Riferimento

BlueXP backup and recovery

NetApp
April 18, 2024

Sommario

Riferimento

Classi di storage di archivio AWS S3 e tempi di recupero del ripristino

Il backup e ripristino BlueXP supporta due classi di storage di archiviazione S3 e la maggior parte delle regioni.

Classi di storage di archiviazione S3 supportate per backup e ripristino BlueXP

Quando i file di backup vengono creati inizialmente, vengono memorizzati nello storage S3 *Standard*. Questo Tier è ottimizzato per l'archiviazione dei dati a cui si accede raramente, ma che consente anche di accedervi immediatamente. Dopo 30 giorni, i backup passano alla classe di storage S3 *Standard-infrequent Access* per risparmiare sui costi.

Se i cluster di origine eseguono ONTAP 9.10.1 o superiore, è possibile scegliere di eseguire il Tier dei backup per lo storage *S3 Glacier* o *S3 Glacier Deep Archive* dopo un certo numero di giorni (in genere più di 30 giorni) per un'ulteriore ottimizzazione dei costi. È possibile impostare su "0" o su 1-999 giorni. Se si imposta su "0" giorni, non sarà possibile modificarlo successivamente a 1-999 giorni.

Non è possibile accedere immediatamente ai dati di questi livelli quando necessario e richiede un costo di recupero più elevato, quindi è necessario considerare la frequenza con cui potrebbe essere necessario ripristinare i dati da questi file di backup archiviati. Consultare la sezione relativa a. ripristino dei dati dallo storage di archiviazione.

- Se non si seleziona alcun livello di archiviazione nella prima policy di backup quando si attiva il backup e ripristino BlueXP, *S3 Glacier* sarà l'unica opzione di archiviazione per le policy future.
- Se si seleziona *S3 Glacier* nella prima policy di backup, è possibile passare al livello *S3 Glacier Deep Archive* per le policy di backup future per quel cluster.
- Se si seleziona *S3 Glacier Deep Archive* nella prima policy di backup, tale Tier sarà l'unico Tier di archiviazione disponibile per future policy di backup per quel cluster.

Si noti che quando si configura il backup e ripristino BlueXP con questo tipo di regola del ciclo di vita, non è necessario configurare alcuna regola del ciclo di vita quando si imposta il bucket nell'account AWS.

"Scopri le classi di storage S3".

Ripristino dei dati dallo storage di archiviazione

Anche se la memorizzazione di file di backup meno recenti nello storage di archiviazione è molto meno costosa rispetto allo storage Standard o Standard-IA, l'accesso ai dati da un file di backup nello storage di archiviazione per le operazioni di ripristino richiederà più tempo e costerà più denaro.

Quanto costa ripristinare i dati da Amazon S3 Glacier e Amazon S3 Glacier Deep Archive?

Sono disponibili 3 priorità di ripristino per il recupero dei dati da Amazon S3 Glacier e 2 priorità di ripristino per il recupero dei dati da Amazon S3 Glacier Deep Archive. S3 Glacier Deep Archive costa meno di S3 Glacier:

Tier di archiviazione	Ripristinare priorità e costi		
	Alto	Standard	Basso

Tier di archiviazione	Ripristinare priorità e costi		
Ghiacciaio S3	Recupero più rapido, costo più elevato	Recupero più lento, costi inferiori	Recupero più lento, costo più basso
S3 Glacier Deep Archive		Recupero più rapido, costi più elevati	Recupero più lento, costo più basso

Ogni metodo ha una tariffa di recupero per GB e una tariffa per richiesta diverse. Per informazioni dettagliate sui prezzi di S3 Glacier per regione AWS, visitare il "Pagina dei prezzi di Amazon S3".

Quanto tempo ci vorrà per ripristinare gli oggetti archiviati in Amazon S3 Glacier?

Il tempo totale di ripristino è costituito da 2 parti:

- **Tempo di recupero**: Tempo necessario per recuperare il file di backup dall'archivio e collocarlo nello storage standard. Questo è talvolta chiamato tempo di "reidratazione". Il tempo di recupero varia a seconda della priorità di ripristino scelta.

Tier di archiviazione	Priorità di ripristino e tempo di recupero		
	Alto	**Standard**	**Basso**
Ghiacciaio S3	3-5 minuti	3-5 ore	5-12 ore
S3 Glacier Deep Archive		12 ore	48 ore

- **Restore Time** (tempo di ripristino): Tempo di ripristino dei dati dal file di backup nello storage standard. Questo tempo non è diverso dall'operazione di ripristino tipica direttamente dallo storage standard, quando non si utilizza un livello di archiviazione.

Per ulteriori informazioni sulle opzioni di recupero di Amazon S3 Glacier e S3 Glacier Deep Archive, fare riferimento a. "Domande frequenti su Amazon relative a queste classi di storage".

Livelli di archiviazione Azure e tempi di recupero del ripristino

Il backup e ripristino BlueXP supporta un unico livello di accesso per l'archiviazione Azure e la maggior parte delle regioni.

Livelli di accesso Azure Blob supportati per backup e ripristino BlueXP

Quando i file di backup vengono creati inizialmente, vengono memorizzati nel Tier di accesso *Cool*. Questo Tier è ottimizzato per l'archiviazione dei dati a cui si accede raramente, ma quando necessario, è possibile accedervi immediatamente.

Se i cluster di origine eseguono ONTAP 9.10.1 o versione successiva, è possibile scegliere di eseguire il tiering dei backup dallo storage *Cool* allo storage *Azure Archive* dopo un certo numero di giorni (in genere più di 30 giorni) per un'ulteriore ottimizzazione dei costi. Non è possibile accedere immediatamente ai dati di questo Tier quando necessario e richiede un costo di recupero più elevato, quindi è necessario considerare la frequenza con cui potrebbe essere necessario ripristinare i dati da questi file di backup archiviati. Consultare la sezione successiva su ripristino dei dati dallo storage di archiviazione.

Si noti che quando si configura il backup e ripristino di BlueXP con questo tipo di regola del ciclo di vita, non è necessario configurare alcuna regola del ciclo di vita quando si imposta il container nell'account Azure.

"Scopri i Tier di accesso di Azure Blob".

Ripristino dei dati dallo storage di archiviazione

Sebbene l'archiviazione di file di backup meno recenti nello storage di archiviazione sia molto meno costosa rispetto allo storage Cool, l'accesso ai dati da un file di backup in Azure Archive per le operazioni di ripristino richiederà più tempo e costerà più denaro.

Quanto costa ripristinare i dati da Azure Archive?

Quando si recuperano i dati da Azure Archive, è possibile scegliere due priorità di ripristino:

- **Alta**: Recupero più rapido, costi più elevati
- **Standard**: Recupero più lento, costi inferiori

Ogni metodo ha una tariffa di recupero per GB e una tariffa per richiesta diverse. Per informazioni dettagliate sui prezzi di Azure Archive per regione Azure, visitare il "Pagina dei prezzi di Azure".

