参照
Cloud Backup

NetApp
July 19, 2022

目次

参照

AWS S3 アーカイブストレージクラスおよびリストアの読み出し時間

Cloud Backup は、 2 つの S3 アーカイブストレージクラスとほとんどのリージョンをサポートします。

Cloud Backup でサポートされている S3 アーカイブストレージクラスです

バックアップファイルが最初に作成されるときは、 S3_Standard_storage に格納されています。この階層は、アクセス頻度の低いデータを格納するために最適化されていますが、すぐにアクセスすることもできます。30 日経過すると、バックアップは S3_Standard - Infrequent Access_storage クラスに移行してコストを削減します。

ソースクラスタで ONTAP 9.10.1 以降が実行されている場合は、特定の日数（通常は 30 日以上）が経過したあとに S3 Glacier Deep Archive_storage にバックアップを階層化して、コストをさらに最適化することができます。これらの階層のデータは、必要なときにすぐにアクセスすることはできず、取得コストが高くなるため、アーカイブされたバックアップファイルからデータをリストアする頻度を考慮する必要があります。についてのセクションを参照してください アーカイブストレージからのデータのリストア。

このタイプのライフサイクルルールでクラウドバックアップを設定する場合は、 AWS アカウントでバケットを設定する際にライフサイクルルールを設定しないでください。

"S3 ストレージクラスについて説明します"。

アーカイブストレージからのデータのリストア

古いバックアップファイルをアーカイブストレージに保存すると、標準または標準の IA ストレージよりもはるかに低コストですが、リストア処理のためにアーカイブストレージ内のバックアップファイルからデータにアクセスすると、時間がかかり、コストがかかります。

Amazon S3 Glacier と **Amazon S3 Glacier Deep Archive** からデータをリストアするのにどれくらいのコストがかかりますか。

Amazon S3 Glacier からデータを読み出すときは 3 つのリストア優先度を選択でき、 Amazon S3 Glacier Deep Archive からデータを読み出すときは 2 つのリストア優先度を選択できます。S3 Glacier Deep Archive のコストは S3 Glacier よりも低く：

アーカイブ階層	優先度とコストを復元します		
	* 高 *	* 標準 *	* 低 *
* S3 Glacier *	高速な読み出し、コストの最大化	取得速度が低下し、コストが削減されます	読み出しに時間がかかり、コストを最小限に抑えます
* S3 Glacier Deep Archive *		高速な読み出し、コストの増大	取得速度が遅く、コストが最も低い

各メソッドには、 GB 単位の取得料金とリクエストごとの料金が異なります。AWS リージョン別の S3 Glacier の詳細な価格設定については、を参照してください "Amazon S3 の価格設定ページ"。

Amazon S3 Glacier にアーカイブされているオブジェクトのリストアにはどれくらいの時間がかかりますか。

リストアの合計時間は、次の 2 つの要素で構成されます。

- * 取得時間 * ：アーカイブからバックアップファイルを取得して標準ストレージに保存する時間。これは、「水和」時間と呼ばれることもあります。取得時間は、選択したリストア優先度によって異なります。

アーカイブ階層	優先度と取得時間のリストア		
	* 高 *	* 標準 *	* 低 *
* S3 Glacier *	3 ～ 5 分	3 ～ 5 時間	5 ～ 12 時間
* S3 Glacier Deep Archive *		12 時間	48 時間

- * リストア時間 * ： Standard ストレージのバックアップファイルからデータをリストアする時間。アーカイブ層を使用しない場合、この時間は標準ストレージから直接実行される通常のリストア処理と同じです。

Amazon S3 Glacier と S3 Glacier Deep Archive の読み出しオプションの詳細については、を参照してください "これらのストレージクラスに関する Amazon FAQ"。

Azure のアーカイブ階層およびリストアの読み出し時間

Cloud Backup は、 1 つの Azure アーカイブアクセス階層とほとんどのリージョンをサポートします。

クラウドバックアップでサポートされている **Azure Blob** アクセス階層

バックアップファイルが最初に作成されるときは、 _Cool _ アクセス層に保存されます。この階層は、アクセス頻度の低いデータを格納するために最適化されていますが、必要に応じてすぐにアクセスできます。

ソースクラスタで ONTAP 9.10.1 以降が実行されている場合は、コストをさらに最適化するために、特定の日数（通常は 30 日以上）後に _Cool _To Azure Archive_storage からバックアップを階層化することを選択できます。この階層のデータは、必要なときにすぐにアクセスすることはできず、取得コストが高くなるため、アーカイブされたバックアップファイルからデータをリストアする頻度を考慮する必要があります。次のセクション About を参照してください アーカイブストレージからのデータのリストア。

このタイプのライフサイクルルールでクラウドバックアップを設定する場合は、 Azure アカウントでコンテナを設定する際にライフサイクルルールを設定しないでください。

"Azure Blob アクセス階層の概要について説明します"。

アーカイブストレージからのデータのリストア

古いバックアップファイルをアーカイブストレージに保存するのは Cool ストレージよりもはるかに安価ですが、リストア処理用に Azure Archive のバックアップファイルからデータにアクセスするには時間がかかり、コストも高くなります。

Azure Archive からデータをリストアするのにどれくらいのコストがかかりますか？

Azure Archive からデータを取得する際に選択できるリストア優先度は 2 つあります。

- * 高い * ：高速な読み出し、コストの増大
- * 標準 * ：読み出し速度が遅く、コストが削減されます

各メソッドには、 GB 単位の取得料金とリクエストごとの料金が異なります。Azure リージョン別の Azure Archive の詳細な価格設定については、を参照してください "Azure の料金体系のページです"。

Azure Archive にアーカイブされたデータをリストアするのにどれくらいの時間がかかりますか。

リストア時間は次の 2 つの要素で構成されます。

- * 取得時間 * ：アーカイブされたバックアップファイルを Azure Archive から取得して Cool Storage に保存する時間。これは、「水和」時間と呼ばれることもあります。読み出し時間は、選択したリストア優先度によって異なります。
  - * 高 * ： 1 時間未満
  - * 標準 * ： 15 時間以内
- * リストア時間 * ： Cool ストレージ内のバックアップファイルからデータをリストアする時間。この時間は、アーカイブ層を使用しないクールストレージからの一般的なリストア処理と同じです。

Azure Archive の読み出しオプションの詳細については、を参照してください "Azure に関する FAQ です"。

クロスアカウント構成とクロスリージョン構成

これらのトピックでは、異なるクラウドプロバイダを使用する場合のクロスアカウント構成用の Cloud Backup の設定方法について説明します。

- "Azure でマルチアカウントアクセスに Cloud Backup を設定"

AWS でマルチアカウントアクセスのバックアップを設定します

Cloud Backup では、ソース Cloud Volumes ONTAP ボリュームとは別の AWS アカウントにバックアップファイルを作成できます。これらのアカウントは、 Cloud Manager Connector がインストールされているアカウントとは異なる場合があります。

