



## 참조하십시오 Cloud Backup

NetApp  
May 24, 2022

This PDF was generated from <https://docs.netapp.com/ko-kr/cloud-manager-backup-restore/reference-aws-backup-tiers.html> on May 24, 2022. Always check docs.netapp.com for the latest.

# 목차

|                                       |   |
|---------------------------------------|---|
| 참조하십시오 .....                          | 1 |
| AWS S3 아카이브 스토리지 클래스 및 복원 검색 시간 ..... | 1 |
| Azure 아카이브 계층 및 복원 검색 시간 .....        | 2 |
| 교차 계정 및 교차 지역 구성 .....                | 3 |

# 참조하십시오

## AWS S3 아카이브 스토리지 클래스 및 복원 검색 시간

Cloud Backup은 2개의 S3 아카이브 스토리지 클래스와 대부분의 영역을 지원합니다.

### Cloud Backup에 지원되는 S3 아카이브 스토리지 클래스

백업 파일이 처음 생성되면 S3\_Standard\_Storage에 저장됩니다. 이 계층은 자주 액세스하지 않는 데이터를 저장하는 데 최적화되어 있지만 이를 즉시 액세스할 수도 있습니다. 30일 후에 백업이 S3\_Standard - Infrequent Access\_storage 클래스로 전환되어 비용이 절감됩니다.

소스 클러스터에서 ONTAP 9.10.1 이상이 실행 중인 경우 추가 비용 최적화를 위해 일정 일(일반적으로 30일 이상) 후에 백업을 S3 Glacier 또는 S3 Glacier Deep Archive\_storage로 계층화하도록 선택할 수 있습니다. 이러한 계층의 데이터는 필요할 때 즉시 액세스할 수 없으며 검색 비용을 더 높여야 하기 때문에 이러한 아카이브 백업 파일에서 데이터를 복원해야 하는 빈도를 고려해야 합니다. 에 대한 섹션을 참조하십시오 [아카이브 스토리지에서 데이터 복원](#).

이러한 유형의 수명주기 규칙을 사용하여 Cloud Backup을 구성할 때는 AWS 계정에서 버킷을 설정할 때 수명주기 규칙을 구성하지 않아야 합니다.

["S3 스토리지 클래스에 대해 알아보십시오"](#).

### 아카이브 스토리지에서 데이터 복원

오래된 백업 파일을 아카이브 스토리지에 저장하는 것은 Standard 또는 Standard-IA 스토리지에 비해 훨씬 저렴하지만, 복원 작업을 위해 아카이브 스토리지에 있는 백업 파일의 데이터에 액세스하는 데 시간이 더 오래 걸리고 비용이 더 많이 듭니다.

### Amazon S3 Glacier 및 Amazon S3 Glacier Deep Archive에서 데이터를 복원하는 데 비용이 얼마나 드나요?

Amazon S3 Glacier에서 데이터를 검색할 때 3가지 복원 우선순위를 선택할 수 있으며, Amazon S3 Glacier Deep Archive에서 데이터를 검색할 경우 2가지 복원 우선순위를 선택할 수 있습니다. S3 Glacier Deep Archive 비용 미만 S3 Glacier:

| 아카이브 계층                     | 복구 우선 순위 및 비용 |                 |                    |
|-----------------------------|---------------|-----------------|--------------------|
|                             | * 높음 *        | * 표준 *          | * 낮음 *             |
| * S3 빙하 *                   | 신속한 검색, 높은 비용 | 검색 속도 감소, 비용 절감 | 가장 느린 검색, 가장 낮은 비용 |
| * S3 Glacier Deep Archive * |               | 빠른 검색, 높은 비용    | 검색 속도 감소, 비용 최소화   |

각 방법은 GB당 검색 비용과 요청당 수수료를 다르게 합니다. AWS 지역별 S3 Glacier 가격 에 대한 자세한 내용은 [참조하십시오 "Amazon S3 가격 페이지"](#).

### Amazon S3 Glacier에 보관된 개체를 복원하는 데 시간이 얼마나 걸립니까?

총 복원 시간을 구성하는 두 가지 부분이 있습니다.

