跨帐户和跨区域配置
Cloud Backup

NetApp
July 13, 2022

目录

跨帐户和跨区域配置

这些主题介绍如何在使用不同的云提供商时为跨帐户配置配置 Cloud Backup 。

- "在 AWS 中配置 Cloud Backup 以实现多帐户访问"
- "在 Azure 中配置 Cloud Backup 以实现多帐户访问"

在 AWS 中为多帐户访问配置备份

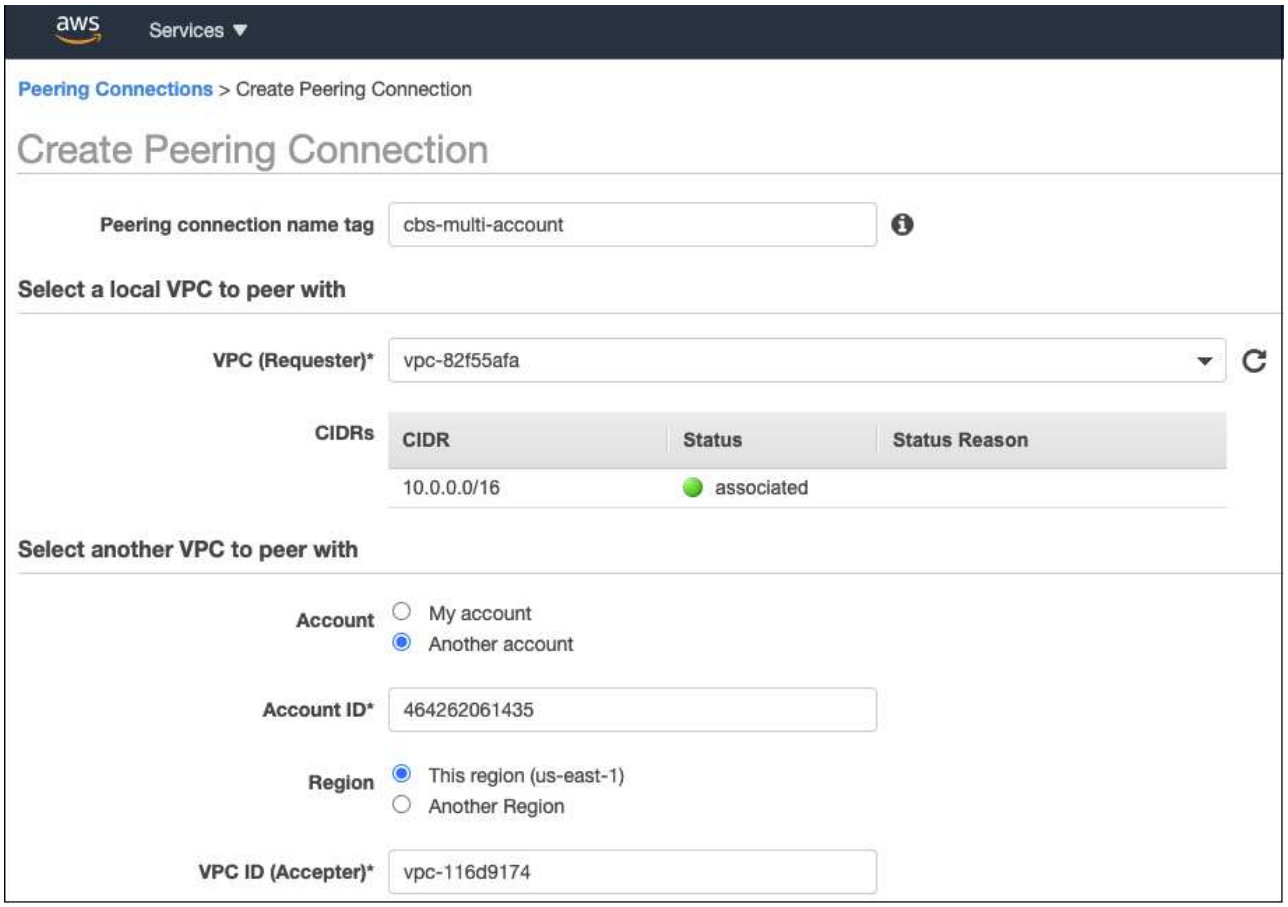
通过 Cloud Backup ，您可以在与源 Cloud Volumes ONTAP 卷所在位置不同的 AWS 帐户中创建备份文件。这两个帐户都可以与 Cloud Manager Connector 所在的帐户不同。

只有在您使用时，才需要执行这些步骤 "将 Cloud Volumes ONTAP 数据备份到 Amazon S3"。

按照以下步骤以这种方式设置您的配置。

在帐户之间设置 VPC 对等关系

1. 登录到第二个帐户并创建对等连接：
    a. 选择本地 VPC ： 选择第二个帐户的 VPC 。
    b. 选择其他 VPC ： 输入第一个帐户的帐户 ID 。
    c. 选择运行 Cloud Manager Connector 的区域。在此测试设置中，两个帐户都在同一区域运行。
    d. VPC ID ： 登录到第一个帐户并输入接收者 VPC ID 。这是 Cloud Manager Connector 的 VPC ID 。



此时将显示成功对话框。

对等连接的状态显示为待接受。

2. 登录到第一个帐户并接受对等请求：

a. 单击 * 是 * 。

此时，此连接将显示为 "Active" 。我们还添加了一个名称标记来标识名为 `CBS-Multi-account` 的对等连接。

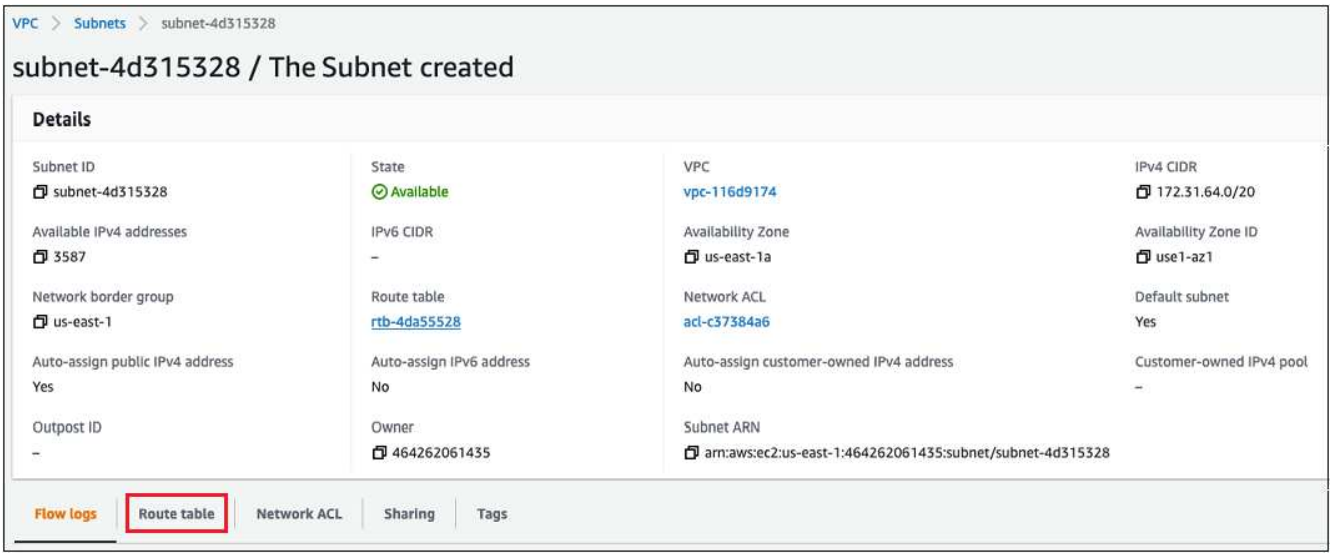
Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
	pcx-004715531514cb0d8	Active	vpc-0647747d | M…	vpc-116d9174	10.2.0.0/24	172.31.0.0/16	464262061435	464262061435
estycvoconnect	pcx-0305041f9cc2dfbdb	Active	vpc-116d9174	vpc-445d4f21	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

