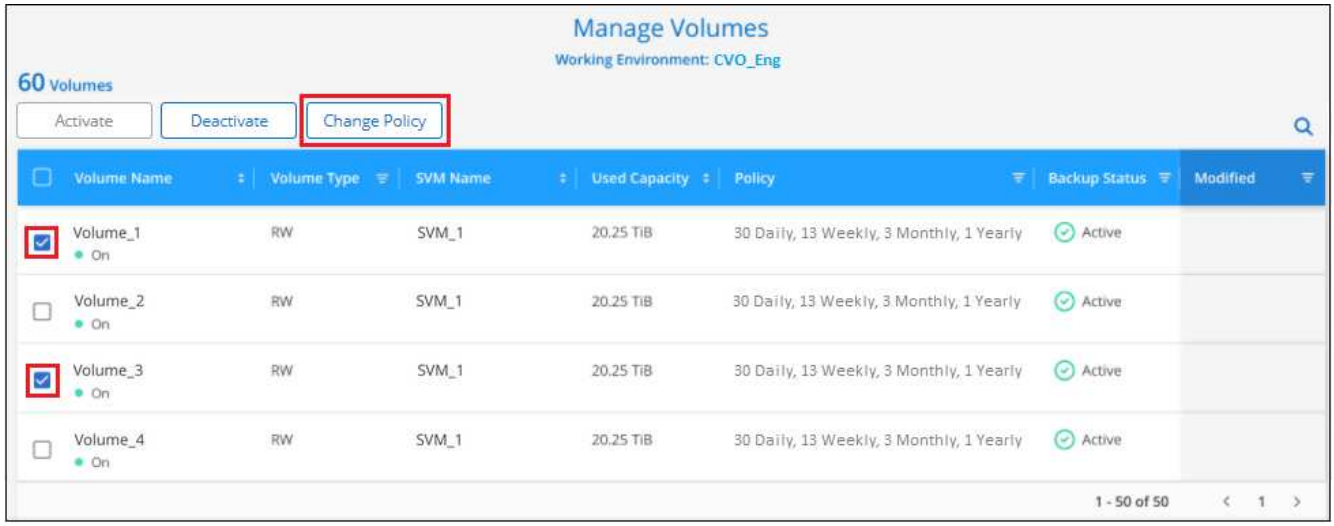
1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.



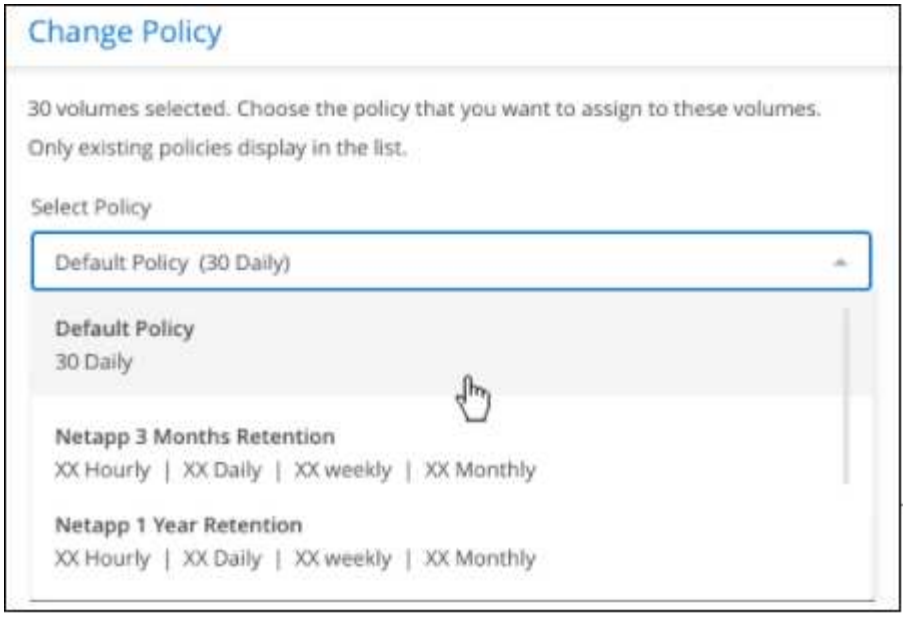

2. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Wählen Sie für die Arbeitsumgebung, in der die Volumina vorhanden sind, **Volumes verwalten** aus.




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




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




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

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

## Erstellung einer manuellen Volume-Sicherung zu jeder Zeit

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

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

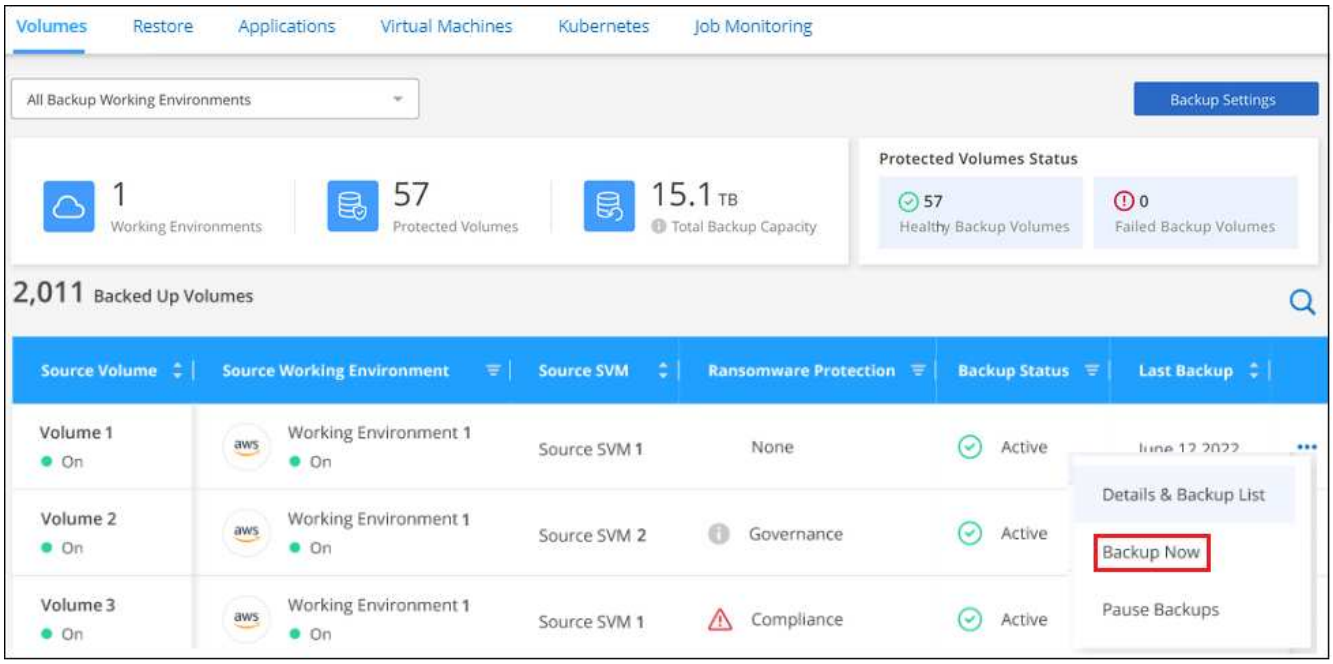
Wenn Sie *DataLock and Ransomware Protection* aktiviert haben, wenn Sie Cloud Backup für diesen Cluster aktivieren, wird das On-Demand-Backup auch mit DataLock konfiguriert, und die Aufbewahrungsfrist beträgt 30 Tage. Ransomware-Scans werden für Ad-hoc-Backups nicht unterstützt. "Erfahren Sie mehr über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

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

Volume-Backups werden auf Datensicherungs-Volumes nicht unterstützt.

**Schritte**

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




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

## Anzeigen der Liste der Backups für jedes Volume

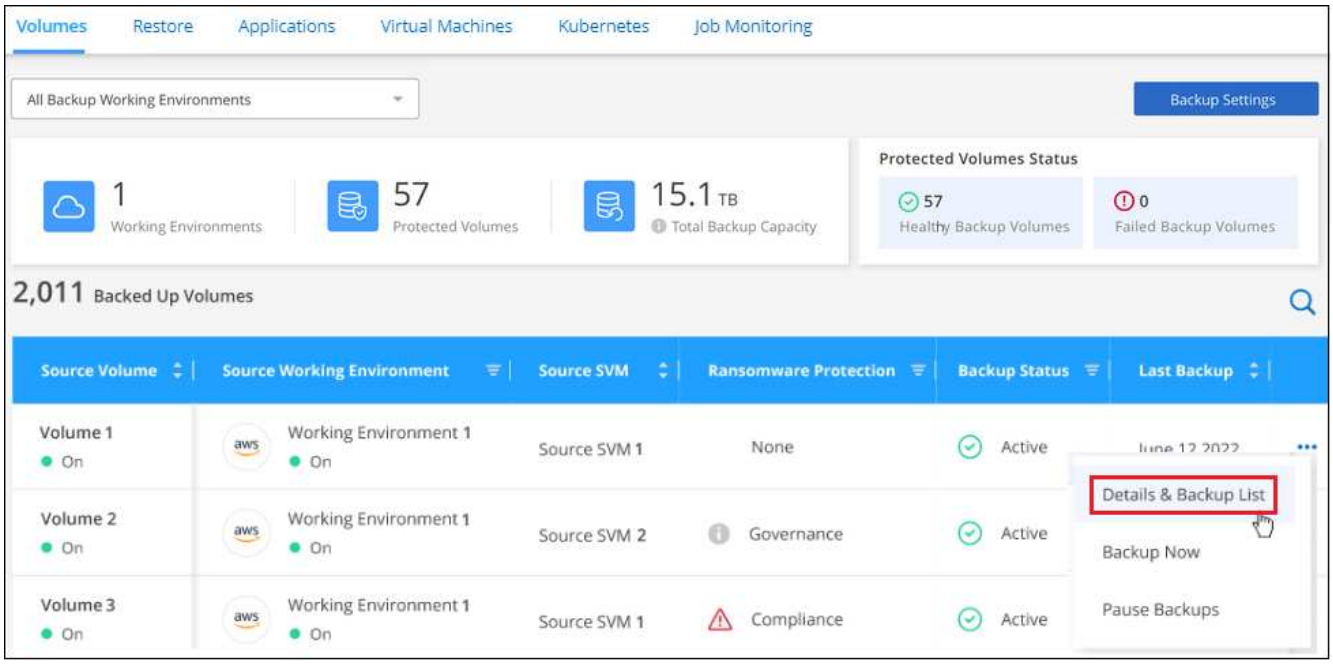
Sie können eine Liste aller Backup-Dateien anzeigen, die für jedes Volume vorhanden sind. Auf dieser Seite werden Details zum Quell-Volume, zum Zielort und zu Backup-Details wie zum Beispiel zum letzten Backup, zur aktuellen Backup-Richtlinie, zur Größe der Sicherungsdatei und mehr angezeigt.

Auf dieser Seite können Sie außerdem die folgenden Aufgaben ausführen:

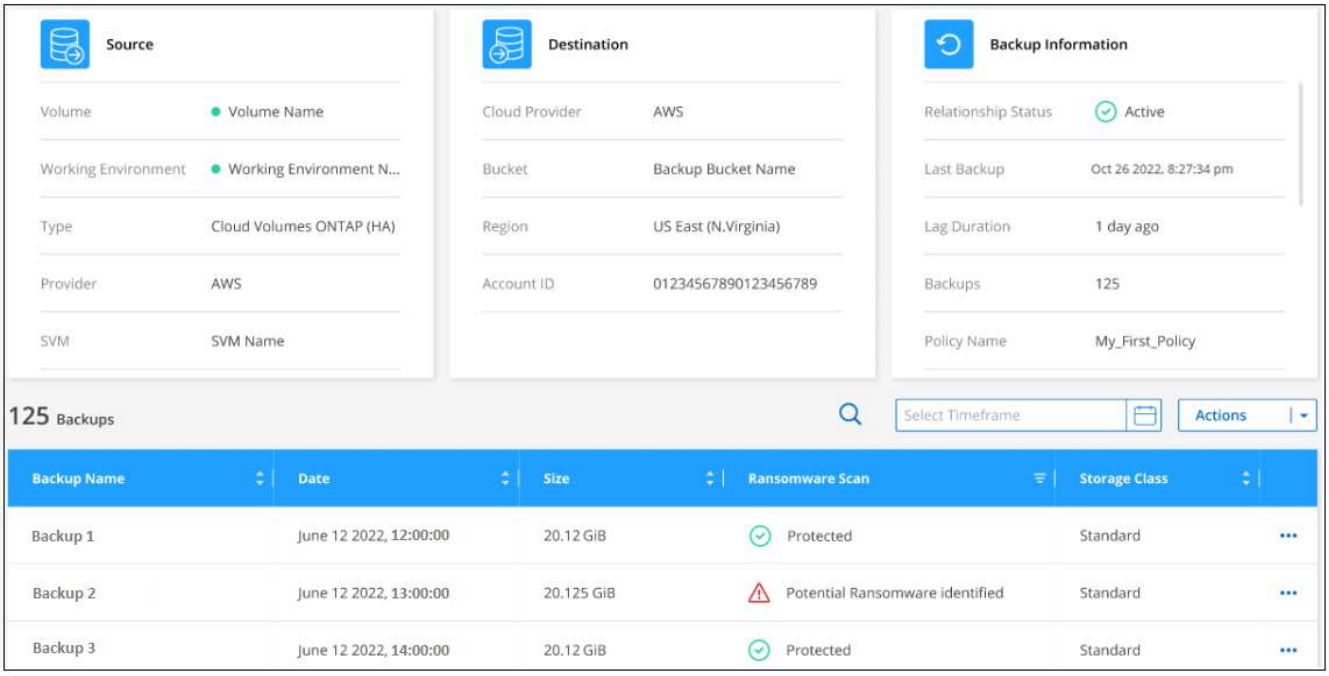
- Löschen Sie alle Sicherungsdateien für das Volume
- Löschen einzelner Backup-Dateien für das Volume
- Backup-Bericht für das Volume herunterladen

### Schritte

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




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




## Durchführung eines Ransomware-Scans bei einem Volume-Backup

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

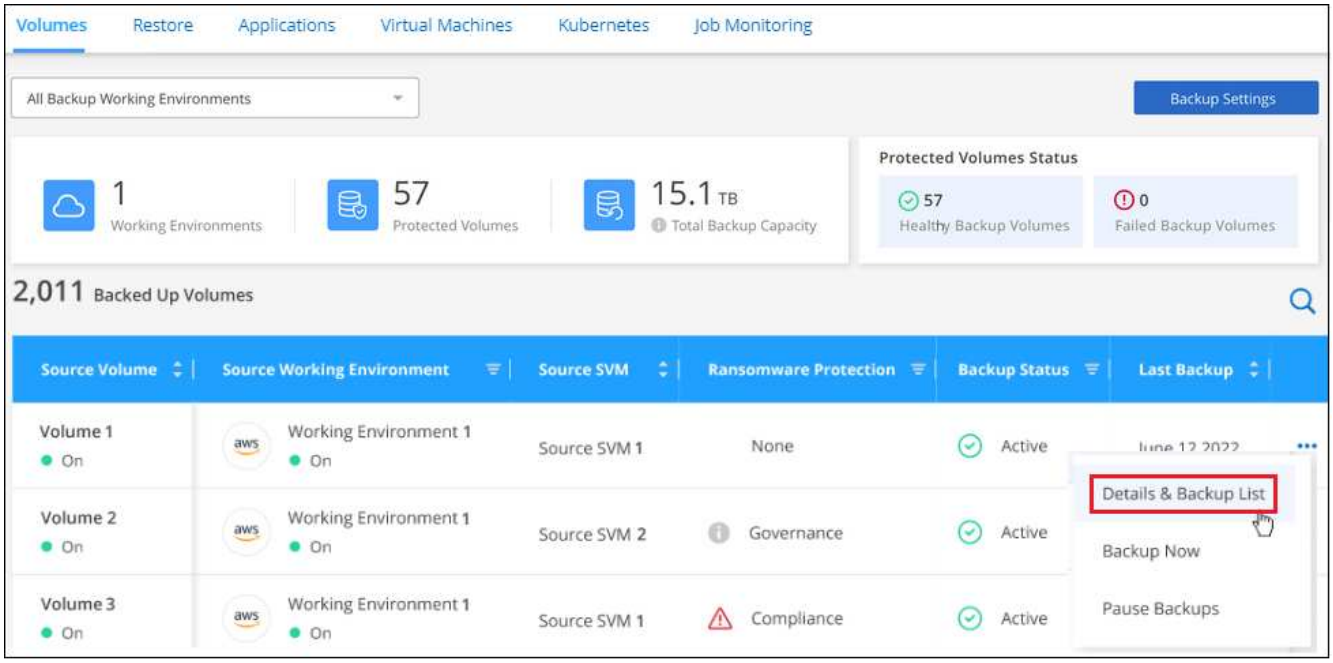
Diese Funktion ist nur verfügbar, wenn die Volume-Sicherung von einem System mit ONTAP 9.11.1 oder höher

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

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

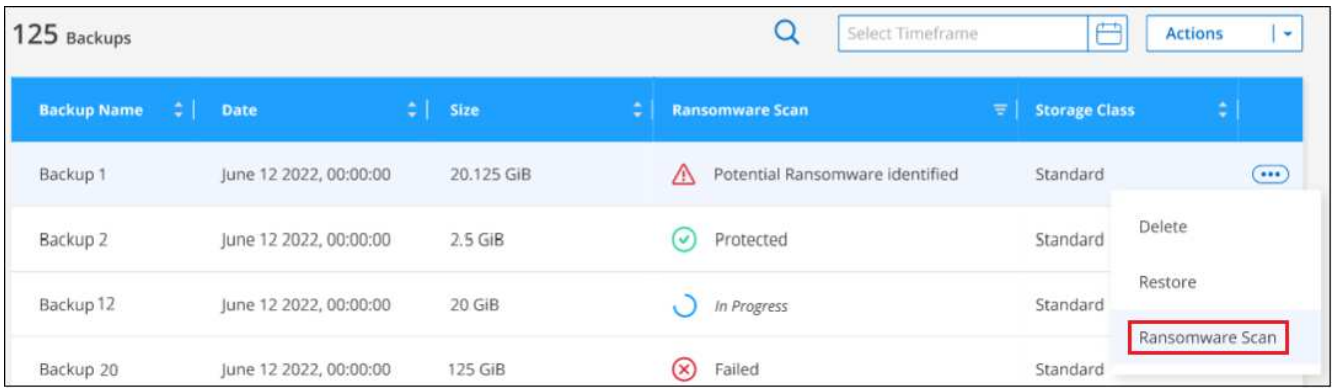
**Schritte**

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




Die Liste aller Sicherungsdateien wird angezeigt.

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




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

## Backups werden gelöscht

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

Beachten Sie, dass Sie keine Sicherungsdateien löschen können, die Sie mit DataLock und Ransomware-Schutz gesperrt haben. Die Option „Löschen“ ist in der Benutzeroberfläche nicht verfügbar, wenn Sie eine oder mehrere gesperrte Sicherungsdateien ausgewählt haben.

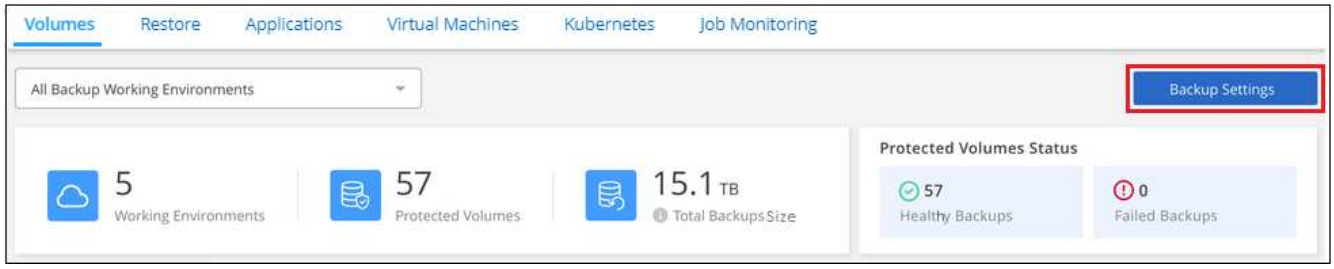
> Wenn Sie planen, eine Arbeitsumgebung oder ein Cluster mit Backups zu löschen, müssen Sie die Backups *löschen, bevor Sie das System löschen. Cloud Backup nicht automatisch löschen Backups, wenn Sie ein System löschen, und es gibt keine aktuelle Unterstützung in der UI, die Backups zu löschen, nachdem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

### Löschen aller Sicherungsdateien für eine Arbeitsumgebung

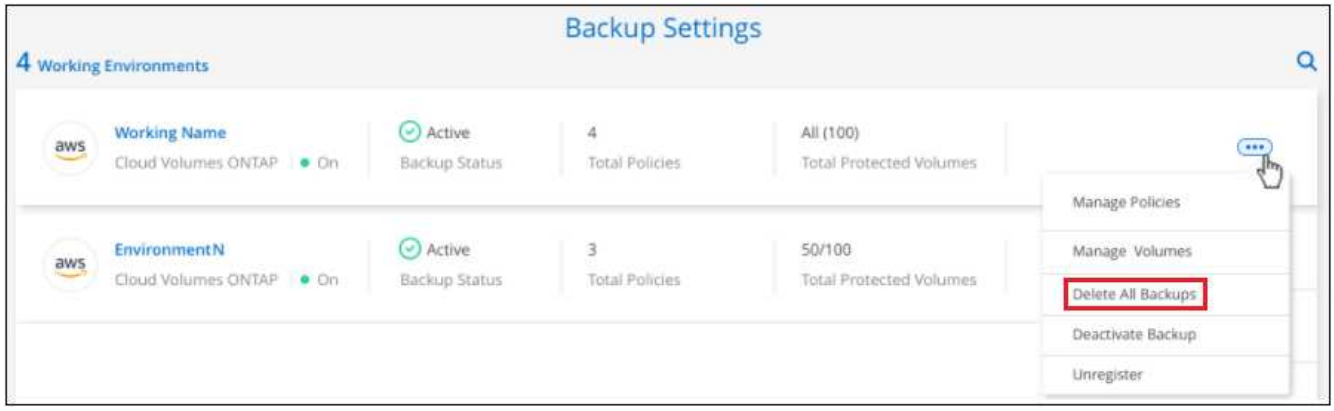
Durch das Löschen aller Backups für eine Arbeitsumgebung werden keine zukünftigen Backups von Volumes in dieser Arbeitsumgebung deaktiviert. Wenn Sie die Erstellung von Backups aller Volumes in einer Arbeitsumgebung beenden möchten, können Sie Backups deaktivieren Wie hier beschrieben.

#### Schritte

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




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




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

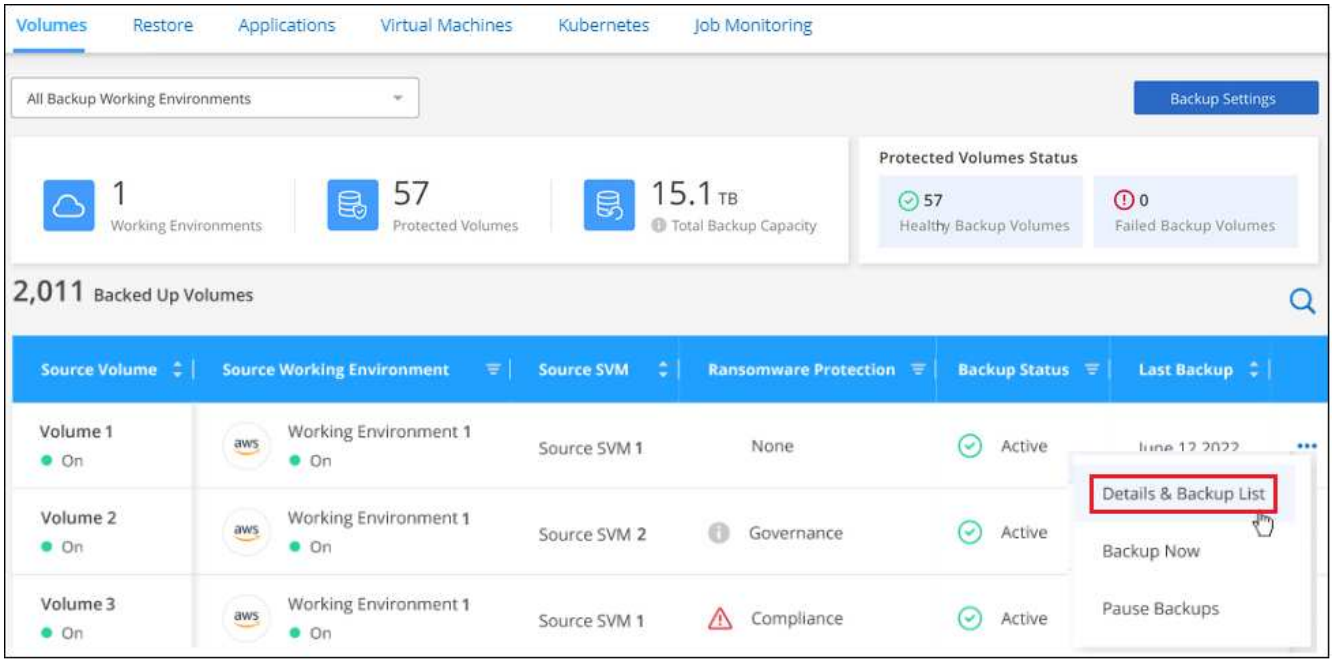
### Löschen aller Sicherungsdateien für ein Volume

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

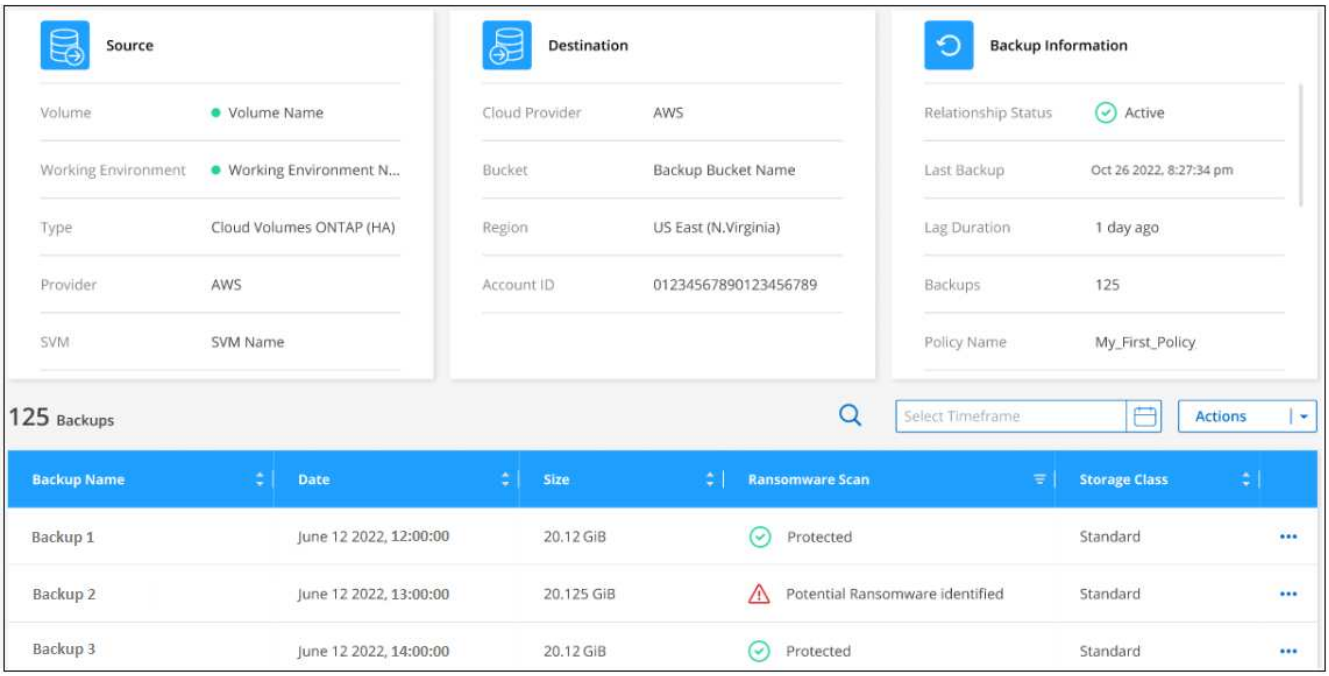
Das können Sie Starten Sie neu, um Backups für das Volume zu erstellen Auf der Seite „Backups verwalten“ können Sie jederzeit Backups managen.

#### Schritte

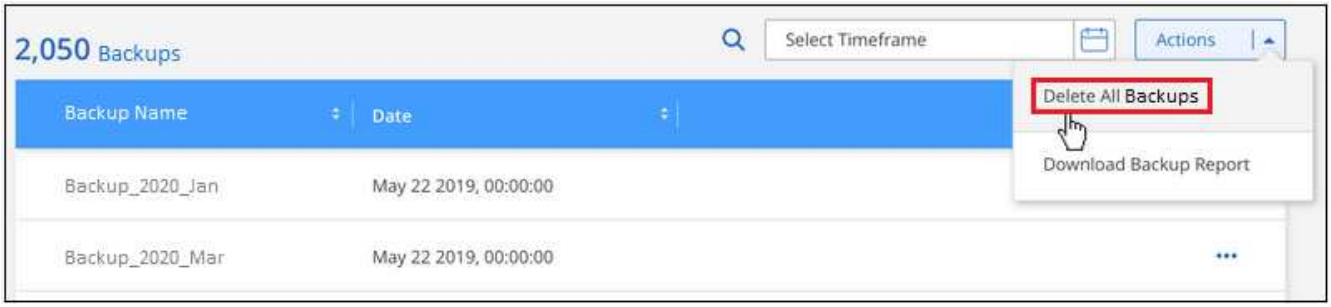
1. Klicken Sie auf der Registerkarte **Volumes** auf ••• Wählen Sie für das Quellvolume **Details & Sicherungsliste** aus.




Die Liste aller Sicherungsdateien wird angezeigt.




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



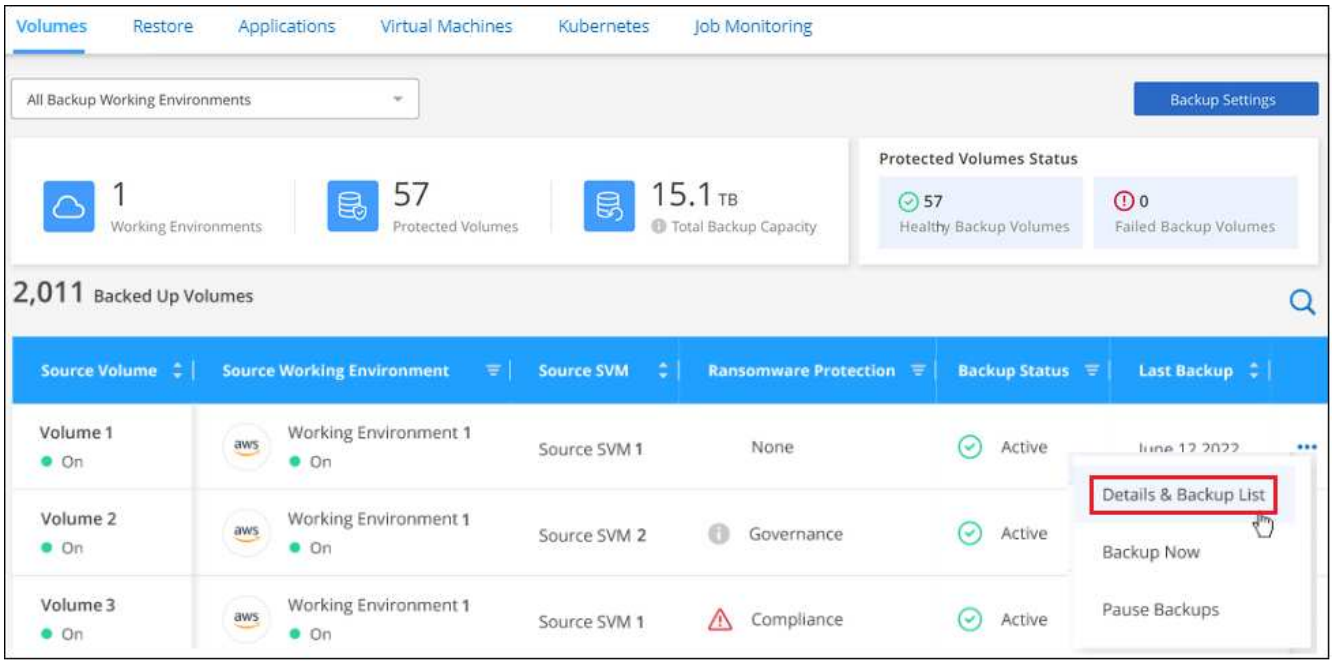

3. Geben Sie im Bestätigungsdialogfeld den Namen des Datenträgers ein und klicken Sie auf **Löschen**.

### Löschen einer einzelnen Backup-Datei für ein Volume

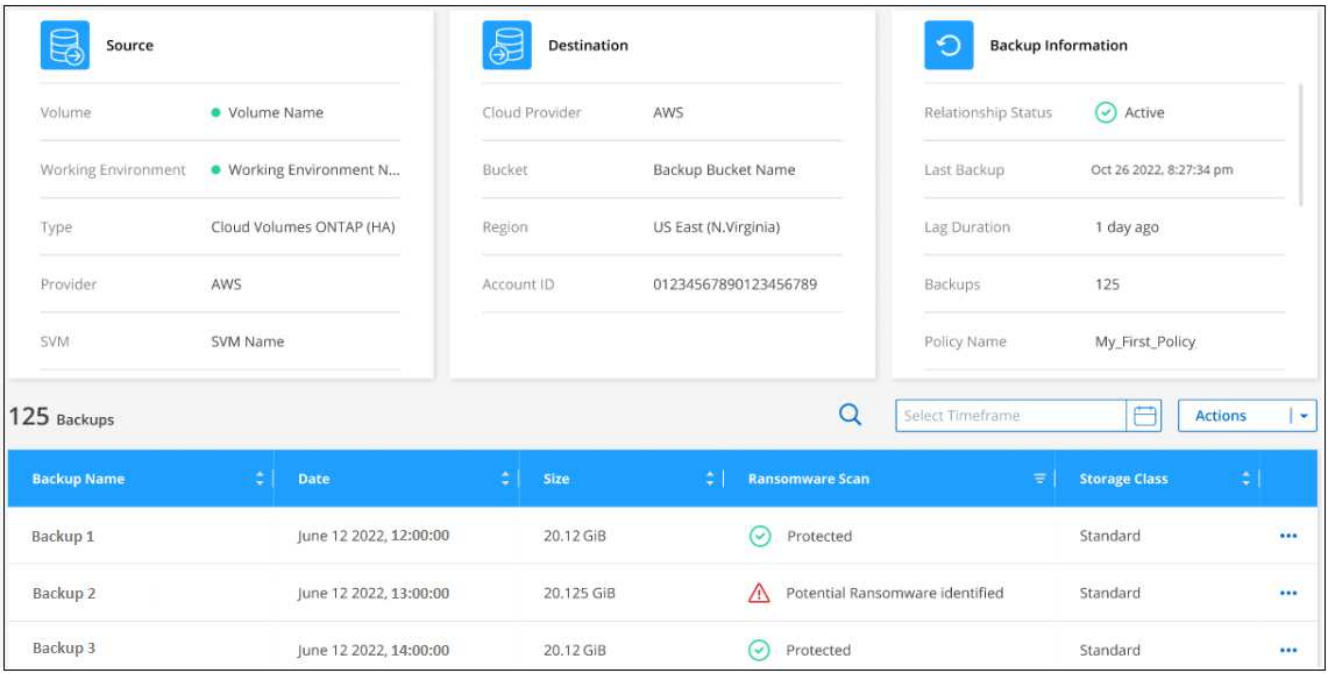
Sie können eine einzelne Sicherungsdatei löschen. Diese Funktion ist nur verfügbar, wenn das Volume Backup aus einem System mit ONTAP 9.8 oder neuer erstellt wurde.

#### Schritte

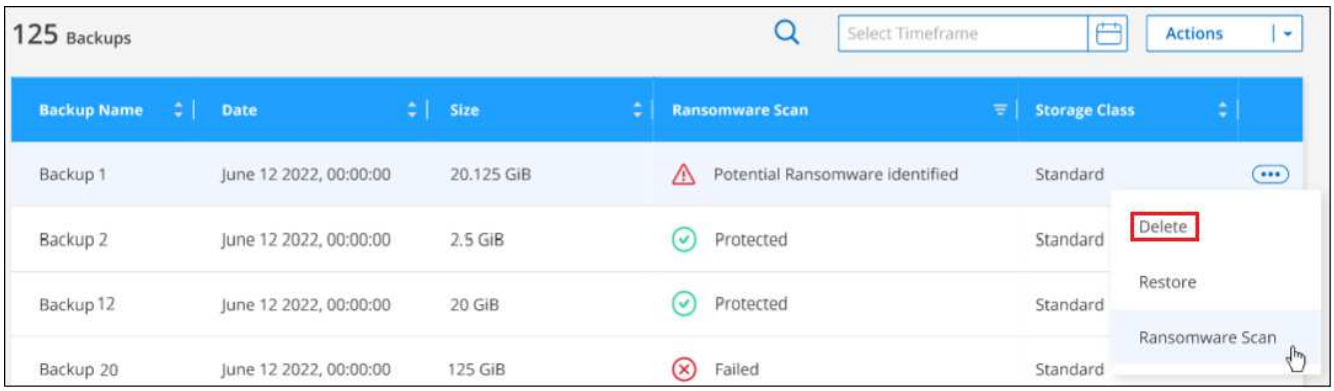
1. Klicken Sie auf der Registerkarte **Volumes** auf ••• Wählen Sie für das Quellvolume **Details & Sicherungsliste** aus.




Die Liste aller Sicherungsdateien wird angezeigt.




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




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

## Löschen von Volume-Backup-Beziehungen

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

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

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

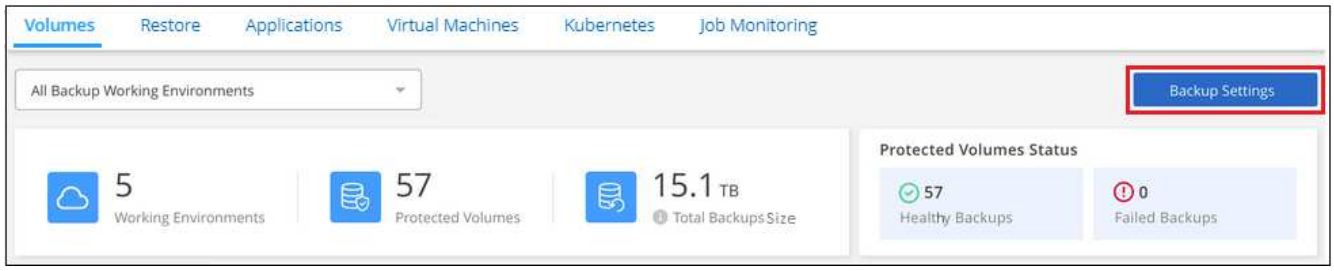
Sie können das Quell-Volume nicht aus der Cloud Backup Benutzeroberfläche löschen. Sie können jedoch die

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

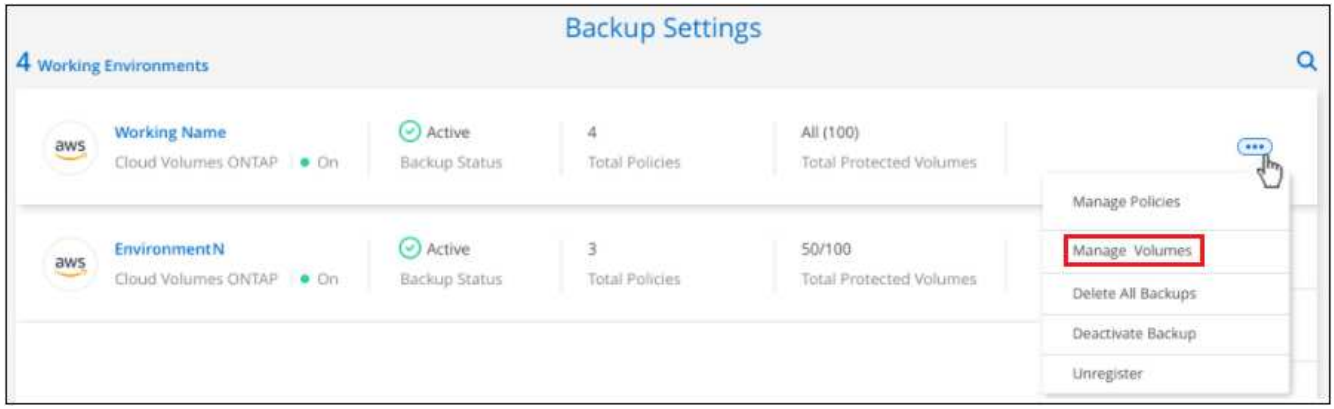
> Sie können einzelne Sicherungsdateien des Volumes nicht löschen, sobald die Beziehung gelöscht wurde. Sie können es jedoch "Löschen Sie alle Backups für das Volume" Wenn Sie alle Sicherungsdateien entfernen möchten.

**Schritte**

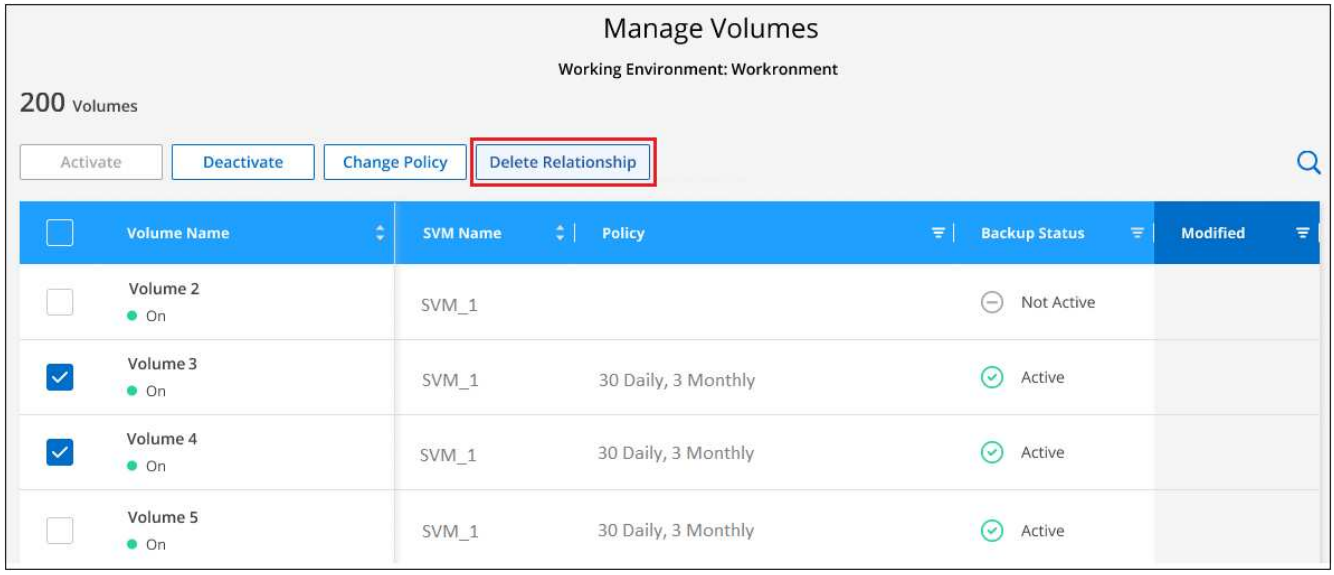
1. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.




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

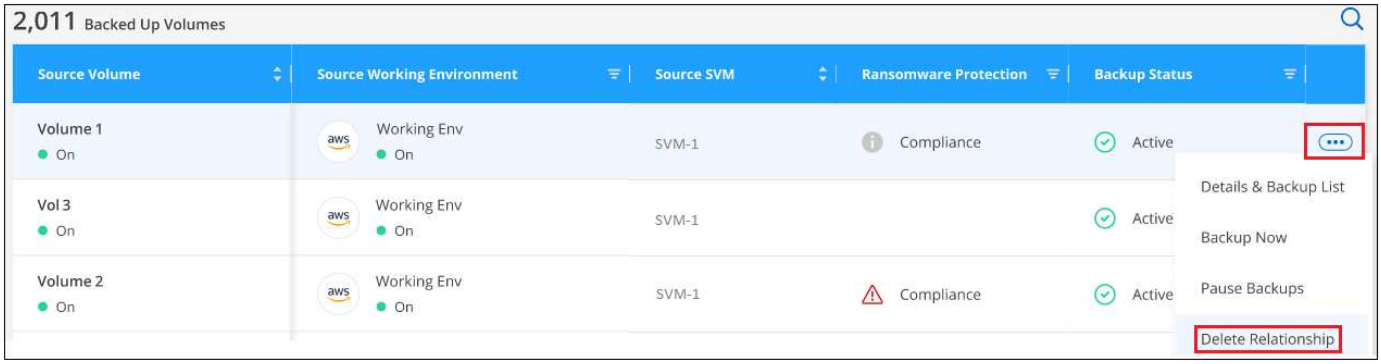



3. Aktivieren Sie das Kontrollkästchen für ein Volume oder Volumes, das Sie die Sicherungsbeziehung löschen möchten, und klicken Sie dann auf **Beziehung löschen**.

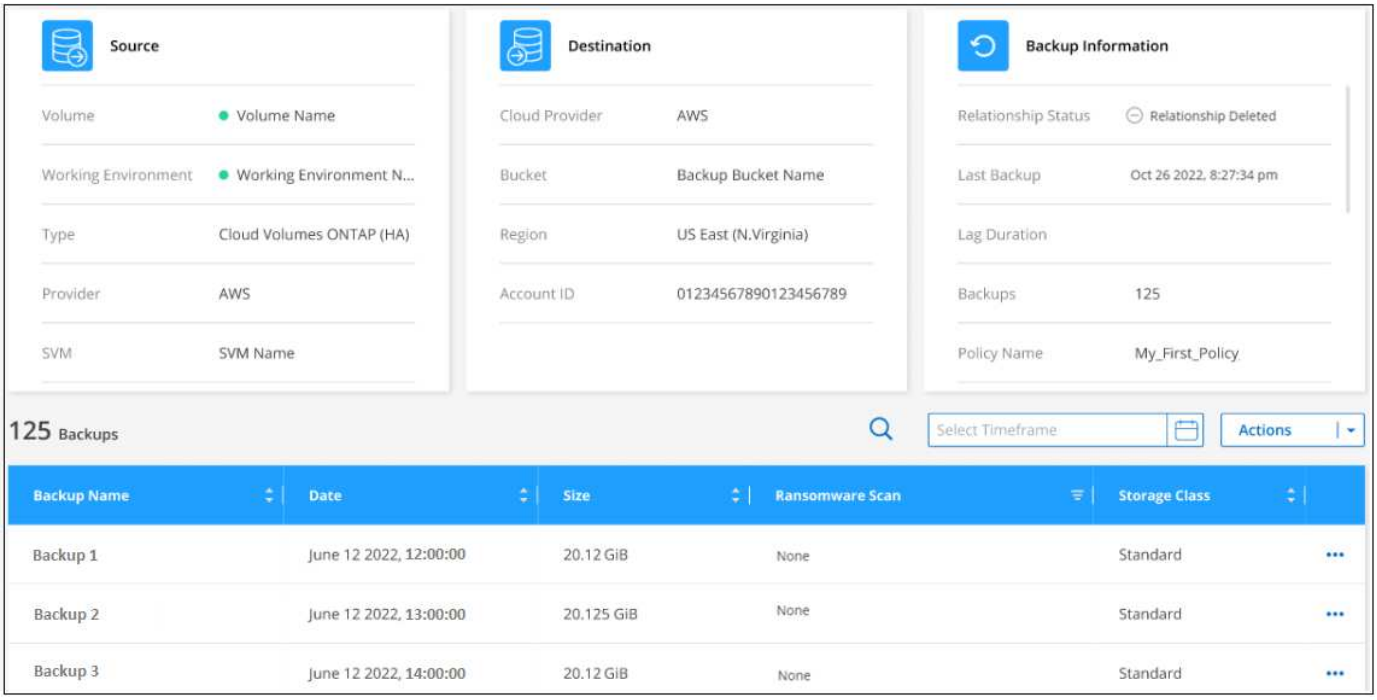


4. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.