> La priorità alta non è supportata quando si ripristinano i dati da Azure ai sistemi StorageGRID.

Quanto tempo ci vorrà per ripristinare i dati archiviati in Azure Archive?

Il tempo di ripristino è costituito da 2 parti:

- **Tempo di recupero**: Il tempo necessario per recuperare il file di backup archiviato da Azure Archive e collocarlo in Cool Storage. Questo è talvolta chiamato tempo di "reidratazione". Il tempo di recupero varia a seconda della priorità di ripristino scelta:
  - **Alto**: < 1 ora
  - **Standard**: < 15 ore
- **Restore Time** (tempo di ripristino): Il tempo necessario per ripristinare i dati dal file di backup in Cool Storage. Questo tempo non è diverso dalla tipica operazione di ripristino direttamente da Cool storage, quando non si utilizza un Tier di archiviazione.

Per ulteriori informazioni sulle opzioni di recupero di Azure Archive, fare riferimento a. "Domande frequenti su Azure".

Classi di storage di archivio e tempi di recupero di Google

Il backup e ripristino BlueXP supporta una classe di storage di archiviazione Google e la maggior parte delle regioni.

Classi di storage di archivio supportate da Google per backup e ripristino BlueXP

Quando i file di backup vengono creati inizialmente, vengono memorizzati nello storage *Standard*. Questo Tier è ottimizzato per l'archiviazione dei dati a cui si accede raramente, ma che consente anche di accedervi immediatamente.

Se il cluster on-premise utilizza ONTAP 9.12.1 o versione successiva, è possibile scegliere di raggruppare i backup più vecchi in storage *Archive* nell'interfaccia utente di backup e ripristino BlueXP dopo un certo numero di giorni (in genere più di 30 giorni) per un'ulteriore ottimizzazione dei costi. I dati in questo Tier richiederanno un costo di recupero più elevato, pertanto è necessario considerare la frequenza con cui potrebbe essere necessario ripristinare i dati da questi file di backup archiviati. Consultare la sezione relativa a. ripristino dei

dati dallo storage di archiviazione.

Si noti che quando si configura il backup e ripristino di BlueXP con questo tipo di regola del ciclo di vita, non è necessario configurare alcuna regola del ciclo di vita quando si imposta il bucket nell'account Google.

"Scopri le classi di storage di Google".

Ripristino dei dati dallo storage di archiviazione

Sebbene la memorizzazione di file di backup meno recenti nello storage di archiviazione sia molto meno costosa rispetto allo storage standard, l'accesso ai dati da un file di backup nello storage di archiviazione per le operazioni di ripristino richiederà un tempo leggermente più lungo e costerà più denaro.

Quanto costa ripristinare i dati da Google Archive?

Per informazioni dettagliate sui prezzi di Google Cloud Storage per regione, visita il "Pagina dei prezzi di Google Cloud Storage".

Quanto tempo ci vorrà per ripristinare gli oggetti archiviati in Google Archive?

Il tempo totale di ripristino è costituito da 2 parti:

- **Tempo di recupero**: Tempo necessario per recuperare il file di backup dall'archivio e collocarlo nello storage standard. Questo è talvolta chiamato tempo di "reidratazione". A differenza delle soluzioni di storage più "fredde" fornite da altri cloud provider, i tuoi dati sono accessibili in pochi millisecondi.
- **Restore Time** (tempo di ripristino): Tempo di ripristino dei dati dal file di backup nello storage standard. Questo tempo non è diverso dall'operazione di ripristino tipica direttamente dallo storage standard, quando non si utilizza un livello di archiviazione.

Configurare il backup per l'accesso multi-account in Azure

Il backup e ripristino BlueXP consente di creare file di backup in un account Azure diverso da quello in cui risiedono i volumi Cloud Volumes ONTAP di origine. Entrambi gli account possono essere diversi dall'account in cui si trova BlueXP Connector.

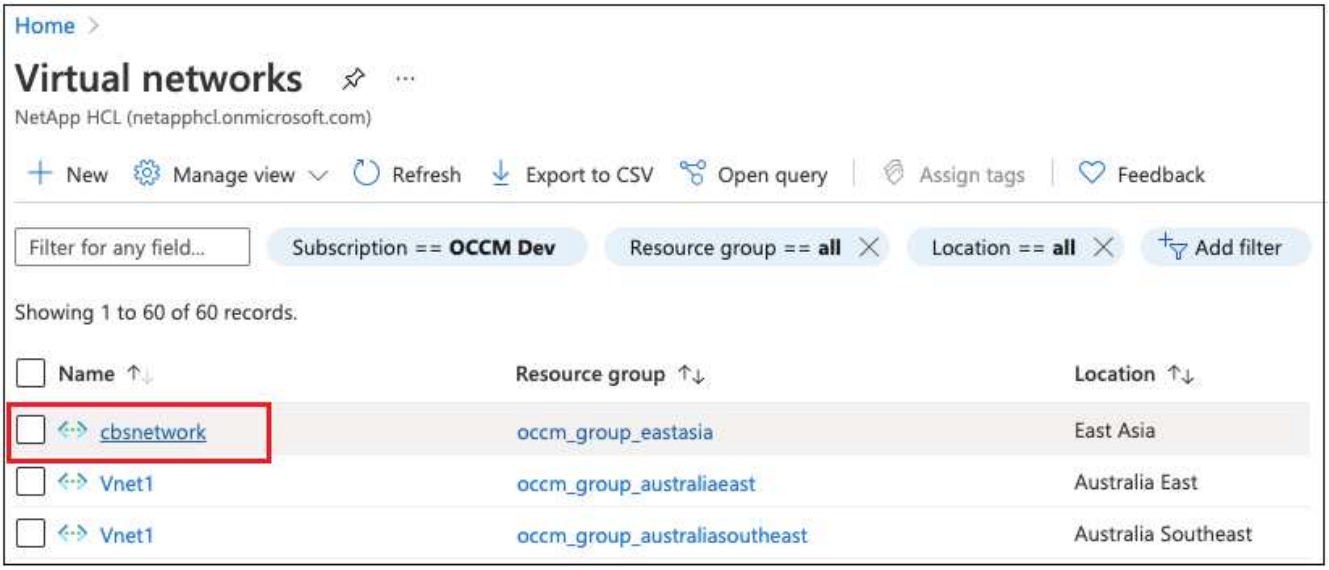
Questi passaggi sono necessari solo quando si è "Backup dei dati Cloud Volumes ONTAP nello storage Azure Blob".

Seguire i passaggi riportati di seguito per configurare la configurazione in questo modo.

