Configure backup for multi-account access in AWS

Cloud Manager

Tom Onacki
June 15, 2021

Table of Contents

Configure backup for multi-account access in AWS . . . 1
Set up VPC peering between accounts . . . 1
Add a route to the route tables in both accounts . . . 3
Add the second AWS account credentials in Cloud Manager . . . 4
Enable backup in the other AWS account . . . 6

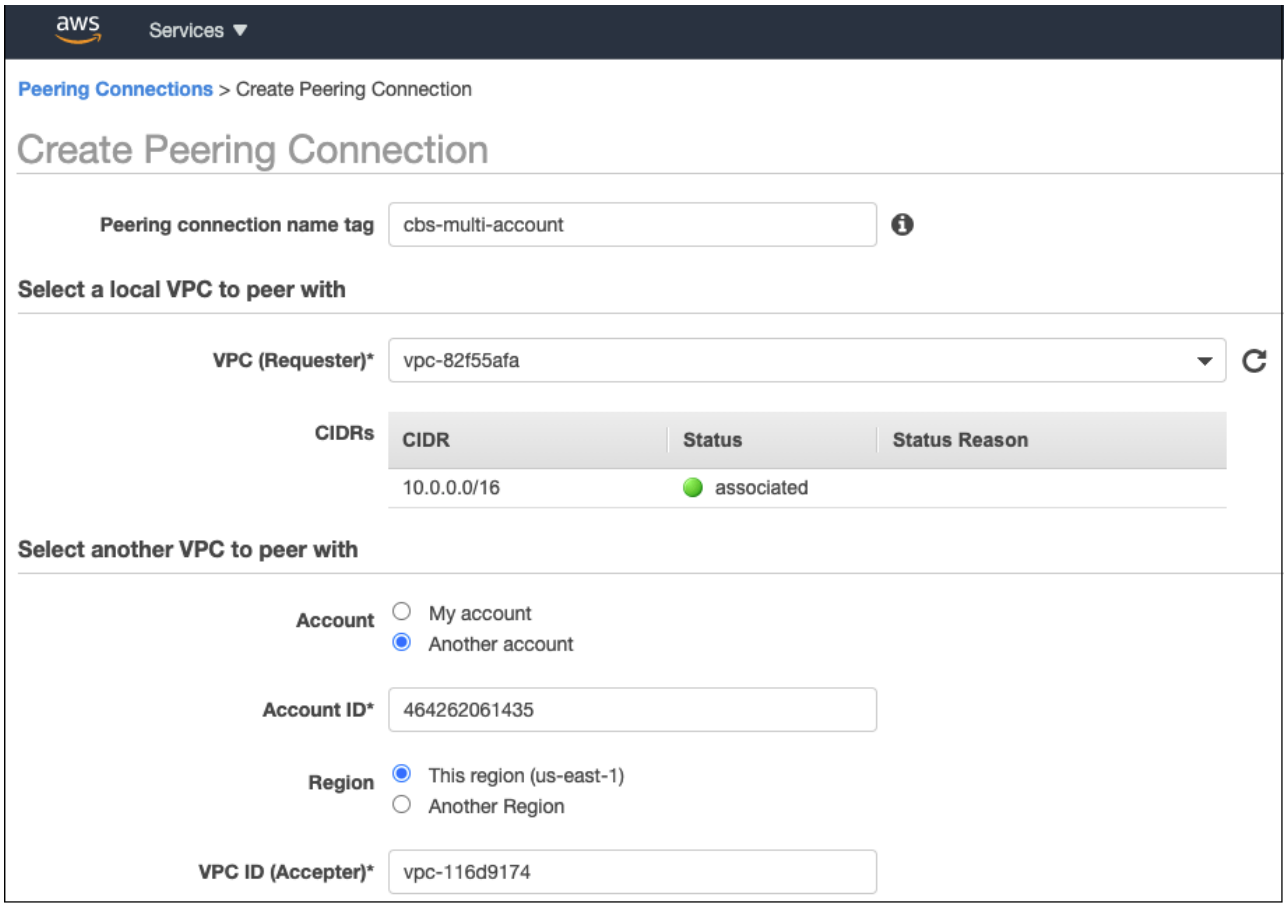
Configure backup for multi-account access in AWS

Cloud Backup enables you to create backup files in an AWS account that is different than where your source volumes reside. And both of those accounts can be different than the account where the Cloud Manager Connector resides.

