



## 参照 Cloud Backup

NetApp  
May 24, 2022

# 目次

参照 .....	1
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 .....	1
Azure のアーカイブ階層およびリストアの読み出し時間 .....	2
クロスアカウント構成とクロスリージョン構成 .....	3

# 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時は、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。

ソースクラスターで 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。

- ["AWS でマルチアカウントアクセス用に Cloud Backup を設定"](#)
- ["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。

**Success**  
 A VPC peering connection (pcx-049758069d9b7c140) has been requested.  
 The owner of **vpc-116d9174** must accept the peering connection.

<b>Requester VPC owner</b>	733004784675 (This account)	<b>Accepter VPC owner</b>	464262061435
<b>Requester VPC ID</b>	vpc-82f55afa	<b>Accepter VPC ID</b>	vpc-116d9174
<b>Requester VPC Region</b>	us-east-1	<b>Accepter VPC Region</b>	us-east-1
<b>Requester VPC CIDRs</b>	10.0.0.0/16	<b>Accepter VPC CIDRs</b>	-

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

Name	Peering Connecti...	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
cbs-multi-ac...	pcx-049758069d9...	<span style="color: orange;">●</span> Pending Acceptance	vpc-82f55afa   VP...	vpc-116d9174	10.0.0.0/16	-	733004784675	464262061435
cbs-multi-peer	pcx-05f2d310cb7f...	<span style="color: red;">●</span> Deleted	vpc-82f55afa   VP...	vpc-116d9174	-	-	733004784675	464262061435
New_Peering	pcx-6d55ca04	<span style="color: green;">●</span> Active	vpc-b16c90d4   V...	vpc-fc2aa39a   De...	172.31.0.0/16	192.168.0.0/16	733004784675	733004784675

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。

Create Peering Connection		Actions ^						
Filter by tags and attributes		Accept Request Reject Request Delete VPC Peering Connection Edit ClassicLink Settings Edit DNS Settings Add/Edit Tags						
Name	Peering Connection	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Requester Owner	Accepter Owner
estycvoconnect	pcx-049758069d9b7c140	Active	vpc-0647747d   M...	vpc-116d9174	10.2.0.0/24	172.31.0.0/16	464262061435	464262061435
hlll-vpc-peer-chen	pcx-0d0e5c7fc4360254d	Active	vpc-116d9174	vpc-445d4f21	172.31.0.0/16	10.129.0.0/20	464262061435	759995470648
	pcx-049758069d9b7c140	Pending Acceptance	vpc-82f55afa	vpc-116d9174	10.0.0.0/16	-	733004784675	464262061435
	pcx-0d0e5c7fc4360254d	Active	vpc-0d12df59528f...	vpc-824dc0e4   nf...	10.0.0.0/24	10.20.30.0/24	464262061435	464262061435

### Accept VPC Peering Connection Request

Are you sure you want to accept this VPC peering connection request (pcx-049758069d9b7c140)?

Requester Account ID	733004784675	Accepter Account ID	464262061435 (This account)
Requester VPC ID	vpc-82f55afa	Accepter VPC ID	vpc-116d9174
Requester VPC Region	us-east-1	Accepter VPC Region	us-east-1
Requester VPC CIDR	10.0.0.0/16	Accepter VPC CIDR	-

Cancel
Yes, Accept

a. 「\* はい \*」をクリックします。

### Accept VPC Peering Connection Request

Your VPC Peering Connection has been established.