a. 刷新第二个帐户中的对等连接，并注意状态将更改为 "Active" 。

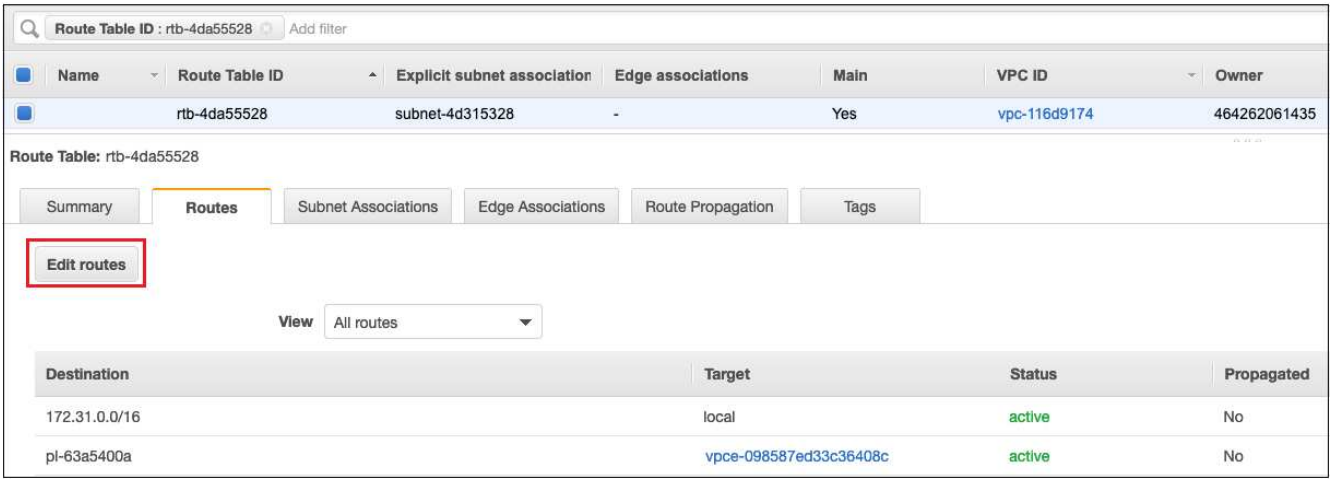
Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
cbs-multi-account	pcx-049758069d9b7c140	Active	vpc-82f55afa | VP…	vpc-116d9174	10.0.0.0/16	172.31.0.0/16	733004784675	464262061435
New_Peering	pcx-6d55ca04	Active	vpc-b16c90d4 | V…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

