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 Manager

Tom Onacki
July 06, 2021

目次

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

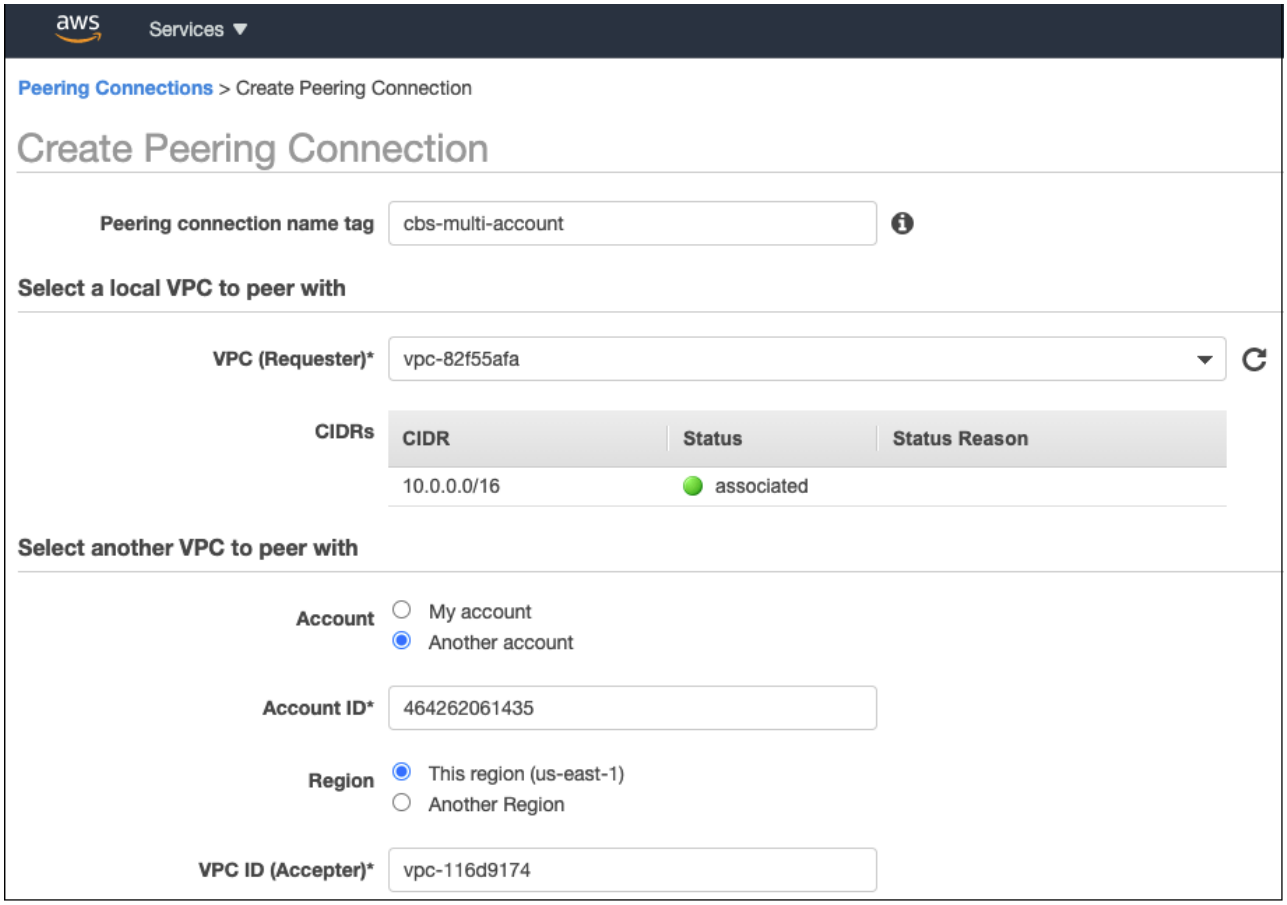
1. 2 つ目のアカウントにログインし、ピアリング接続を作成します。

    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。

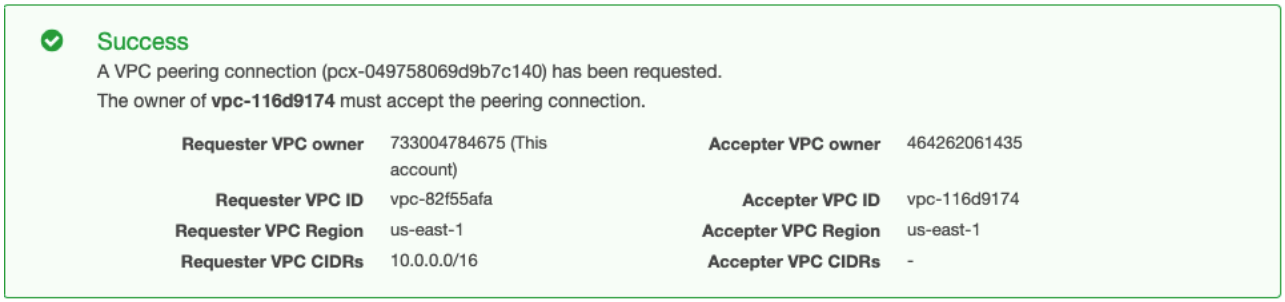
    b. 別の VPC を選択：最初のアカウントのアカウント ID を入力します。

    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。

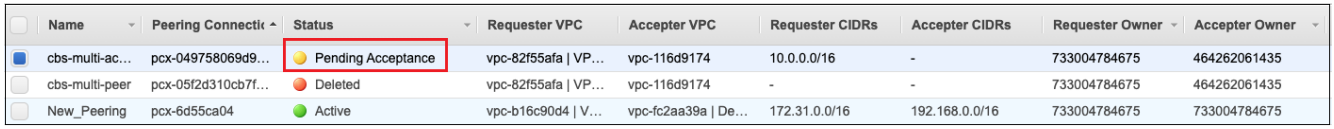
    d. VPC ID ：最初のアカウントにログインし、アクセプタ VPC ID を入力します。Cloud Manager Connector の VPC ID です。



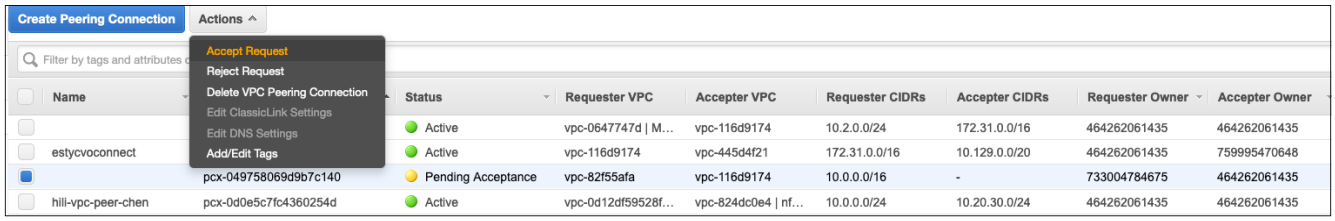
成功ダイアログが表示されます。