To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables. [Learn more](#)

[Modify my route tables now](#)

Close

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
hlll-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。



VPC > Subnets > subnet-4d315328

## subnet-4d315328 / The Subnet created

**Details**

Subnet ID subnet-4d315328	State Available	VPC vpc-116d9174	IPv4 CIDR 172.31.64.0/20
Available IPv4 addresses 3587	IPv6 CIDR -	Availability Zone us-east-1a	Availability Zone ID use1-az1
Network border group us-east-1	Route table rtb-4da55528	Network ACL acl-c37384a6	Default subnet Yes
Auto-assign public IPv4 address Yes	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool -
Outpost ID -	Owner 464262061435	Subnet ARN arn:aws:ec2:us-east-1:464262061435:subnet/subnet-4d315328	

[Flow logs](#)
[Route table](#)
[Network ACL](#)
[Sharing](#)
[Tags](#)

2. [ ルート ] タブをクリックします。

Route Table ID : rtb-4da55528 Add filter

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
rtb-4da55528	subnet-4d315328	-		Yes	vpc-116d9174	464262061435

Route Table: rtb-4da55528

[Summary](#)
[Routes](#)
[Subnet Associations](#)
[Edge Associations](#)
[Route Propagation](#)
[Tags](#)

[Edit routes](#)

View All routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
pl-63a5400a	vpce-098587ed33c36408c	active	No

3. \* ルートの編集 \* をクリックします。

## Edit routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	active	No
10.20.30.0/24	pcx-0791b47f6f9a27d65	active	No
10.129.0.0/20	pcx-0305041f9cc2dfbdb	active	No

[Add route](#)

\* Required

[Cancel](#)
[Save routes](#)

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。



**Edit routes**

Destination	Target	Status	Propagated	
172.31.0.0/16	local	active	No	
10.20.30.0/24	pcx-0791b47f6f9a27d65	active	No	✕
10.129.0.0/20	pcx-0305041f9cc2dfbdb	active	No	✕
10.0.0.0/24	pcx-		No	✕

**Add route**

\* Required

pcx-05f2d310cb7f49843

pcx-004715531514cb0d8

pcx-049758069d9b7c140 cbs-multi-account

pcx-094f9fdb10a2045ea hill-peer-vadim-vpc

pcx-0791b47f6f9a27d65

pcx-0305041f9cc2dfbdb estycvoconnect

**Cancel Save routes**

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

**Route Tables > Edit routes**

**Edit routes**

✓ Routes successfully edited

**Close**

**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*。

**Credentials** **+ Add Credentials**

3 Credentials

**aws Instance Profile** Credential Type: AWS Keys

464262061435 AWS Account ID

aws-sub-a2 Subscription

CBS-SR-OCCMOCCM1620912870830... IAM Role

2 Working Environments

**aws Saran-XCP-Dev** Credential Type: AWS Keys

733004784675 AWS Account ID

aws-sub-a2 Subscription

AKIA2VKT5MQRZRAWW3HI AWS Access Key

0 Working Environments

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。

Choose an AWS region and then select the working environment that you want to discover.

AWS Region  
US East | N. Virginia

---

**aws** AWS Credentials

Credential Name

Saran-XCP-Dev | Account ID: 733004784675

Instance Profile | Account ID: 464262061435

To add new AWS credentials, go to the [Credentials settings](#).

Apply Cancel

- 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。

Add an Existing Cloud Volumes ONTAP Region

↑ Previous Step This working environment will be created in Cloud Provider Account: **Saran-XCP-Dev** | Account ID: 733004784675 | [Switch Account](#)

Choose an AWS region and then select the working environment that you want to discover.

AWS Region  
US East | N. Virginia

Cloud Volumes ONTAP instances found

Name	VPC Name	Availability Zone	Subnet Id	Cloud Formation Name	Cluster Address	Type
cbscv001	VPC-NAT	us-east-1f	subnet-68e8d464	cbscv001	10.0.0.80	Cloud Volumes ONTAP
testbyolliraz	VPC for VSA	us-east-1a	subnet-c1d99699	testbyolliraz	172.31.5.142	Cloud Volumes ONTAP
ldanAwsHa991001	VPC for VSA	us-east-1a	subnet-c1d99699	ldanAwsHa991001	172.31.5.234, 172.31.5.110	HA Cloud Volumes ONTAP