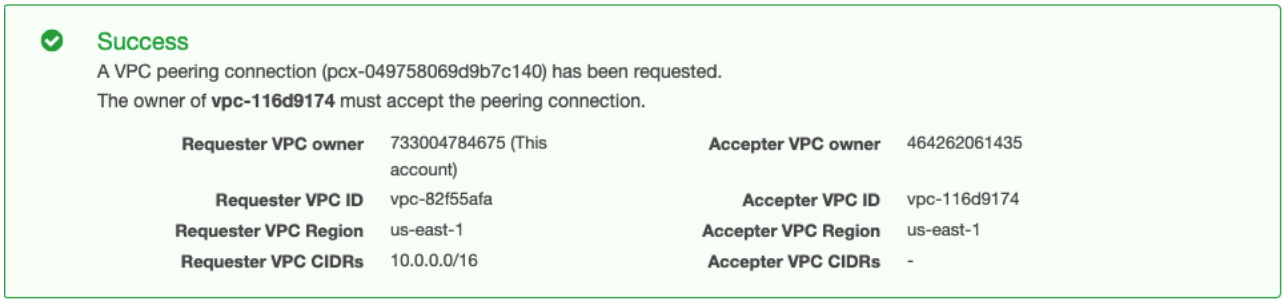
Just follow the steps below to set up your configuration in this manner.

Set up VPC peering between accounts

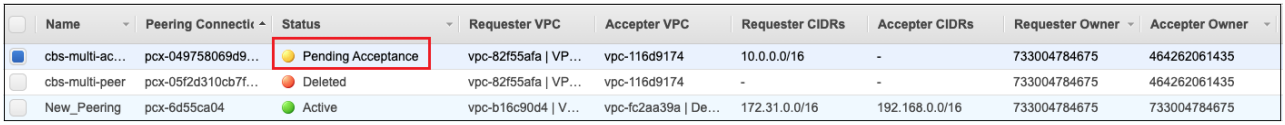
1. Log in to second account and Create Peering Connection:
    a. Select a local VPC: Select the VPC of the second account.
    b. Select another VPC: Enter the account ID of the first account.
    c. Select the Region where the Cloud Manager Connector is running. In this test setup both accounts are running in same region.
    d. VPC ID: Log into first account and enter the acceptor VPC ID. This is the VPC ID of the Cloud Manager Connector.



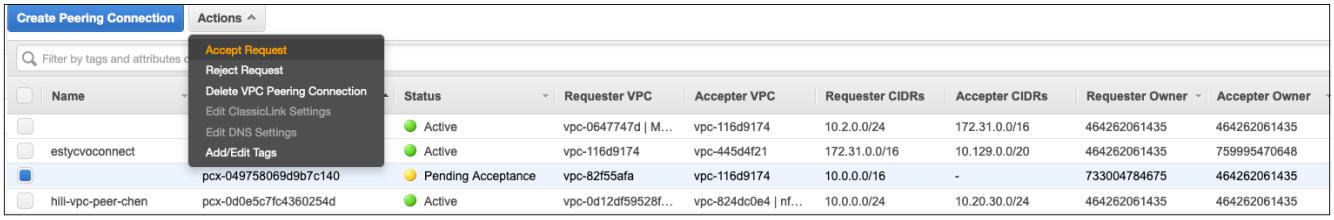
A Success dialog displays.



The status of the peering connection shows as Pending Acceptance.



2. Log into the first account and accept the peering request:



a. Click **Yes**.

The connection now shows as Active. We have also added a Name tag to identify the peering connection called `cbs-multi-account`.

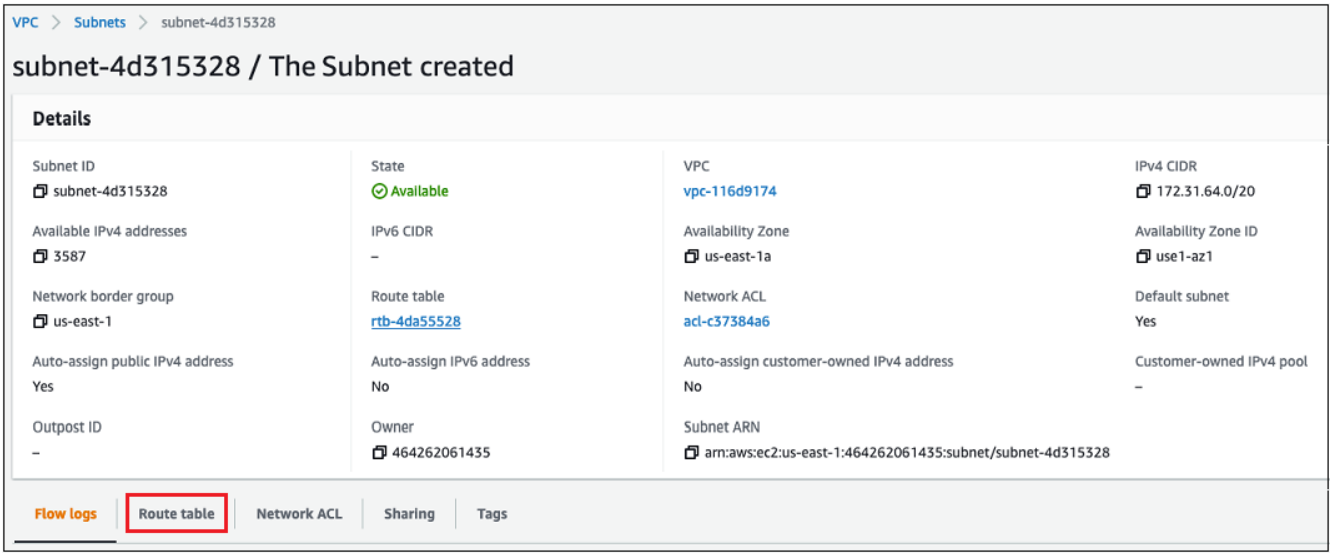
Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
	pcx-004715531514cb0d8	Active	vpc-0647747d | M…	vpc-116d9174	10.2.0.0/24	172.31.0.0/16	464262061435	464262061435
estycvoconnect	pcx-0305041f9cc2dfbdb	Active	vpc-116d9174	vpc-445d4f21	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
hill-vpc-peer-chen	pcx-0d0e5c7fc4360254d	Active	vpc-0d12df59528f…	vpc-824dc0e4 | nf…	10.0.0.0/24	10.20.30.0/24	464262061435	464262061435