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。

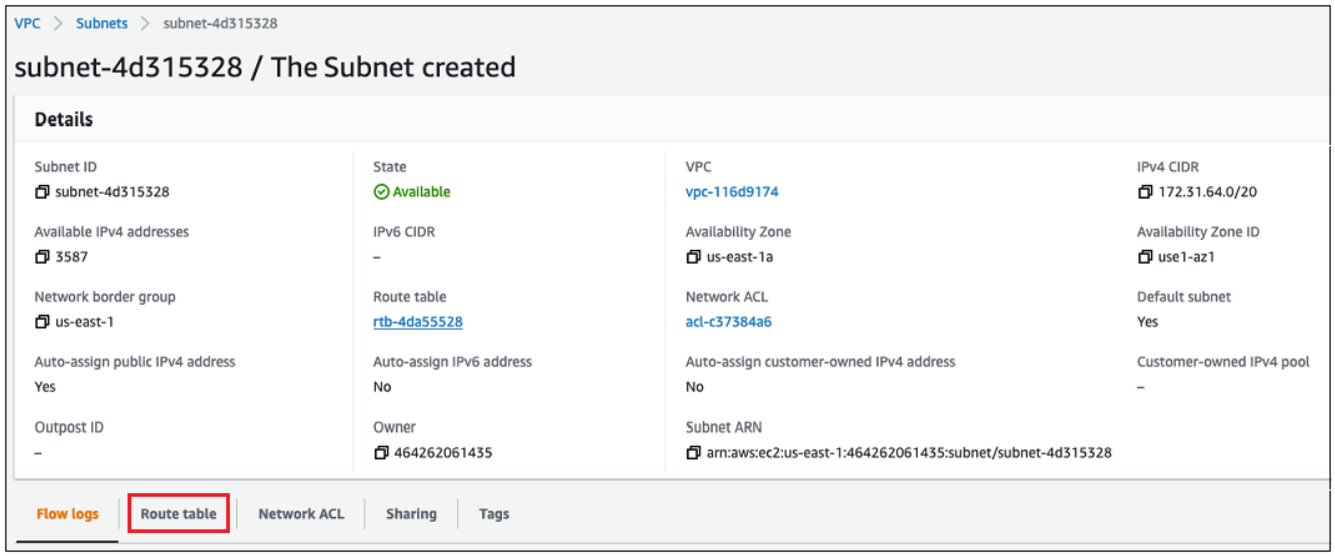
Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
	pcx-004715531514cb0d8	Active	vpc-0647747d | M...	vpc-116d9174	10.2.0.0/24	172.31.0.0/16	464262061435	464262061435
estycvoconnect	pcx-0305041f9cc2dfbdb	Active	vpc-116d9174	vpc-445d4f21	172.31.0.0/16	10.129.0.0/20	464262061435	759995470648
cbs-multi-account	pcx-049758069d9b7c140	Active	vpc-82f55afa	vpc-116d9174	10.0.0.0/16	172.31.0.0/16	733004784675	464262061435
hili-vpc-peer-chen	pcx-0d0e5c7fc4360254d	Active	vpc-0d12df59528f...	vpc-824dc0e4 | nf...	10.0.0.0/24	10.20.30.0/24	464262061435	464262061435