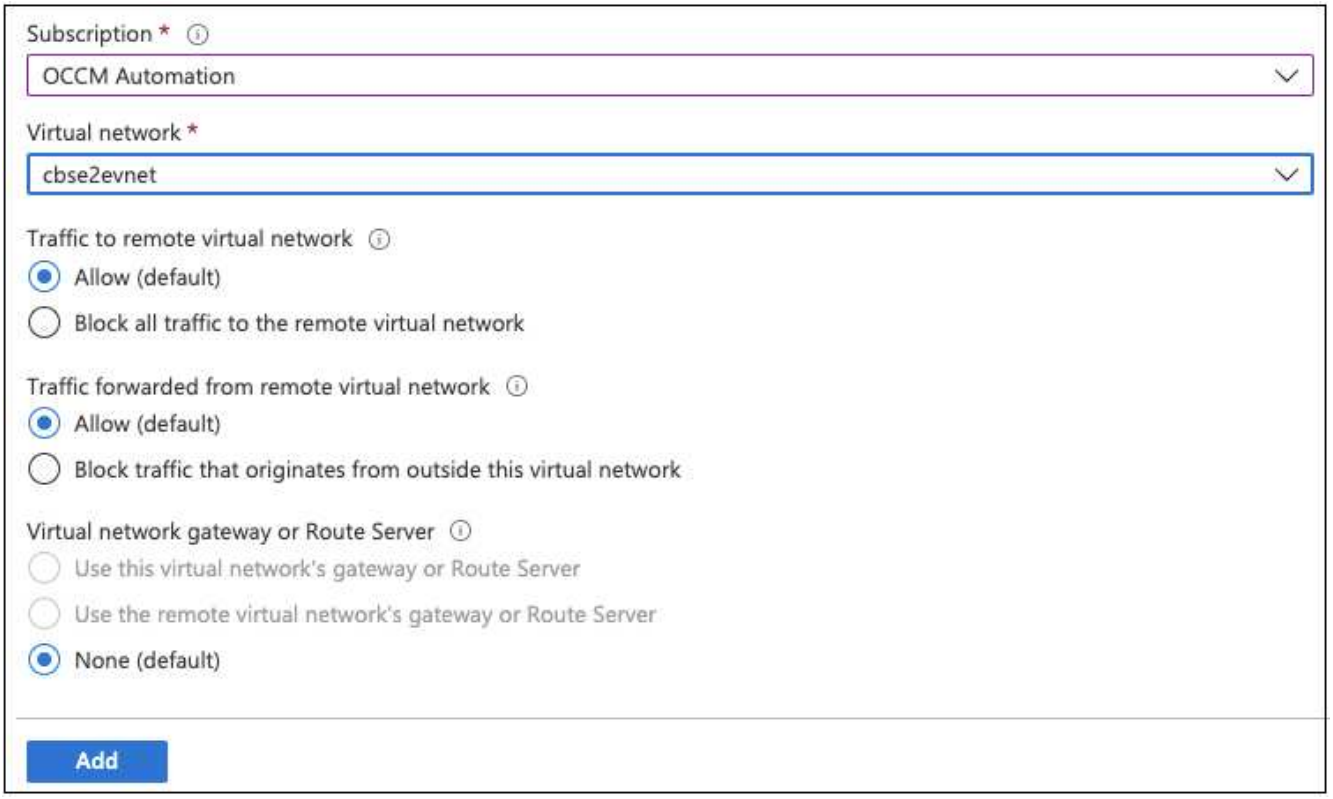
Impostare il peering VNET tra gli account

Si noti che se si desidera che BlueXP gestisca il sistema Cloud Volumes ONTAP in un account/regione differente, è necessario configurare il peering VNET. Il peering VNET non è richiesto per la connettività degli account di storage.

1. Accedere al portale Azure e da casa, selezionare Virtual Networks (reti virtuali).
2. Selezionare l'abbonamento che si sta utilizzando come abbonamento 1 e fare clic su VNET in cui si desidera impostare il peering.

