



## **Referenz**

NetApp Backup and Recovery

NetApp  
February 11, 2026

# Inhalt

Referenz .....	1
Richtlinien in SnapCenter im Vergleich zu denen in NetApp Backup and Recovery .....	1
Zeitplanstufen .....	1
Mehrere Richtlinien in SnapCenter mit derselben Zeitplanebene .....	1
Importierte SnapCenter -Tagespläne .....	1
Importierte SnapCenter -Stundenpläne .....	2
Protokollaufbewahrung aus SnapCenter -Richtlinien .....	2
Aufbewahrungsdauer der Protokollsicherung .....	2
Aufbewahrungsanzahl aus SnapCenter -Richtlinien .....	2
SnapMirror -Labels aus SnapCenter -Richtlinien .....	3
NetApp Backup and Recovery Identity and Access Management (IAM)-Rollen .....	3
Wiederherstellen der NetApp Backup and Recovery -Konfigurationsdaten in einer Dark Site .....	3
Wiederherstellen von NetApp Backup and Recovery -Daten auf einem neuen Konsolenagenten .....	4
Unterstützte AWS-Archivspeicherebenen mit NetApp Backup and Recovery .....	8
Unterstützte S3-Archivspeicherklassen für NetApp Backup and Recovery .....	9
Daten aus dem Archivspeicher wiederherstellen .....	9
Unterstützte Azure-Archivzugriffsebenen mit NetApp Backup and Recovery .....	10
Unterstützte Azure Blob-Zugriffsebenen für NetApp Backup and Recovery .....	10
Daten aus dem Archivspeicher wiederherstellen .....	11
Unterstützte Google-Archivspeicherebenen mit NetApp Backup and Recovery .....	11
Unterstützte Google-Archivspeicherklassen für NetApp Backup and Recovery .....	12
Daten aus dem Archivspeicher wiederherstellen .....	12

# Referenz

## Richtlinien in SnapCenter im Vergleich zu denen in NetApp Backup and Recovery

Es gibt einige Unterschiede zwischen den in SnapCenter und den in NetApp Backup and Recovery verwendeten Richtlinien, die sich auf die Anzeige nach dem Importieren von Ressourcen und Richtlinien aus SnapCenter auswirken können.

### Zeitplanstufen

SnapCenter verwendet die folgenden Zeitplanebenen:

- **Stündlich:** Mehrere Stunden und Minuten mit beliebigen Stunden (0-23) und beliebigen Minuten (0-60).
- **Täglich:** Option zur Wiederholung nach einer festgelegten Anzahl von Tagen, beispielsweise alle 3 Tage.
- **Wöchentlich:** Sonntag bis Montag, mit der Option, am ersten Tag der Woche oder an mehreren Tagen der Woche einen Snapshot durchzuführen.
- **Monatlich:** Januar bis Dezember, mit der Option, an bestimmten oder mehreren Tagen im Monat aufzutreten, zum Beispiel am 7.

NetApp Backup and Recovery verwendet die folgenden Zeitplanebenen, die sich leicht unterscheiden:

- **Stündlich:** Führt Snapshots nur in 15-Minuten-Intervallen aus, beispielsweise alle 1 Stunde oder in 15-Minuten-Intervallen unter 60.
- **Täglich:** Stunden des Tages (0–23) mit Startzeit beispielsweise um 10:00 Uhr mit der Option, alle paar Stunden eine Ausführung durchzuführen.
- **Wöchentlich:** Wochentag (Sonntag bis Montag) mit der Option, an einem oder mehreren Tagen aufzutreten. Dies ist dasselbe wie SnapCenter.
- **Monatlich:** Daten des Monats (0–30) mit einer Startzeit an mehreren Daten des Monats.
- **Jährlich:** Monatlich. Dies entspricht dem monatlichen SnapCenter.

### Mehrere Richtlinien in SnapCenter mit derselben Zeitplanebene

Sie können einer Ressource in SnapCenter mehrere Richtlinien mit derselben Zeitplanebene zuweisen. NetApp Backup and Recovery unterstützt jedoch nicht mehrere Richtlinien für eine Ressource, die dieselbe Zeitplanebene verwendet.

**Beispiel:** Wenn Sie in SnapCenter drei Richtlinien (für Daten, Protokoll und Protokoll von Snapshots) verwenden, verwendet NetApp Backup and Recovery nach der Migration von SnapCenter eine einzige Richtlinie anstelle aller drei.