b. Refresh the peering connection in the second account and notice that the status changes to Active.

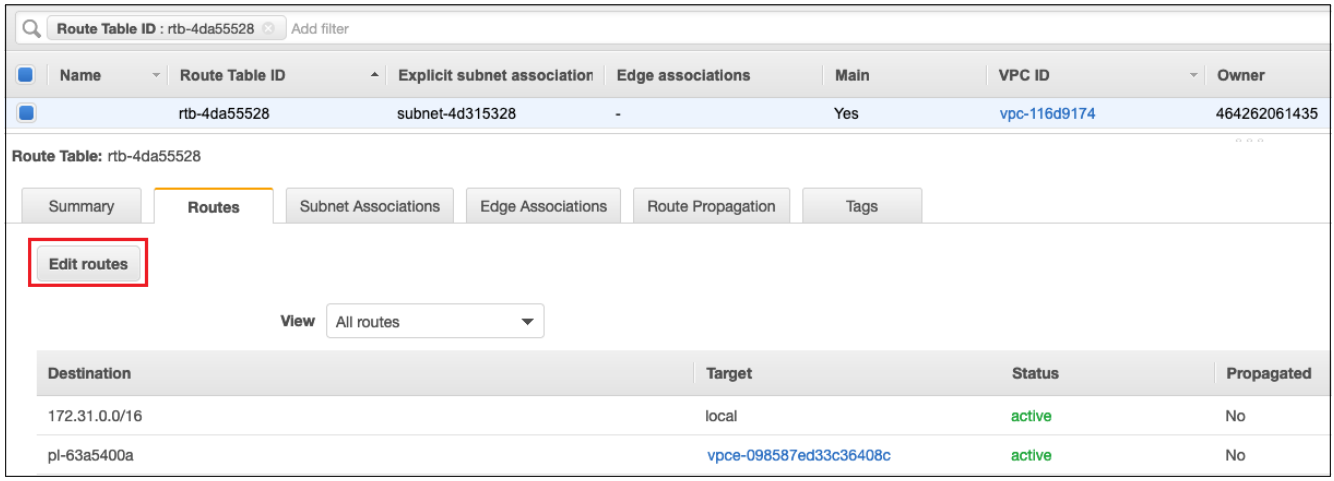
Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
cbs-multi-account	pcx-049758069d9b7c140	Active	vpc-82f55afa | VP…	vpc-116d9174	10.0.0.0/16	172.31.0.0/16	733004784675	464262061435
New_Peering	pcx-6d55ca04	Active	vpc-b16c90d4 | V…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