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




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



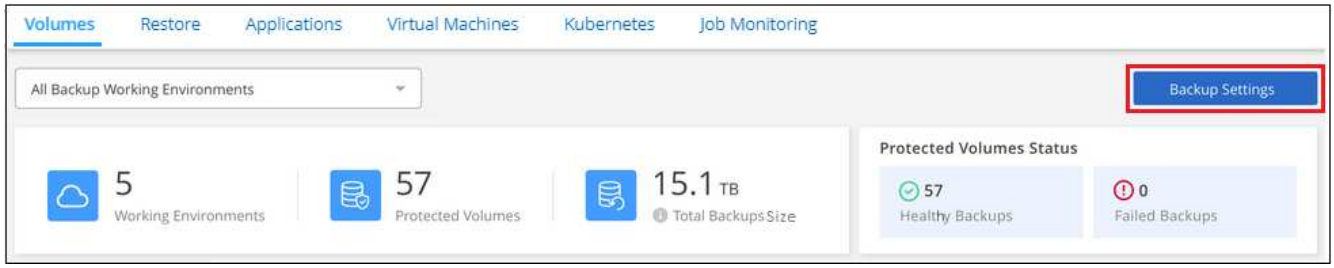

## Deaktivieren von Cloud Backup für eine Arbeitsumgebung

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

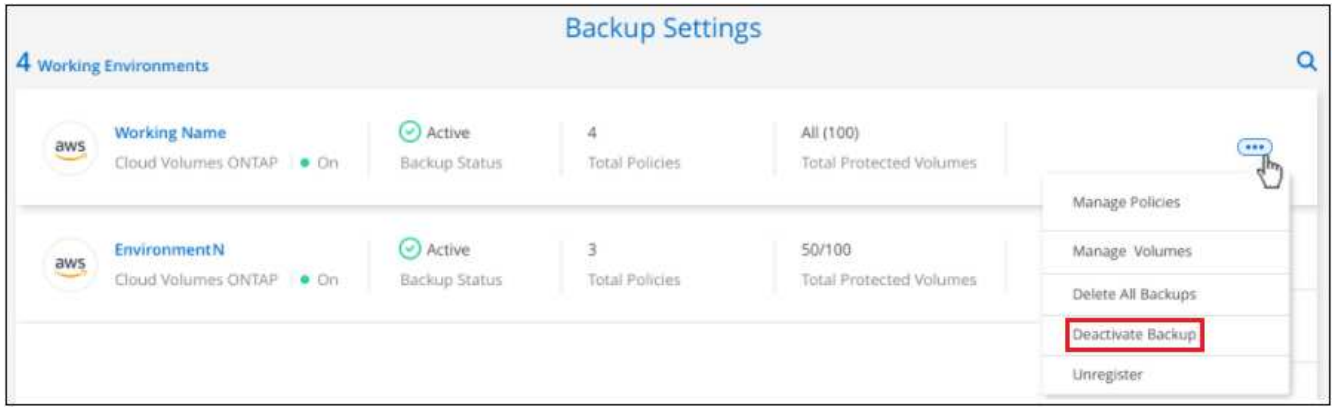
Beachten Sie, dass Cloud-Provider Ihnen weiterhin die Kosten für Objekt-Storage für die Kapazität in Ihrem Backup in Rechnung stellen, es sei denn, Sie sind erforderlich Löschen Sie die Backups.

### Schritte

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




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




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

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

## Registrieren von Cloud Backup für eine Arbeitsumgebung wird aufgehoben

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

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

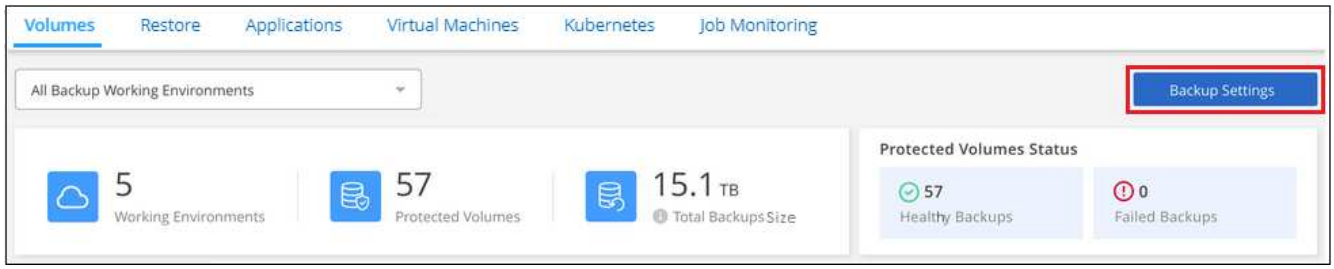
Bevor Sie die Registrierung von Cloud Backup aufheben können, müssen Sie die folgenden Schritte in der folgenden Reihenfolge durchführen:

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

Die Option zum Aufheben der Registrierung ist erst verfügbar, wenn diese beiden Aktionen abgeschlossen sind.

### Schritte

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




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

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

# Verwalten von Backup-Einstellungen auf Cluster-Ebene

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

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

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

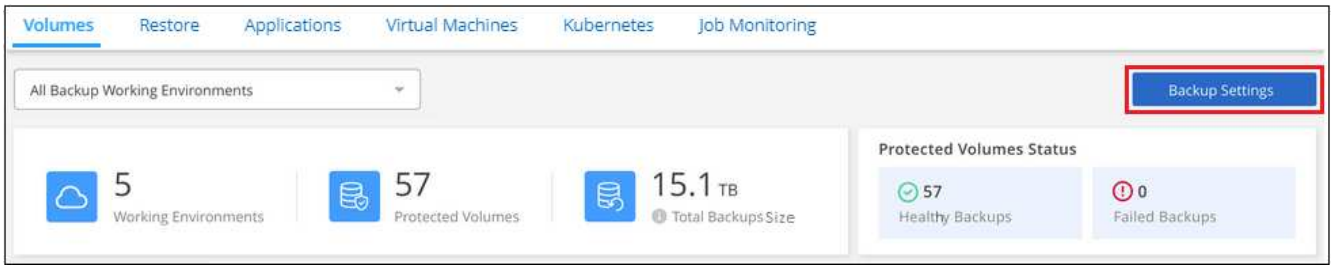
- Ändern der Storage-Schlüssel, die Ihrem ONTAP-System Zugriff auf Objekt-Storage gewähren
- Ändern des ONTAP-IPspaces, der mit Objekt-Storage verbunden ist
- Ändern der Netzwerkbandbreite, die für das Hochladen von Backups in den Objektspeicher zugewiesen ist
- Ändern der automatischen Backup-Einstellung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

## Zeigen Sie Backup-Einstellungen auf Cluster-Ebene an

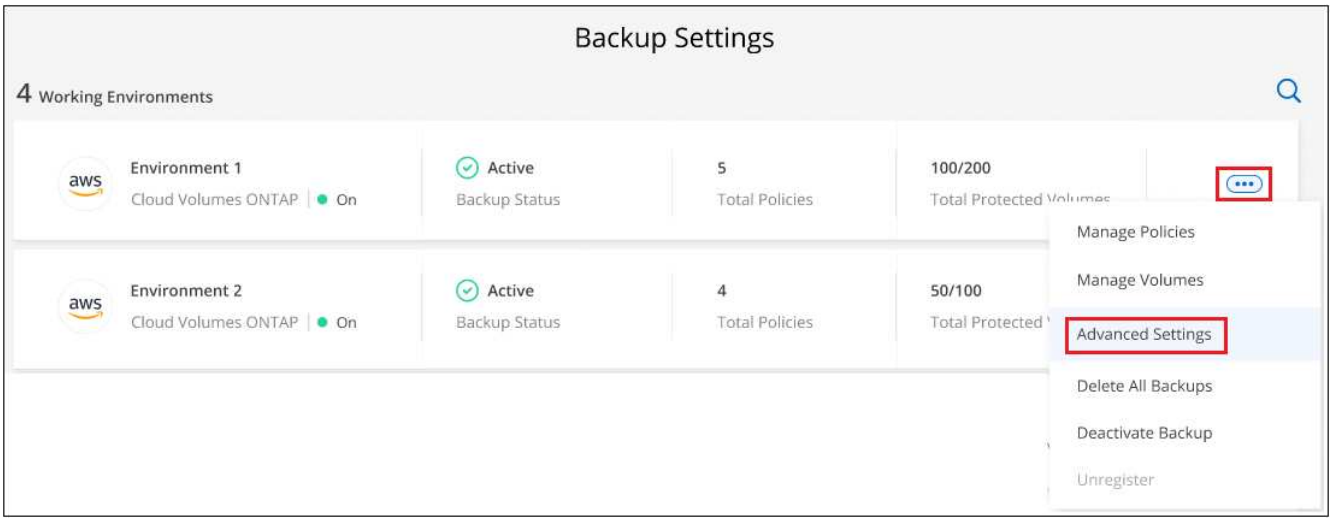
Sie können die Backup-Einstellungen auf Clusterebene für jede Arbeitsumgebung anzeigen.

**Schritte**

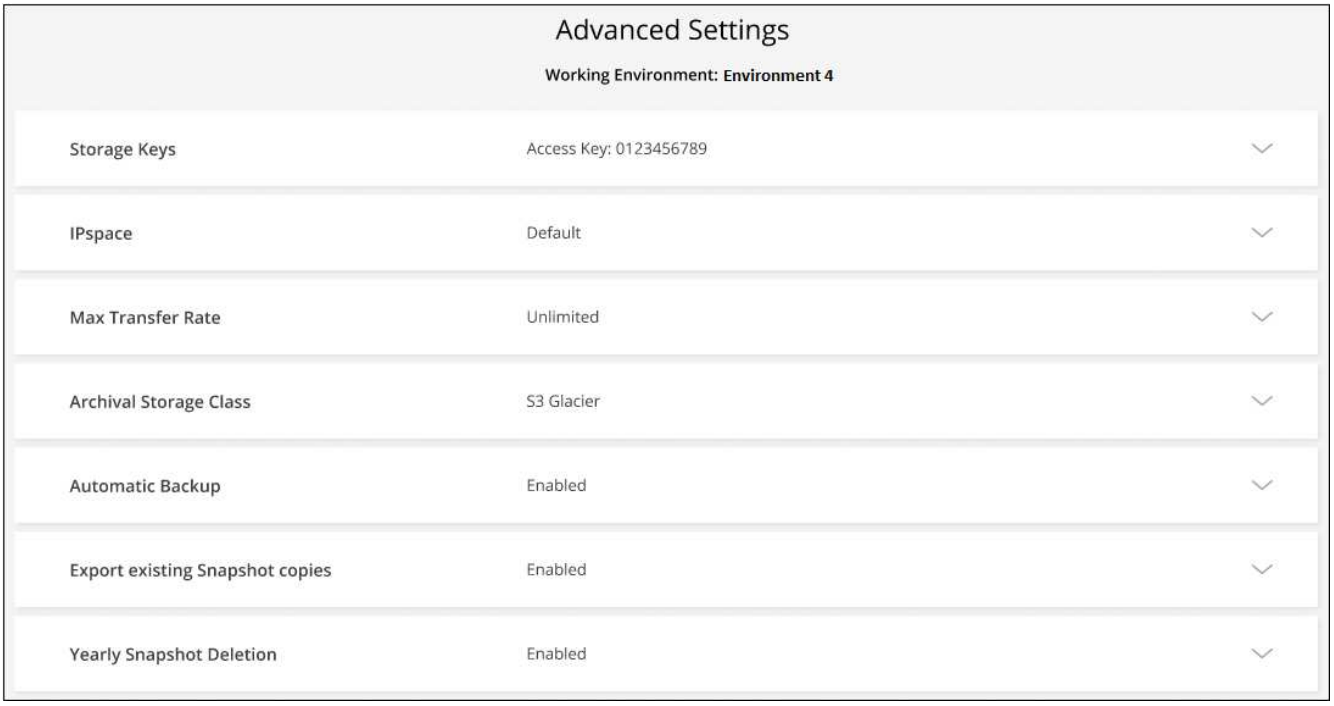
1. Wählen Sie im Menü BlueXP die Option **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie auf der Registerkarte **Volumes** die Option **Backup-Einstellungen** aus.




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




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



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

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

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

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

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

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

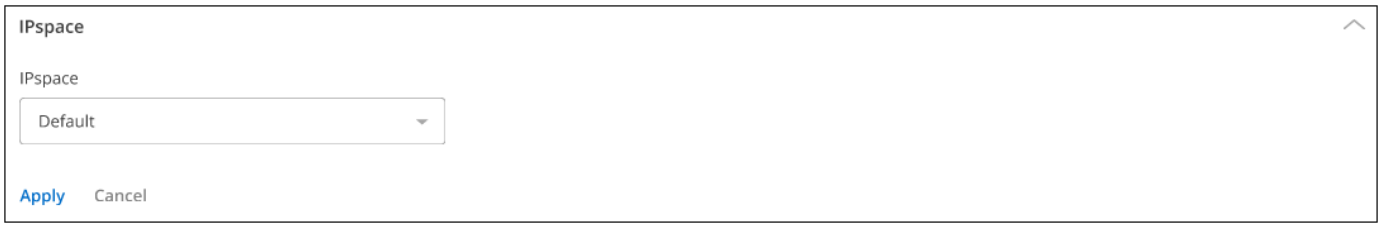
## Ändern Sie den ONTAP-IPspace, der mit dem Objekt-Storage verbunden ist

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

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

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

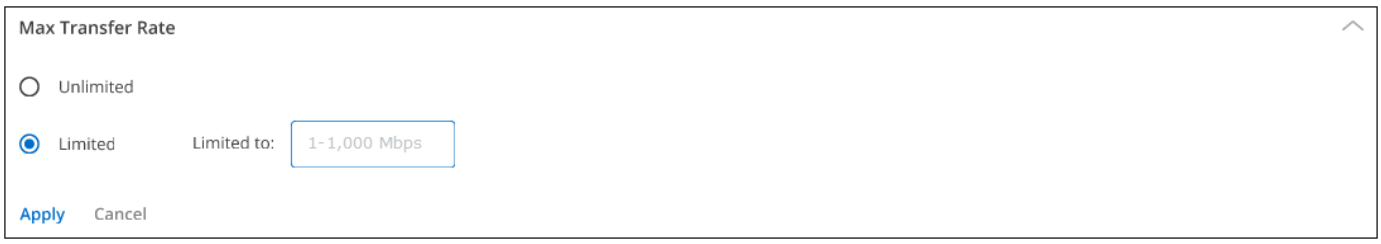
- Auf jedem ONTAP Node ist eine Intercluster-LIF erforderlich, die die Volumes hostet, die Sie sichern möchten.
- Die LIF muss dem IPspace zugewiesen sein, den ONTAP zum Herstellen einer Verbindung mit Objekt-Storage verwenden sollte.
- Die Intercluster-LIFs der Nodes müssen auf den Objektspeicher zugreifen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




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

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

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



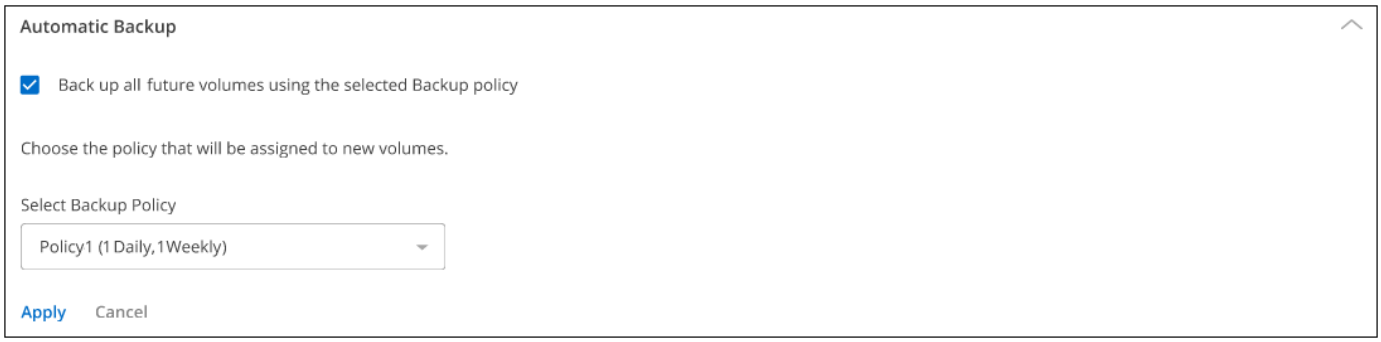

Wählen Sie das Optionsfeld **begrenzt** und geben Sie die maximale Bandbreite ein, die verwendet werden kann, oder wählen Sie **unbegrenzt**, um anzuzeigen, dass keine Begrenzung vorhanden ist.

## Ändern Sie die automatische Backup-Einstellung für zukünftige Volumes

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

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

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

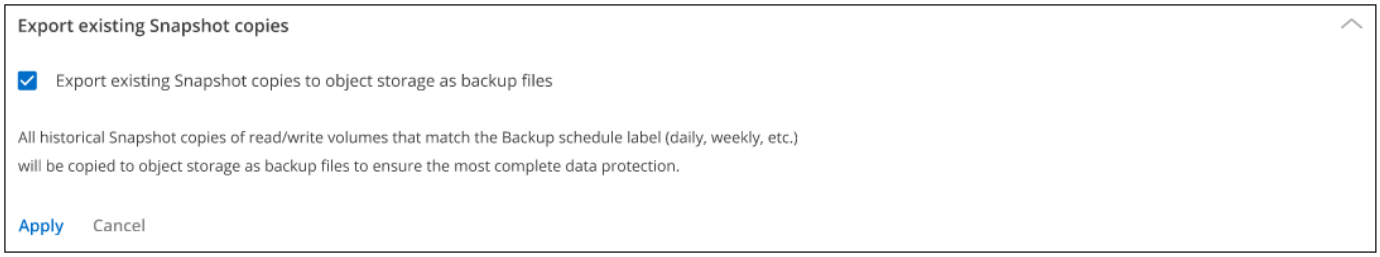



Sobald diese Backup-Richtlinie aktiviert ist, wird sie auf alle neuen Volumes angewendet, die in dieser Arbeitsumgebung mithilfe von BlueXP, System Manager, der ONTAP CLI oder den APIs erstellt wurden.

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

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

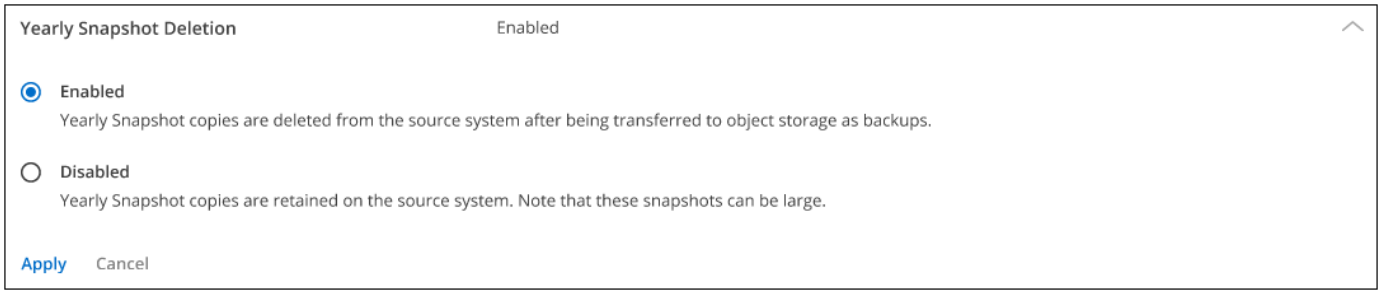
Beachten Sie, dass diese Option nur für neue Backup-Dateien für neue Lese-/Schreib-Volumes gilt und nicht für Datensicherungs-Volumes unterstützt wird.




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

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

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




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

# Wiederherstellen von ONTAP Daten aus Backup-Dateien

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

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

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

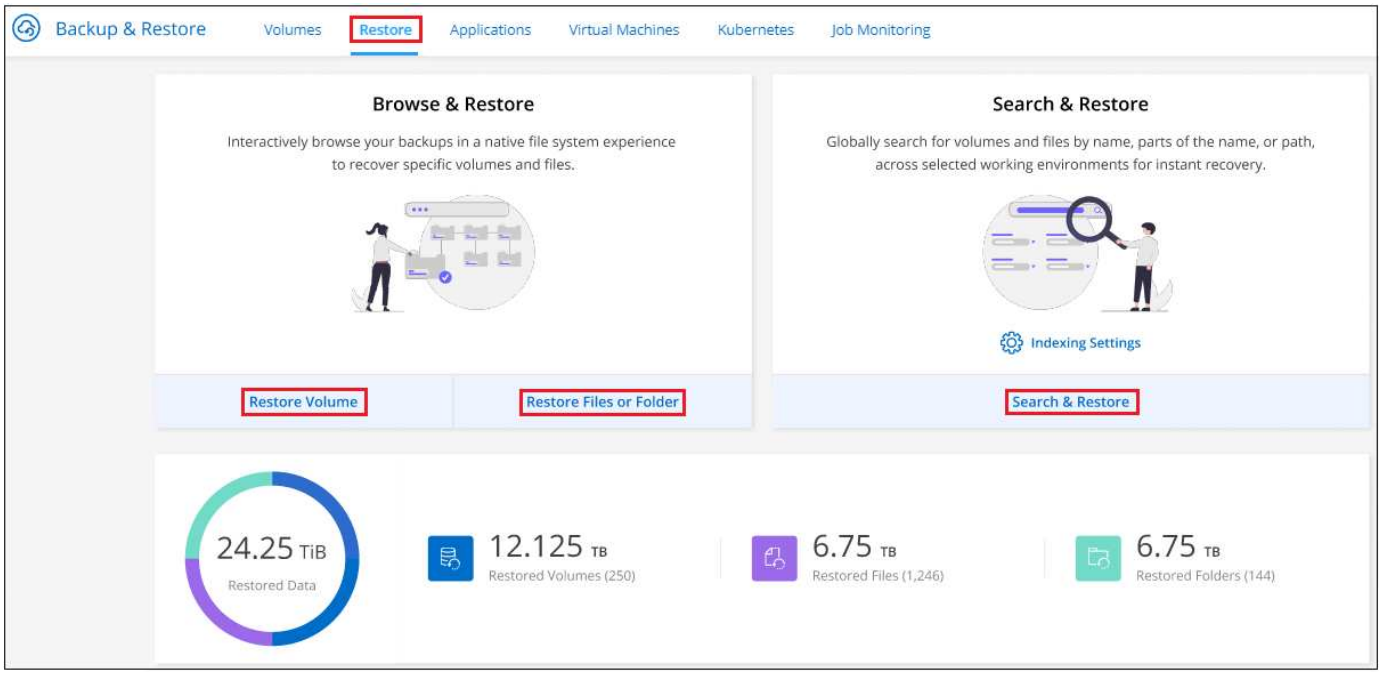
Sie können **Dateien** auf einem Volume in der ursprünglichen Arbeitsumgebung, auf einem Volume in einer anderen Arbeitsumgebung, in der dieselben Cloud-Konten verwendet werden, oder auf einem Volume in einem lokalen ONTAP System wiederherstellen.

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

## Das Restore Dashboard

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

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




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

## Vergleichen von Durchsuchen und Wiederherstellen und Suchen und Wiederherstellen

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

Diese Tabelle enthält einen Vergleich der beiden Methoden.

| Suchen Und Wiederherstellen | Suche Und Wiederherstellung |
|---|---|
| Durchsuchen Sie eine Struktur im Ordnerstil, um nach Volumes, Ordnern oder Dateien in einer einzelnen Backup-Datei zu suchen | Suchen Sie nach einem Volume, einem Ordner oder einer Datei über **alle Backup-Dateien** nach einem partiellen oder vollständigen Volume-Namen, einem Teil- oder vollständigen Ordner-/Dateinamen, einem Größenbereich und zusätzlichen Suchfiltern |
| Die Wiederherstellung von Volumes und Dateien erfolgt mit Backup-Dateien, die in Amazon S3, Azure Blob, Google Cloud und NetApp StorageGRID gespeichert sind | Die Wiederherstellung von Volumes und Dateien erfolgt mit Backup-Dateien, die in Amazon S3, Azure Blob, Google Cloud und NetApp StorageGRID gespeichert sind |
| Stellen Sie Volumes, Ordner und Dateien von StorageGRID in Sites ohne Internetzugang wieder her | Wird nicht in dunklen Seiten unterstützt |
| Behandelt keine Dateien, die umbenannt oder gelöscht wurden | Verarbeitet neu erstellte/gelöschte/umbenannte Verzeichnisse und neu erstellte/gelöschte/umbenannte Dateien |

| Suchen Und Wiederherstellen | Suche Und Wiederherstellung |
|---|---|
| Durchsuchen Sie nach Ergebnissen über Public und Private Clouds hinweg | Durchsuchen Sie Public Clouds und lokale Snapshot Kopien nach Ergebnissen |
| Es sind keine zusätzlichen Ressourcen für Cloud-Provider erforderlich | Pro Konto sind zusätzliche Bucket- und Public-Cloud-Provider-Ressourcen erforderlich |
| Es sind keine zusätzlichen Kosten für Cloud-Provider erforderlich | Kosten im Zusammenhang mit Public-Cloud-Provider-Ressourcen bei der Überprüfung Ihrer Backups und Volumes für Suchergebnisse |

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

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

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

## Wiederherstellen von ONTAP-Daten mithilfe von Durchsuchen und Wiederherstellen

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

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

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

### Unterstützte Arbeitsumgebungen und Objekt-Storage-Anbieter durchsuchen und wiederherstellen

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

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

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

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

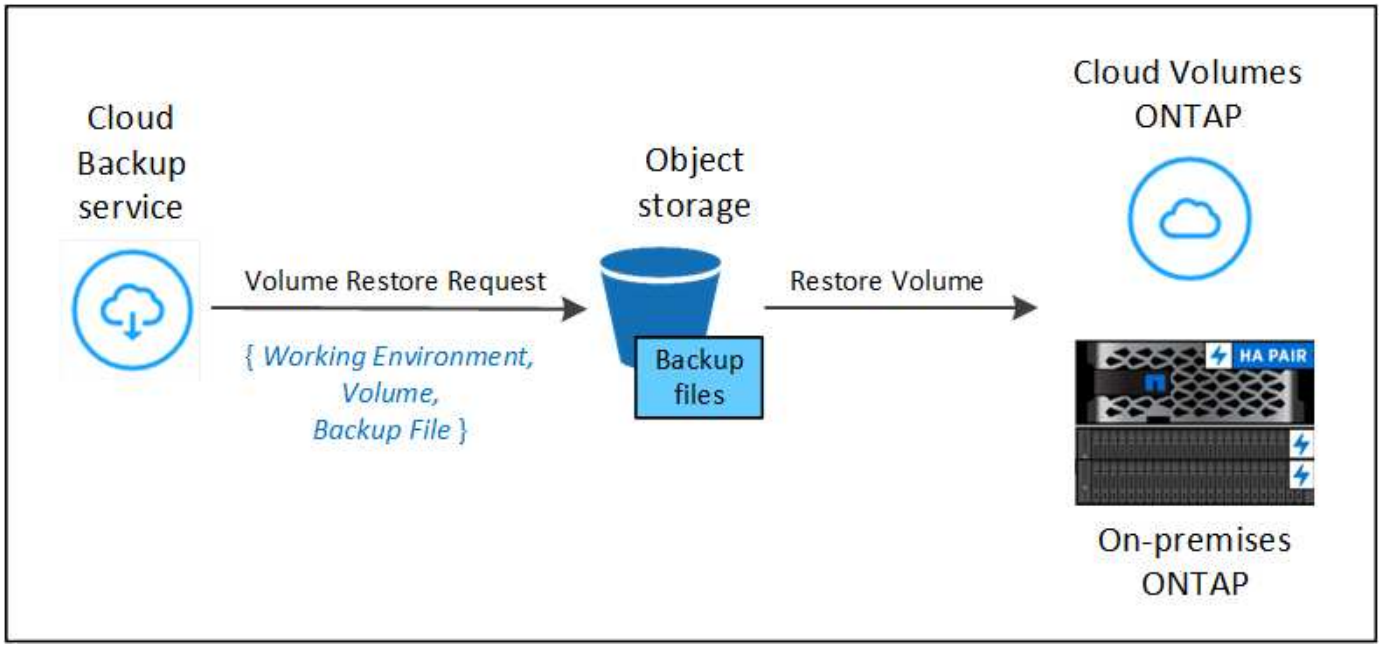
- Für Google Cloud Storage muss der Connector in Ihrer Google Cloud Platform VPC implementiert werden
- Für StorageGRID muss der Connector in Ihrem Haus bereitgestellt werden

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

> Sie können keine Ordner oder Dateien wiederherstellen, wenn die Sicherungsdatei mit DataLock & Ransomware konfiguriert wurde. In diesem Fall können Sie das gesamte Volume aus der Sicherungsdatei wiederherstellen und anschließend auf die von Ihnen benötigten Dateien zugreifen.

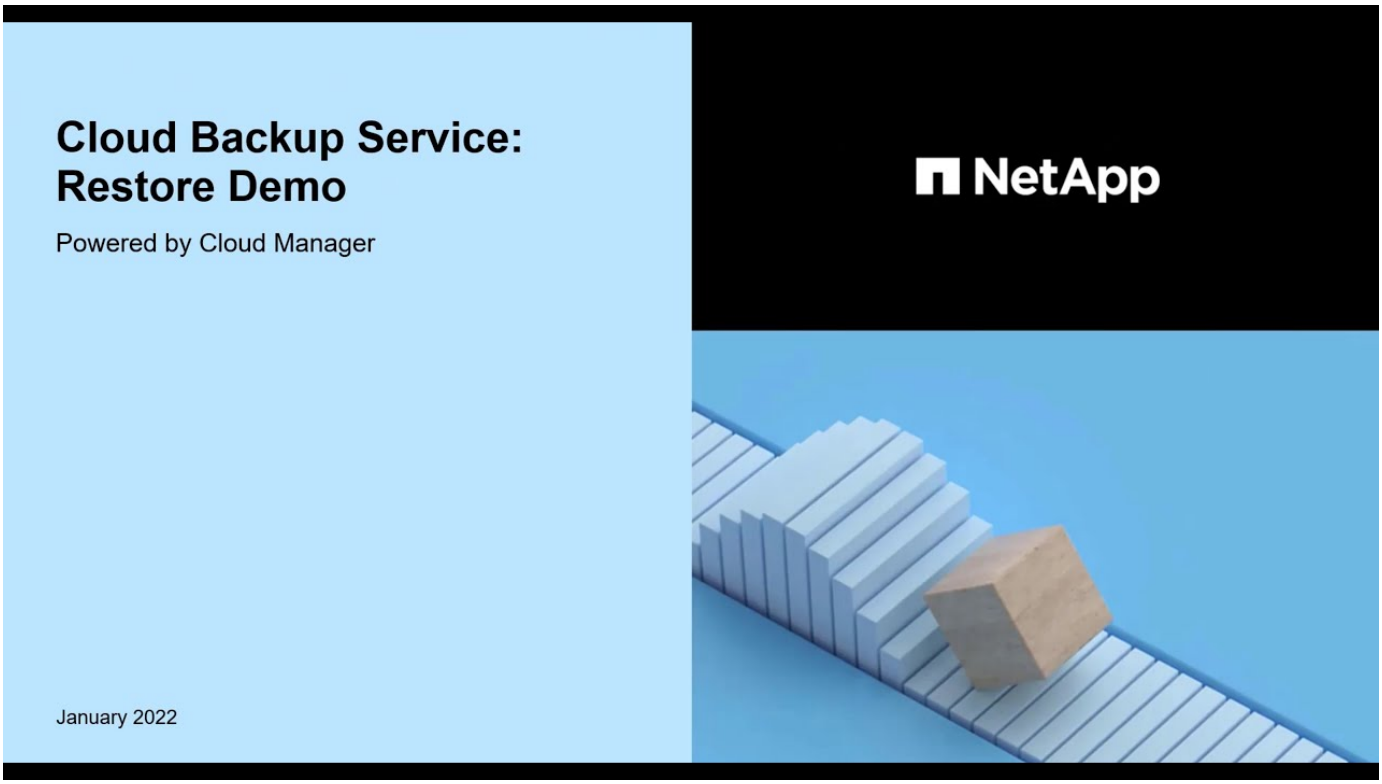
**Wiederherstellen von Volumes mit Durchsuchen und Wiederherstellen**

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




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

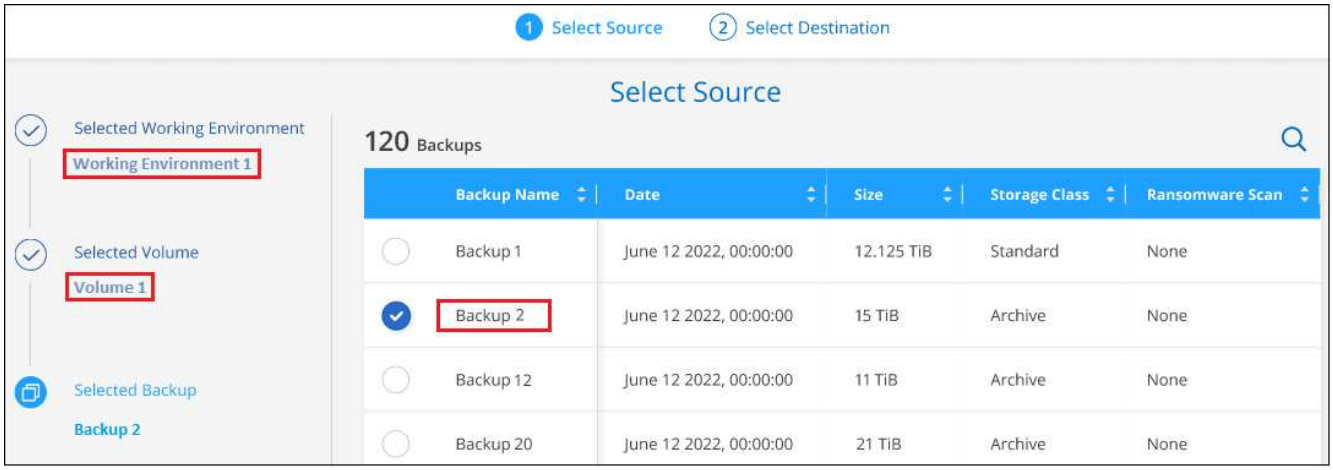
Das folgende Video zeigt einen kurzen Spaziergang zur Wiederherstellung eines Volumens:




**Schritte**

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

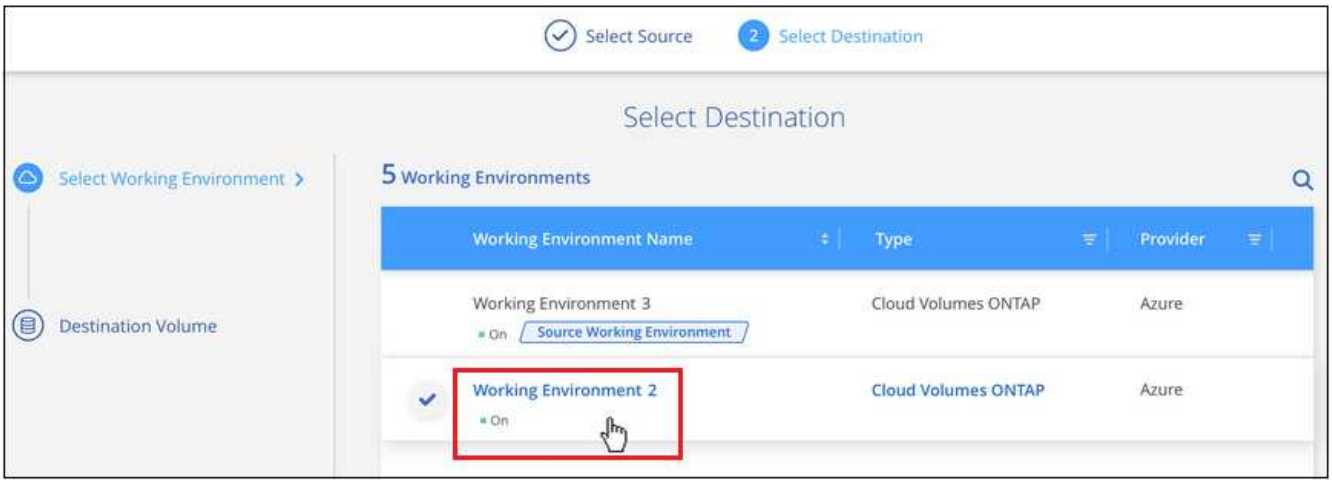
4. Navigieren Sie auf der Seite *Quelle auswählen* zur Sicherungsdatei für das Volume, das Sie wiederherstellen möchten. Wählen Sie die Datei * Working Environment*, **Volume** und die Datei **Backup** aus, die den Datums-/Zeitstempel enthält, aus dem Sie wiederherstellen möchten.




5. Klicken Sie Auf **Weiter**.

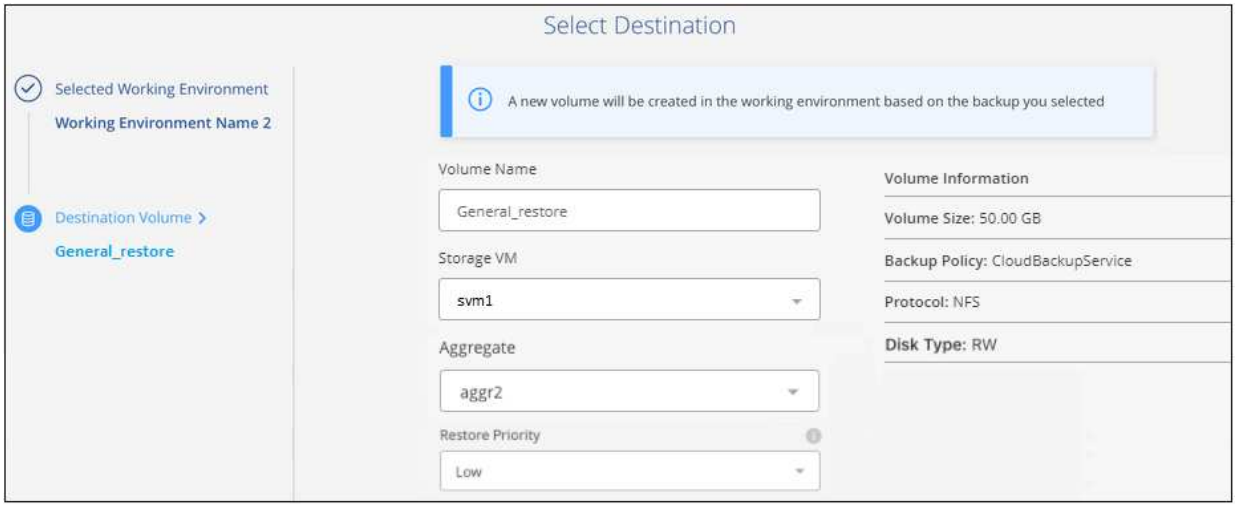
   Sollte der Ransomware-Schutz für die Backup-Datei aktiv sein (wenn Sie DataLock und Ransomware-Schutz in der Backup-Richtlinie aktiviert haben), werden Sie aufgefordert, vor dem Wiederherstellen der Daten einen zusätzlichen Ransomware-Scan auf der Backup-Datei durchzuführen. Wir empfehlen, die Backup-Datei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

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




7. Wenn Sie ein lokales ONTAP System auswählen und die Cluster-Verbindung mit dem Objekt-Storage nicht bereits konfiguriert haben, werden zusätzliche Informationen benötigt:
   - Wählen Sie bei der Wiederherstellung aus 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.

     a. Geben Sie den Namen ein, den Sie für das wiederhergestellte Volume verwenden möchten, und wählen Sie die Storage VM und das Aggregat aus, auf dem sich das Volume befinden soll. Standardmäßig wird **<source_Volume_Name>_restore** als Volume-Name verwendet.




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

"Erfahren Sie mehr über die Wiederherstellung aus 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 **Wiederherstellen** und Sie werden wieder zum Restore Dashboard zurückgekehrt, damit Sie den Fortschritt des Wiederherstellungsvorgangs überprüfen können.

**Ergebnis**

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

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

**Wiederherstellen von Ordnern und Dateien mit Durchsuchen und Wiederherstellen**

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

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

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

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

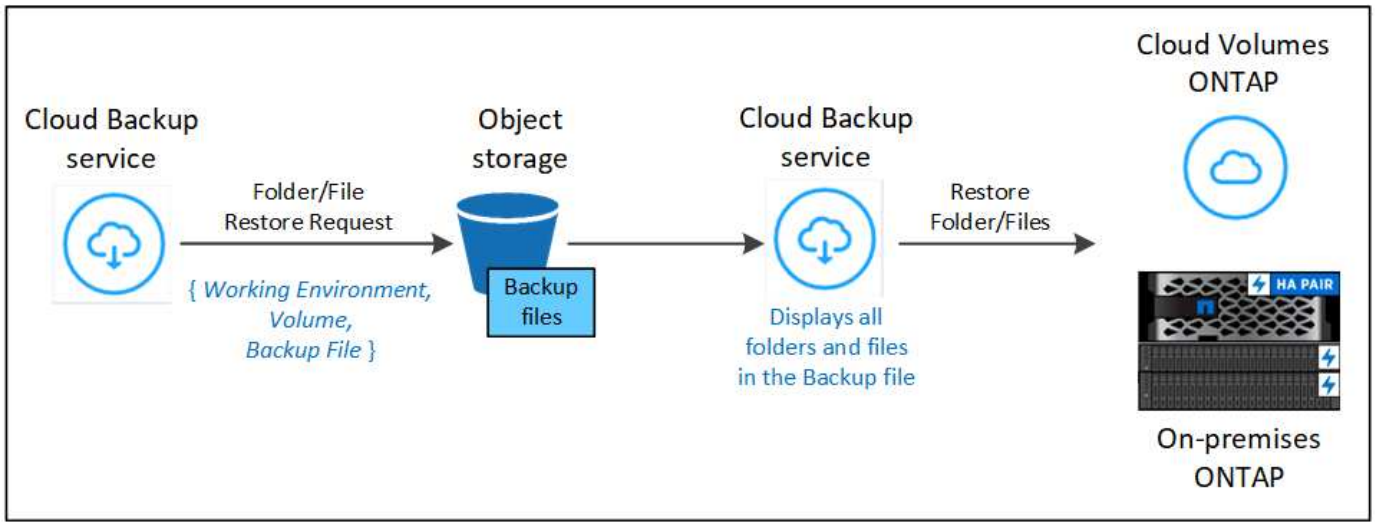
#### Voraussetzungen

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

#### Wiederherstellung von Ordnern und Dateien

Der Prozess geht wie folgt vor:

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

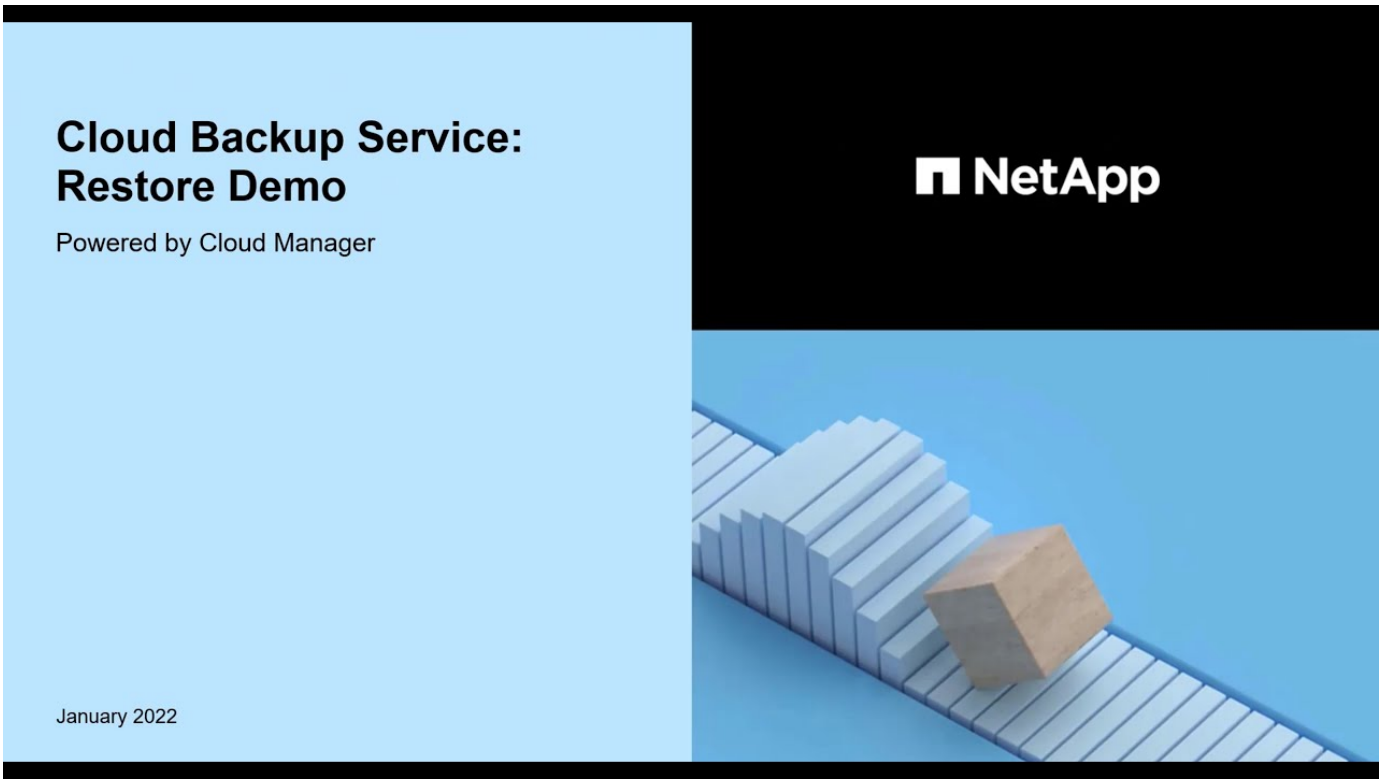



Wie Sie sehen, müssen Sie den Namen der Arbeitsumgebung, den Namen des Volumes, das Datum der Sicherungsdatei und den Ordner-/Dateinamen kennen, um einen Ordner oder eine Dateiwiederherstellung durchzuführen.