- \* 검색 시간 \*: 아카이브에서 백업 파일을 검색하여 표준 저장소에 저장하는 시간입니다. 이를 "재수화" 시간이라고도 합니다. 검색 시간은 선택한 복원 우선 순위에 따라 다릅니다.

| 아카이브 계층                     | 복구 우선 순위 및 검색 시간 |        |        |
|-----------------------------|------------------|--------|--------|
|                             | * 높음 *           | * 표준 * | * 낮음 * |
| * S3 빙하 *                   | 3-5분             | 3-5시간  | 5-12시간 |
| * S3 Glacier Deep Archive * |                  | 12시간   | 48시간   |

- \* 복구 시간 \*: 표준 저장소의 백업 파일에서 데이터를 복원하는 시간입니다. 이 시간은 아카이브 계층을 사용하지 않을 때 표준 스토리지에서 직접 수행하는 일반적인 복원 작업과 다르지 않습니다.

Amazon S3 Glacier 및 S3 Glacier Deep Archive 검색 옵션에 대한 자세한 내용은 을 참조하십시오 ["이러한 스토리지 클래스에 대한 Amazon FAQ가 있습니다"](#).

## Azure 아카이브 계층 및 복원 검색 시간

Cloud Backup은 하나의 Azure 아카이브 액세스 계층 및 대부분의 영역을 지원합니다.

### Cloud Backup에 지원되는 Azure Blob 액세스 계층

백업 파일이 처음 생성될 때는 \_Cool\_access 계층에 저장됩니다. 이 계층은 자주 액세스하지 않는 데이터를 저장하는 데 최적화되어 있지만 필요할 때 즉시 액세스할 수 있습니다.

소스 클러스터에서 ONTAP 9.10.1 이상이 실행 중인 경우 추가 비용 최적화를 위해 일정 일(일반적으로 30일 이상) 후에 \_Cool\_to\_Azure Archive\_storage에서 백업을 계층화하도록 선택할 수 있습니다. 이 계층의 데이터는 필요할 때 즉시 액세스할 수 없으며 검색 비용을 더 높여야 하기 때문에 이러한 아카이브 백업 파일에서 데이터를 복원해야 하는 빈도를 고려해야 합니다. 에 대한 다음 섹션을 참조하십시오 [아카이브 스토리지에서 데이터 복원](#).

이러한 유형의 수명 주기 규칙으로 Cloud Backup을 구성할 때는 Azure 계정에서 컨테이너를 설정할 때 수명 주기 규칙을 구성하지 않아야 합니다.

["Azure Blob 액세스 계층에 대해 알아보십시오"](#).

### 아카이브 스토리지에서 데이터 복원

오래된 백업 파일을 아카이브 스토리지에 저장하는 것은 Cool 스토리지보다 훨씬 저렴하지만, 복원 작업을 위해 Azure Archive의 백업 파일에서 데이터에 액세스하는 데 더 많은 시간이 걸리고 비용이 더 많이 듭니다.

#### Azure Archive에서 데이터를 복원하는 데 비용이 얼마나 드는가?

Azure Archive에서 데이터를 검색할 때 선택할 수 있는 두 가지 복원 우선 순위가 있습니다.

- \* 높음 \*: 가장 빠른 검색, 높은 비용
- \* 표준 \*: 검색 속도 감소, 비용 절감

각 방법은 GB당 검색 비용과 요청당 수수료를 다르게 합니다. Azure 지역별 Azure Archive에 대한 자세한 가격을 보려면 를 방문하십시오 ["Azure 가격 책정 페이지입니다"](#).

#### Azure Archive에 보관된 데이터를 복원하는 데 시간이 얼마나 걸립니까?

복원 시간을 구성하는 두 가지 부분이 있습니다.

- \* 검색 시간 \*: Azure Archive에서 보관된 백업 파일을 검색하여 Cool storage에 저장하는 시간입니다. 이를

"재수화" 시간이라고도 합니다. 검색 시간은 선택한 복원 우선 순위에 따라 다릅니다.