Add a route to the route tables in both accounts

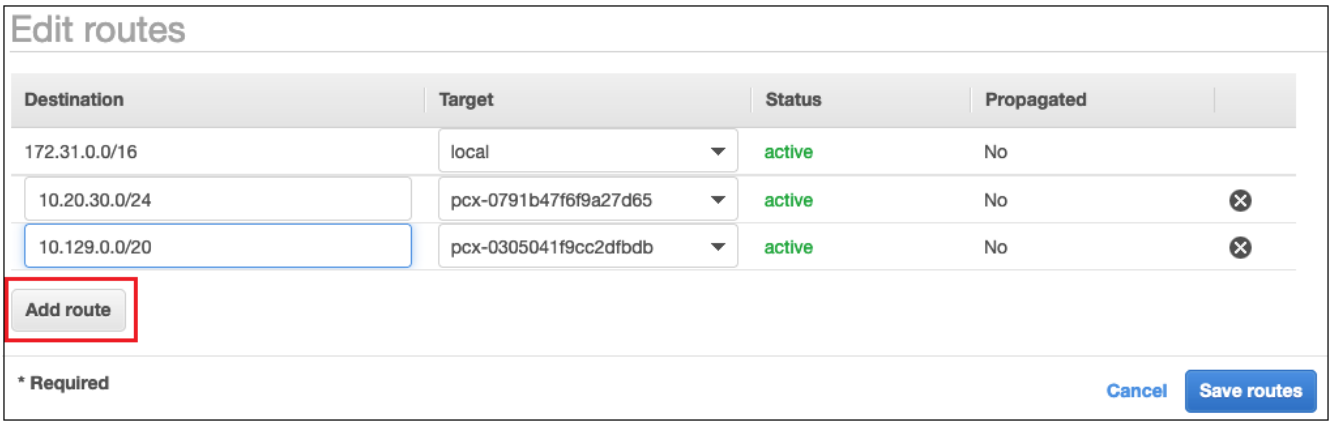
1. Go to VPC > Subnet > Route table.



2. Click on the Routes tab.

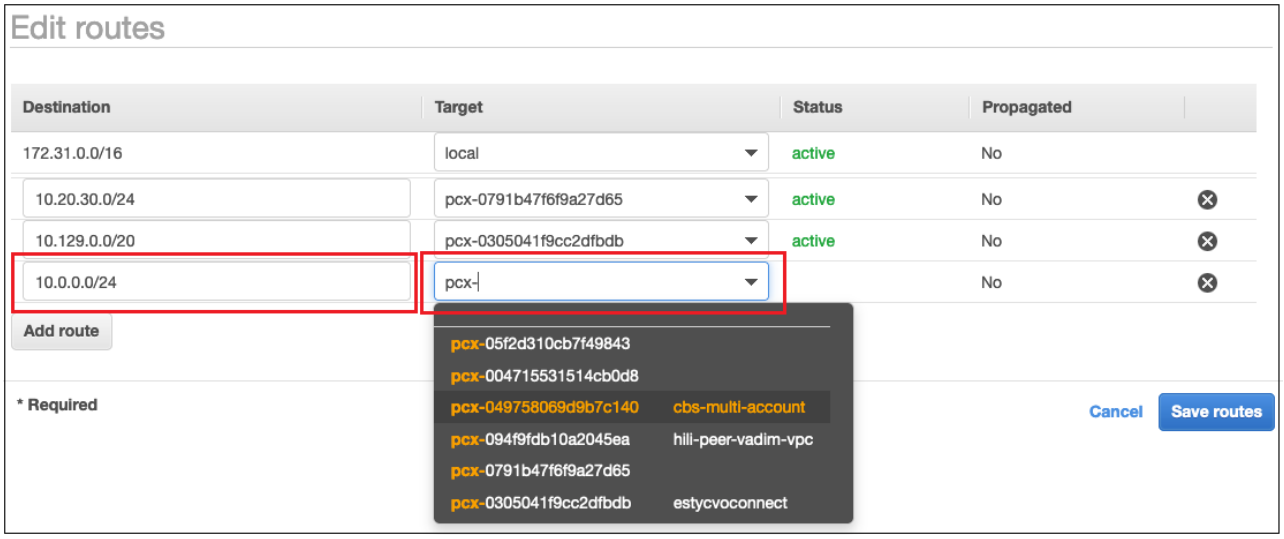


3. Click **Edit routes**.

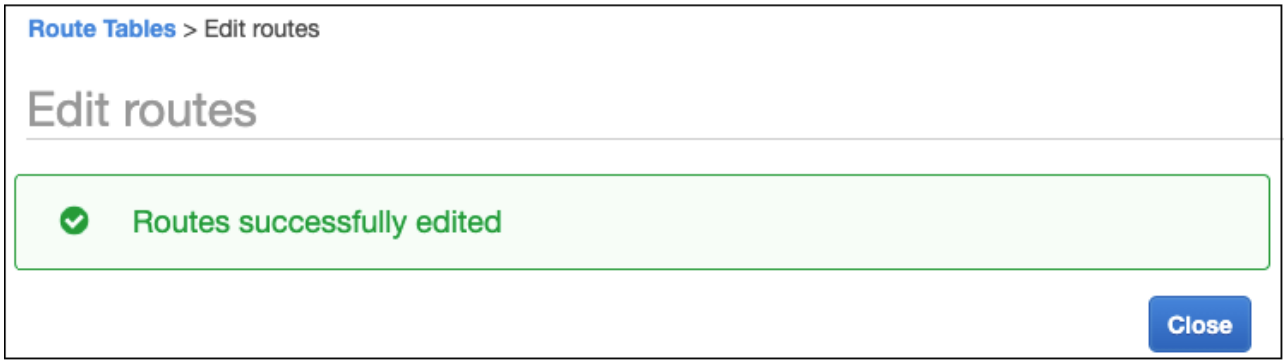


4. Click **Add route**, and from the Target drop-down list select **Peering Connection**, and then select the peering connection that you created.

   a. In the Destination, enter the other account's subnet CIDR.