#### Ordner und Dateien werden wiederhergestellt

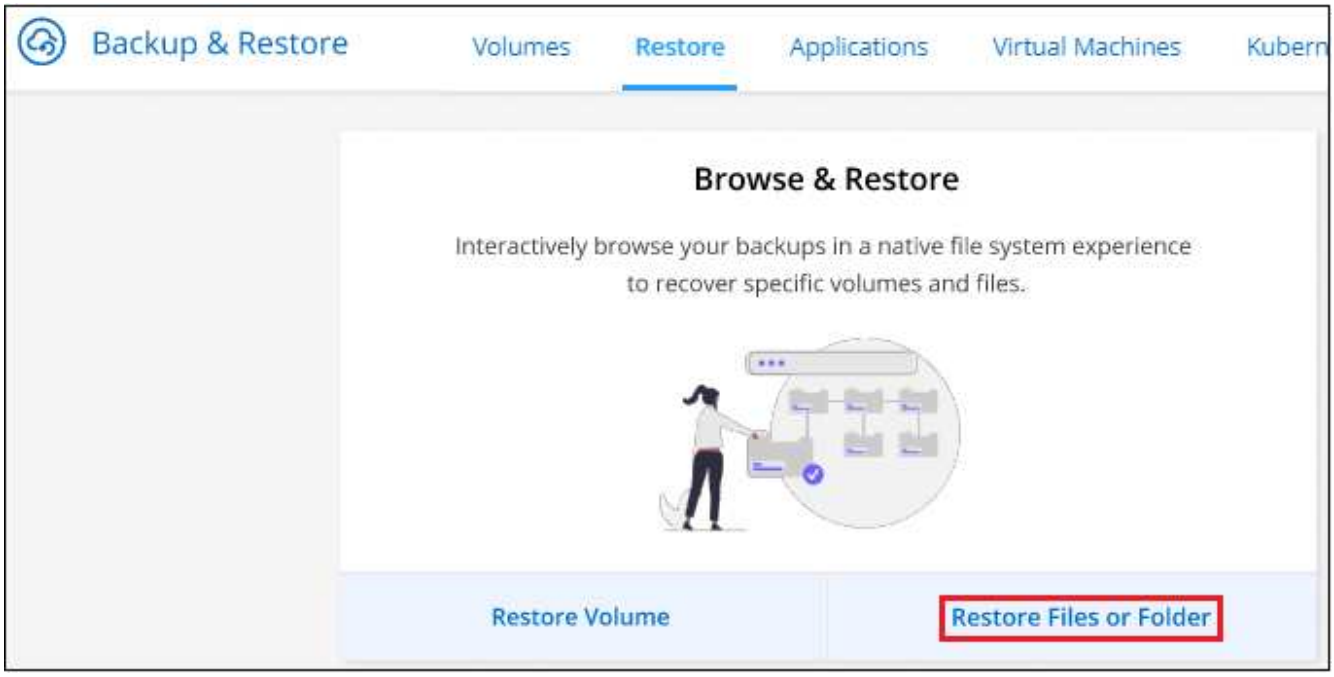
Führen Sie diese Schritte aus, um Ordner oder Dateien auf einem Volume von einem ONTAP Volume-Backup wiederherzustellen. Sie sollten den Namen des Volumes und das Datum der Sicherungsdatei kennen, die Sie zum Wiederherstellen des Ordners oder der Datei(en) verwenden möchten. Diese Funktion verwendet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

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

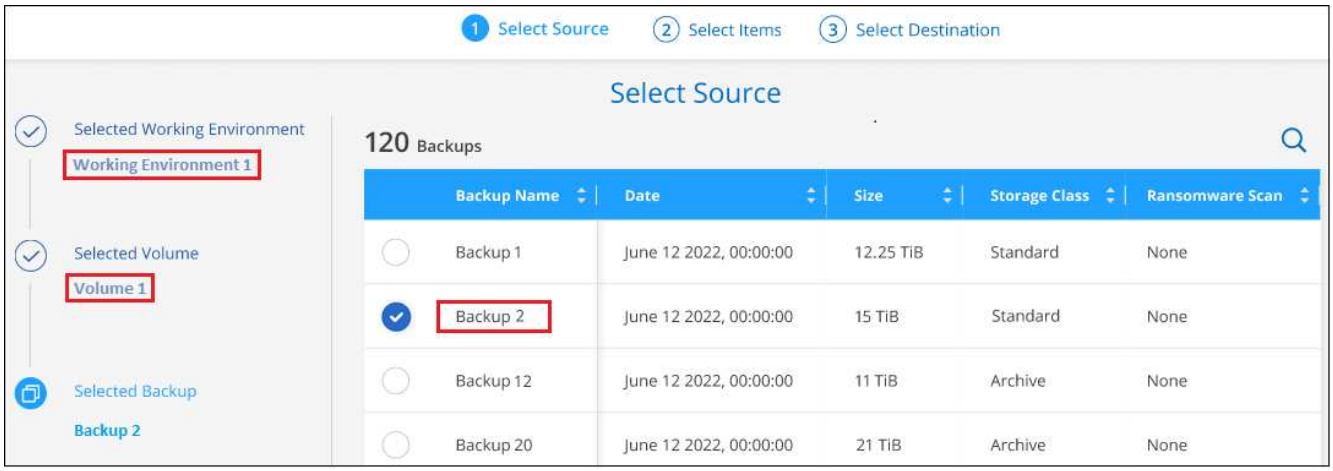



**Schritte**

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




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



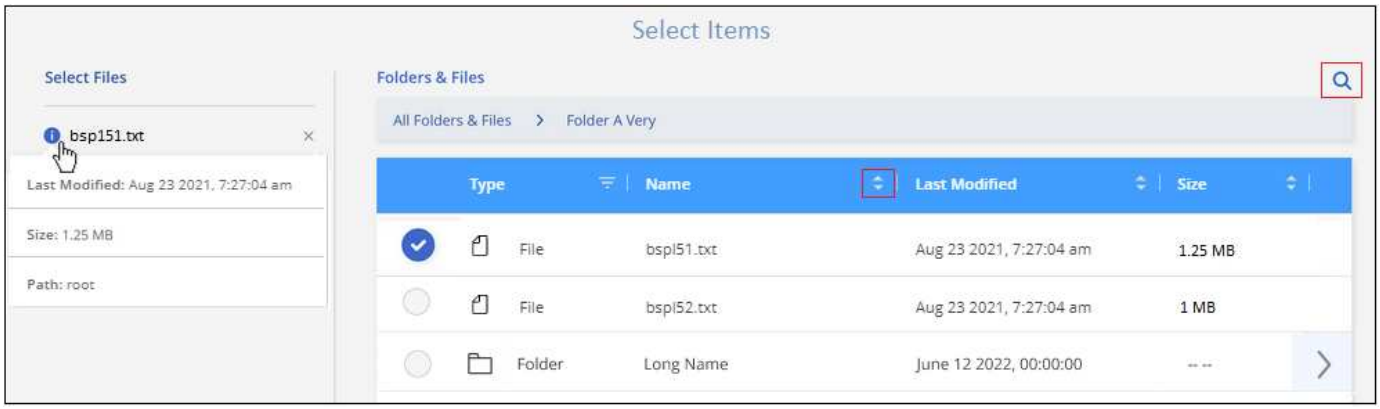

5. Klicken Sie auf **Weiter** und die Liste der Ordner und Dateien aus der Volume-Sicherung wird angezeigt.

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

"Erfahren Sie mehr über die Wiederherstellung aus Google Archiv-Storage". Backup-Dateien werden auf der Google Archiv Storage Tier nahezu sofort wiederhergestellt und müssen keine Restore-Priorität erhalten.

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

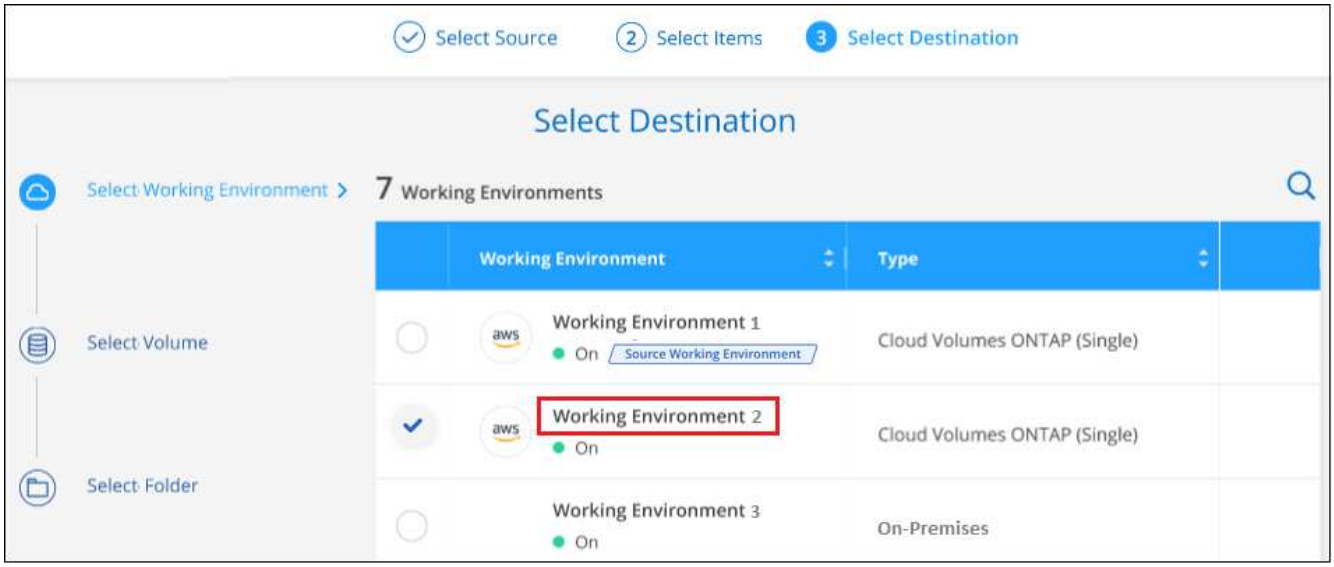
+




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

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

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

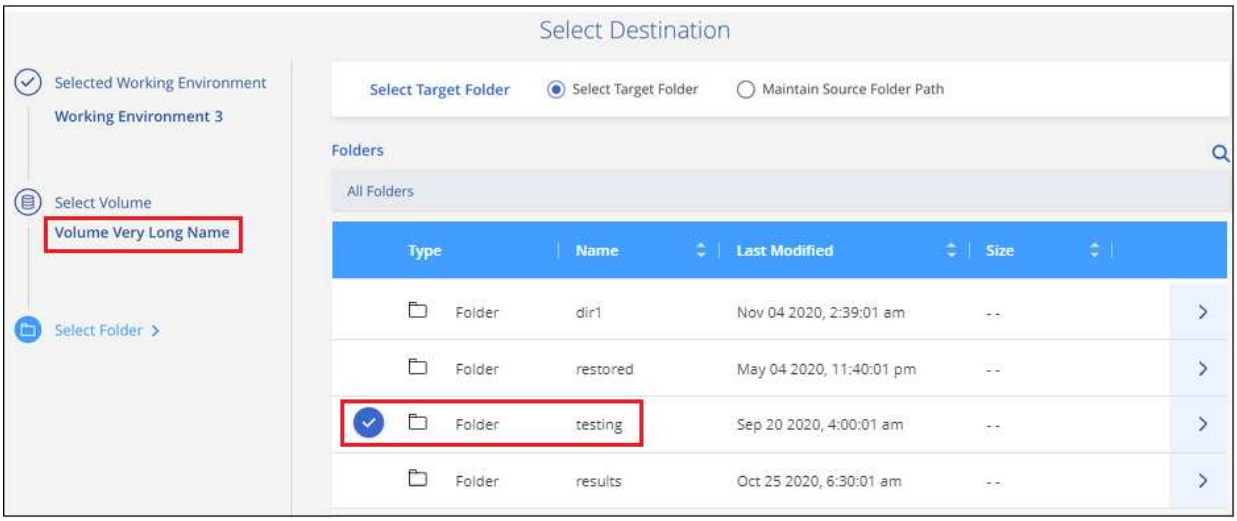



   Wenn Sie ein On-Premises-Cluster auswählen und noch nicht die Cluster-Verbindung mit dem Objekt-Storage konfiguriert haben, werden zusätzliche Informationen benötigt:

   - 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.

## Wiederherstellen von ONTAP-Daten mithilfe von Suche und Wiederherstellung

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

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

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

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

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

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

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

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

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

### Unterstützte Arbeitsumgebungen und Objektspeicheranbieter suchen und wiederherstellen

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

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

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

- Für Google Cloud Storage muss der Connector in Ihrer Google Cloud Platform VPC implementiert werden
- Für StorageGRID muss der Connector in Ihrem Haus bereitgestellt werden; mit Internetverbindung

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

### Voraussetzungen

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

verfügen.

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

- 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".

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

- StorageGRID-Anforderungen:

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

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

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

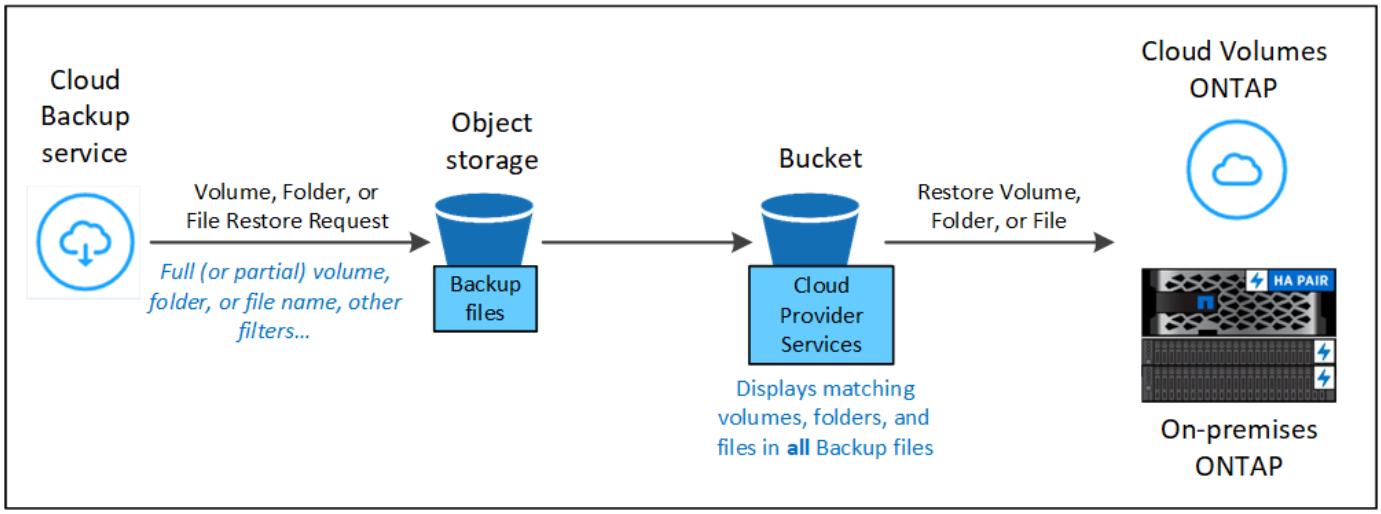
### Such- und Wiederherstellungsvorgang

Der Prozess geht wie folgt vor:

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

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

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




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

### Aktivierung des indizierten Katalogs für jede Arbeitsumgebung

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

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

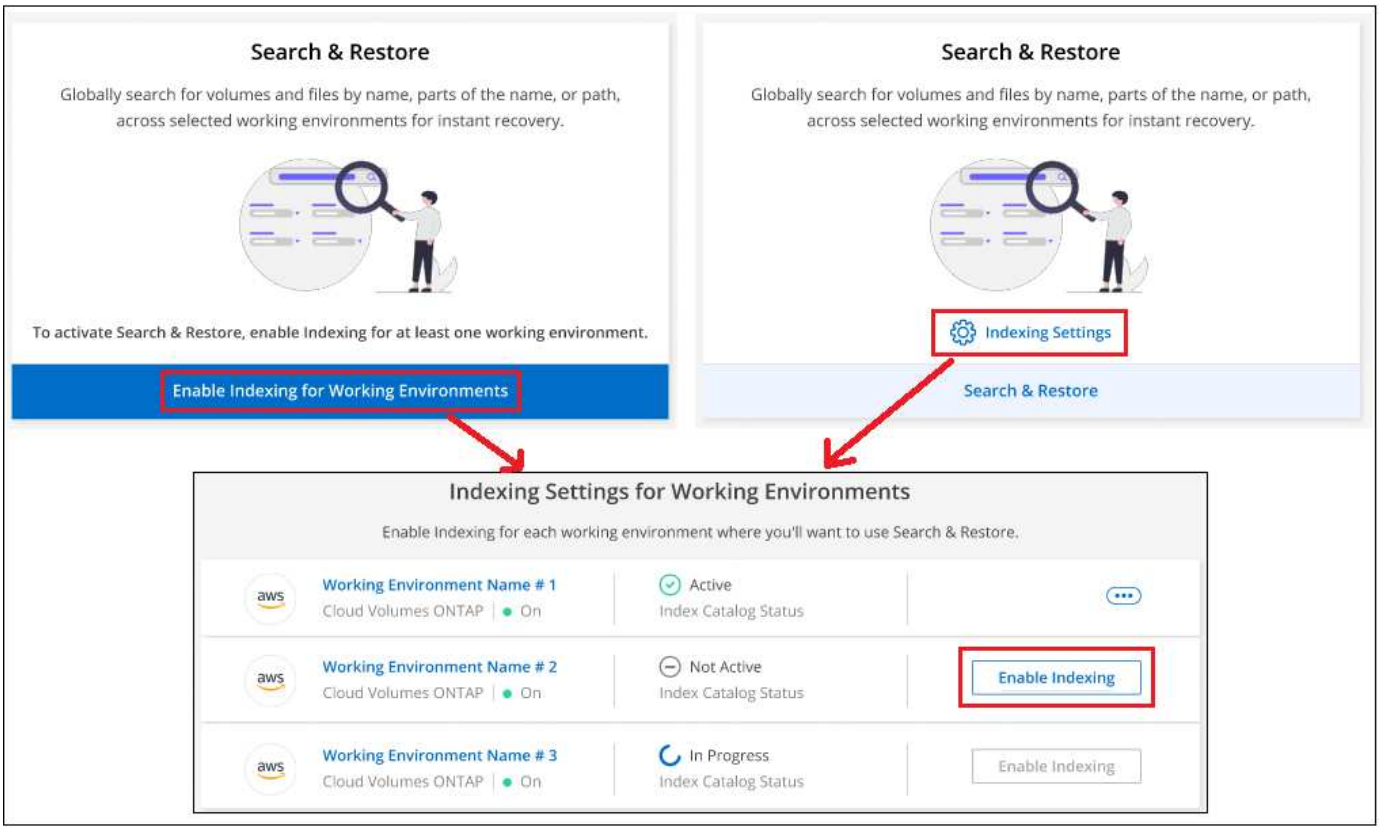
- Für Backups, die in Google Cloud gespeichert sind, stellt die IT einen neuen Bucket bereit und "Google Cloud BigQuery Services" Werden auf Konto-/Projektebene bereitgestellt.
- Für Backups, die in StorageGRID gespeichert sind, stellt das Unternehmen Speicherplatz auf dem Connector oder der Cloud-Provider-Umgebung bereit.

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

So aktivieren Sie die Indizierung für eine Arbeitsumgebung:

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

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




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

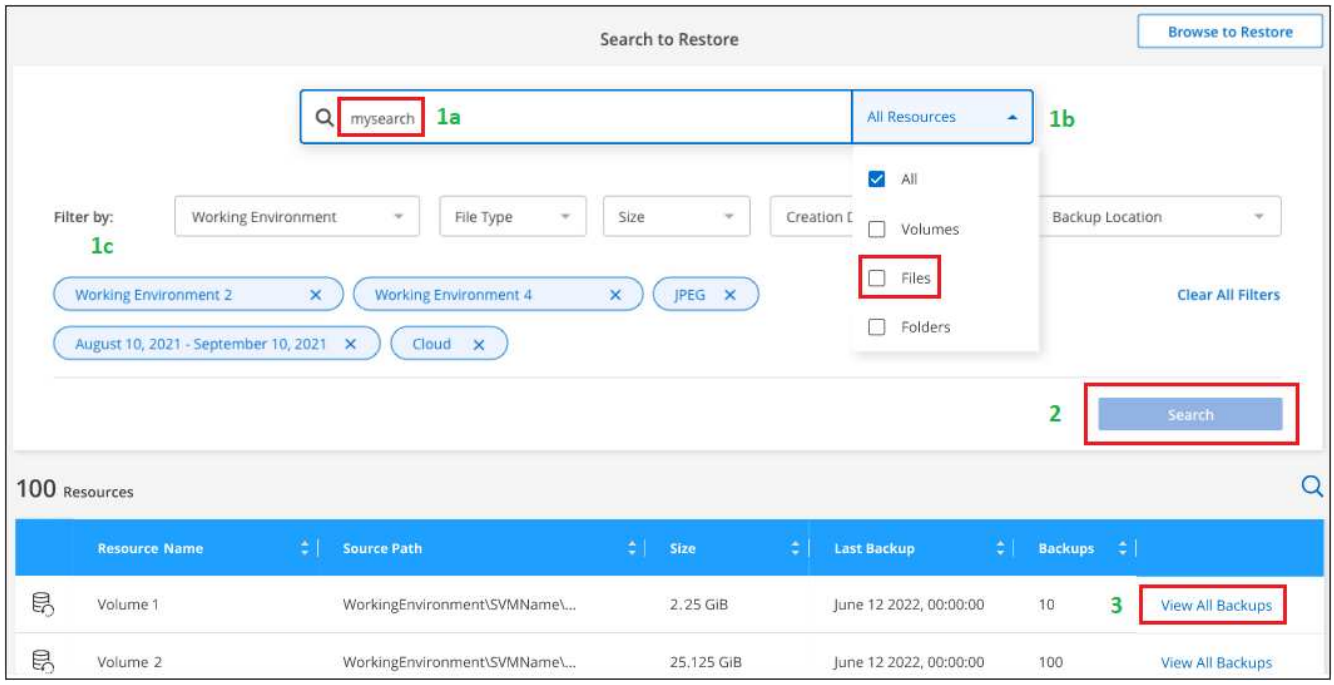
### Wiederherstellen von Volumes, Ordnern und Dateien mithilfe von Search & Restore

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

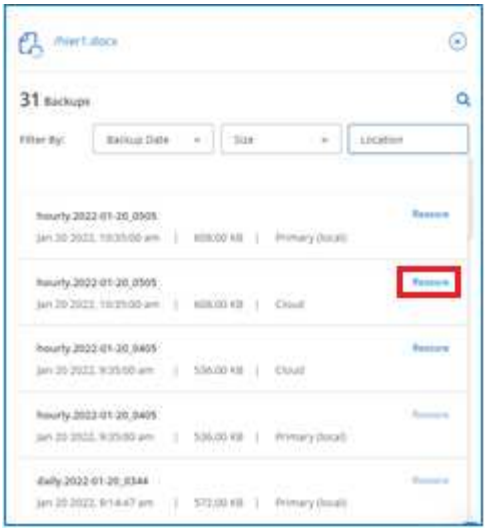
#### Schritte

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

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




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




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

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

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

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

     - Wählen Sie bei der Wiederherstellung aus 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".

**Ergebnisse**

Die Volume-, Ordner- oder Datei(en) werden wiederhergestellt und Sie werden zum Restore Dashboard zurückgebracht, damit Sie den Fortschritt des Wiederherstellungsvorgangs überprüfen können. Sie können

auch auf die Registerkarte **Job Monitoring** klicken, um den Wiederherstellungsfortschritt anzuzeigen.

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

# Backup und Wiederherstellung von Kubernetes-Daten

## Kubernetes-Cluster-Daten mit Cloud Backup schützen

Cloud Backup bietet Backup- und Restore-Funktionen zur Sicherung und zum langfristigen Archiv Ihrer Kubernetes-Cluster-Daten. Backups werden automatisch erstellt und in einem Objektspeicher in Ihrem Public oder Private Cloud-Konto gespeichert.

Bei Bedarf können Sie ein ganzes *Volume* von einem Backup in dieselbe oder andere Arbeitsumgebung wiederherstellen.

### Funktionen

Backup-Funktionen:

- Sichern Sie unabhängige Kopien Ihrer persistenten Volumes 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
- Backup-Daten werden mit AES-256-Bit-Verschlüsselung im Ruhezustand und TLS 1.2 HTTPS-Verbindungen im Übertragungsprozess gesichert.
- Unterstützung für bis zu 4,000 Backups eines einzelnen Volumes.

Wiederherstellungsfunktionen:

- Wiederherstellung von Daten aus einem bestimmten Zeitpunkt
- Stellen Sie ein Volume auf dem Quellsystem oder einem anderen System wieder her.
- Stellt Daten auf Blockebene wieder her, indem die Daten direkt an dem von Ihnen angegebenen Speicherort platziert werden, während gleichzeitig die ursprünglichen ACLs beibehalten werden.

### Unterstützte Kubernetes-Arbeitsumgebungen und Objekt-Storage-Provider

Cloud Backup ermöglicht die Erstellung von Kubernetes Volumes aus den folgenden Arbeitsumgebungen in Objekt-Storage bei folgenden Public- und Private-Cloud-Providern:

| Quelle Arbeitsumgebung | Ziel der Backup-Datei ifdef::aws[] |
|---|---|
| Kubernetes-Cluster in AWS | Amazon S3 endif::aws[] ifdef::Azure[] |
| Kubernetes-Cluster in Azure | Azure Blob endif::Azure[] ifdef::gcp[] |
| Kubernetes-Cluster in Google | Google Cloud Storage endif::gcp[] |

Sie können ein Volume aus einer Kubernetes-Backup-Datei in den folgenden Arbeitsumgebungen wiederherstellen:

| Speicherort Der Sicherungsdatei | Zielarbeitsumgebung ifdef::aws[] |
|---|---|
| Amazon S3 | Kubernetes Cluster in AWS endif::AWS[] ifdef::Azure[] |

| Speicherort Der Sicherungsdatei | Zielarbeitsumgebung ifdef::aws[] |
|---|---|
| Azure Blob | Kubernetes Cluster in Azure endif::Azure[] ifdef::gcp[] |
| Google Cloud Storage | Kubernetes Cluster in Google endif::gcp[] |

## Kosten

Mit Cloud Backup fallen zwei Kostenarten in Verbindung: Ressourcengebühren und Servicegebühren.

### Ressourcengebühren

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

### Servicegebühren

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

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

## Lizenzierung

Cloud Backup ist in zwei Lizenzoptionen erhältlich: Pay-as-you-go (PAYGO) und Bring-Your-Own-License (BYOL). Eine kostenlose 30-Tage-Testversion ist verfügbar, wenn Sie keine Lizenz haben.

### Kostenlose Testversion

Wenn Sie die kostenlose 30-Tage-Testversion verwenden, werden Sie über die Anzahl der kostenlosen Testtage informiert, die noch verbleiben. Am Ende Ihrer kostenlosen Testversion werden Backups nicht mehr erstellt. Sie müssen den Service abonnieren oder eine Lizenz erwerben, um den Service weiterhin nutzen zu können.

Sicherungsdateien werden nicht gelöscht, wenn der Dienst deaktiviert ist. Cloud-Provider stellen weiterhin die Kosten für Objekt-Storage für die von Ihren Backups verwendete Kapazität in Rechnung, es sei denn, die Backups werden gelöscht.

### Pay-as-you-go-Abonnement

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

Sie sollten sich auch dann abonnieren, wenn Sie eine kostenlose Testversion haben oder Ihre eigene Lizenz mitbringen (BYOL):

- Das Abonnieren sorgt dafür, dass es keine Serviceunterbrechung gibt, nachdem Ihre kostenlose Testversion endet.

  Wenn die Studie endet, werden Sie stündlich nach der Menge der Daten, die Sie sichern berechnet.

- Wenn Sie mehr Daten als mit Ihrer BYOL-Lizenz zulässig sichern, wird das Daten-Backup über Ihr Pay-as-you-go-Abonnement fortgesetzt.

  Wenn Sie beispielsweise eine 10-TB-BYOL-Lizenz haben, wird die gesamte Kapazität über 10 TB hinaus über das PAYGO Abonnement abgerechnet.

Sie werden nicht von Ihrem Pay-as-you-go-Abonnement während der kostenlosen Testversion oder wenn Sie nicht überschritten haben Ihre Byol-Lizenz.

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

**Mit Ihrer eigenen Lizenz**

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

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

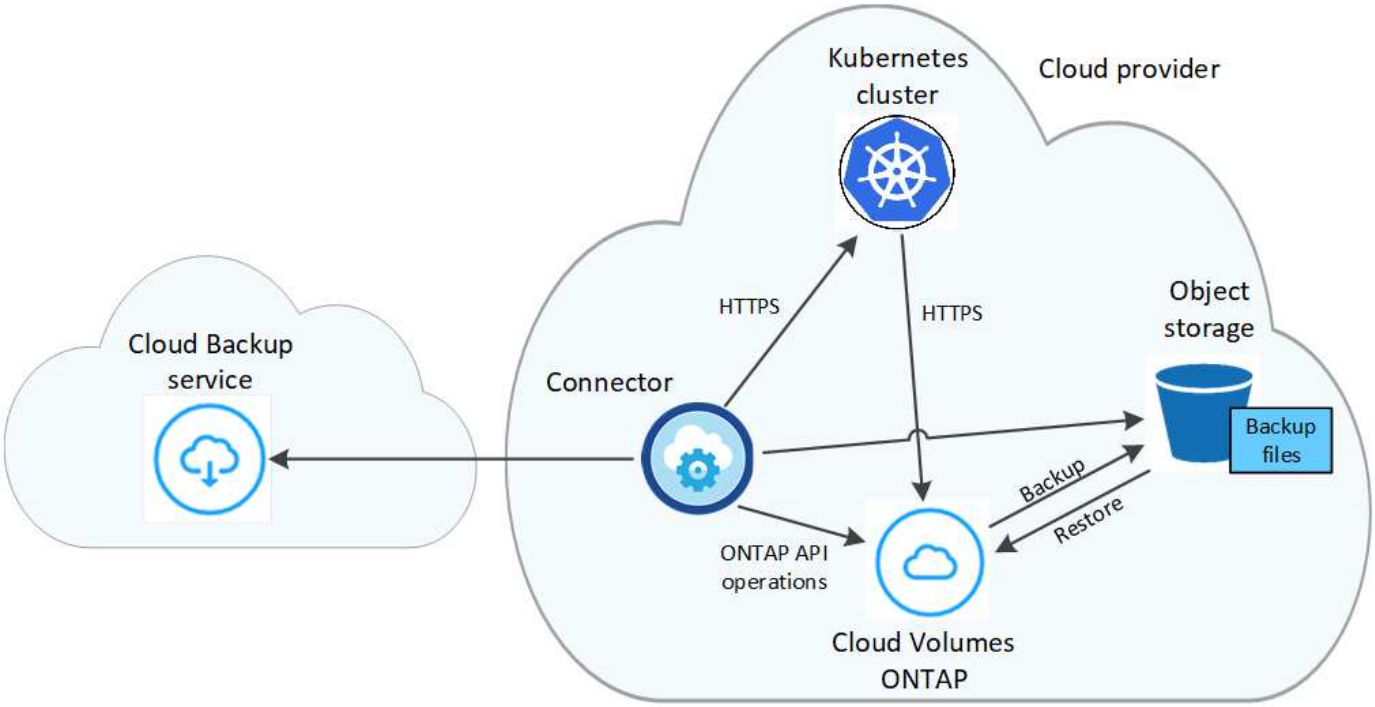
"Erfahren Sie, wie Sie Ihre BYOL-Lizenzen managen".

## Funktionsweise von Cloud Backup

Wenn Sie Cloud-Backup auf einem Kubernetes-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.

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

Die folgende Abbildung zeigt die Beziehung zwischen den einzelnen Komponenten:




**Unterstützte Storage-Klassen oder Zugriffsebenen**

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

**Individuell anpassbare Backup-Zeitpläne und Aufbewahrungseinstellungen pro Cluster**

Wenn Sie Cloud-Backup für eine Arbeitsumgebung aktivieren, werden alle Volumes, die Sie anfangs auswählen, mithilfe der 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.

Es steht eine Kombination aus stündlichen, täglichen, wöchentlichen und monatlichen Backups aller Volumes zur Verfügung.

Sobald Sie die maximale Anzahl von Backups für eine Kategorie oder ein Intervall erreicht haben, werden ältere Backups entfernt, sodass Sie immer über die aktuellsten Backups verfügen.

## Unterstützte Volumes

Cloud Backup unterstützt persistente Volumes (PVS).

## Einschränkungen

- Wenn eine Backup-Richtlinie erstellt oder bearbeitet wird, wenn dieser Richtlinie keine Volumes zugewiesen werden, kann die Anzahl der zurückbehaltenen Backups maximal 1018 sein. Als Workaround können Sie die Anzahl der Backups zur Erstellung der Richtlinie verringern. Anschließend können Sie die Richtlinie bearbeiten, um bis zu 4000 Backups zu erstellen, nachdem Sie der Richtlinie Volumes zugewiesen haben.
- Ad-hoc-Volume-Backups mit dem Button **Backup Now** werden auf Kubernetes-Volumes nicht unterstützt.

# Sichern Sie persistente Kubernetes-Volume-Daten auf Google Cloud Storage

Führen Sie einige Schritte aus, um Daten von Ihren persistenten Volumes auf GKE Kubernetes-Clustern auf Google Cloud Storage zu sichern.

## Schnellstart

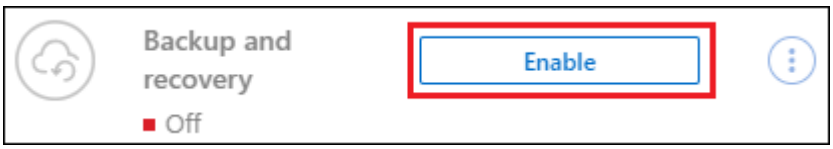
Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

### 1 Voraussetzungen prüfen

- Sie haben den Kubernetes Cluster als BlueXP-Arbeitsumgebung erkannt.
  - Trident muss auf dem Cluster installiert sein, und die Trident Version muss mindestens 21.1 sein.
  - Alle PVCs, die verwendet werden sollen, um persistente Volumes zu erstellen, die Sie sichern möchten, müssen „Snapshot Policy“ auf „Standard“ gesetzt sein.
  - Der Cluster muss für seinen Back-End Storage Cloud Volumes ONTAP auf GCP verwenden.
  - Das Cloud Volumes ONTAP System muss ONTAP 9.7P5 oder höher ausführen.
- Sie verfügen über ein gültiges GCP-Abonnement für den Speicherplatz, in dem sich Ihre Backups befinden.
- Sie verfügen über ein Service-Konto in Ihrem Google Cloud Projekt, das über die vordefinierte Rolle „Storage Admin“ verfügt.
- Sie haben sich für das angemeldet "BlueXP Marketplace Backup-Angebot", Oder Sie haben gekauft "Und aktiviert" Eine Cloud Backup BYOL-Lizenz von NetApp

### 2 Cloud Backup für bestehenden Kubernetes Cluster aktivieren

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




### 3 Definieren der Backup-Richtlinie

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

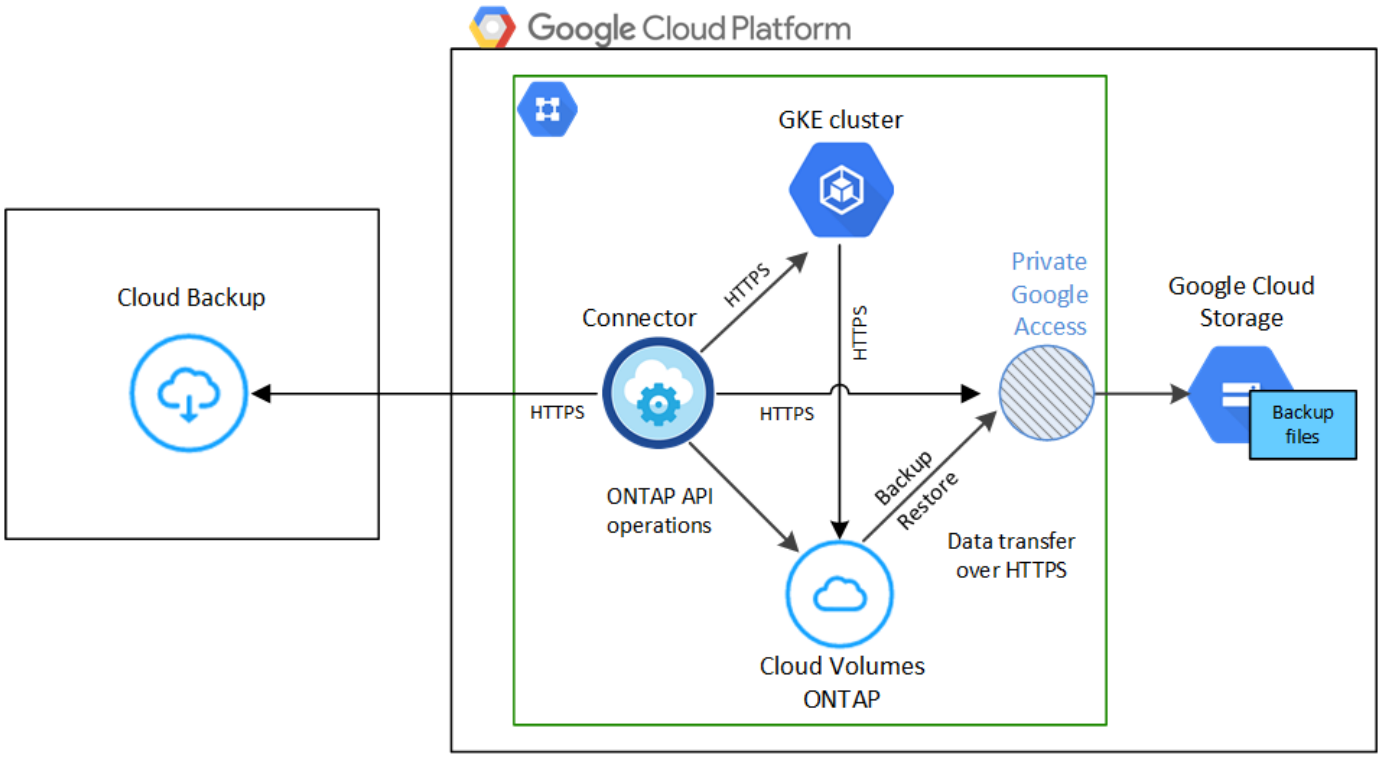
**4** **Wählen Sie die Volumes aus, die Sie sichern möchten**

Legen Sie fest, welche Volumes Sie in der Seite Volumes auswählen sichern möchten. Die Backup-Dateien werden in einem Google Cloud Storage Bucket gespeichert, der dasselbe GCP-Abonnement und dieselbe Region wie das Cloud Volumes ONTAP System verwendet.

## Anforderungen

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie mit dem Backup persistenter Kubernetes-Volumes in Google Cloud-Storage beginnen.

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




Beachten Sie, dass der private Endpunkt optional ist.

**Kubernetes-Cluster-Anforderungen**

- Sie haben den Kubernetes Cluster als BlueXP-Arbeitsumgebung erkannt. "Erkennung des Kubernetes-Clusters".
- Trident muss auf dem Cluster installiert werden, und die Trident Version muss mindestens 21.1 sein. Siehe "Anleitung zur Installation von Trident" Oder "So aktualisieren Sie die Trident Version".
- Der Cluster muss für seinen Back-End Storage Cloud Volumes ONTAP auf GCP verwenden.
- Das Cloud Volumes ONTAP System muss sich in derselben GCP-Region wie der Kubernetes-Cluster befinden. Es muss ONTAP 9.7P5 oder höher ausgeführt werden (ONTAP 9.8P11 und höher wird empfohlen).

  Beachten Sie, dass Kubernetes-Cluster an On-Premises-Standorten nicht unterstützt werden. Es werden nur Kubernetes-Cluster in Cloud-Implementierungen unterstützt, die Cloud Volumes ONTAP Systeme nutzen.

- Für alle Persistent Volume Claim-Objekte, die zum Erstellen der persistenten Volumes verwendet werden sollen, die Sie sichern möchten, muss „Snapshot Policy“ auf „Standard“ gesetzt sein.

  Sie können dies für einzelne VES tun, indem Sie hinzufügen `snapshotPolicy` Unter Anmerkungen:

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver
```

  Sie können dies für alle VES, die mit einem bestimmten Back-End-Speicher verknüpft sind, tun, indem Sie die hinzufügen `snapshotPolicy` Feld unter den Standardeinstellungen im `backend.json` Datei:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
  deletionPolicy: retain
```

**Unterstützte GCP-Regionen**

Cloud Backup wird in allen GCP-Regionen unterstützt "Wobei Cloud Volumes ONTAP unterstützt wird".

**Lizenzanforderungen**

Für Cloud Backup PAYGO-Lizenzen ist ein Abonnement über das verfügbar "GCP Marketplace" Ist erforderlich, bevor Sie Cloud Backup aktivieren. Die Abrechnung für Cloud Backup erfolgt über dieses Abonnement. "Sie können sich auf der Seite Details Credentials des Assistenten für die Arbeitsumgebung anmelden".

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

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

**GCP-Service-Konto**

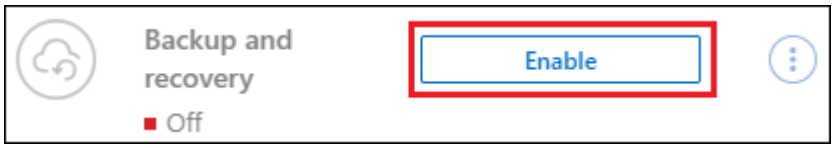
Sie benötigen ein Servicekonto in Ihrem Google Cloud Projekt, das über die vordefinierte Rolle „Storage Admin“ verfügt. "Erfahren Sie, wie Sie ein Servicekonto erstellen".

## Unterstützung Von Cloud Backup

Cloud-Backup kann jederzeit direkt aus der Kubernetes-Arbeitsumgebung aktiviert werden.

**Schritte**

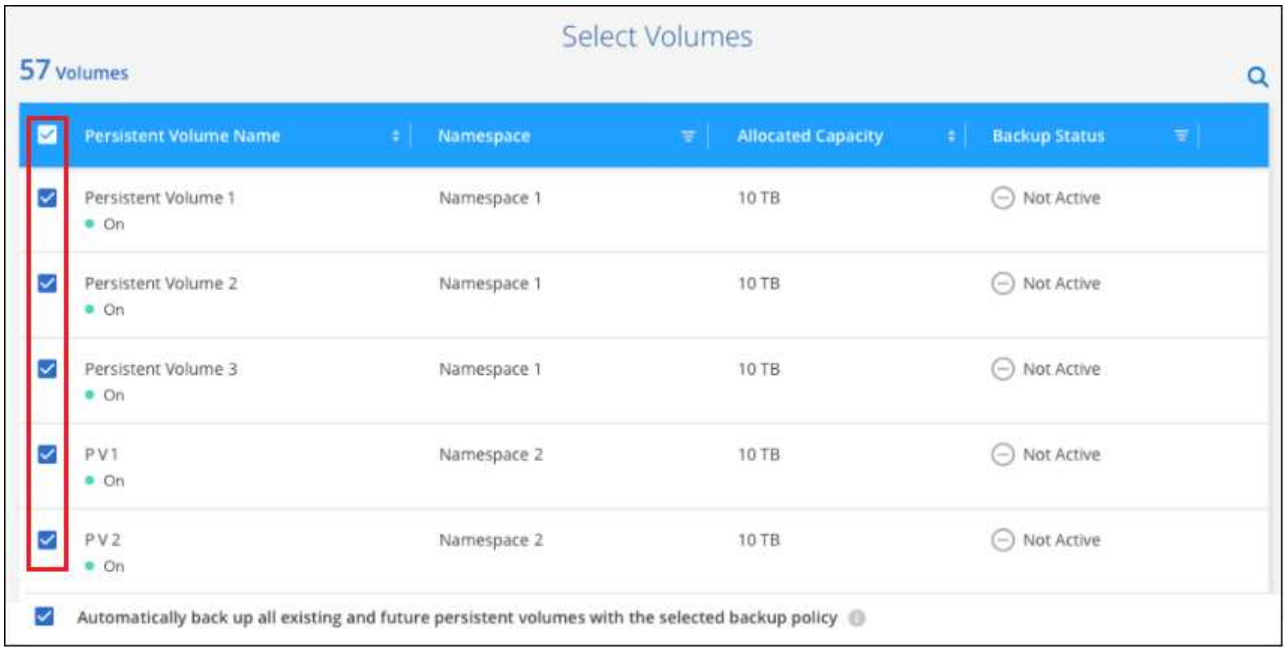
1. Wählen Sie die Arbeitsumgebung aus und klicken Sie auf **Aktivieren** neben dem Backup- und Recovery-Dienst im rechten Fenster.




2. Geben Sie die Backup Policy Details ein und klicken Sie auf **Weiter**.

   Sie können den Backup-Zeitplan festlegen und die Anzahl der zu behaltenden Backups auswählen.

3. Wählen Sie die persistenten Volumes aus, die Sie sichern möchten.
   - Um alle Volumes zu sichern, aktivieren Sie das Kontrollkästchen in der Titelzeile ( Volume Name ).
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume ( Volume_1 ).




4. Wenn Sie möchten, dass alle aktuellen und zukünftigen Volumes Backups aktiviert sind, lassen Sie einfach das Kontrollkästchen „zukünftige Volumes automatisch sichern…“ aktiviert. Wenn Sie diese Einstellung deaktivieren, müssen Sie manuell Backups für zukünftige Volumes aktivieren.

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

**Ergebnis**

Die Backup-Dateien werden in einem Google Cloud Storage Bucket gespeichert, der dasselbe GCP-Abonnement und dieselbe Region wie das Cloud Volumes ONTAP System verwendet.

Das Kubernetes Dashboard wird angezeigt, damit Sie den Status der Backups überwachen können.

**Was kommt als Nächstes?**

Das können Sie "Starten und Stoppen von Backups für Volumes oder Ändern des Backup-Zeitplans". Das können Sie auch "Wiederherstellung vollständiger Volumes aus einer Backup-Datei" Für ein neues Volume im selben oder einem anderen Kubernetes Cluster in GCP (in derselben Region).

# Das Backup-Management für Kubernetes-Systeme

Backups für Kubernetes-Systeme lassen sich verwalten, indem der Backup-Zeitplan geändert, Volume-Backups aktiviert/deaktiviert, Backups gelöscht usw.