向两个帐户中的路由表添加路由

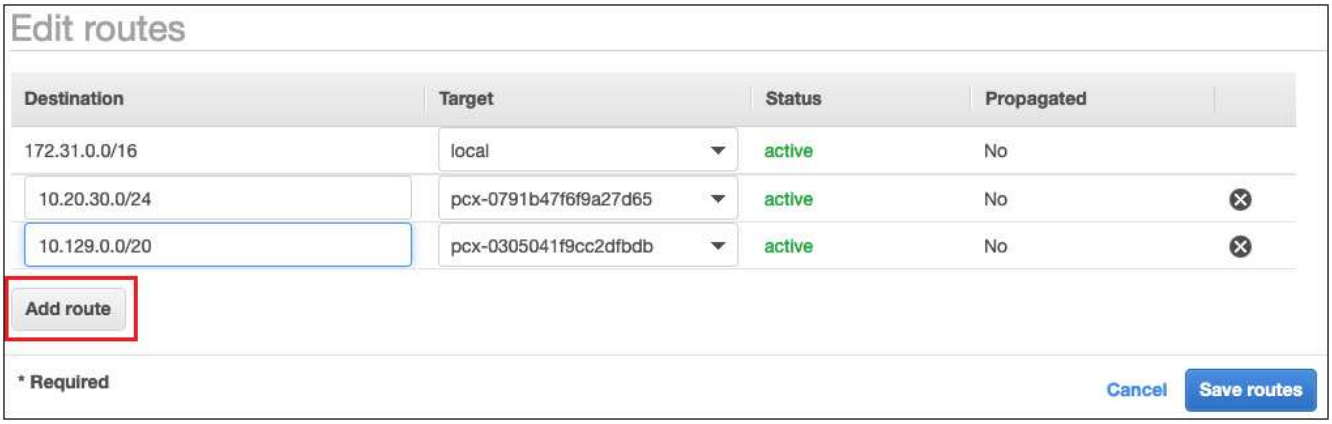
1. 转至 VPC > 子网 > 路由表。



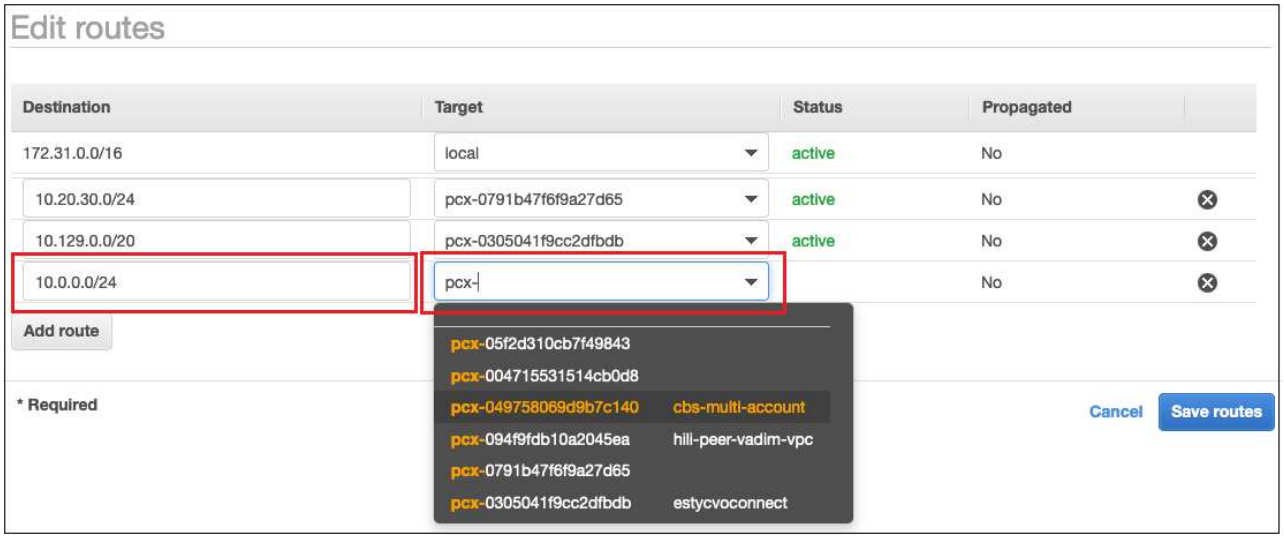
2. 单击路由选项卡。



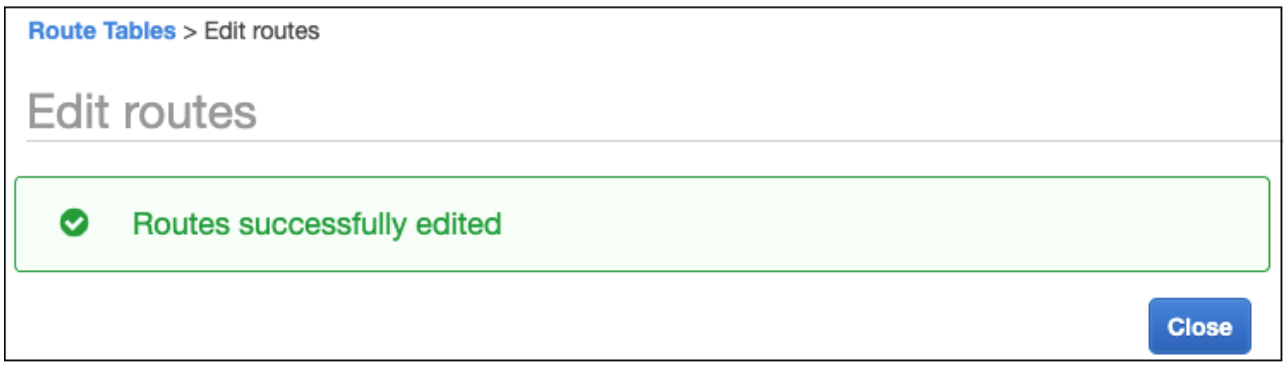
3. 单击 * 编辑路由 * 。



4. 单击 * 添加路由 * ，然后从目标下拉列表中选择 * 对等连接 * ，然后选择您创建的对等连接。
   a. 在目标中，输入另一帐户的子网 CIDR 。