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。

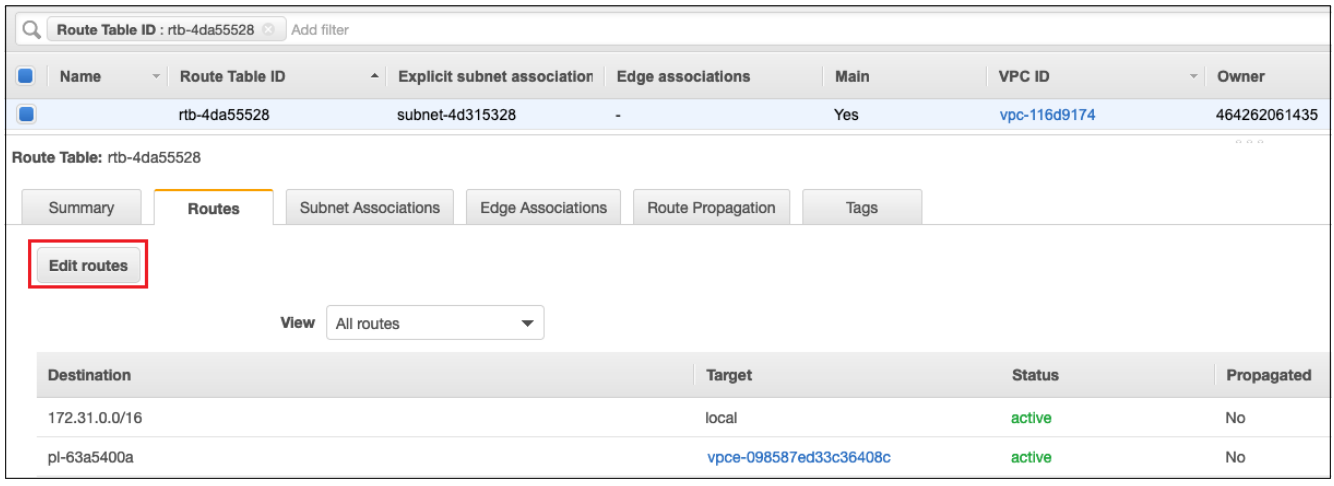
Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
cbs-multi-account	pcx-049758069d9b7c140	Active	vpc-82f55afa | VP...	vpc-116d9174	10.0.0.0/16	172.31.0.0/16	733004784675	464262061435
New_Peering	pcx-6d55ca04	Active	vpc-b16c90d4 | V...	vpc-fc2aa39a | De...	172.31.0.0/16	192.168.0.0/16	733004784675	733004784675