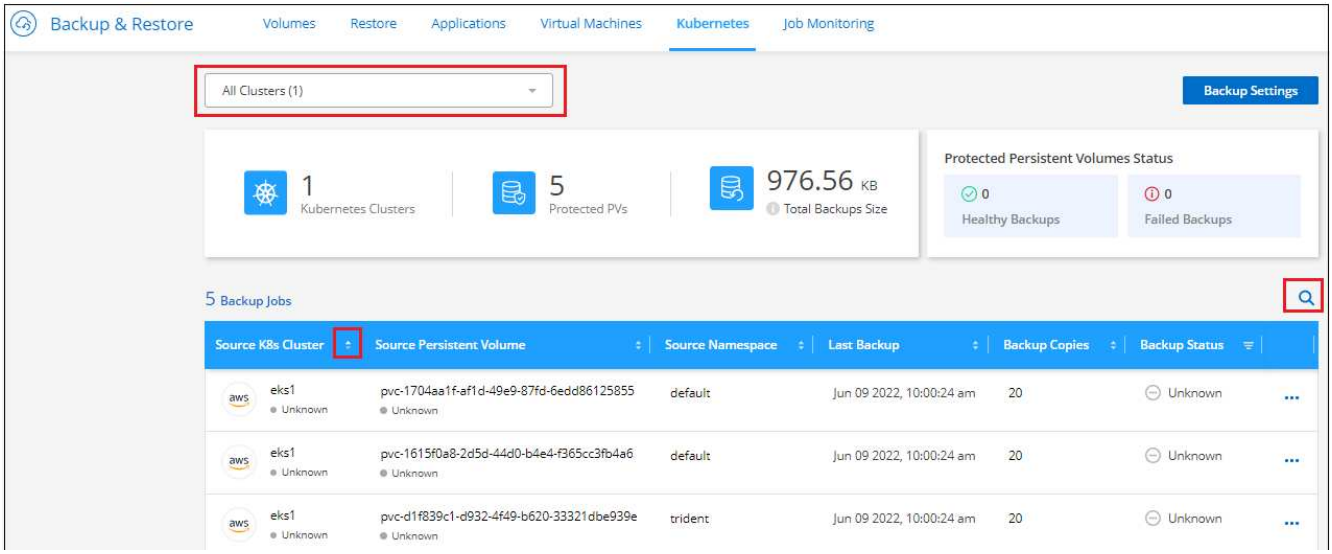
> Backup-Dateien lassen sich nicht direkt in der Umgebung Ihrer Cloud-Provider managen oder ändern. Dies kann die Dateien beschädigen und zu einer nicht unterstützten Konfiguration führen.

## Anzeigen der Volumes, die gesichert werden

Sie können eine Liste aller Volumes anzeigen, die derzeit durch Cloud Backup gesichert werden.

**Schritte**

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



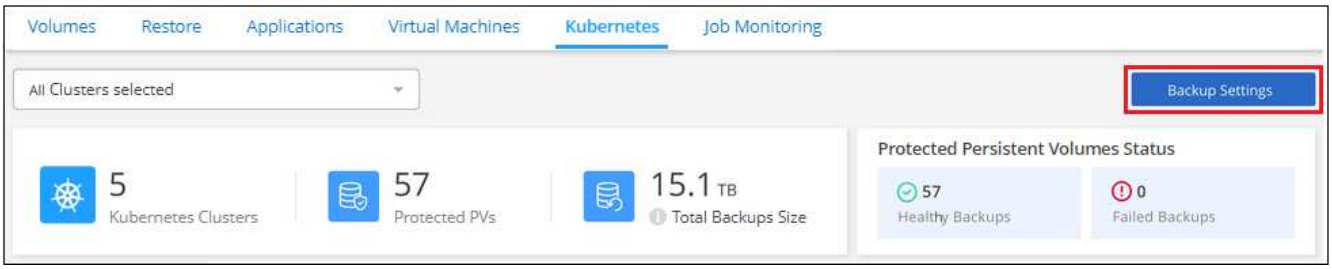

Wenn Sie in bestimmten Clustern nach bestimmten Volumes suchen, können Sie die Liste nach Cluster und Volume verfeinern oder Sie verwenden den Suchfilter.

## Aktivieren und Deaktivieren von Backups von Volumes

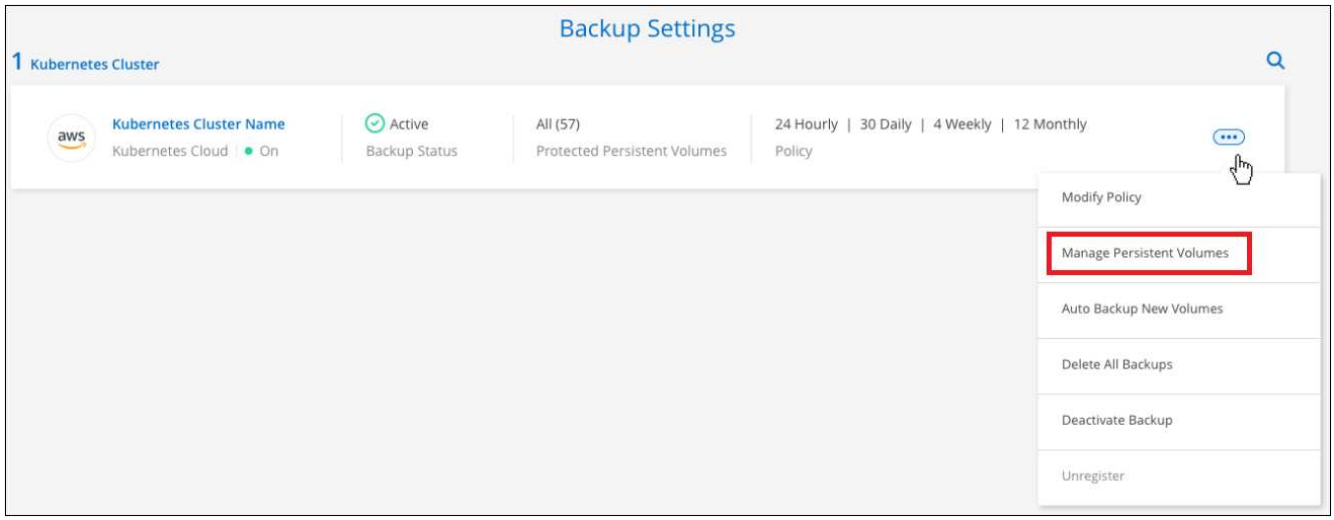
Sie können die Sicherung eines Volumes anhalten, wenn Sie keine Backup-Kopien dieses Volumes benötigen und nicht für die Kosten für die Speicherung der Backups bezahlen möchten. Sie können auch ein neues Volume zur Backup-Liste hinzufügen, wenn das Volume derzeit nicht gesichert wird.

### Schritte

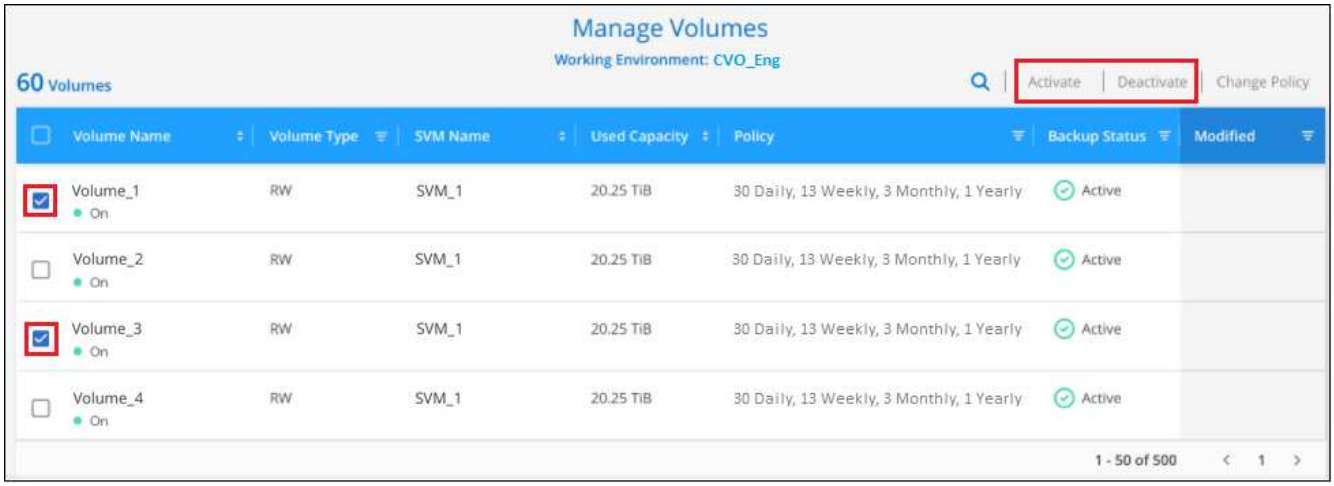
1. Wählen Sie auf der Registerkarte **Kubernetes** die Option **Backup-Einstellungen** aus.




2. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Wählen Sie für den Kubernetes-Cluster **Persistent Volumes** managen aus.




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



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

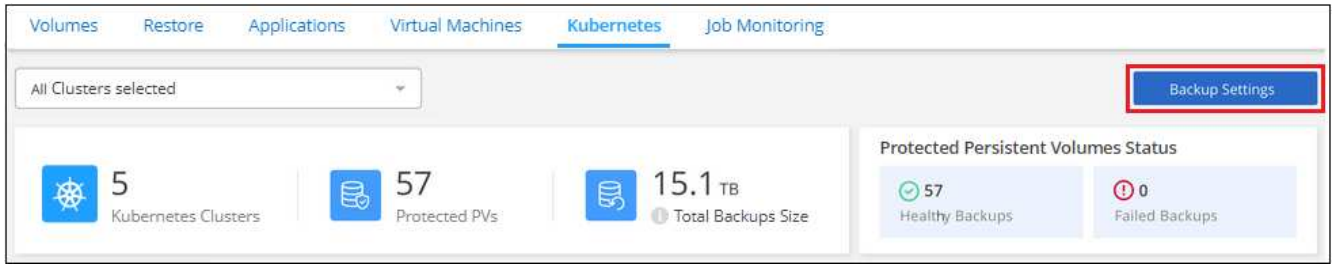
**Hinweis:** Wenn ein Volume nicht gesichert werden soll, werden Sie Ihrem Cloud Provider weiterhin die Kosten für die Objektspeicherung für die Kapazität in Rechnung gestellt, die die Backups nutzen, es sei denn, Sie Löschen Sie die Backups.

## Bearbeiten einer vorhandenen Backup-Richtlinie

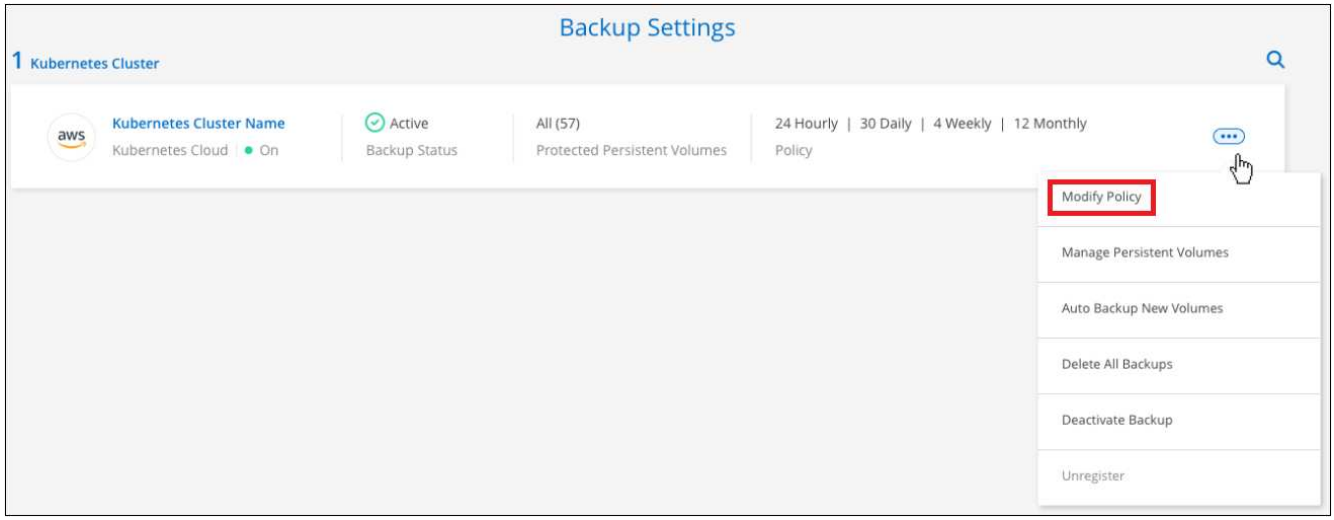
Sie können die Attribute für eine Backup-Richtlinie ändern, die derzeit auf Volumes in einer Arbeitsumgebung angewendet wird. Die Änderung der Backup-Richtlinie wirkt sich auf alle vorhandenen Volumes aus, die diese Richtlinie verwenden.

### Schritte

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

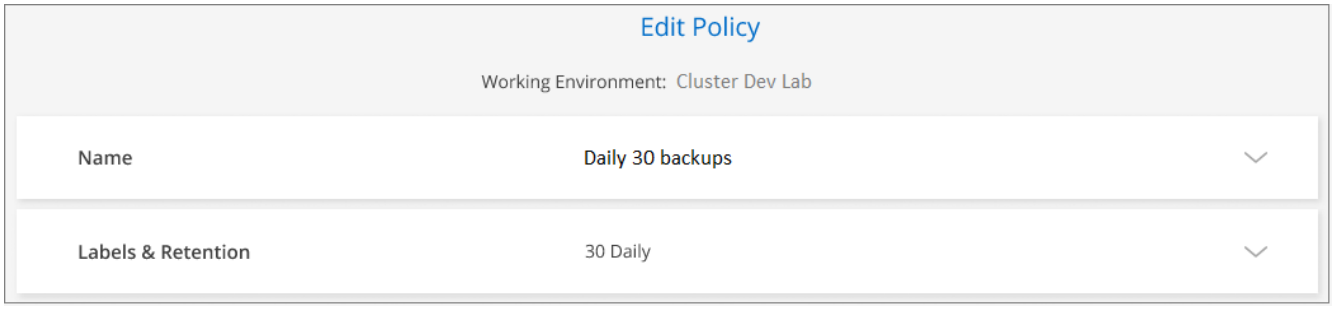



2. Klicken Sie auf der Seite „ Backup Settings_“ auf ••• Wählen Sie für die Arbeitsumgebung, in der Sie die Einstellungen ändern möchten, und wählen Sie **Richtlinien verwalten**.




3. Klicken Sie auf der Seite *Manage Policies* auf **Edit Policy** für die Backup Policy, die Sie in dieser Arbeitsumgebung ändern möchten.

4. Ändern Sie auf der Seite *Edit Policy* den Zeitplan und die Backup-Aufbewahrung und klicken Sie auf **Save**.




## Legen Sie eine Backup-Richtlinie fest, die neuen Volumes zugewiesen werden soll

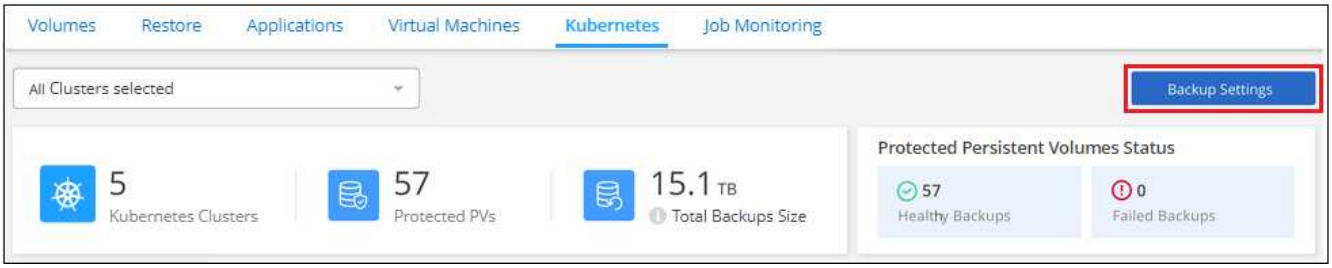
Falls Sie beim ersten Aktivieren von Cloud Backup auf Ihrem Kubernetes Cluster nicht die Option zum automatischen Zuweisen einer Backup-Richtlinie zu neu erstellten Volumes gewählt haben, können Sie diese Option später auf der Seite „*Backup Settings* “ auswählen. Eine Backup-Richtlinie, die neu erstellten Volumes zugewiesen wurde, stellt sicher, dass alle Ihre Daten geschützt sind.

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

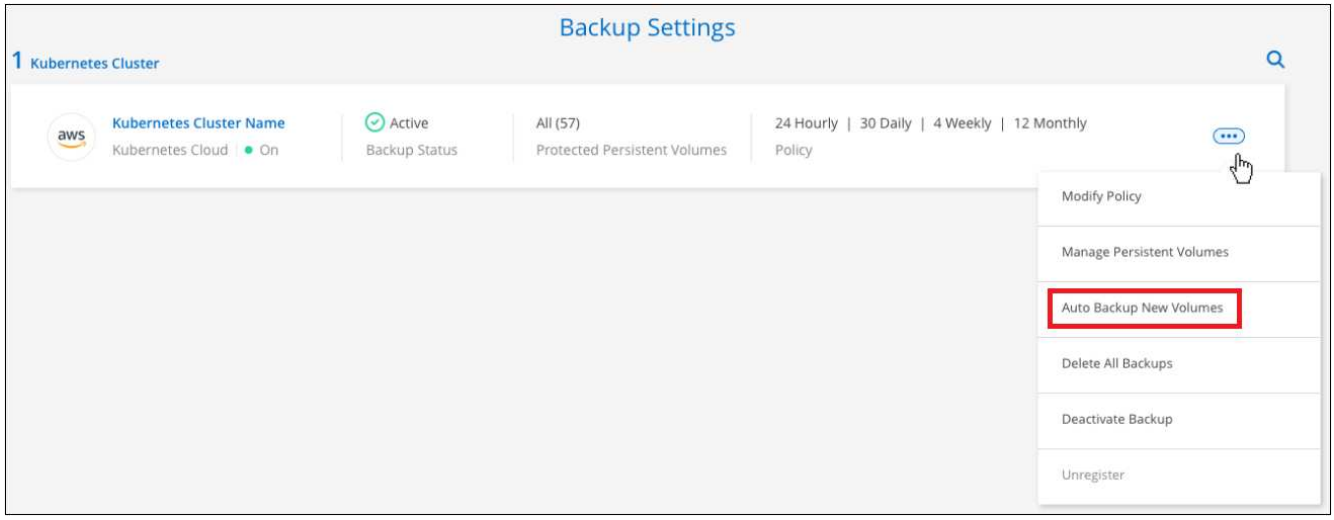
Sie können diese Einstellung auch deaktivieren, damit neu erstellte Volumes nicht automatisch gesichert werden. In diesem Fall müssen Sie Backups manuell für alle spezifischen Volumes aktivieren, die Sie in Zukunft sichern möchten.

### Schritte

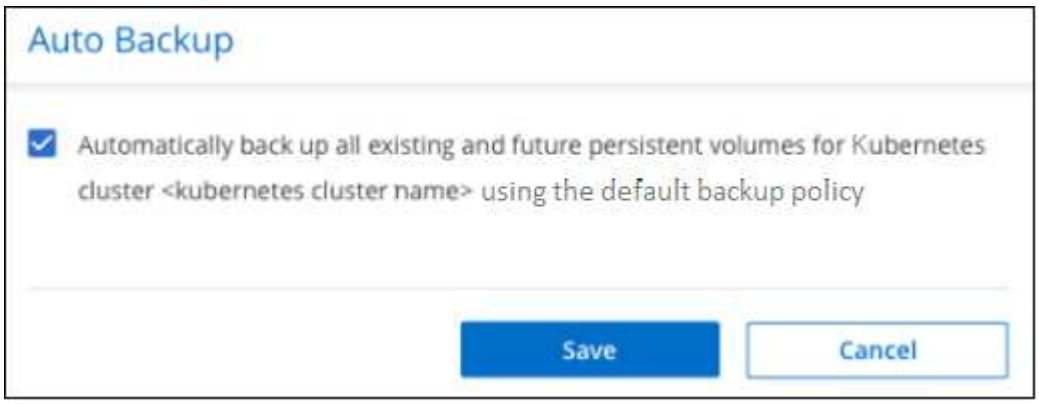
1. Wählen Sie auf der Registerkarte **Kubernetes** die Option **Backup-Einstellungen** aus.




2. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Wählen Sie für den Kubernetes-Cluster, in dem die Volumes vorhanden sind, **Auto Backup New Volumes** aus.




3. Aktivieren Sie das Kontrollkästchen „künftige persistente Volumes automatisch sichern…“, wählen Sie die Backup-Richtlinie aus, die Sie auf neue Volumes anwenden möchten, und klicken Sie auf **Speichern**.




**Ergebnis**

Diese Backup-Richtlinie wird nun auf alle neuen Volumes angewendet, die in diesem Kubernetes Cluster erstellt wurden.

## Anzeigen der Liste der Backups für jedes Volume

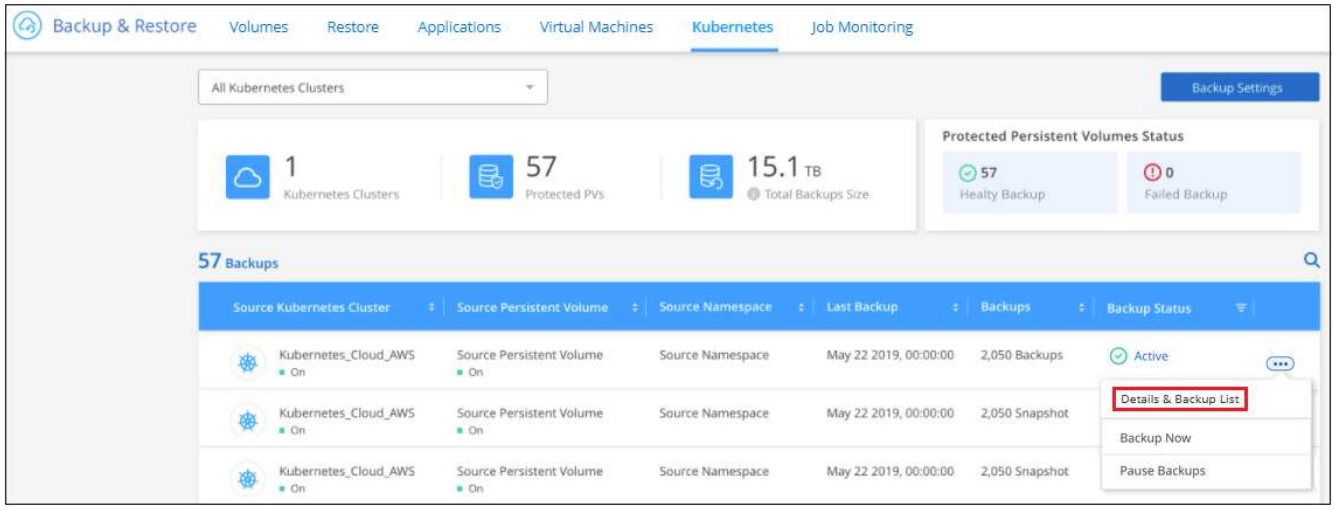
Sie können eine Liste aller Backup-Dateien anzeigen, die für jedes Volume vorhanden sind. Auf dieser Seite werden Details zum Quell-Volume, zum Zielort und zu Backup-Details wie zum Beispiel zum letzten Backup, zur aktuellen Backup-Richtlinie, zur Größe der Sicherungsdatei und mehr angezeigt.

Auf dieser Seite können Sie außerdem die folgenden Aufgaben ausführen:

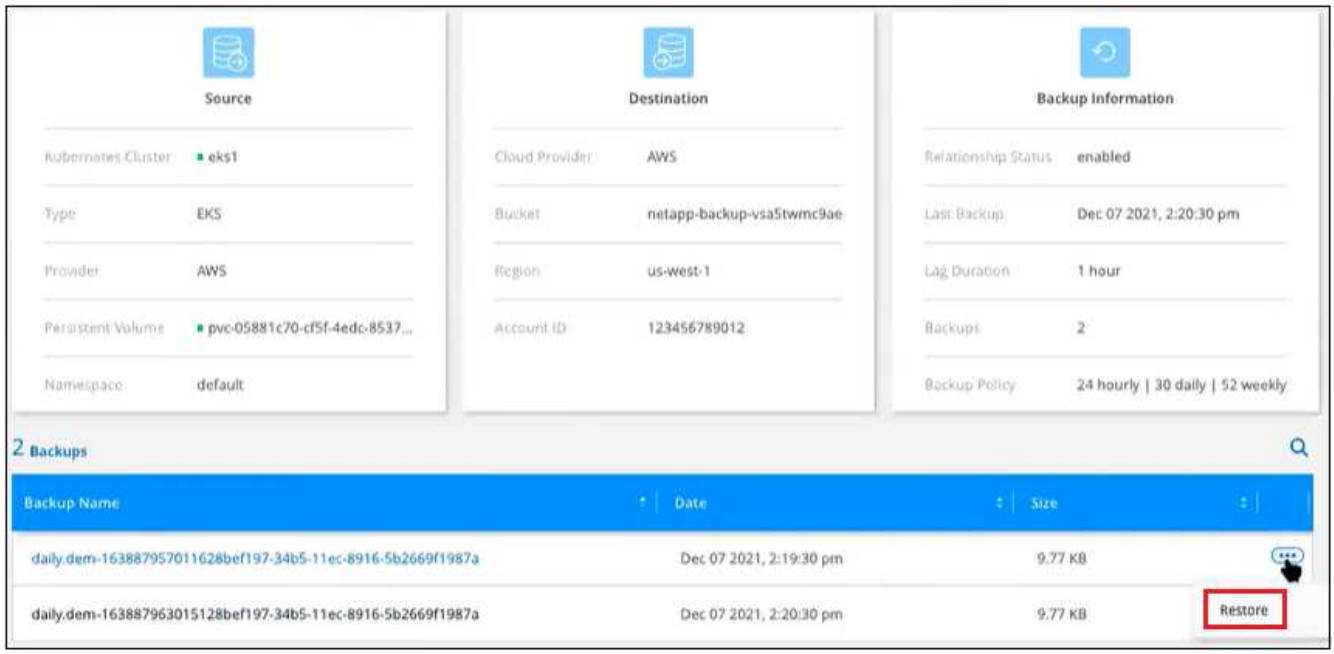
- Löschen Sie alle Sicherungsdateien für das Volume
- Löschen einzelner Backup-Dateien für das Volume
- Backup-Bericht für das Volume herunterladen

**Schritte**

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




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




## Backups werden gelöscht

Cloud Backup ermöglicht die Löschung einer einzelnen Backup-Datei, das Löschen aller Backups für ein Volume oder das Löschen aller Backups aller Volumes in einem Kubernetes Cluster. Sie können alle Backups löschen, wenn Sie die Backups nicht mehr benötigen oder wenn Sie das Quell-Volume gelöscht haben und alle Backups entfernen möchten.

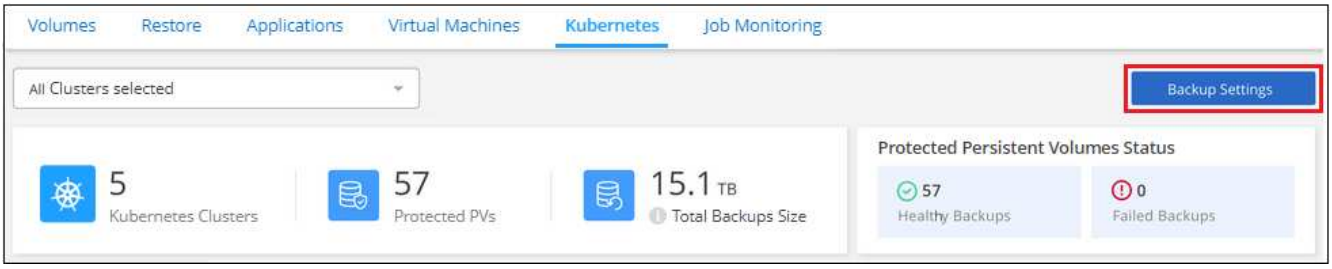
> Wenn Sie planen, eine Arbeitsumgebung oder ein Cluster mit Backups zu löschen, müssen Sie die Backups *löschen, bevor Sie das System löschen. Cloud Backup nicht automatisch löschen Backups, wenn Sie ein System löschen, und es gibt keine aktuelle Unterstützung in der UI, die Backups zu löschen, nachdem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

### Löschen aller Sicherungsdateien für eine Arbeitsumgebung

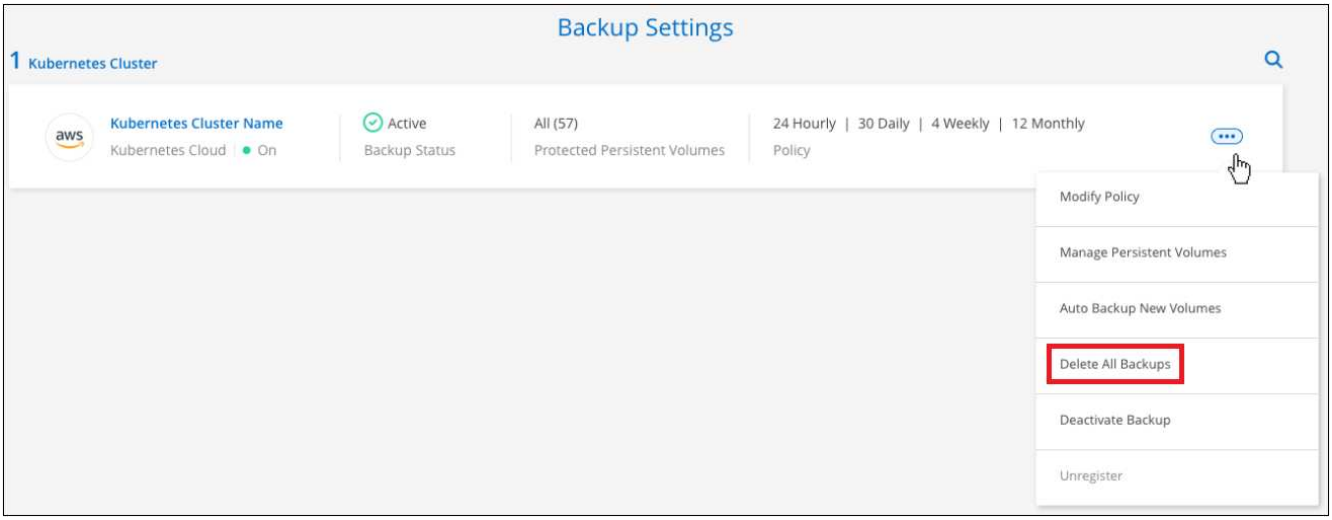
Durch das Löschen aller Backups für eine Arbeitsumgebung werden keine zukünftigen Backups von Volumes in dieser Arbeitsumgebung deaktiviert. Wenn Sie die Erstellung von Backups aller Volumes in einer Arbeitsumgebung beenden möchten, können Sie Backups deaktivieren Wie hier beschrieben.

#### Schritte

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




2. Klicken Sie Auf ••• Für den Kubernetes-Cluster, wo Sie alle Backups löschen und wählen Sie **Alle Backups löschen**.




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

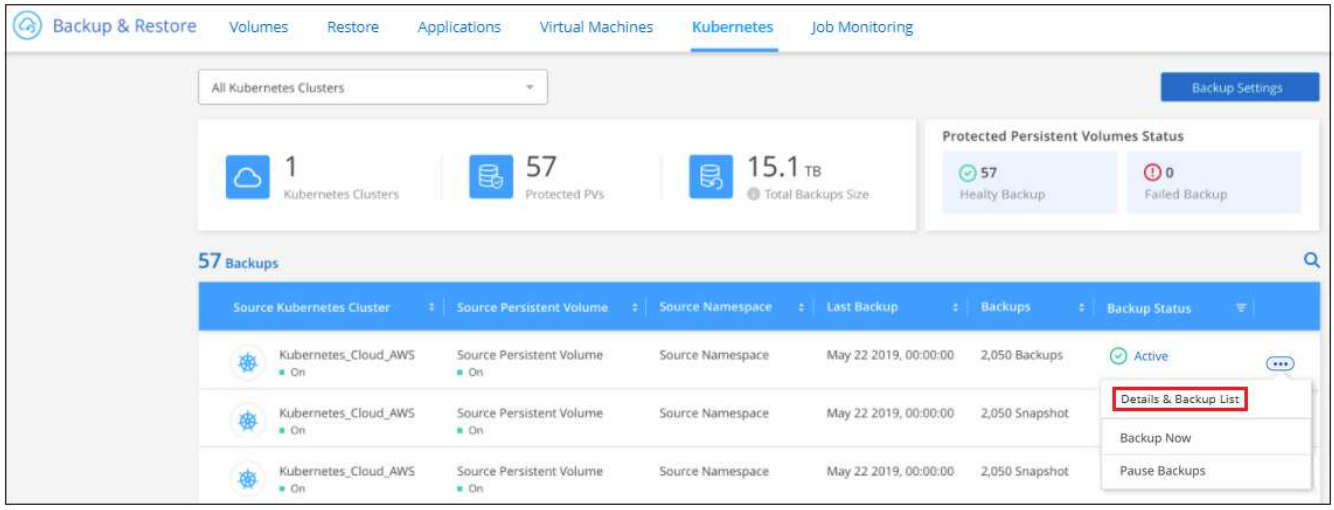
### Löschen aller Sicherungsdateien für ein Volume

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

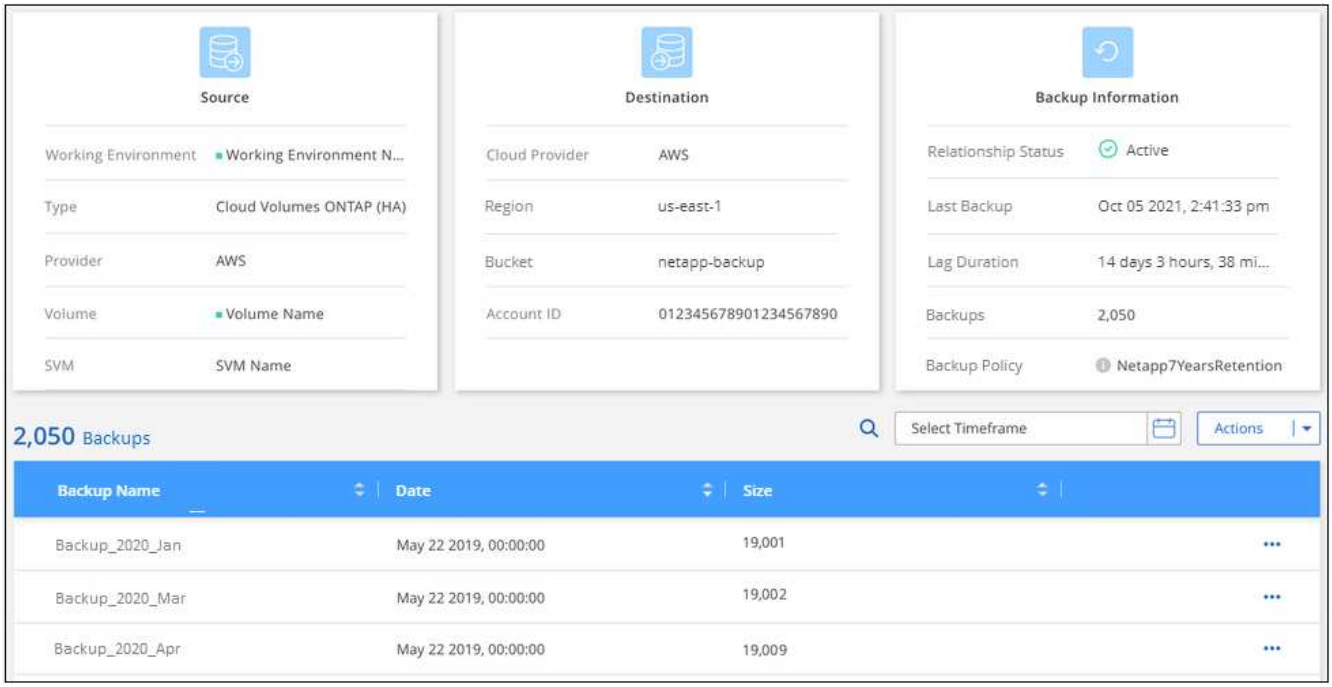
Das können Sie Starten Sie neu, um Backups für das Volume zu erstellen Auf der Seite „Backups verwalten“ können Sie jederzeit Backups managen.

#### Schritte

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




Die Liste aller Sicherungsdateien wird angezeigt.




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

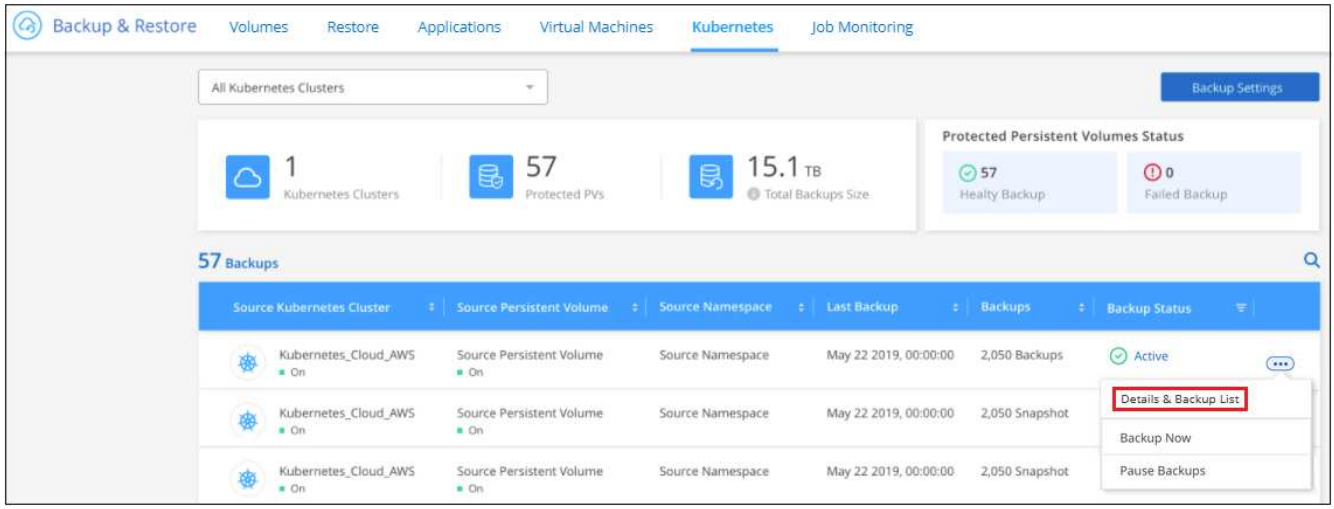
3. Geben Sie im Bestätigungsdialogfeld den Namen des Datenträgers ein und klicken Sie auf **Löschen**.

### Löschen einer einzelnen Backup-Datei für ein Volume

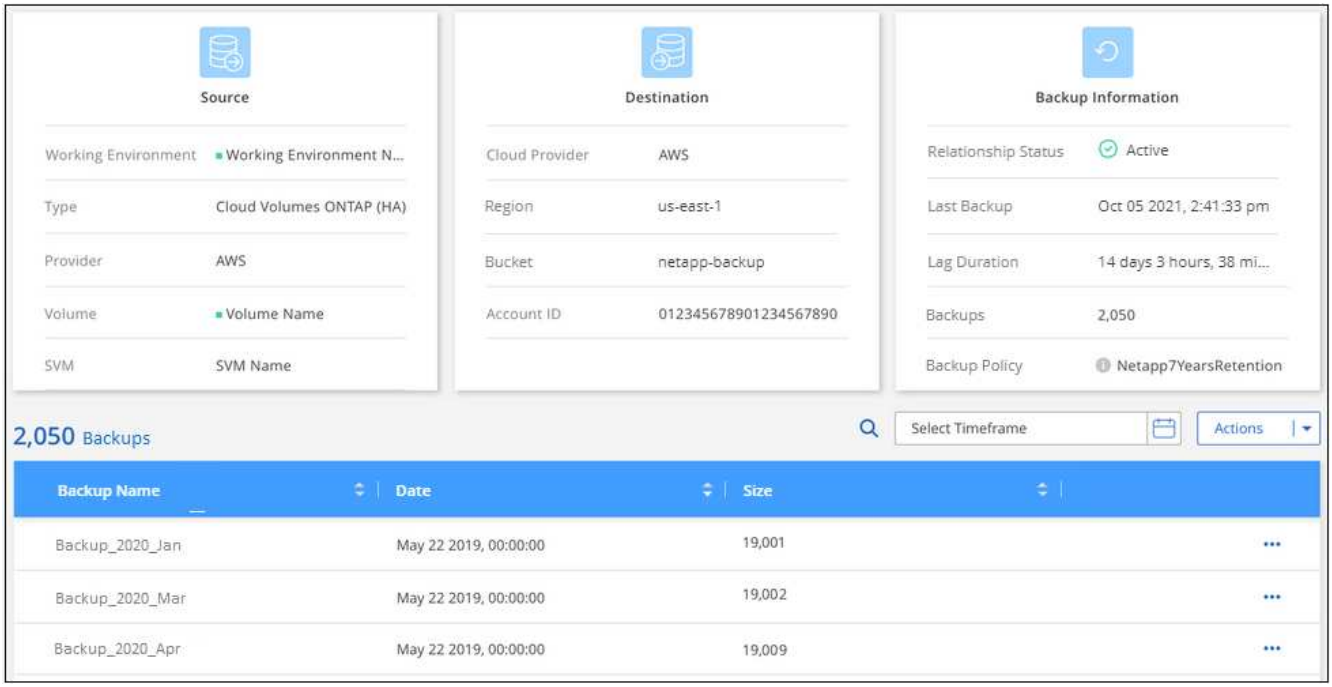
Sie können eine einzelne Sicherungsdatei löschen. Diese Funktion ist nur verfügbar, wenn das Volume Backup aus einem System mit ONTAP 9.8 oder neuer erstellt wurde.

#### Schritte

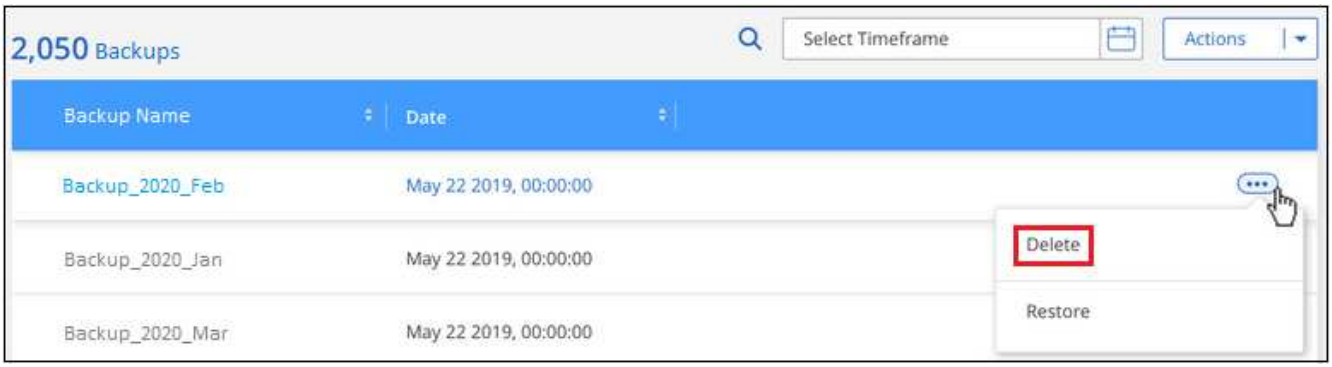
1. Klicken Sie auf der Registerkarte **Kubernetes** auf ••• Wählen Sie für das Quellvolume **Details & Sicherungsliste** aus.




Die Liste aller Sicherungsdateien wird angezeigt.




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




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

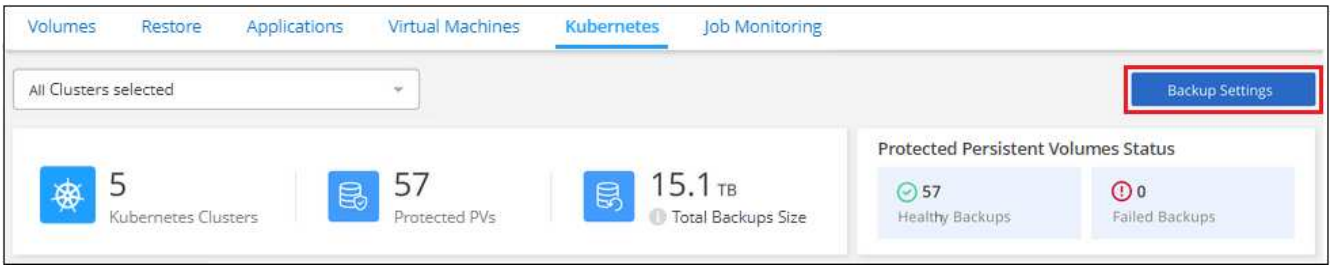
## Deaktivieren von Cloud Backup für eine Arbeitsumgebung

Durch das Deaktivieren von Cloud Backup für eine Arbeitsumgebung werden 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.

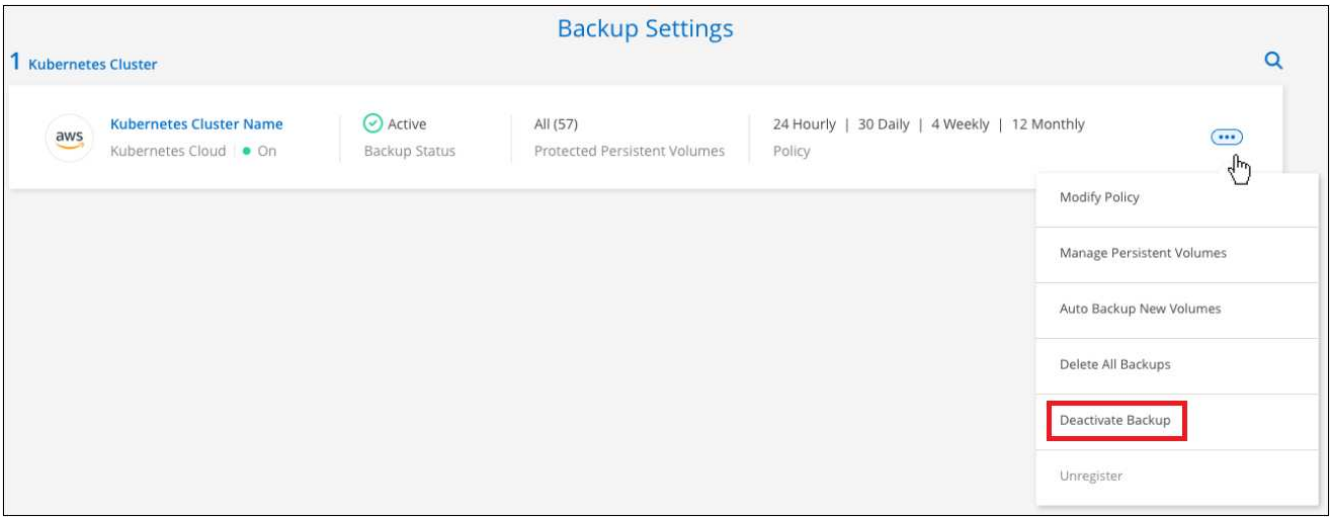
Beachten Sie, dass Cloud-Provider Ihnen weiterhin die Kosten für Objekt-Storage für die Kapazität in Ihrem Backup in Rechnung stellen, es sei denn, Sie sind erforderlich Löschen Sie die Backups.