- \* 높음 \*: 1시간 미만
- \* 표준 \*: 15시간 미만
- \* 복원 시간 \*: Cool storage의 백업 파일에서 데이터를 복원하는 시간입니다. 이 시간은 보관 계층을 사용하지 않을 때 Cool 스토리지에서 직접 수행하는 일반적인 복원 작업과 다르지 않습니다.

Azure Archive 검색 옵션에 대한 자세한 내용은 [이 Azure FAQ를 참조하십시오](#).

## 교차 계정 및 교차 지역 구성

이 항목에서는 여러 클라우드 공급자를 사용할 때 계정 간에 구성할 수 있도록 Cloud Backup을 구성하는 방법을 설명합니다.

- ["AWS에서 다중 계정 액세스를 위해 Cloud Backup을 구성합니다"](#)
- ["Azure에서 다중 계정 액세스를 위해 Cloud Backup을 구성합니다"](#)

### AWS에서 다중 계정 액세스를 위한 백업을 구성합니다

Cloud Backup을 사용하면 소스 Cloud Volumes ONTAP 볼륨이 상주하는 위치와 다른 AWS 계정으로 백업 파일을 생성할 수 있습니다. 이 두 계정 모두 Cloud Manager Connector가 있는 계정과 다를 수 있습니다.

이 단계는 사용자가 있을 때만 필요합니다 ["Cloud Volumes ONTAP 데이터를 Amazon S3에 백업"](#).

아래 단계에 따라 이러한 방법으로 구성을 설정하십시오.

고객 간에 **VPC** 피어링을 설정합니다

1. 두 번째 계정에 로그인하고 피어링 연결 생성:
  - a. 로컬 VPC 선택: 두 번째 계정의 VPC를 선택합니다.
  - b. 다른 VPC 선택: 첫 번째 계정의 계정 ID를 입력합니다.
  - c. Cloud Manager Connector가 실행 중인 지역을 선택합니다. 이 테스트 설정에서는 두 계정이 동일한 지역에서 실행되고 있습니다.
  - d. VPC ID: 첫 번째 계정에 로그인하고 수락 VPC ID를 입력합니다. Cloud Manager Connector의 VPC ID입니다.

aws Services ▾

Peering Connections > Create Peering Connection

## Create Peering Connection

Peering connection name tag  ⓘ

Select a local VPC to peer with

VPC (Requester)\*  ↕ ↻

| CIDRs | CIDR        | Status       | Status Reason |
|-------|-------------|--------------|---------------|
|       | 10.0.0.0/16 | ● associated |               |

Select another VPC to peer with

Account ☐ My account ☒ Another account

Account ID\*

Region ☒ This region (us-east-1) ☐ Another Region

VPC ID (Accepter)\*

성공 대화 상자가 표시됩니다.

**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>  | -            |

피어링 연결의 상태는 Pending Acceptance(수락 보류)로 표시됩니다.

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

2. 첫 번째 계정에 로그인하고 피어링 요청을 수락합니다.

| Create Peering Connection           |                    | Actions ▾  |   |                     |                      |                 |                |                 |                |
|-------------------------------------|--------------------|--|---|---------------------|----------------------|-----------------|----------------|-----------------|----------------|
|                                     |                    | Accept Request<br>Reject Request<br>Delete VPC Peering Connection<br>Edit ClassicLink Settings<br>Edit DNS Settings<br>Add/Edit Tags |   |                     |                      |                 |                |                 |                |
|                                     | Name               | Peering Connection   | Status  | Requester VPC       | Accepter VPC         | Requester CIDRs | Accepter CIDRs | Requester Owner | Accepter Owner |
| <input type="checkbox"/>            |                    |  | <span style="background-color: green;">● Active</span>              | vpc-0647747d   M... | vpc-116d9174         | 10.2.0.0/24     | 172.31.0.0/16  | 464262061435    | 464262061435   |
| <input type="checkbox"/>            | estycvoconnect     |  | <span style="background-color: green;">● Active</span>              | vpc-116d9174        | vpc-445d4f21         | 172.31.0.0/16   | 10.129.0.0/20  | 464262061435    | 759995470648   |
| <input checked="" type="checkbox"/> |                    | pcx-049758069d9b7c140  | <span style="background-color: yellow;">● Pending Acceptance</span> | vpc-82f55afa        | vpc-116d9174         | 10.0.0.0/16     | -              | 733004784675    | 464262061435   |
| <input type="checkbox"/>            | hlli-vpc-peer-chen | pcx-0d0e5c7fc4360254d  | <span style="background-color: green;">● Active</span>              | 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