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

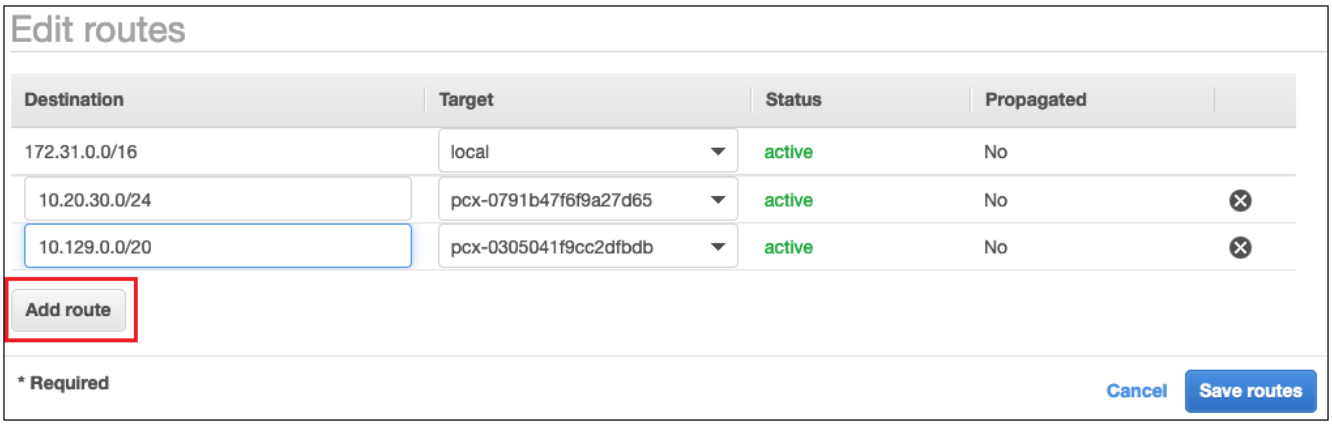
1. VPC > サブネット > ルートテーブルに移動します。



2. [ルート] タブをクリックします。

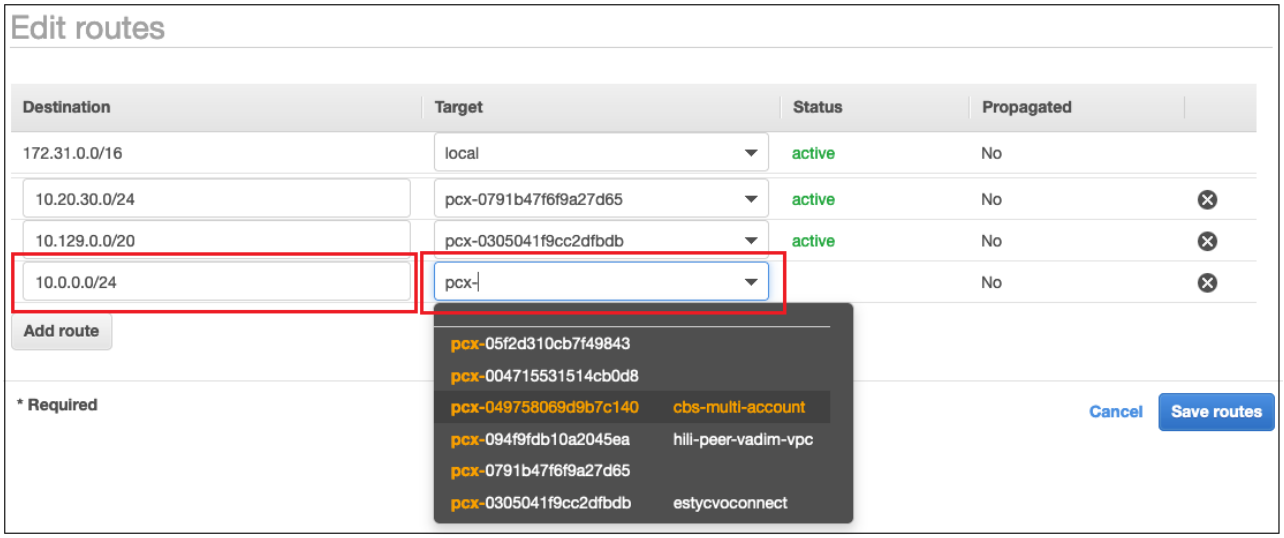


3. * ルートの編集 * をクリックします。

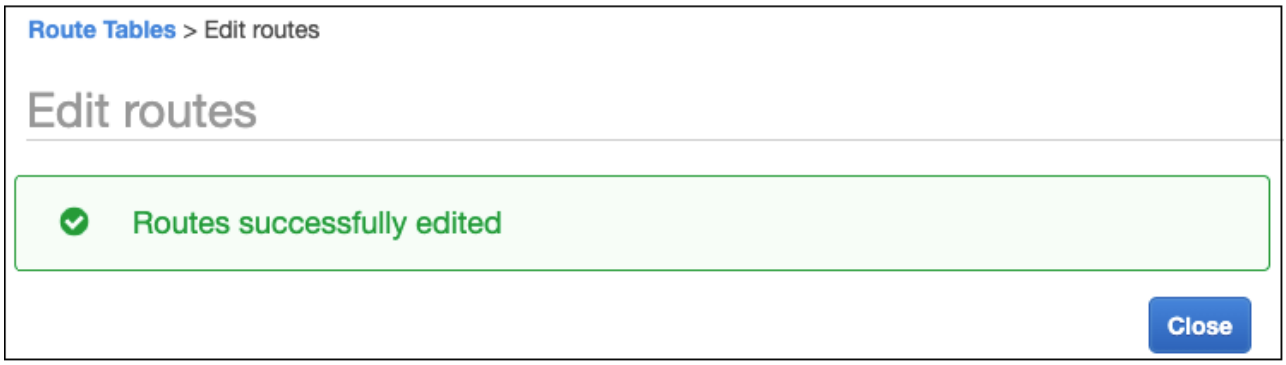


4. [Add route*] をクリックし、 [Target] ドロップダウンリストから [* ピアリング接続 *] を選択して、作成したピアリング接続を選択します。