### Schritte

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




2. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Für die Arbeitsumgebung oder den Kubernetes-Cluster, wo Sie Backups deaktivieren und **deactivate Backup** wählen möchten.



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

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

## Registrieren von Cloud Backup für eine Arbeitsumgebung wird aufgehoben

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

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

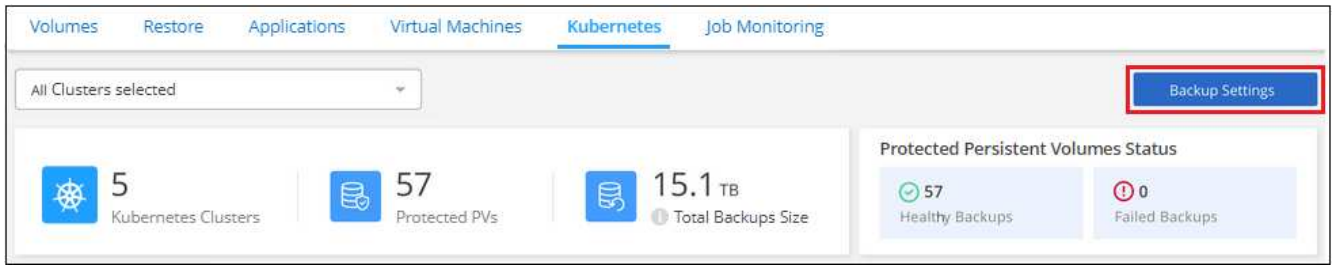
Bevor Sie die Registrierung von Cloud Backup aufheben können, müssen Sie die folgenden Schritte in der folgenden Reihenfolge durchführen:

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

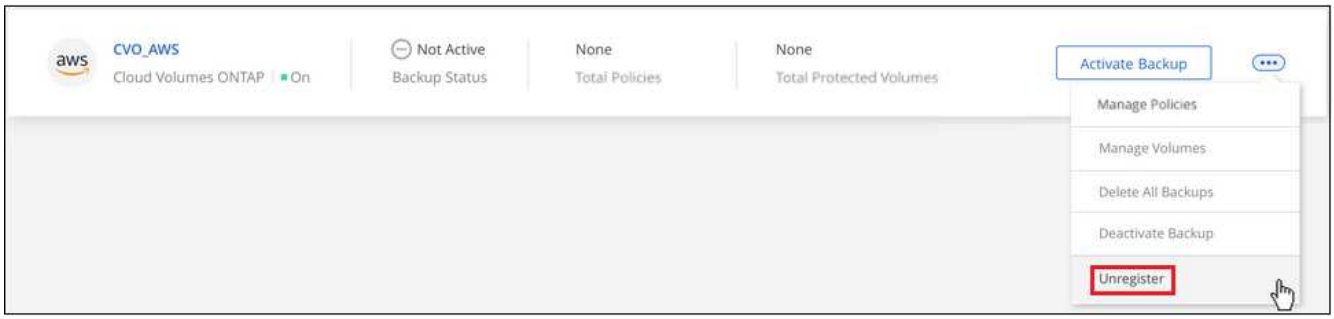
Die Option zum Aufheben der Registrierung ist erst verfügbar, wenn diese beiden Aktionen abgeschlossen sind.

**Schritte**

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




2. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Für den Kubernetes-Cluster, wo Sie den Backup-Service wieder registrieren und wählen Sie **Unregister**.




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

# Wiederherstellung von Kubernetes-Daten aus Backup-Dateien

Backups werden in einem Objektspeicher in Ihrem Cloud-Konto gespeichert, sodass Sie Daten von einem bestimmten Zeitpunkt wiederherstellen können. Sie können ein gesamtes persistentes Kubernetes Volume aus einer gespeicherten Backup-Datei wiederherstellen.

Sie können ein persistentes Volume (als neues Volume) in derselben Arbeitsumgebung oder in einer anderen Arbeitsumgebung wiederherstellen, die dasselbe Cloud-Konto verwendet.

## Unterstützte Arbeitsumgebungen und Objekt-Storage-Anbieter

Sie können ein Volume aus einer Kubernetes-Backup-Datei in den folgenden Arbeitsumgebungen wiederherstellen:

| Speicherort Der Sicherungsdatei | Zielarbeitsumgebung ifdef::aws[] |
|---|---|
| Amazon S3 | Kubernetes Cluster in AWS endif::AWS[] ifdef::Azure[] |
| Azure Blob | Kubernetes Cluster in Azure endif::Azure[] ifdef::gcp[] |
| Google Cloud Storage | Kubernetes Cluster in Google endif::gcp[] |

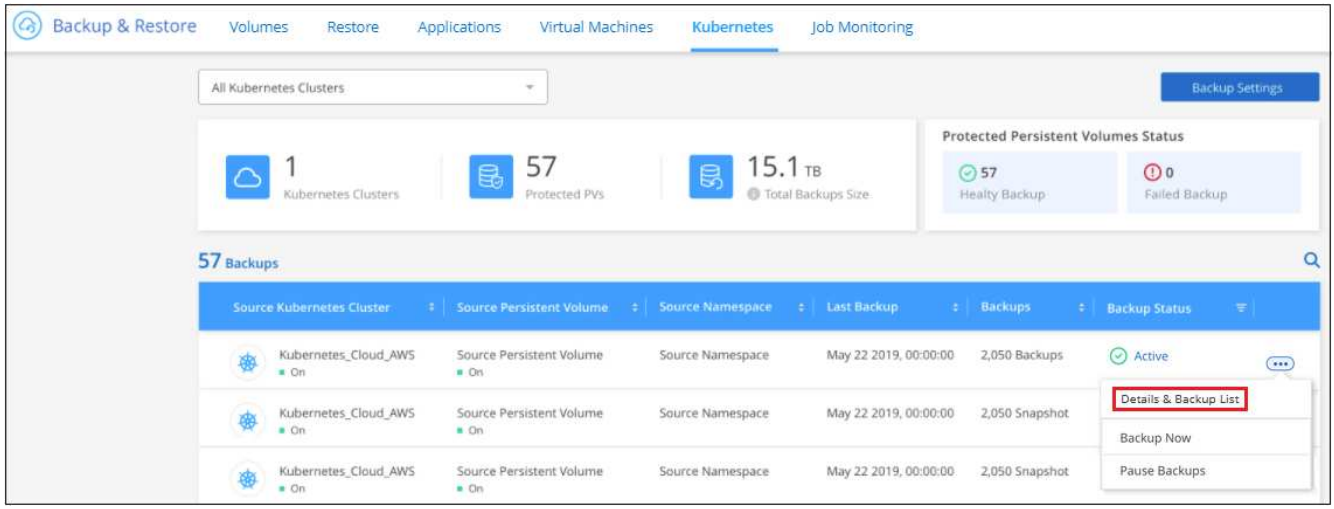
## Wiederherstellung von Volumes aus einer Kubernetes-Backup-Datei

Wenn Sie ein persistentes Volume aus einer Sicherungsdatei wiederherstellen, erstellt BlueXP mithilfe der Daten aus dem Backup ein *neues* Volume. Die Daten können in einem Volume im selben Kubernetes-Cluster oder in einem anderen Kubernetes-Cluster wiederhergestellt werden, der sich im selben Cloud-Konto wie der Kubernetes-Quell-Cluster befindet.

Bevor Sie beginnen, sollten Sie den Namen des wiederherzustellenden Volumes und das Datum der Sicherungsdatei kennen, mit der Sie das neu wiederhergestellte Volume erstellen möchten.

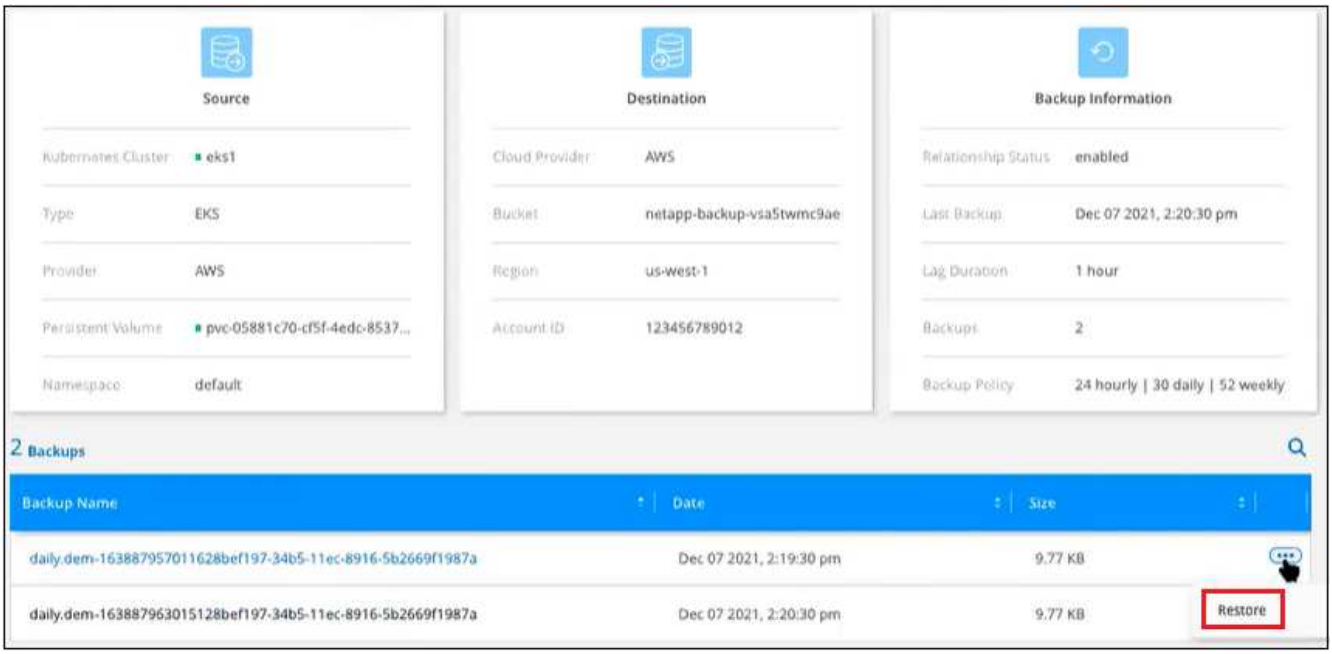
### Schritte

1. Wählen Sie im Menü BlueXP die Option **Schutz > Sicherung und Wiederherstellung**.
2. Klicken Sie auf die Registerkarte **Kubernetes** und das Kubernetes Dashboard wird angezeigt.



3. Suchen Sie das wiederherzustellende Volume, klicken Sie auf •••, Und klicken Sie dann auf **Details & Sicherungsliste**.

   Die Liste aller Backup-Dateien für dieses Volume wird zusammen mit Details zum Quell-Volume, zum Zielspeicherort und Backup-Details angezeigt.




4. Suchen Sie anhand des Datums-/Zeitstempels die Backup-Datei, die Sie wiederherstellen möchten, und klicken Sie auf •••, Und dann **Restore**.
5. Wählen Sie auf der Seite *Select Destination* den *Kubernetes Cluster* aus, wo Sie das Volume, den *Namespace*, die *Storage Class* und den neuen Namen *Persistent Volume* wiederherstellen möchten.

6. Klicken Sie auf **Restore** und Sie werden wieder zum Kubernetes Dashboard, damit Sie den Fortschritt des Wiederherstellungsvorgangs überprüfen können.

**Ergebnis**

BlueXP erstellt im Kubernetes-Cluster ein neues Volume basierend auf dem ausgewählten Backup. Das können Sie "Verwalten Sie die Backup-Einstellungen für dieses neue Volume" Nach Bedarf.

# Backup und Restore von Applikationsdaten

## Backup und Restore von On-Premises-Applikationsdaten

### Sichern Sie Ihre lokalen Applikationsdaten

Sie können Cloud Backup für Applikationen in BlueXP (früher Cloud Manager) und On-Premises-SnapCenter integrieren und so die applikationskonsistenten Snapshots aus lokalen ONTAP in die Cloud sichern. Bei Bedarf können Sie die Daten aus der Cloud auf lokalen SnapCenter Server wiederherstellen.

Sie können Backups von Oracle, Microsoft SQL und SAP HANA Applikationsdaten von lokalen ONTAP Systemen auf Amazon Web Services, Microsoft Azure, Google Cloud Platform und StorageGRID erstellen.

> Sie sollten die SnapCenter-Software 4.6 oder höher verwenden.

Weitere Informationen zu Cloud-Backup für Applikationen finden Sie unter:

- "Applikationsorientiertes Backup mit Cloud Backup und SnapCenter"
- "Podcast zum Thema Cloud Backup für Applikationen"

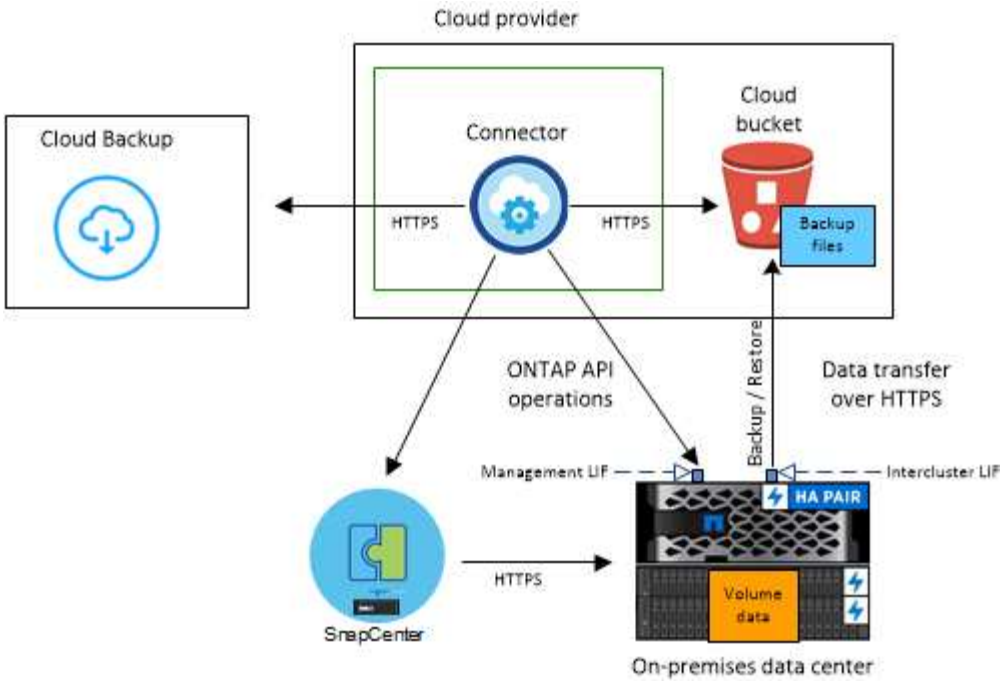
#### Anforderungen

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie mit dem Backup von Applikationsdaten in Cloud-Services beginnen.

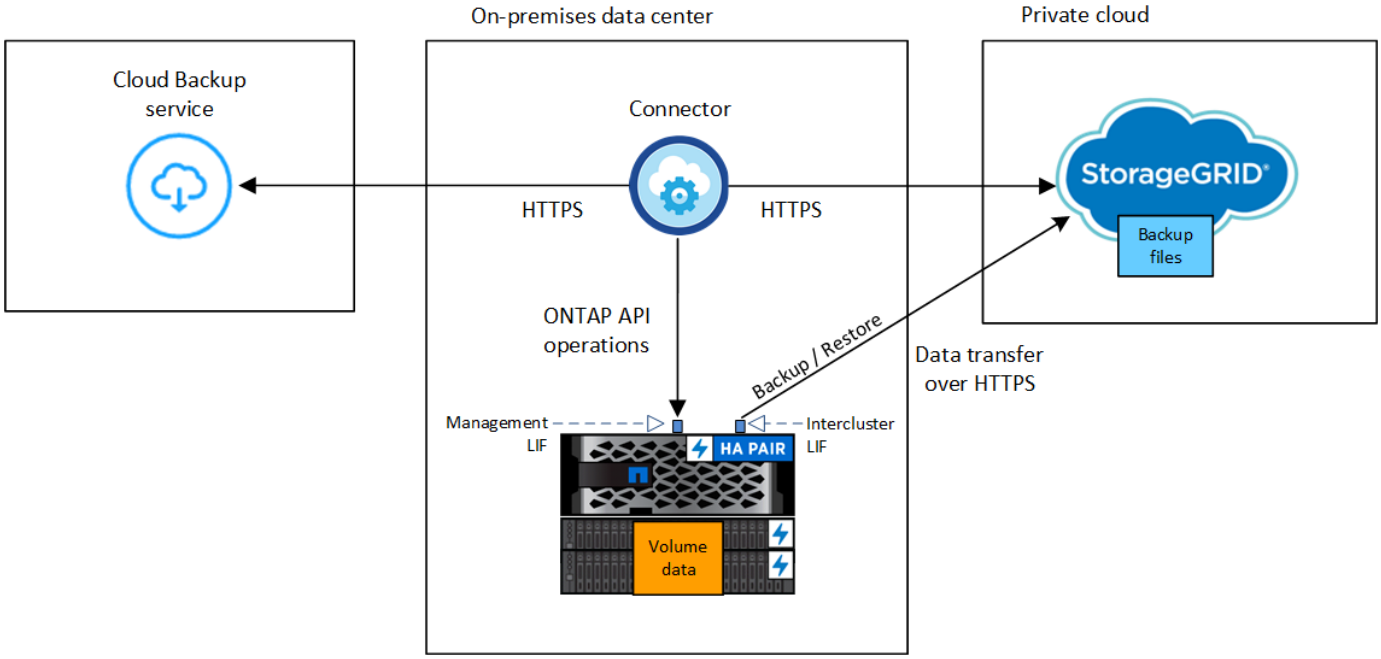
- ONTAP 9.8 oder höher
- BlueXP 3.9
- SnapCenter Server 4.6 oder höher Sie sollten SnapCenter Server 4.7 verwenden, wenn Sie die folgenden Funktionen nutzen möchten:
  - Sichern von Backups vor Ort aus sekundärem Storage
  - Schutz von SAP HANA Applikationen
  - Sichern Sie Oracle und SQL Applikationen auf VMware Umgebung
  - Mount-Backups
  - Backups deaktivieren
  - SnapCenter-Server nicht registrieren
- Mindestens ein Backup pro Applikation sollte auf dem SnapCenter-Server verfügbar sein
- Mindestens eine Tages-, Wochen- oder Monatsrichtlinie in SnapCenter ohne Etikett oder dieselbe Bezeichnung wie die der Cloud Backup for Applications-Richtlinie in BlueXP.

> Cloud Backup für Applikationen unterstützt keinen Schutz von Applikationen, die sich auf SVMs befinden, die mit FQDN oder IP-Adresse hinzugefügt wurden.

Die folgende Abbildung zeigt die einzelnen Komponenten beim Backup in der Cloud und die Verbindungen, die zwischen ihnen vorbereitet werden müssen:




Die folgende Abbildung zeigt jede Komponente beim Backup in StorageGRID und die Verbindungen, die zwischen ihnen vorbereitet werden müssen:




## Registrieren Sie den SnapCenter-Server

Nur ein Benutzer mit SnapCenterAdmin-Rolle kann den Host registrieren, auf dem SnapCenter Server 4.6 oder höher ausgeführt wird. Sie können mehrere SnapCenter-Server-Hosts registrieren.

### Schritte

1. Klicken Sie in BlueXP UI auf **Schutz** > **Sicherung und Wiederherstellung** > **Anwendungen**.

2. Klicken Sie im Dropdown-Menü **Einstellungen** auf **SnapCenter Server**.
3. Klicken Sie auf **SnapCenter-Server registrieren**.
4. Geben Sie folgende Details an:
   a. Geben Sie im Feld SnapCenter-Server den FQDN oder die IP-Adresse des SnapCenter-Serverhosts an.
   b. Geben Sie im Feld Port die Portnummer an, auf der der SnapCenter-Server ausgeführt wird.

      Sie sollten sicherstellen, dass der Port offen ist, damit die Kommunikation zwischen SnapCenter Server und Cloud Backup for Applications erfolgen kann.

   c. Geben Sie im Feld Tags einen Standortnamen, einen Städtenamen oder einen benutzerdefinierten Namen an, mit dem der SnapCenter-Server markiert werden soll.

      Die Tags sind durch Komma getrennt.

   d. Geben Sie im Feld Benutzername und Kennwort die Anmeldeinformationen des Benutzers mit der Rolle SnapCenterAdmin an.
5. Klicken Sie Auf **Registrieren**.

**Nach Ihrer Beendigung**

Klicken Sie auf **Backup & Restore** > **Anwendungen**, um alle Anwendungen anzuzeigen, die mit dem registrierten SnapCenter Server-Host geschützt sind.

Standardmäßig werden die Anwendungen automatisch jeden Tag um Mitternacht erkannt. Sie können den Zeitplan so konfigurieren, dass die Anwendungen ermittelt werden.

> Bei SQL Server-Datenbanken zeigt die Spalte Anwendungsname den Namen im Format *Application_Name (Instanzname)* an.

Folgende Applikationen und ihre Konfigurationen werden unterstützt:

- Oracle Datenbank:
  - Vollständige Backups (Daten + Protokoll) werden mit mindestens einem täglichen, wöchentlichen oder monatlichen Zeitplan erstellt
  - SAN, NFS, VMDK-SAN, VMDK-NFS UND RDM
- Microsoft SQL Server Datenbank:
  - Standalone, Failover-Cluster-Instanzen und Verfügbarkeitsgruppen
  - Vollständige Backups, die mit mindestens einem täglichen, wöchentlichen oder monatlichen Zeitplan erstellt wurden
  - SAN, VMDK-SAN, VMDK-NFS UND RDM
- SAP HANA Datenbank:
  - Einzelner Container 1.x
  - Mehrere Datenbank-Container 2.x
  - HANA System Replication (HSR)

    Sie sollten mindestens ein Backup am primären und sekundären Standort haben. Sie können entscheiden, einen pro-aktiven Ausfall oder einen verzögerten Failover auf das sekundäre zu tun.

- Nicht-Daten-Volumes (NDV) Ressourcen wie HANA-Binärdateien, HANA Archiv-Log-Volume, HANA Shared Volume usw.

Die folgenden Datenbanken werden nicht angezeigt:

- Datenbanken ohne Backups
- Datenbanken mit nur bedarfsgerechter oder stündlicher Richtlinie
- Oracle-Datenbanken auf NVMe

## Erstellen einer Richtlinie für das Backup von Applikationen

Sie können entweder eine der vordefinierten Richtlinien verwenden oder eine individuelle Richtlinie für das Backup der Applikationsdaten in der Cloud erstellen. Sie können Richtlinien erstellen, wenn Sie die vordefinierten Richtlinien nicht bearbeiten möchten.

Die vordefinierten Richtlinien sind:

| Name Der Richtlinie | Etikett | Aufbewahrungswert |
|---|---|---|
| 1 Jahr tägliche LTR | Täglich | 366 |
| 5 Jahre tägliche LTR | Täglich | 1830 |
| 7 Jahre wöchentlicher LTR | Wöchentlich | 370 |
| 10 Jahre Monatliche LTR | Monatlich | 120 |

**Schritte**

1. Klicken Sie in BlueXP UI auf **Schutz** > **Sicherung und Wiederherstellung** > **Anwendungen**.
2. Klicken Sie im Dropdown-Menü Einstellungen auf **Richtlinien** > **Richtlinien erstellen**.
3. Geben Sie im Abschnitt Richtliniendetails den Richtliniennamen an.
4. Wählen Sie im Abschnitt Aufbewahrung einen Aufbewahrungstyp aus und geben Sie die Anzahl der zu behaltenden Backups an.
5. Wählen Sie Primary oder Secondary als Backup-Speicherquelle aus.
6. (Optional) Wenn Sie Backups nach einer bestimmten Anzahl von Tagen zur Kostenoptimierung vom Objektspeicher in den Archivspeicher verschieben möchten, aktivieren Sie das Kontrollkästchen **Tiering Backups in Archive**.

   Sie können Backups nur dann von einem Objektspeicher in einen Archiv-Storage verschieben, wenn Sie ONTAP 9.10.1 oder höher und Amazon Web Services oder Azure als Cloud-Provider verwenden. Sie sollten die Zugriffsebene für den Archiv für jeden Cloud-Provider konfigurieren.

7. Klicken Sie Auf **Erstellen**.

   Sie können die angepassten Richtlinien bearbeiten, kopieren und löschen.

> Eine Richtlinie, die einer Anwendung zugeordnet ist, kann nicht bearbeitet oder gelöscht werden.

## Sichern Sie On-Premises-Applikationsdaten auf der Google Cloud Platform

Durch die Integration von Cloud Backup für Anwendungen in BlueXP und On-Premises-SnapCenter können Sie Backups der Applikationsdaten von ONTAP auf der Google Cloud-Plattform erstellen.

Sie können eine oder mehrere Applikationen gleichzeitig mit einer einzigen Richtlinie in der Cloud sichern.

> Sie können nur eine Anwendung gleichzeitig schützen, wenn Sie die BlueXP-GUI verwenden. Wenn SIE JEDOCH REST-APIs verwenden, können Sie mehrere Applikationen gleichzeitig sichern.

**Schritte**

1. Klicken Sie in BlueXP UI auf **Schutz** > **Sicherung und Wiederherstellung** > **Anwendungen**.
2. Klicken Sie Auf ••• Entsprechend der Anwendung und klicken Sie auf **Backup aktivieren**.
3. Wählen Sie auf der Seite Richtlinie zuweisen die Richtlinie aus und klicken Sie auf **Weiter**.
4. Fügen Sie die Arbeitsumgebung hinzu.

   Konfigurieren Sie den ONTAP-Cluster, der die SVM hostet, auf dem die Applikation ausgeführt wird. Nach dem Hinzufügen der Arbeitsumgebung für eine der Applikationen kann sie für alle anderen Applikationen in demselben ONTAP Cluster wiederverwendet werden.

   a. Wählen Sie die SVM aus und klicken Sie auf **Arbeitsumgebung hinzufügen**.
   b. Im Assistenten „Arbeitsumgebung hinzufügen“:
      i. Geben Sie die IP-Adresse des ONTAP-Clusters an.
      ii. Geben Sie die Admin-Anmeldedaten an.

      Cloud Backup für Applikationen unterstützt nur Cluster-Administratoren.

   c. Klicken Sie Auf **Arbeitsumgebung Hinzufügen**.
5. Wählen Sie **Google Cloud Platform** als Cloud-Provider aus.
   a. Wählen Sie das Google Cloud Projekt aus, in dem der Google Cloud Storage-Bucket für Backups erstellt werden soll.
   b. Geben Sie im Feld Google Cloud Access Key den Schlüssel an.
   c. Geben Sie im Feld Google Cloud Secret Key das Passwort an.
   d. Wählen Sie den Bereich aus, in dem Sie die Backups erstellen möchten.
   e. Geben Sie den IP-Speicherplatz an.
6. Überprüfen Sie die Details und klicken Sie auf **Backup aktivieren**.

## Sichern Sie On-Premises-Applikationsdaten in StorageGRID

Durch die Integration von Cloud Backup für Applikationen in BlueXP und On-Premises-

## SnapCenter können Sie ein Backup der Applikationsdaten von ONTAP in StorageGRID erstellen.

Sie können eine oder mehrere Applikationen gleichzeitig mit einer einzigen Richtlinie in StorageGRID sichern.

> Sie können nur eine Anwendung gleichzeitig schützen, wenn Sie die BlueXP-GUI verwenden. Wenn SIE JEDOCH REST-APIs verwenden, können Sie mehrere Applikationen gleichzeitig sichern.

**Was Sie brauchen**

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

Weitere Informationen finden Sie unter "Anschlüsse für StorageGRID erstellen".

**Schritte**

1. Klicken Sie in BlueXP UI auf **Schutz** > **Sicherung und Wiederherstellung** > **Anwendungen**.
2. Klicken Sie Auf ••• Entsprechend der Anwendung und klicken Sie auf **Backup aktivieren**.
3. Wählen Sie auf der Seite Richtlinie zuweisen die Richtlinie aus und klicken Sie auf **Weiter**.
4. Fügen Sie die Arbeitsumgebung hinzu.

   Konfigurieren Sie den ONTAP-Cluster, der die SVM hostet, auf dem die Applikation ausgeführt wird. Nach dem Hinzufügen der Arbeitsumgebung für eine der Applikationen kann sie für alle anderen Applikationen in demselben ONTAP Cluster wiederverwendet werden.

   a. Wählen Sie die SVM aus und klicken Sie auf **Arbeitsumgebung hinzufügen**.
   b. Im Assistenten „Arbeitsumgebung hinzufügen“:
      i. Geben Sie die IP-Adresse des ONTAP-Clusters an.
      ii. Geben Sie die Admin-Anmeldedaten an.

      Cloud Backup für Applikationen unterstützt nur Cluster-Administratoren.

   c. Klicken Sie Auf **Arbeitsumgebung Hinzufügen**.
5. Wählen Sie **StorageGRID**.
   a. Geben Sie den FQDN des StorageGRID-Servers und den Port an, auf dem der StorageGRID-Server ausgeführt wird.

      Geben Sie die Details im Format FQDN:PORT ein.

   b. Geben Sie im Feld Zugriffsschlüssel den Schlüssel an.
   c. Geben Sie im Feld Geheimer Schlüssel das Passwort an.
   d. Geben Sie den IP-Speicherplatz an.
6. Überprüfen Sie die Details und klicken Sie auf **Backup aktivieren**.

## Management der Sicherung von Applikationen

Sie können den Schutz von Anwendungen verwalten, indem Sie verschiedene Vorgänge über die Benutzeroberfläche von BlueXP ausführen.

### Anzeigen von Richtlinien

Sie können alle Richtlinien anzeigen. Wenn Sie die Details anzeigen, werden für jede dieser Richtlinien alle zugehörigen Anwendungen aufgelistet.

1. Klicken Sie auf **Backup und Recovery** > **Anwendungen**.
2. Klicken Sie im Dropdown-Menü **Einstellungen** auf **Richtlinien**.
3. Klicken Sie auf **Details anzeigen** entsprechend der Richtlinie, deren Details Sie anzeigen möchten.

   Die zugehörigen Anwendungen werden aufgelistet.

> Eine Richtlinie, die einer Anwendung zugeordnet ist, kann nicht bearbeitet oder gelöscht werden.

Sie können sich auch SnapCenter-Richtlinien für die Cloud anzeigen lassen, indem Sie auf ausführen `Get-SmResources` SnapCenter Cmdlet: Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von Get-Help Command_Name abgerufen werden. Alternativ können Sie auch die verweisen "SnapCenter Software Cmdlet Referenzhandbuch".

### Anzeigen von Backups in der Cloud

Sie können die Backups in der Cloud in der BlueXP UI anzeigen.

1. Klicken Sie auf **Backup und Recovery** > **Anwendungen**.
2. Klicken Sie Auf ••• Entsprechend der Anwendung und klicken Sie auf **Details anzeigen**.

> Die für die Auflistung der Backups benötigte Zeit hängt von dem standardmäßigen Replizierungsplan von ONTAP (maximal 1 Stunde) und BlueXP (maximal 6 Stunden) ab.

- Bei Oracle Datenbanken werden sowohl Daten- als auch Log-Backups, SCN-Nummer für jedes Backup, Enddatum für jedes Backup aufgeführt. Sie können nur das Daten-Backup auswählen und die Datenbank auf dem lokalen SnapCenter Server wiederherstellen.
- Bei Microsoft SQL Server-Datenbanken werden nur die vollständigen Backups und das Enddatum für jedes Backup aufgeführt. Sie können das Backup auswählen und die Datenbank auf dem lokalen SnapCenter Server wiederherstellen.
- Bei Microsoft SQL Server werden Backups nicht nur in den Datenbanken aufgeführt, unter denen diese Instanz steht.
- Bei SAP HANA Datenbanken werden nur die Daten-Backups und das Enddatum für jedes Backup aufgeführt. Sie können das Backup auswählen und Mount-Vorgang durchführen.

> Die vor Aktivierung der Cloud-Sicherung erstellten Backups werden nicht zur Wiederherstellung aufgeführt.

Sie können diese Backups auch anzeigen, indem Sie die ausführen `Get-SmBackup` SnapCenter Cmdlet: Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von Get-Help Command_Name abgerufen werden. Alternativ können Sie auch die verweisen "SnapCenter Software Cmdlet Referenzhandbuch".

### Datenbanklayout ändern

Wenn Volumes zur Datenbank hinzugefügt werden, kennzeichnet SnapCenter Server die Snapshots auf den neuen Volumes automatisch gemäß Richtlinie und Zeitplan. Diese neuen Volumes verfügen nicht über den Endpunkt des Objektspeichers, und Sie sollten die Aktualisierung durch die folgenden Schritte durchführen:

1. Klicken Sie auf **Backup und Recovery** > **Anwendungen**.
2. Klicken Sie im Dropdown-Menü **Einstellungen** auf **SnapCenter Server**.
3. Klicken Sie Auf ••• Entsprechend dem SnapCenter-Server, der die Anwendung hostet, und klicken Sie auf **Aktualisieren**.

   Die neuen Volumes werden ermittelt.

4. Klicken Sie Auf ••• Entsprechend der Anwendung und klicken Sie auf **Refresh Protection**, um den Cloud-Schutz für das neue Volume zu aktivieren.

Wenn ein Storage-Volume nach der Konfiguration des Cloud-Service aus der Applikation entfernt wird, kennzeichnet SnapCenter Server für neue Backups nur die Snapshots, auf denen sich die Anwendung befindet. Wenn das entfernte Volume von anderen Anwendungen nicht verwendet wird, sollten Sie die Objektspeicherbeziehung manuell löschen. Wenn Sie den Anwendungsbestand aktualisieren, enthält dieser das aktuelle Speicherlayout der Anwendung.

### Änderung der Richtlinie oder Ressourcengruppe

Wenn die SnapCenter-Richtlinie oder Ressourcengruppe geändert wird, müssen Sie den Schutz aktualisieren.

1. Klicken Sie auf **Backup und Recovery** > **Anwendungen**.
2. Klicken Sie Auf ••• Entsprechend der Anwendung und klicken Sie auf **Aktualisierungsschutz**.

### SnapCenter-Server nicht registrieren

1. Klicken Sie auf **Backup und Recovery** > **Anwendungen**.
2. Klicken Sie im Dropdown-Menü **Einstellungen** auf **SnapCenter Server**.
3. Klicken Sie Auf ••• Entsprechend dem SnapCenter-Server und klicken Sie auf **Registrierung aufheben**.

### Überwachen Von Jobs

Für alle Cloud-Backup-Vorgänge werden Jobs erstellt. Sie können alle Jobs und alle Unteraufgaben, die als Teil jeder Aufgabe ausgeführt werden, überwachen.

1. Klicken Sie auf **Sicherung und Wiederherstellung** > **Jobüberwachung**.

   Wenn Sie einen Vorgang starten, wird ein Fenster angezeigt, in dem Sie angeben, dass der Job gestartet wird. Sie können auf den Link klicken, um den Job zu überwachen.

2. Klicken Sie auf die primäre Aufgabe, um die Unteraufgaben und den Status der einzelnen Unteraufgaben anzuzeigen.

### Legen Sie IP-Speicherplatz für die primäre Arbeitsumgebung fest

Wenn Sie ein Backup wiederherstellen oder mounten möchten, das vom sekundären Storage in einen Objektspeicher verschoben wurde, sollten Sie die Details zur primären Arbeitsumgebung hinzufügen und den IP-Speicherplatz festlegen.

#### Schritte

1. Klicken Sie in BlueXP UI auf **Storage** > **Leinwand** > **Meine Arbeitsumgebung** > **Arbeitsumgebung hinzufügen**.
2. Geben Sie die Details der primären Arbeitsumgebung an und klicken Sie auf **Hinzufügen**.
3. Klicken Sie auf **Backup und Recovery** > **Volumes**.
4. Klicken Sie Auf ••• Entsprechend einem der Volumen und klicken Sie auf **Details**.
5. Klicken Sie Auf ••• Entsprechend der Sicherung und klicken Sie auf **Wiederherstellen**.
6. Wählen Sie im Assistenten die neu hinzugefügte primäre Arbeitsumgebung als Ziel aus.
7. Geben Sie den IP-Speicherplatz an.

### Konfigurieren Sie CA-Zertifikate

Wenn Sie CA-Zertifikate haben, sollten Sie die Stammzertifizierungszertifikate manuell auf den Verbindungscomputer kopieren.

Wenn Sie jedoch keine CA-Zertifikate besitzen, können Sie ohne die Konfiguration von CA-Zertifikaten fortfahren.

#### Schritte

1. Kopieren Sie das Zertifikat in das Volume, auf das über den Docker-Agent zugegriffen werden kann.
   - `cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir sc_certs`
   - `chmod 777 sc_certs`
2. Kopieren Sie die RootCA-Zertifikatdateien in den obigen Ordner auf dem Verbindungscomputer.

   ```
   cp <path on connector>/<filename>
   /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/sc_certs
   ```

3. Kopieren Sie die CRL-Datei in das Volume, auf das über den Docker-Agent zugegriffen werden kann.
   - `cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir sc_crl`
   - `chmod 777 sc_crl`
4. Kopieren Sie die CRL-Dateien in den obigen Ordner auf dem Verbindungscomputer.

   ```
   cp <path on connector>/<filename>
   /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/sc_crl
   ```

5. Nachdem Sie die Zertifikate und CRL-Dateien kopiert haben, starten Sie den Service Cloud Backup for Apps neu.
   - `sudo docker exec cloudmanager_snapcenter sed -i 's/skipSCCertValidation: true/skipSCCertValidation: false/g' /opt/netapp/cloudmanager-snapcenter-`

```
agent/config/config.yml
```

- `sudo docker restart cloudmanager_snapcenter`

## Wiederherstellung von Applikationsdaten

### Oracle Datenbank wiederherstellen

Die Oracle-Datenbank kann nur auf demselben SnapCenter-Serverhost, derselben SVM oder demselben Datenbank-Host wiederhergestellt werden. Bei einer RAC-Datenbank werden die Daten auf dem On-Premises-Node, an dem das Backup erstellt wurde, wiederhergestellt.

> Die Wiederherstellung von sekundären Backups über primären Server wird unterstützt.

Es wird nur eine vollständige Datenbank mit Wiederherstellung der Kontrolldatei unterstützt. Wenn die Archivprotokolle nicht im AFS vorhanden sind, müssen Sie den Speicherort angeben, der die für die Wiederherstellung erforderlichen Archivprotokolle enthält.

> Single File Restore (SFR) wird nicht unterstützt.

#### Was Sie brauchen

Wenn Sie ein Backup wiederherstellen möchten, das vom sekundären Storage in einen Objektspeicher verschoben wurde, sollten Sie die Details zur primären Arbeitsumgebung hinzufügen und den IP-Speicherplatz festlegen. Weitere Informationen finden Sie unter "Legen Sie IP-Speicherplatz für die primäre Arbeitsumgebung fest".

#### Schritte

1. Klicken Sie in BlueXP UI auf **Schutz** > **Sicherung und Wiederherstellung** > **Anwendungen**.
2. Wählen Sie im Feld **Filtern nach** den Filter **Typ** aus und wählen Sie aus der Dropdown-Liste **Oracle** aus.
3. Klicken Sie auf **Details anzeigen**, die der Datenbank entsprechen, die Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellen**.
4. Führen Sie auf der Seite Wiederherstellungstyp die folgenden Aktionen durch:

   a. Wählen Sie **Datenbankstatus** aus, wenn Sie den Status der Datenbank in den Zustand ändern möchten, der für die Wiederherstellung und Wiederherstellung erforderlich ist.

      Die verschiedenen Status einer Datenbank von höher bis niedriger sind offen, montiert, gestartet und heruntergefahren. Sie müssen dieses Kontrollkästchen aktivieren, wenn sich die Datenbank in einem höheren Zustand befindet, der Status jedoch in einen niedrigeren Zustand geändert werden muss, um einen Wiederherstellungsvorgang durchzuführen. Wenn sich die Datenbank in einem niedrigeren Zustand befindet, aber der Status in einen höheren Zustand geändert werden muss, um den Wiederherstellungsvorgang auszuführen, wird der Datenbankstatus automatisch geändert, auch wenn Sie das Kontrollkästchen nicht aktivieren.

   Wenn sich eine Datenbank im Status „offen“ befindet und die Datenbank für die Wiederherstellung im Status „angehängt“ befinden muss, wird der Datenbankzustand nur geändert, wenn Sie dieses Kontrollkästchen aktivieren.

a. Wählen Sie **Kontrolldateien** aus, wenn Sie Steuerdatei zusammen mit der vollständigen Datenbank wiederherstellen möchten.

b. Wenn sich der Snapshot im Archiv-Speicher befindet, geben Sie die Priorität an, um Ihre Daten aus dem Archiv-Speicher wiederherzustellen.

5. Führen Sie auf der Seite „Recovery Scope“ die folgenden Schritte aus:

a. Geben Sie den Recovery-Umfang an.

| Sie suchen… | Tun Sie das… |
|---|---|
| Möchten Sie die letzte Transaktion wiederherstellen | Wählen Sie **Alle Protokolle**. |
| Wiederherstellen einer bestimmten Systemänderungsnummer (SCN) | Wählen Sie **bis SCN (Systemänderungsnummer)**. |
| Möchten Sie Daten zu einer bestimmten Zeit wiederherstellen | Wählen Sie **Datum und Uhrzeit**.<br><br>Sie müssen Datum und Uhrzeit der Zeitzone des Datenbank-Hosts angeben. |
| Möchten Sie nicht wiederherstellen | Wählen Sie **Keine Wiederherstellung**. |
| Soll beliebige externe Archiv-Log-Speicherorte angeben | Wenn die Archivprotokolle nicht im AFS vorhanden sind, müssen Sie den Speicherort angeben, der die für die Wiederherstellung erforderlichen Archivprotokolle enthält. |

b. Aktivieren Sie das Kontrollkästchen, wenn Sie die Datenbank nach der Wiederherstellung öffnen möchten.

In einem RAC-Setup wird nach der Wiederherstellung nur die RAC-Instanz geöffnet, die für die Wiederherstellung verwendet wird.

6. Überprüfen Sie die Details und klicken Sie auf **Wiederherstellen**.

#### SQL Server Datenbank wiederherstellen

Sie können eine SQL Server-Datenbank auf demselben Host oder auf dem alternativen Host wiederherstellen. Das Recovery von Protokoll-Backups und das erneute Seeding von Verfügbarkeitsgruppen wird nicht unterstützt.

WICHTIG: Die Wiederherstellung von sekundären Backups über Primärsystem wird unterstützt.

Single File Restore (SFR) wird nicht unterstützt.

#### Was Sie brauchen

Wenn Sie ein Backup wiederherstellen möchten, das vom sekundären Storage in einen Objektspeicher verschoben wurde, sollten Sie die Details zur primären Arbeitsumgebung hinzufügen und den IP-Speicherplatz

festlegen. Weitere Informationen finden Sie unter "Legen Sie IP-Speicherplatz für die primäre Arbeitsumgebung fest".

**Schritte**

1. Klicken Sie in BlueXP UI auf **Schutz** > **Sicherung und Wiederherstellung** > **Anwendungen**.
2. Wählen Sie im Feld **Filtern nach** den Filter **Typ** aus und wählen Sie aus dem Dropdown-Menü **SQL** aus.
3. Klicken Sie auf **Details anzeigen**, um alle verfügbaren Backups anzuzeigen.
4. Wählen Sie das Backup aus und klicken Sie auf **Wiederherstellen**.
5. Wählen Sie den Speicherort aus, an dem die Datenbankdateien wiederhergestellt werden sollen.

| Option | Beschreibung |
|---|---|
| Stellen Sie die Datenbank auf demselben Host wieder her, auf dem das Backup erstellt wurde | Wählen Sie diese Option aus, wenn Sie die Datenbank auf demselben SQL-Server wiederherstellen möchten, auf dem die Backups erstellt werden. |
| Wiederherstellung der Datenbank auf einem alternativen Host | Wählen Sie diese Option aus, wenn die Datenbank auf einem anderen SQL-Server auf demselben oder einem anderen Host wiederhergestellt werden soll, auf dem Backups erstellt werden.<br><br>Wählen Sie einen Hostnamen aus, geben Sie einen Datenbanknamen ein (optional), wählen Sie eine Instanz aus und geben Sie die Wiederherstellungspfade an.<br><br>Die im alternativen Pfad angegebene Dateierweiterung muss mit der Dateiendung der ursprünglichen Datenbankdatei identisch sein.<br><br>Wenn die Option **Datenbank auf alternativen Host** wiederherstellen nicht auf der Seite „Bereich wiederherstellen“ angezeigt wird, löschen Sie den Browser-Cache. |

6. Wenn sich der Snapshot im Archiv-Speicher befindet, geben Sie die Priorität an, um Ihre Daten aus dem Archiv-Speicher wiederherzustellen.
7. Wählen Sie auf der Seite **Pre Restore Options** eine der folgenden Optionen aus:
   - Wählen Sie **Überschreiben Sie die Datenbank mit demselben Namen während der Wiederherstellung** aus, um die Datenbank mit dem gleichen Namen wiederherzustellen.
   - Wählen Sie **SQL-Datenbankreplikationseinstellungen beibehalten** aus, um die Datenbank wiederherzustellen und die vorhandenen Replikationseinstellungen beizubehalten.
8. Wählen Sie auf der Seite **Optionen zur Wiederherstellung nach der Wiederherstellung** den Datenbankstatus für die Wiederherstellung weiterer Transaktionsprotokolle aus, eine der folgenden Optionen aus:

- Wählen Sie **Operational, aber nicht verfügbar** aus, wenn Sie jetzt alle notwendigen Backups wiederherstellen.

  Dies ist das Standardverhalten, das die Datenbank durch ein Rollback der nicht gesicherten Transaktionen einsatzbereit macht. Sie können erst dann weitere Transaktionsprotokolle wiederherstellen, wenn Sie ein Backup erstellen.

- Wählen Sie * nicht betriebsbereit, aber verfügbar* aus, um die Datenbank nicht betriebsbereit zu lassen, ohne die nicht gesicherten Transaktionen zurückzurollen.

  Zusätzliche Transaktions-Logs können wiederhergestellt werden. Sie können die Datenbank erst verwenden, wenn sie wiederhergestellt ist.

- Wählen Sie **schreibgeschützter Modus und verfügbar**, um die Datenbank im schreibgeschützten Modus zu belassen.

  Mit dieser Option werden nicht gesicherte Transaktionen rückgängig gemacht, die nicht rückgängig gemachte Aktionen werden jedoch in einer Standby-Datei gespeichert, sodass Recovery-Effekte rückgängig gemacht werden können.

