Referenz

BlueXP backup and recovery

NetApp
April 18, 2024

Inhalt

Referenz

AWS S3-Archiv-Storage-Klassen und Restore Abrufzeiten

BlueXP Backup und Recovery unterstützt zwei S3 Archiv-Storage-Klassen und die meisten Regionen.

Unterstützte S3 Archiv-Storage-Klassen für BlueXP Backup und Recovery

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. Sie können dies auf „0“ oder auf 1-999 Tage einstellen. Wenn Sie den Wert auf „0“ Tage setzen, können Sie ihn später nicht mehr in 1-999 Tage ändern.

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 BlueXP Backup und Recovery in Ihrer ersten Backup-Richtlinie keinen Archiv-Tier auswählen, wird *S3 Glacier* Ihre einzige Archivierungsoption für zukünftige Richtlinien sein.
- Wenn Sie in Ihrer ersten Backup-Richtlinie *S3 Glacier* auswählen, können Sie für zukünftige Backup-Richtlinien für diesen Cluster in die *S3 Glacier Deep Archive*-Ebene wechseln.
- Wenn Sie in Ihrer ersten Backup-Richtlinie *S3 Glacier Deep Archive* auswählen, ist diese Tier die einzige Archiv-Tier, die für zukünftige Backup-Richtlinien für diesen Cluster verfügbar ist.

Wenn Sie BlueXP Backup und Recovery mit dieser Lebenszyklusregel konfigurieren, dürfen Sie beim Einrichten des Buckets in Ihrem AWS-Konto keine Lebenszyklusregeln 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

Archivebene	Priorität Und Kosten Wiederherstellen		
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

BlueXP Backup und Recovery unterstützt nur eine Azure Zugriffsebene für Archivierung und in den meisten Regionen.

Unterstützte Azure Blob-Zugriffs-Tiers für Backup und Recovery von BlueXP

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.

Wenn Sie BlueXP Backup und Recovery mit dieser Lebenszyklusregel konfigurieren, dürfen Sie beim Einrichten des Containers in Ihrem Azure-Konto keine Lebenszyklusregeln konfigurieren.

"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".

> Die hohe Priorität wird nicht unterstützt, wenn Daten von Azure auf StorageGRID-Systeme wiederhergestellt werden.

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

BlueXP Backup und Recovery unterstützen eine einzige Google Archiv-Storage-Klasse und die meisten Regionen.

Unterstützte Google Archiv-Storage-Klassen für BlueXP Backup und Recovery

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-Premises-Cluster ONTAP 9.12.1 oder höher verwendet, können Sie nach einer bestimmten Anzahl von Tagen (in der Regel länger als 30 Tage) ältere Backups in den *Archiv* Storage in der BlueXP Backup- und Recovery-UI verschieben, um weitere Kosten zu optimieren. 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 BlueXP Backup und Recovery 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

Mit BlueXP Backup und Recovery können Sie Backup-Dateien in einem Azure Konto erstellen, das sich von dem unterscheidet, wo sich Ihre Cloud Volumes ONTAP Quell-Volumes befinden. Beide Konten können unterschiedlich sein, als das Konto, bei dem sich der BlueXP Connector befindet.

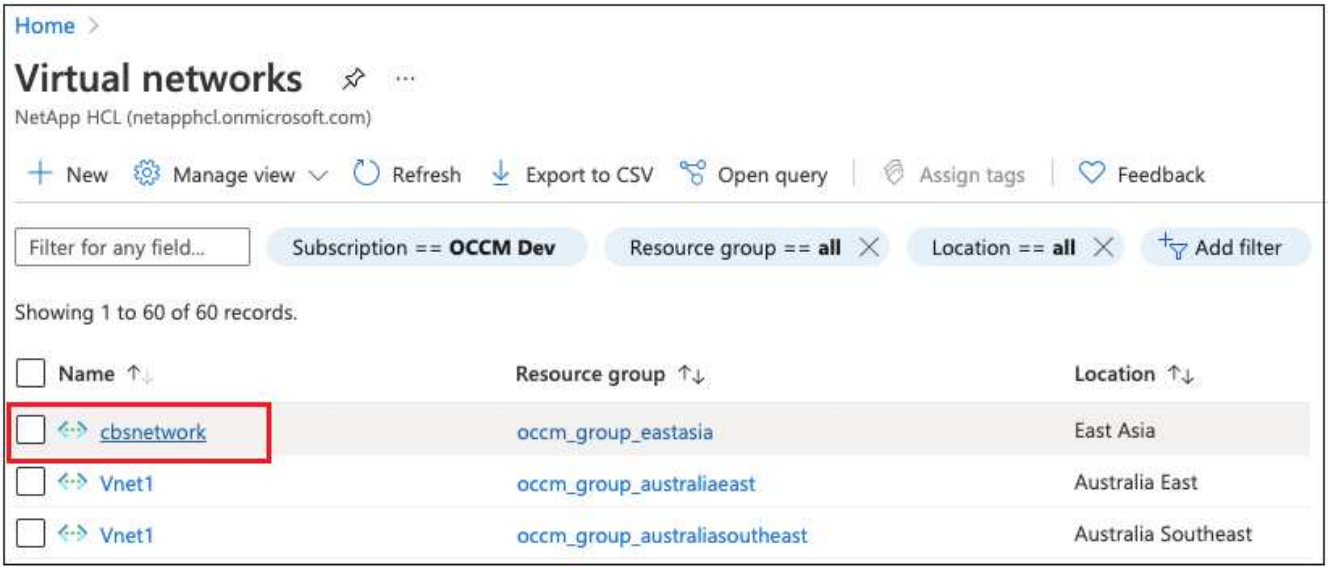
Diese Schritte sind nur erforderlich, wenn Sie sich befinden "Sichern von Cloud Volumes ONTAP-Daten auf Azure Blob Storage".

