



Referenz

Cloud Backup

NetApp
November 17, 2022

This PDF was generated from <https://docs.netapp.com/de-de/cloud-manager-backup-restore/aws/concept-cloud-backup-policies.html> on November 17, 2022. Always check docs.netapp.com for the latest.

Inhaltsverzeichnis

- Referenz 1
 - Konfigurationseinstellungen für Cloud-Backup-Richtlinien 1
 - AWS S3-Archiv-Storage-Klassen und Restore Abrufzeiten 7
 - Azure-Archivierungsebenen und Wiederherstellungszeiten 9
 - Backup für Multi-Account-Zugriff in Azure konfigurieren 10

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.

The screenshot displays the 'Labels & Retention' configuration panel. It features a search bar and a list of 12 labels. The 'Selected Labels (2)' section shows two selected labels: 'Hourly' with 'Number of Backups to Retain' set to 12, and 'Daily' with 'Number of Backups to Retain' set to 30. Below this, the 'DataLock & Ransomware Protection' is set to 'None', and the 'Archival Policy' is set to 'Disabled'.

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 Richtlinien-aufbewahrung 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.

The screenshot displays the configuration for a backup policy. The 'DataLock & Ransomware Protection' section is highlighted with an orange border. It shows three options: 'None' (selected), 'Governance', and 'Compliance'. The 'Governance' option is noted as not being available with StorageGRID. To the right, an information box explains that the protection mode is immutable, files are locked during retention, and ransomware scans are performed automatically. The 'Archival Policy' at the bottom is currently disabled.

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 <code>ifdef::aws[]</code>
Cloud Volumes ONTAP in AWS	Amazon S3 <code>endif::aws[]</code> <code>ifdef::Azure[]</code> <code>endif::azurAzure[]</code> <code>ifdef::gcp[]</code> <code>endif::gcp[]</code>
Lokales ONTAP System	<code>ifdef::aws[]</code> Amazon S3 <code>endif::aws[]</code> <code>ifdef::azurAzure[]</code> <code>endif::azurAzure[]</code> <code>ifdef::gcp[]</code> <code>endif::gcp[]</code> NetApp StorageGRID

Anforderungen

- Ihre Cluster müssen ONTAP 9.11.1 oder höher ausführen
- Sie müssen BlueXP 3.9.21 oder höher verwenden
- Für AWS:
 - Der Connector muss in der Cloud implementiert werden
 - Die folgenden S3-Berechtigungen müssen Teil der IAM-Rolle sein, die dem Connector Berechtigungen erteilt. Sie befinden sich im Abschnitt „BackupS3Policy“ für die Ressource „arn:aws:s3::netapp-Backup-*“:
 - `s3:GetObjectVersionTagging`
 - `s3:GetBucketObjectLockConfiguration`
 - `s3:GetObjectVersionAcl`
 - `s3:PutObjectTagging`
 - `s3:DeleteObject`
 - `s3:DeleteObjectTagging`
 - `s3:GetObjectRetention`
 - `s3:DeleteObjectVersionTagging`
 - `s3:PutObject`
 - `s3:GetObject`
 - `s3:PutBucketObjectLockConfiguration`
 - `s3:GetLifecycleKonfiguration`
 - `s3:ListBucketByTags`
 - `s3:GetBucketTagging`
 - `s3:DeleteObjectVersion`
 - `s3:ListBucketVersions`
 - `s3:ListBucket`
 - `s3:PutBucketTagging`
 - `s3:GetObjectTagging`

- s3:PutBucketVersionierung
- s3:PutObjectVersionTagging
- s3:GetBucketVersionierung
- s3:GetBucketAcl
- s3:BypassGovernanceAufbewahrung
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

„s3:BypassGovernanceRetention“ muss nur hinzugefügt werden, wenn Sie möchten, dass Ihre Admin-Benutzer in der Lage sind, Sicherungsdateien, die im Governance-Modus gesperrt sind, zu überschreiben oder zu löschen.

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

- 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.

Daten in Archivebenen können nicht sofort abgerufen werden, wenn nötig, und erfordert eine höhere Abrufkosten, so müssen Sie überlegen, wie oft Sie Daten aus archivierten Backup-Dateien wiederherstellen müssen.

Beim Erstellen von Backup-Dateien in AWS oder Azure bietet jede Backup-Richtlinie einen Abschnitt für „*Archival Policy*“, den Sie auf Ihre Backup-Dateien anwenden können.

Name	Default_Policy_Name	▼
Labels & Retention	30 Daily	▼
DataLock & Ransomware Protection	None	▼
Archival Policy	<p>Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.</p> <p><input checked="" type="checkbox"/> Tier Backups to Archive</p> <div> <div>Archive After (Days)</div> <div>Storage Class</div> </div> <div> <div>30</div> <div>S3 Glacier ▼</div> </div>	

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

Falls Ihr Cluster ONTAP 9.10.1 oder höher nutzt, können Sie ältere Backups nach einer bestimmten Anzahl von Tagen entweder auf *S3 Glacier* oder *S3 Glacier Deep Archive* Storage abstufen, um die Kosten weiter zu optimieren. "[Weitere Informationen zu AWS Archiv-Storage](#)".