### Importierte SnapCenter -Tagespläne

NetApp Backup and Recovery passt die SnapCenter -Zeitpläne wie folgt an:

- Wenn der SnapCenter -Zeitplan auf weniger als oder gleich 7 Tage eingestellt ist, legt NetApp Backup and Recovery den Zeitplan auf wöchentlich fest. Einige Schnappschüsse werden während der Woche übersprungen.

**Beispiel:** Wenn Sie über eine SnapCenter -Tagesrichtlinie mit einem Wiederholungsintervall von drei Tagen ab Montag verfügen, legt NetApp Backup and Recovery den Zeitplan auf wöchentlich am Montag, Donnerstag und Sonntag fest. Einige Tage werden übersprungen, da es nicht genau alle 3 Tage ist.

- Wenn der SnapCenter -Zeitplan auf mehr als 7 Tage eingestellt ist, legt NetApp Backup and Recovery den Zeitplan auf monatlich fest. Einige Schnapschüsse werden im Laufe des Monats übersprungen.

**Beispiel:** Wenn Sie über eine SnapCenter -Tagesrichtlinie mit einem Wiederholungsintervall von 10 Tagen ab dem 2. des Monats verfügen, legt NetApp Backup and Recovery den Zeitplan nach der Migration am 2., 12. und 22. Tag des Monats auf monatlich fest. Bei NetApp Backup and Recovery werden im nächsten Monat einige Tage ausgelassen.

## Importierte SnapCenter -Stundenpläne

Stündliche SnapCenter -Richtlinien mit Wiederholungsintervallen von mehr als einer Stunde werden in NetApp Backup and Recovery in eine tägliche Richtlinie umgewandelt.

Bei jeder stündlichen Richtlinie mit Wiederholungsintervallen, die kein Faktor von 24 sind (z. B. 5, 7 usw.), werden einige Snapshots an einem Tag übersprungen.

**Beispiel:** Wenn Sie über eine stündliche SnapCenter -Richtlinie mit einem Wiederholungsintervall alle 5 Stunden ab 1:00 Uhr verfügen, legt NetApp Backup and Recovery (nach der Migration) den Zeitplan auf täglich mit 5-Stunden-Intervallen um 1:00 Uhr, 6:00 Uhr, 11:00 Uhr, 16:00 Uhr und 21:00 Uhr fest. Einige Stunden werden übersprungen. Nach 21:00 Uhr sollte es 2:00 Uhr sein, um es alle 5 Stunden zu wiederholen, aber es wird immer 1:00 Uhr sein.

## Protokollaufbewahrung aus SnapCenter -Richtlinien

Wenn Sie in SnapCenter über eine Ressource mit mehreren Richtlinien verfügen, verwendet NetApp Backup and Recovery die folgende Prioritätsreihenfolge, um den Protokollaufbewahrungswert zuzuweisen:

- Für „Vollständige Sicherung mit Protokollsicherungsrichtlinie“ plus „Nur-Protokoll“-Richtlinien in SnapCenter verwendet NetApp Backup and Recovery den Aufbewahrungswert der Nur-Protokoll-Richtlinie.
- Für die Richtlinien „Vollständige Sicherung nur mit Protokoll“ und „Vollständig und Protokoll“ in SnapCenter verwendet NetApp Backup and Recovery den Nur-Protokoll-Aufbewahrungswert.
- Für „Vollständige Sicherung und Protokoll“ plus „Vollständige Sicherung“ in SnapCenter verwendet NetApp Backup and Recovery den Aufbewahrungswert „Vollständige Sicherung und Protokoll“.
- Wenn Sie in SnapCenter nur über eine vollständige Sicherung verfügen, aktiviert NetApp Backup and Recovery die Protokollsicherung nicht.

## Aufbewahrungsduer der Protokollsicherung

SnapCenter unterstützt mehrere Aufbewahrungswerte für Richtlinien für eine Ressource. NetApp Backup and Recovery unterstützt nur einen Aufbewahrungswert pro Ressource.

## Aufbewahrungsanzahl aus SnapCenter -Richtlinien

Wenn Sie über eine Ressource mit aktiviertem sekundärem Schutz in SnapCenter mit mehreren Quellvolumes, mehreren Zielvolumes und mehreren SnapMirror -Beziehungen verfügen, verwendet NetApp Backup and Recovery nur die Aufbewahrungsanzahl der ersten Richtlinie.

**Beispiel:** Wenn Sie eine SnapCenter -Richtlinie mit einer Aufbewahrungsanzahl von 5 und eine andere

Richtlinie mit einer Aufbewahrungsanzahl von 10 haben, verwendet NetApp Backup and Recovery die Aufbewahrungsanzahl von 5.