Befolgen Sie einfach die nachstehenden Schritte, um Ihre Konfiguration auf diese Weise einzurichten.

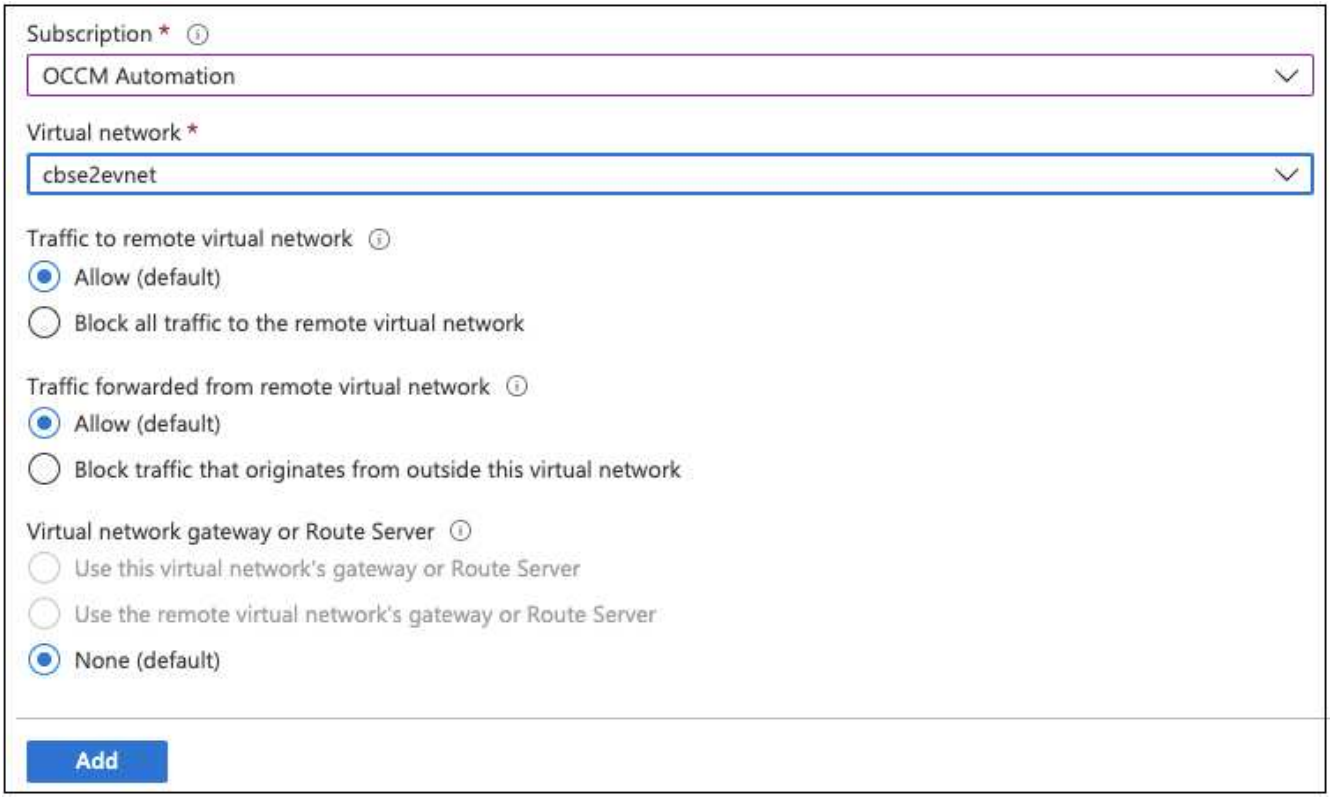
Vnet-Peering zwischen Konten einrichten

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.