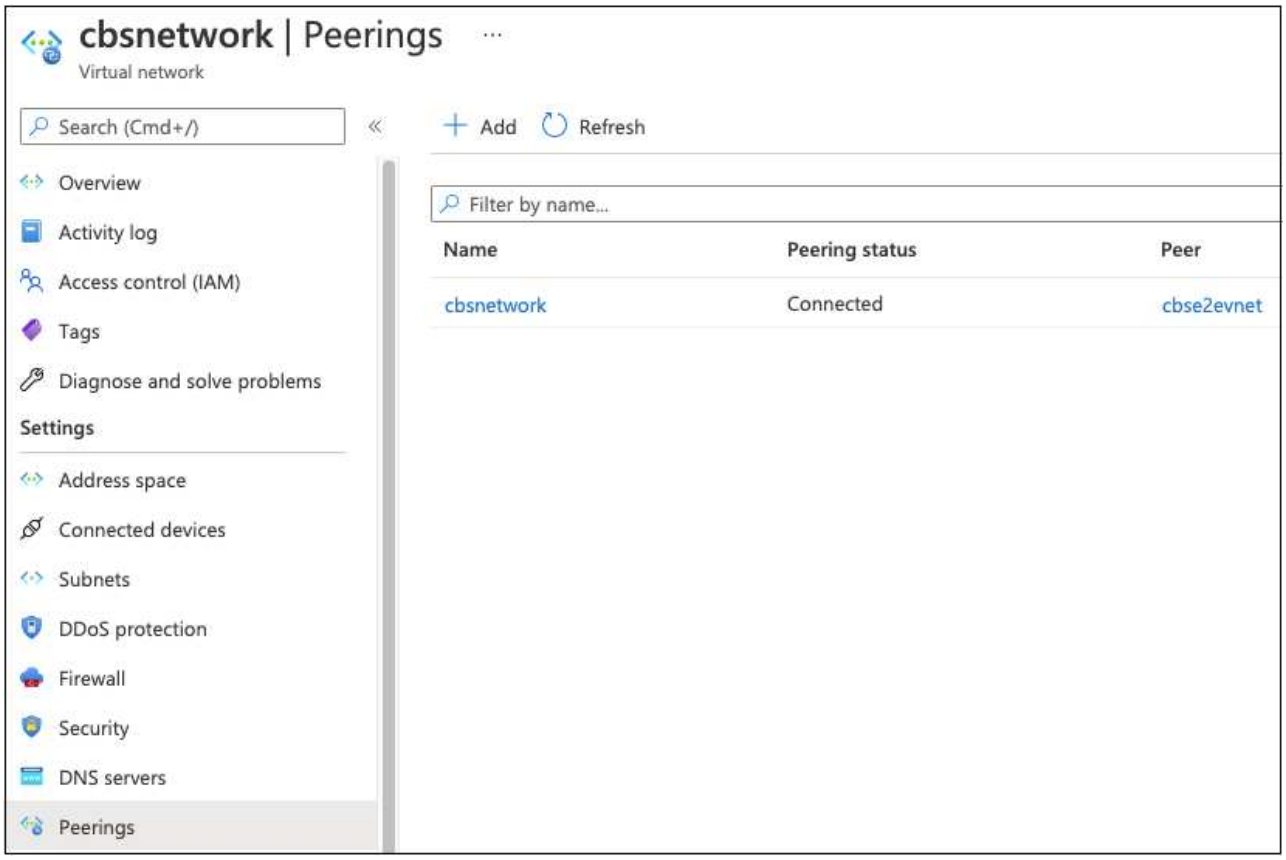


3. Selezionare **cbsnetwork** e dal pannello di sinistra, fare clic su **Peerings**, quindi fare clic su **Add**.

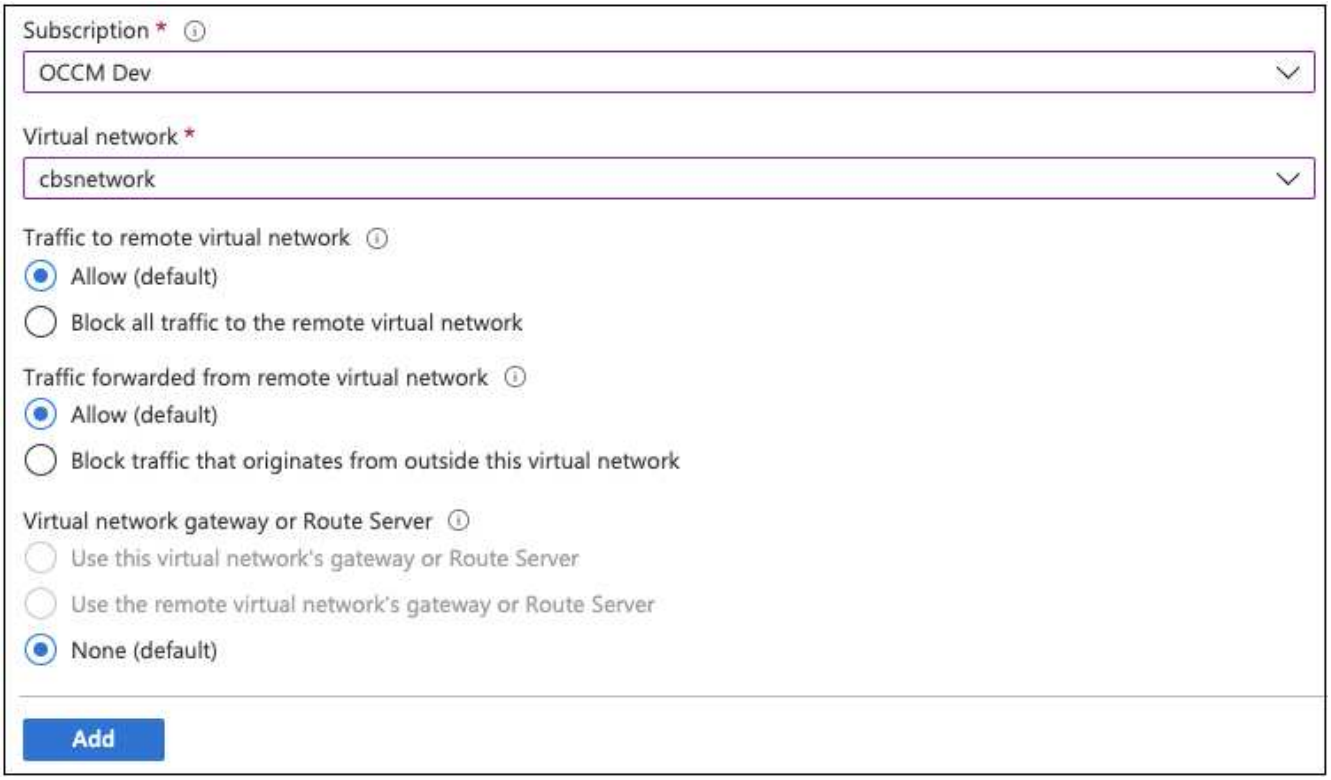


4. Inserire le seguenti informazioni nella pagina di peering, quindi fare clic su **Aggiungi**.
   - Peering link name for this network (Nome collegamento peering per questa rete): È possibile assegnare un nome qualsiasi per identificare la connessione peering.
   - Remote virtual network peering link name (Nome collegamento peering rete virtuale remota): Immettere un nome per identificare il VNET remoto.
   - Mantenere tutte le selezioni come valori predefiniti.
   - In Subscription (abbonamento), selezionare l'abbonamento 2.
   - Virtual network (rete virtuale), selezionare la rete virtuale con abbonamento 2 a cui si desidera