## SnapMirror -Labels aus SnapCenter -Richtlinien

SnapCenter behält nach der Migration SnapMirror -Beschriftungen für jede Richtlinie bei, auch wenn sich die Ebene ändert.

**Beispiel:** Eine stündliche Richtlinie von SnapCenter kann in NetApp Backup and Recovery auf täglich geändert werden. Die SnapMirror -Beschriftungen bleiben jedoch nach der Migration gleich.

## NetApp Backup and Recovery Identity and Access Management (IAM)-Rollen

NetApp Backup and Recovery verwendet Identity and Access Management (IAM), um den Zugriff jedes Benutzers auf bestimmte Funktionen und Aktionen zu regeln.

Weitere Informationen zu IAM-Rollen, die speziell für NetApp Backup and Recovery gelten, finden Sie unter "[NetApp Backup and Recovery -Rollen in der NetApp Console](#)".

## Wiederherstellen der NetApp Backup and Recovery -Konfigurationsdaten in einer Dark Site

Wenn Sie NetApp Backup and Recovery an einem Standort ohne Internetzugang verwenden (bekannt als *privater Modus*), werden die Konfigurationsdaten von NetApp Backup and Recovery im StorageGRID oder ONTAP S3-Bucket gesichert, in dem Ihre Backups gespeichert werden. Wenn Sie ein Problem mit dem Hostsystem des Konsolenagenten haben, können Sie einen neuen Konsolenagenten bereitstellen und die kritischen NetApp Backup and Recovery -Daten wiederherstellen.



Dieses Verfahren gilt nur für ONTAP Volume-Daten.

Wenn Sie NetApp Backup and Recovery in einer SaaS-Umgebung verwenden und der Konsolenagent bei Ihrem Cloud-Anbieter oder auf Ihrem eigenen mit dem Internet verbundenen Host bereitgestellt wird, sichert und schützt das System alle wichtigen Konfigurationsdaten in der Cloud. Wenn Sie ein Problem mit dem Konsolenagenten haben, erstellen Sie einen neuen Konsolenagenten und fügen Sie Ihre Systeme hinzu. Die Sicherungsdetails werden automatisch wiederhergestellt.

Es werden zwei Arten von Daten gesichert:

- NetApp Backup and Recovery -Datenbank – enthält eine Liste aller Volumes, Sicherungsdateien, Sicherungsrichtlinien und Konfigurationsinformationen.
- Indizierte Katalogdateien – enthalten detaillierte Indizes, die für die Such- und Wiederherstellungsfunktion verwendet werden und Ihre Suche nach Volumedaten, die Sie wiederherstellen möchten, sehr schnell und effizient machen.

Diese Daten werden einmal täglich um Mitternacht gesichert und es werden maximal 7 Kopien jeder Datei aufbewahrt. Wenn der Konsolenagent mehrere lokale ONTAP -Systeme verwaltet, werden die NetApp Backup and Recovery im Bucket des zuerst aktivierten Systems gespeichert.



In der NetApp Backup and Recovery -Datenbank oder in den indizierten Katalogdateien sind niemals Volumedaten enthalten.

## Wiederherstellen von NetApp Backup and Recovery -Daten auf einem neuen Konsolenagenten

Wenn Ihr lokaler Konsolenagent nicht mehr funktioniert, müssen Sie einen neuen Konsolenagenten installieren und dann die NetApp Backup and Recovery -Daten auf dem neuen Konsolenagenten wiederherstellen.

Sie müssen die folgenden Aufgaben ausführen, um Ihr NetApp Backup and Recovery -System wieder in einen funktionsfähigen Zustand zu versetzen:

- Installieren Sie einen neuen Konsolenagenten
- Wiederherstellen der NetApp Backup and Recovery -Datenbank
- Wiederherstellen der indizierten Katalogdateien
- Erkennen Sie alle Ihre On-Premise ONTAP -Systeme und StorageGRID Systeme erneut in der NetApp Console Benutzeroberfläche.

Nachdem Sie überprüft haben, ob Ihr System funktioniert, erstellen Sie neue Sicherungsdateien.

### Was du brauchst

Sie müssen auf die aktuellsten Datenbank- und Indexsicherungen aus dem StorageGRID oder ONTAP S3-Bucket zugreifen, in dem Ihre Sicherungsdateien gespeichert sind:

- NetApp Backup and Recovery MySQL-Datenbankdatei

Diese Datei befindet sich am folgenden Speicherort im Bucket `netapp-backup-<GUID>/mysql_backup/` und es heißt `CBS_DB_Backup_<day>_<month>_<year>.sql`.