これらの手順は、を実行している場合にのみ必要です "Amazon S3 への Cloud Volumes ONTAP データのバックアップ"。

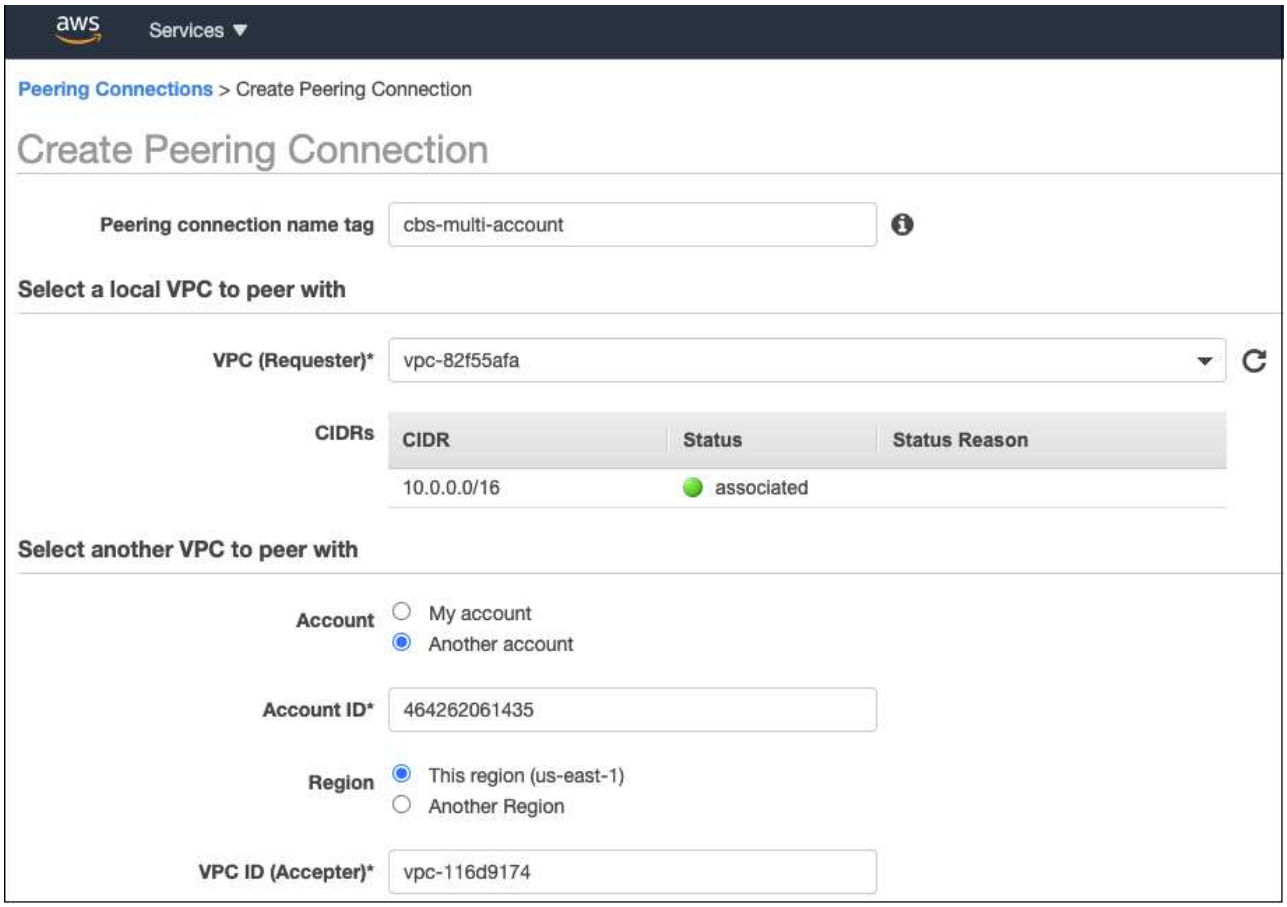
この方法で設定を行うには、次の手順に従います。

アカウント間に **VPC** ピアリングを設定します

1. 2 つ目のアカウントにログインし、ピアリング接続を作成します。
   a. ローカル VPC を選択： 2 つ目のアカウントの VPC を選択します。
   b. 別の VPC を選択：最初のアカウントのアカウント ID を入力します。

c. Cloud Manager Connector が実行されているリージョンを選択します。このテストセットアップでは、両方のアカウントが同じリージョンで実行されています。

d. VPC ID ：最初のアカウントにログインし、アクセプタ VPC ID を入力します。Cloud Manager Connector の VPC ID です。



成功ダイアログが表示されます。

ピアリング接続のステータスは、 Pending Acceptance と表示されます。

2. 最初のアカウントにログインし、ピアリング要求を承認します。

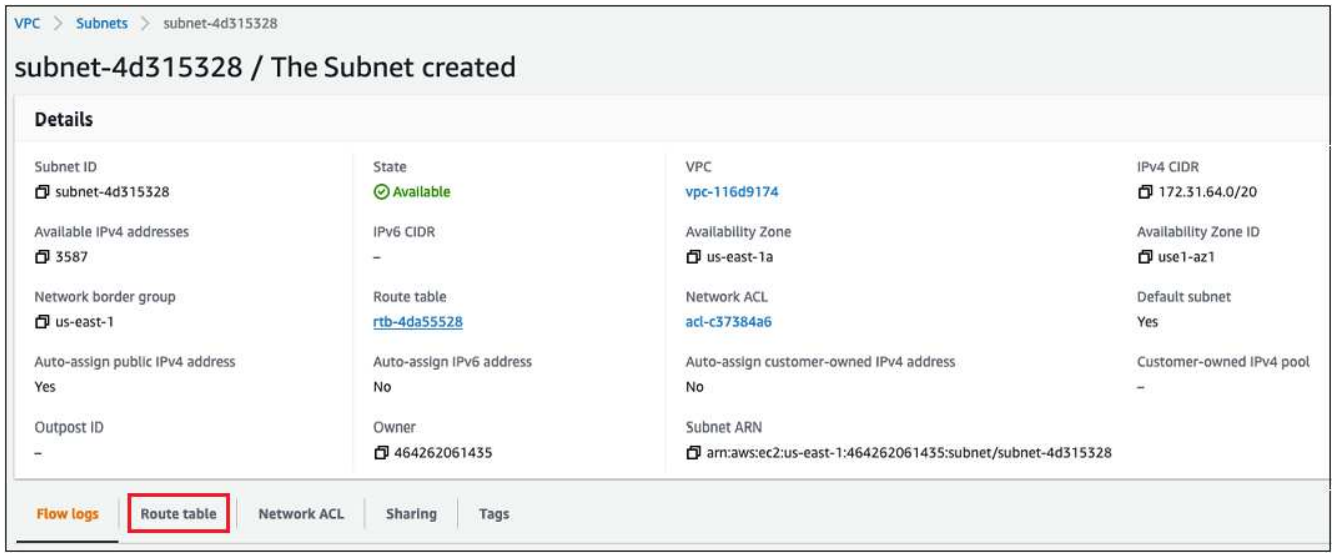
a. 「 * はい * 」をクリックします。

接続がアクティブと表示されます。また、「 CBS-multi-account 」と呼ばれるピアリング接続を識別するための Name タグも追加しました。

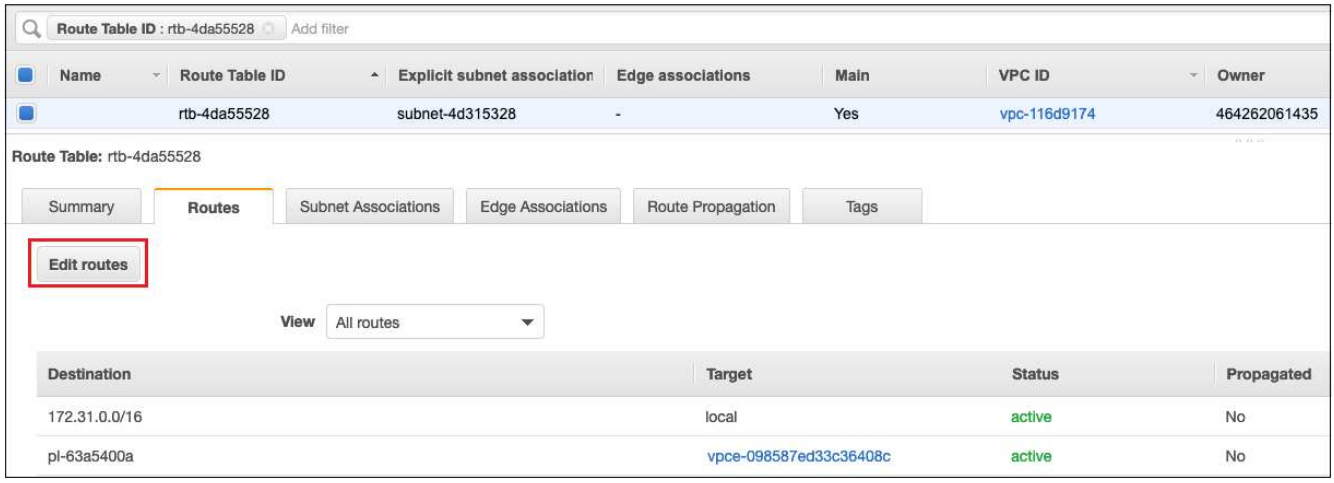
a. 2 つ目のアカウントのピアリング接続を更新し、ステータスが Active に変わったことを確認します。