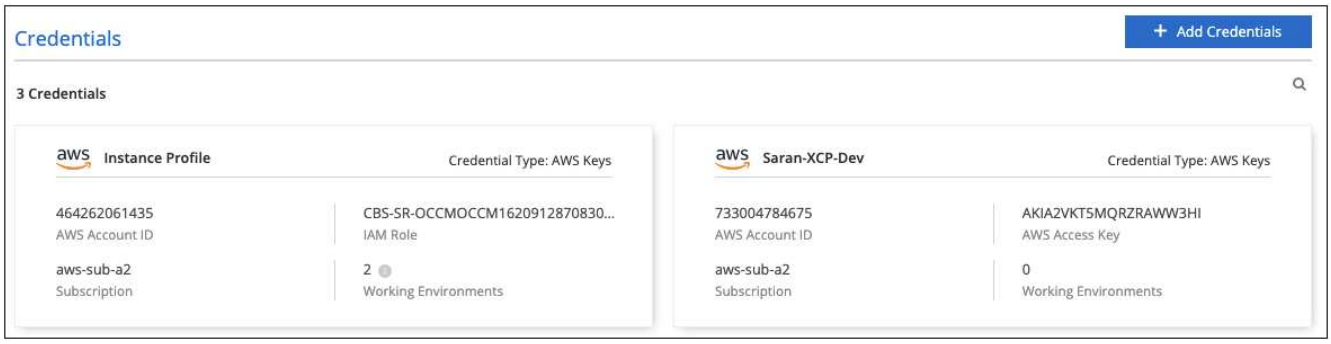


b. 单击 * 保存路由 * ，此时将显示一个成功对话框。

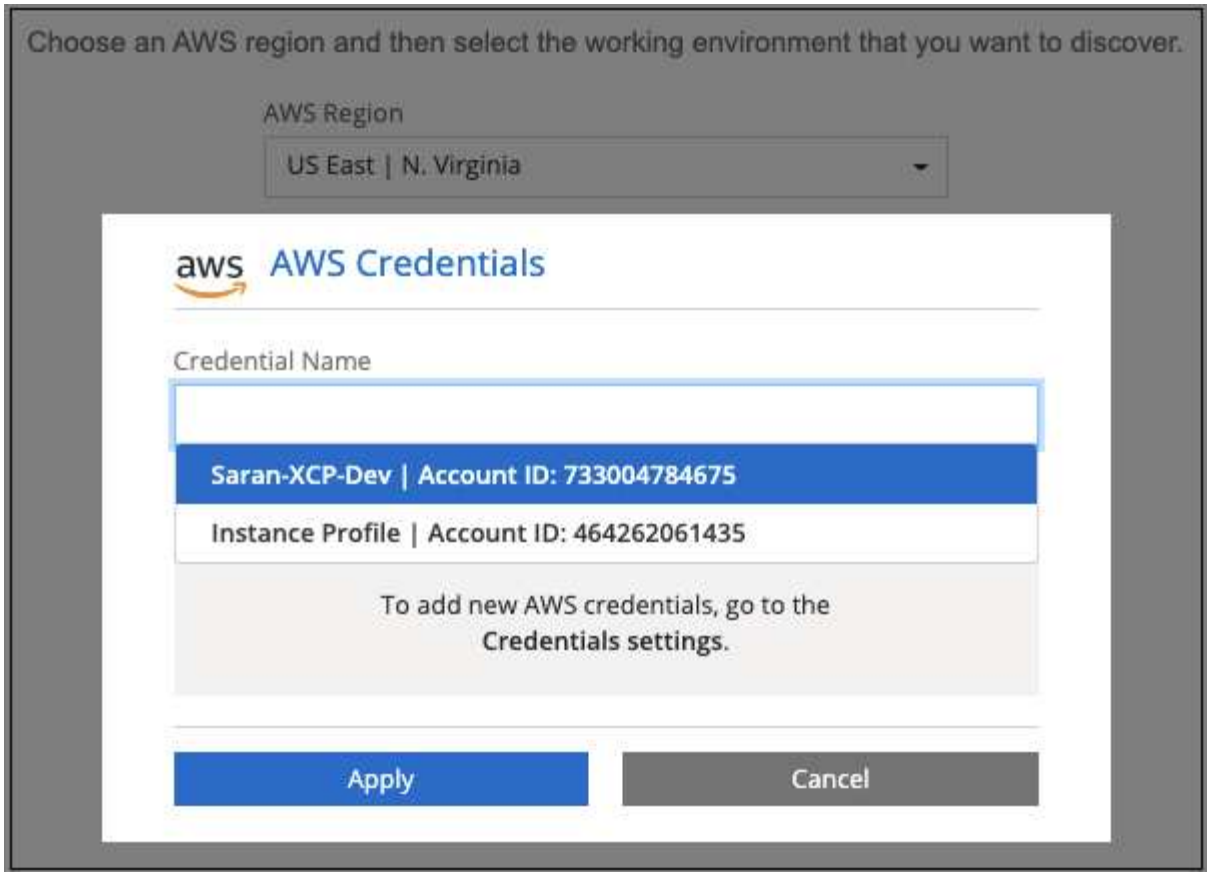


在 **Cloud Manager** 中添加第二个 **AWS** 帐户凭据

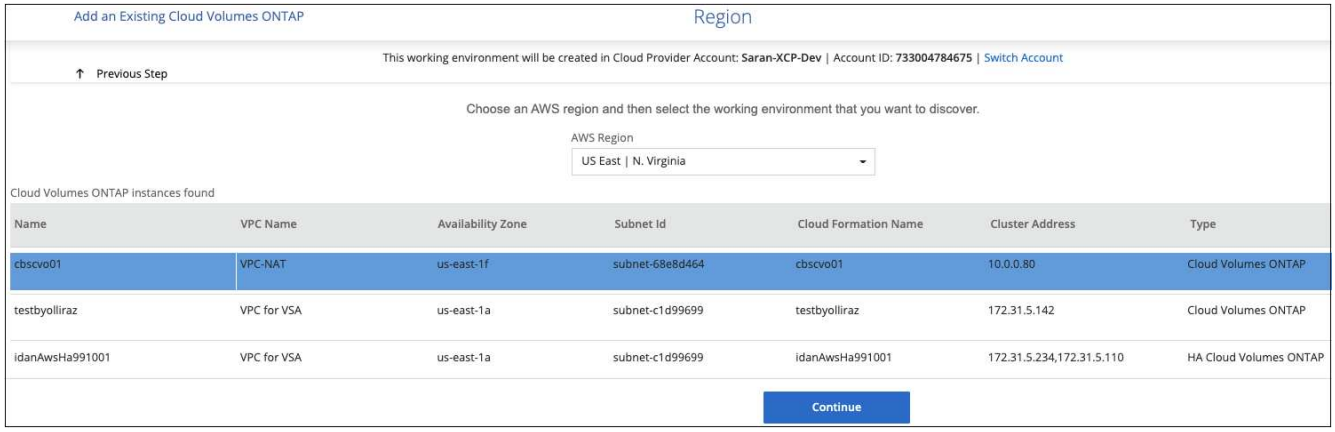
1. 添加第二个 AWS 帐户，例如 *Saran-XCP-Dev* 。



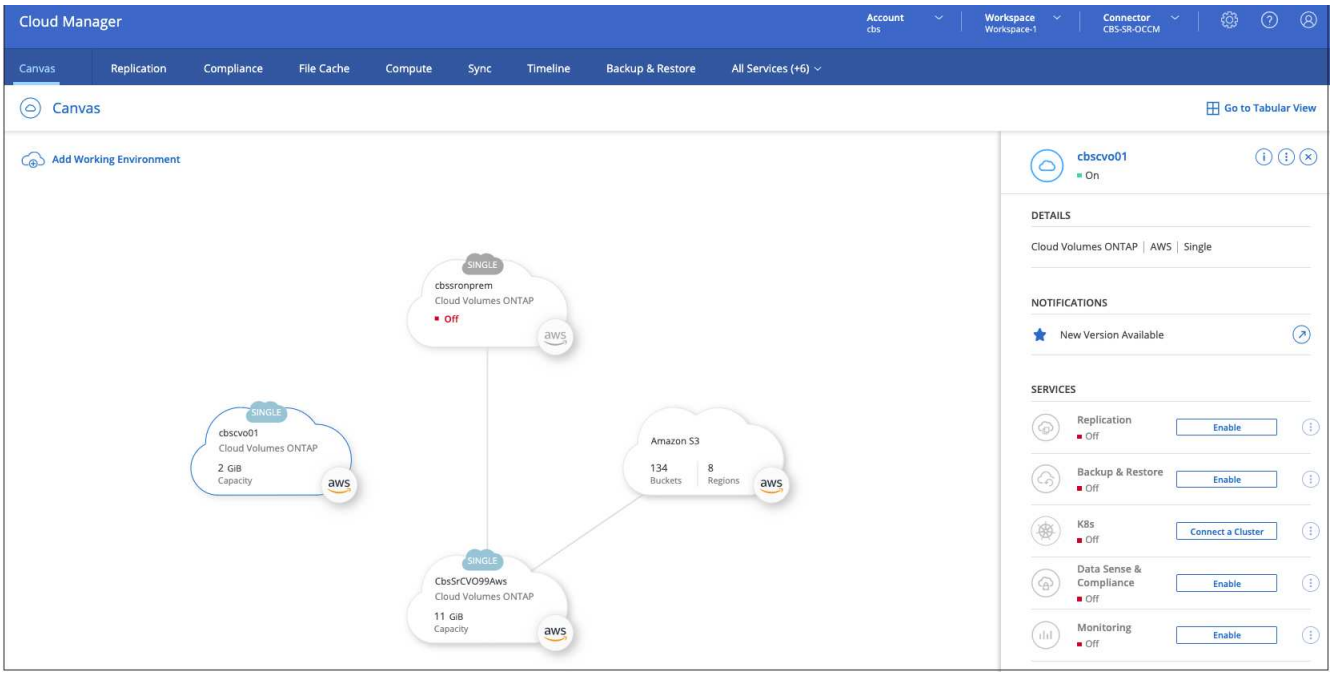
2. 在发现 Cloud Volumes ONTAP 页面中，选择新添加的凭据。