- ZIP-Sicherungsdatei des indizierten Katalogs

Diese Datei befindet sich am folgenden Speicherort im Bucket `netapp-backup-<GUID>/catalog_backup/` und es heißt `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip`.

### Installieren Sie einen neuen Konsolen-Agenten auf einem neuen lokalen Linux-Host

Laden Sie beim Installieren eines neuen Konsolenagenten dieselbe Softwareversion herunter wie beim ursprünglichen Agenten. Änderungen an der NetApp Backup and Recovery -Datenbank können dazu führen, dass neuere Softwareversionen nicht mit alten Datenbanksicherungen funktionieren. Du kannst "[Aktualisieren Sie die Konsolen-Agent-Software auf die neueste Version, nachdem Sie die Backup-Datenbank wiederhergestellt haben.](#)" .

1. ["Installieren Sie den Konsolen-Agenten auf einem neuen lokalen Linux-Host"](#)
2. Melden Sie sich mit den soeben erstellten Administrator-Benutzeranmeldeinformationen bei der Konsole an.

### Wiederherstellen der NetApp Backup and Recovery -Datenbank

1. Kopieren Sie die MySQL-Sicherung vom Sicherungsspeicherort auf den neuen Konsolen-Agent-Host. Wir verwenden unten den Beispieldateinamen „`CBS_DB_Backup_23_05_2023.sql`“.

2. Kopieren Sie die Sicherung mit einem der folgenden Befehle in den MySQL-Docker-Container, je nachdem, ob Sie einen Docker- oder Podman-Container verwenden:

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Rufen Sie die MySQL-Container-Shell mit einem der folgenden Befehle auf, je nachdem, ob Sie einen Docker- oder Podman-Container verwenden:

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. Stellen Sie in der Container-Shell die „Umgebung“ bereit.
5. Sie benötigen das MySQL-DB-Password. Kopieren Sie daher den Wert des Schlüssels „MYSQL\_ROOT\_PASSWORD“.
6. Stellen Sie die MySQL-Datenbank von NetApp Backup and Recovery mit dem folgenden Befehl wieder her:

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Überprüfen Sie mit den folgenden SQL-Befehlen, ob die MySQL-Datenbank von NetApp Backup and Recovery korrekt wiederhergestellt wurde:

```
mysql -u root -p cloud_backup
```

8. Geben Sie das Passwort ein.

```
mysql> show tables;  
mysql> select * from volume;
```

9. Stellen Sie sicher, dass die angezeigten Volumina mit denen Ihrer ursprünglichen Umgebung übereinstimmen.

## **Wiederherstellen der indizierten Katalogdateien**

1. Kopieren Sie die ZIP-Sicherungsdatei des indizierten Katalogs (wir verwenden den Beispieldateinamen „Indexed\_Catalog\_DB\_Backup\_catalogdb1\_23\_05\_2023.zip“) vom Sicherungsspeicherort auf den neuen Konsolenagent-Host im Ordner „/opt/application/netapp/cbs“.

2. Entpacken Sie die Datei „Indexed\_Catalog\_DB\_Backup\_catalogdb1\_23\_05\_2023.zip“ mit dem folgenden Befehl:

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Führen Sie den Befehl **ls** aus, um sicherzustellen, dass der Ordner „catalogdb1“ mit den darunter liegenden Unterordnern „changes“ und „snapshots“ erstellt wurde.

## Entdecken Sie Ihre ONTAP -Cluster und StorageGRID Systeme

1. ["Entdecken Sie alle On-Premise ONTAP Systeme"](#) die in Ihrer vorherigen Umgebung verfügbar waren.  
Dazu gehört auch das ONTAP -System, das Sie als S3-Server verwendet haben.
2. ["Entdecken Sie Ihre StorageGRID -Systeme"](#).

## Einrichten der StorageGRID -Umgebungsdetails

Fügen Sie die Details des StorageGRID -Systems hinzu, das mit Ihren ONTAP -Systemen verknüpft ist, wie sie im ursprünglichen Konsolen-Agent-Setup eingerichtet wurden, mithilfe des ["NetApp Console -APIs"](#) .

Die folgenden Informationen gelten für Installationen im privaten Modus ab NetApp Console 3.9.xx. Bei älteren Versionen gehen Sie wie folgt vor: ["DarkSite Cloud Backup: MySQL und indizierter Katalog sichern und wiederherstellen"](#) .