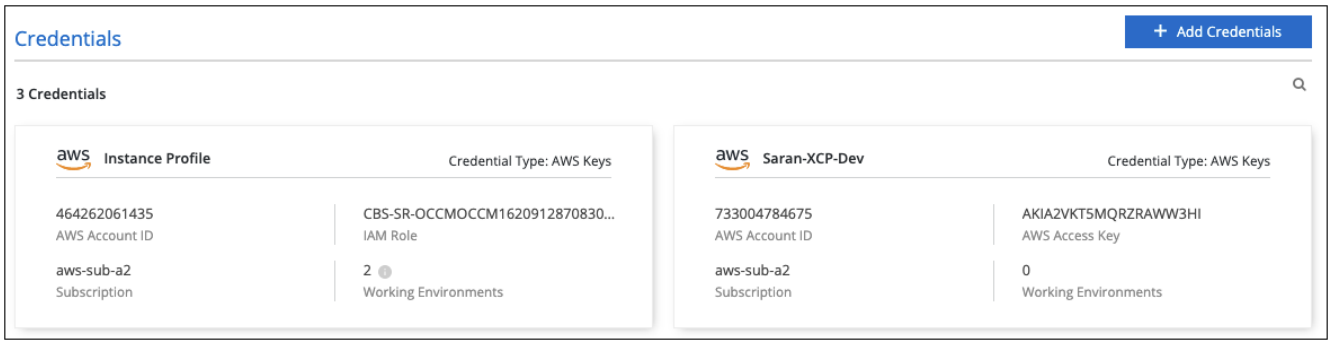


   b. Click **Save routes** and a Success dialog displays.