両方のアカウントのルートテーブルにルートを追加します

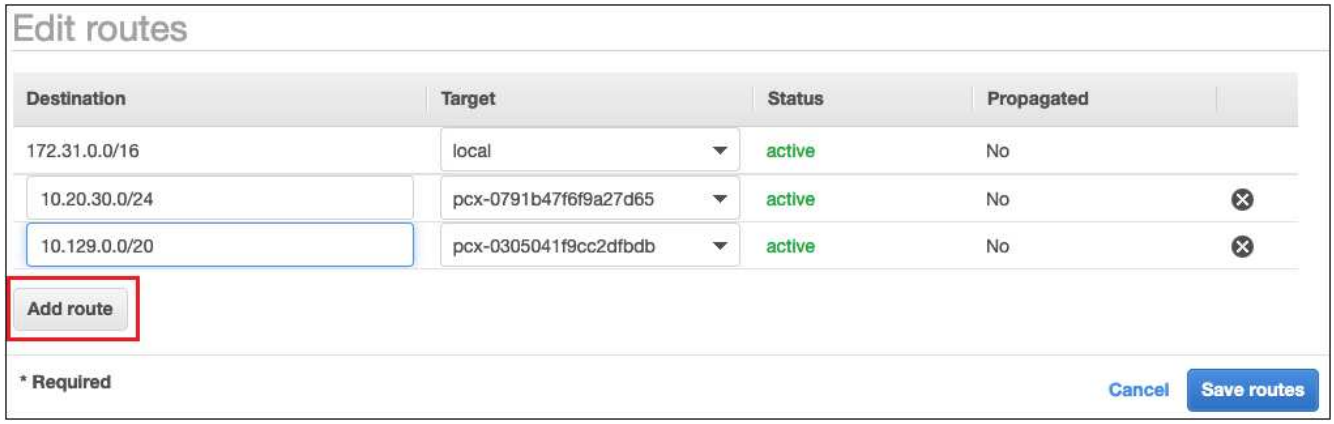
1. VPC > サブネット > ルートテーブルに移動します。



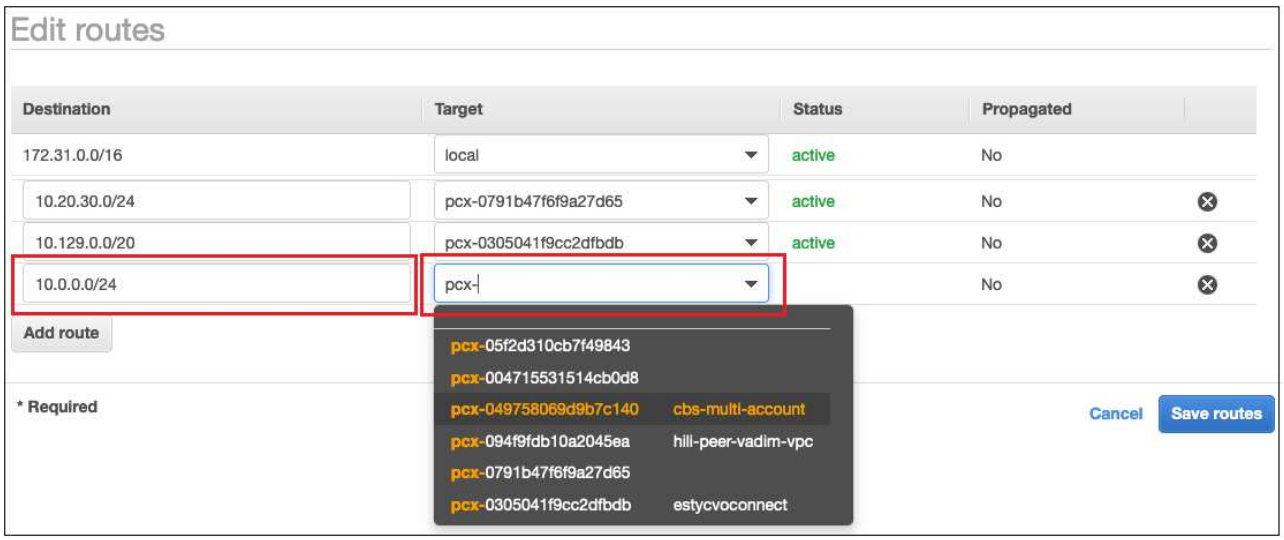
2. [ルート] タブをクリックします。



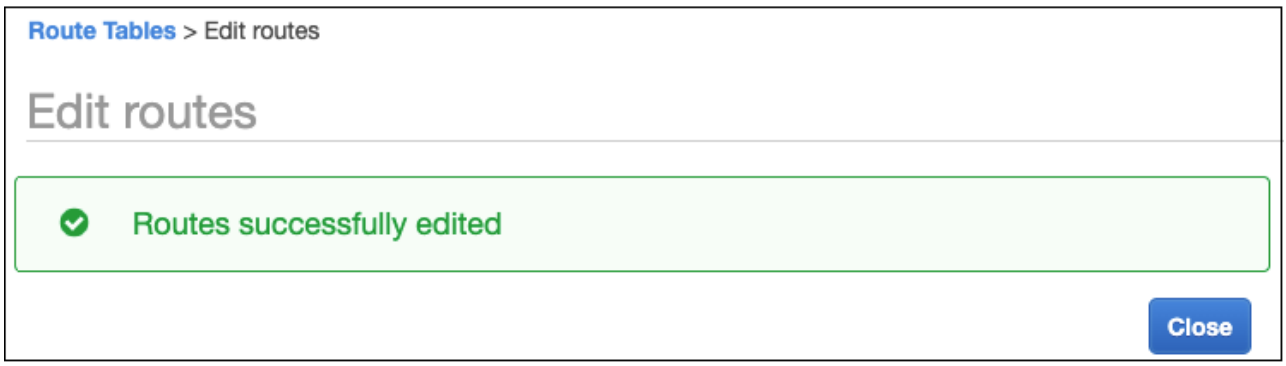
3. * ルートの編集 * をクリックします。



4. [Add route*] をクリックし、 [Target] ドロップダウンリストから [* ピアリング接続 *] を選択して、作成したピアリング接続を選択します。
   a. デスティネーションで、もう一方のアカウントのサブネット CIDR を入力します。