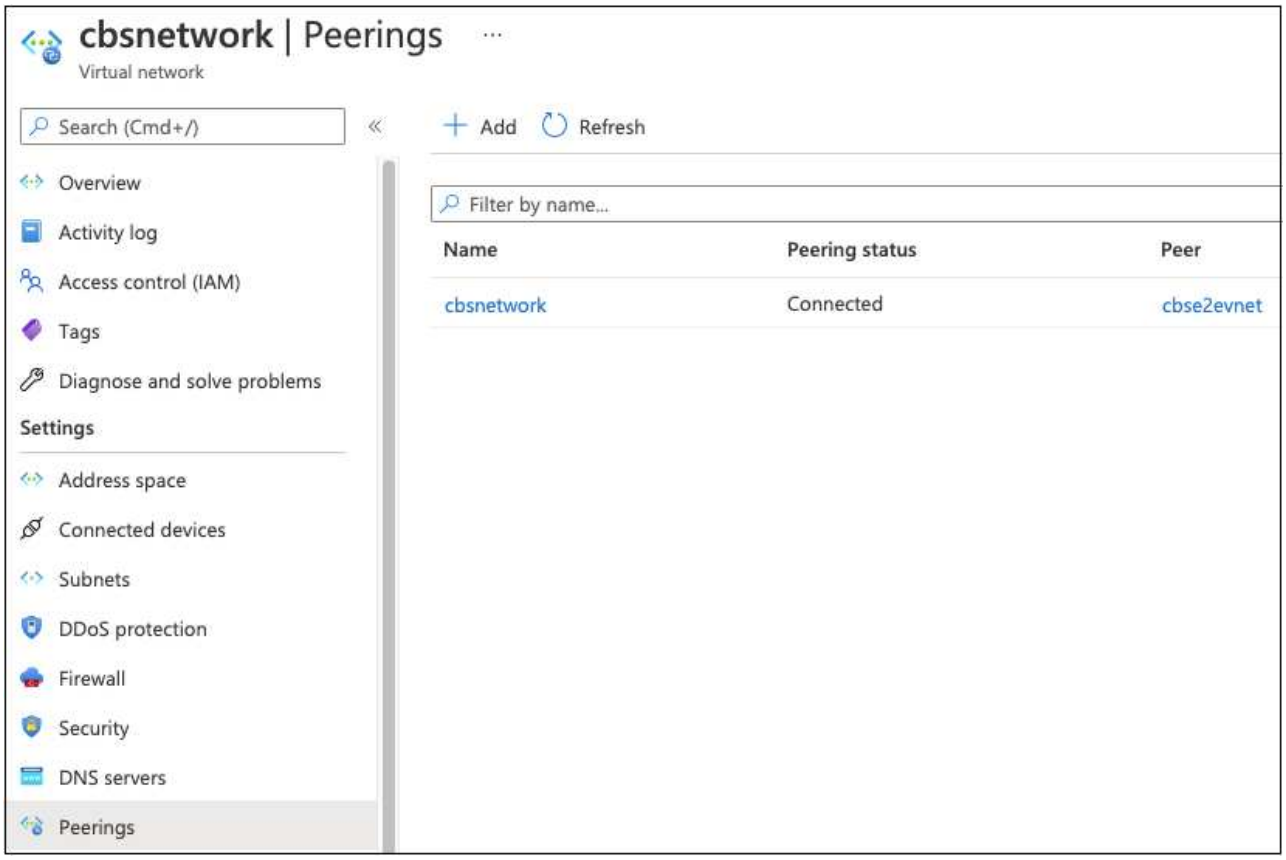


3. Wählen Sie **cbsnetzwerk** und klicken Sie im linken Bereich auf **Peerings** und dann auf **Add**.

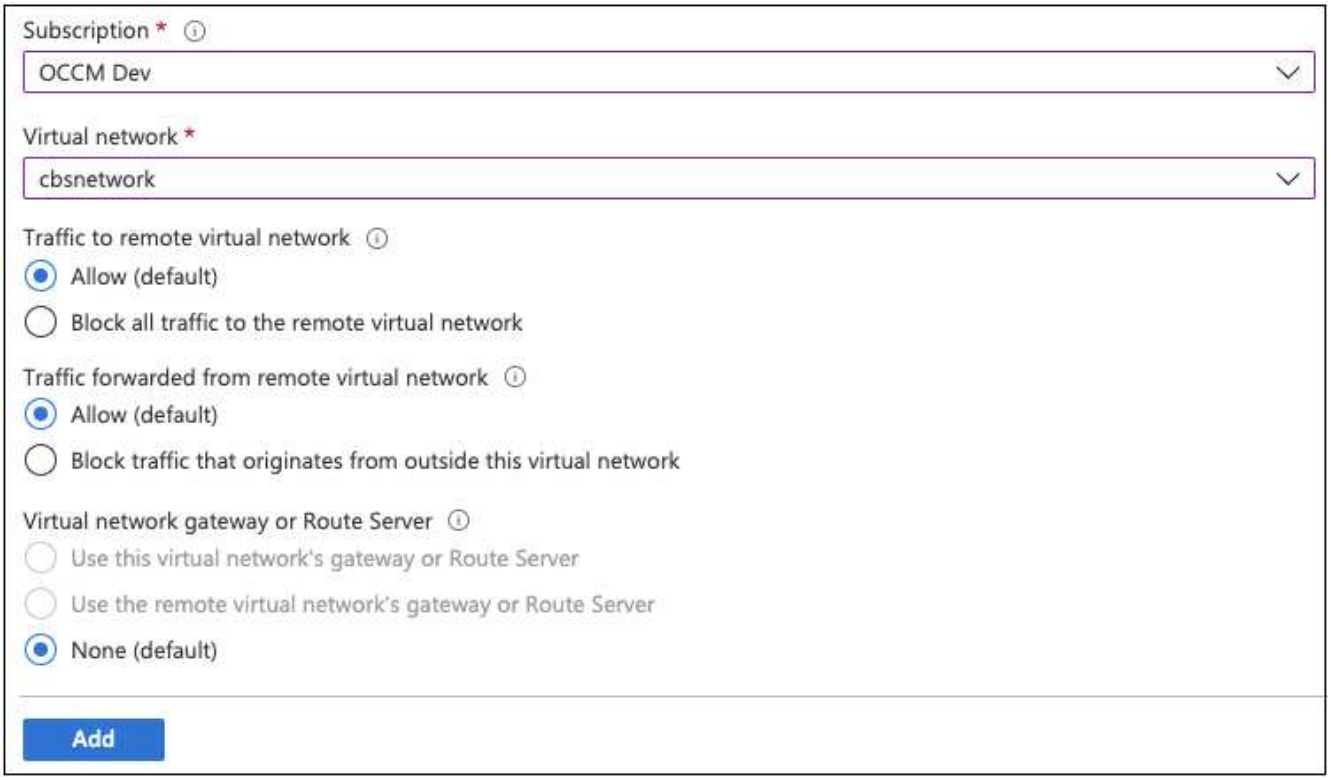


4. Geben Sie die folgenden Informationen auf der Peering-Seite ein und klicken Sie dann auf **Hinzufügen**.
   - Peering-Linkname für dieses Netzwerk: Sie können einen beliebigen Namen angeben, um die Peering-Verbindung zu identifizieren.
   - Remote Virtual Network Peering Linkname: Geben Sie einen 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