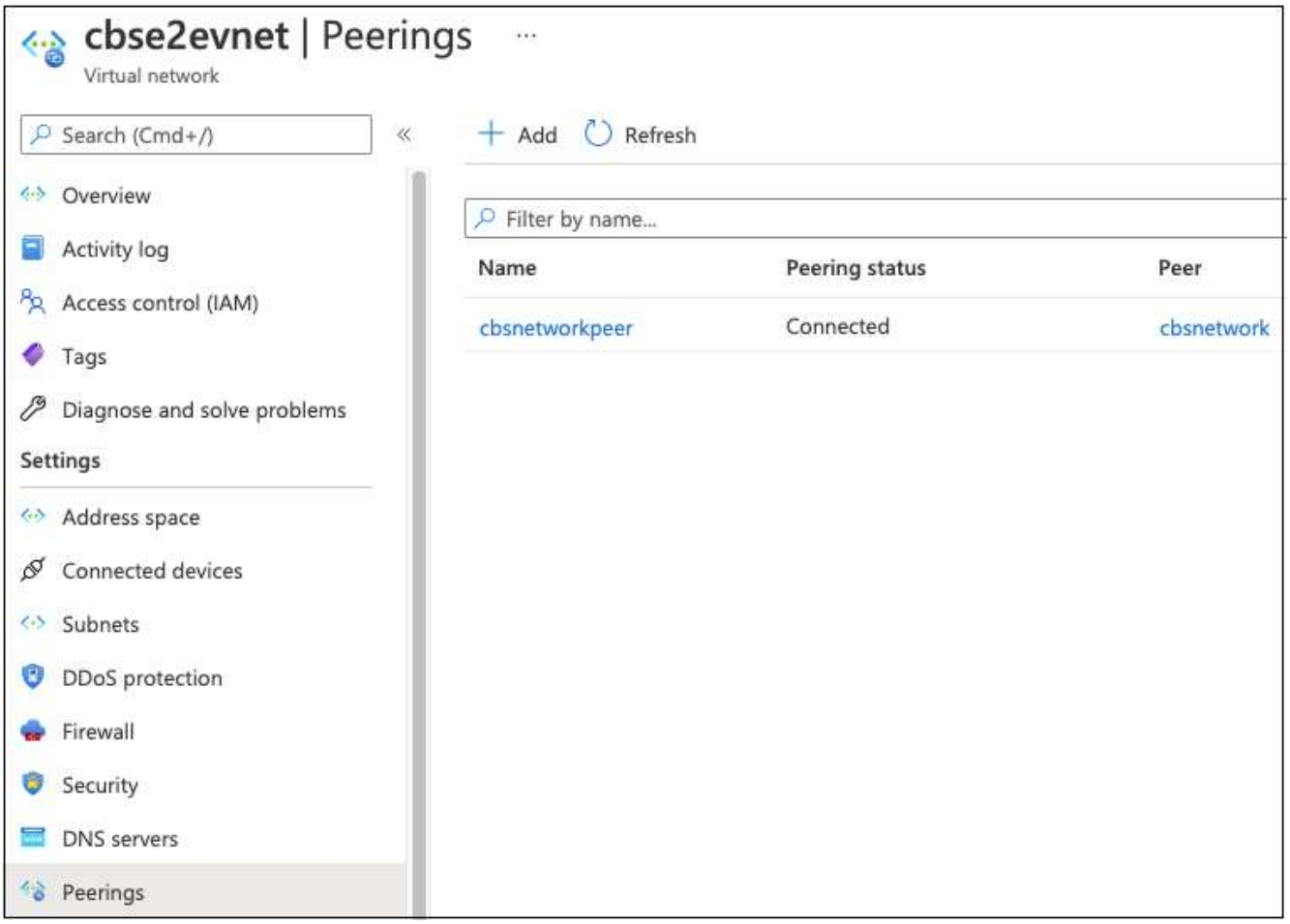
impostare il peering.



5. Eseguire le stesse operazioni in Subscription 2 VNET e specificare l'abbonamento e i dettagli VNET remoti dell'abbonamento 1.



Vengono aggiunte le impostazioni di peering.



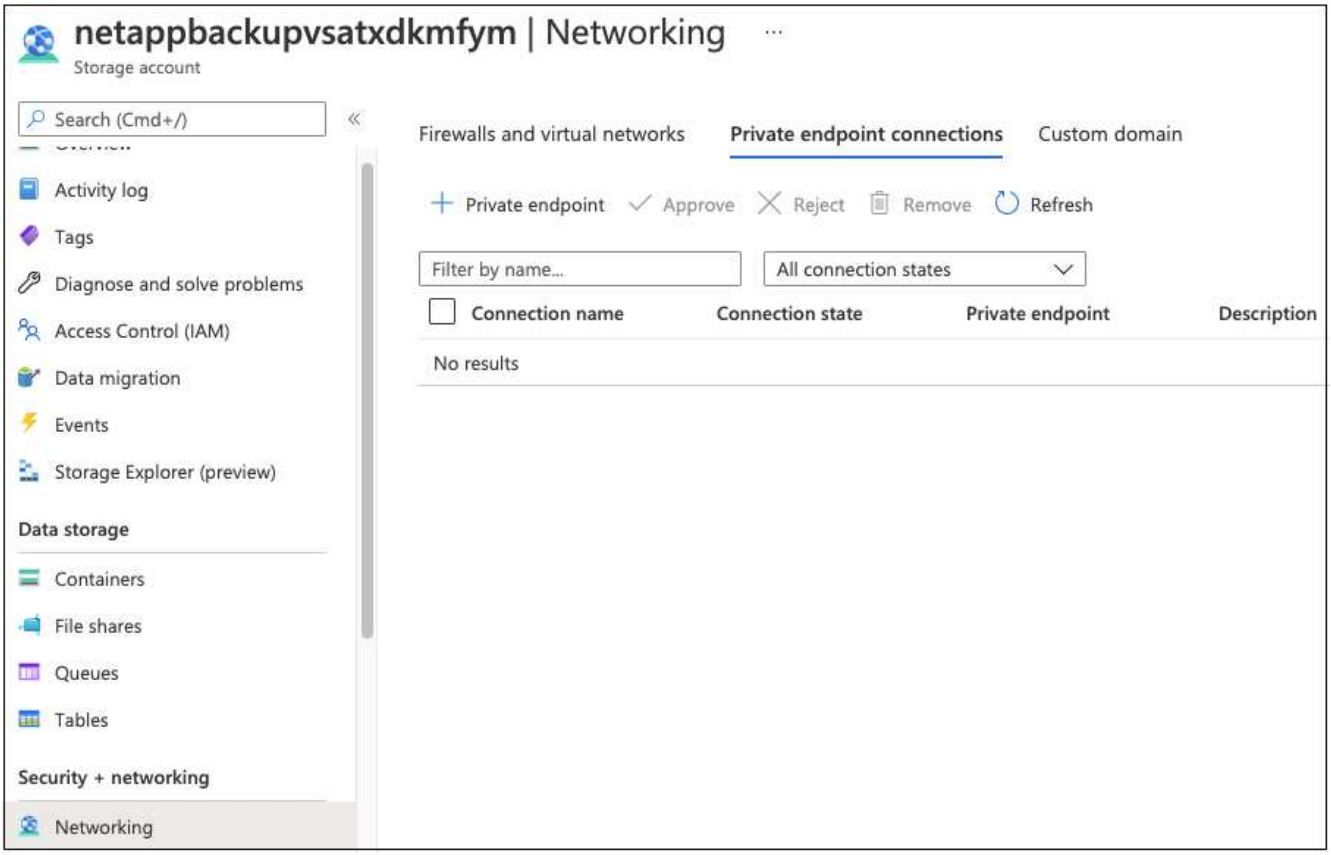
Creare un endpoint privato per l'account storage

Ora è necessario creare un endpoint privato per l'account storage. In questo esempio, l'account storage viene creato nell'abbonamento 1 e il sistema Cloud Volumes ONTAP viene eseguito nell'abbonamento 2.