   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。

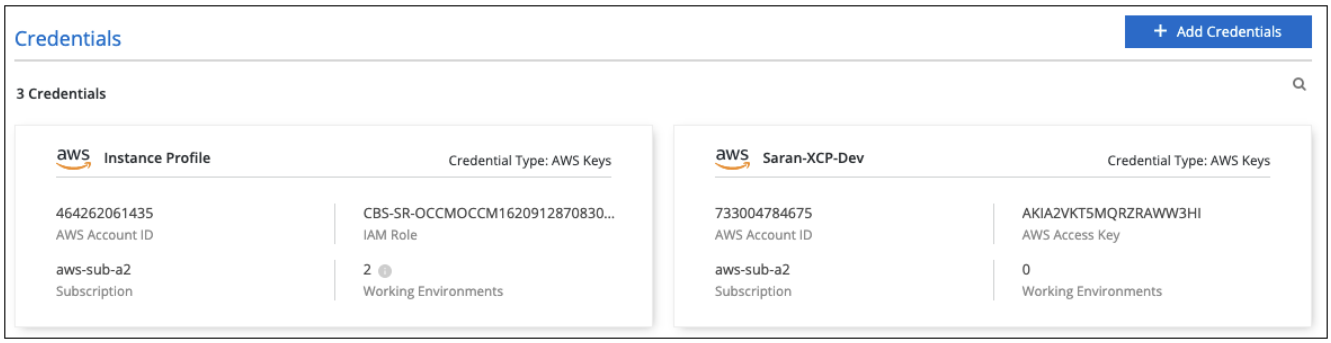


   b. [ルートの保存（ Save Routes ）] をクリックすると、 [成功（ Success ）] ダイアログが