Sie müssen diese Schritte für jedes System ausführen, das Daten auf StorageGRID sichert.

1. Extrahieren Sie das Autorisierungstoken mithilfe der folgenden OAuth/Token-API.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept: application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '{ "username": "admin@netapp.com", "password": "Netapp@123", "grant_type": "password" }' > '
```

Während es sich bei der IP-Adresse, dem Benutzernamen und den Passwörtern um benutzerdefinierte Werte handelt, ist dies beim Kontonamen nicht der Fall. Der Kontoname lautet immer „account-DARKSITE1“. Außerdem muss der Benutzername einen Namen im E-Mail-Format verwenden.

Diese API gibt eine Antwort wie die folgende zurück. Sie können das Autorisierungstoken wie unten gezeigt abrufen.

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJ1MGFizjRiIn0eyJzdWIiOjYvY2NtYXV0aHwxIiwiYXVkJpbImh0dHBzOi8vY
XBpLmNsb3VkLm51dGFwcC5jb20ixSwiaHR0cDovL2Nsb3VkLm51dGFwcC5jb20vZnVsbF9uY
W11IjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS91bWFpbCI6ImFkbWluQG51d
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxliiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23PoK
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVmYHqywZ4nNFa1MvAh4xEsc5jfOKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGENDzzwOKfUoUoe1Fg3ch--7JFkF1-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSzCUbIA"}
```

## 2. Extrahieren Sie die System-ID und die X-Agent-ID mithilfe der Tenancy/External/Resource-API.

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJ1MGFizjRiIn0eyJzdWIiOjYvY
2NtYXV0aHwxIiwiYXVkJpbImh0dHBzOi8vYXBpLmNsb3VkLm51dGFwcC5jb20ixSwiaHR0c
DovL2Nsb3VkLm51dGFwcC5jb20vZnVsbF9uYW11IjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS91bWFpbCI6ImFkbWluQG51dGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBw
m9maWxliiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMMSImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdU_kN-
fLWpdJX98HODwPpVUiLcxV28_sQhuopjWobozPe1NISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdsWjWcNvw2rRkfzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGfo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Diese API gibt eine Antwort wie die folgende zurück. Der Wert unter „resourceIdentifier“ bezeichnet die *WorkingEnvironment-ID* und der Wert unter „agentId“ bezeichnet *x-agent-id*.

```
[{"resourceIdentifier": "OnPremWorkingEnvironment-
pMtZND0M", "resourceType": "ON_PREM", "agentId": "vB_1xShPpBtUosjD7wfB1LIhqD
gIPA0wclients", "resourceClass": "ON_PREM", "name": "CBSFAS8300-01-
02", "metadata": "{\"clusterUuid\": \"2cb6cb4b-dc07-11ec-9114-
d039ea931e09\"}", "workspaceIds": ["workspace2wKYjTy9"], "agentIds": ["vB_1x
ShPpBtUosjD7wfB1LIhqDgIPA0wclients"]}]
```

## 3. Aktualisieren Sie die NetApp Backup and Recovery -Datenbank mit den Details des mit den Systemen verknüpften StorageGRID Systems. Stellen Sie sicher, dass Sie den vollqualifizierten Domänennamen des StorageGRID sowie den Zugriffsschlüssel und den Speicherschlüssel wie unten gezeigt eingeben:

```

curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFIZjRiIn0eyJzdWIiOiJvY
2NTYXV0aHwxIiwiYXVkJpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXswiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW11ijo1YWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS91bWFpbCI6ImFkbWluQG51dGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWx1IiwigiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMMSImlzcyI6Imh0dHA6L
y9vY2NTYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdw_kN-
fLWpdJWX98HODwPpVUiLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdsbjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4kr0ewgKHGfo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfB1LIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4Lj1XQOFnzSzP/T0zR4ZQ1G0w1xgWsB" }'

```

## Überprüfen der NetApp Backup and Recovery -Einstellungen

1. Wählen Sie jedes ONTAP -System aus und klicken Sie im rechten Bereich neben dem Sicherungs- und Wiederherstellungsdiensst auf **Sicherungen anzeigen**.  
  
Sie sollten alle für Ihre Volumes erstellten Backups sehen.
2. Klicken Sie im Wiederherstellungs-Dashboard im Abschnitt „Suchen und Wiederherstellen“ auf **Indizierungseinstellungen**.  
  