Wenn die Option „Verzeichnis aufheben“ aktiviert ist, werden mehr Transaktionsprotokolle wiederhergestellt. Wenn der Wiederherstellungsvorgang für das Transaktionsprotokoll nicht erfolgreich ist, können die Änderungen zurückgesetzt werden. Die SQL Server-Dokumentation enthält weitere Informationen.

9. Überprüfen Sie die Details und klicken Sie auf **Wiederherstellen**.

## Binden Sie Backups von Applikationen ein

SnapCenter unterstützt die Wiederherstellung von Oracle und HANA Backups auf einem alternativen Host nicht. Damit können Sie mit Cloud Backup für Anwendungen die Oracle- und HANA-Backups auf den angegebenen Host mounten.

### Was Sie brauchen

Wenn Sie ein Backup mounten möchten, das vom sekundären Storage in einen Objektspeicher verschoben wurde, sollten Sie die Details zur primären Arbeitsumgebung hinzufügen und den IP-Speicherplatz festlegen. Weitere Informationen finden Sie unter "Legen Sie IP-Speicherplatz für die primäre Arbeitsumgebung fest".

### Schritte

1. Klicken Sie in BlueXP UI auf **Schutz** > **Sicherung und Wiederherstellung** > **Anwendungen**.
2. Wählen Sie im Feld Filtern nach die Option **Typ** aus und wählen Sie im Dropdown-Menü die Option **SAP HANA** oder **Oracle** aus.
3. Klicken Sie Auf ••• Entsprechend der geschützten Anwendung und wählen Sie **Details anzeigen**.
4. Klicken Sie Auf ••• Entsprechend der Sicherung und wählen Sie **Mount**.
   a. Geben Sie eine der folgenden Optionen an:
      i. Geben Sie in der NAS-Umgebung den FQDN oder die IP-Adresse des Hosts an, auf den aus dem Objektspeicher wiederhergestellte alternative Volumes exportiert werden sollen.
      ii. Geben Sie in der SAN-Umgebung die Initiatoren des Hosts an, denen aus dem Objektspeicher wiederhergestellte LUNs eines alternativen Volumes zugeordnet werden sollen.

b. Geben Sie das Suffix an, das dem alternativen Volume-Namen hinzugefügt wird.

c. Wenn sich der Snapshot im Archiv-Storage befindet, geben Sie die Priorität an, um Ihre Daten aus dem Archiv-Storage abzurufen.

d. Klicken Sie Auf **Mount**.

Dieser Vorgang bindet nur den Storage auf dem angegebenen Host ein. Sie sollten das Dateisystem manuell mounten und die Datenbank aufrufen. Nach Nutzung des alternativen Volumes kann der Storage-Administrator das Volume aus dem ONTAP-Cluster löschen.

Weitere Informationen zum Einrichten der SAP HANA-Datenbank finden Sie unter: "TR-4667: Automatisierung von SAP HANA Systemkopie und Klonvorgängen mit SnapCenter".

# Backup und Restore von Cloud-nativen Applikationsdaten

## Sichern Sie Ihre Daten aus Cloud-nativen Applikationen

Cloud Backup für Applikationen ist ein SaaS-basierter Service mit Datensicherungsfunktionen für Applikationen, die auf NetApp Cloud Storage ausgeführt werden. Cloud Backup für Applikationen innerhalb von NetApp BlueXP (früher Cloud Manager) bietet effiziente, applikationskonsistente, richtlinienbasierte Backups und Restores von Oracle Datenbanken auf Amazon FSX für NetApp ONTAP.

### Der Netapp Architektur Sind

Die Architektur von Cloud Backup für Applikationen umfasst die folgenden Komponenten:

- Cloud Backup für Applikationen ist eine Reihe von Datensicherungsservices, die von NetApp als SaaS-Service gehostet werden und auf der BlueXP SaaS-Plattform basieren.

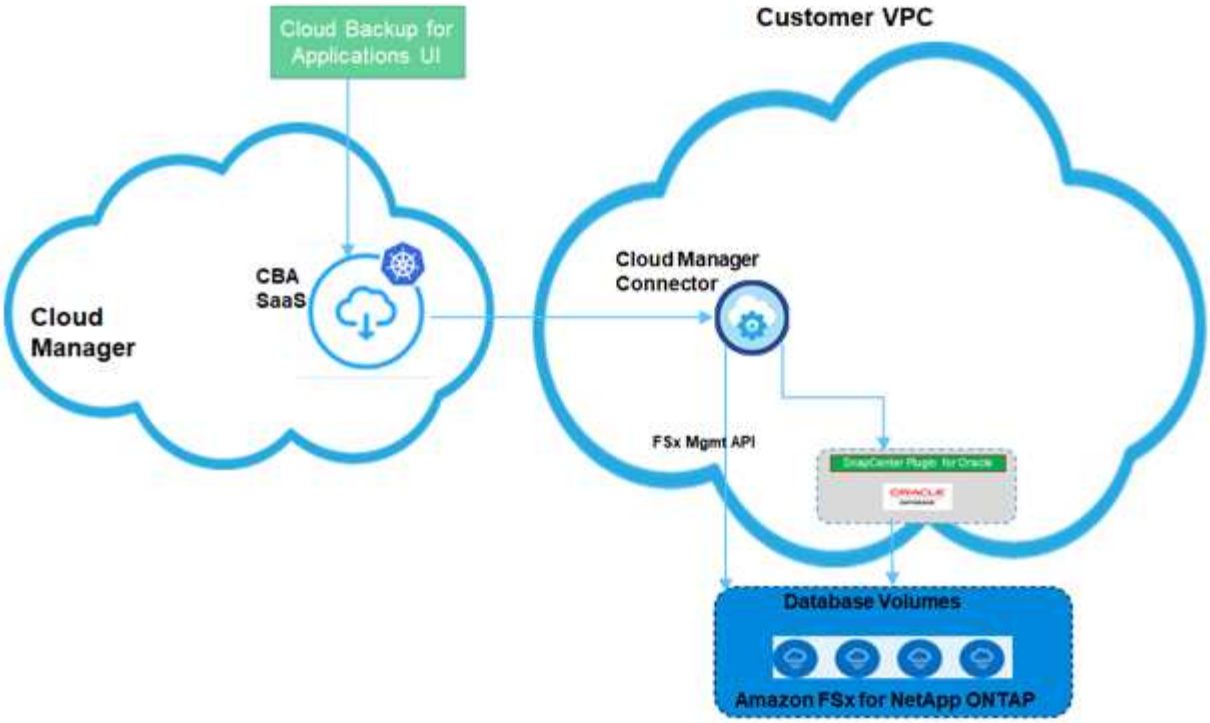
  Die Datensicherungs-Workflows werden für Applikationen auf NetApp Cloud Storage orchestriert.

- Die Benutzeroberfläche von Cloud Backup für Applikationen ist in die Benutzeroberfläche von BlueXP integriert.

  Die Benutzeroberfläche von Cloud Backup für Applikationen bietet diverse Storage- und Datenmanagement-Funktionen.

- BlueXP Connector ist eine Komponente von BlueXP, die in Ihrem Cloud-Netzwerk ausgeführt wird und mit Amazon FSX Storage-Dateisystemen und dem SnapCenter-Plug-in für Oracle interagiert, die auf Oracle-Datenbank-Hosts ausgeführt werden.
- Das SnapCenter Plug-in für Oracle ist eine Komponente, die auf jedem Oracle Datenbank-Host ausgeführt wird und mit den auf dem Host ausgeführten Oracle Datenbanken interagiert, während gleichzeitig Datensicherungsprozesse durchgeführt werden.

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




Für alle von Benutzern initiierten Anfragen kommuniziert die Benutzeroberfläche von Cloud Backup for Applications mit dem SaaS von BlueXP, das bei der Validierung der Anfrageprozesse identisch ist. Wenn die Anforderung einen Workflow wie Backup oder Wiederherstellung ausführen soll, initiiert der SaaS-Service den Workflow und leitet den Anruf an den BlueXP Connector weiter. Der Connector kommuniziert dann mit Amazon FSX für NetApp ONTAP und das SnapCenter Plug-in für Oracle, um die Workflow-Aufgaben auszuführen.

Der Connector kann in derselben VPC wie die der Oracle Datenbanken oder in einer anderen implementiert werden. Wenn sich die Connector- und Oracle-Datenbanken in einem anderen Netzwerk befinden, sollten Sie eine Netzwerkverbindung zwischen ihnen herstellen.

> Die Infrastruktur von Cloud Backup für Applikationen kann Ausfälle der Verfügbarkeitszone innerhalb einer Region nicht kompensieren. Jetzt werden regionale Ausfälle unterstützt, indem ein Failover auf eine neue Region durchgeführt wird, was mit etwa zwei Stunden Ausfallzeit verbunden ist.

### Unterstützte Konfigurationen

- Betriebssystem:
  - RHEL 7.5 oder höher und 8.x
  - L 7.5 oder höher und 8.x
- Storage-System Amazon FSX für ONTAP
- Storage-Layouts: NFS v3 und v4.1 (dNFS wird unterstützt) und iSCSI mit ASM (ASMFD, ASMLib und ASMUdev)
- Applikationen: Oracle Standard und Oracle Enterprise – Standalone (alt und mandantenfähig – CDB und PDB)
- Oracle Versionen: 12cR2, 18c und 19c

### Funktionen

- Automatische Erkennung von Oracle-Datenbanken
- Sichern von Oracle Datenbanken auf Amazon FSX für NetApp ONTAP
  - Vollständiges Backup (Daten + Kontrolle + Archivprotokolldateien)
  - On-Demand-Backup
  - Ein geplantes Backup basiert auf den systemdefinierten oder benutzerdefinierten Richtlinien

    Sie können verschiedene Planungsfrequenzen wie stündlich, täglich, wöchentlich und monatlich in der Richtlinie festlegen.
- Aufbewahrung von Backups anhand der Richtlinie
- Wiederherstellen der vollständigen Oracle-Datenbank (Datendateien + Kontrolldatei) aus dem angegebenen Backup
- Nur Datendateien wiederherstellen und nur Dateien aus dem angegebenen Backup steuern
- Wiederherstellen der Oracle-Datenbank mit bis SCN, bis zu der Zeit, alle verfügbaren Protokolle und keine Recovery-Optionen
- Überwachung von Backups und anderen Aufgaben
- Anzeigen der Schutzzusammenfassung im Dashboard
- Senden von Benachrichtigungen per E-Mail

### Einschränkungen

- Oracle Versionen 11g und 21c werden nicht unterstützt
- Mount-, Klon-, Katalog- und Verifizierungsvorgänge für Backups werden nicht unterstützt
- Bietet keine Unterstützung für Oracle auf RAC und Data Guard
- Backup-Einschränkungen:
  - Bietet keine Unterstützung für Online-Daten oder lediglich für Backup-Protokollierung
  - Keine Unterstützung von Offline-Backups
  - Unterstützt keine Sicherung der Oracle-Datenbank, die sich auf rekursiven Bereitstellungspunkten befindet
  - Unterstützt keine Snapshots von Konsistenzgruppen für Oracle Datenbanken, die sich auf mehreren ASM-Festplattengruppen mit Überschneidungen von FSX Volumes befinden
  - Wenn Ihre Oracle-Datenbanken auf ASM konfiguriert sind, stellen Sie sicher, dass Ihre SVM-Namen für die FSX-Systeme eindeutig sind. Wenn Sie in den FSX-Systemen denselben SVM-Namen haben, werden Backups der auf diesen SVMs befindlichen Oracle Datenbanken nicht unterstützt.
- Einschränkungen bei Wiederherstellungen:
  - Keine Unterstützung für granulare Restores, beispielsweise beim Wiederherstellen von Tabellen und PDBs
  - Unterstützt nur die in-Place-Wiederherstellung von Oracle-Datenbanken unter NAS- und SAN-Layouts
  - Unterstützt nicht die Wiederherstellung von Kontrolldatei nur oder Datendateien + Kontrolldatei von Oracle-Datenbanken auf SAN-Layouts
  - Im SAN-Layout schlägt der Wiederherstellungsvorgang fehl, wenn das SnapCenter Plug-in für Oracle andere fremde Dateien als Oracle-Datendateien auf der ASM-Festplattengruppe findet. Die

Fremddateien können eine oder mehrere der folgenden Typen sein:

- Parameter
- Passwort
- Archivprotokoll
- Online-Protokoll
- ASM-Parameterdatei.

  Aktivieren Sie das Kontrollkästchen in-Place-Wiederherstellung erzwingen, um die fremden Dateien von Typ-Parameter, Passwort und Archivprotokoll zu überschreiben.

> Wenn es andere Arten von Fremddateien gibt, schlägt der Wiederherstellungsvorgang fehl und die Datenbank kann nicht wiederhergestellt werden. Wenn Sie andere Arten von Fremddateien haben, sollten Sie sie löschen oder an einen anderen Speicherort verschieben, bevor Sie den Wiederherstellungsvorgang durchführen.

Aufgrund eines bekannten Problems wird die Fehlermeldung aufgrund von Fremddateien nicht auf der Jobseite in der UI angezeigt. Prüfen Sie die Connector-Protokolle, wenn während der Phase der SAN-Vorabwiederherstellung ein Fehler auftritt, um die Ursache des Problems zu ermitteln.

## Voraussetzungen

Sie sollten Zugriff auf BlueXP haben, ein BlueXP-Konto erstellt, die Arbeitsumgebung und den Connector erstellt und das SnapCenter-Plug-in für Oracle bereitgestellt haben.

### Zugriff auf BlueXP

Sollten Sie "Melden Sie sich bei BlueXP an", Und dann eine "NetApp Konto".

### Erstellung von FSX für ONTAP-Arbeitsumgebung

Sie sollten Amazon FSX für ONTAP-Arbeitsumgebungen erstellen, in denen Ihre Datenbanken gehostet werden. Weitere Informationen finden Sie unter "Erste Schritte mit Amazon FSX für ONTAP" Und "Erstellung und Management einer Amazon FSX für ONTAP Arbeitsumgebung".

Sie können NetApp FSX entweder mit BlueXP oder AWS erstellen. Falls Sie mit AWS erstellt haben, sollten Sie die FSX für ONTAP Systeme in BlueXP entdecken.

### Einen Konnektor erstellen

Ein Account-Administrator muss einen Connector in AWS implementieren, der es BlueXP ermöglicht, Ressourcen und Prozesse in Ihrer Public-Cloud-Umgebung zu managen.

Weitere Informationen finden Sie unter "Erstellen eines Connectors in AWS aus BlueXP".

- Sie sollten denselben Konnektor verwenden, um sowohl FSX-Arbeitsumgebung als auch Oracle-Datenbanken zu verwalten.
- Wenn Sie über die FSX-Arbeitsumgebung und Oracle-Datenbanken in derselben VPC verfügen, können Sie den Connector in derselben VPC implementieren.
- Wenn Sie über die FSX-Arbeitsumgebung und Oracle-Datenbanken in verschiedenen VPCs verfügen:

- Wenn auf FSX NAS-Workloads (NFS) konfiguriert sind, können Sie den Connector auf einem der VPCs erstellen.
- Wenn nur SAN-Workloads konfiguriert sind und keine NAS- (NFS-) Workloads verwendet werden sollen, sollte der Connector in der VPC erstellt werden, über den das FSX-System erstellt wird.

> Für die Verwendung von NAS-Workloads (NFS) sollte ein Transit-Gateway zwischen der Oracle Database VPC und FSX VPC vorhanden sein. Auf die NFS-IP-Adresse, die eine unverankerte IP-Adresse ist, kann von einer anderen VPC nur über das Transit-Gateway zugegriffen werden. Wir können nicht auf die Floating IP-Adressen zugreifen, indem wir die VPCs Peering.

Klicken Sie nach dem Erstellen des Connectors auf **Storage** > **Canvas** > **Meine Arbeitsumgebung** > **Arbeitsumgebung hinzufügen** und folgen Sie den Anweisungen, um die Arbeitsumgebung hinzuzufügen. Stellen Sie sicher, dass Konnektivität zwischen dem Connector und den Oracle-Datenbank-Hosts und der FSX-Arbeitsumgebung vorhanden ist. Der Anschluss sollte eine Verbindung zur Cluster-Management-IP-Adresse der FSX-Arbeitsumgebung herstellen können.

> Klicken Sie nach dem Erstellen des Connectors auf **Connector > Steckverbinder verwalten**; wählen Sie den Namen des Connectors aus, und kopieren Sie die Konnektor-ID.

### Implementieren Sie das SnapCenter Plug-in für Oracle

Sie sollten das SnapCenter Plug-in für Oracle auf jedem der Oracle Datenbank-Hosts bereitstellen. Je nachdem, ob auf dem Oracle-Host die SSH-Schlüsselauthentifizierung aktiviert ist, können Sie eine der Methoden zur Bereitstellung des Plug-ins befolgen.

> Stellen Sie sicher, DASS JAVA 8 auf jedem der Oracle-Datenbank-Hosts installiert ist und die JAVA_HOME-Variable entsprechend eingestellt ist.

#### Plug-in-Implementierung mit SSH-schlüsselbasierter Authentifizierung

Wenn die SSH-Schlüsselauthentifizierung auf dem Oracle-Host aktiviert ist, können Sie zum Bereitstellen des Plug-ins die folgenden Schritte durchführen. Bevor Sie die Schritte durchführen, stellen Sie sicher, dass die SSH-Verbindung zum Connector aktiviert ist.

1. Melden Sie sich bei der Connector-VM als nicht-Root-Benutzer an.
2. Ermitteln Sie den Mount-Pfad für die Basis.
   ```
   sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo
   docker volume inspect | grep Mountpoint
   ```
3. Plug-in implementieren

   ```
   sudo <base_mount_path>/scripts/oracle_plugin_copy_and_install.sh --host
   <host_name> --sshkey <ssh_key_file> --username <user_name> --port <ssh_port>
   --pluginport <plugin_port> --installdir <install_dir>
   ```

   - Host_Name ist der Name des Oracle-Hosts, und dies ist ein obligatorischer Parameter.
   - ssh_Key_file ist SSH-Schlüssel, der für die Verbindung zum Oracle-Host verwendet wird und dies ist ein obligatorischer Parameter.
   - User_Name: Benutzer mit SSH-Berechtigungen auf dem Oracle-Host und dies ist ein optionaler Parameter. Der Standardwert ist ec2-user.

- ssh_Port: SSH-Port auf dem Oracle-Host und dies ist ein optionaler Parameter. Der Standardwert ist 22
- Plugin_Port: Port verwendet vom Plug-in und dies ist ein optionaler Parameter. Der Standardwert ist 8145
- Install_dir: Verzeichnis, in dem das Plug-in bereitgestellt wird und dies ein optionaler Parameter ist. Standardwert ist /opt.

Beispiel: `sudo /var/lib/docker/volumes/service-manager-2_cloudmanager_scs_cloud_volume/_data/scripts/oracle_plugin_copy_and_install.sh --host xxx.xx.x.x --sshkey /keys/netapp-ssh.ppk`

#### Manuelle Implementierung des Plug-ins

Wenn die SSH-Schlüsselauthentifizierung auf dem Oracle-Host nicht aktiviert ist, sollten Sie die folgenden manuellen Schritte durchführen, um das Plug-in bereitzustellen.

1. Melden Sie sich bei der Connector-VM an.
2. Laden Sie die SnapCenter Linux Host Plug-in-Binärdatei herunter.
   ```
   sudo docker exec -it cloudmanager_scs_cloud curl -X GET
   'http://127.0.0.1/deploy/downloadLinuxPlugin'
   ```
3. Ermitteln Sie den Mount-Pfad für die Basis.
   ```
   sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo
   docker volume inspect | grep Mountpoint
   ```
4. Den Binärpfad des heruntergeladenen Plug-ins abrufen.
   ```
   sudo ls <base_mount_path> $(sudo docker ps|grep -Po
   "cloudmanager_scs_cloud:.*? "|sed -e 's/ *$//'|cut -f2 -d":")/sc-linux-host
   -plugin/snapcenter_linux_host_plugin_scs.bin
   ```
5. Kopieren Sie *snapcenter_linux_Host_Plugin_scs.bin* auf jeden der Oracle-Datenbank-Hosts, entweder mit scp oder anderen alternativen Methoden.
6. Führen Sie auf dem Oracle-Datenbank-Host den folgenden Befehl aus, um Berechtigungen für die Binärdatei auszuführen.
   ```
   chmod +x snapcenter_linux_host_plugin_scs.bin
   ```
7. Implementieren Sie das Oracle Plug-in als Root-Benutzer.
   ```
   ./snapcenter_linux_host_plugin_scs.bin -i silent
   ```
8. Kopieren Sie *Certificate.p12* von *<base_Mount_PATH>/Client/Certificate/* Pfad der Connector-VM auf den Plug-in-Host zu */var/opt/snapcenter/spl/etc/*.
   a. Navigieren Sie zu */var/opt/snapcenter/spl/etc* und führen Sie den keytool-Befehl aus, um das Zertifikat zu importieren.
      ```
      keytool -v -importkeystore -srckeystore certificate.p12 -srcstoretype PKCS12
      -destkeystore keystore.jks -deststoretype JKS -srcstorepass snapcenter
      -deststorepass snapcenter -srcalias agentcert -destalias agentcert -noprompt
      ```
   b. SPL neu starten: `systemctl restart spl`

## Backup von Cloud-nativen Applikationsdaten

### Erkennen Sie die Anwendungen

Sie sollten die Datenbanken auf dem Host erkennen, um Richtlinien zuzuweisen und Backups zu erstellen.

#### Was Sie brauchen

- Sie sollten die FSX für die Arbeitsumgebung ONTAP und den Connector erstellt haben.
- Stellen Sie sicher, dass der Connector mit dem FSX für die ONTAP-Arbeitsumgebung und den Oracle-Datenbank-Hosts verbunden ist.
- Stellen Sie sicher, dass der BlueXP-Benutzer über die Rolle „Account Admin“ verfügt.
- Sie sollten das SnapCenter Plug-in für Oracle implementiert haben. "Weitere Informationen .".

#### Schritte

1. Klicken Sie in BlueXP UI auf **Schutz** > **Sicherung und Wiederherstellung** > **Anwendungen**.
2. Klicken Sie Auf Anwendungen Ermitteln.
3. Wählen Sie **Cloud Native** und klicken Sie auf **Next**.

   Ein Servicekonto mit der Rolle *SnapCenter System* wird erstellt, um für alle Benutzer dieses Kontos geplante Datensicherungsvorgänge durchzuführen.

   - Klicken Sie auf **Konto** > **Konto verwalten** > **Mitglieder**, um das Servicekonto anzuzeigen.

     Das Service-Konto (*SnapCenter-Account-<accountid>*) wird für die Ausführung der geplanten Backup-Vorgänge verwendet. Sie sollten das Dienstkonto niemals löschen.

4. Geben Sie auf der Seite Hostdetails angeben die Details des Oracle-Datenbank-Hosts ein, aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass das Plug-in auf dem Host installiert ist, und klicken Sie auf **Entdecken**.
   - Zeigt alle Datenbanken auf dem Host an. Wenn die Betriebssystemauthentifizierung für die Datenbank deaktiviert ist, sollten Sie die Datenbankauthentifizierung konfigurieren, indem Sie auf **Configure** klicken. Weitere Informationen finden Sie unter Konfigurieren Sie die Anmeldedaten für die Oracle-Datenbank.
   - Klicken Sie auf **Anwendung verwalten**, wählen Sie **Hinzufügen**, um einen neuen Host hinzuzufügen, **Aktualisieren**, um neue Datenbanken zu entdecken, oder **Entfernen**, um einen Datenbank-Host zu entfernen.
   - Klicken Sie auf **Einstellungen** und wählen Sie **Richtlinien**, um die vordefinierten Richtlinien anzuzeigen. Überprüfen Sie die vordefinierten Richtlinien, und wenn Sie möchten, können Sie sie entweder bearbeiten, um Ihre Anforderung zu erfüllen, oder erstellen Sie eine neue Richtlinie.

#### Konfigurieren Sie die Anmeldedaten für die Oracle-Datenbank

Sie sollten Anmeldedaten konfigurieren, die für Datensicherungsvorgänge in Oracle-Datenbanken verwendet werden.

#### Schritte

1. Wenn die Betriebssystemauthentifizierung für die Datenbank deaktiviert ist, sollten Sie die Datenbankauthentifizierung konfigurieren, indem Sie auf **Configure** klicken.

2. Geben Sie den Benutzernamen, das Kennwort und die Anschlussdetails entweder im Abschnitt Datenbankeinstellungen oder ASM-Einstellungen an.

   Der Oracle-Benutzer sollte über sysdba-Berechtigungen verfügen, und ASM-Benutzer sollten sysmasm-Berechtigungen haben.

3. Klicken Sie Auf **Konfigurieren**.

#### Erstellen einer Richtlinie

Sie können Richtlinien erstellen, wenn Sie die vordefinierten Richtlinien nicht bearbeiten möchten.

**Schritte**

1. Wählen Sie auf der Seite Anwendungen aus der Dropdown-Liste Einstellungen die Option **Richtlinien** aus.
2. Klicken Sie auf **Create Policy**.
3. Geben Sie einen Richtliniennamen an.
4. (Optional) Bearbeiten Sie das Format des Backup-Namens.
5. Geben Sie den Zeitplan und die Aufbewahrungsdetails an.
6. Klicken Sie Auf **Erstellen**.

### Backup der Cloud-nativen Applikationsdaten

Sie können entweder eine vordefinierte Richtlinie zuweisen oder eine Richtlinie erstellen und sie dann der Datenbank zuweisen. Sobald die Richtlinie zugewiesen ist, werden die Backups gemäß dem in der Richtlinie definierten Zeitplan erstellt. Sie können auch ein On-Demand-Backup erstellen.

> Wenn Sie ASM-Festplattengruppen für Oracle erstellen, stellen Sie sicher, dass keine gemeinsamen Volumes in Festplattengruppen vorhanden sind. Jede Festplattengruppe benötigt dedizierte Volumes.

**Schritte**

1. Wenn die Datenbank nicht mit einer Richtlinie geschützt ist, klicken Sie auf der Seite Anwendungen auf **Richtlinie zuweisen**.

   Wenn die Datenbank mit einer oder mehreren Richtlinien geschützt ist, können Sie durch Klicken auf weitere Richtlinien zuweisen ••• > **Richtlinie Zuweisen**.

2. Wählen Sie die Richtlinie aus und klicken Sie auf **Zuweisen**.

   Die Backups werden gemäß dem in der Richtlinie definierten Zeitplan erstellt.

   > Das Servicekonto (*SnapCenter-Account-<Account_id>*) wird zur Ausführung der geplanten Backup-Vorgänge verwendet.

#### Erstellen von On-Demand-Backups

Nach der Zuweisung der Richtlinie können Sie ein On-Demand-Backup der Applikation erstellen.

### Schritte

1. Klicken Sie auf der Seite Anwendungen auf ••• Entsprechend der Anwendung und klicken Sie auf **On-Demand Backup**.
2. Wenn der Anwendung mehrere Richtlinien zugewiesen werden, wählen Sie die Richtlinie, den Aufbewahrungswert aus und klicken Sie dann auf **Backup erstellen**.

### Weitere Informationen

Nach dem Wiederherstellen einer großen Datenbank (250 GB oder mehr), wenn Sie ein vollständiges Online-Backup in derselben Datenbank durchführen, kann der Vorgang mit dem folgenden Fehler fehlschlagen:

```
failed with status code 500, error
{\"error\":{\"code\":\"app_internal_error\",\"message\":\"Failed to create
snapshot. Reason: Snapshot operation not allowed due to clones backed by
snapshots. Try again after sometime.
```

Informationen zur Behebung dieses Problems finden Sie unter: "Der Snapshot-Vorgang ist aufgrund von durch Snapshots gesicherten Klonen nicht zulässig".

## Sicherung von Cloud-nativen Applikationsdaten managen

### Überwachen von Jobs

Sie können den Status der Jobs überwachen, die in Ihren Arbeitsumgebungen initiiert wurden. Auf diese Weise können Sie die Aufträge sehen, die erfolgreich abgeschlossen wurden, die derzeit in Bearbeitung sind und die, die nicht erfolgreich abgeschlossen wurden, damit Sie Probleme diagnostizieren und beheben können.

Sie können eine Liste aller Vorgänge und deren Status anzeigen. Jeder Vorgang oder Job hat eine eindeutige ID und einen Status. Der Status kann lauten:

- Erfolgreich
- In Bearbeitung
- Warteschlange
- Warnung
- Fehlgeschlagen

### Schritte

1. Klicken Sie auf **Backup und Recovery**.
2. Klicken Sie Auf **Jobüberwachung**

   Sie können auf den Namen eines Jobs klicken, um die entsprechenden Details anzuzeigen. Wenn Sie nach einer bestimmten Stelle suchen, können Sie:

   - Verwenden Sie die Zeitauswahl oben auf der Seite, um Jobs für einen bestimmten Zeitraum anzuzeigen
   - Geben Sie einen Teil des Jobnamens in das Suchfeld ein
   - Sortieren Sie die Ergebnisse mithilfe des Filters in jeder Spaltenüberschrift

### Zeigen Sie Backup-Details an

Sie können die Gesamtzahl der erstellten Backups, die Richtlinien zum Erstellen von Backups, die Datenbankversion und die Agenten-ID anzeigen.

1. Klicken Sie auf **Backup und Recovery** > **Anwendungen**.
2. Klicken Sie Auf ••• Entsprechend der Anwendung und klicken Sie auf **Details anzeigen**.

> Die Agent-ID ist dem Konnektor zugeordnet. Wenn ein Connector, der bei der Registrierung des Oracle-Datenbank-Hosts verwendet wurde, nicht mehr vorhanden ist, schlagen die nachfolgenden Backups dieser Anwendung fehl, da die Agent-ID des neuen Connectors anders ist. Sie sollten die API **Connector-Update** ausführen, um die Agenten-ID zu ändern.

### Aktualisieren Sie die Verbindungsdetails

Wenn ein Connector, der bei der Registrierung des Oracle-Datenbank-Hosts verwendet wurde, nicht mehr existiert oder in AWS beschädigt ist, sollten Sie einen neuen Konnektor bereitstellen. Nach der Bereitstellung des neuen Connectors sollten Sie die **Connector-Update** API ausführen, um die Connector-Details zu aktualisieren.

```
curl --location --request PATCH
'https://snapcenter.cloudmanager.cloud.netapp.com/api/oracle/databases/con
nector-update' \
--header 'x-account-id: <CM account-id>' \
--header 'x-agent-id: <connector Agent ID >' \
--header 'Authorization: Bearer token' \
--header 'Content-Type: application/json' \
--data-raw '{
"old_connector_id": "Old connector id that no longer exist",
"new_connector_id": "New connector Id"
}
```

Nach dem Aktualisieren der Connector-Details sollten Sie eine Verbindung zum Oracle-Datenbank-Host herstellen und die folgenden Schritte durchführen:

1. Holen Sie die Plug-in-Informationen ab, die auf dem Oracle Database Host ausgeführt werden.
   `rpm -qi netapp-snapcenter-plugin-oracle`
2. Deinstallieren Sie das Plug-in.
   `sudo /opt/NetApp/snapcenter/spl/installation/plugins/uninstall`
3. Überprüfen Sie, ob das Plug-in erfolgreich deinstalliert wurde.
   `rpm -qi netapp-snapcenter-plugin-oracle`

Nachdem Sie das Plug-in deinstalliert haben, können Sie das Plug-in bereitstellen. "Weitere Informationen .".

### Konfigurieren Sie das Zertifikat der Zertifizierungsstelle

Sie können ein Zertifikat mit Zertifizierungsstelle konfigurieren, wenn Sie zusätzliche Sicherheit in Ihre Umgebung aufnehmen möchten.

#### Konfigurieren Sie das Zertifikat einer Zertifizierungsstelle für die Authentifizierung des Clientzertifikats

Der Anschluss verwendet ein selbstsigniertes Zertifikat, um mit dem Plug-in zu kommunizieren. Das selbstsignierte Zertifikat wird vom Installationsskript in den Schlüsselspeicher importiert. Sie können die folgenden Schritte durchführen, um das selbstsignierte Zertifikat durch CA-signiertes Zertifikat zu ersetzen.

**Was Sie brauchen**

Sie können den folgenden Befehl ausführen, um *<base_Mount_path>* zu erhalten:

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo
docker volume inspect | grep Mountpoint
```

**Schritte**

1. Melden Sie sich bei Connector an.
2. Löschen Sie alle vorhandenen Dateien unter *<base_Mount_PATH>/Client/Certificate* in der virtuellen Connector-Maschine.
3. Kopieren Sie das von der Zertifizierungsstelle signierte Zertifikat und die Schlüsseldatei in die virtuelle Konnektor-Maschine *<base_Mount_PATH>/Client/Certificate*.

   Der Dateiname sollte Certificate.pem und key.pem sein. Das Zertifikat.pem sollte die gesamte Kette der Zertifikate wie Zwischenzertifikat und Root CA haben.

4. Erstellen Sie das PKCS12-Format des Zertifikats mit dem Namen Certificate.p12 und behalten Sie *<base_Mount_path>/Client/Certificate*.
5. Kopieren Sie das Zertifikat.p12 und die Zertifikate für alle Zwischenkatopie und Root-CA auf den Plug-in-Host unter */var/opt/snapcenter/spl/etc/*.
6. Melden Sie sich beim Plug-in-Host an.
7. Navigieren Sie zu */var/opt/snapcenter/spl/etc* und führen Sie den keytool-Befehl aus, um die Datei Certificate.p12 zu importieren.
   ```
   keytool -v -importkeystore -srckeystore certificate.p12 -srcstoretype PKCS12
   -destkeystore keystore.jks -deststoretype JKS -srcstorepass snapcenter
   -deststorepass snapcenter -srcalias agentcert -destalias agentcert -noprompt
   ```
8. Importieren Sie die Stammzertifizierungsstelle und die Zwischenzertifikate.
   ```
   keytool -import -trustcacerts -keystore keystore.jks -storepass snapcenter
   -alias trustedca -file <certificate.crt>
   ```

   > Die certfile.crt bezieht sich auf die Zertifikate der Root CA sowie der Zwischenzertifizierungsstelle.

9. SPL neu starten: `systemctl restart spl`

#### Konfigurieren Sie das CA-Zertifikat für das Server-Zertifikat des Plug-ins

Das CA-Zertifikat sollte den genauen Namen des Oracle-Plug-in-Hosts haben, mit dem die virtuelle Connector-Maschine kommuniziert.

**Was Sie brauchen**

Sie können den folgenden Befehl ausführen, um *<base_Mount_path>* zu erhalten:

```
sudo docker volume ls | grep scs_cloud_volume | awk {'print $2'} | xargs sudo
```

```
docker volume inspect | grep Mountpoint
```

**Schritte**

1. Führen Sie auf dem Plug-in-Host folgende Schritte durch:
   a. Navigieren Sie zum Ordner mit dem SPL-Schlüsselspeicher */var/opt/snapcenter/spl/etc*.
   b. Erstellen Sie das PKCS12-Format des Zertifikats, das sowohl ein Zertifikat als auch einen Schlüssel mit dem Alias *splkeystore* hat.
   c. Fügen Sie das CA-Zertifikat hinzu.
      ```
      keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS -srcalias splkeystore -destalias splkeystore -noprompt
      ```
   d. Überprüfen Sie die Zertifikate.
      ```
      keytool -list -v -keystore keystore.jks
      ```
   e. SPL neu starten: `systemctl restart spl`
2. Führen Sie die folgenden Schritte auf dem Konnektor aus:
   a. Melden Sie sich beim Connector als nicht-Root-Benutzer an.
   b. Kopieren Sie die gesamte Kette der CA-Zertifikate auf das persistente Volume unter *<base_Mount_PATH>/Server*.

      Erstellen Sie den Serverordner, falls er nicht vorhanden ist.

   c. Verbinden Sie sich mit dem cloudmanager_scs_Cloud und ändern Sie den **enableCACert** in *config.yml* an **true**.
      ```
      sudo docker exec -t cloudmanager_scs_cloud sed -i 's/enableCACert: false/enableCACert: true/g' /opt/netapp/cloudmanager-scs-cloud/config/config.yml
      ```
   d. Starten Sie den Cloud-Manager_scs_Cloud-Container neu.
      ```
      sudo docker restart cloudmanager_scs_cloud
      ```

**Zugriff auf REST-APIs**

ES sind DIE REST-APIs zum Schutz der Applikationen in der Cloud verfügbar "Hier".

Sie sollten das Benutzer-Token mit gebündelter Authentifizierung erhalten, um auf DIE REST-APIs zuzugreifen. Informationen zum Abrufen des Benutzer-Tokens finden Sie unter "Erstellen Sie ein Benutzer-Token mit gebündelter Authentifizierung".

## Stellen Sie Cloud-native Applikationsdaten wieder her

Im Falle eines Datenverlustes können Sie die Datendateien, Kontrolldateien oder beides wiederherstellen. Anschließend können Sie die Datenbank wiederherstellen.

**Schritte**

1. Klicken Sie Auf ••• Entsprechend der Datenbank, die Sie wiederherstellen möchten, und klicken Sie auf **Details anzeigen**.
2. Klicken Sie Auf ••• Entsprechend der Datensicherung, die Sie für die Wiederherstellung verwenden

möchten, und klicken Sie auf **Restore**.

3. Führen Sie im Abschnitt „Umfang wiederherstellen“ die folgenden Aktionen durch:

| Sie suchen… | Tun Sie das… |
|---|---|
| Möchten nur die Datendateien wiederherstellen | Wählen Sie **Alle Datendateien**. |
| Möchten nur die Kontrolldateien wiederherstellen | Wählen Sie **Steuerdateien** |
| Kunden möchten sowohl Datendateien als auch Kontrolldateien wiederherstellen | Wählen Sie **Alle Datendateien** und **Kontrolldateien** aus. |

> Die Wiederherstellung von Datendateien mit Kontrolldateien oder nur Kontrolldateien wird für iSCSI im ASM-Layout nicht unterstützt.

Sie können auch das Kontrollkästchen **in-Place-Wiederherstellung erzwingen** aktivieren.

Die Option **Kraft in-Place Restore** überschreibt die Datei spfile, Password file und Archivprotokolldateien aus der Diskgroup der Datendateien. Sie sollten das neueste Backup verwenden, wenn die Option **in-Place Restore** erzwingen ausgewählt ist.

4. Führen Sie im Abschnitt „Recovery Scope“ die folgenden Schritte aus:

| Sie suchen… | Tun Sie das… |
|---|---|
| Möchten Sie die letzte Transaktion wiederherstellen | Wählen Sie **Alle Protokolle**. |
| Wiederherstellen einer bestimmten Systemänderungsnummer (SCN) | Wählen Sie **bis Systemänderungsnummer** und geben Sie das SCN an. |
| Sie möchten ein Recovery zu einem bestimmten Datum und einer bestimmten Zeit durchführen | Wählen Sie **Datum und Uhrzeit**. |
| Möchten Sie nicht wiederherstellen | Wählen Sie **Keine Wiederherstellung**. |

Für den ausgewählten Wiederherstellungsbereich können Sie im Feld **Archiv Log Files Locations** optional den Speicherort angeben, der die für die Wiederherstellung erforderlichen Archivprotokolle enthält.

Aktivieren Sie das Kontrollkästchen, wenn Sie die Datenbank nach der Wiederherstellung im LESE-SCHREIB-Modus öffnen möchten.

5. Klicken Sie auf **Weiter** und prüfen Sie die Details.
6. Klicken Sie Auf **Wiederherstellen**.

# Daten von Virtual Machines sichern und wiederherstellen

## Sichern Sie Ihre Daten von Virtual Machines

Durch die Integration des SnapCenter Plug-ins für VMware vSphere in BlueXP (ehemals Cloud Manager) können Sie Daten auf Ihren virtuellen Maschinen schützen. Sie können Datastores in der Cloud sichern und Virtual Machines problemlos im lokalen SnapCenter Plug-in für VMware vSphere wiederherstellen.

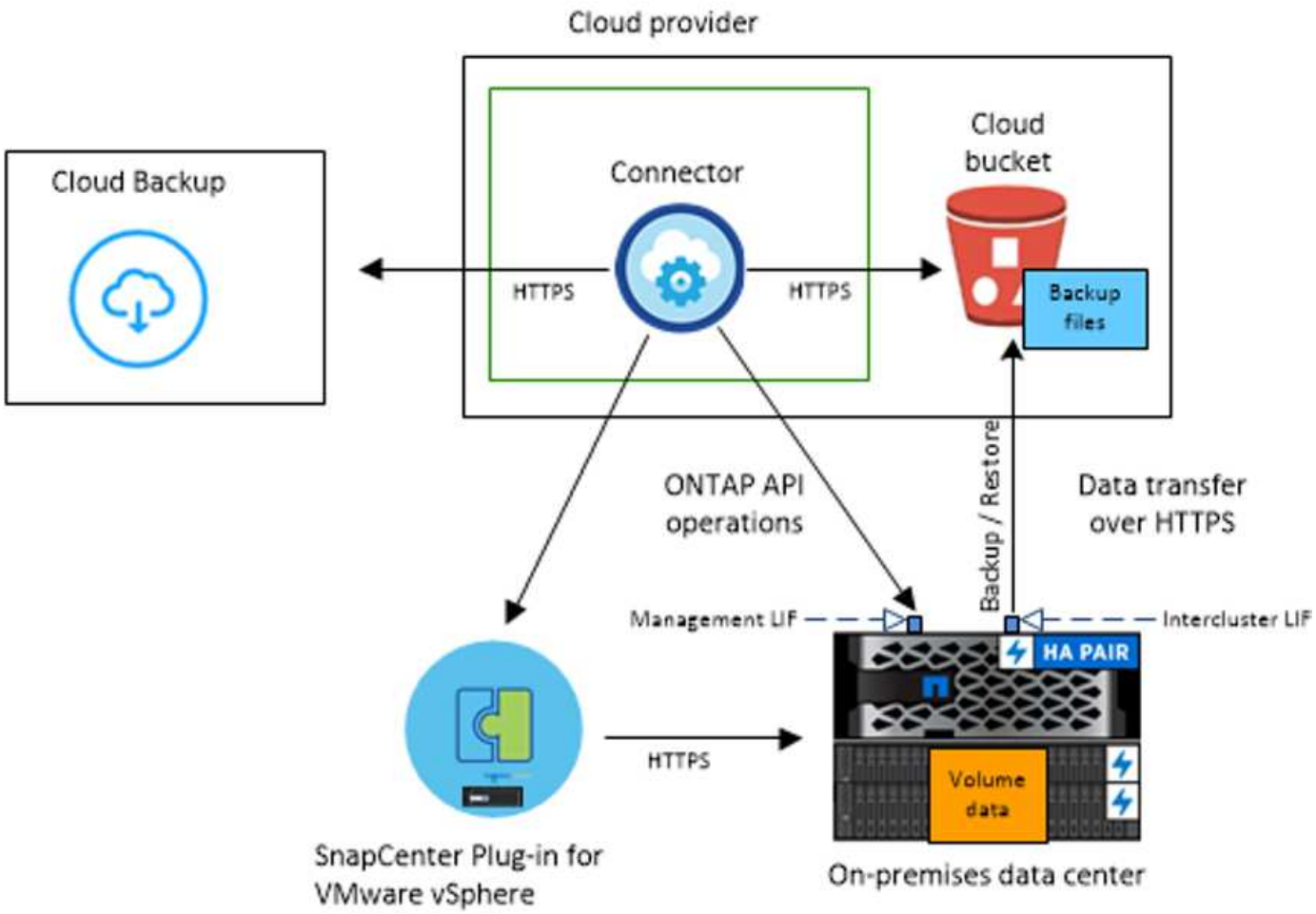
Sie können Backups von Datastores auf Amazon Web Services S3, Microsoft Azure Blob und StorageGRID erstellen.

### Anforderungen

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie mit dem Backup von Datastores und Virtual Machines in Cloud-Services beginnen.

- SnapCenter Plug-in für VMware vSphere 4.6P1 oder höher
- ONTAP 9.8 oder höher
- BlueXP 3.9 oder höher
- In SnapCenter-Plug-in für VMware vSphere 4.6P1 sollte mindestens ein Backup erstellt werden.
- In SnapCenter Plug-in für VMware vSphere wird mindestens eine Tages-, Wochen- oder Monatsrichtlinie verwendet, ohne dass ein Etikett oder dieselbe Bezeichnung wie die Richtlinie für Cloud Backup für virtuelle Maschinen in BlueXP lautet.
- Im Rahmen einer vordefinierten Richtlinie sollte die Zeitplanebene für den Datenspeicher im SnapCenter Plug-in für VMware vSphere und in der Cloud identisch sein.
- Stellen Sie sicher, dass keine FlexGroup Volumes im Datenspeicher vorhanden sind, da Backup und Wiederherstellung von FlexGroup Volumes nicht unterstützt werden.
- Stellen Sie sicher, dass keines der Volumes verschlüsselt ist, da die Wiederherstellung verschlüsselter Volumes nicht unterstützt wird.
- Deaktivieren Sie „**_recent**“ für die erforderlichen Ressourcengruppen. Wenn Sie für die Ressourcengruppe „**_recent**“ aktiviert haben, können die Backups dieser Ressourcengruppen nicht für den Datenschutz in der Cloud verwendet und können anschließend nicht für den Wiederherstellungsvorgang verwendet werden.
- Stellen Sie sicher, dass der Ziel-Datastore, auf dem die virtuelle Maschine wiederhergestellt wird, genügend Speicherplatz für eine Kopie aller VM-Dateien wie VMDK, VMX, VMSD usw. hat.
- Stellen Sie sicher, dass im Zieldatenspeicher keine veralteten Dateien der virtuellen Maschine im Format restore_xxx_xxxxxx_filename aus dem vorherigen Wiederherstellungsvorgang vorliegen. Sie sollten die veralteten Dateien löschen, bevor Sie eine Wiederherstellung durchführen.

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




# Registrieren Sie das SnapCenter Plug-in für VMware vSphere

Sie sollten das SnapCenter-Plug-in für VMware vSphere in BlueXP registrieren, damit die Datenspeicher und virtuellen Maschinen in BlueXP angezeigt werden. Das SnapCenter Plug-in für VMware vSphere kann nur von Benutzern mit Administratorzugriff registriert werden.

> Sie können mehrere SnapCenter Plug-in für VMware vSphere registrieren. Nach der Registrierung können Sie jedoch das SnapCenter-Plug-in für VMware vSphere nicht mehr entfernen.

**Schritte**

1. Klicken Sie in BlueXP UI auf **Schutz** > **Sicherung und Wiederherstellung** > **Virtuelle Maschinen**.
2. Klicken Sie im Dropdown-Menü **Einstellungen** auf **SnapCenter Plug-in für VMware vSphere**.
3. Klicken Sie auf **Registrieren SnapCenter Plug-in für VMware vSphere**.
4. Geben Sie folgende Details an:
   a. Geben Sie im Feld SnapCenter-Plug-in für VMware vSphere den FQDN oder die IP-Adresse des SnapCenter-Plug-ins für VMware vSphere an.
   b. Geben Sie im Feld Port die Portnummer an, auf der das SnapCenter Plug-in für VMware vSphere

ausgeführt wird.

Sie sollten sicherstellen, dass der Port für die Kommunikation zwischen SnapCenter Plug-in für VMware vSphere und Cloud Backup für virtuelle Maschinen offen ist.

c. Geben Sie im Feld Benutzername und Kennwort die Anmeldeinformationen des Benutzers mit der Administratorrolle an.

5. Klicken Sie Auf **Registrieren**.

**Nach Ihrer Beendigung**

Klicken Sie auf **Sicherung und Wiederherstellung** > **Virtuelle Maschinen**, um alle Datastores und virtuellen Maschinen anzuzeigen, die mit dem registrierten SnapCenter Plug-in für VMware vSphere geschützt werden können.

# Erstellen einer Richtlinie zum Backup von Virtual Machines

Sie können eine Richtlinie erstellen oder eine der folgenden vordefinierten Richtlinien verwenden, die in BlueXP verfügbar sind.

| Name Der Richtlinie | Etikett | Aufbewahrungswert |
|---|---|---|
| 1 Jahr tägliche LTR | Täglich | 366 |
| 5 Jahre tägliche LTR | Täglich | 1830 |
| 7 Jahre wöchentlicher LTR | Wöchentlich | 370 |
| 10 Jahre Monatliche LTR | Monatlich | 120 |

Sie sollten Richtlinien erstellen, wenn Sie die vordefinierten Richtlinien nicht bearbeiten möchten.

**Schritte**

1. Wählen Sie auf der Seite Virtuelle Maschinen aus der Dropdown-Liste Einstellungen die Option **Richtlinien** aus.
2. Klicken Sie auf **Create Policy**.
3. Geben Sie einen Richtliniennamen an.
4. Geben Sie den Zeitplan und die Aufbewahrungsdetails an.

   Standardmäßig wird die Sicherungsquelle als primäre Quelle ausgewählt.

5. Klicken Sie Auf **Erstellen**.

# Sichern Sie Datenspeicher in StorageGRID

Durch Integration des SnapCenter Plug-ins für VMware vSphere mit BlueXP können Sie ein oder mehrere Datastores in StorageGRID sichern. So können VM-Administratoren Daten für Storage-Effizienz einfach und schnell sichern und archivieren und die Cloud-

Transition beschleunigen.

> Stellen Sie sicher, dass Sie alle erfüllt haben "Anforderungen" Vor dem Backup von Datastores in der Cloud.

**Schritte**

1. Klicken Sie in BlueXP UI auf **Schutz** > **Sicherung und Wiederherstellung** > **Virtuelle Maschinen**.
2. Klicken Sie Auf ••• Entsprechend dem Datastore, den Sie sichern möchten, und klicken Sie auf **Backup aktivieren**.
3. Wählen Sie auf der Seite Richtlinie zuweisen die Richtlinie aus und klicken Sie auf **Weiter**.
4. Fügen Sie die Arbeitsumgebung hinzu.

   Konfigurieren Sie die ONTAP-Cluster, die BlueXP zum Sichern Ihrer Datenspeicher entdecken soll. Nachdem Sie die Arbeitsumgebung für einen der Datenspeicher hinzugefügt haben, können Sie sie für alle anderen Datenspeicher im selben ONTAP Cluster verwenden.

   a. Klicken Sie auf **Arbeitsumgebung hinzufügen** der SVM.
   b. Im Assistenten „Arbeitsumgebung hinzufügen“:
      i. Geben Sie die IP-Adresse des ONTAP-Clusters an.
      ii. Geben Sie die Anmeldedaten des ONTAP-Cluster-Benutzers an.
   c. Klicken Sie Auf **Arbeitsumgebung Hinzufügen**.
5. Wählen Sie **StorageGRID**.
   a. Geben Sie die Speicher-Server-IP an.
   b. Wählen Sie den Zugriffsschlüssel und den geheimen Schlüssel aus.
6. Überprüfen Sie die Details und klicken Sie auf **Backup aktivieren**.

# Management der Sicherung von Virtual Machines

Sie können Richtlinien, Datastores und Virtual Machines anzeigen, bevor Sie Daten sichern und wiederherstellen. Abhängig von der Änderung in der Datenbank, Richtlinien oder Ressourcengruppen können Sie die Updates über die BlueXP-Benutzeroberfläche aktualisieren.

## Anzeigen von Richtlinien

Sie können alle vordefinierten Standardrichtlinien anzeigen. Wenn Sie die Details anzeigen, werden für jede dieser Richtlinien alle zugehörigen Cloud Backup für Virtual Machines und alle zugehörigen Virtual Machines aufgelistet.

1. Klicken Sie in BlueXP UI auf **Schutz** > **Sicherung und Wiederherstellung** > **Virtuelle Maschinen**.
2. Klicken Sie im Dropdown-Menü **Einstellungen** auf **Richtlinien**.
3. Klicken Sie auf **Details anzeigen** entsprechend der Richtlinie, deren Details Sie anzeigen möchten.

Die zugehörigen Richtlinien für Cloud Backup für Virtual Machines und alle Virtual Machines werden aufgelistet.

## Sehen Sie sich die Datenspeicher und Virtual Machines an

Es werden die Datenspeicher und Virtual Machines angezeigt, die mit dem registrierten SnapCenter Plug-in für VMware vSphere gesichert sind.

### Über diese Aufgabe

- Nur NFS-Datastores werden angezeigt.
- Es werden nur Datastores angezeigt, für die mindestens eine erfolgreiche Sicherung im SnapCenter-Plug-in für VMware vSphere erfolgt ist.

### Schritte

1. Klicken Sie in BlueXP UI auf **Schutz** > **Sicherung und Wiederherstellung** > **Virtuelle Maschinen** > **Einstellungen** > **SnapCenter Plug-in für VMware vSphere**.
2. Klicken Sie auf das SnapCenter-Plug-in für VMware vSphere, dessen Datenspeicher und Virtual Machines angezeigt werden sollen.

## Bearbeiten Sie das SnapCenter Plug-in für die VMware vSphere-Instanz

Die Details zum SnapCenter Plug-in für VMware vSphere können Sie unter BlueXP bearbeiten

### Schritte

1. Klicken Sie in BlueXP UI auf **Schutz** > **Sicherung und Wiederherstellung** > **Virtuelle Maschinen** > **Einstellungen** > **SnapCenter Plug-in für VMware vSphere**.
2. Klicken Sie auf und wählen Sie **Bearbeiten**
3. Ändern Sie die Details nach Bedarf
4. Klicken Sie Auf **Speichern**.

## Aktualisieren Sie Den Sicherungsstatus

Wenn der Datenbank neue Volumes hinzugefügt werden oder sich die Richtlinie oder Ressourcengruppe ändert, sollten Sie den Schutz aktualisieren.

1. Klicken Sie auf **Backup und Wiederherstellung** > **Virtuelle Maschinen**.
2. Klicken Sie im Dropdown-Menü **Einstellungen** auf **SnapCenter Plug-in für VMware vSphere**.
3. Klicken Sie Auf ••• Entsprechend dem SnapCenter Plug-in für VMware vSphere, das die virtuelle Maschine hostet, und klicken Sie auf **Aktualisieren**.

   Die neuen Änderungen werden ermittelt.

4. Klicken Sie Auf ••• Entsprechend dem Datastore und klicken Sie auf **Refresh Protection**, um den Cloud-Schutz für die Änderungen zu aktivieren.

## Überwachen Von Jobs

Für alle Cloud-Backup-Vorgänge werden Jobs erstellt. Sie können alle Jobs und alle Unteraufgaben, die als Teil jeder Aufgabe ausgeführt werden, überwachen.

1. Klicken Sie auf **Sicherung und Wiederherstellung** > **Jobüberwachung**.

   Wenn Sie einen Vorgang starten, wird ein Fenster angezeigt, in dem Sie angeben, dass der Job gestartet

wird. Sie können auf den Link klicken, um den Job zu überwachen.

2. Klicken Sie auf die primäre Aufgabe, um die Unteraufgaben und den Status der einzelnen Unteraufgaben anzuzeigen.

# Wiederherstellung von Virtual Machines aus der Cloud

Sie können Virtual Machines aus der Cloud wieder in vCenter vor Ort wiederherstellen. Das Backup wird an genau demselben Ort wiederhergestellt, von wo aus das Backup durchgeführt wurde. Sie können das Backup nicht an einem anderen alternativen Speicherort wiederherstellen. Sie können Virtual Machines aus dem Datastore oder aus der VM-Ansicht wiederherstellen.

> Sie können keine virtuellen Maschinen wiederherstellen, die von mehreren Datenspeichern verteilt sind.

**Was Sie benötigen**

Stellen Sie sicher, dass Sie alle erfüllt haben "Anforderungen" Vor dem Wiederherstellen von virtuellen Maschinen aus der Cloud.

**Schritte**

1. Klicken Sie in BlueXP UI auf **Schutz** > **Sicherung und Wiederherstellung** > **Virtuelle Maschinen** > **SnapCenter Plug-in für VMware vSphere** und wählen Sie das SnapCenter Plug-in für VMware vSphere aus, dessen virtuelle Maschine Sie wiederherstellen möchten.

> Wenn die virtuelle Quellmaschine an einen anderen Speicherort (vMotion) verschoben wird und der Benutzer eine Wiederherstellung dieser virtuellen Maschine aus BlueXP auslöst, wird die Virtual Machine wieder auf dem ursprünglichen Quellspeicherort wiederhergestellt, von dem aus das Backup durchgeführt wurde.

1. So stellen Sie Daten aus dem Datastore wieder her:
   a. Klicken Sie Auf ••• Entsprechend dem Datenspeicher, den Sie wiederherstellen möchten, und klicken Sie auf **Details anzeigen**.
   b. Klicken Sie auf **Wiederherstellen**, die der Sicherungskopie entsprechen, die Sie wiederherstellen möchten.
   c. Wählen Sie die virtuelle Maschine aus, die Sie aus dem Backup wiederherstellen möchten, und klicken Sie auf **Weiter**.
   d. Überprüfen Sie die Details und klicken Sie auf **Wiederherstellen**.
2. So stellen Sie Daten von virtuellen Maschinen wieder her:
   a. Klicken Sie Auf ••• Entsprechend der virtuellen Maschine, die Sie wiederherstellen möchten, und klicken Sie auf **Wiederherstellen**.
   b. Wählen Sie das Backup aus, über das Sie die virtuelle Maschine wiederherstellen möchten, und klicken Sie auf **Weiter**.
   c. Überprüfen Sie die Details und klicken Sie auf **Wiederherstellen**.

Die VM wird an demselben Ort wiederhergestellt, von dem das Backup durchgeführt wurde.

# Cloud-Backup-APIs

Die Cloud Backup-Funktionen, die über die Web-Oberfläche verfügbar sind, sind auch über die RESTful API verfügbar.

Im Cloud Backup Service sind acht Kategorien von Endpunkten definiert:

- Backup
- Katalog
- Cloud
- Job
- Lizenz
- Wiederherstellen
- Single File-Level Restore (SFR)
- Arbeitsumgebung

## Erste Schritte

Für den Einstieg in die Cloud Backup APIs benötigen Sie ein Benutzer-Token, Ihre Cloud Central Account-ID und die Cloud Connector-ID.

Wenn Sie API-Aufrufe tätigen, fügen Sie das Benutzer-Token in die Autorisierungs-Kopfzeile und die Cloud Connector-ID in die X-Agent-id-Kopfzeile ein. Sie sollten die Cloud Central-Konto-ID in den APIs verwenden.

**Schritte**

1. Holen Sie sich ein Benutzer-Token von NetApp Cloud Central.

   Stellen Sie sicher, dass Sie das Aktualisierungstoken über den folgenden Link generieren: https://services.cloud.netapp.com/refresh-token/. Das Aktualisieren-Token ist eine alphanumerische Zeichenfolge, mit der Sie ein Benutzer-Token generieren.

   ```
   curl --location --request POST 'https://netapp-cloud-
   account.auth0.com/oauth/token?=' \
   --header 'Content-Type: application/json' \
   -d '{
       "grant_type": "refresh_token",
       "refresh_token": "JxaVHn9cGkX92aPVCkhat3zxxxxxwsC9qMl_pLHkZtsVA",
       "client_id": "Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC"
   }'
   ```

   Das Benutzer-Token von NetApp Cloud Central hat ein Ablaufdatum. Die API-Antwort enthält ein Feld "expires_in", das angibt, wann das Token abläuft. Um das Token zu aktualisieren, müssen Sie diese API erneut aufrufen.

2. Beschaffen Ihrer NetApp Cloud Central Account-ID