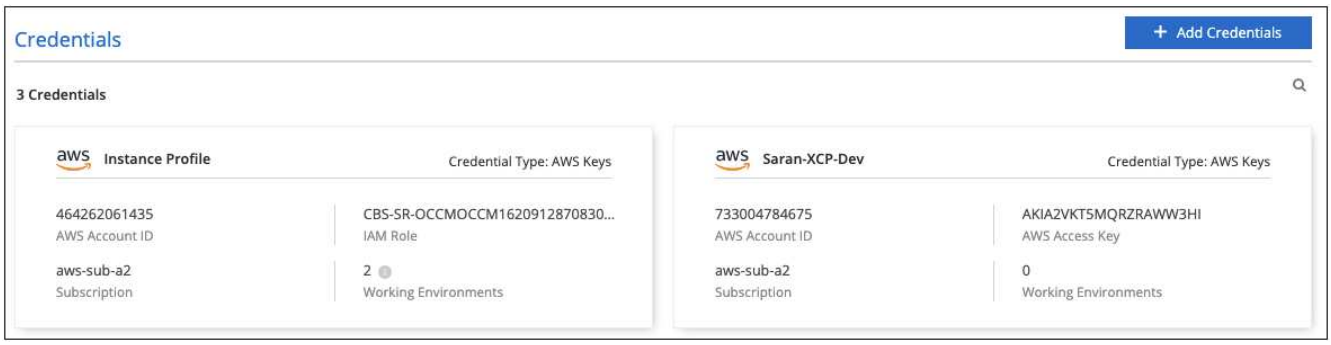


b. [ルートの保存（ Save Routes ）] をクリックすると、 [成功（ Success ）] ダイアログが

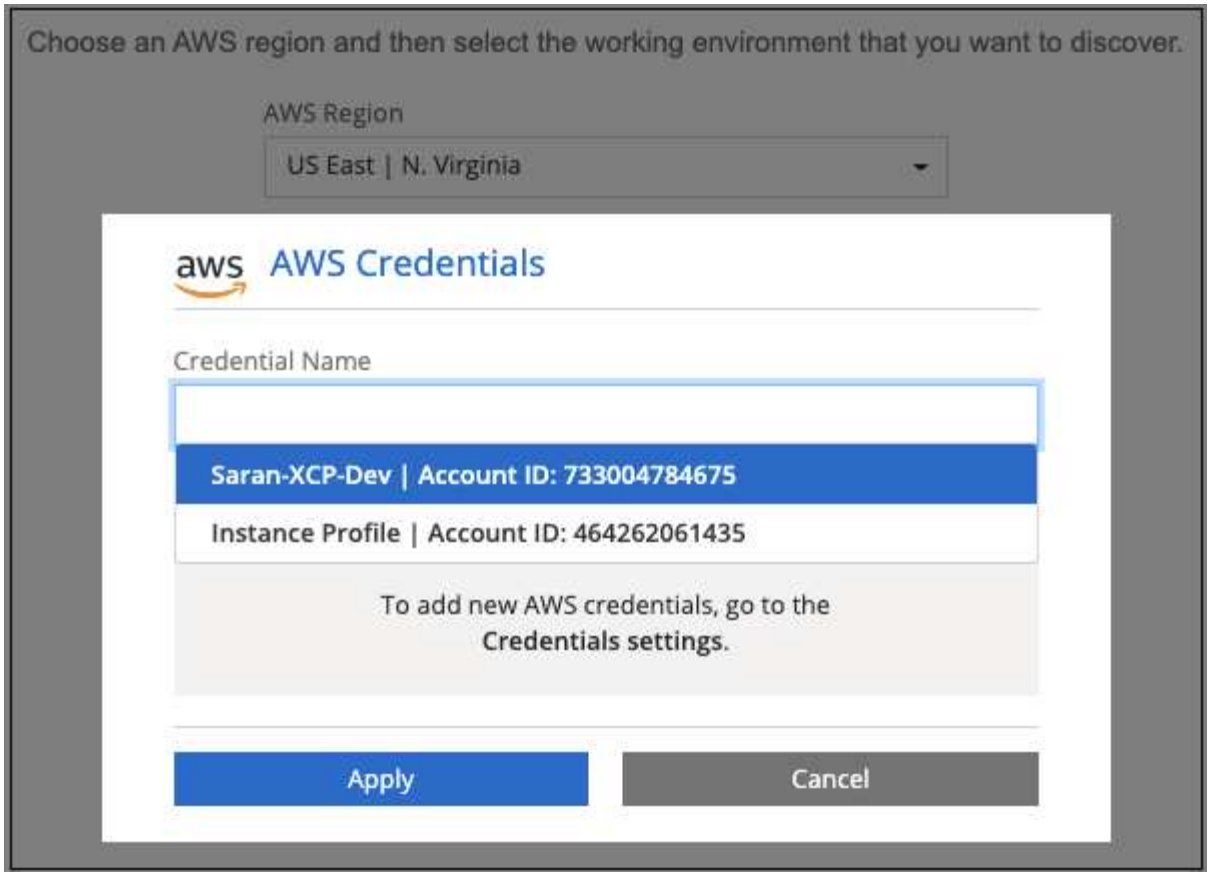


Cloud Manager で **2** つ目の **AWS** アカウントのクレデンシャルを追加します

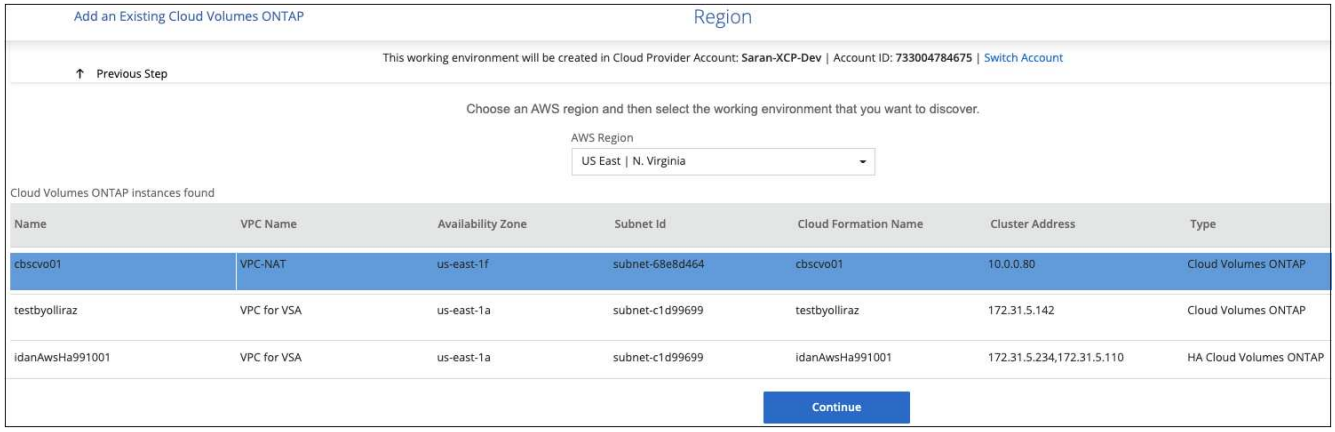
1. 2 つ目の AWS アカウントを追加します。例： *Saran - XCP - Dev*.



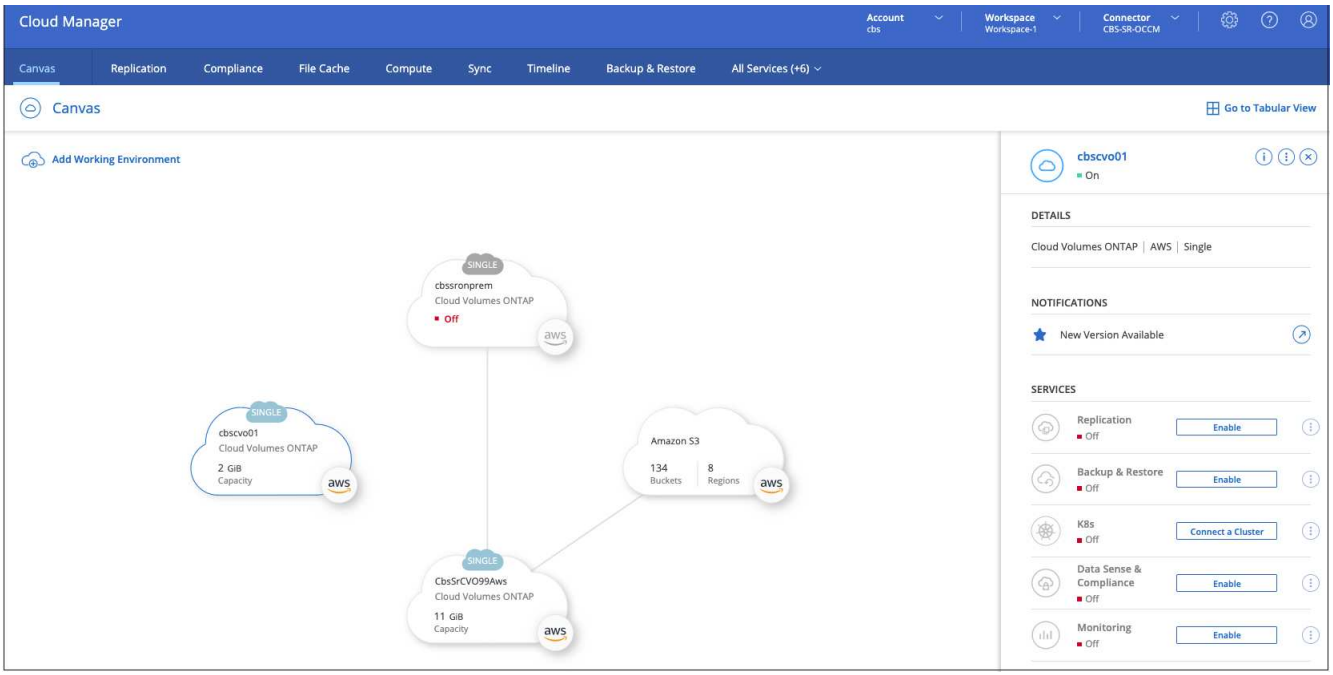
2. Discover Cloud Volumes ONTAP ページで、新しく追加したクレデンシャルを選択します。



3. 2 つ目のアカウントから検出する Cloud Volumes ONTAP システムを選択します。2 番目のアカウントに新しい Cloud Volumes ONTAP システムを導入することもできます。

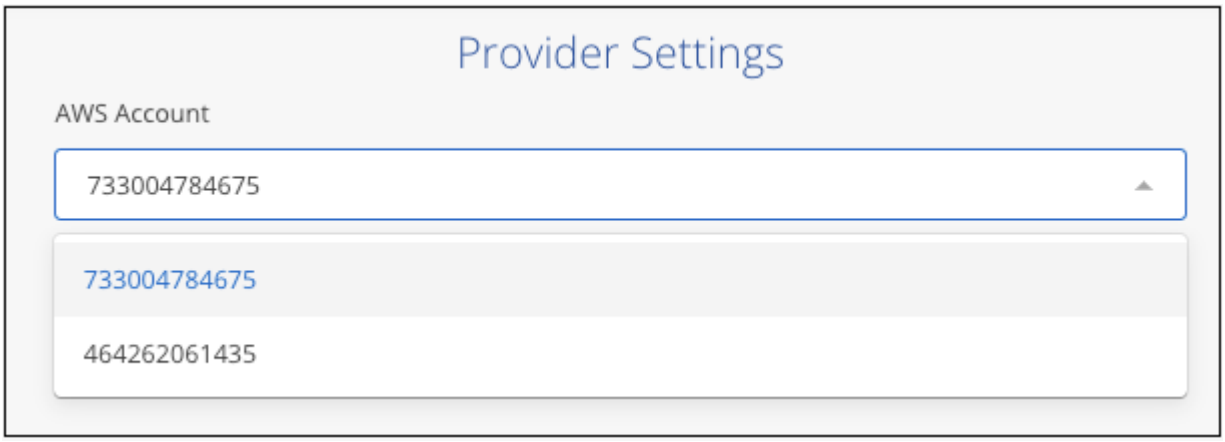


2 番目のアカウントの Cloud Volumes ONTAP システムが、別のアカウントで実行されている Cloud Manager に追加されます。



もう一方の **AWS** アカウントでバックアップを有効にします

1. Cloud Manager で、最初のアカウントで実行されている Cloud Volumes ONTAP システムのバックアップを有効にし、 2 番目のアカウントをバックアップファイルの作成場所として選択します。



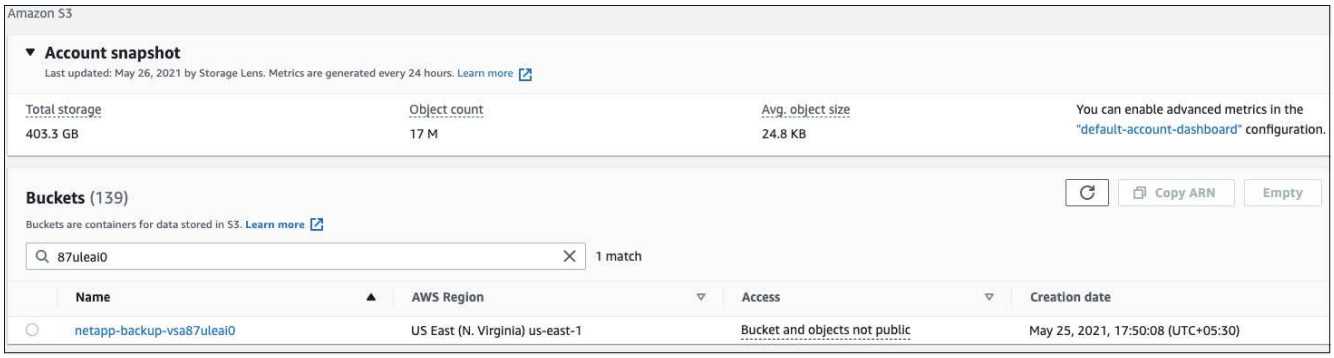
2. 次に、バックアップポリシーとバックアップするボリュームを選択し、 Cloud Backup は選択したアカウントで新しいバケットを作成しようとします。

   ただし、 Cloud Volumes ONTAP システムへのバケットの追加は失敗します。これは、 Cloud Backup がインスタンスプロファイルを使用してバケットを追加するためで、 Cloud Manager インスタンスプロファイルが 2 番目のアカウントのリソースにアクセスできないためです。