Continue

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。

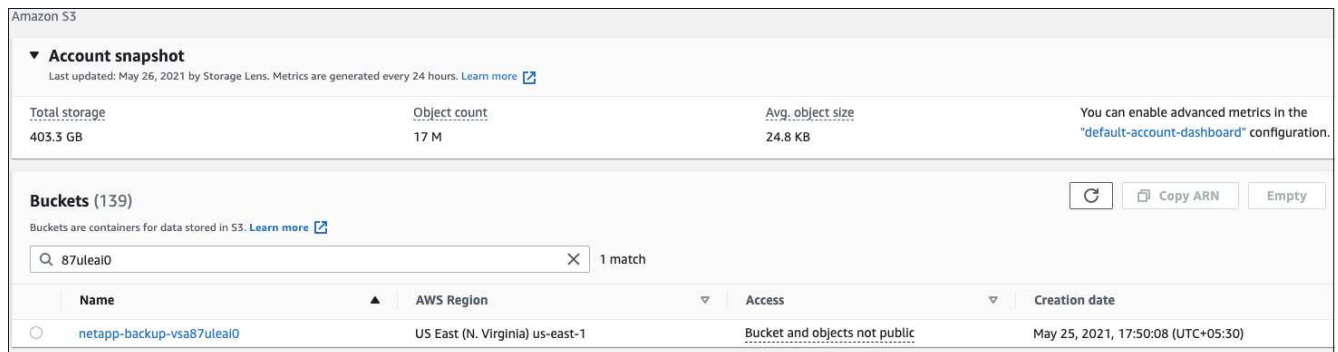
ただし、Cloud Volumes ONTAP システムへのバケットの追加は失敗します。これは、Cloud Backup がインスタンスプロファイルを使用してバケットを追加するため、Cloud Manager インスタンスプロファイルが 2 番目のアカウントのリソースにアクセスできないためです。

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

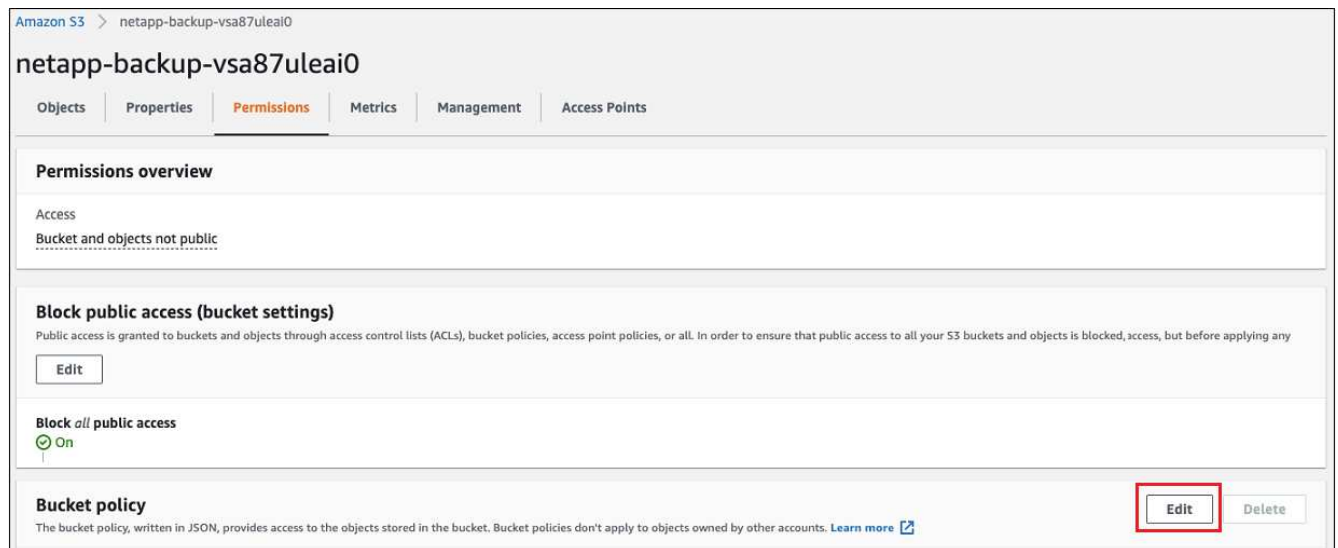


Cloud Backup は「NetApp-backup-」というプレフィックスを付けてすべてのバケットを作成し、作業環境 ID を含めます。たとえば「87ULeAI0」となります