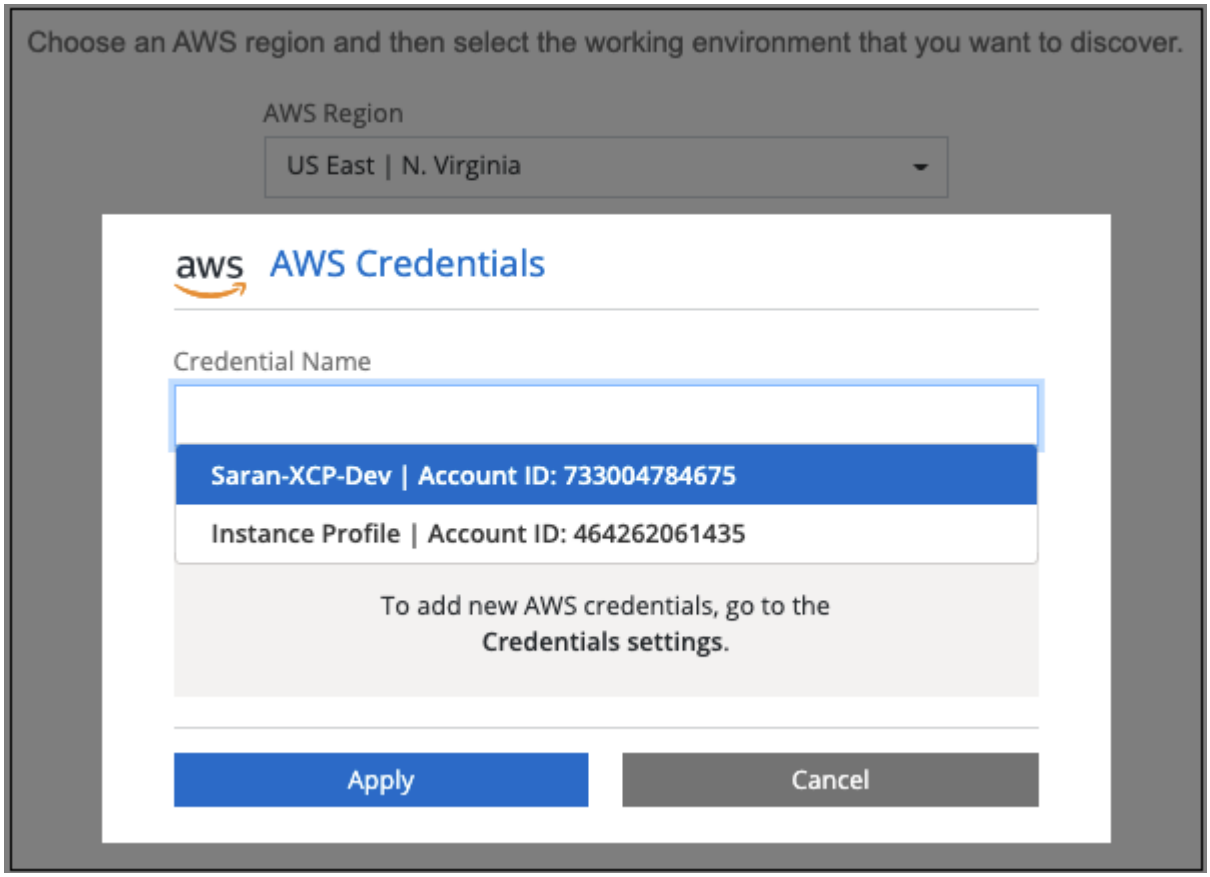


Cloud Manager で 2 つ目の AWS アカウントのクレデンシャルを追加します

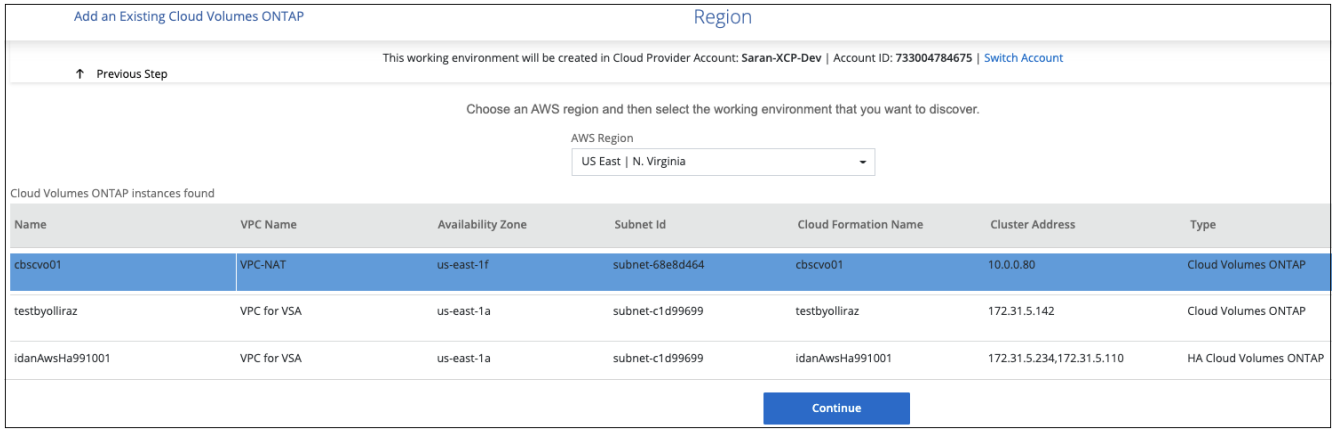
1. 2 つ目の AWS アカウントを追加します。例： *Saran - XCP - Dev*.