3. 选择要从第二个帐户发现的 Cloud Volumes ONTAP 系统。您也可以在第二个帐户中部署新的 Cloud Volumes ONTAP 系统。

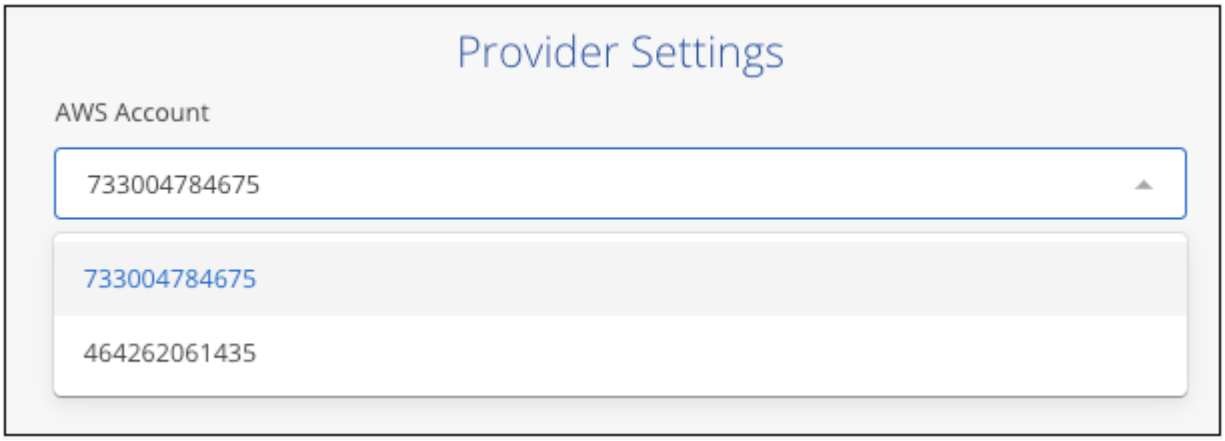


现在，第二个帐户中的 Cloud Volumes ONTAP 系统将添加到在其他帐户中运行的 Cloud Manager 中。



在其他 **AWS** 帐户中启用备份

1. 在 Cloud Manager 中，为第一个帐户中运行的 Cloud Volumes ONTAP 系统启用备份，但选择第二个帐户作为创建备份文件的位置。



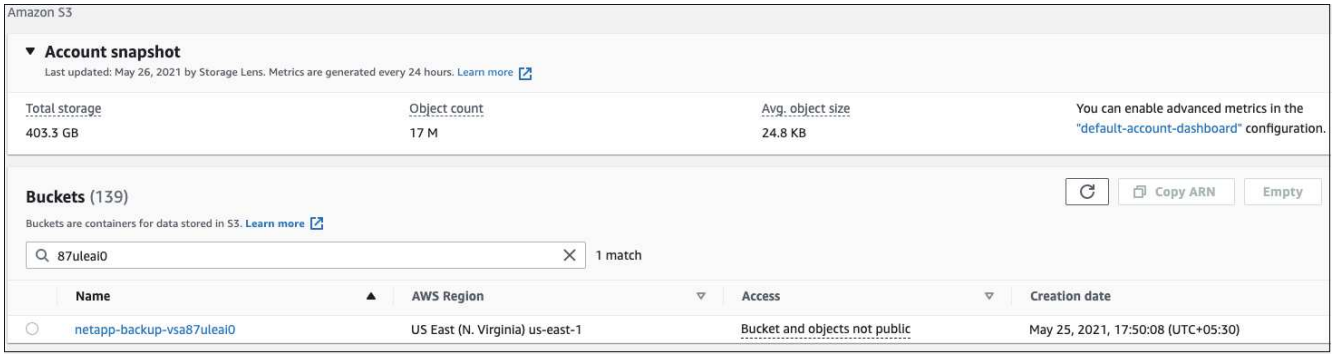
2. 然后，选择一个备份策略以及要备份的卷， Cloud Backup 将尝试在选定帐户中创建一个新存储分段。

   但是，将存储分段添加到 Cloud Volumes ONTAP 系统将失败，因为 Cloud Backup 使用实例配置文件添加存储分段，而 Cloud Manager 实例配置文件无法访问第二个帐户中的资源。

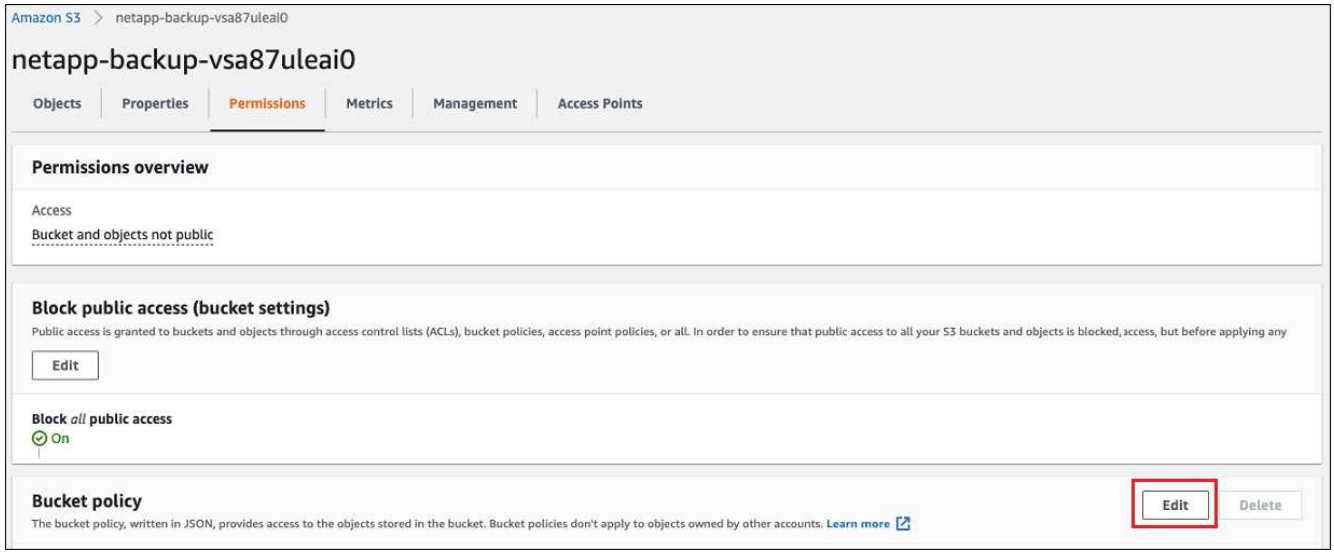
3. 获取 Cloud Volumes ONTAP 系统的工作环境 ID 。

Cloud Backup 会创建前缀为 `netapp-backup-` 的每个存储分段，并包含工作环境 ID ；例如： `87ULeA10`

4. 在 EC2 门户中，转到 S3 并搜索名称以 `87uLeA10` 结尾的分段，此时您将看到分段名称显示为 `NetApp-backup-vsa87uLeA10` 。



5. 单击存储分段，然后单击权限选项卡，然后单击存储分段策略部分中的 * 编辑 * 。



6. 为新创建的存储分段添加存储分段策略，以访问 Cloud Manager 的 AWS 帐户，然后保存更改。

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

请注意， "AWs"： "ARN： AWS： iam：： 464262061435： root" 为帐户 464262061435 中的所有资源提供了此存储分段的完全访问权限。如果要将策略缩减为特定角色，级别，则可以使用特定角色更新策略。如果要添加单个角色，请确保同时添加了 occa 角色，否则备份将不会在 Cloud Backup UI 中更新。