Requester VPC ID

vpc-82f55afa

Requester VPC Region

us-east-1

Requester VPC CIDR

10.0.0.0/16

Accepter Account ID

464262061435 (This account)

Accepter VPC ID

vpc-116d9174

Accepter VPC Region

us-east-1

Accepter VPC CIDR

-

Cancel

Yes, Accept

a. 예 \* 를 클릭합니다.

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

이제 연결이 활성으로 표시됩니다. 또한 CBS-multi-account라는 피어링 연결을 식별하기 위해 Name 태그를 추가했습니다.

|  | 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. 두 번째 계정에서 피어링 연결을 새로 고치고 상태가 활성으로 변경된다는 것을 확인합니다.

|  | 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   |

두 계정의 라우트 테이블에 경로를 추가합니다

1. VPC > 서브넷 > 경로 테이블 으로 이동합니다.

VPC > Subnets > subnet-4d315328

## subnet-4d315328 / The Subnet created

**Details**

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

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

2. 루트 탭을 클릭합니다.

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. 배관 편집 \* 을 클릭합니다.

## 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. 라우트 추가 \* 를 클릭하고 대상 드롭다운 목록에서 \* 피어링 연결 \* 을 선택한 다음, 생성한 피어링 연결을 선택합니다.

a. 대상에 다른 계정의 서브넷 CIDR을 입력합니다.



### 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. 루트 저장 \* 을 클릭하면 성공 대화 상자가 표시됩니다.

### Route Tables > Edit routes

### Edit routes

✓ Routes successfully edited

**Close**

Cloud Manager에서 두 번째 AWS 계정 자격 증명을 추가합니다

1. 두 번째 AWS 계정(예: *Saran-xCP-Dev*)을 추가합니다.

### Credentials

+ Add Credentials

3 Credentials

**aws Instance Profile**

Credential Type: AWS Keys

464262061435  
AWS Account ID

CBS-SR-OCCMOCCM1620912870830...  
IAM Role

aws-sub-a2  
Subscription

2  
Working Environments

**aws Saran-XCP-Dev**

Credential Type: AWS Keys

733004784675  
AWS Account ID

AKIA2VKT5MQRZRAWW3HI  
AWS Access Key

aws-sub-a2  
Subscription

0  
Working Environments

2. Discover Cloud Volumes ONTAP 페이지에서 새로 추가된 자격 증명을 선택합니다.

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

3. 두 번째 계정에서 검색할 Cloud Volumes ONTAP 시스템을 선택합니다. 두 번째 계정에 새 Cloud Volumes ONTAP 시스템을 배포할 수도 있습니다.

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

이제 두 번째 계정의 Cloud Volumes ONTAP 시스템이 다른 계정에서 실행되는 Cloud Manager에 추가됩니다.



다른 **AWS** 계정에서 백업을 활성화합니다

1. Cloud Manager에서 첫 번째 계정에서 실행 중인 Cloud Volumes ONTAP 시스템에 대한 백업을 활성화하지만 두 번째 계정을 백업 파일 생성 위치로 선택합니다.



2. 그런 다음 백업 정책과 백업할 볼륨을 선택하고 Cloud Backup은 선택한 계정에 새 버킷을 생성하려고 시도합니다.

하지만 Cloud Backup은 인스턴스 프로필을 사용하여 버킷을 추가하고 Cloud Manager 인스턴스 프로필은 두 번째 계정의 리소스에 액세스할 수 없으므로 Cloud Volumes ONTAP 시스템에 버킷을 추가하지 못합니다.