```
GET 'https://cloudmanager.cloud.netapp.com/tenancy/account' -H
'authority: cloudmanager.cloud.netapp.com'
Header:
-H 'accept: application/json'
-H 'accept-language: en-GB,en;q=0.9'
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR……
```

Diese API gibt eine Antwort wie die folgende zurück. Sie können die Konto-ID abrufen, indem Sie die Ausgabe von **[0].[ buchPublicID]** analysiert haben.

```
[{"accountPublicId":"account-
i6vJXvZW","accountName":"rashidn","isSaas":true,"isGov":false,"isPrivate
PreviewEnabled":false,"is3rdPartyServicesEnabled":false,"accountSerial":
"96064469711530003565","userRole":"Role-1"}……
```

3. Holen Sie sich die x-Agent-id, die die BlueXP Connector-ID enthält.

```
GET curl 'https://api.services.cloud.netapp.com/occm/list-occms/account-
OOnAR4ZS?excludeStandalone=true&source=saas' \
Header:
  -H 'authority: api.services.cloud.netapp.com' \
  -H 'accept: application/json' \
  -H 'accept-language: en-GB,en;q=0.9' \
  -H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5……
```

Diese API gibt eine Antwort wie die folgende zurück. Sie können die Agenten-id abrufen, indem Sie die Ausgabe von **occm.[0].[Agent].[AGENTID]** parsen.

```
{"occms":[{"account":"account-
OOnAR4ZS","accountName":"cbs","occm":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Z",
"agentId":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Z","status":"ready","occmName"
:"cbsgcpdevcntsg-
asia","primaryCallbackUri":"http://34.93.197.21","manualOverrideUris":[]
,"automaticCallbackUris":["http://34.93.197.21","http://34.93.197.21/occ
mui","https://34.93.197.21","https://34.93.197.21/occmui","http://10.138
.0.16","http://10.138.0.16/occmui","https://10.138.0.16","https://10.138
.0.16/occmui","http://localhost","http://localhost/occmui","http://local
host:1337","http://localhost:1337/occmui","https://localhost","https://l
ocalhost/occmui","https://localhost:1337","https://localhost:1337/occmui
"],"createDate":"1652120369286","agent":{"useDockerInfra":true,"network"
:"default","name":"cbsgcpdevcntsg-
asia","agentId":"imEdsEW4HyYTFbt8ZcNKTKDF05jMIe6Zclients","provider":"gc
p","systemId":"a3aa3578-bfee-4d16-9e10-
```


# Beispiel mit den APIs

Das folgende Beispiel zeigt einen API-Aufruf zur Aktivierung des Backups in der Arbeitsumgebung mit einer neuen Richtlinie, in der Tages-, Stunden- und Wochenbeschriftungen nach 180 Tagen festgelegt und archiviert werden, in Ost-US-2-Regionen in der Azure-Cloud. Bitte beachten Sie, dass dies eine Datensicherung nur auf der Arbeitsumgebung ermöglicht, aber keine Volumes gesichert werden. Wenn Sie „Auto-Backup-Enabled“ wählen: „True“, dann würden bereits im System vorhandene Volumes gesichert, plus künftige Volumes hinzugefügt.

#### API-Anfrage

Wie Sie sehen, wird die Konto-ID von Cloud Central verwendet `account-DpTFcxN3`, BlueXP Connector-ID `iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients`Und Benutzer-Token `Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwkeMwHc4ValobjUmju2x0xUH48g` In diesem Befehl.

```
curl --location --request POST
'https://cloudmanager.cloud.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v3/backup/working-
environment/VsaWorkingEnvironment-99hPYEgk' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…y6nyhBjwk
eMwHc4ValobjUmju2x0xUH48g' \
--data-raw '{
    "provider":"AZURE",
    "backup-policy": {
      "archive-after-days": 180,
      "rule": [
        {
          "label": "hourly",
          "retention": "2"
        },
        {
          "label": "daily",
          "retention": "30"
        },
        {
          "label": "weekly",
          "retention": "52"
        }
      ]
    },
    "ip-space": "Default",
    "region": "eastus2",
    "azure": {
      "resource-group": "rn-test-backup-rg",
      "subscription": "3beb4dd0-25d4-464f-9bb0-303d7cf5c0c2"
    }
  }'
```

**Die Antwort ist eine Job-ID, die Sie dann überwachen können.**

```
{
    "job-id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a"
}
```

**Überwachen Sie die Antwort.**

```
curl --location --request GET
'https://cloudmanager.cloud.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v1/job/1b34b6f6-8f43-40fb-9a52-
485b0dfe893a' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik5rSXlPVFUzUWpZek1E…hE9ss2Nub
K6wZRHUdSaORI7JvcOorUhJ8srqdiUiW6MvuGIFAQIh668of2M3dLbhVDBe8BBMtsa939UGnJx
7Qz6Eg'
```

**Antwort:**

```
{
    "job": [
        {
            "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
            "type": "backup-working-environment",
            "status": "PENDING",
            "error": "",
            "time": 1651852160000
        }
    ]
}
```

**Überwachen Sie, bis „Status“ ABGESCHLOSSEN ist.**

```
{
    "job": [
        {
            "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
            "type": "backup-working-environment",
            "status": "COMPLETED",
            "error": "",
            "time": 1651852160000
        }
    ]
}
```

# API-Referenz

Für jede Cloud-Backup-API steht eine Dokumentation zur Verfügung https://docs.netapp.com/us-en/cloud-

manager-automation/cbs/overview.html.

# Referenz

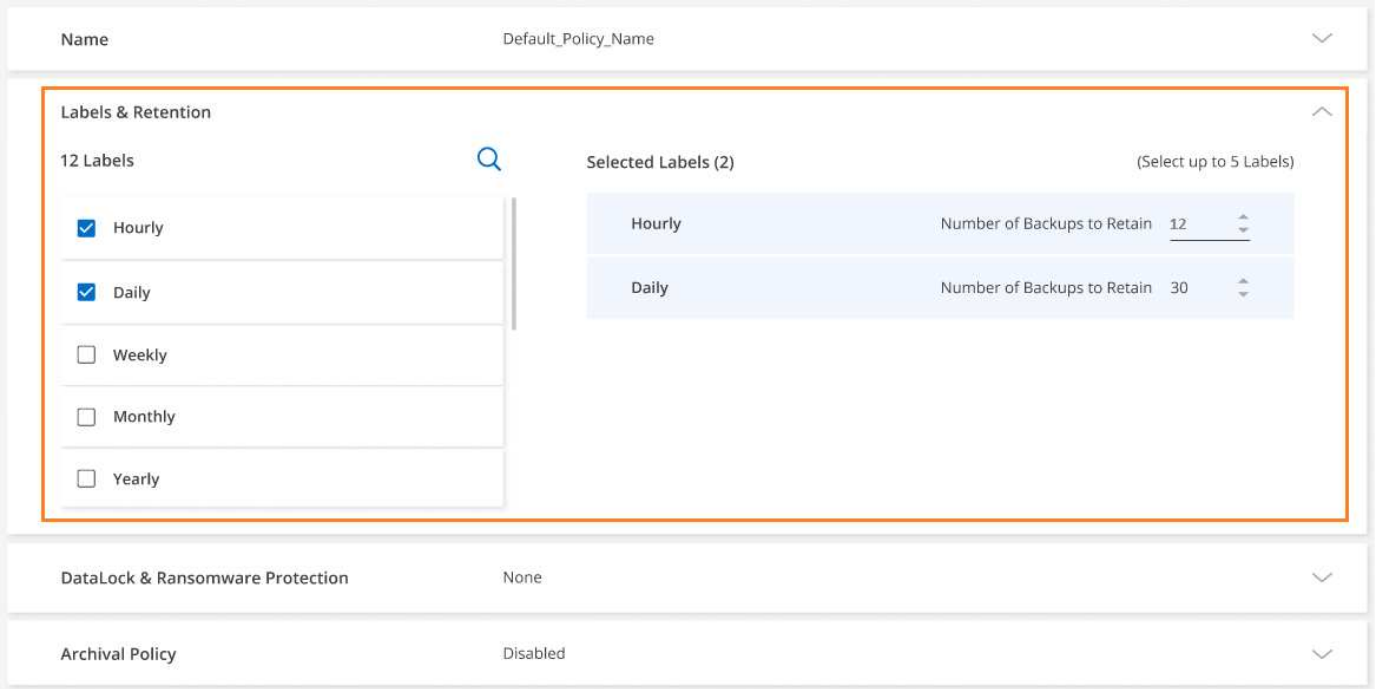
## Konfigurationseinstellungen für Cloud-Backup-Richtlinien

Dieses Dokument beschreibt die Konfigurationseinstellungen für die Backup-Richtlinie für On-Premises-ONTAP-Systeme und Cloud Volumes ONTAP-Systeme bei Verwendung des Cloud Backup Service.

### Backup-Pläne

Mit Cloud Backup können Sie mehrere Backup-Richtlinien mit individuellen 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.




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-Schutz

Cloud Backup unterstützt DataLock und Ransomware-Schutz für Ihre Volume-Backups. Dank dieser Funktionen können Sie Ihre Backup-Dateien sperren und scannen, um mögliche Ransomware auf 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 dieser Funktionen schützen Ihre Backup-Dateien, damit stets eine gültige Backup-Datei zur Wiederherstellung von Daten im Falle eines Ransomware-Angriffs auf Ihre Quelldaten zur Verfügung steht. Darüber hinaus hilft es bei der Einhaltung bestimmter gesetzlicher Vorgaben, bei denen Backups für einen bestimmten Zeitraum gesperrt und aufbewahrt werden müssen. Bei aktiviertem DataLock und Ransomware-Schutz sind in dem Cloud-Bucket, der im Rahmen der Cloud Backup-Aktivierung bereitgestellt wird, Objektsperren und Objektversionierung aktiviert.

Diese Funktion bietet keinen Schutz für Ihre Quell-Volumes, sondern nur für die Backups dieser Quell-Volumes. Mit NetApp "Cloud Insights und Cloud Secure", Oder einige der "Ransomware-Schutz durch ONTAP" Um Ihre Quell-Volumes zu schützen.

- Wenn Sie Vorhaben, DataLock- und Ransomware-Schutz zu verwenden, müssen Sie es beim Erstellen der ersten Backup-Richtlinie aktivieren und Cloud Backup für diesen Cluster aktivieren.
- DataLock- und Ransomware-Schutz kann nach der Konfiguration für einen Cluster nicht deaktiviert werden. Aktivieren Sie diese Funktion nicht auf einem Cluster, um sie auszuprobieren.

### Was ist DataLock

DataLock schützt Ihre Backup-Dateien vor einer bestimmten Zeit zu ändern oder zu löschen. Bei dieser Funktionalität kommt Technologie des Objekt-Storage-Anbieters zum Einsatz, um Objekte zu sperren. Der Zeitraum, in dem die Sicherungsdatei gesperrt (und aufbewahrt) ist, wird als Aufbewahrungszeitraum für DataLock bezeichnet. Er basiert auf dem von Ihnen definierten Backup-Richtlinienplan und der Aufbewahrungseinstellung sowie einem Puffer von 14 Tagen. Jede DataLock-Aufbewahrungsrichtlinie, die weniger als 30 Tage beträgt, wird auf mindestens 30 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 Aufbewahrung erstellen, ist jedes Backup für 12 Monate (plus 14 Tage) 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 44 Tage (30 Tage plus 14 Tage Puffer), die „7 wöchentlichen“ Backups würden 9 Wochen (7 Wochen plus 14 Tage) aufbewahrt und die „12 monatlichen“ Backups würden 12 Monate (plus 14 Tage) aufbewahrt.
- 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 für 44 Tage gesperrt und aufbewahrt (30 Tage plus 14 Tage Puffer).

  Sie können in diesem letzten Fall sehen, dass, wenn jede Backup-Datei für 44 Tage gesperrt ist, Sie am Ende mit vielen mehr Backup-Dateien stehen, als normalerweise mit einer stündlichen/24-Aufbewahrungs-Richtlinie aufbewahrt werden würde. In der Regel, wenn Cloud Backup die 25. Backup-Datei erstellt, würde es das älteste Backup löschen, um die maximalen Aufbewahrung 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. Falls in einer Backup-Datei potenzielle Ransomware im Vergleich zur vorherigen Backup-Datei identifiziert wird, 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 erfolgen an 3 Punkten im Backup- und Restore-Prozess:

- Beim Erstellen einer Sicherungsdatei

  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.

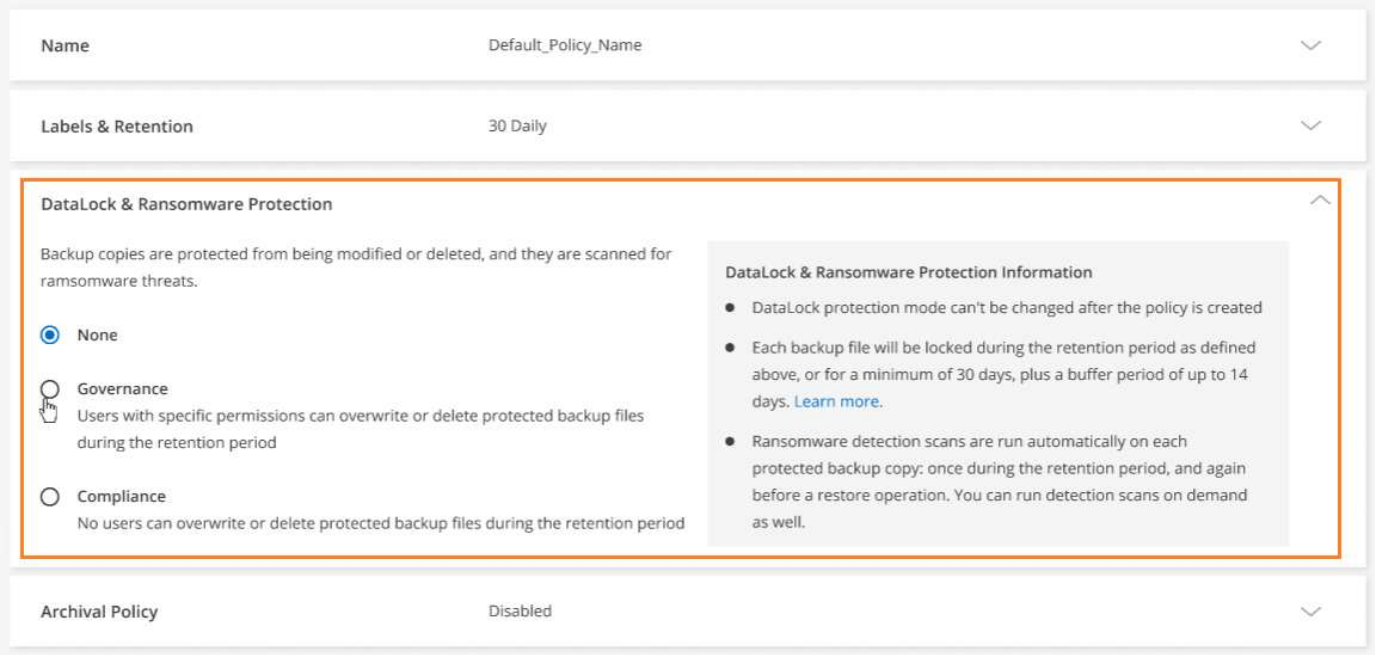
- Manuell

  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.

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

### Einstellungen für DataLock und Ransomware-Schutz

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




Für jede Backup-Richtlinie stehen folgende Einstellungen zur Verfügung:

- Keine (Standard)

  DataLock-Schutz und Ransomware-Schutz sind deaktiviert.

- Governance (nicht verfügbar mit StorageGRID)

  DataLock ist auf *Governance*-Modus gesetzt, in dem Benutzer mit bestimmten Berechtigungen ("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.

Die StorageGRID S3-Objektsperre bietet einen einzelnen DataLock-Modus, der dem Compliance-Modus entspricht. Ein gleichwertiger Governance-Modus wird nicht unterstützt, sodass keine Benutzer die Möglichkeit haben, Aufbewahrungseinstellungen zu umgehen, geschützte Backups zu überschreiben oder gesperrte Backups zu löschen.

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

#### Anforderungen

- Ihre Cluster müssen ONTAP 9.11.1 oder höher ausführen
- Sie müssen BlueXP 3.9.21 oder höher verwenden
- Für StorageGRID:
  - Der Connector muss auf Ihrem Gelände bereitgestellt werden (er kann auf einer Website mit oder ohne Internetzugang installiert werden).
  - Für die vollständige Unterstützung von DataLock-Funktionen ist StorageGRID 11.6.0.3 und höher erforderlich

#### Einschränkungen

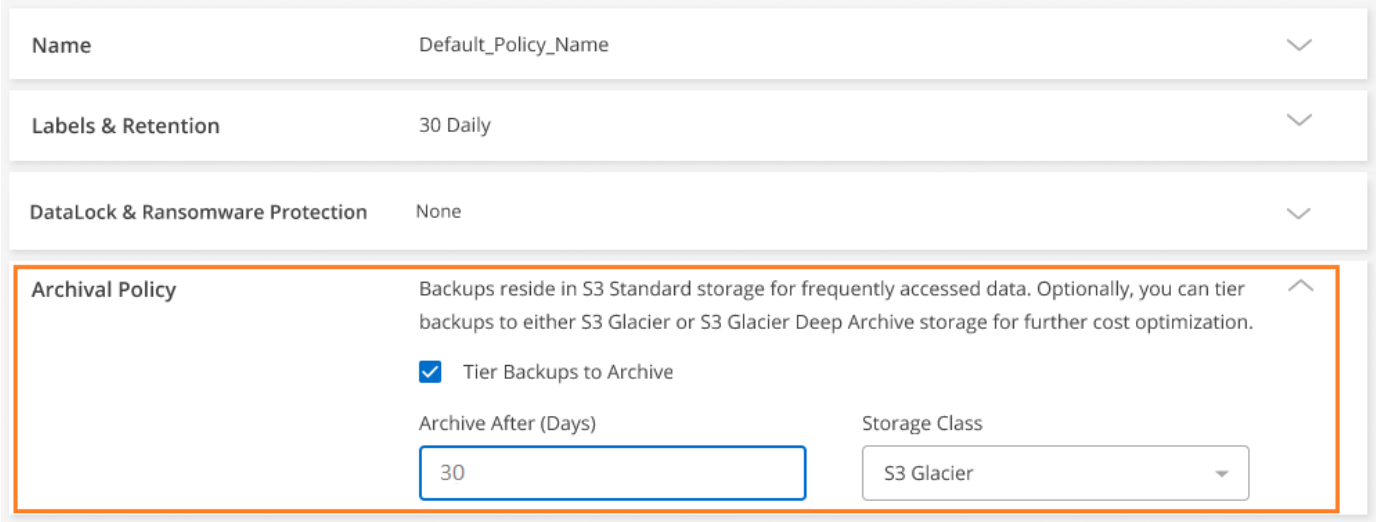
- DataLock- und Ransomware-Schutz ist nicht verfügbar, wenn Sie Archiv-Storage in der Backup-Richtlinie konfiguriert haben.
- Die bei der Aktivierung von Cloud Backup (entweder Governance oder Compliance) ausgewählte DataLock-Option muss für alle Backup-Richtlinien für diesen Cluster verwendet werden. Sie können die Sperrung des Governance- und Compliance-Modus nicht 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 Funktion nicht aktivieren, nachdem Cloud Backup aktiviert wurde.

## Einstellungen für Archiv-Storage

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

Auf Daten in Archivebenen kann nicht unmittelbar bei Bedarf zugegriffen werden und sind mit höheren Abrufkosten verbunden. Daher müssen Sie berücksichtigen, wie oft Sie Daten aus archivierten Backup-Dateien wiederherstellen müssen.

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




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

  Wenn Ihr On-Prem-Cluster ONTAP 9.12.1 oder höher verwendet, können Sie nach einer bestimmten Anzahl von Tagen ältere Backups als *Archive* Storage in der Cloud Backup UI verschieben, um die Kosten weiter zu optimieren. (Diese Funktion ist derzeit für Cloud Volumes ONTAP Systeme nicht verfügbar.) "Erfahren Sie mehr über Google Archivspeicher".

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

  Derzeit ist kein Archiv-Tier verfügbar.

# AWS S3-Archiv-Storage-Klassen und Restore Abrufzeiten

Cloud Backup unterstützt zwei S3-Archiv-Storage-Klassen und die meisten Regionen.

## Unterstützte S3-Archiv-Storage-Klassen für Cloud Backup

Beim ersten Erstellen von Backup-Dateien werden sie im S3 *Standard* Storage gespeichert. Diese Tier ist für die Speicherung von Daten optimiert, auf die selten zugegriffen wird. Dadurch können Sie jedoch auch sofort auf die Daten zugreifen. Nach 30 Tagen erfolgen die Backups auf die S3 *Standard-infrequent Access* Storage-Klasse, um Kosten zu sparen.

Wenn in den Quellclustern ONTAP 9.10.1 oder neuer ausgeführt wird, können Sie Backups entweder nach einer bestimmten Anzahl von Tagen (normalerweise über 30 Tage) als Tiering zu *S3 Glacier Deep Archive* oder *S3 Glacier Deep Archive* Storage abstufen, um die Kosten weiter zu optimieren. Auf Daten in diesen Tiers kann bei Bedarf nicht sofort zugegriffen werden und verursachen höhere Abrufkosten. Daher müssen Sie bedenken, wie oft Sie Daten aus diesen archivierten Backup-Dateien wiederherstellen müssen. Siehe Abschnitt zu Wiederherstellen von Daten aus Archiv-Storage.

Wenn Sie bei der Aktivierung von Cloud Backup *S3 Glacier* oder *S3 Glacier Deep Archive* in Ihrer ersten Backup-Richtlinie auswählen, wird dieser Tier die einzige Archiv-Tier sein, die für zukünftige Backup-Richtlinien für diesen Cluster verfügbar ist. Falls Sie in Ihrer ersten Backup-Richtlinie keinen Archiv-Tier auswählen, ist *S3 Glacier* die einzige Archivoption für zukünftige Richtlinien.

Wenn Sie Cloud Backup mit dieser Art von Lifecycle-Regel konfigurieren, müssen Sie beim Einrichten des Bucket in Ihrem AWS-Konto keine Lifecycle-Regeln konfigurieren.

"Erfahren Sie mehr über S3-Storage-Klassen".

### Wiederherstellen von Daten aus Archiv-Storage

Das Speichern älterer Backup-Dateien im Archiv-Storage ist viel kostengünstiger als Standard- oder Standard-IA-Storage. Der Zugriff auf Daten aus einer Backup-Datei im Archiv-Storage für Wiederherstellungsvorgänge dauert viel länger und kostet mehr Geld.

**Wie hoch sind die Kosten für die Wiederherstellung von Daten aus Amazon S3 Glacier und Amazon S3 Glacier Deep Archive?**

Es gibt 3 Wiederherstellungsprioritäten, die beim Abrufen von Daten aus Amazon S3 Glacier und beim Abrufen der Daten aus dem Amazon S3 Glacier Deep Archive zwei Wiederherstellungsprioritäten zur Verfügung stehen. S3 Glacier Deep Archive kostet weniger als S3 Glacier:

| Archivebene | Priorität Und Kosten Wiederherstellen | | |
|---|---|---|---|
| | **Hoch** | **Standard** | **Niedrig** |
| **S3-Gletscher** | Schnellster Abruf, höchste Kosten | Langsameres Abrufen, geringere Kosten | Langsamster Abruf, niedrigste Kosten |
| **S3 Glacier Deep Archive** | | Schnelleres Abrufen, höhere Kosten | Langsameres Abrufen, geringste Kosten |

Jede Methode hat eine andere Abrufgebühr pro GB und eine andere Gebühr pro Anfrage. Detaillierte Informationen zu den S3-Glacier-Preisen nach AWS Region finden Sie im "Preisseite von Amazon S3".

**Wie lange dauert es, meine in Amazon S3 Glacier archivierten Objekte wiederherzustellen?**

Es gibt zwei Teile, aus denen sich die gesamte Wiederherstellungszeit ergibt:

- **Retrieval Time**: Der Zeitpunkt, um die Sicherungsdatei aus dem Archiv abzurufen und in den Standard-Speicher zu legen. Dies wird manchmal als die "Rehydrierung" Zeit bezeichnet. Die Abrufzeit ist je nach gewählter Wiederherstellungspriorität unterschiedlich.

| Archivebene | Stellen Sie Die Priorität Und Den Abruf Wieder Her | | |
|---|---|---|---|
| | **Hoch** | **Standard** | **Niedrig** |
| **S3-Gletscher** | 3-5 Minuten | 3-5 Stunden | 5-12 Stunden |
| **S3 Glacier Deep Archive** | | 12 Stunden | 48 Stunden |

- **Restore Time**: Der Zeitpunkt, um die Daten aus der Sicherungsdatei im Standard-Speicher wiederherzustellen. Dieser Vorgang unterscheidet sich nicht von dem typischen Restore-Vorgang direkt vom Standard-Storage, wenn keine Archivebene verwendet wird.

Weitere Informationen zu den Abruffoptionen für Amazon S3 Glacier und S3 Glacier Deep Archive finden Sie unter "Die Amazon FAQ zu diesen Speicherklassen".

# Azure-Archivierungsebenen und Wiederherstellungszeiten

Cloud Backup unterstützt eine Azure-ArchivierungszugriffTier und die meisten Regionen.

## Unterstützte Azure Blob-Zugriffsebenen für Cloud Backup

Beim ersten Erstellen von Sicherungsdateien werden sie in der Zugriffsebene *Cool* gespeichert. Diese Tier ist für die Speicherung von Daten optimiert, auf die selten zugegriffen wird. Bei Bedarf kann jedoch sofort zugegriffen werden.

Wenn in Ihren Quellclustern ONTAP 9.10.1 oder neuer ausgeführt wird, können Sie zur weiteren Kostenoptimierung Backups von *Cool* zu *Azure Archive* Storage nach einer bestimmten Anzahl von Tagen (normalerweise über 30 Tage) abstufen. Auf die Daten in dieser Tier kann nicht unmittelbar bei Bedarf zugegriffen werden und sind mit höheren Abrufkosten verbunden. Daher müssen Sie bedenken, wie oft Sie Daten aus diesen archivierten Backup-Dateien wiederherstellen müssen. Weitere Informationen finden Sie im nächsten Abschnitt Wiederherstellen von Daten aus Archiv-Storage.

Beachten Sie, dass Sie beim Konfigurieren von Cloud Backup mit dieser Lebenszyklusregel keine Lebenszyklusregeln konfigurieren müssen, wenn Sie den Container in Ihrem Azure-Konto einrichten.

"Erfahren Sie mehr über Azure Blob Zugriffsebenen".

## Wiederherstellen von Daten aus Archiv-Storage

Das Speichern älterer Backup-Dateien im Archiv-Storage ist viel günstiger als Cool Storage. Der Zugriff auf Daten aus einer Backup-Datei im Azure Archiv für Restore-Vorgänge dauert etwas länger und kostet mehr Geld.

**Wie viel kostet die Wiederherstellung von Daten aus dem Azure-Archiv?**

Beim Abrufen von Daten aus dem Azure Archiv stehen zwei Wiederherstellungsprioritäten zur Verfügung:

- **Hoch**: Schnellster Abruf, höhere Kosten
- **Standard**: Langsamer Abruf, niedrigere Kosten

Jede Methode hat eine andere Abrufgebühr pro GB und eine andere Gebühr pro Anfrage. Detaillierte Informationen zu den Azure Archivpreisen nach Azure Region finden Sie im "Azure-Preisseite".

**Wie lange wird es dauern, bis meine im Azure-Archiv archivierten Daten wiederhergestellt sind?**

Die Wiederherstellungszeit besteht aus zwei Teilen:

- **Retrieval Time**: Der Zeitpunkt, um die archivierte Backup-Datei aus dem Azure Archiv abzurufen und in Cool Storage zu platzieren. Dies wird manchmal als die "Rehydrierung" Zeit bezeichnet. Die Abrufzeit ist je nach gewählter Wiederherstellungspriorität unterschiedlich:
  - **Hoch**: < 1 Stunde
  - **Standard**: < 15 Stunden
- **Restore Time**: Der Zeitpunkt, um die Daten aus der Sicherungsdatei in Cool Storage wiederherzustellen. Diese Zeit unterscheidet sich nicht von dem typischen Restore-Vorgang direkt von Cool Storage, wenn kein Archivtier verwendet wird.

Weitere Informationen zu Abruffoptionen für Azure Archive finden Sie unter "Diese Azure FAQ".

# Google Archivspeicherklassen und Abrufzeiten wiederherstellen

Cloud Backup unterstützt eine Google-Archiv-Storage-Klasse und in den meisten

Regionen.

### Unterstützte Google-Archivierungs-Storageklassen für Cloud-Backup

Beim ersten Erstellen von Backup-Dateien werden sie im *Standard* Storage gespeichert. Diese Tier ist für die Speicherung von Daten optimiert, auf die selten zugegriffen wird. Dadurch können Sie jedoch auch sofort auf die Daten zugreifen.

Wenn Ihr On-Prem-Cluster ONTAP 9.12.1 oder höher verwendet, können Sie ältere Backups nach einer bestimmten Anzahl von Tagen (normalerweise über 30 Tage) in der Cloud-Backup-UI auf *Archive* Storage abstufen, um die Kosten weiter zu optimieren. (Diese Funktion ist derzeit für Cloud Volumes ONTAP Systeme nicht verfügbar.) Für Daten in dieser Tier fallen höhere Abrufkosten an. Daher müssen Sie bedenken, wie oft Sie Daten aus diesen archivierten Backup-Dateien wiederherstellen müssen. Siehe Abschnitt zu Wiederherstellen von Daten aus Archiv-Storage.

Wenn Sie Cloud Backup mit dieser Lebenszyklusregel konfigurieren, dürfen Sie beim Einrichten des Buckets in Ihrem Google-Konto keine Lebenszyklusregeln konfigurieren.

"Erfahren Sie mehr über Google Speicherklassen".

### Wiederherstellen von Daten aus Archiv-Storage

Das Speichern älterer Backup-Dateien im Archiv-Storage ist viel kostengünstiger als Standard-Storage. Der Zugriff auf Daten von einer Backup-Datei im Archiv-Storage für Wiederherstellungsvorgänge dauert etwas länger und kostet mehr Geld.

**Wie viel kostet es, Daten aus dem Google-Archiv wiederherzustellen?**

Detaillierte Google Cloud Storage Preise nach Region finden Sie im "Preise für Google Cloud Storage".

**Wie lange dauert es, meine im Google-Archiv archivierten Objekte wiederherzustellen?**

Es gibt zwei Teile, aus denen sich die gesamte Wiederherstellungszeit ergibt:

- **Retrieval Time**: Der Zeitpunkt, um die Sicherungsdatei aus dem Archiv abzurufen und in den Standard-Speicher zu legen. Dies wird manchmal als die "Rehydrierung" Zeit bezeichnet. Im Gegensatz zu den am seltensten benötigten Storage-Lösungen anderer Cloud-Provider sind Ihre Daten innerhalb von Millisekunden verfügbar.
- **Restore Time**: Der Zeitpunkt, um die Daten aus der Sicherungsdatei im Standard-Speicher wiederherzustellen. Dieser Vorgang unterscheidet sich nicht von dem typischen Restore-Vorgang direkt vom Standard-Storage, wenn keine Archivebene verwendet wird.

# Backup für Multi-Account-Zugriff in Azure konfigurieren

Cloud Backup ermöglicht die Erstellung von Backup-Dateien in einem Azure Konto, das sich von dem der Quell-Cloud Volumes ONTAP Volumes unterscheidet. Und beide Konten können sich von dem Konto unterscheiden, in dem sich der BlueXP Connector befindet.

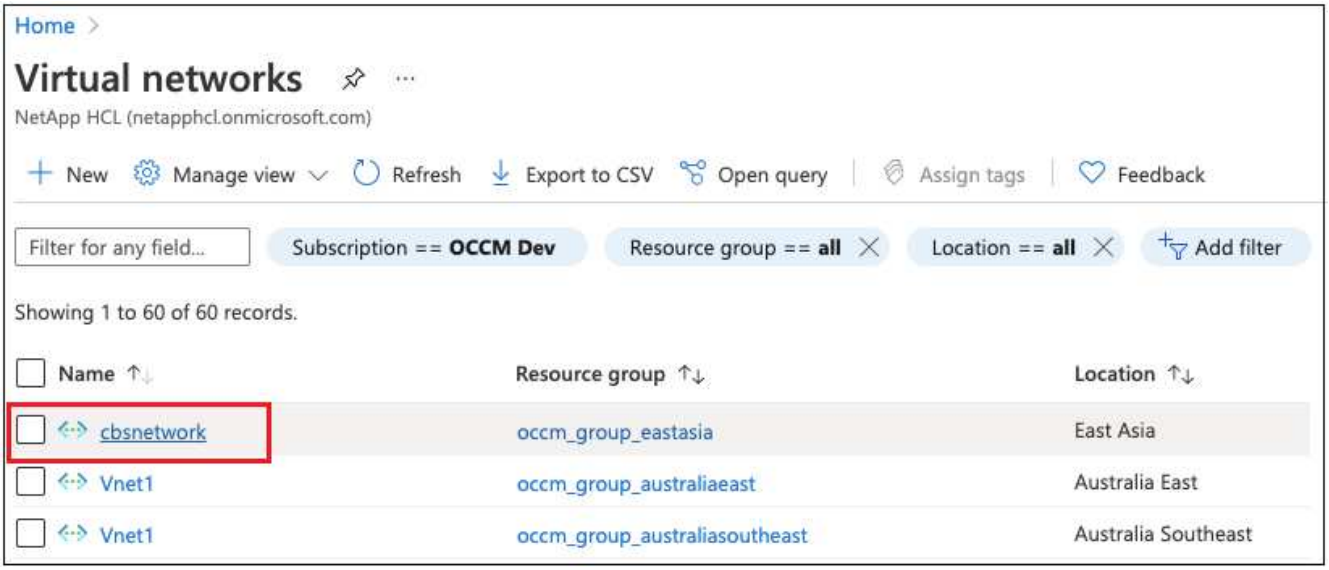
Diese Schritte sind nur erforderlich, wenn Sie sich befinden "Sichern von Cloud Volumes ONTAP-Daten auf Azure Blob Storage".

Befolgen Sie einfach die nachstehenden Schritte, um Ihre Konfiguration auf diese Weise einzurichten.

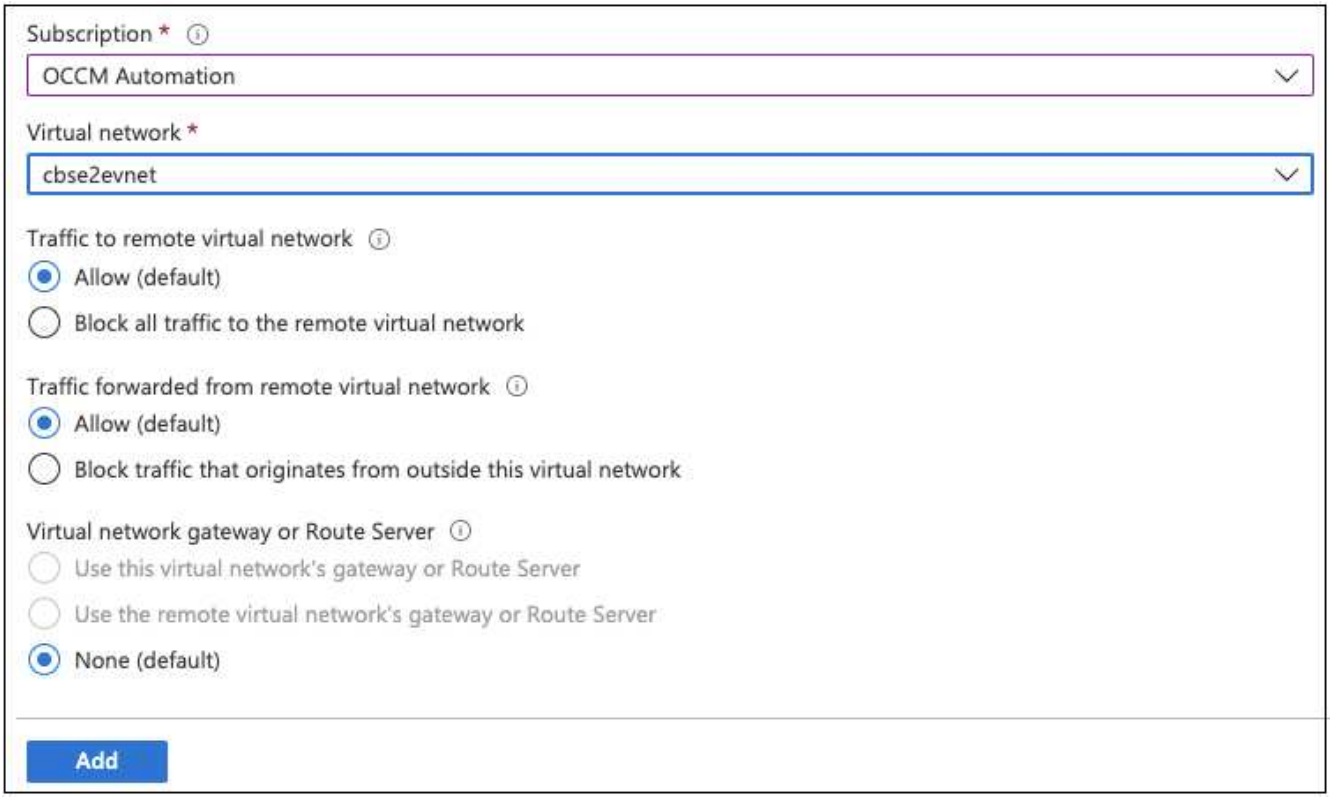
## Vnet-Peering zwischen Konten einrichten

Wenn Sie möchten, dass BlueXP Ihr Cloud Volumes ONTAP-System in einem anderen Konto/einer anderen Region verwaltet, müssen Sie vnet Peering einrichten. Vnet-Peering ist für die Konnektivität des Storage-Kontos nicht erforderlich.

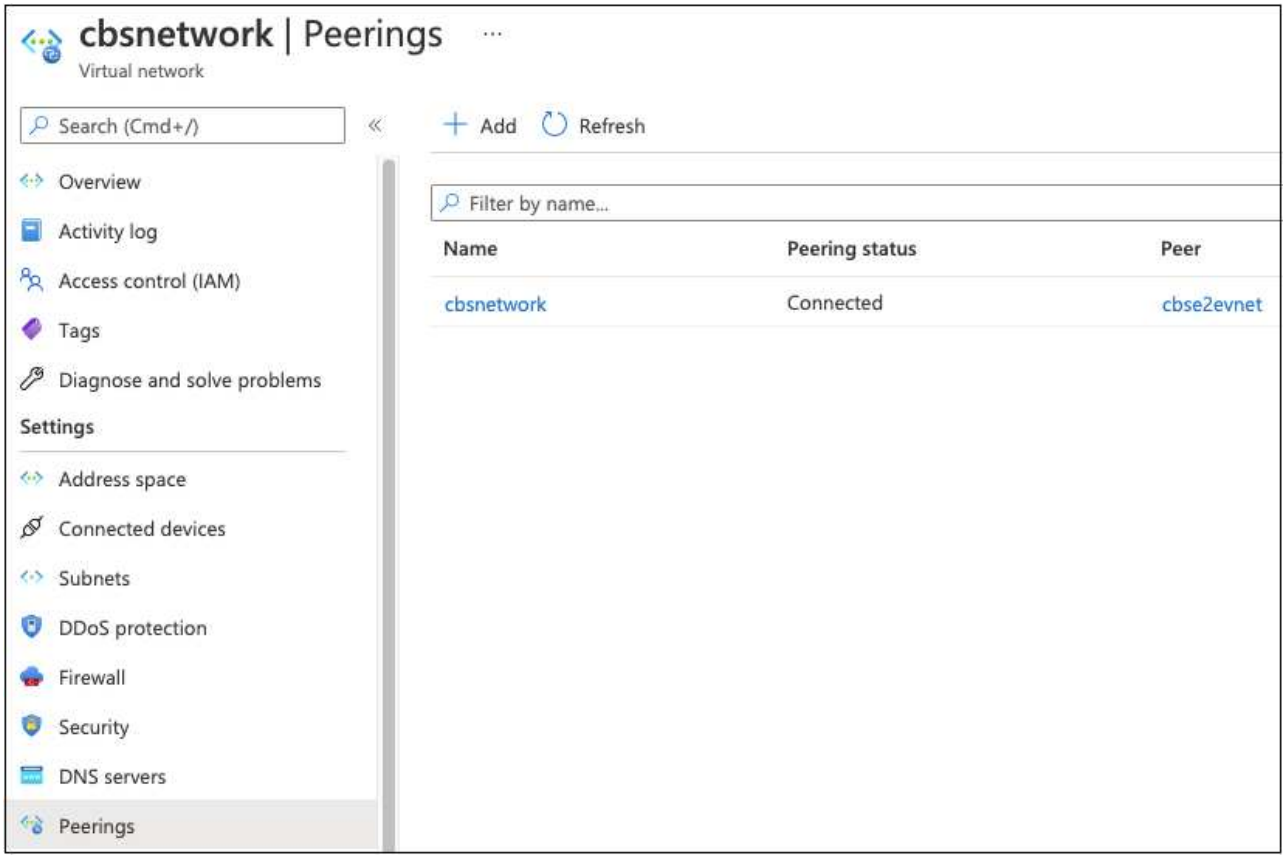
1. Melden Sie sich beim Azure-Portal an, und wählen Sie dann von Zuhause aus Virtual Networks aus.
2. Wählen Sie das Abonnement aus, das Sie als Abonnement verwenden 1, und klicken Sie auf das vnet, wo Sie Peering einrichten möchten.




3. Wählen Sie **cbsnetzwerk** und klicken Sie im linken Bereich auf **Peerings** und dann auf **Add**.



4. Geben Sie die folgenden Informationen auf der Peering-Seite ein und klicken Sie dann auf **Hinzufügen**.
    - Peering-Linkname für dieses Netzwerk: Sie können einen beliebigen Namen angeben, um die Peering-Verbindung zu identifizieren.
    - Remote Virtual Network Peering Linkname: Geben Sie einen Namen ein, um das Remote vnet zu identifizieren.
    - Behalten Sie alle Auswahlen als Standardwerte bei.
    - Wählen Sie unter Abonnement das Abonnement 2 aus.
    - Virtuelles Netzwerk, wählen Sie das virtuelle Netzwerk in Abo 2 aus, zu dem Sie das Peering einrichten möchten.




5. Führen Sie die gleichen Schritte in Subskription 2 vnet aus und geben Sie die Abonnement- und Remote vnet-Details von Abo 1 an.

Subscription *
OCCM Dev

Virtual network *
cbsnetwork

Traffic to remote virtual network
- (•) Allow (default)
- ( ) Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network
- (•) Allow (default)
- ( ) Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server
- ( ) Use this virtual network's gateway or Route Server
- ( ) Use the remote virtual network's gateway or Route Server
- (•) None (default)

Add

Die Peering-Einstellungen werden hinzugefügt.

cbse2evnet | Peerings
Virtual network

Search (Cmd+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

Settings

Address space
Connected devices
Subnets
DDoS protection
Firewall
Security
DNS servers
Peerings

Add Refresh

Filter by name...

| Name | Peering status | Peer |
|---|---|---|
| cbsnetworkpeer | Connected | cbsnetwork |

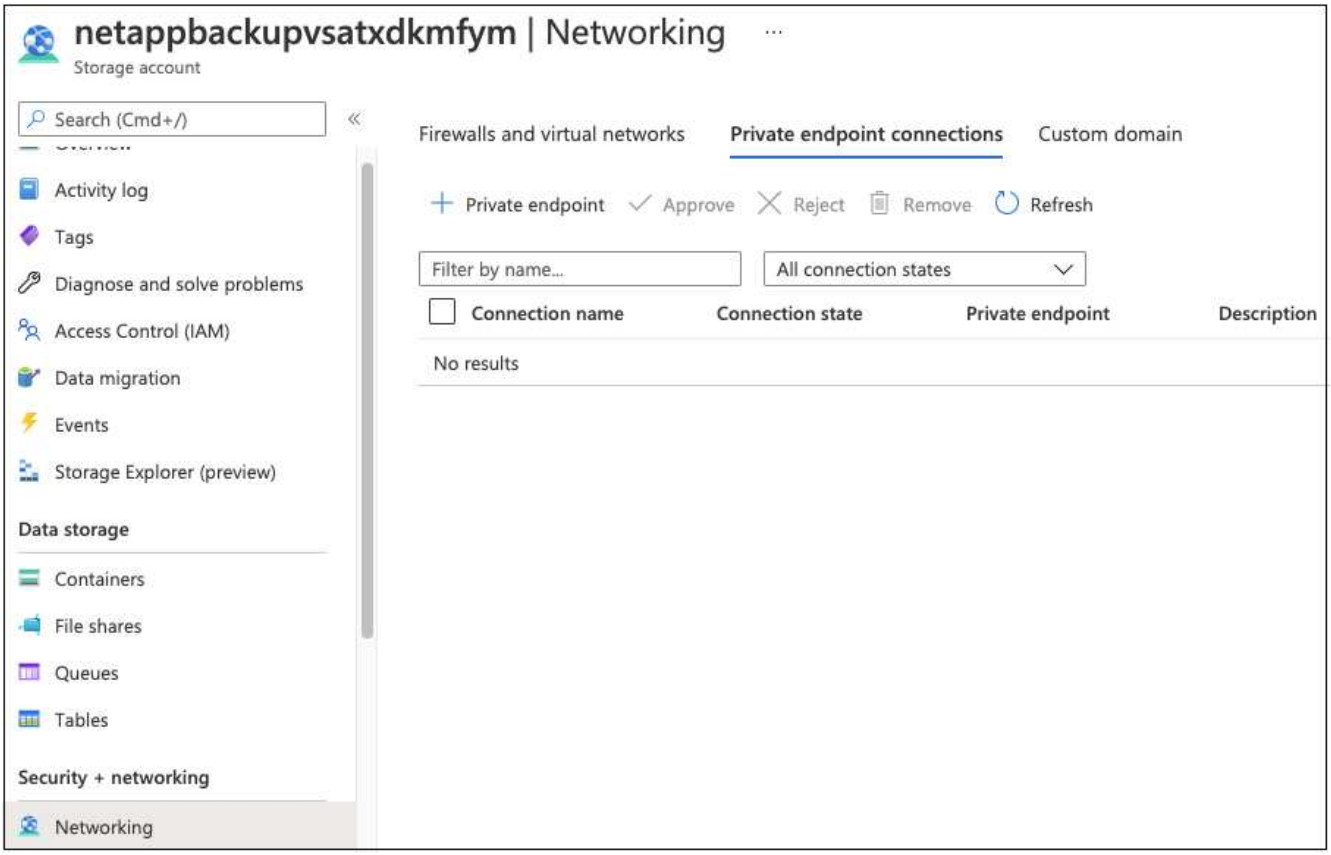
## Erstellen eines privaten Endpunkts für das Storage-Konto

Jetzt müssen Sie einen privaten Endpunkt für das Storage-Konto erstellen. In diesem Beispiel wird das Speicherkonto in Abo 1 erstellt und das Cloud Volumes ONTAP System wird in Abonnement 2 ausgeführt.

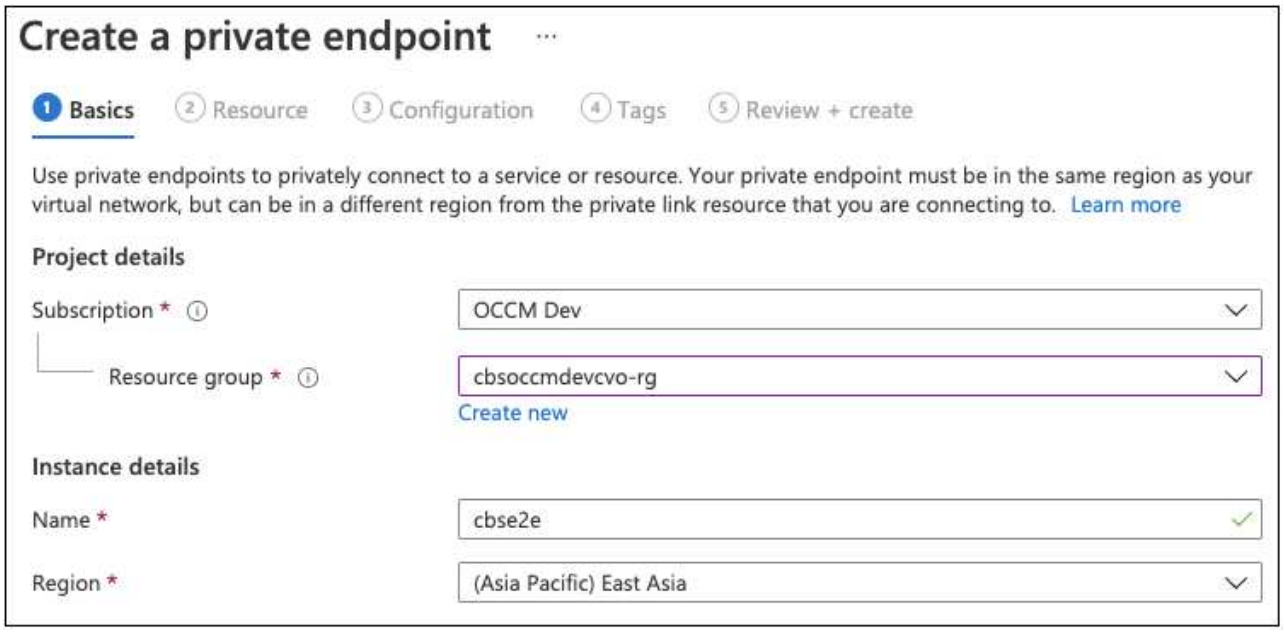
> Sie benötigen die Berechtigung von Netzwerkbeitragenden, um die folgende Aktion auszuführen.