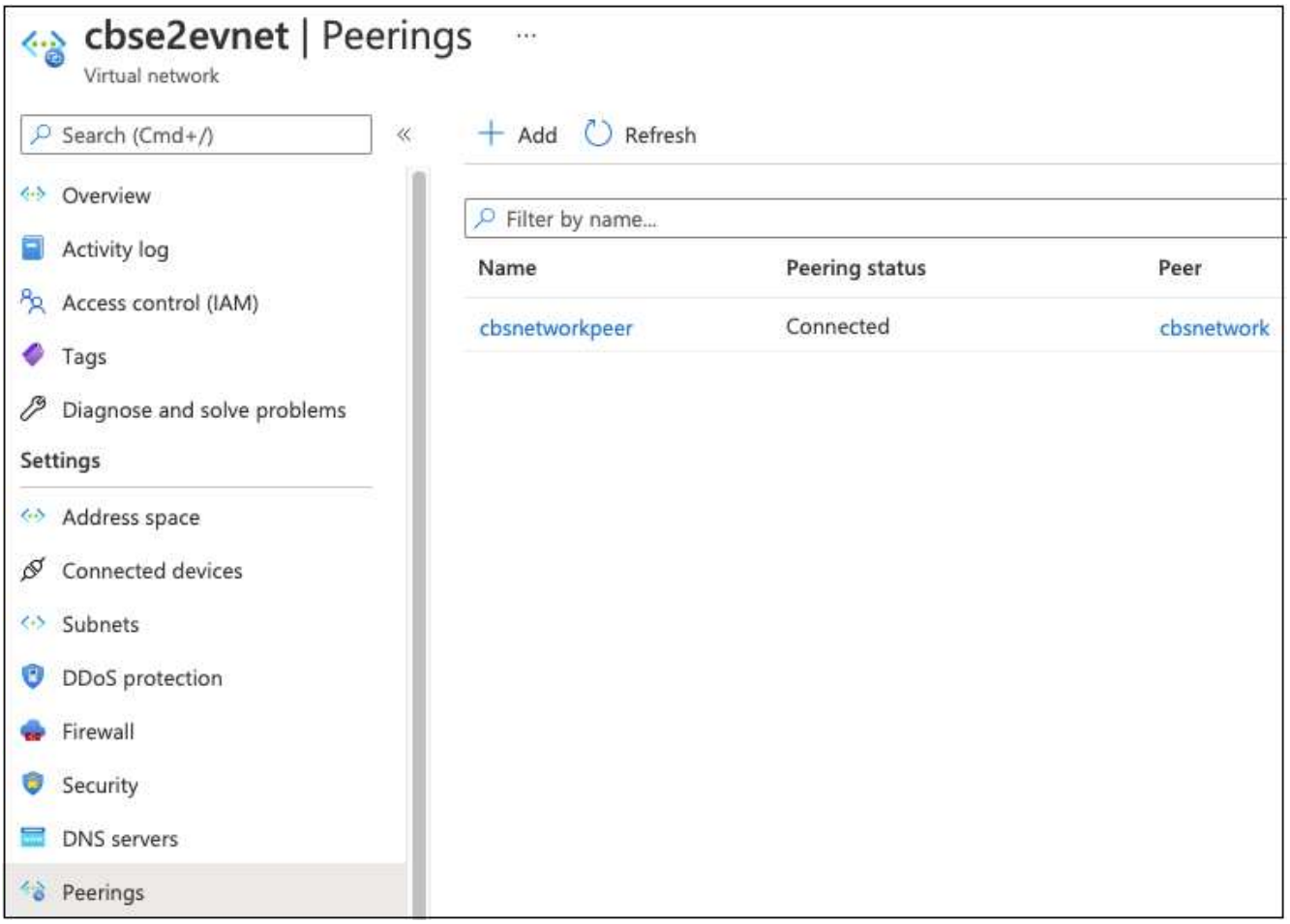
möchten.



5. Führen Sie die gleichen Schritte in Subskription 2 vnet aus und geben Sie die Abonnement- und Remote vnet-Details von Abo 1 an.



Die Peering-Einstellungen werden hinzugefügt.



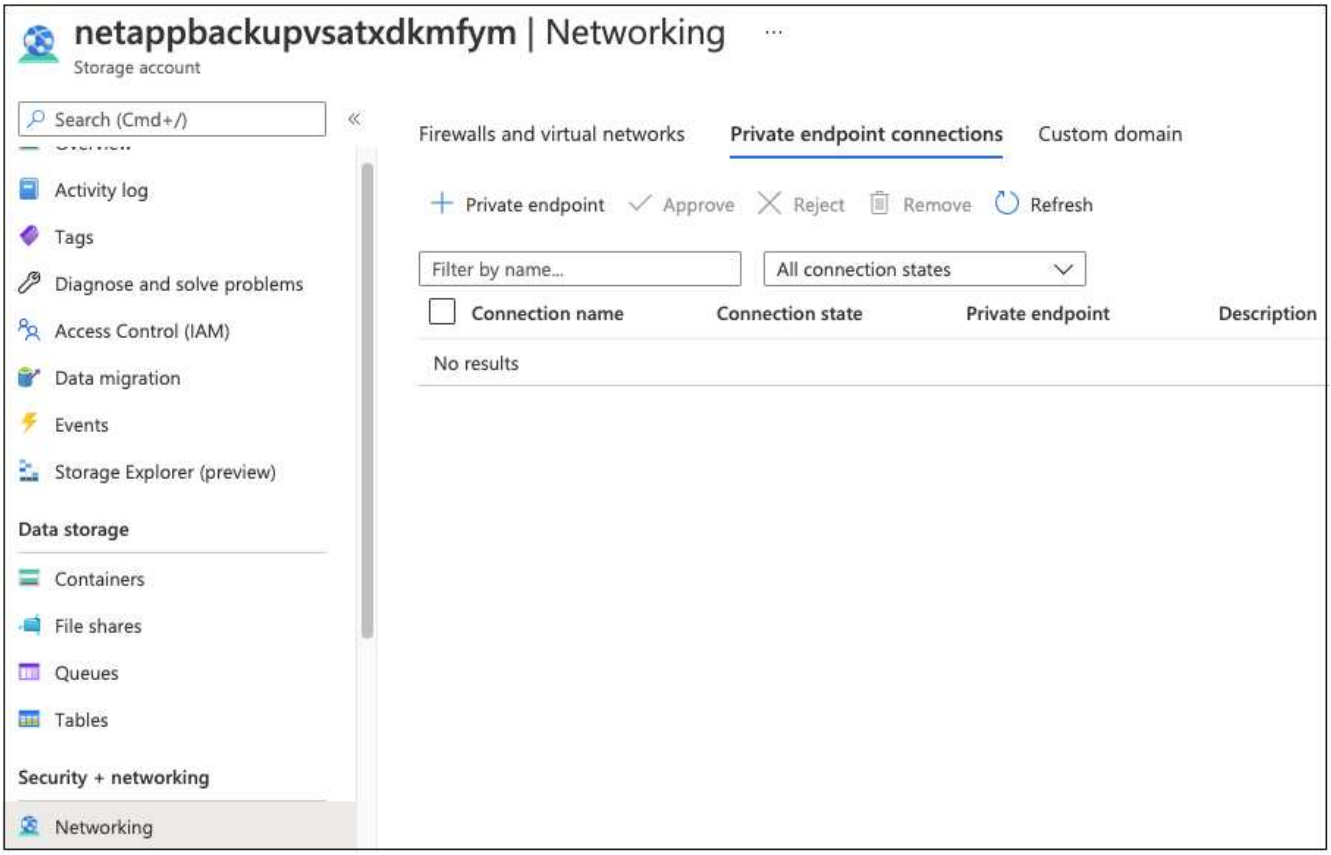
Erstellen eines privaten Endpunkts für das Storage-Konto