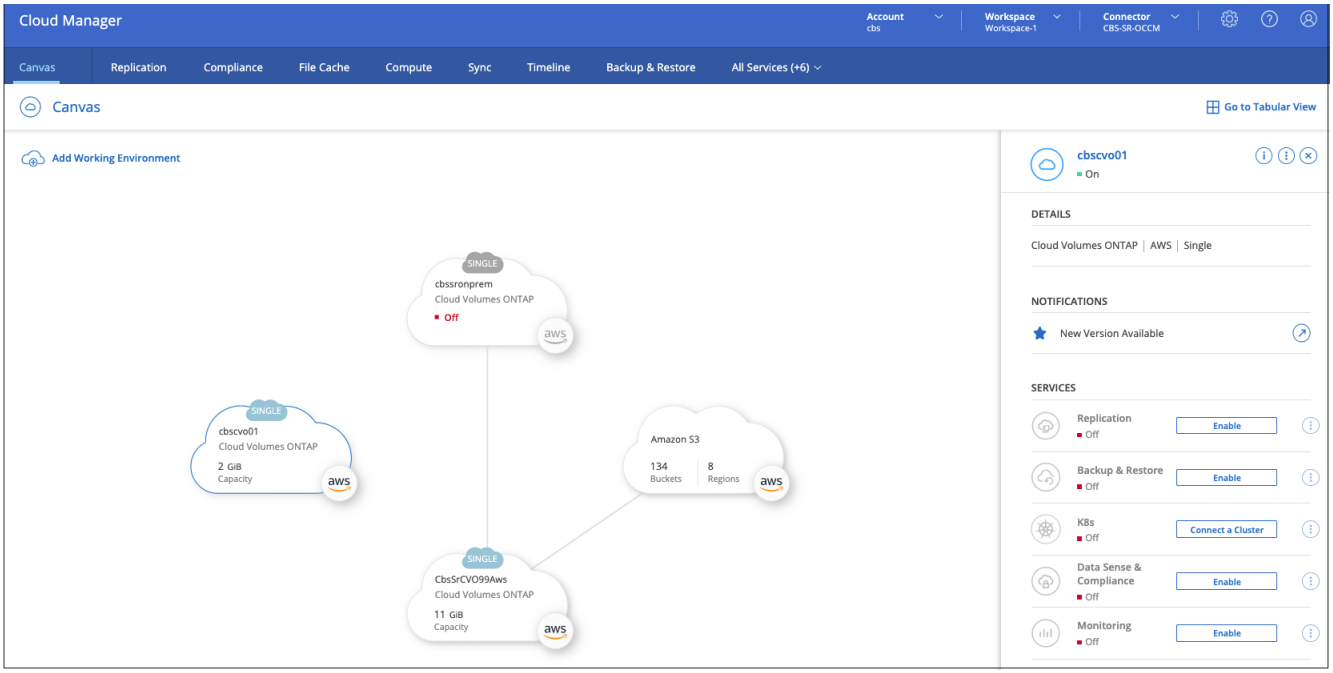
2. Discover Cloud Volumes ONTAP ページで、新しく追加したクレデンシャルを選択します。



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。

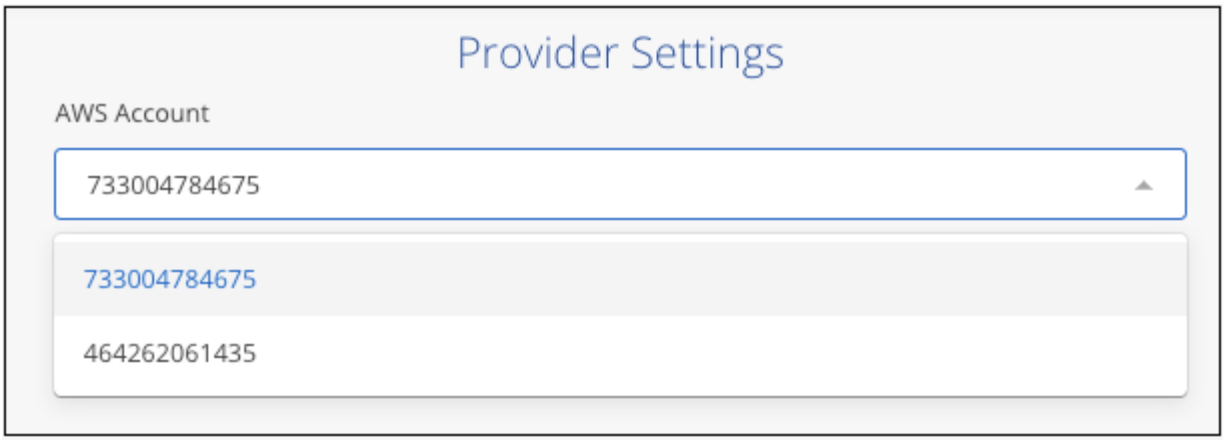


2 番目のアカウントの Cloud Volumes ONTAP システムが、別のアカウントで実行されている Cloud Manager に追加されます。



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

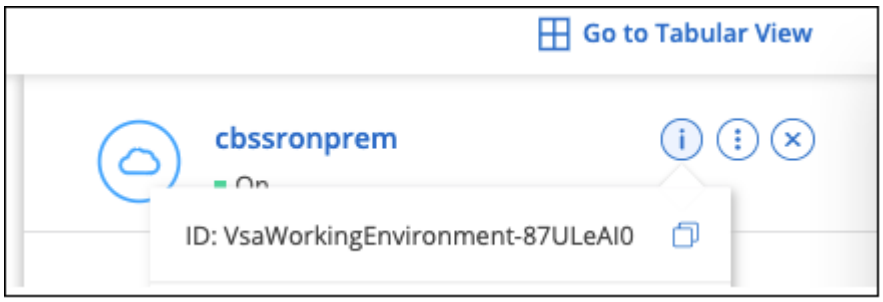
1. Cloud Manager で、最初のアカウントで実行されている Cloud Volumes ONTAP システムのバックアップを有効にし、 2 番目のアカウントをバックアップファイルの作成場所として選択します。