例如： "AWs"： "ARN： AWS： iam：： 464262061435： role/cvo-instance-profile-version10-d8e-IamInstanceRole-ikjpJ1HC2E7R"

7. 请重试在 Cloud Volumes ONTAP 系统上启用云备份，此时应成功启用。

在 Azure 中配置用于多帐户访问的备份

通过 Cloud Backup ，您可以在与源 Cloud Volumes ONTAP 卷所在位置不同的 Azure 帐户中创建备份文件。这两个帐户都可以与 Cloud Manager Connector 所在的帐户不同。

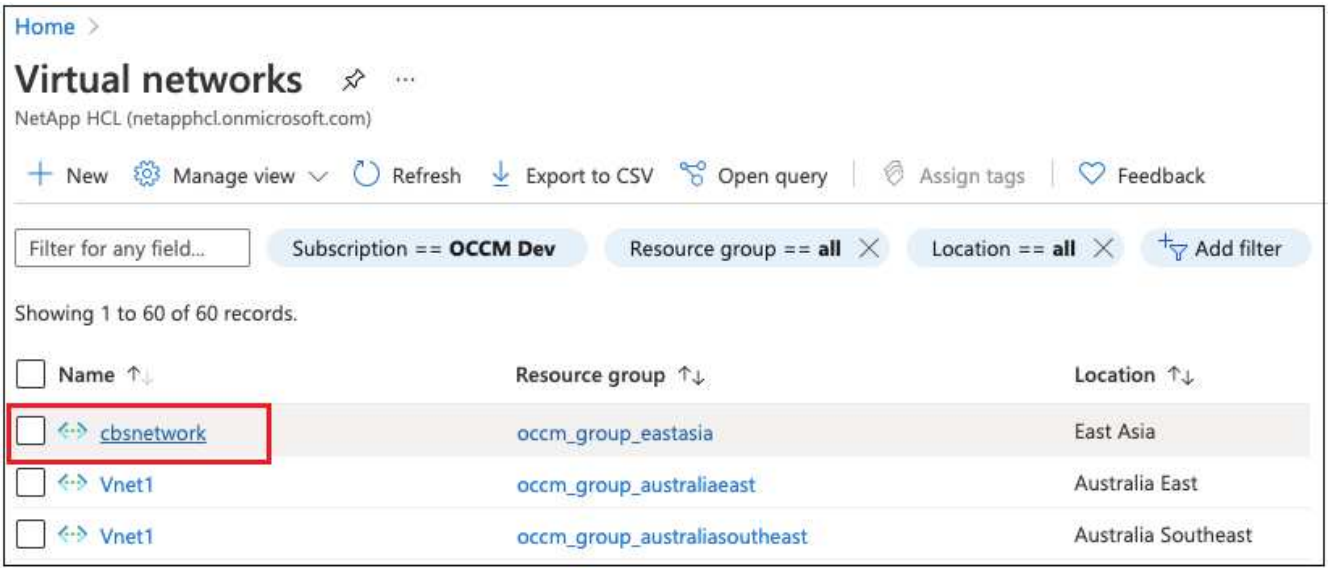
只有在您使用时，才需要执行这些步骤 "将 Cloud Volumes ONTAP 数据备份到 Azure Blob 存储"。

只需按照以下步骤以这种方式设置您的配置即可。

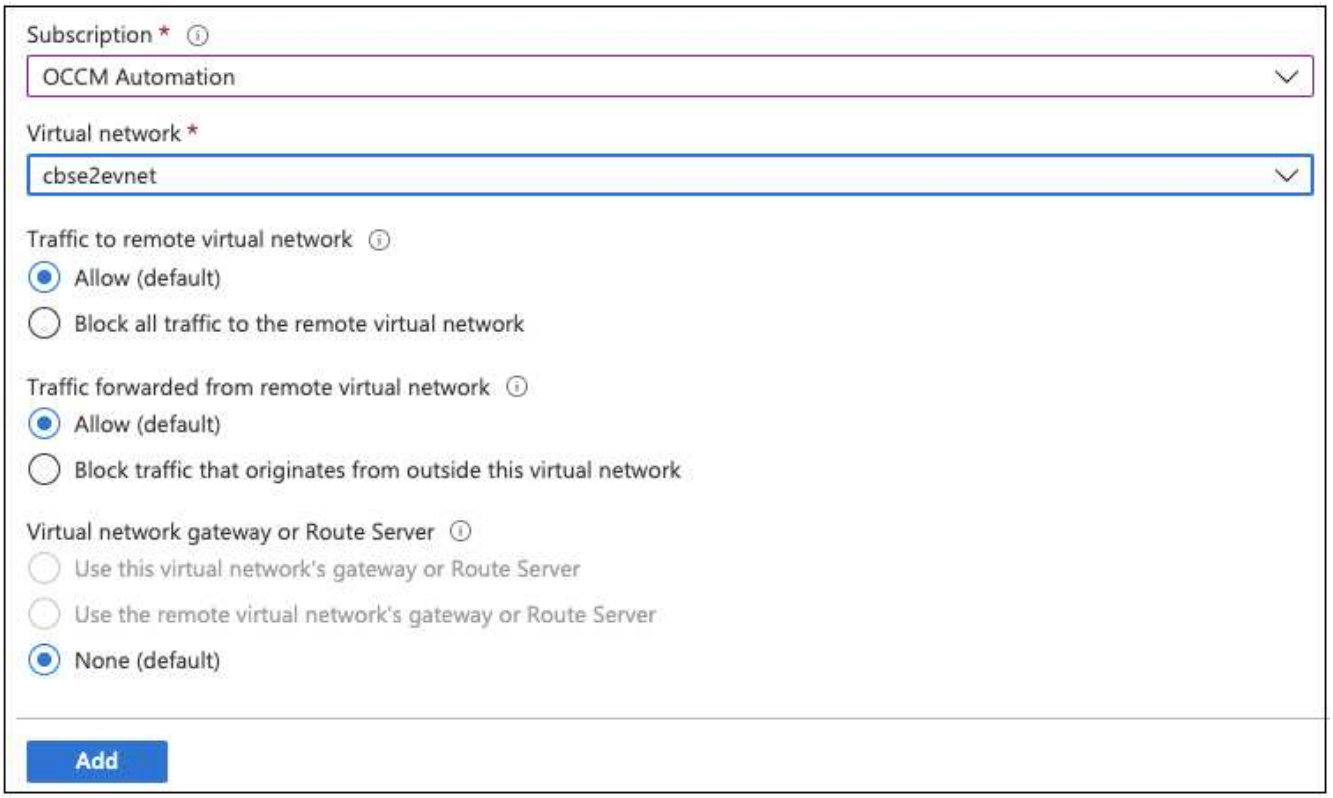
在帐户之间设置 vNet 对等关系

请注意，如果您希望 Cloud Manager 在其他帐户 / 区域管理您的 Cloud Volumes ONTAP 系统，则需要设置 vNet 对等关系。存储帐户连接不需要建立 vNet 对等关系。