4. EC2 ポータルで S3 に移動し、「87uLeAI0」で終わる名前のバケットを検索すると、「NetApp-backup-vsa87uLeAI0」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-lamInstanceRole-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。

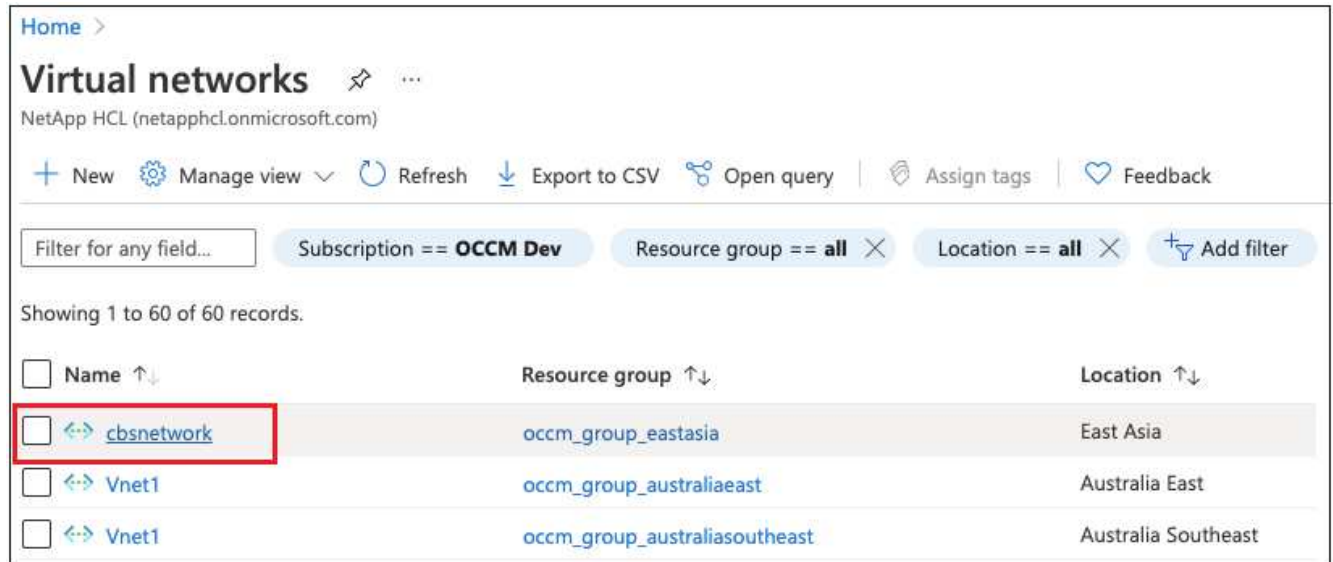
これらの手順は、を実行している場合にのみ必要です ["Cloud Volumes ONTAP データの Azure BLOB ストレージへのバックアップ"](#)。

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。

Subscription \* ⓘ  
OCCM Automation

Virtual network \*  
cbse2evnet

Traffic to remote virtual network ⓘ  
☒ Allow (default)  
☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ  
☒ Allow (default)  
☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ  
☐ Use this virtual network's gateway or Route Server  
☐ Use the remote virtual network's gateway or Route Server  
☒ None (default)

Add

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。

The screenshot shows the 'cbsnetwork | Peerings' page in the Azure portal. The left sidebar contains navigation links: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and a Settings section with links to Address space, Connected devices, Subnets, DDoS protection, Firewall, Security, DNS servers, and Peerings (which is highlighted). The main content area has a search bar, '+ Add' and 'Refresh' buttons, and a table of peerings.