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。

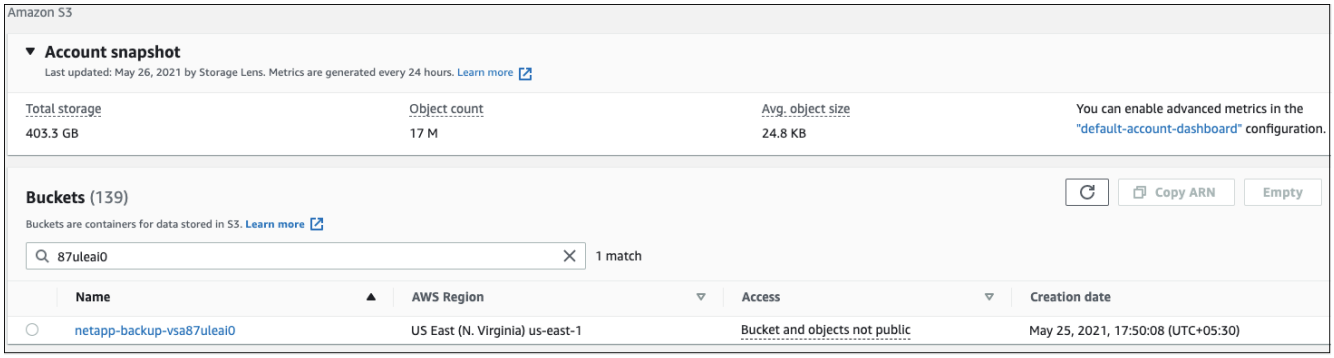
   ただし、 Cloud Volumes ONTAP システムへのバケットの追加は失敗します。これは、 Cloud Backup がインスタンスプロファイルを使用してバケットを追加するためで、 Cloud Manager インスタンスプロファイルが 2 番目のアカウントのリソースにアクセスできないためです。

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

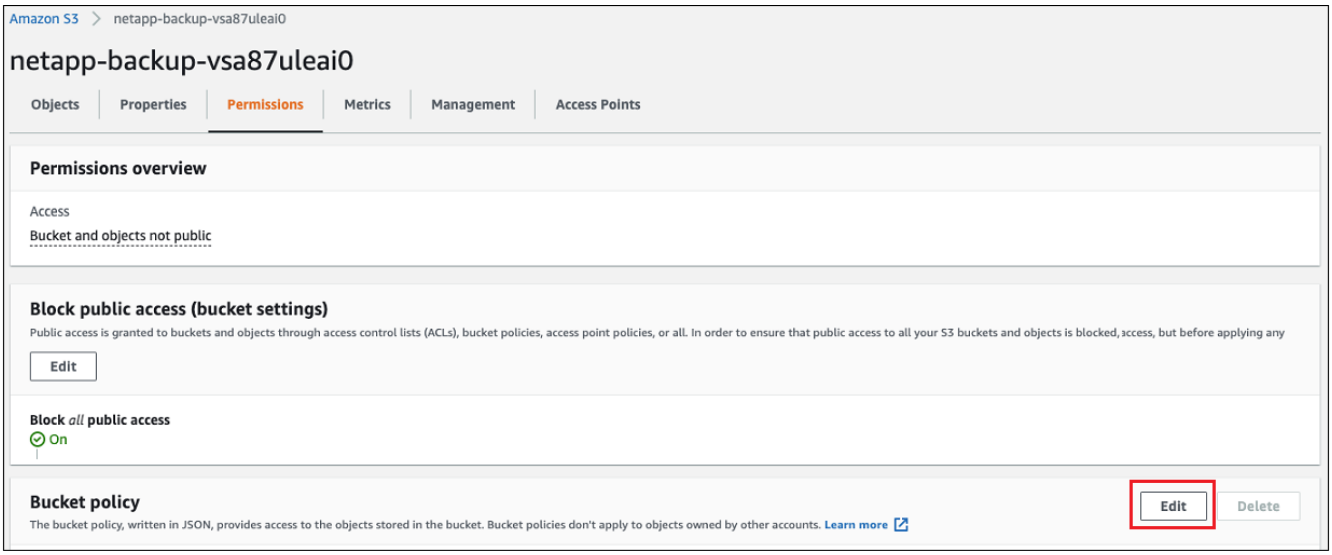


   Cloud Backup は「 NetApp-backup- 」というプレフィックスを付けてすべてのバケットを作成し、作業環境 ID を含めます。たとえば「 87ULea10 」となります

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。