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.

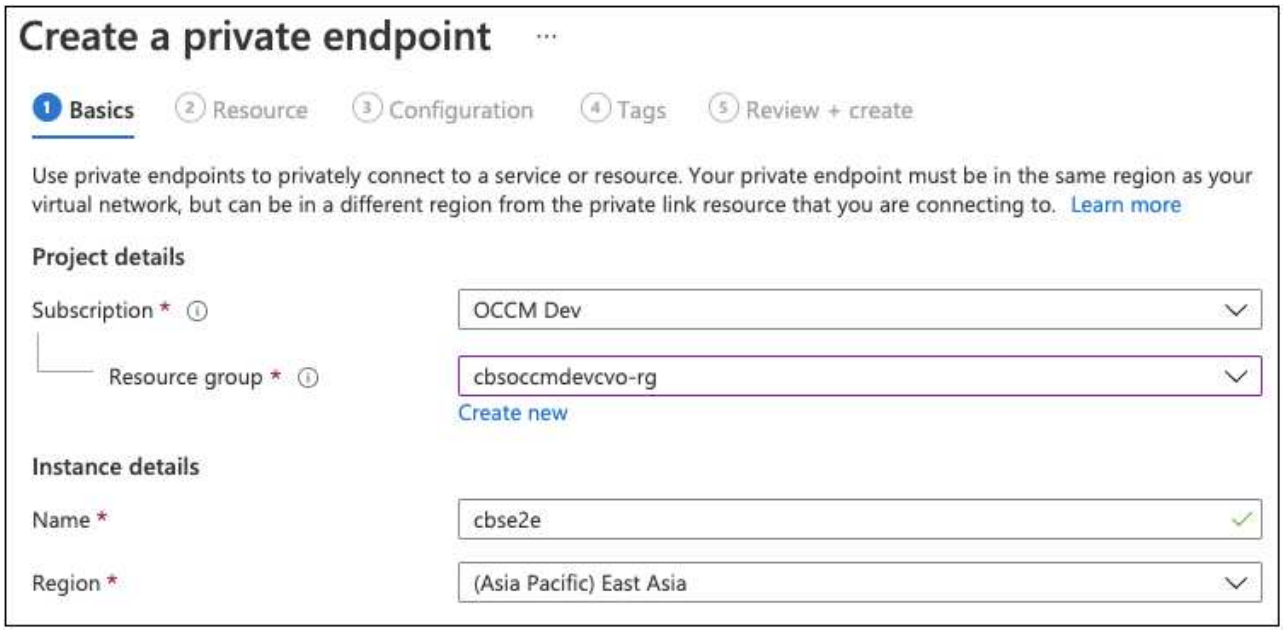
Sie benötigen die Berechtigung von Netzwerkbeitragenden, um die folgende Aktion auszuführen.

```
{
  "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": []
      }
    ]
  }
}
```

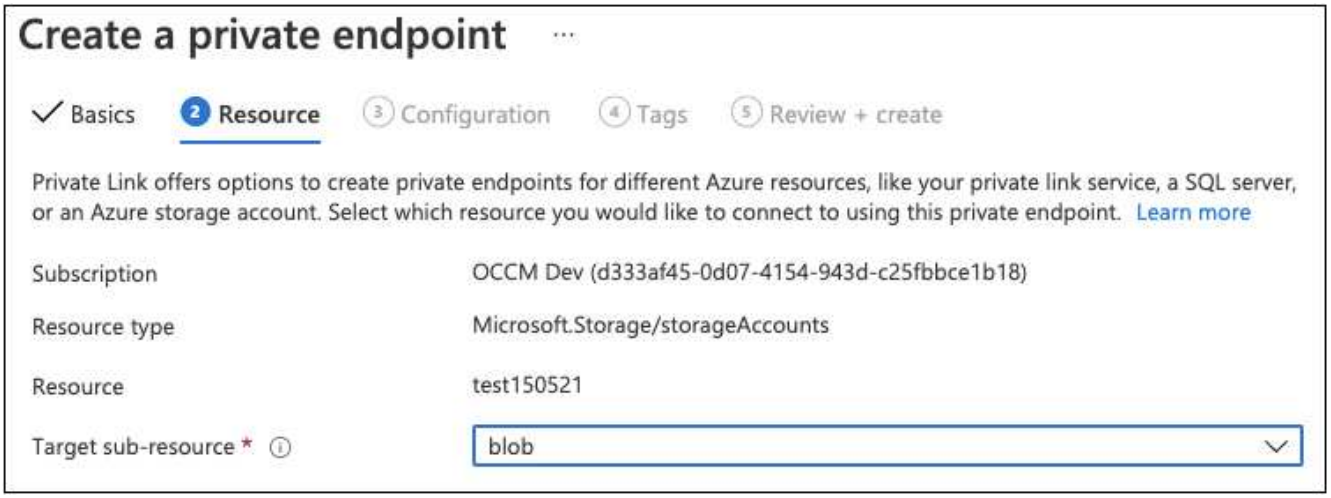
1. Wechseln Sie zum Storage-Konto > Netzwerk > Private Endpunktverbindungen, und klicken Sie auf **+ Private Endpunktverbindungen**.