Stellen Sie sicher, dass die Systeme, bei denen die indizierte Katalogisierung zuvor aktiviert war, aktiviert bleiben.
3. Führen Sie auf der Seite „Suchen und Wiederherstellen“ einige Katalogsuchen durch, um zu bestätigen, dass die Wiederherstellung des indizierten Katalogs erfolgreich abgeschlossen wurde.

## Unterstützte AWS-Archivspeicherebenen mit NetApp Backup and Recovery

NetApp Backup and Recovery unterstützt zwei S3-Archivspeicherklassen und die meisten Regionen.



Informationen zum Wechseln zwischen NetApp Backup and Recovery -UI-Versionen finden Sie unter "["Wechseln Sie zur vorherigen NetApp Backup and Recovery -Benutzeroberfläche"](#)".

## Unterstützte S3-Archivspeicherklassen für NetApp Backup and Recovery

Wenn Sicherungsdateien zunächst erstellt werden, werden sie im S3-Standardspeicher gespeichert. Diese Ebene ist für die Speicherung selten abgerufener Daten optimiert, ermöglicht Ihnen aber auch den sofortigen Zugriff darauf. Nach 30 Tagen werden die Backups aus Kostengründen in die Speicherklasse S3 Standard-*Infrequent Access* verschoben.

Wenn auf Ihren Quellclustern ONTAP 9.10.1 oder höher ausgeführt wird, können Sie zur weiteren Kostenoptimierung Backups nach einer bestimmten Anzahl von Tagen (normalerweise mehr als 30 Tage) entweder auf S3 *Glacier*- oder S3 *Glacier Deep Archive*-Speicher verschieben. Sie können dies auf „0“ oder auf 1–999 Tage einstellen. Wenn Sie es auf „0“ Tage einstellen, können Sie es später nicht auf 1–999 Tage ändern.

Auf die Daten in diesen Ebenen kann bei Bedarf nicht sofort zugegriffen werden und der Abruf ist mit höheren Kosten verbunden. Sie müssen daher berücksichtigen, wie oft Sie Daten aus diesen archivierten Sicherungsdateien wiederherstellen müssen. Weitere Informationen zum Wiederherstellen von Daten aus dem Archivspeicher finden Sie im Abschnitt auf dieser Seite.

- Wenn Sie bei der Aktivierung von NetApp Backup and Recovery in Ihrer ersten Sicherungsrichtlinie keine Archivebene auswählen, ist S3 *Glacier* Ihre einzige Archivierungsoption für zukünftige Richtlinien.
- Wenn Sie in Ihrer ersten Sicherungsrichtlinie S3 *Glacier* auswählen, können Sie für zukünftige Sicherungsrichtlinien für diesen Cluster zur Ebene S3 *Glacier Deep Archive* wechseln.
- Wenn Sie in Ihrer ersten Sicherungsrichtlinie S3 *Glacier Deep Archive* auswählen, ist diese Ebene die einzige Archivebene, die für zukünftige Sicherungsrichtlinien für diesen Cluster verfügbar ist.

Beachten Sie, dass Sie beim Konfigurieren von NetApp Backup and Recovery mit dieser Art von Lebenszyklusregel beim Einrichten des Buckets in Ihrem AWS-Konto keine Lebenszyklusregeln konfigurieren dürfen.

["Erfahren Sie mehr über S3-Speicherklassen".](#)

## Daten aus dem Archivspeicher wiederherstellen

Während die Speicherung älterer Sicherungsdateien im Archivspeicher wesentlich weniger kostspielig ist als die Speicherung im Standard- oder Standard-IA-Speicher, dauert der Zugriff auf Daten aus einer Sicherungsdatei im Archivspeicher für Wiederherstellungsvorgänge länger und ist teurer.

### Wie viel kostet die Wiederherstellung von Daten aus Amazon S3 Glacier und Amazon S3 Glacier Deep Archive?

Beim Abrufen von Daten aus Amazon S3 *Glacier* können Sie zwischen 3 Wiederherstellungsrioritäten und beim Abrufen von Daten aus Amazon S3 *Glacier Deep Archive* zwischen 2 Wiederherstellungsrioritäten wählen. S3 *Glacier Deep Archive* kostet weniger als S3 *Glacier*:

Archivebene	Wiederherstellungsriorität und -kosten		
	Hoch	Standard	Niedrig

Archivebene	Wiederherstellungsriorität und -kosten		
S3 Gletscher	Schnellster Abruf, höchste Kosten	Langsamere Abfrage, geringere Kosten	Langsamster Abruf, niedrigste Kosten
S3 Glacier Deep-Archiv		Schnellere Abfrage, höhere Kosten	Langsamerer Abruf, niedrigste Kosten

Für jede Methode fallen unterschiedliche Abruf- und Anforderungsgebühren pro GB an. Detaillierte S3 Glacier-Preise nach AWS-Region finden Sie auf der "[Amazon S3-Preisseite](#)" .