Name	Peering status	Peer
cbsnetwork	Connected	cbse2evnet

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。



Subscription \* ⓘ

OCCM Dev

Virtual network \*

cbsnetwork

Traffic to remote virtual network ⓘ

☒ Allow (default)

☐ Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

☒ Allow (default)

☐ Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server ⓘ

☐ Use this virtual network's gateway or Route Server

☐ Use the remote virtual network's gateway or Route Server

☒ None (default)

Add

ピアリング設定が追加されます。

cbse2evnet | Peerings ...

Virtual network

Search (Cmd+ /) << + Add Refresh

Filter by name...

Name	Peering status	Peer
cbsnetworkpeer	Connected	cbsnetwork

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

Security

DNS servers

Peerings

## 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/4d97b98b-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。

## Create a private endpoint

1 Basics 2 Resource 3 Configuration 4 Tags 5 Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

**Project details**

Subscription \* ① OCCM Dev

Resource group \* ① cbsoccmdevcvo-rg [Create new](#)

**Instance details**

Name \* cbse2e

Region \* (Asia Pacific) East Asia

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

## Create a private endpoint ...

✓ Basics **2 Resource** 3 Configuration 4 Tags 5 Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Subscription OCCM Dev (d333af45-0d07-4154-943d-c25fbbce1b18)

Resource type Microsoft.Storage/storageAccounts

Resource test150521

Target sub-resource \* ⓘ

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。

## Create a private endpoint ...

✓ Basics ✓ Resource **3 Configuration** 4 Tags 5 Review + create

### Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network \* ⓘ

Subnet \* ⓘ

ⓘ If you have a network security group (NSG) enabled for the subnet above, it will be disabled for private endpoints on this subnet only. Other resources on the subnet will still have NSG enforcement.

### Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone ☒ Yes ☐ No

Configuration name	Subscription	Private DNS zone
privatelink-blob-core-...	OCCM Dev	privatelink.blob.core.windows.net

**Review + create** < Previous Next : Tags >

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。

Configuration name	Subscription	Private DNS zone
privatelink-blob-core-...	OCCM Dev	privatelink.blob.core.windows.net
		<input type="text" value="Filter private DNS zones"/>
		<div> <div>occm_group_centralus</div> <div>privatelink.blob.core.windows.net</div> </div>
		<div> <div>occm_group_eastus</div> <div>privatelink.blob.core.windows.net</div> </div>
		<div> <div>occm_group_eastus2</div> <div>privatelink.blob.core.windows.net</div> </div>

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。

- 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

Copyright © 2022 NetApp, Inc. All rights reserved. 米国で印刷されていますこのドキュメントは著作権によって保護されています。画像媒体、電子媒体、および写真複写、記録媒体などの機械媒体など、いかなる形式および方法による複製も禁止します。テープ媒体、または電子検索システムへの保管-著作権所有者の書面による事前承諾なし。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、いかなる場合でも、間接的、偶発的、特別、懲罰的、またはまたは結果的損害（代替品または代替サービスの調達、使用の損失、データ、利益、またはこれらに限定されないものを含みますが、これらに限定されません。）ただし、契約、厳格責任、または本ソフトウェアの使用に起因する不法行為（過失やその他を含む）のいずれであっても、かかる損害の可能性について知らされていた場合でも、責任の理論に基づいて発生します。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、またはその他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1 つ以上の米国特許、その他の国の特許、および出願中の特許により特許、その他の国の特許、および出願中の特許。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7103（1988 年 10 月）および FAR 52-227-19（1987 年 6 月）の Rights in Technical Data and Computer Software（技術データおよびコンピュータソフトウェアに関する諸権利）条項の（c）（1）（ii）項、に規定された制限が適用されます。

## 商標情報

NetApp、NetAppのロゴ、に記載されているマーク <http://www.netapp.com/TM> は、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。