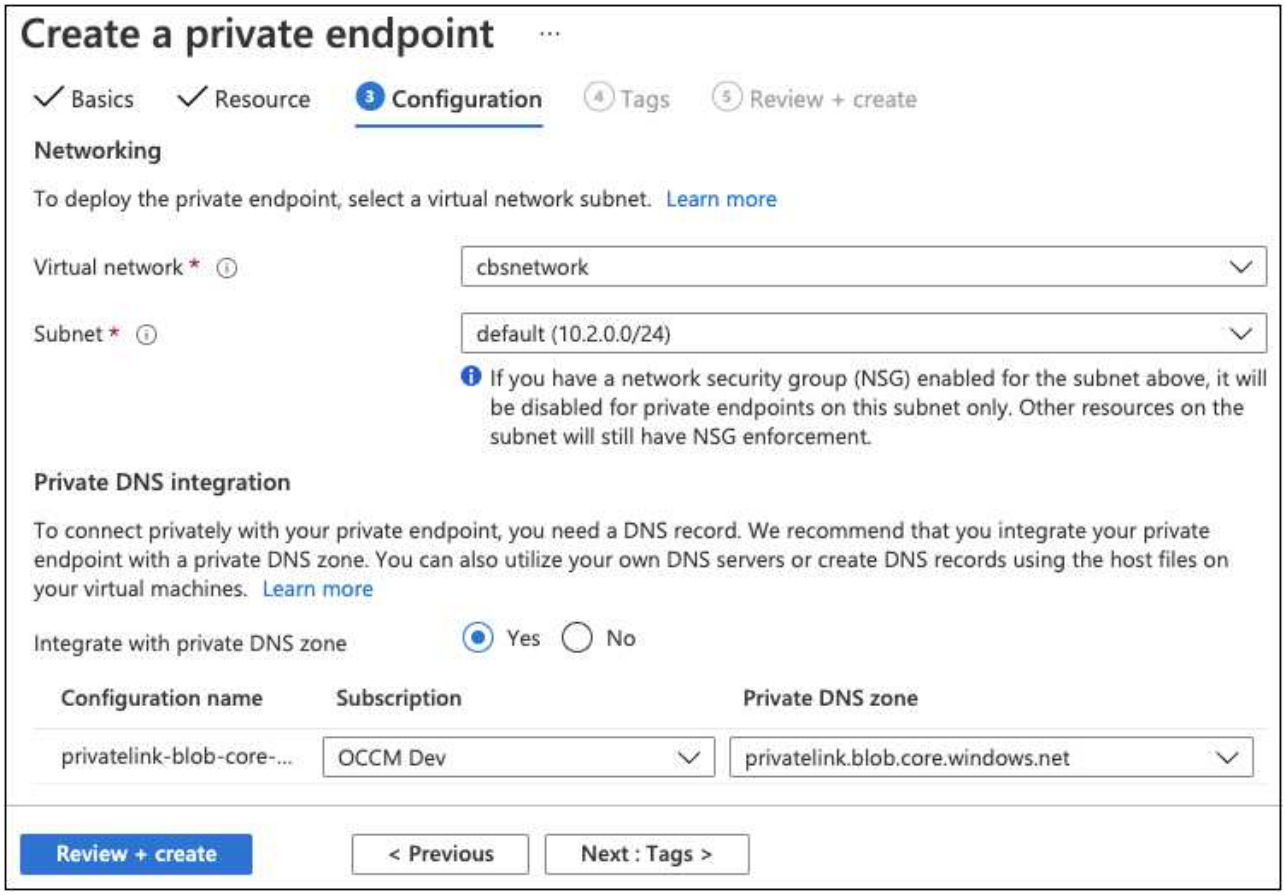
2. Auf der Seite Private Endpoint_Basics_:
   - Wählen Sie Subskription 2 (wo BlueXP Connector und Cloud Volumes ONTAP System bereitgestellt werden) und die Ressourcengruppe aus.
   - Geben Sie einen Endpunktnamen ein.
   - Wählen Sie die Region aus.