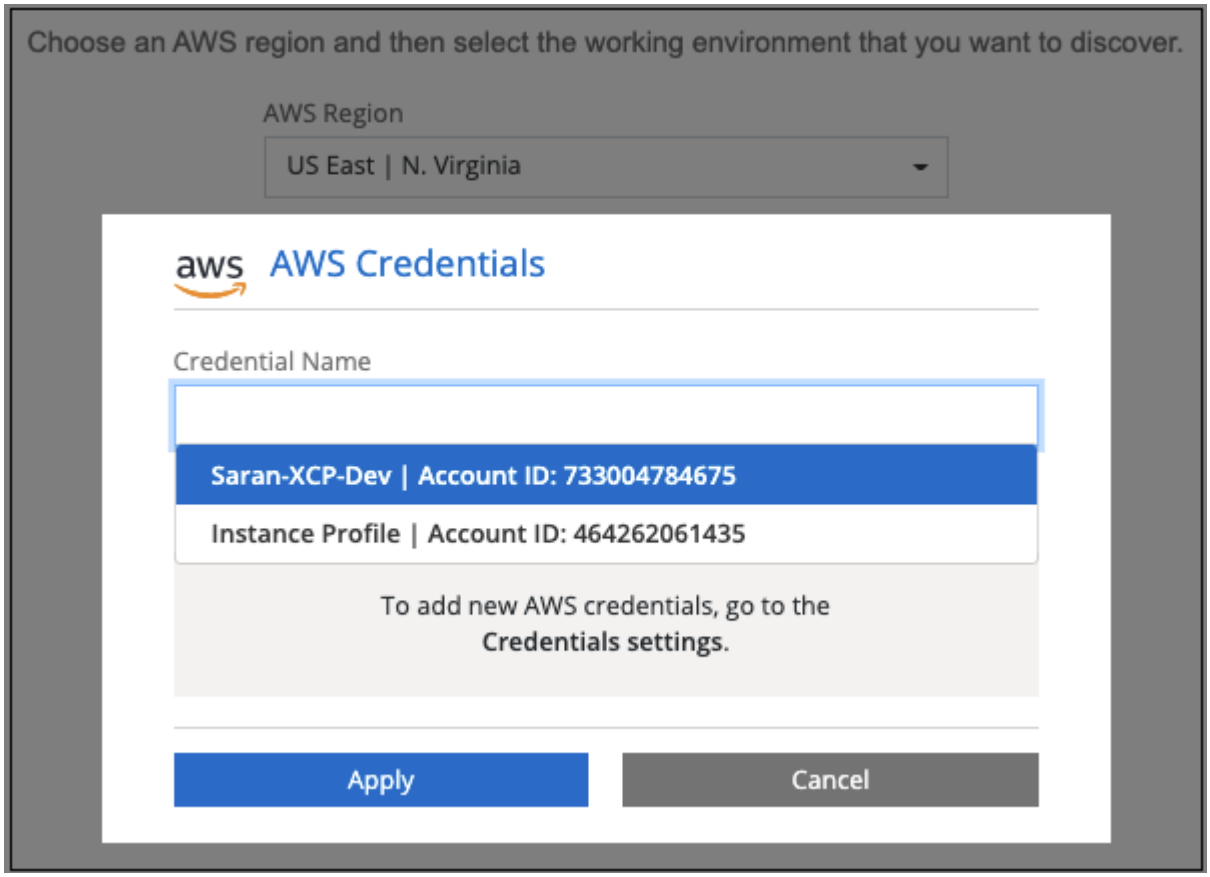


Add the second AWS account credentials in Cloud Manager

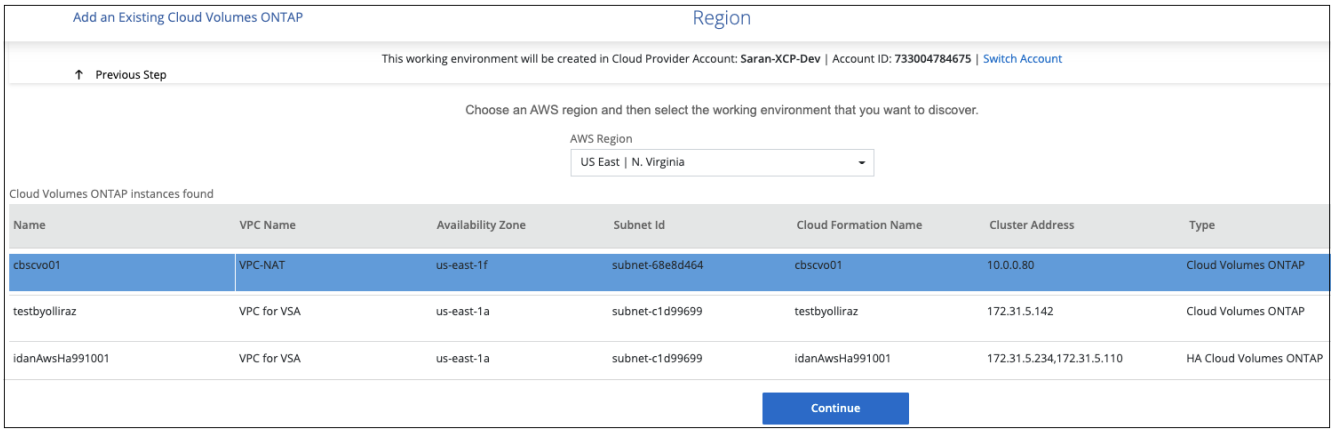
1. Add the second AWS account, for example, *Saran-XCP-Dev*.



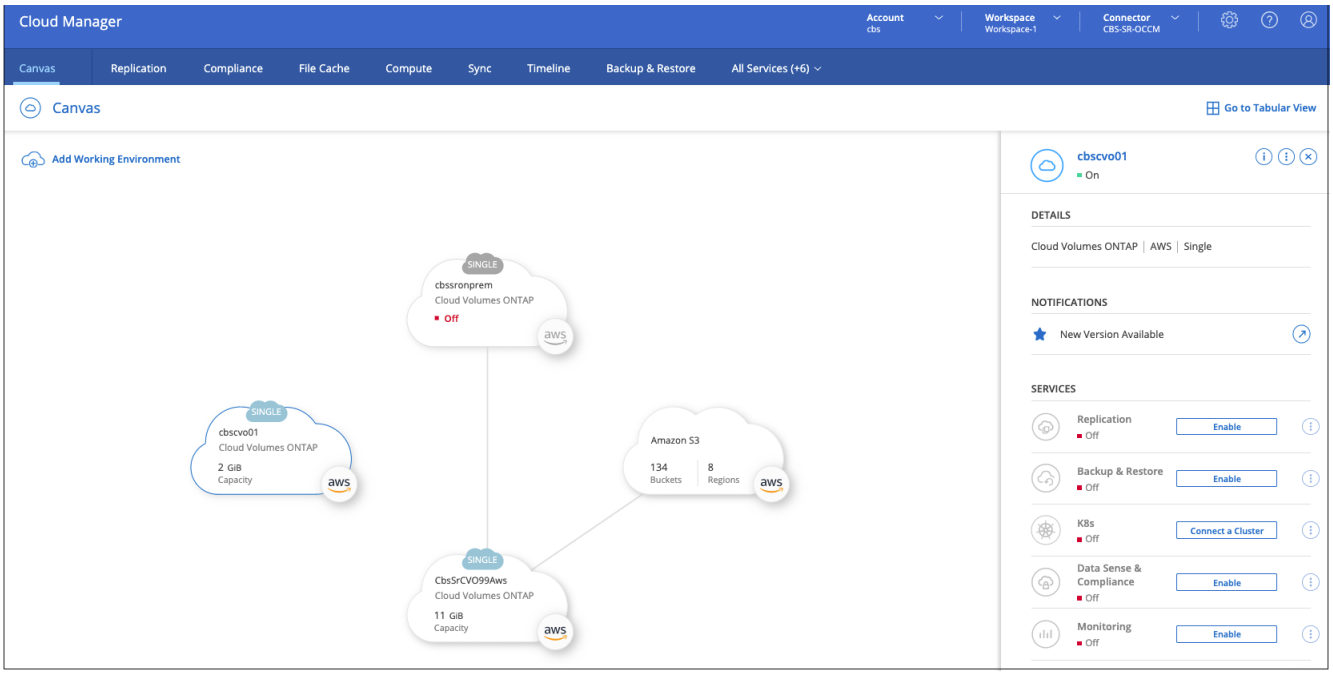
2. In the Discover Cloud Volumes ONTAP page, select the newly added credentials.