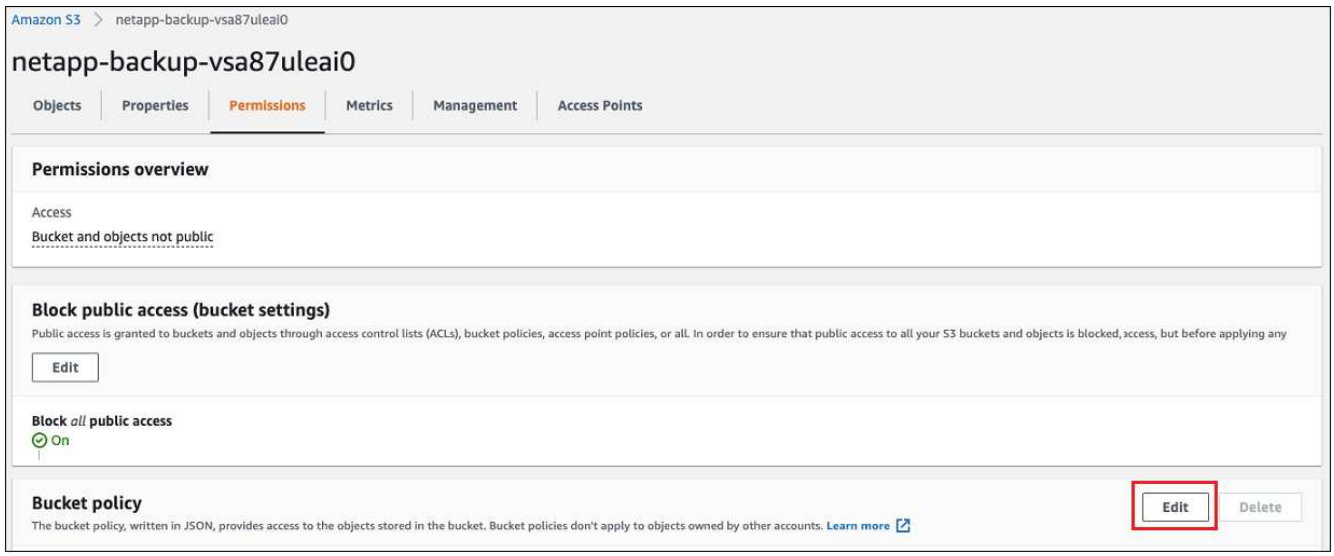
3. Cloud Volumes ONTAP システムの作業環境 ID を取得します。

Cloud Backup は「 NetApp-backup- 」というプレフィックスを付けてすべてのバケットを作成し、作業環境 ID を含めます。たとえば「 87ULea10 」となります