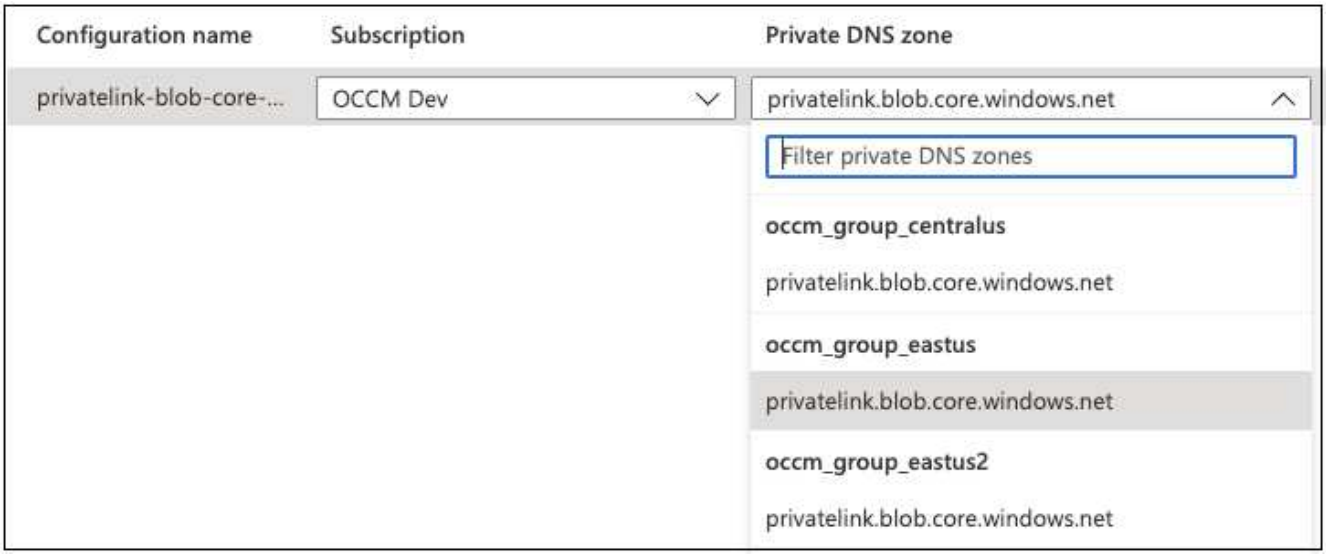
3. Wählen Sie auf der Seite *Ressource* die Unterressource Ziel als **Blob** aus.



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, BlueXP Backup und Recovery auf dem Cloud Volumes ONTAP System zu aktivieren. Dies sollte diesmal erfolgreich sein.

Stellen Sie BlueXP Backup- und Recovery-Daten an einem dunklen Standort wieder her

Wenn Sie BlueXP Backup und Recovery an einem Standort ohne Internetzugang nutzen, den sogenannten *Private Mode*, werden die Backup- und Recovery-Konfigurationsdaten von BlueXP auf den StorageGRID oder ONTAP S3 Bucket gesichert, auf dem die Backups gespeichert werden. Wenn Sie in Zukunft Probleme mit dem BlueXP Connector-Host-System haben, können Sie einen neuen Connector implementieren und die kritischen BlueXP Backup- und Recovery-Daten wiederherstellen.

Beachten Sie, dass wenn Sie BlueXP Backup und Recovery in einer SaaS-Umgebung nutzen, bei der BlueXP Connector bei Ihrem Cloud-Provider oder in Ihrem eigenen Host-System mit Internetzugang implementiert wird, alle wichtigen BlueXP Backup- und Recovery-Konfigurationsdaten gesichert und in der Cloud gesichert werden. Wenn Sie ein Problem mit dem Connector haben, erstellen Sie einfach einen neuen Connector und fügen Sie Ihre Arbeitsumgebungen hinzu. Die Sicherungsdetails werden automatisch wiederhergestellt.

Es gibt 2 Arten von Daten, die gesichert werden:

- BlueXP Backup- und Recovery-Datenbank – enthält eine Liste aller Volumes, Backup-Dateien, Backup-Richtlinien und Konfigurationsinformationen.
- Indizierte Katalogdateien – enthält detaillierte Indizes, die für die Such- und Wiederherstellungsfunktion verwendet werden, sodass Ihre Suchvorgänge sehr schnell und effizient bei der Suche nach Volume-Daten, die Sie wiederherstellen möchten, durchgeführt werden.

Diese Daten werden einmal am Tag um Mitternacht gesichert und maximal 7 Kopien jeder Datei werden aufbewahrt. Wenn der Connector mehrere lokale ONTAP-Arbeitsumgebungen managt, befinden sich die Backup- und Recovery-Dateien von BlueXP im Bucket der Arbeitsumgebung, die zuerst aktiviert wurde.

In der BlueXP Backup- und Recovery-Datenbank oder den indizierten Katalogdateien werden keine Volume-Daten jemals enthalten sein.

Wiederherstellung von BlueXP Backup- und Recovery-Daten in einem neuen Connector

Wenn Ihr lokaler Connector bei einem schwerwiegenden Ausfall auftritt, müssen Sie einen neuen Connector installieren und anschließend die BlueXP Backup- und Recovery-Daten im neuen Connector wiederherstellen.

Es gibt 4 Aufgaben, die Sie durchführen müssen, um den Betriebszustand Ihres BlueXP Backup- und Recovery-Systems wiederherzustellen:

- Installieren Sie einen neuen BlueXP Connector
- Wiederherstellung der BlueXP Backup- und Recovery-Datenbank
- Stellen Sie die indizierten Katalogdateien wieder her
- Alle On-Prem-ONTAP-Systeme und StorageGRID-Systeme finden Sie in der BlueXP-Benutzeroberfläche wieder

Sobald Sie überprüfen, ob Ihr System wieder in einem Arbeitsauftrag ist, empfehlen wir Ihnen, neue Sicherungsdateien zu erstellen.

Was Sie benötigen

Sie müssen über den StorageGRID oder ONTAP S3 Bucket auf die neuesten Datenbank- und Index-Backups zugreifen, in denen Ihre Backup-Dateien gespeichert werden:

- BlueXP Backup und Recovery der MySQL-Datenbankdatei

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

- ZIP-Datei für die Sicherung des indizierten Katalogs

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

Installieren Sie einen neuen Konnektor auf einem neuen lokalen Linux-Host

Wenn Sie einen neuen BlueXP Connector installieren, stellen Sie sicher, dass Sie die gleiche Version von Software herunterladen, die Sie auf dem ursprünglichen Connector installiert hatten. Regelmäßige Änderungen an der BlueXP Datenbank-Struktur für Backup und Recovery führen möglicherweise dazu, dass neuere Software-Versionen mit den ursprünglichen Datenbank-Backups nicht kompatibel sind. Das können Sie "Aktualisieren Sie die Connector-Software auf die aktuellste Version, nachdem Sie die Backup-Datenbank wiederhergestellt haben".