3. Select the Cloud Volumes ONTAP system you want to discover from second account. You can also deploy a new Cloud Volumes ONTAP system in the second account.

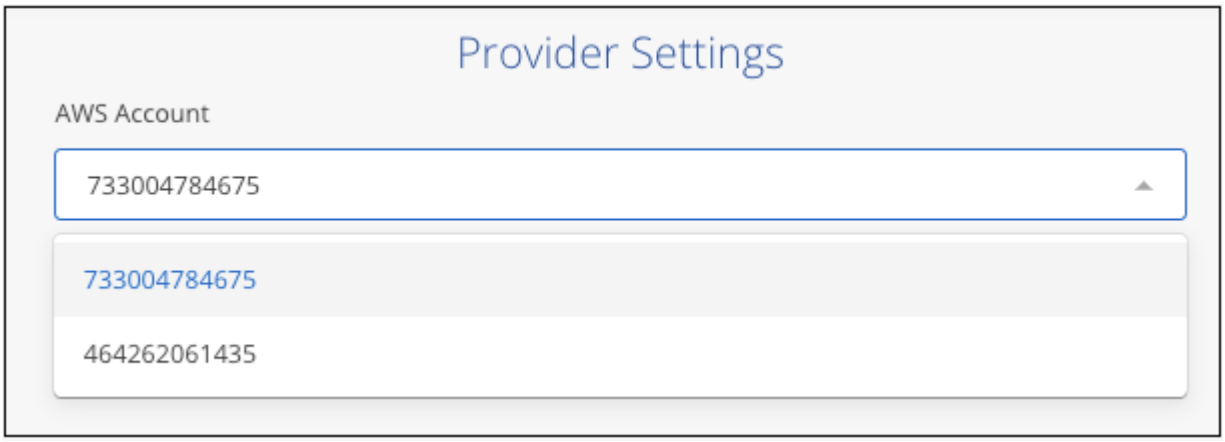


The Cloud Volumes ONTAP system from the second account is now added to Cloud Manager which is running in a different account.



Enable backup in the other AWS account

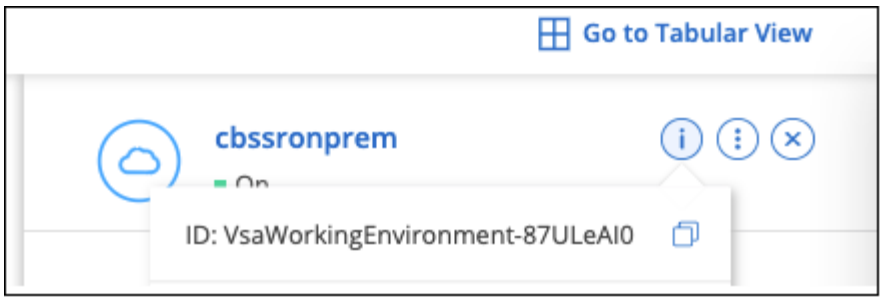
1. In Cloud Manager, enable backup for the Cloud Volumes ONTAP system running in the first account, but select the second account as the location for creating the backup files.



2. Then select a backup policy and the volumes you want to back up, and Cloud Backup attempts to create a new bucket in the selected account.