4. EC2 ポータルで S3 に移動し、「 87uLea10 」で終わる名前のバケットを検索すると、「 NetApp-backup-vsa87uLea10 」と表示されるバケット名が表示されます。



5. バケットをクリックし、 [権限] タブをクリックして、 [バケットポリシー] セクションの **Edit** をクリックします。



6. 新しく作成したバケットのバケットポリシーを追加して、 Cloud Manager の AWS アカウントにアクセスできるようにしてから、変更を保存します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicRead",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::464262061435:root"
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::netapp-backup-vsa87uleai0",
        "arn:aws:s3:::netapp-backup-vsa87uleai0/*"
      ]
    }
  ]
}
```

「 aws 」 ： "aws ： "arn ： aws ： 464262061435 ： root 」ではアカウント 464262061435 のすべてのリソースにこのバケットへのアクセスを許可しています。特定のロールレベルに減らすには、特定のロールでポリシーを更新します。ロールを個別に追加する場合は、 occm ロールも追加する必要があります。追加しないと、 Cloud Backup UI でバックアップが更新されません。

例： "AWS" ： "arn ： aws ： IAM ： 464262061435 ： role/CVO-instance-profileversion10-d8e-IamInstanceRole-IKJP1HC2E7R"

7. Cloud Volumes ONTAP システムでクラウドバックアップの有効化を再度実行して、成功することを確認します。

Azure でマルチアカウントアクセスのバックアップを設定する

Cloud Backup では、ソース Cloud Volumes ONTAP ボリュームとは別の Azure アカウントにバックアップファイルを作成できます。これらのアカウントは、 Cloud Manager Connector がインストールされているアカウントとは異なる場合があります。