1. "Installieren Sie den BlueXP Connector auf einem neuen lokalen Linux-Host"
2. Melden Sie sich mit den soeben erstellten Admin-Benutzeranmeldeinformationen bei BlueXP an.

Wiederherstellung der BlueXP Backup- und Recovery-Datenbank

1. Kopieren Sie das MySQL-Backup vom Backup-Speicherort auf den neuen Connector-Host. Wir verwenden

unten den Beispieldateinamen „CBS_DB_Backup_23_05_2023.sql“.

2. Kopieren Sie das Backup mit dem folgenden Befehl in den MySQL-Docker-Container:

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

3. Geben Sie die MySQL-Container-Shell mithilfe des folgenden Befehls ein:

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

4. In der Container-Shell, stellen Sie die "env".
5. Sie benötigen das MySQL DB Passwort, kopieren Sie also den Wert des Schlüssels "MYSQL_ROOT_PASSWORD".
6. Stellen Sie die BlueXP Backup und Recovery MySQL DB mit folgendem 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 BlueXP Backup- und Recovery-MySQL DB korrekt wiederhergestellt wurde:

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

Geben Sie das Passwort ein.

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

Überprüfen Sie, ob die angezeigten Volumen dieselben sind wie die in Ihrer ursprünglichen Umgebung.

Stellen Sie die indizierten Katalogdateien wieder her

1. Kopieren Sie die ZIP-Datei mit dem indizierten Katalog (wir verwenden den Beispieldateinamen „indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip“) vom Sicherungsverzeichnis auf den neuen Connector-Host im Ordner „/opt/Application/netapp/cbs“.
2. Entpacken Sie die Datei „indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip“ mit folgendem 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 Unterordnern "changes" und "catalogs" darunter angelegt wurde.

Erkennen Sie Ihre ONTAP Cluster und StorageGRID Systeme

1. "Hier finden Sie alle On-Premises-ONTAP-Arbeitsumgebungen" Die in Ihrer vorherigen Umgebung verfügbar waren. Dazu gehört auch das ONTAP-System, das Sie als S3-Server genutzt haben.
2. "Erkennen Sie Ihre StorageGRID Systeme".

Richten Sie die Details zur StorageGRID Umgebung ein

Fügen Sie die Details des StorageGRID-Systems zu Ihren ONTAP-Arbeitsumgebungen hinzu, da diese auf dem ursprünglichen Konnektor-Setup mithilfe der eingerichtet wurden "BlueXP APIs".

Sie müssen diese Schritte für jedes ONTAP System durchführen, das Daten in StorageGRID sichert.

1. Extrahieren Sie das Autorisierungs-Token mithilfe der folgenden oauth/Token-API.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'User-Agent:
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:100101 Firefox/108.0'
-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":"pass
word"}
> '
```

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


```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```


2. Extrahieren Sie die ID der Arbeitsumgebung 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
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Diese API gibt eine Antwort wie die folgende zurück. Der Wert unter der "resourceIdentifier" bezeichnet die *WorkingEnvironment ID* und der Wert unter "AGENTID" bezeichnet *x-Agent-id*.

3. Aktualisieren Sie die BlueXP Backup- und Recovery-Datenbank mit den Details des StorageGRID Systems, das den Arbeitsumgebungen zugeordnet ist. Stellen Sie sicher, dass Sie den vollständig qualifizierten Domänennamen der StorageGRID sowie den Zugriffsschlüssel und den Speicherschlüssel wie unten dargestellt 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
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

Überprüfen Sie die Backup- und Recovery-Einstellungen von BlueXP

1. Wählen Sie jede ONTAP Arbeitsumgebung aus und klicken Sie auf **Backups anzeigen** neben dem Backup- und Recovery-Service im rechten Fenster.

   Sie sollten in der Lage sein alle Backups zu sehen, die für Ihre Volumes erstellt wurden.

2. Klicken Sie im Dashboard wiederherstellen im Abschnitt Suchen & Wiederherstellen auf **Indexing-Einstellungen**.

   Stellen Sie sicher, dass die Arbeitsumgebungen, in denen die Indexierung bereits aktiviert war, zuvor aktiviert bleiben.

3. Führen Sie auf der Seite Suchen & Wiederherstellen einige Katalogsuchen aus, um zu bestätigen, dass die Wiederherstellung des indizierten Katalogs erfolgreich abgeschlossen wurde.

Starten Sie den BlueXP Backup- und Recovery-Service neu

Unter bestimmten Umständen muss der BlueXP Backup- und Recovery-Service neu gestartet werden.

Die Backup- und Recovery-Funktionen von BlueXP sind in den BlueXP Connector integriert. Sie müssen verschiedene erste Schritte ausführen, um den Dienst neu zu starten, je nachdem, ob Sie den Connector in der Cloud bereitgestellt haben oder ob Sie den Connector manuell auf einem Linux-System installiert haben.

Schritte

1. Stellen Sie eine Verbindung zum Linux-System her, auf dem der Connector ausgeführt wird.

Position des Steckers	Verfahren
Cloud-Implementierung	Befolgen Sie die Anweisungen für "Verbindung mit der virtuellen Connector Linux-Maschine herstellen" Je nachdem, welchen Cloud-Provider Sie verwenden.
Manuelle Installation	Melden Sie sich beim Linux-System an.

2. Geben Sie den Befehl ein, um den Service neu zu starten.

Position des Steckers	Befehl
Cloud-Implementierung	`docker restart cloudmanager_cbs`
Manuelle Installation mit Internetzugang	`docker restart cloudmanager_cbs`
Manuelle Installation ohne Internetzugang	`docker restart ds_cloudmanager_cbs_1`