1. 登录到 Azure 门户，然后从主页选择 Virtual Networks 。
2. 选择要用作订阅 1 的订阅，然后单击要设置对等关系的 vNet 。

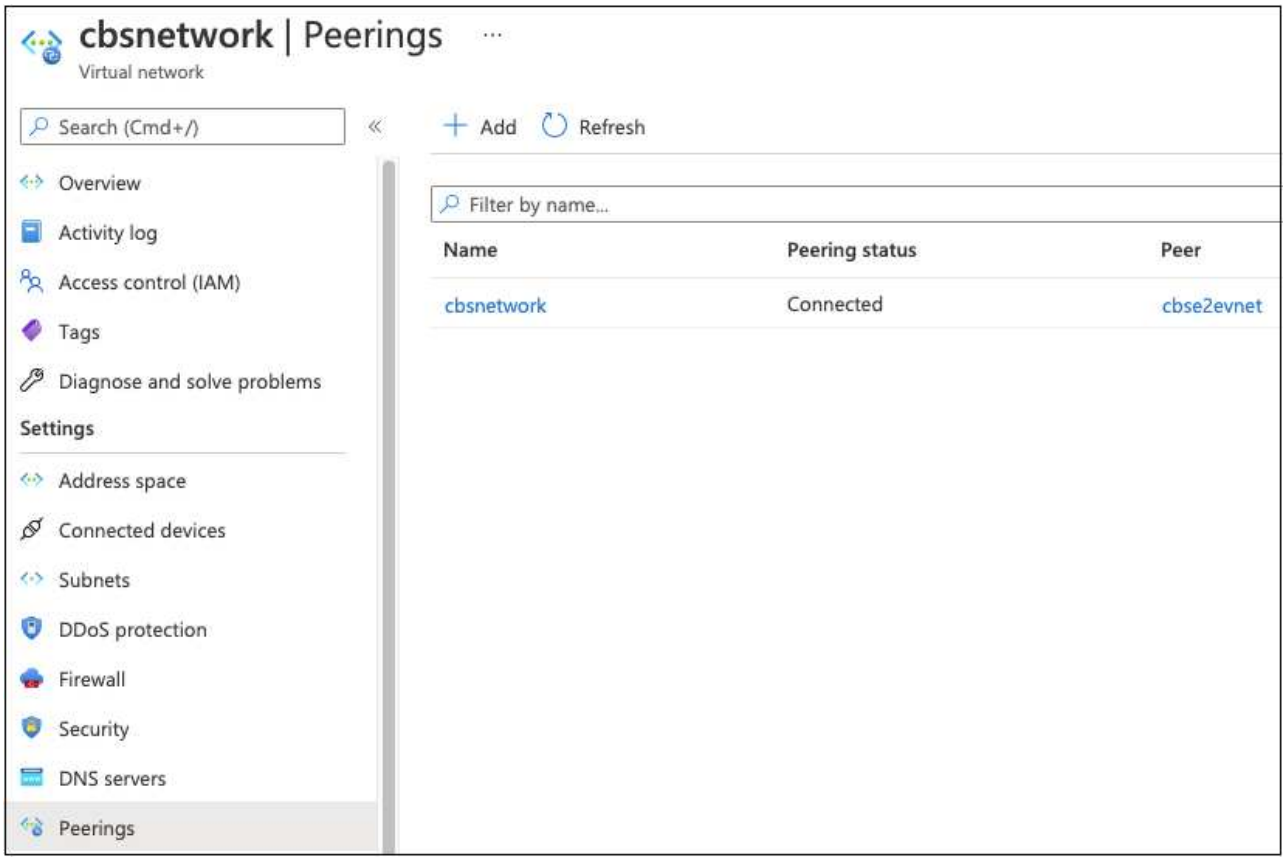


3. 选择 * cbsnetwork* ，然后从左侧面板中单击 * 产品 * ，然后单击 * 添加 * 。

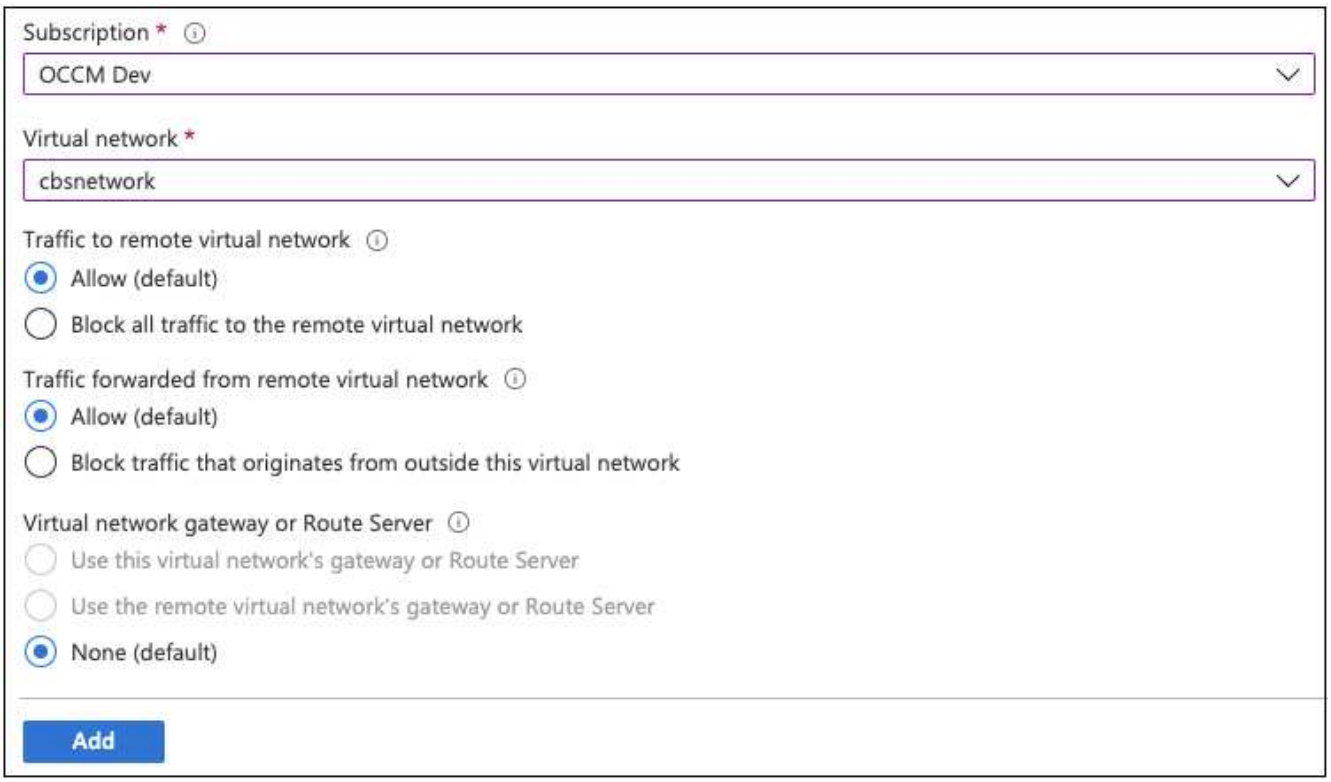


4. 在对等页面上输入以下信息，然后单击 * 添加 * 。
   - 此网络的对等链路名称：您可以提供任何名称来标识对等连接。
   - 远程虚拟网络对等链路名称：输入一个名称以标识远程 vNet 。
   - 将所有选择保留为默认值。

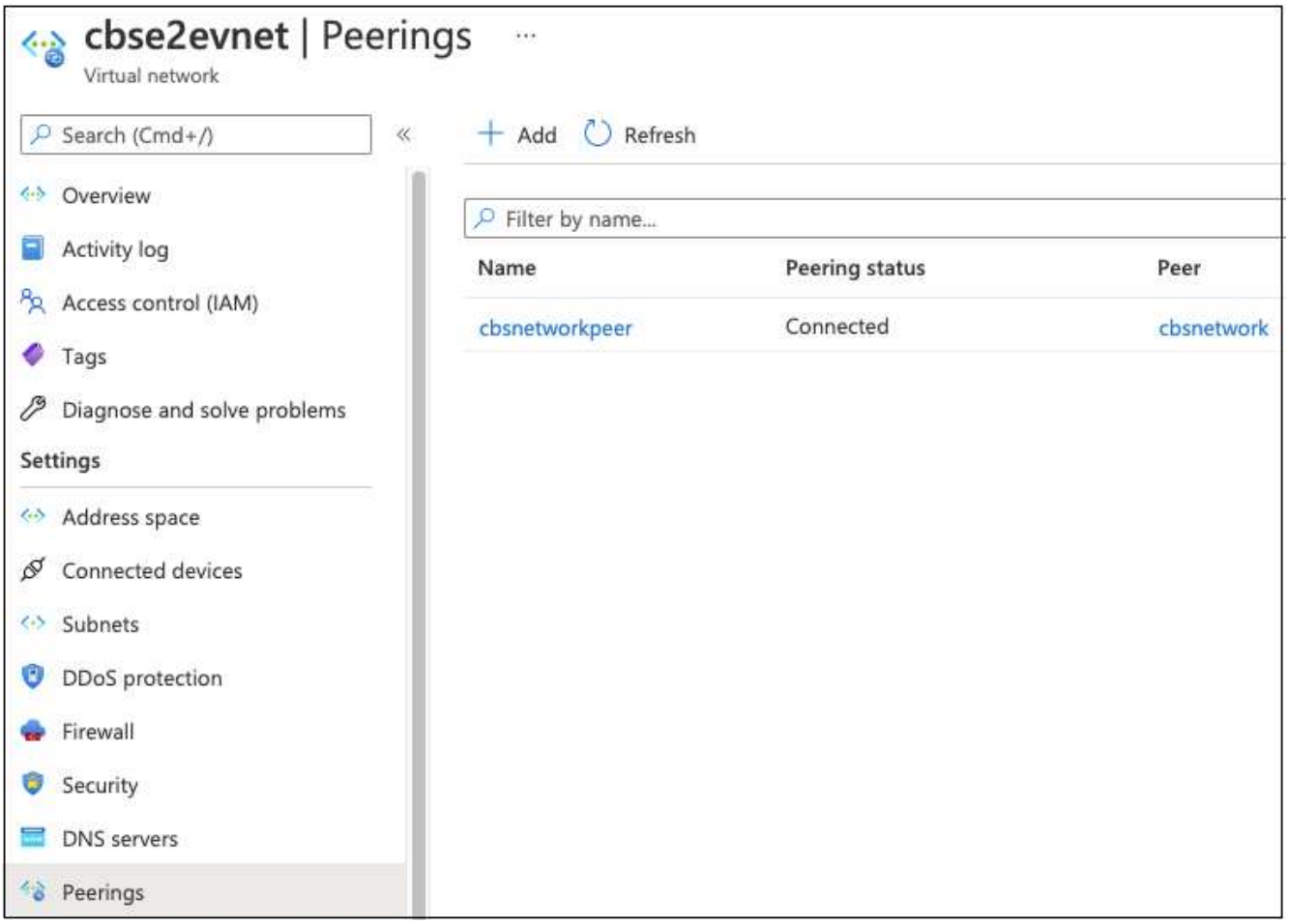
- 在订阅下，选择订阅 2.
- 虚拟网络，请在订阅 2 中选择要设置对等关系的虚拟网络。