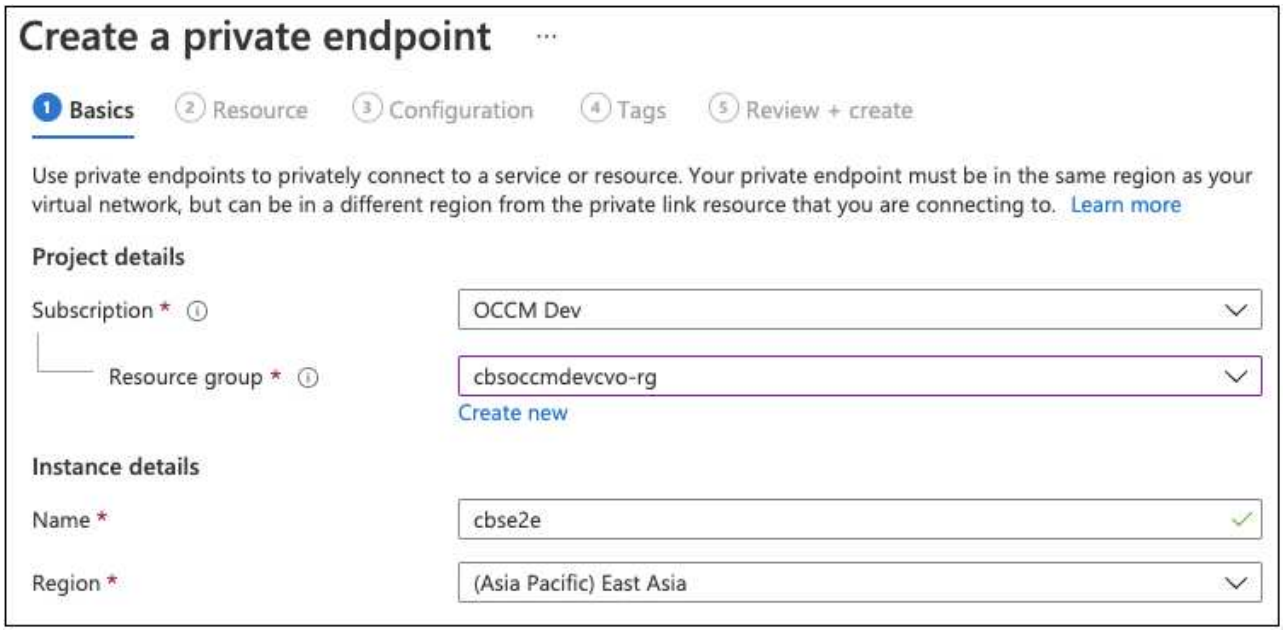
> Per eseguire la seguente azione, è necessario disporre dell'autorizzazione di un collaboratore di rete.

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

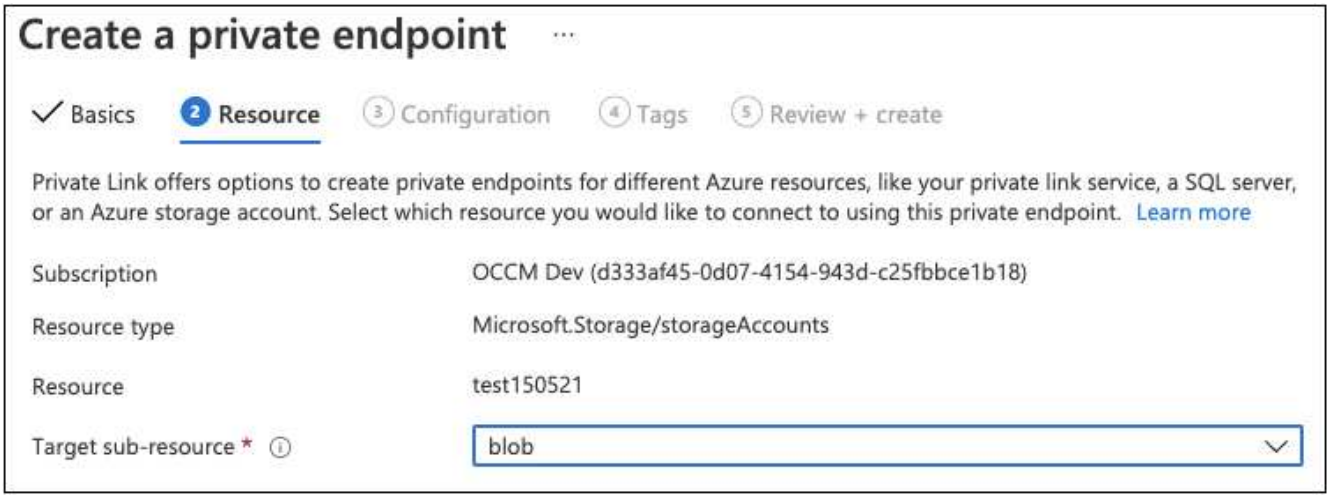
1. Accedere all'account Storage > Networking > Private endpoint Connections e fare clic su **+ Private endpoint**.



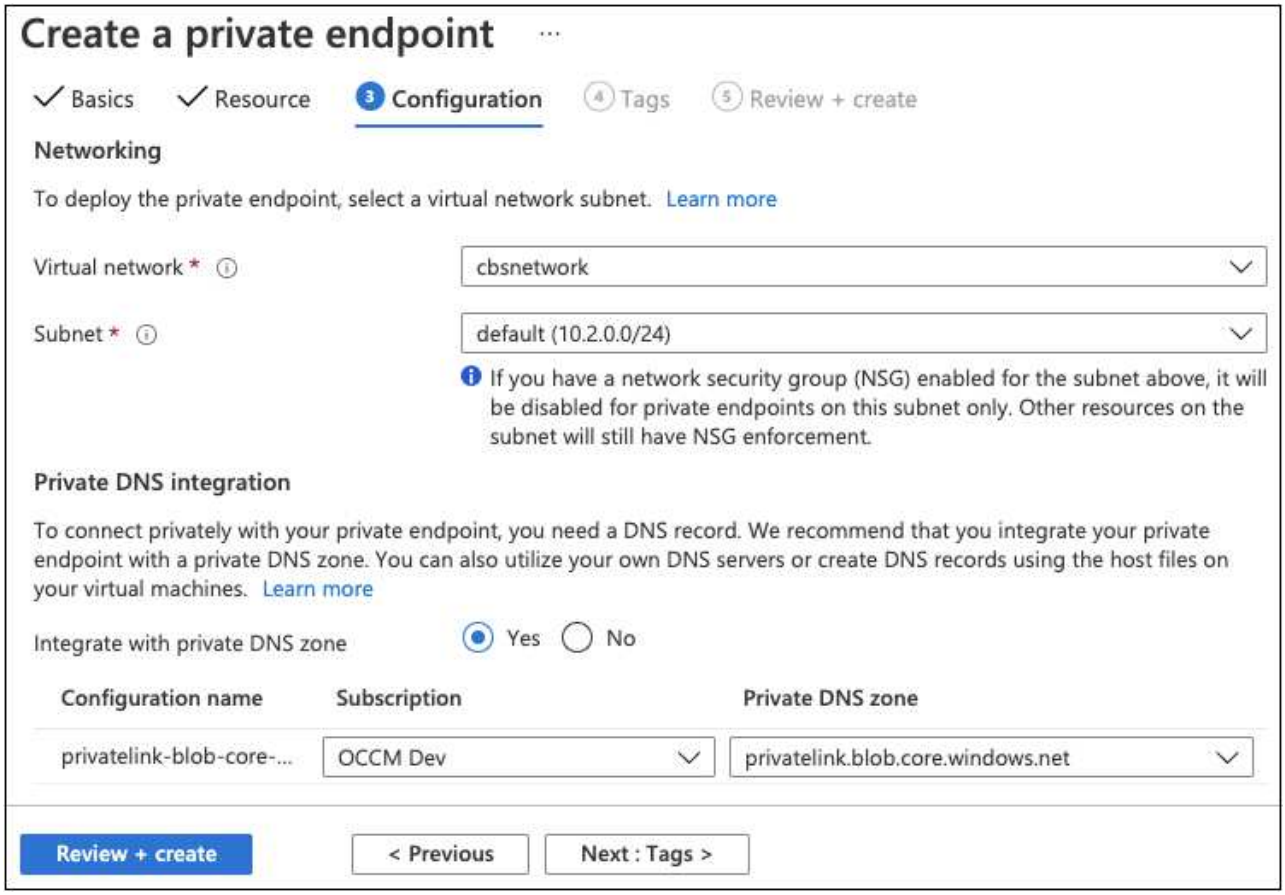
2. Nella pagina *Basics* dell'endpoint privato:
   - Selezionare Subscription 2 (abbonamento 2) (in cui vengono implementati il connettore BlueXP e il sistema Cloud Volumes ONTAP) e il gruppo di risorse.
   - Inserire un nome endpoint.
   - Selezionare la regione.