#### Wie lange dauert die Wiederherstellung meiner in Amazon S3 Glacier archivierten Objekte?

Die gesamte Wiederherstellungszeit besteht aus zwei Teilen:

- **Abrufzeit:** Die Zeit, die zum Abrufen der Sicherungsdatei aus dem Archiv und zum Platzieren im Standardspeicher benötigt wird. Dies wird manchmal als „Rehydratationszeit“ bezeichnet. Die Abrufzeit ist je nach gewählter Wiederherstellungsriorität unterschiedlich.

Archivebene	Wiederherstellungsriorität und Abrufzeit		
	Hoch	Standard	Niedrig
S3 Gletscher	3-5 Minuten	3-5 Stunden	5-12 Stunden
S3 Glacier Deep-Archiv		12 Stunden	48 Stunden

- **Wiederherstellungszeit:** Die Zeit, die zum Wiederherstellen der Daten aus der Sicherungsdatei im Standardspeicher benötigt wird. Diese Zeit unterscheidet sich nicht von der typischen Wiederherstellungsoperation direkt vom Standardspeicher – wenn keine Archivierungsebene verwendet wird.

Weitere Informationen zu den Abrufoptionen von Amazon S3 Glacier und S3 Glacier Deep Archive finden Sie unter "[die Amazon FAQ zu diesen Lagerklassen](#)" .

## Unterstützte Azure-Archivzugriffsebenen mit NetApp Backup and Recovery

NetApp Backup and Recovery unterstützt eine Azure-Archivzugriffsebene und die meisten Regionen.



Informationen zum Wechseln zwischen NetApp Backup and Recovery -UI-Versionen finden Sie unter "[Wechseln Sie zur vorherigen NetApp Backup and Recovery -Benutzeroberfläche](#)" .

## Unterstützte Azure Blob-Zugriffsebenen für NetApp Backup and Recovery

Wenn Sicherungsdateien zunächst erstellt werden, werden sie in der Zugriffsebene *Cool* gespeichert. Diese Ebene ist für die Speicherung von Daten optimiert, auf die selten zugegriffen wird, auf die bei Bedarf jedoch sofort zugegriffen werden kann.

Wenn auf Ihren Quellclustern ONTAP 9.10.1 oder höher ausgeführt wird, können Sie zur weiteren

Kostenoptimierung Backups nach einer bestimmten Anzahl von Tagen (normalerweise mehr als 30 Tage) vom Cool- in den Azure Archive-Speicher verschieben. Auf Daten dieser Ebene kann bei Bedarf nicht sofort zugegriffen werden und der Abruf ist mit höheren Kosten verbunden. Sie müssen daher berücksichtigen, wie oft Sie Daten aus diesen archivierten Sicherungsdateien wiederherstellen müssen. Weitere Informationen zum Wiederherstellen von Daten aus dem Archivspeicher finden Sie im Abschnitt auf dieser Seite.

Beachten Sie, dass Sie beim Konfigurieren von NetApp Backup and Recovery mit dieser Art von Lebenszyklusregel beim Einrichten des Containers in Ihrem Azure-Konto keine Lebenszyklusregeln konfigurieren dürfen.

["Informationen zu Azure Blob-Zugriffsebenen".](#)

## Daten aus dem Archivspeicher wiederherstellen

Während das Speichern älterer Sicherungsdateien im Archivspeicher wesentlich weniger kostspielig ist als die Speicherung im Cool-Speicher, dauert der Zugriff auf Daten aus einer Sicherungsdatei im Azure-Archiv für Wiederherstellungsvorgänge länger und ist teurer.

### Wie viel kostet die Wiederherstellung von Daten aus Azure Archive?

Beim Abrufen von Daten aus dem Azure-Archiv können Sie zwischen zwei Wiederherstellungsrioritäten wählen:

- **Hoch:** Schnellster Abruf, höhere Kosten
- **Standard:** Langsamerer Abruf, geringere Kosten

Für jede Methode fallen unterschiedliche Abruf- und Anforderungsgebühren pro GB an. Detaillierte Azure Archive-Preise nach Azure-Region finden Sie auf der ["Azure-Preisseite"](#).



Die hohe Priorität wird beim Wiederherstellen von Daten von Azure auf StorageGRID-Systemen nicht unterstützt.