```
{
  "id": "/subscriptions/d333af45-0d07-4154-
943dc25fbbce1b18/providers/Microsoft.Authorization/roleDefinitions/4d97b98
b-1d4f-4787-a291-c67834d212e7",
  "properties": {
    "roleName": "Network Contributor",
    "description": "Lets you manage networks, but not access to them.",
    "assignableScopes": [
      "/"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/*/read",
          "Microsoft.Insights/alertRules/*",
          "Microsoft.Network/*",
          "Microsoft.ResourceHealth/availabilityStatuses/read",
          "Microsoft.Resources/deployments/*",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Support/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

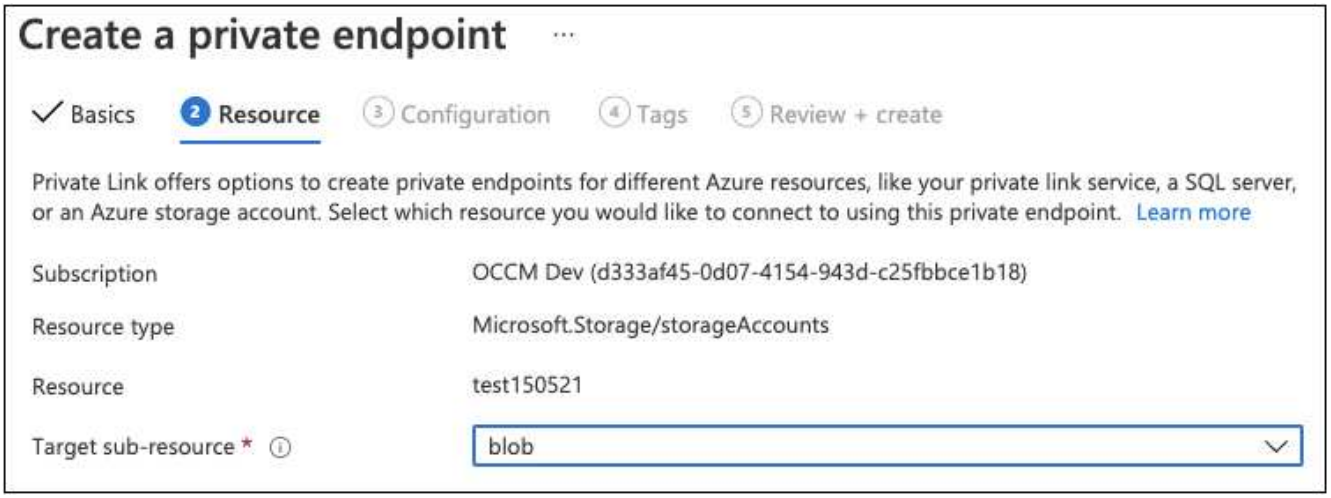
1. Wechseln Sie zum Storage-Konto > Networking > Verbindungen zu privaten Endpunkten und klicken Sie auf **+ Private Endpunkt**.



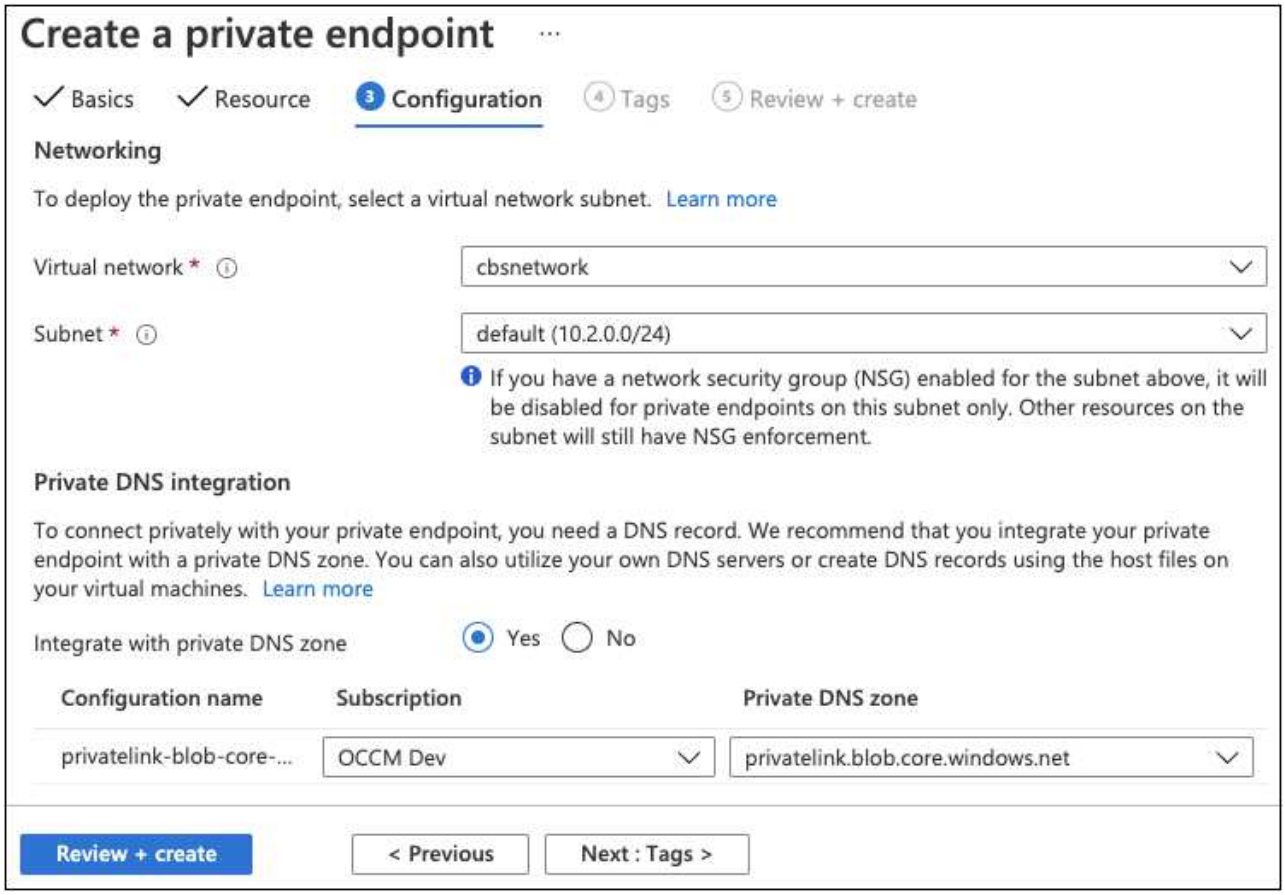

2. Auf der Seite Private Endpoint_Basics_:
   - Wählen Sie Subskription 2 (wo BlueXP Connector und Cloud Volumes ONTAP System bereitgestellt werden) und die Ressourcengruppe aus.
   - Geben Sie einen Endpunktnamen ein.
   - Wählen Sie die Region aus.



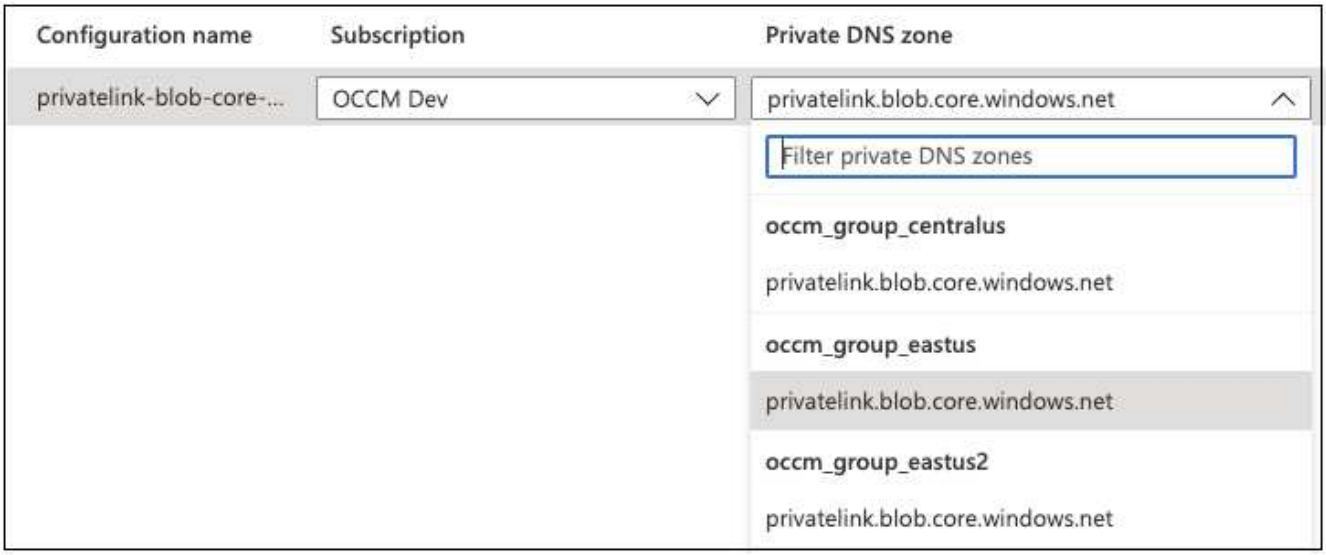

3. Wählen Sie auf der Seite *Ressource* die Unterressource Ziel als **Blob** aus.




4. Auf der Konfigurationsseite:
   - Wählen Sie das virtuelle Netzwerk und das Subnetz aus.
   - Klicken Sie auf das Optionsfeld **Ja**, um "in private DNS-Zone integrieren".




5. Stellen Sie in der Liste Private DNS Zone sicher, dass die Private Zone aus der richtigen Region ausgewählt ist, und klicken Sie auf **Review + Create**.




Nun hat das Speicherkonto (in Abo 1) Zugriff auf das Cloud Volumes ONTAP-System, das im Abonnement ausgeführt wird 2.

6. Versuchen Sie erneut, Cloud Backup auf dem Cloud Volumes ONTAP System zu aktivieren, und dieses Mal sollte es erfolgreich sein.

# Wissen und Support

## Für den Support anmelden

Bevor Sie einen Support-Fall beim technischen Support von NetApp eröffnen können, müssen Sie BlueXP einen NetApp Support Site Account (NSS) hinzufügen und sich dann für den Support registrieren.

### Übersicht über die Support-Registrierung

Es gibt zwei Registrierungsformulare, um die Support-Berechtigung zu aktivieren:

- Registrieren Ihres BlueXP-Konto-ID-Support-Abonnements (Ihre 20-stellige Seriennummer 960xxxxxxxxx auf der Seite Support-Ressourcen in BlueXP).

  Dies dient als Ihre einzige Support-Abonnement-ID für jeden Service in BlueXP. Jedes BlueXP-Abonnement für Support auf Kontoebene muss registriert werden.

- Registrieren der Cloud Volumes ONTAP Seriennummern für ein Abonnement auf dem Markt Ihres Cloud-Providers (dies sind 20-stellige Seriennummern von 909201xxxxxx).

  Diese Seriennummern werden als *PAYGO Seriennummern* bezeichnet und werden zum Zeitpunkt der Cloud Volumes ONTAP Implementierung von BlueXP generiert.

Durch das Registrieren beider Arten von Seriennummern können Kunden Funktionen wie das Öffnen von Support-Tickets und die automatische Erstellung von Support-Cases nutzen.

Ihre Anmeldung hängt davon ab, ob Sie ein neuer oder bereits bestehender Kunde oder Partner sind.

- Bestehender Kunde oder Partner

  Als bestehender NetApp Kunde oder Partner können Sie mit Ihrem NSS SSO-Konto (NetApp Support Site) die oben genannten Registrierungen durchführen. Im Support Dashboard stellt BlueXP eine **NSS Management**-Seite zur Verfügung, auf der Sie Ihr NSS-Konto hinzufügen können. Sobald Sie Ihr NSS-Konto hinzugefügt haben, registriert BlueXP diese Seriennummern automatisch für Sie.

  Erfahren Sie, wie Sie Ihr NSS-Konto hinzufügen.

- Neu bei NetApp

  Wenn Sie neu bei NetApp sind, müssen Sie eine einmalige Registrierung Ihrer BlueXP Account ID Seriennummer auf der Support-Registrierungsseite von NetApp abschließen. Sobald Sie diese Registrierung abgeschlossen und ein neues NSS-Konto erstellt haben, können Sie dieses Konto in BlueXP verwenden, um sich in Zukunft automatisch zu registrieren.

  Erfahren Sie, wie Sie sich mit NetApp anmelden können.

### Fügen Sie ein NSS-Konto zu BlueXP hinzu

Über das Support Dashboard können Sie Ihre NetApp Support Site Konten zur Verwendung mit BlueXP hinzufügen und managen.

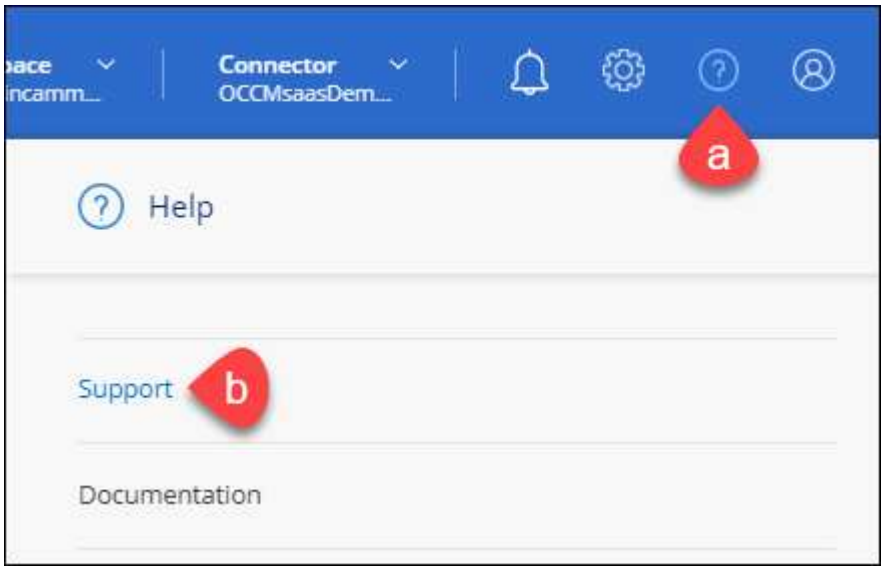
- Wenn Sie über ein Konto auf Kundenebene verfügen, können Sie ein oder mehrere NSS-Konten

hinzufügen.

- Wenn Sie einen Partner- oder Reseller-Account haben, können Sie ein oder mehrere NSS-Konten hinzufügen, können aber nicht neben Kunden-Level Accounts hinzugefügt werden.

**Schritte**

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.




2. Klicken Sie auf **NSS Management > NSS-Konto hinzufügen**.
3. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Weiter**, um auf eine Microsoft-Login-Seite umgeleitet zu werden.

   NetApp verwendet Microsoft Azure Active Directory als Identitäts-Provider für Authentifizierungsservices, die sich speziell für Support und Lizenzierung entscheiden.

4. Geben Sie auf der Anmeldeseite die registrierte E-Mail-Adresse und das Kennwort Ihrer NetApp Support Site an, um den Authentifizierungsvorgang durchzuführen.

   Mit diesen Aktionen kann BlueXP Ihr NSS-Konto für Dinge wie Lizenzdownloads, Softwareaktualisierungs-Verifizierung und zukünftige Support-Registrierungen verwenden.

   Beachten Sie Folgendes:

   - Das Konto muss ein Kundenkonto auf Kundenebene sein (kein Gast- oder Temporkonto).
   - Bei der erfolgreichen Anmeldung wird NetApp den NSS-Benutzernamen speichern. Dies ist eine vom System generierte ID, die Ihrer E-Mail zugeordnet wird. Auf der Seite **NSS Management** können Sie Ihre E-Mail über anzeigen ••• Menü.
   - Wenn Sie jemals Ihre Anmeldeinformationen aktualisieren müssen, gibt es im auch eine **Anmeldeinformationen aktualisieren**-Option ••• Menü. Wenn Sie diese Option verwenden, werden Sie aufgefordert, sich erneut anzumelden.

## Mit NetApp registrieren

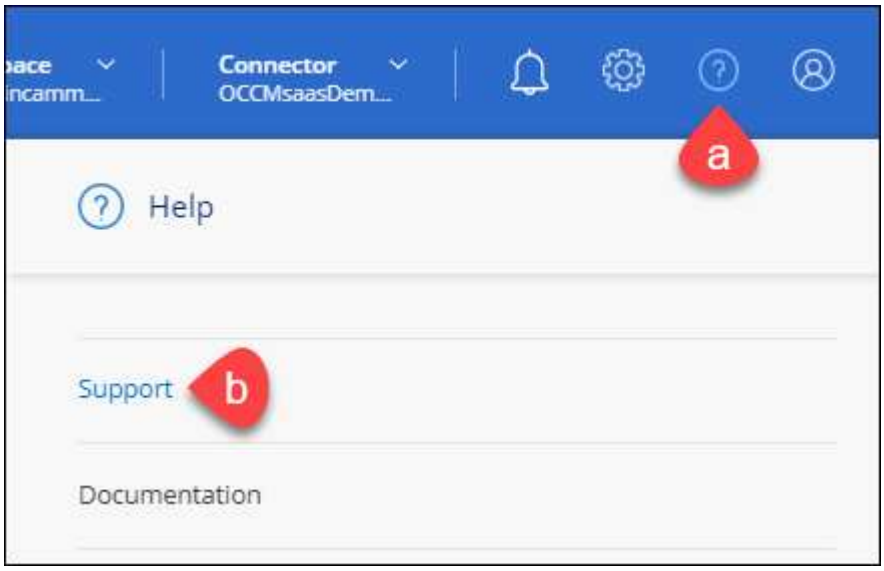
Wie Sie sich für den NetApp Support registrieren, hängt davon ab, ob Sie bereits über einen NSS Account (NetApp Support Site) verfügen.

### Bestandskunde mit NSS-Konto

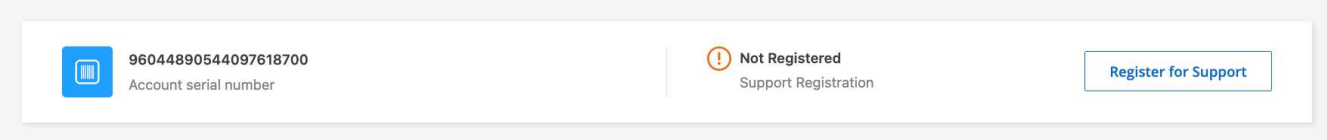
Wenn Sie ein NetApp Kunde mit einem NSS-Konto sind, müssen Sie sich lediglich für den Support über BlueXP registrieren.

#### Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.




2. Wenn Sie dies noch nicht getan haben, fügen Sie Ihr NSS-Konto bei BlueXP hinzu.
3. Klicken Sie auf der Seite **Ressourcen** auf **für Support registrieren**.




### Vorhandener Kunde, aber kein NSS-Konto

Wenn Sie bereits Kunde von NetApp mit vorhandenen Lizenzen und Seriennummern sind, aber *no* NSS Konto, müssen Sie nur ein NSS-Konto erstellen.

#### Schritte

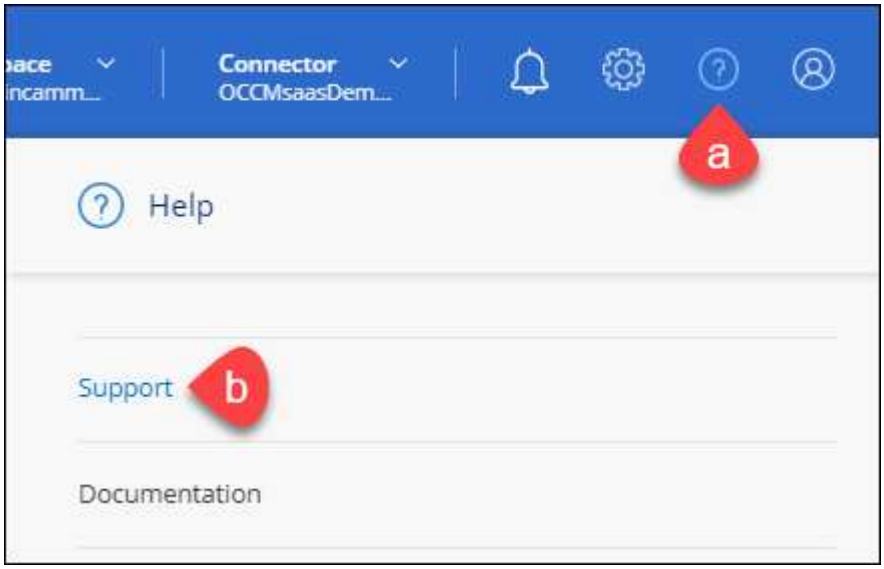
1. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen "NetApp Support Site-Formular zur Benutzerregistrierung"
   a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
   b. Kopieren Sie unbedingt die oben verwendete BlueXP-Kontonummer (960xxxx) für das Feld Seriennummer. Dadurch wird die Kontobearbeitung beschleunigt.

### Neu bei NetApp

Wenn Sie neu bei NetApp sind und über keinen NSS-Account verfügen, befolgen Sie jeden Schritt unten.

#### Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.




2. Suchen Sie auf der Seite für die Support-Registrierung die Seriennummer Ihres Kontos.

3. Navigieren Sie zu "Die Support-Registrierungs-Website von NetApp" Und wählen Sie **Ich bin kein registrierter NetApp Kunde**.
4. Füllen Sie die Pflichtfelder aus (mit roten Sternchen).
5. Wählen Sie im Feld **Product Line** die Option **Cloud Manager** aus, und wählen Sie dann den gewünschten Abrechnungsanbieter aus.
6. Kopieren Sie die Seriennummer des Kontos von Schritt 2 oben, füllen Sie die Sicherheitsprüfung aus und bestätigen Sie dann, dass Sie die globale Datenschutzrichtlinie von NetApp lesen.

   Zur Fertigstellung dieser sicheren Transaktion wird sofort eine E-Mail an die angegebene Mailbox gesendet. Überprüfen Sie Ihre Spam-Ordner, wenn die Validierungs-E-Mail nicht in wenigen Minuten ankommt.

7. Bestätigen Sie die Aktion in der E-Mail.

   Indem Sie Ihre Anfrage an NetApp senden, wird Ihnen die Erstellung eines NetApp Support Site Kontos empfohlen.

8. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen "NetApp Support Site-Formular zur Benutzerregistrierung"
   a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
   b. Kopieren Sie die oben angegebene Seriennummer (960xxxx) für das Feld „Seriennummer“. Dadurch wird die Kontobearbeitung beschleunigt.

**Nachdem Sie fertig sind**

NetApp sollte sich bei diesem Prozess mit Ihnen in Verbindung setzen. Dies ist eine einmalige Onboarding-Übung für neue Benutzer.

Sobald Sie Ihren NetApp Support Site Account besitzen, können Sie im Portal BlueXP diesen NSS-Account für zukünftige Registrierungen hinzufügen.

# Holen Sie sich Hilfe

NetApp bietet Unterstützung für BlueXP und seine Cloud-Services auf unterschiedliche Weise. Umfassende kostenlose Self-Support-Optionen stehen rund um die Uhr zur Verfügung, wie etwa Knowledge Base-Artikel (KB) und ein Community-Forum. Ihre Support-Registrierung umfasst technischen Remote-Support über Web-Ticketing.

## Self-Support

Diese Optionen sind kostenlos verfügbar, 24 Stunden am Tag, 7 Tage die Woche:

- "Wissensdatenbank"

  Suchen Sie in der BlueXP Knowledge Base nach hilfreichen Artikeln zur Fehlerbehebung.

- "Communitys"

  Treten Sie der BlueXP Community bei, um laufende Diskussionen zu verfolgen oder neue zu erstellen.

- Dokumentation

  Die BlueXP-Dokumentation, die Sie gerade anzeigen.

- Mailto:ng-cloudmanager-feedback@netapp.com[Feedback email]

  Wir wissen Ihre Vorschläge zu schätzen. Senden Sie uns Ihr Feedback, um BlueXP zu verbessern.

## NetApp Support

Zusätzlich zu den oben genannten Self-Support-Optionen können Sie gemeinsam mit einem NetApp Support-Experten eventuelle Probleme nach der Aktivierung des Supports beheben.

#### Bevor Sie beginnen

Um die * Case erstellen*-Fähigkeit zu verwenden, müssen Sie zuerst eine einmalige Registrierung Ihrer BlueXP Account ID-Seriennummer (dh 960xxxx) mit NetApp "Erfahren Sie, wie Sie sich für Support registrieren".

#### Schritte

1. Klicken Sie in BlueXP auf **Hilfe > Support**.
2. Wählen Sie eine der verfügbaren Optionen unter Technical Support:
   a. Klicken Sie auf **Rufen Sie uns an**, wenn Sie mit jemandem am Telefon sprechen möchten. Sie werden zu einer Seite auf netapp.com weitergeleitet, auf der die Telefonnummern aufgeführt sind, die Sie anrufen können.
   b. Klicken Sie auf **Case erstellen**, um ein Ticket mit einem NetApp Support-Experten zu öffnen:
      - **NetApp Support Site Account**: Wählen Sie das entsprechende NSS-Konto für die Person aus, die den Support-Case eröffnet. Diese Person ist der primäre Ansprechpartner bei NetApp, der Sie sich zusätzlich zu den unten aufgeführten zusätzlichen E-Mails mit anderen Kunden in Verbindung setzen kann.

Wenn Ihr NSS-Konto nicht angezeigt wird, können Sie im Support-Bereich von BlueXP zur Registerkarte **NSS Management** navigieren, um es dort hinzuzufügen.

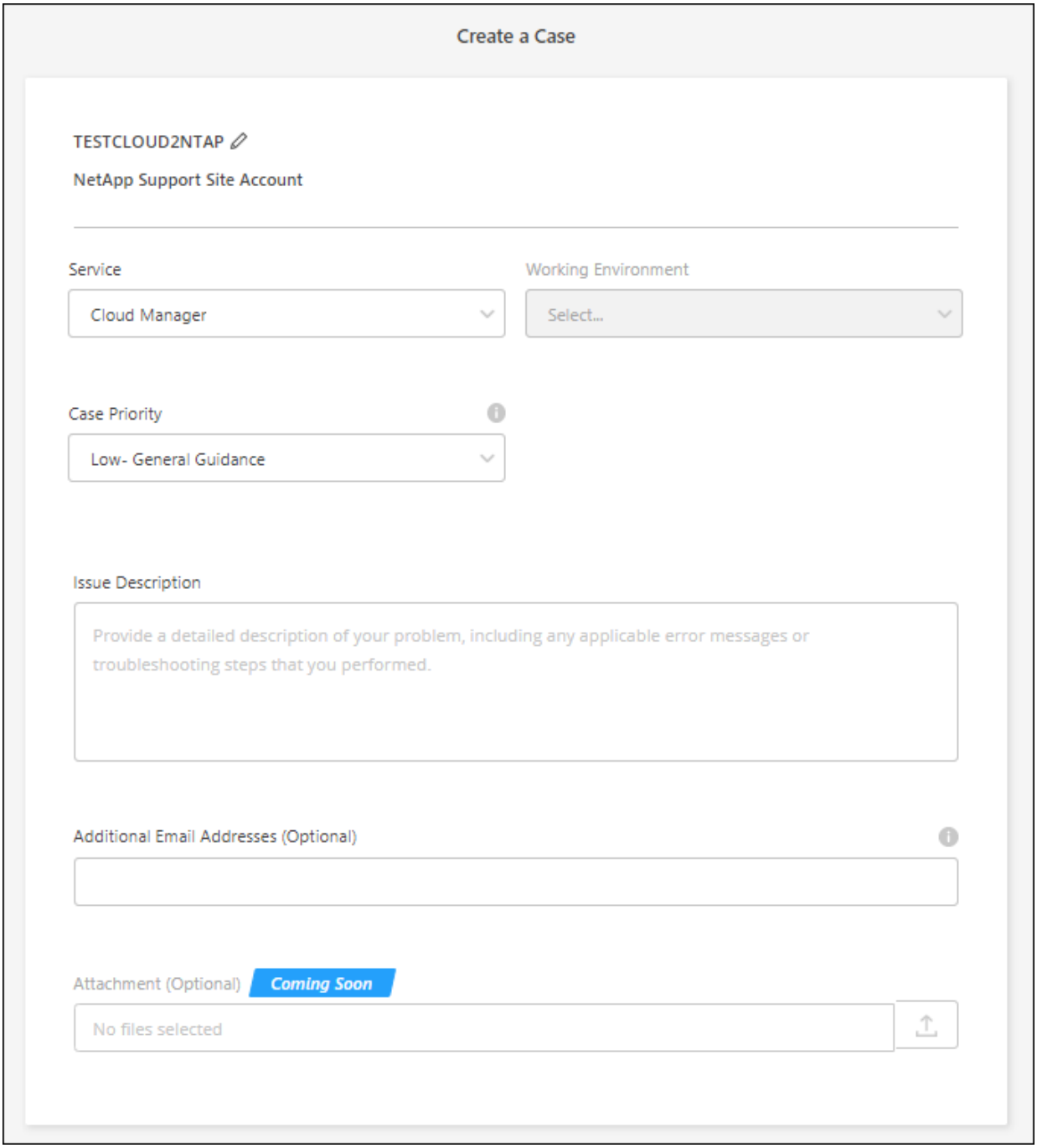
- **Service**: Wählen Sie den Dienst aus, mit dem das Problem verknüpft ist. Beispiel: BlueXP, wenn es sich um ein Problem des technischen Supports mit Workflows oder Funktionen im Service handelt.
- **Arbeitsumgebung**: Wählen Sie **Cloud Volumes ONTAP** oder **On-Prem** und anschließend die zugehörige Arbeitsumgebung aus.

  Die Liste der Arbeitsumgebungen liegt im Bereich des BlueXP-Kontos, des Arbeitsbereichs und des Connectors, den Sie im oberen Banner des Dienstes ausgewählt haben.

- **Case Priority**: Wählen Sie die Priorität für den Fall, der niedrig, Mittel, hoch oder kritisch sein kann.

  Wenn Sie weitere Informationen zu diesen Prioritäten wünschen, bewegen Sie den Mauszeiger über das Informationssymbol neben dem Feldnamen.

- **Problembeschreibung**: Geben Sie eine detaillierte Beschreibung Ihres Problems an, einschließlich aller anwendbaren Fehlermeldungen oder Fehlerbehebungsschritte, die Sie durchgeführt haben.
- **Zusätzliche E-Mail-Adressen**: Geben Sie zusätzliche E-Mail-Adressen ein, wenn Sie jemand anderes auf dieses Problem aufmerksam machen möchten.




**Nachdem Sie fertig sind**

Es wird ein Popup-Fenster mit der Support-Fallnummer angezeigt. Ein NetApp Support-Experte prüft Ihren Fall und macht Sie umgehend mit.

Für eine Historie Ihrer Supportfälle können Sie auf **Einstellungen > Timeline** klicken und nach Aktionen mit dem Namen „Support Case erstellen“ suchen. Mit einer Schaltfläche ganz rechts können Sie die Aktion erweitern, um Details anzuzeigen.

Es ist möglich, dass beim Versuch, einen Fall zu erstellen, möglicherweise die folgende Fehlermeldung angezeigt wird:

„Sie sind nicht berechtigt, einen Fall für den ausgewählten Service zu erstellen.“

Dieser Fehler könnte bedeuten, dass das NSS-Konto und das Unternehmen des Datensatzes, mit dem es verbunden ist, nicht das gleiche Unternehmen des Eintrags für die BlueXP Account Seriennummer (dh 960xxxx) oder Seriennummer der Arbeitsumgebung. Sie können Ihre Liste der NSS-Konten oben im **Case erstellen**-Formular überprüfen, um die richtige Übereinstimmung zu finden, oder Sie können Hilfe mit einer der folgenden Optionen suchen:

- Verwenden Sie den Chat im Produkt
- Übermitteln eines nicht-technischen Cases unter https://mysupport.netapp.com/site/help

# Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

## Urheberrecht

http://www.netapp.com/us/legal/copyright.aspx

## Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

http://www.netapp.com/us/legal/netapptmlist.aspx

## Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/us/media/patents-page.pdf

## Datenschutzrichtlinie

https://www.netapp.com/us/legal/privacypolicy/index.aspx

## Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

- "Hinweis für BlueXP"
- "Hinweis zum Cloud Backup"
- "Hinweis zur Wiederherstellung einzelner Dateien"

**Copyright-Informationen**

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

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

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

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

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

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

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

**Markeninformationen**

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