Wenn Sie bei der Aktivierung von Cloud Backup *S3 Glacier* oder *S3 Glacier Deep Archive* als erste Backup-Richtlinie auswählen, wird dieser Tier zur einzigen Archiv-Tier, 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.

- 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 *data from archival storage*, 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-Archivierungszugriffstier 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 *data from archival storage*, 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"](#).

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.

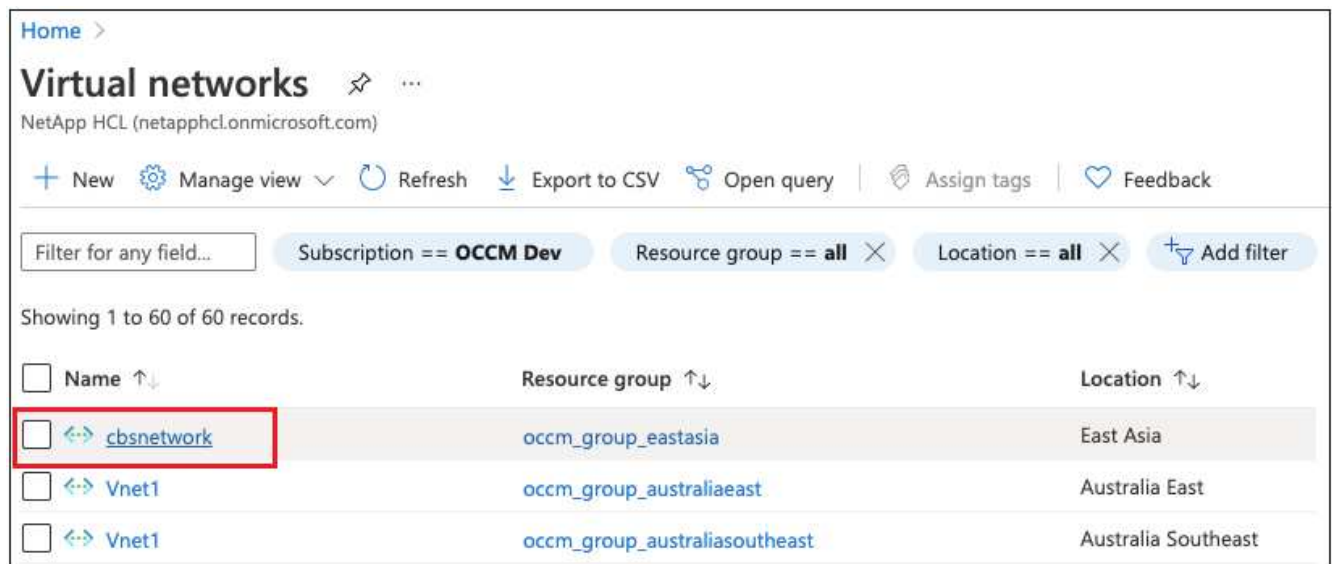
Diese Schritte sind nur erforderlich, wenn Sie sich befinden ["Sichern von Cloud Volumes ONTAP-Daten auf Azure Blob Storage"](#).

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**.

Subscription * ⓘ

OCCM Automation

Virtual network *

cbse2evnet

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

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.


cbsnetwork | Peerings

Virtual network

«
+ Add
↻ Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

Security

DNS servers

Peerings

Name	Peering status	Peer
cbsnetwork	Connected	cbse2evnet

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

<<
+ Add
↻ Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

Security

DNS servers

Peerings

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/4d97b98b-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.

Create a private endpoint

1 Basics 2 Resource 3 Configuration 4 Tags 5 Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

Project details

Subscription * ⓘ OCCM Dev

Resource group * ⓘ cbsoccmdevcvo-rg [Create new](#)

Instance details

Name * cbse2e ✓

Region * (Asia Pacific) East Asia

3. Wählen Sie auf der Seite *Ressource* die Unterressource Ziel als **Blob** aus.

Create a private endpoint ...

✓ Basics **2 Resource** 3 Configuration 4 Tags 5 Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Subscription OCCM Dev (d333af45-0d07-4154-943d-c25fbbce1b18)

Resource type Microsoft.Storage/storageAccounts

Resource test150521

Target sub-resource * ⓘ

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".

Create a private endpoint ...

✓ Basics ✓ Resource **3 Configuration** 4 Tags 5 Review + create

Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network * ⓘ

Subnet * ⓘ

ⓘ If you have a network security group (NSG) enabled for the subnet above, it will be disabled for private endpoints on this subnet only. Other resources on the subnet will still have NSG enforcement.

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone ☒ Yes ☐ No

Configuration name	Subscription	Private DNS zone
privatelink-blob-core-...	OCCM Dev	privatelink.blob.core.windows.net

Review + create < Previous Next : Tags >

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**.

Configuration name	Subscription	Private DNS zone
privatelink-blob-core-...	OCCM Dev	privatelink.blob.core.windows.net
		<input type="text" value="Filter private DNS zones"/>
		<div> <div>occm_group_centralus</div> <div>privatelink.blob.core.windows.net</div> </div>
		<div> <div>occm_group_eastus</div> <div>privatelink.blob.core.windows.net</div> </div>
		<div> <div>occm_group_eastus2</div> <div>privatelink.blob.core.windows.net</div> </div>

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.

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 IRGEND EINER 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.