### Wie lange dauert die Wiederherstellung meiner im Azure-Archiv archivierten Daten?

Die Wiederherstellungszeit besteht aus zwei Teilen:

- **Abrufzeit:** Die Zeit, die zum Abrufen der archivierten Sicherungsdatei aus dem Azure-Archiv und zum Platzieren im Cool-Speicher benötigt wird. Dies wird manchmal als „Rehydratationszeit“ bezeichnet. Die Abrufzeit ist je nach gewählter Wiederherstellungsriorität unterschiedlich:
  - **Hoch:** < 1 Stunde
  - **Standard:** < 15 Stunden
- **Wiederherstellungszeit:** Die Zeit zum Wiederherstellen der Daten aus der Sicherungsdatei im Cool-Speicher. Diese Zeit unterscheidet sich nicht von der typischen Wiederherstellungsoperation direkt aus dem Cool-Speicher – wenn keine Archivierungsebene verwendet wird.

Weitere Informationen zu den Abrufoptionen für Azure-Archive finden Sie unter ["diese Azure-FAQ"](#).

## Unterstützte Google-Archivspeicherebenen mit NetApp Backup and Recovery

NetApp Backup and Recovery unterstützt eine Archivspeicherklasse von Google und die meisten Regionen.



Informationen zum Wechseln zwischen NetApp Backup and Recovery -UI-Versionen finden Sie unter "["Wechseln Sie zur vorherigen NetApp Backup and Recovery -Benutzeroberfläche"](#)".

## Unterstützte Google-Archivspeicherklassen für NetApp Backup and Recovery

Wenn Sicherungsdateien zunächst erstellt werden, werden sie im *Standard*-Speicher gespeichert. Diese Ebene ist für die Speicherung selten abgerufener Daten optimiert, ermöglicht Ihnen aber auch den sofortigen Zugriff darauf.

Wenn Ihr Cluster vor Ort ONTAP 9.12.1 oder höher verwendet, können Sie zur weiteren Kostenoptimierung in der NetApp Backup and Recovery Benutzeroberfläche ältere Backups nach einer bestimmten Anzahl von Tagen (normalerweise mehr als 30 Tage) in den Archivspeicher verschieben. Für die Datenabfrage in dieser Ebene fallen höhere Kosten an. Sie müssen daher berücksichtigen, wie oft Sie Daten aus diesen archivierten Sicherungsdateien wiederherstellen müssen. Weitere Informationen zum Wiederherstellen von Daten aus dem Archivspeicher finden Sie im Abschnitt auf dieser Seite.

Beachten Sie, dass Sie beim Konfigurieren von NetApp Backup and Recovery mit dieser Art von Lebenszyklusregel beim Einrichten des Buckets in Ihrem Google-Konto keine Lebenszyklusregeln konfigurieren dürfen.

["Informationen zu Google-Speicherklassen".](#)

## Daten aus dem Archivspeicher wiederherstellen

Während die Speicherung älterer Sicherungsdateien im Archivspeicher wesentlich günstiger ist als die Speicherung im Standardspeicher, dauert der Zugriff auf Daten aus einer Sicherungsdatei im Archivspeicher für Wiederherstellungsvorgänge etwas länger und ist teurer.

### Wie viel kostet die Wiederherstellung von Daten aus dem Google-Archiv?

Detaillierte Preise für Google Cloud Storage nach Regionen finden Sie auf der ["Preisseite für Google Cloud Storage"](#).

### Wie lange dauert die Wiederherstellung meiner im Google-Archiv archivierten Objekte?

Die gesamte Wiederherstellungszeit besteht aus zwei Teilen:

- **Abrufzeit:** Die Zeit, die zum Abrufen der Sicherungsdatei aus dem Archiv und zum Platzieren im Standardspeicher benötigt wird. Dies wird manchmal als „Rehydratationszeit“ bezeichnet. Im Gegensatz zu den „kältesten“ Speicherlösungen anderer Cloud-Anbieter sind Ihre Daten innerhalb von Millisekunden zugänglich.
- **Wiederherstellungszeit:** Die Zeit, die zum Wiederherstellen der Daten aus der Sicherungsdatei im Standardspeicher benötigt wird. Diese Zeit unterscheidet sich nicht von der typischen Wiederherstellungsoperation direkt vom Standardspeicher – wenn keine Archivierungsebene verwendet wird.

## **Copyright-Informationen**

Copyright © 2026 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 BESCHRÄNKKT 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 BESCHRÄNKKT 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 IRGENDERWEINER 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.