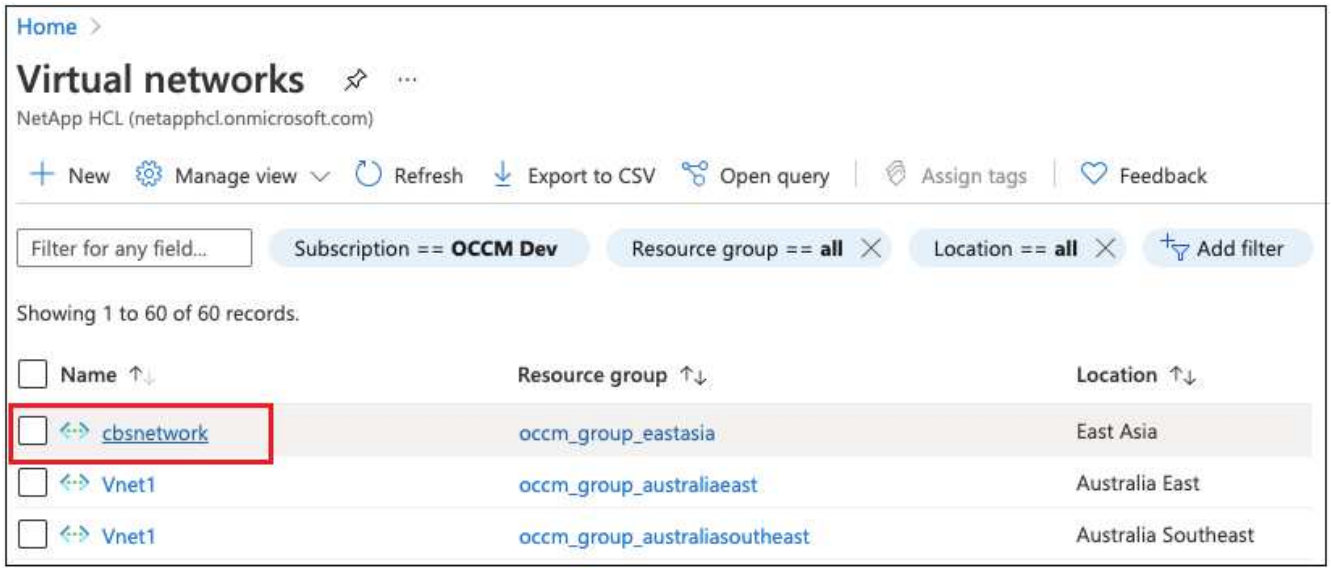
これらの手順は、を実行している場合にのみ必要です "Cloud Volumes ONTAP データの Azure BLOB ストレージへのバックアップ"。

この方法で設定を行うには、次の手順を実行します。

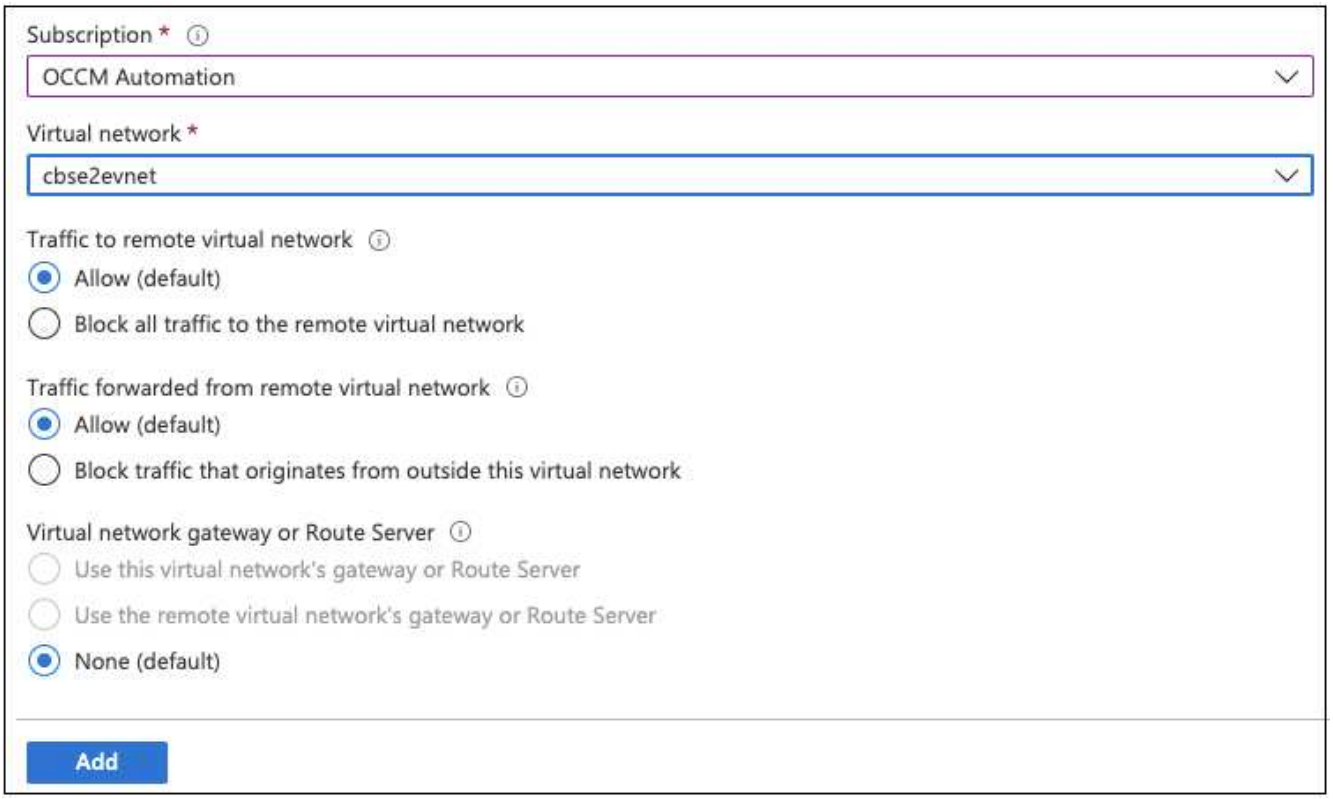
アカウント間の **VNet** ピアリングを設定します

Cloud Manager で別のアカウントやリージョンの Cloud Volumes ONTAP システムを管理する場合は、 VNet ピアリングを設定する必要があります。ストレージアカウントの接続に VNet ピアリングは必要ありません。

1. Azure ポータルにログインし、ホームから仮想ネットワークを選択します。
2. サブスクリプション 1 として使用するサブスクリプションを選択し、ピアリングを設定する VNet 上でクリックします。

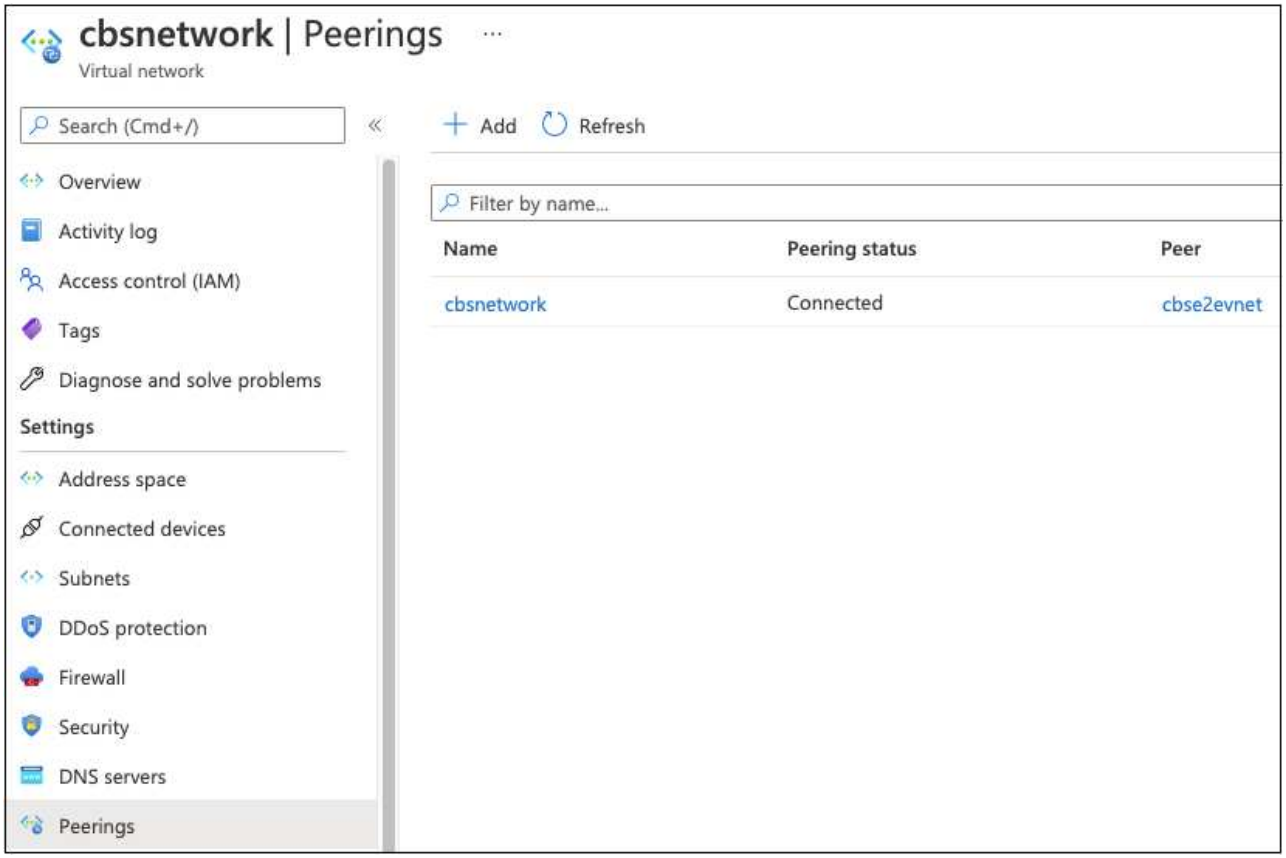


3. **cbsnetwork** を選択し、左パネルから **peerings** をクリックし、 * Add * をクリックします。

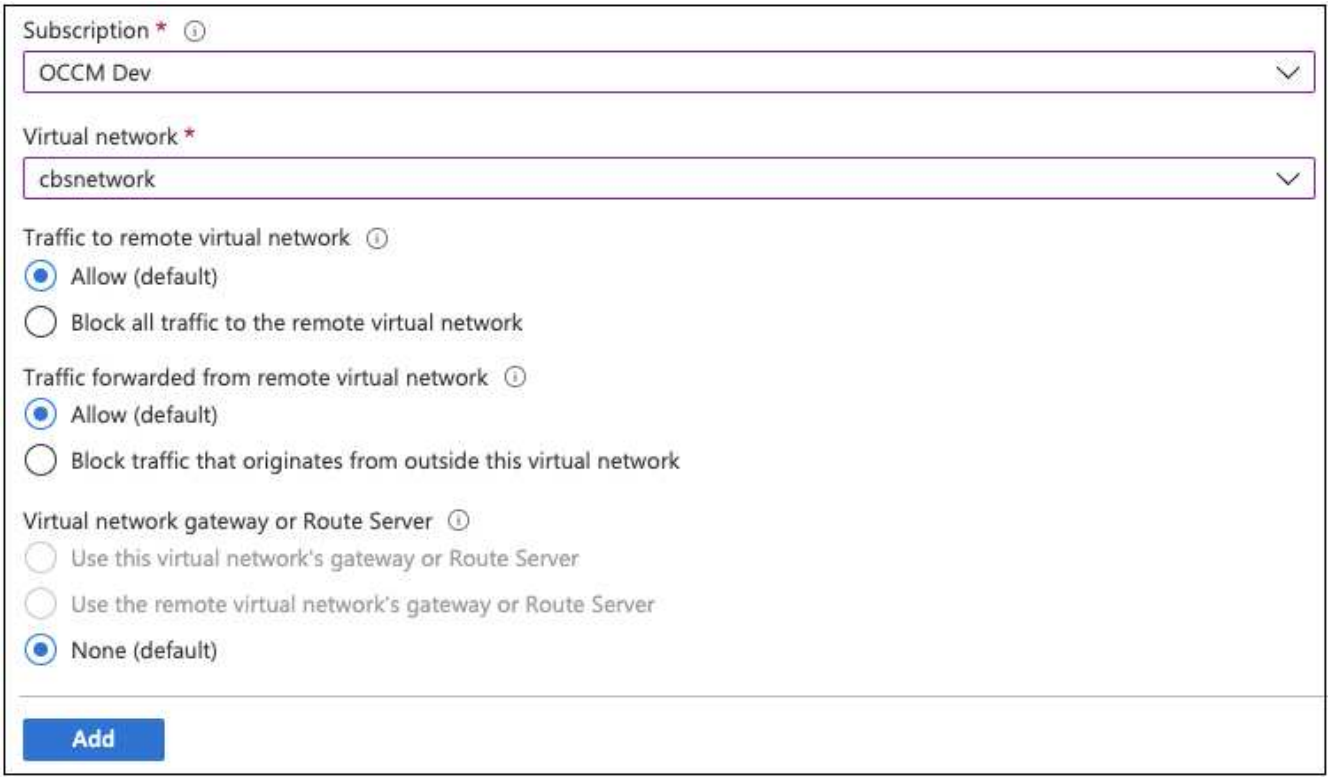


4. ピアリングページで次の情報を入力し、 * 追加 * をクリックします。

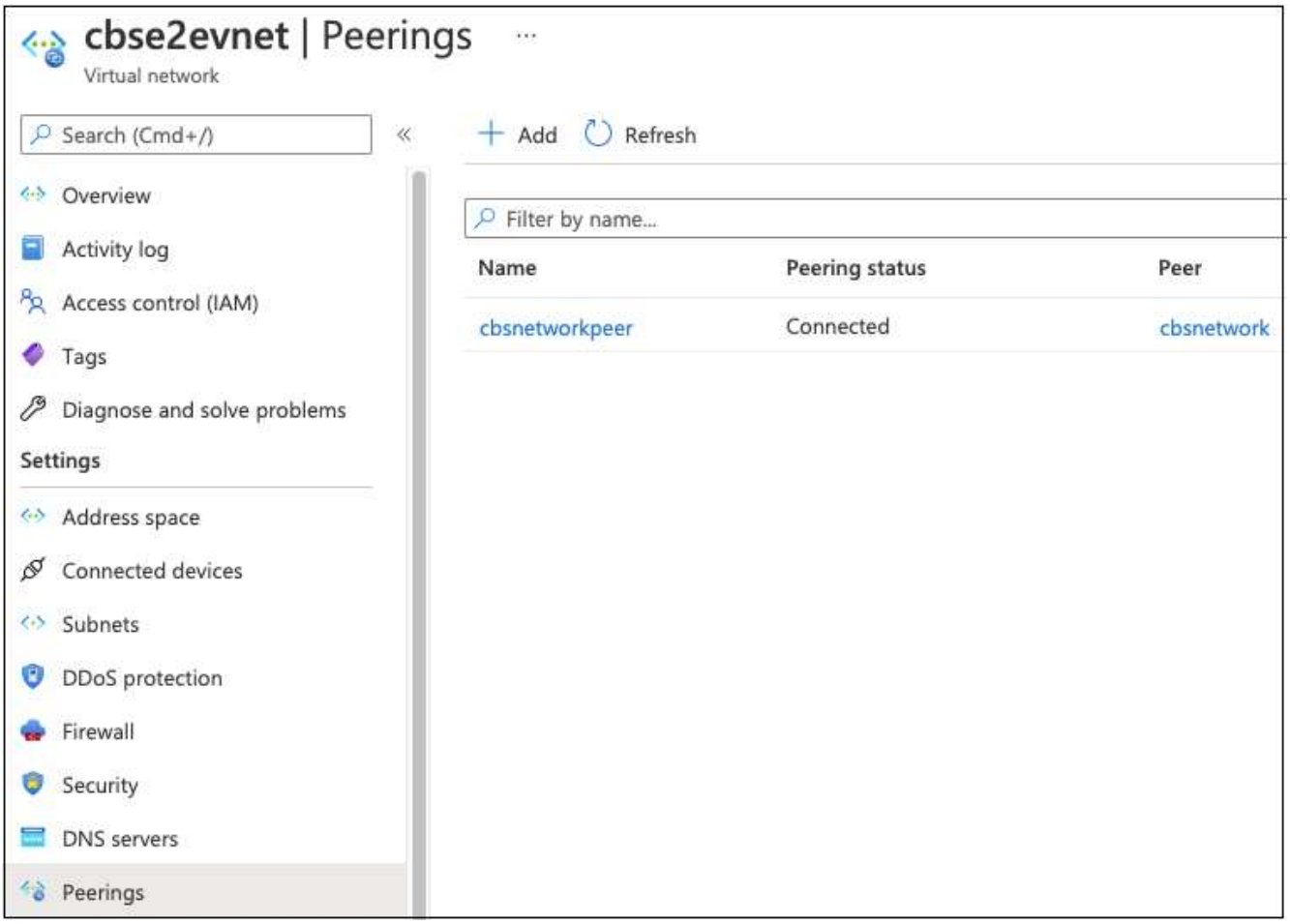
- このネットワークのピアリングリンク名：ピアリング接続を識別する任意の名前を指定できます。
- リモート仮想ネットワークピアリングリンク名：リモート VNet を識別するための名前を入力します。
- すべての選択をデフォルト値のままにします。
- [サブスクリプション] で、サブスクリプション 2 を選択します。
- 仮想ネットワーク：ピアリングを設定するサブスクリプション 2 の仮想ネットワークを選択します。



5. サブスクリプション 2 VNet 内で同じ手順を実行し、サブスクリプション 1 のサブスクリプションおよびリモート VNet の詳細を指定します。



ピアリング設定が追加されます。



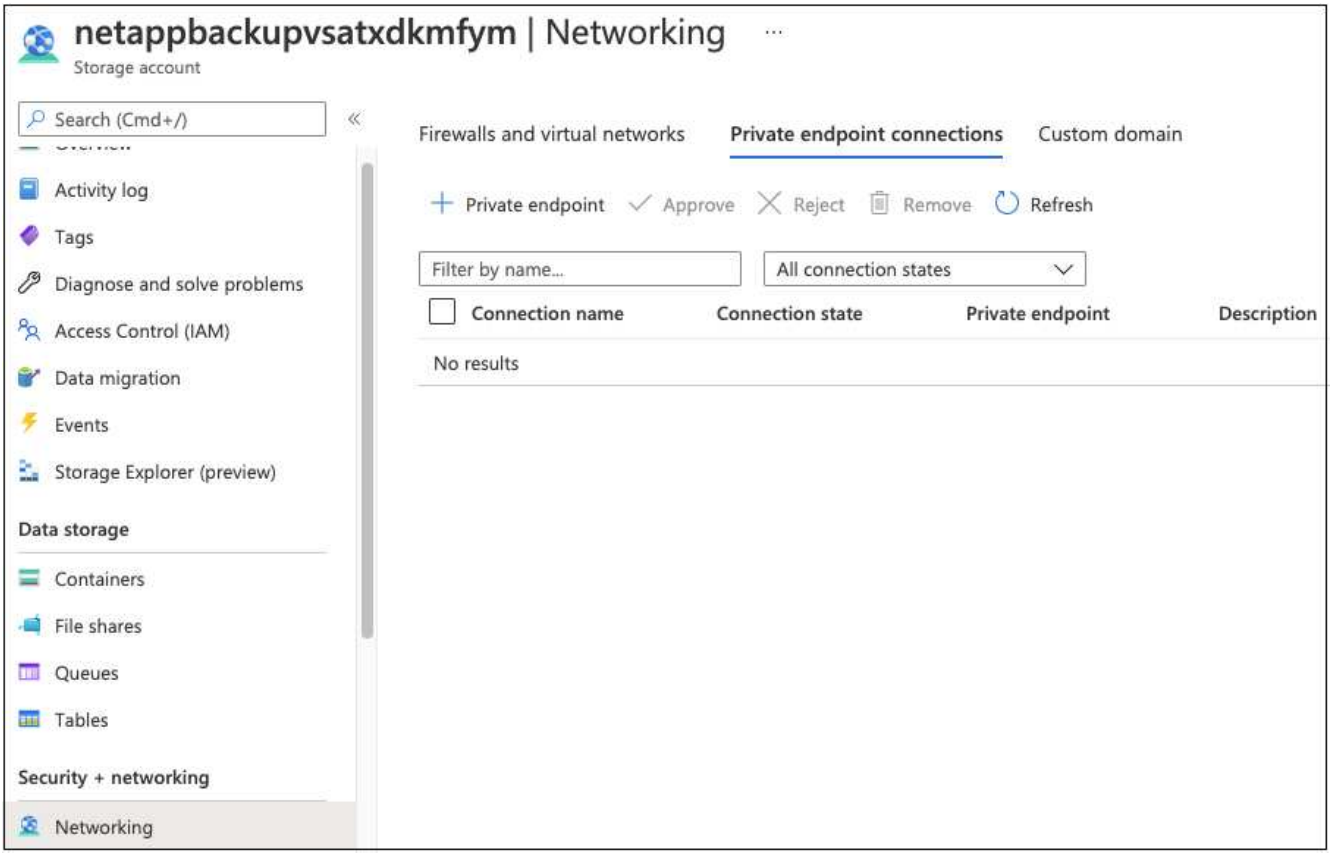