5. 在 subscription 2 vNet 中执行相同的步骤，并指定 subscription 1 的订阅和远程 vNet 详细信息。



此时将添加对等设置。



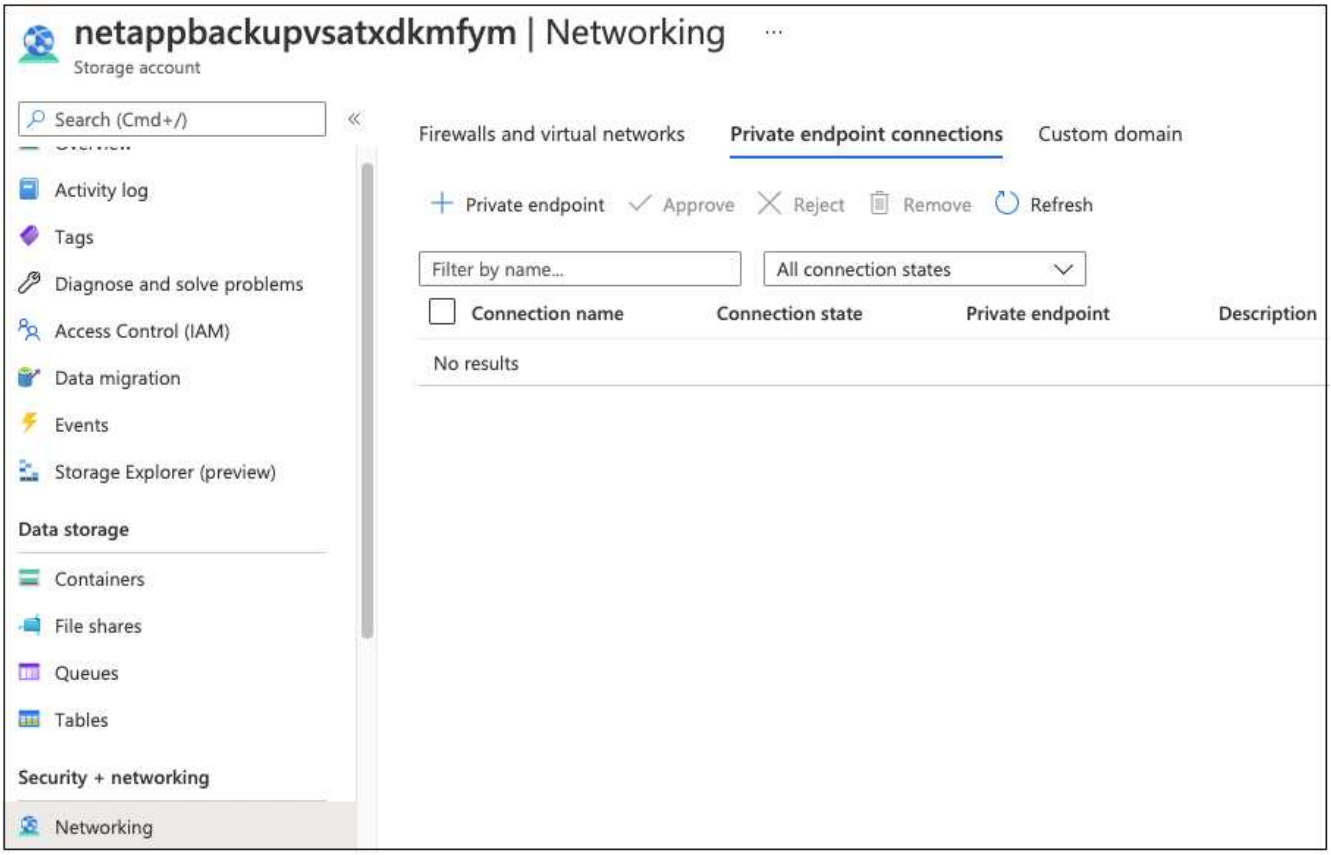
为存储帐户创建私有端点

现在，您需要为此存储帐户创建一个专用端点。在此示例中，存储帐户在订阅 1 中创建， Cloud Volumes ONTAP 系统在订阅 2 中运行。

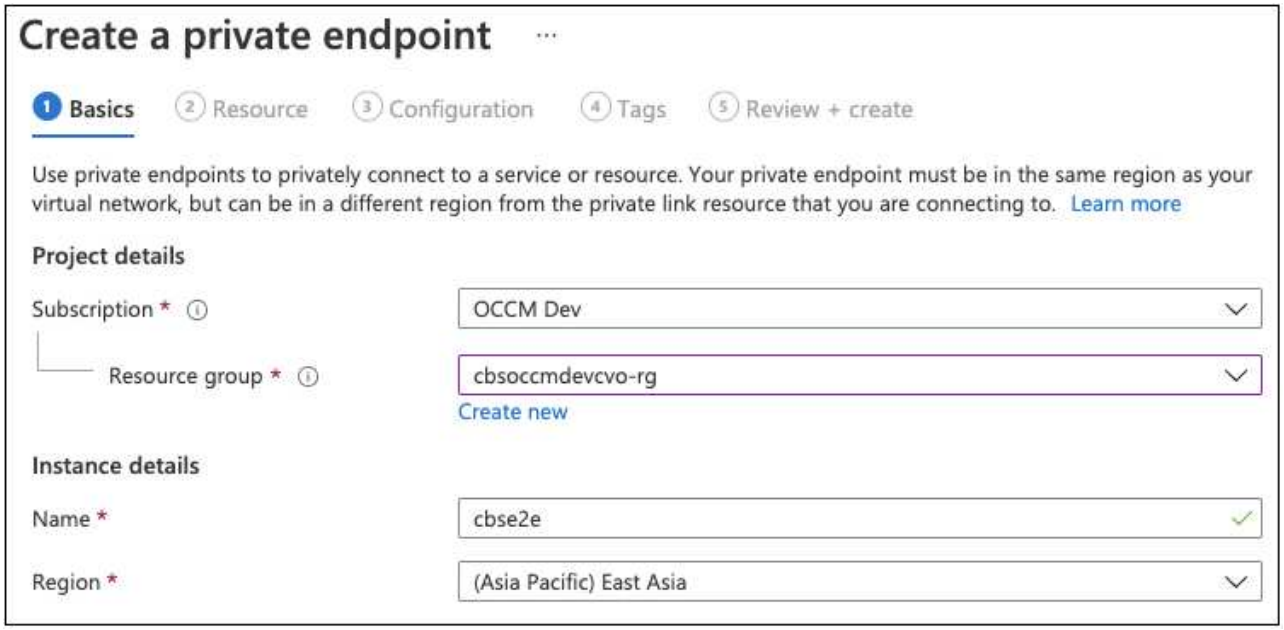
要执行以下操作，您需要网络贡献者权限。

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

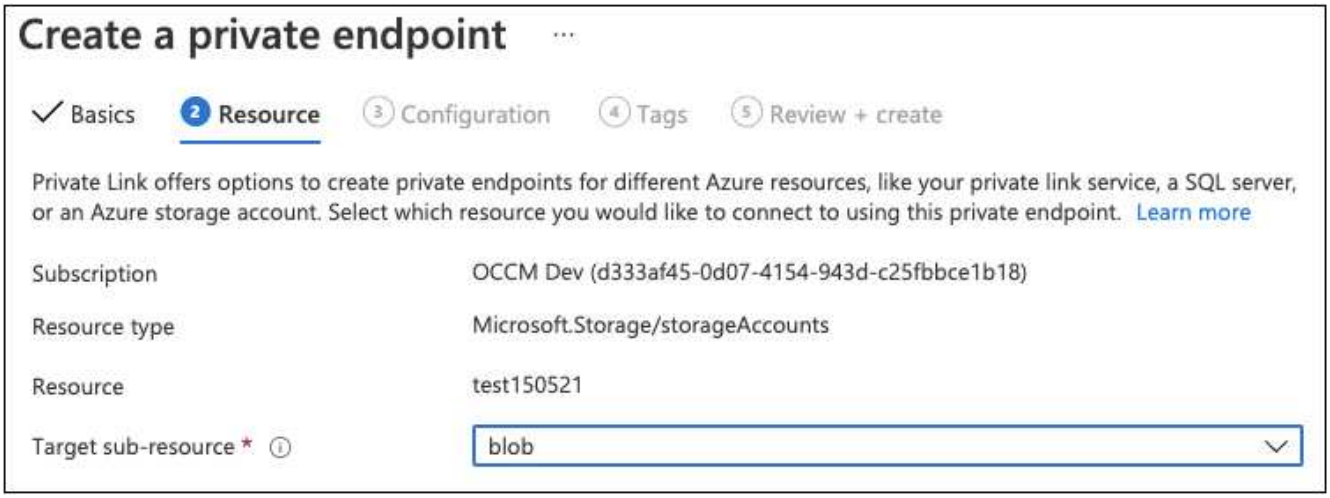
1. 转到存储帐户 > 网络 > 专用端点连接，然后单击 * + 专用端点 * 。



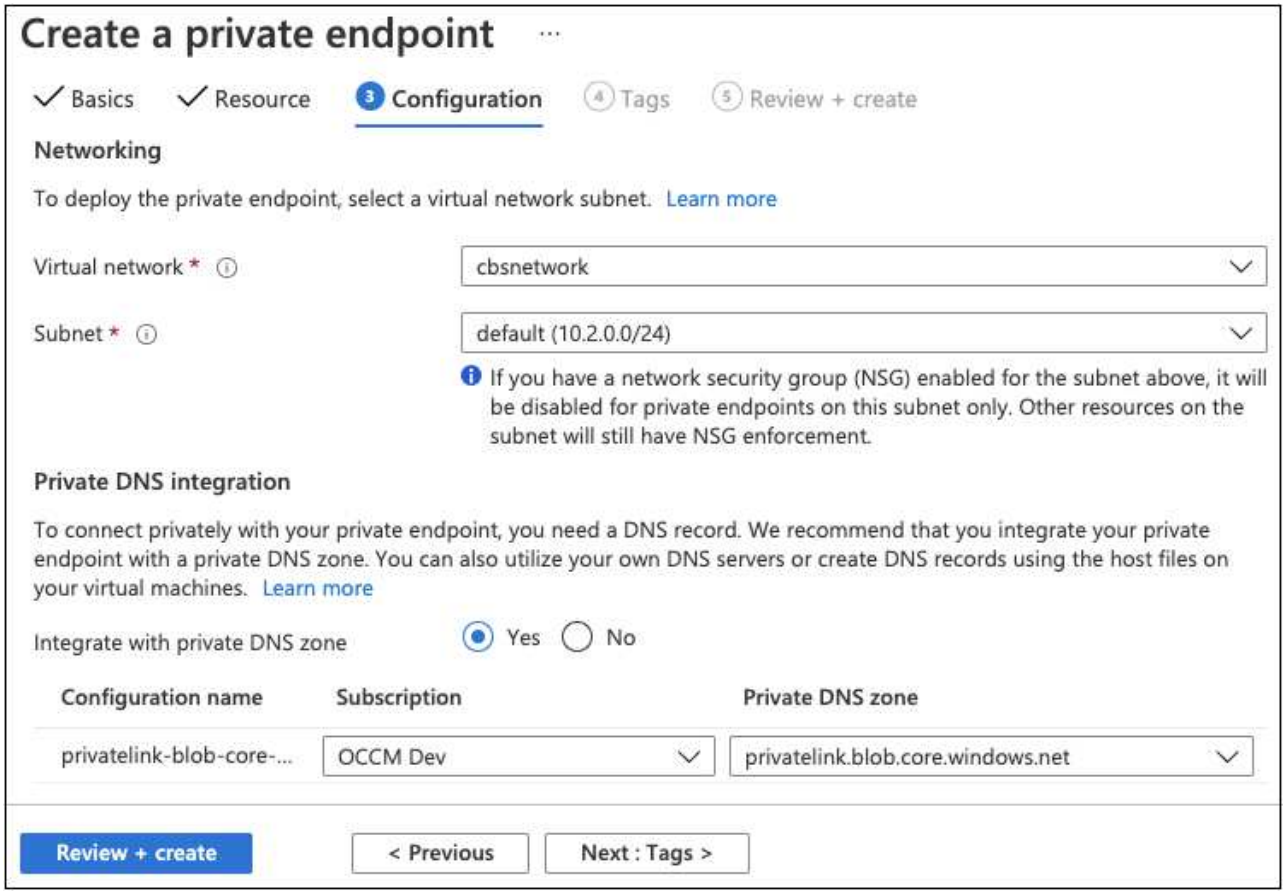
2. 在 Private Endpoint _Basics 页面中：
   - 选择订阅 2 （部署 Cloud Manager Connector 和 Cloud Volumes ONTAP 系统的位置）和资源组。
   - 输入端点名称。
   - 选择区域。



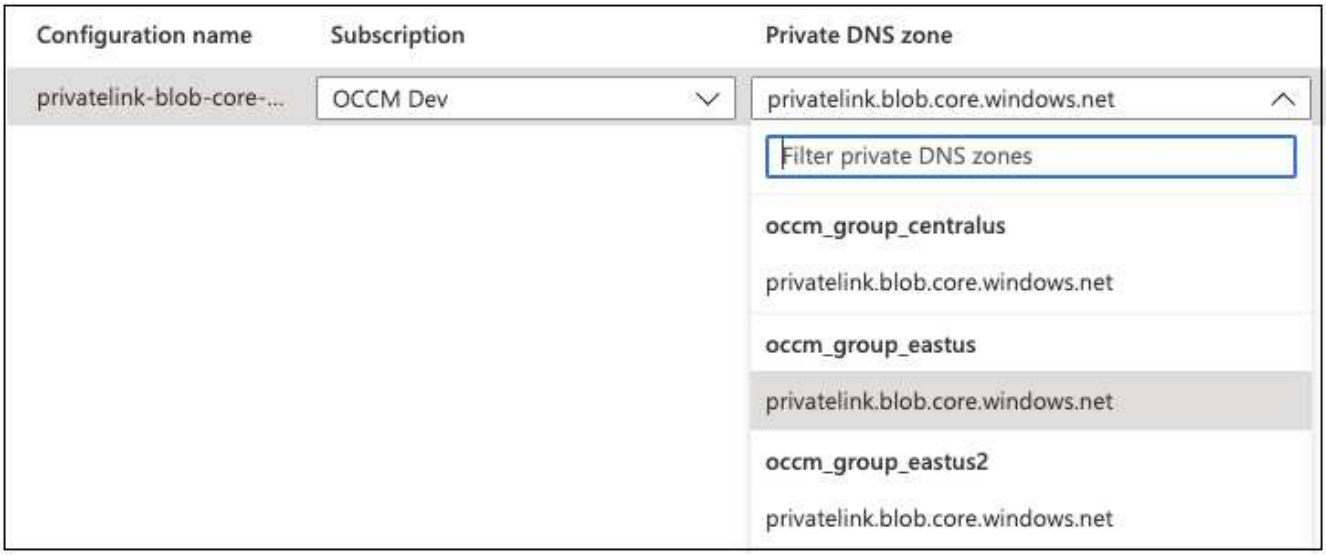
3. 在 *Resources* 页面中，选择目标子资源为 * BLOB * 。



4. 在配置页面中：
   - 选择虚拟网络和子网。
   - 单击 * 是 * 单选按钮以 " 与专用 DNS 区域集成 " 。



5. 在专用 DNS 区域列表中，确保从正确的区域中选择了专用区域，然后单击 * 查看 + 创建 * 。



现在，存储帐户（在订阅 1 中）可以访问在订阅 2 中运行的 Cloud Volumes ONTAP 系统。

6. 请重试在 Cloud Volumes ONTAP 系统上启用云备份，此时应成功启用。