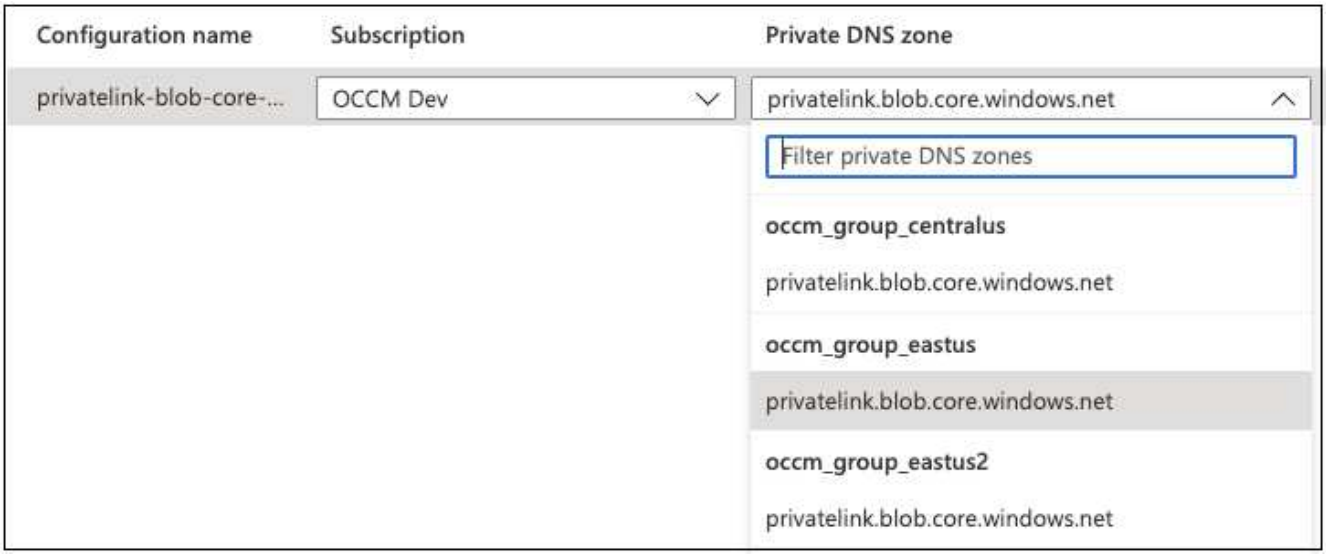
3. Nella pagina *Resource*, selezionare la sottorisorsa di destinazione come **blob**.



4. Nella pagina di configurazione:
   - Selezionare la rete virtuale e la subnet.
   - Fare clic sul pulsante di opzione **Sì** per "integrare con la zona DNS privata".



5. Nell'elenco Private DNS zone (zona DNS privata), assicurarsi che la zona privata sia selezionata dalla regione corretta e fare clic su **Review + Create** (Rivedi + Crea).



Ora l'account storage (nell'abbonamento 1) ha accesso al sistema Cloud Volumes ONTAP in esecuzione nell'abbonamento 2.

6. Riprovare ad abilitare il backup e il ripristino BlueXP sul sistema Cloud Volumes ONTAP e questa volta dovrebbe essere possibile.

Ripristinare i dati di backup e ripristino BlueXP in un sito buio

Quando utilizzi il backup e recovery di BlueXP in un sito senza accesso a Internet, noto come *modalità privata*, viene eseguito il backup dei dati di configurazione di backup e recovery di BlueXP nel bucket StorageGRID o ONTAP S3 in cui vengono archiviati i backup. In caso di problemi con il sistema host BlueXP Connector in futuro, è possibile implementare un nuovo connettore e ripristinare i dati critici di backup e ripristino di BlueXP.

Si noti che quando si utilizza il backup e ripristino BlueXP in un ambiente SaaS in cui BlueXP Connector viene implementato presso il provider cloud o sul proprio sistema host dotato di accesso a Internet, tutti i dati importanti di configurazione di backup e ripristino BlueXP vengono sottoposti a backup e protetti nel cloud. In caso di problemi con il connettore, è sufficiente creare un nuovo connettore e aggiungere gli ambienti di lavoro per ripristinare automaticamente i dettagli del backup.

Sono disponibili 2 tipi di dati di cui viene eseguito il backup:

- Database di backup e ripristino BlueXP - contiene un elenco di tutti i volumi, i file di backup, i criteri di backup e le informazioni di configurazione.
- File di catalogo indicizzati - contiene indici dettagliati utilizzati per la funzionalità di ricerca e ripristino che rendono le ricerche molto rapide ed efficienti quando si cercano i dati dei volumi che si desidera ripristinare.

Il backup di questi dati viene eseguito una volta al giorno a mezzanotte e viene conservato un massimo di 7 copie di ciascun file. Se il connettore gestisce più ambienti di lavoro ONTAP on-premise, i file di backup e ripristino BlueXP si trovano nel bucket dell'ambiente di lavoro attivato per primo.

Nessun dato di volume è mai incluso nel database di backup e ripristino BlueXP o nei file di catalogo indicizzati.