ストレージアカウントのプライベートエンドポイントを作成します

次に、ストレージアカウント用のプライベートエンドポイントを作成する必要があります。この例では、サブスクリプション 1 でストレージアカウントが作成され、 Cloud Volumes ONTAP システムはサブスクリプション 2 で実行されています。

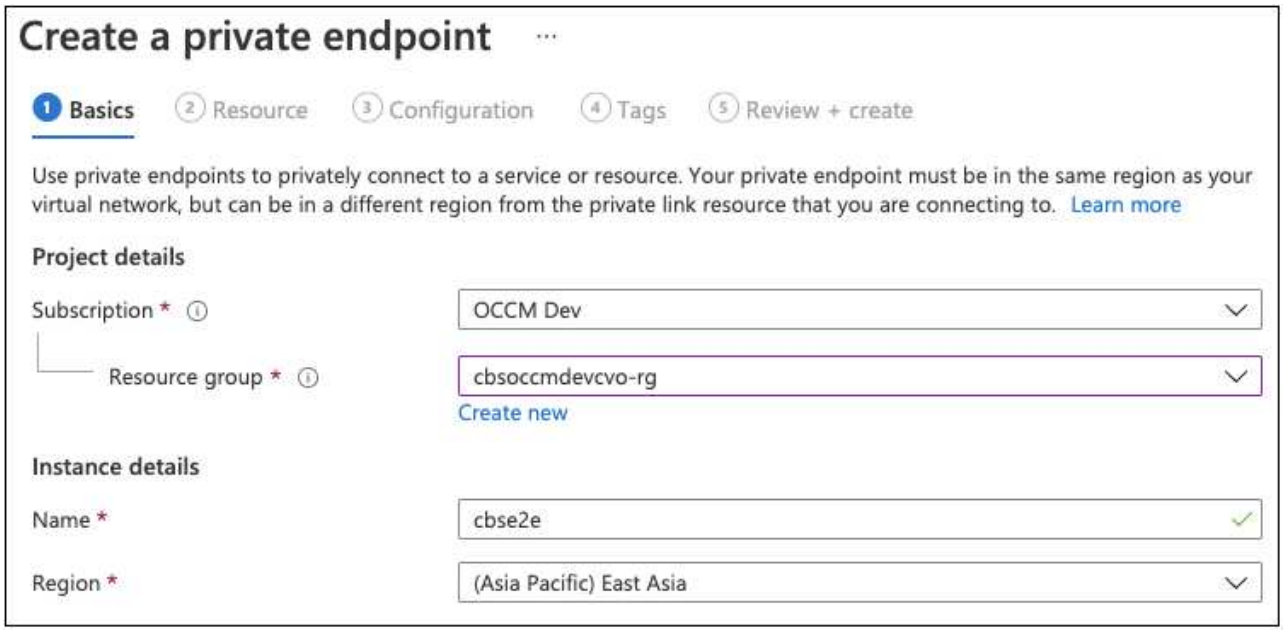
次の操作を実行するには、ネットワーク作成者の権限が必要です。

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

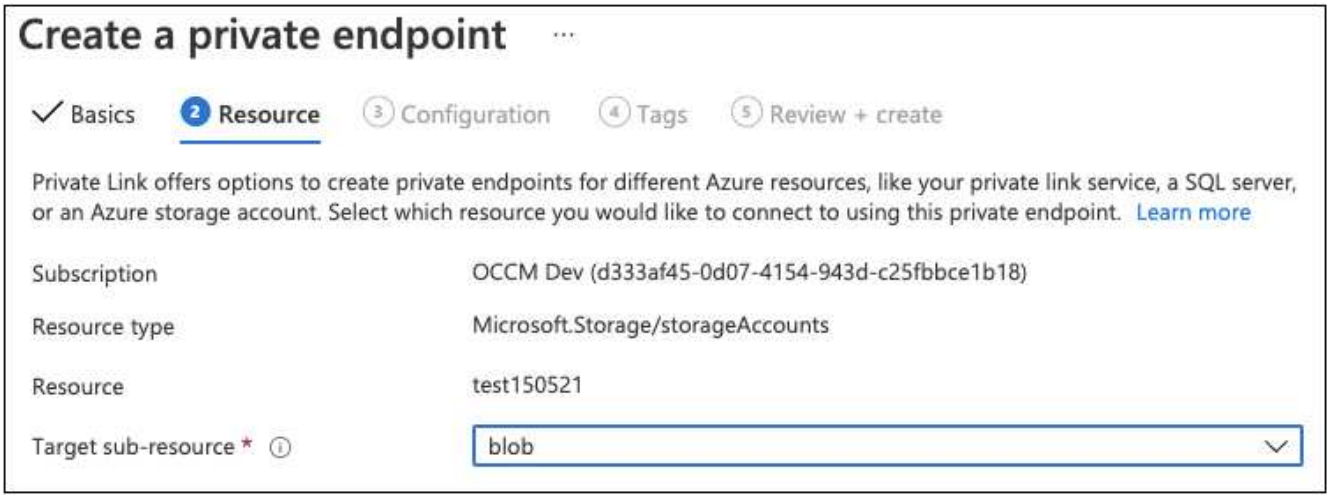
1. ストレージアカウント > ネットワーク > プライベートエンドポイント接続に移動し、 * + プライベートエンドポイント * をクリックします。



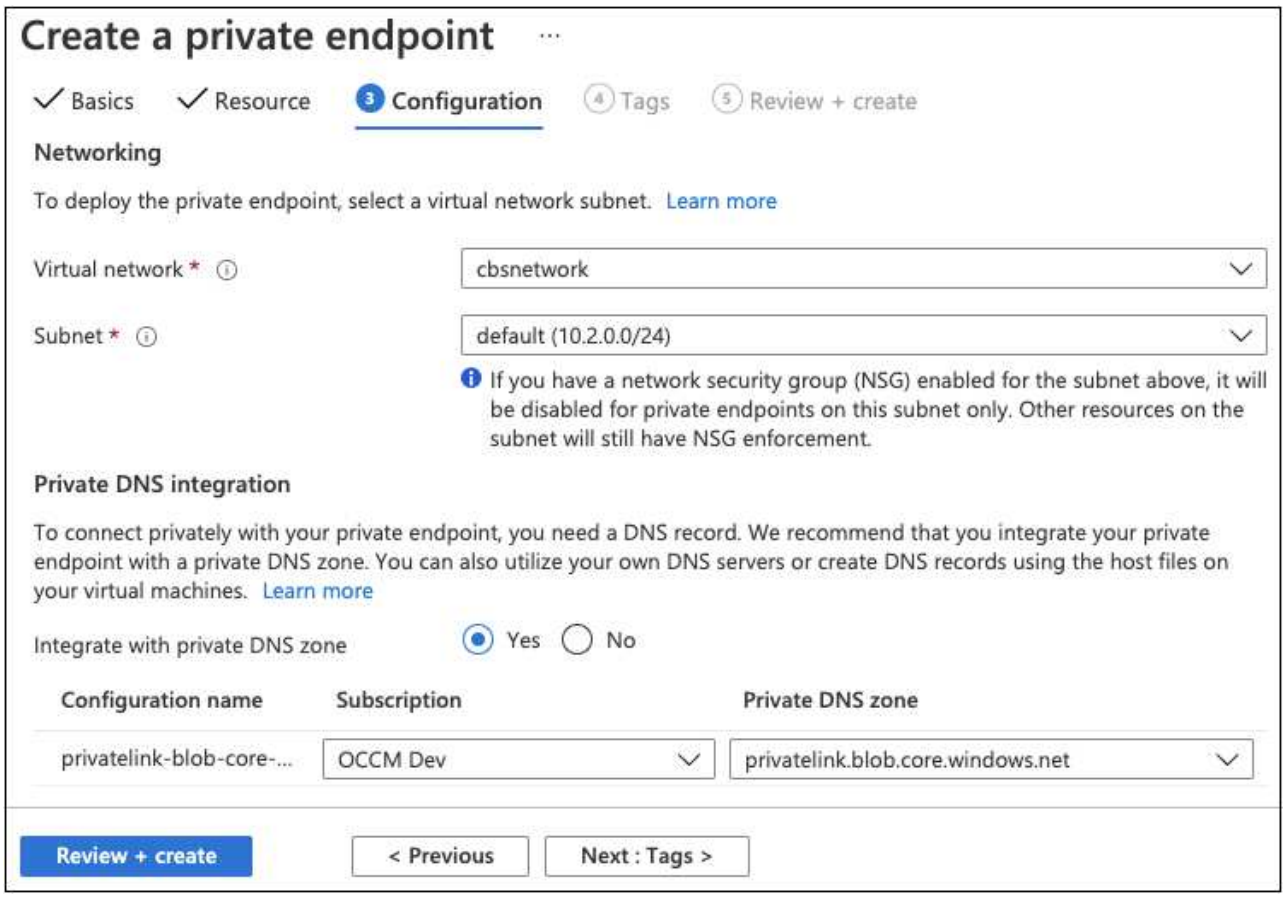
2. Private Endpoint_Basics_page で、次の手順を実行します。
   - サブスクリプション 2 （ Cloud Manager Connector と Cloud Volumes ONTAP システムを導入する場所）とリソースグループを選択します。
   - エンドポイント名を入力します。
   - リージョンを選択します。



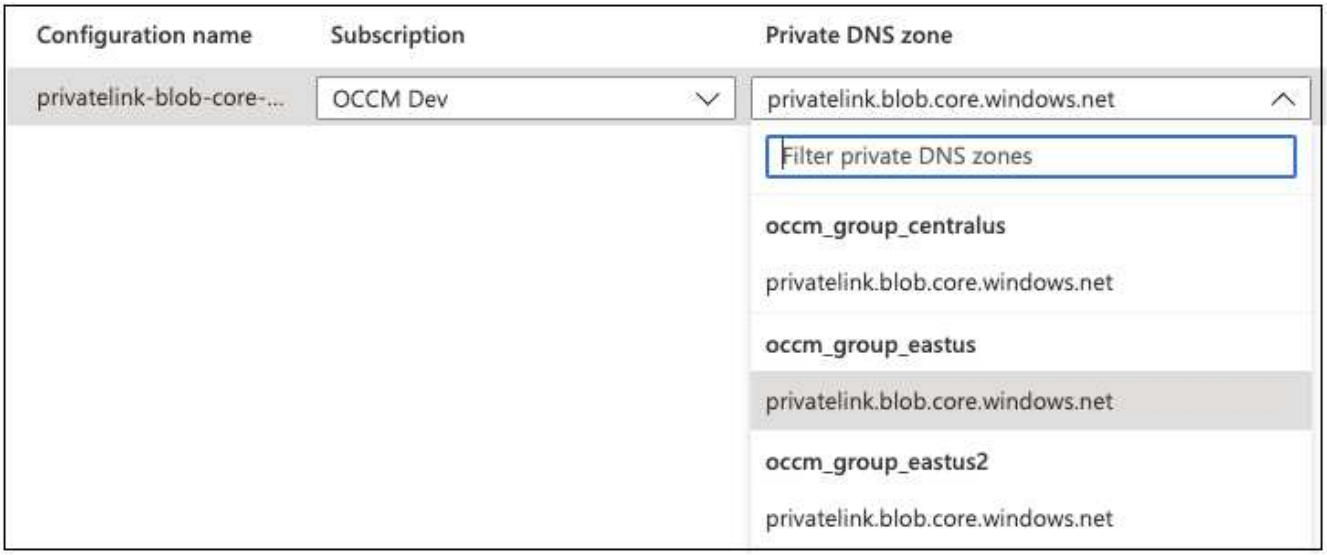
3. _Resource_page で ' ターゲットサブリソースとして *blob * を選択します



4. 設定ページで、次の操作を行います。
   - 仮想ネットワークとサブネットを選択します。
   - [はい *] ラジオボタンをクリックして、 [プライベート DNS ゾーンと統合] を選択します。



5. [プライベート DNS ゾーン] リストで、正しいリージョンからプライベートゾーンが選択されていることを確認し、 [* レビュー + 作成 *] をクリックします。



これで、ストレージアカウント（サブスクリプション 1 ）は、サブスクリプション 2 で実行されている Cloud Volumes ONTAP システムにアクセスできます。

6. Cloud Volumes ONTAP システムでクラウドバックアップの有効化を再度実行して、成功することを確認します。

著作権情報

商標情報