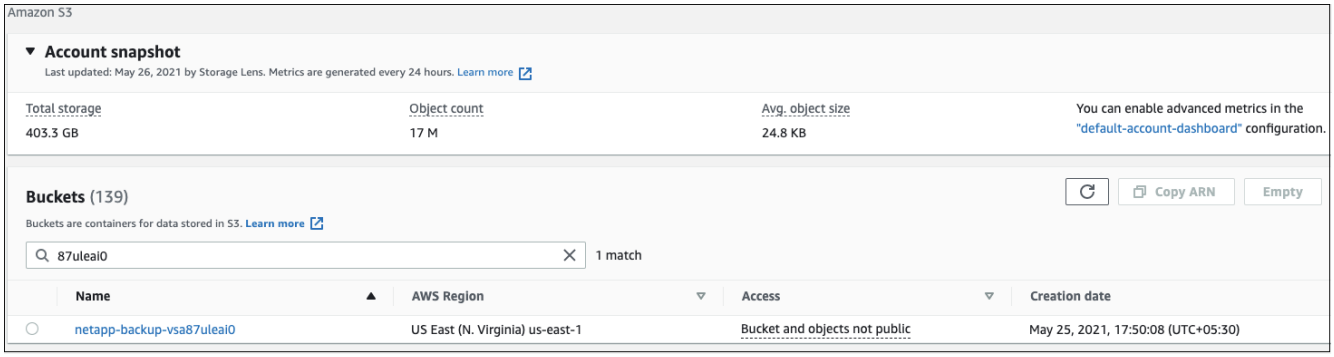
   However, adding the bucket to the Cloud Volumes ONTAP system will fail because Cloud Backup uses the instance profile to add the bucket and the Cloud Manager instance profile doesn't have access to the resources in the second account.

3. Get the working environment ID for the Cloud Volumes ONTAP system.

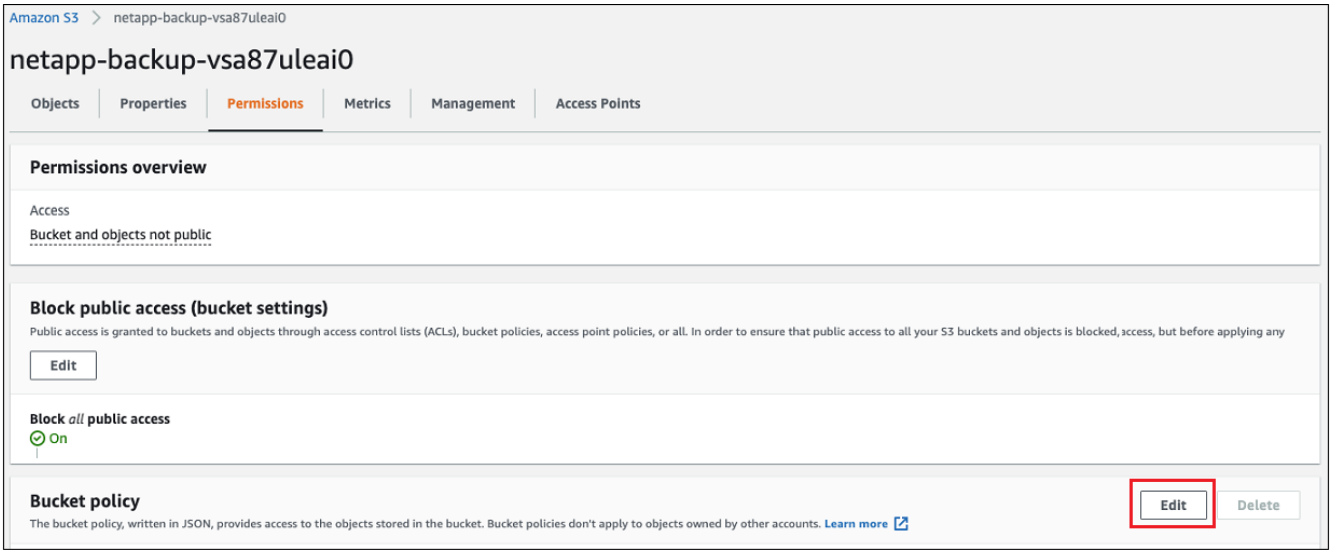


Cloud Backup creates every bucket with the prefix `Netapp-backup-` and will include the working environment ID; for example: `87ULeA10`

4. In the EC2 portal, go to S3 and search for the bucket with name ending with `87uLeA10` and you'll see the bucket name displayed as `Netapp-backup-vsa87uLeA10`.



5. Click on the bucket, then click the Permissions tab, and then click **Edit** in the Bucket policy section.



6. Add a bucket policy for the newly created bucket to provide access to the Cloud Manager's AWS account, and then Save the changes.

```
{
  "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/*"
      ]
    }
  ]
}
```

Note that "AWS": "arn:aws:iam::464262061435:root" gives complete access this bucket for all resources in account 464262061435. If you want to reduce it to specific role, level, you can update the policy with specific role(s). If you are adding individual roles, ensure that occm role also added, otherwise backups will not get updated in the Cloud Backup UI.

For example: "AWS": "arn:aws:iam::464262061435:role/cvo-instance-profile-version10-d8e-IamInstanceRole-IKJPJ1HC2E7R"

7. Retry enabling Cloud Backup on the Cloud Volumes ONTAP system and this time it should be successful.