Ripristinare i dati di backup e ripristino di BlueXP su un nuovo connettore

Se il connettore on-premise presenta un guasto catastrofico, è necessario installare un nuovo connettore e ripristinare i dati di backup e ripristino di BlueXP nel nuovo connettore.

Per riportare il sistema di backup e ripristino BlueXP a uno stato operativo, è necessario eseguire 4 operazioni:

- Installare un nuovo connettore BlueXP
- Ripristinare il database di backup e ripristino BlueXP
- Ripristinare i file di catalogo indicizzati
- Riscopri tutti i tuoi sistemi ONTAP e StorageGRID on-premise nell'interfaccia utente di BlueXP

Una volta verificato il corretto funzionamento del sistema, si consiglia di creare nuovi file di backup.

Di cosa hai bisogno

È necessario accedere ai backup di database e indici più recenti dal bucket StorageGRID o ONTAP S3 in cui vengono memorizzati i file di backup:

- File di database MySQL per backup e ripristino BlueXP

  Questo file si trova nella seguente posizione nel bucket `netapp-backup-<GUID>/mysql_backup/`e viene chiamato `CBS_DB_Backup_<day>_<month>_<year>.sql`.

- File zip di backup del catalogo indicizzato

  Questo file si trova nella seguente posizione nel bucket `netapp-backup-<GUID>/catalog_backup/`e viene chiamato `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip`.

Installare un nuovo connettore su un nuovo host Linux on-premise

Quando si installa un nuovo connettore BlueXP, assicurarsi di scaricare la stessa versione del software installata sul connettore originale. Le modifiche periodiche alla struttura del database di backup e ripristino di BlueXP possono rendere incompatibili le versioni software più recenti con i backup del database originali. È possibile "Aggiornare il software del connettore alla versione più recente dopo il ripristino del database di backup".

1. "Installare il connettore BlueXP su un nuovo host Linux on-premise"
2. Accedere a BlueXP utilizzando le credenziali utente amministratore appena create.

Ripristinare il database di backup e ripristino BlueXP

1. Copiare il backup MySQL dalla posizione di backup al nuovo host del connettore. Verrà utilizzato il nome del file di esempio "CBS_DB_Backup_23_05_2023.sql" riportato di seguito.
2. Copiare il backup nel contenitore MySQL docker utilizzando il seguente comando:

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

3. Inserire la shell del container MySQL usando il seguente comando:

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

4. Nella shell container, implementare "env".
5. Avrai bisogno della password MySQL DB, quindi copia il valore della chiave "MYSQL_ROOT_PASSWORD".
6. Ripristinare il backup e ripristino di BlueXP MySQL DB utilizzando il seguente comando:

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

7. Verificare che MySQL DB di backup e ripristino BlueXP sia stato ripristinato correttamente utilizzando i seguenti comandi SQL:

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

Inserire la password.

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

Verificare che i volumi visualizzati siano gli stessi dell'ambiente originale.

Ripristinare i file di catalogo indicizzati

1. Copiare il file zip di backup del catalogo indicizzato (verrà utilizzato il nome del file di esempio "indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip") dalla posizione di backup al nuovo host del connettore nella cartella "/opt/application/netapp/cbs".
2. Decomprimere il file "indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip" utilizzando il seguente comando:

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

3. Eseguire il comando **ls** per assicurarsi che la cartella "catalogdb1" sia stata creata con le sottocartelle "Changes" e "Snapshot" sottostanti.

Scopri i tuoi cluster ONTAP e i sistemi StorageGRID

1. "Scopri tutti gli ambienti di lavoro ONTAP on-premise" che erano disponibili nel tuo ambiente precedente. Questo include il sistema ONTAP utilizzato come server S3.

2. "Scopri i tuoi sistemi StorageGRID".

Impostare i dettagli dell'ambiente StorageGRID

Aggiungere i dettagli del sistema StorageGRID associato agli ambienti di lavoro ONTAP così come sono stati configurati nella configurazione originale del connettore utilizzando "API BlueXP".

È necessario eseguire questa procedura per ogni sistema ONTAP che esegue il backup dei dati su StorageGRID.

1. Estrarre il token di autorizzazione utilizzando la seguente API oauth/token.

```
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"}
> '
```

   Questa API restituirà una risposta simile a quella riportata di seguito. È possibile recuperare il token di autorizzazione come mostrato di seguito.


```
{"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. Estrarre l'ID dell'ambiente di lavoro e l'ID dell'agente X utilizzando l'API di tenancy/esterno/risorsa.

```
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'
```

Questa API restituirà una risposta simile a quella riportata di seguito. Il valore sotto "resourceIdentifier" indica *WorkingEnvironment Id* e il valore sotto "agentId" indica *x-Agent-id*.

3. Aggiornare il database di backup e ripristino BlueXP con i dettagli del sistema StorageGRID associato agli ambienti di lavoro. Assicurarsi di immettere il nome di dominio completo del StorageGRID, la chiave di accesso e la chiave di storage come mostrato di seguito:

```
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" }'
```

Verificare le impostazioni di backup e ripristino di BlueXP

1. Selezionare ciascun ambiente di lavoro ONTAP e fare clic su **Visualizza backup** accanto al servizio di backup e ripristino nel pannello di destra.

   Dovrebbe essere possibile visualizzare tutti i backup creati per i volumi.

2. Dalla dashboard di ripristino, nella sezione Search & Restore (Ricerca e ripristino), fare clic su **Indexing Settings** (Impostazioni di indicizzazione).

   Assicurarsi che gli ambienti di lavoro che in precedenza avevano attivato la catalogazione indicizzata rimangano abilitati.

3. Dalla pagina Search & Restore (Ricerca e ripristino), eseguire alcune ricerche nel catalogo per confermare che il ripristino del catalogo indicizzato è stato completato correttamente.

Riavviare il servizio di backup e ripristino BlueXP

In alcuni casi potrebbe essere necessario riavviare il servizio di backup e ripristino BlueXP.

La funzionalità di backup e ripristino BlueXP è integrata nel connettore BlueXP. Per riavviare il servizio, è necessario seguire diversi passaggi iniziali a seconda che il connettore sia stato implementato nel cloud o che il connettore sia stato installato manualmente su un sistema Linux.

Fasi

1. Connettersi al sistema Linux su cui è in esecuzione il connettore.

Posizione del connettore	Procedura
Implementazione del cloud	Seguire le istruzioni per "Connessione alla macchina virtuale Connector Linux" a seconda del cloud provider utilizzato.
Installazione manuale	Accedere al sistema Linux.

2. Immettere il comando per riavviare il servizio.

Posizione del connettore	Comando
Implementazione del cloud	`docker restart cloudmanager_cbs`
Installazione manuale con accesso a Internet	`docker restart cloudmanager_cbs`
Installazione manuale senza accesso a Internet	`docker restart ds_cloudmanager_cbs_1`