3. Cloud Volumes ONTAP 시스템의 작업 환경 ID를 가져옵니다.



Cloud Backup은 접두사 NetApp-backup으로 모든 버킷을 생성하며 작업 환경 ID(예: 87ULeAI0)를 포함합니다

4. EC2 포털에서 S3로 이동하여 이름이 87uLeAI0으로 끝나는 버킷을 검색하면 버킷 이름이 NetApp-BACKUP-vsa87uLeAI0으로 표시됩니다.



5. 버킷을 클릭한 다음 사용 권한 탭을 클릭하고 버킷 정책 섹션에서 \* 편집 \* 을 클릭합니다.



6. 새로 생성한 버킷에 대한 버킷 정책을 추가하여 Cloud Manager의 AWS 계정에 대한 액세스를 제공한 다음 변경 사항을 저장합니다.

```
{
  "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": "arn:AWS:IAM::464262061435:root"를 사용하면 계정 464262061435의 모든 리소스에 대해 이 버킷에 완벽하게 액세스할 수 있습니다. 특정 역할인 수준으로 줄이려면 특정 역할로 정책을 업데이트할 수 있습니다. 개별 역할을 추가하는 경우 occm 역할도 추가되어야 합니다. 그렇지 않으면 Cloud Backup UI에서 백업이 업데이트되지 않습니다.

예: "AWS": "arn:AWS:IAM::464262061435: role/cvo-instance-profile-version10-d8e-lamInstanceRole-IKJ1HC2E7R"

7. Cloud Volumes ONTAP 시스템에서 클라우드 백업을 다시 활성화해 보십시오. 이번에는 성공적으로 완료되어야 합니다.

## Azure에서 다중 계정 액세스에 대한 백업을 구성합니다

클라우드 백업을 사용하면 소스 Cloud Volumes ONTAP 볼륨이 상주하는 위치와 다른 Azure 계정에서 백업 파일을 생성할 수 있습니다. 이 두 계정 모두 Cloud Manager Connector가 있는 계정과 다를 수 있습니다.

이 단계는 사용자가 있을 때만 필요합니다 ["Azure Blob 저장소에 Cloud Volumes ONTAP 데이터 백업"](#).

아래 단계에 따라 이러한 방법으로 구성을 설정하기만 하면 됩니다.

계정 간 **VNET** 피어링을 설정합니다

클라우드 관리자가 다른 계정/지역에서 Cloud Volumes ONTAP 시스템을 관리하도록 하려면 VNET 피어링을 설정해야 합니다. 스토리지 계정 접속에 VNET 피어링이 필요하지 않습니다.

1. Azure 포털에 로그인하고 집에서 가상 네트워크를 선택합니다.
2. 구독 1로 사용 중인 가입을 선택하고 피어링을 설정할 VNET를 클릭합니다.

Home > Virtual networks

NetApp HCL (netapphcl.onmicrosoft.com)

+ New Manage view Refresh Export to CSV Open query Assign tags Feedback

Filter for any field... Subscription == OCCM Dev Resource group == all Location == all Add filter

Showing 1 to 60 of 60 records.

| <input type="checkbox"/> Name ↑↓    | Resource group ↑↓             | Location ↑↓         |
|-------------------------------------|-------------------------------|---------------------|
| <input type="checkbox"/> cbsnetwork | occm_group_eastasia           | East Asia           |
| <input type="checkbox"/> Vnet1      | occm_group_australiaeast      | Australia East      |
| <input type="checkbox"/> Vnet1      | occm_group_australiasoutheast | Australia Southeast |

3. cbsnetwork \* 를 선택하고 왼쪽 패널에서 \* Pebsland \* 를 클릭한 다음 \* Add \* 를 클릭합니다.

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. 피어링 페이지에 다음 정보를 입력한 다음 \* 추가 \* 를 클릭합니다.

- 이 네트워크의 피어링 링크 이름: 임의의 이름을 지정하여 피어링 연결을 식별할 수 있습니다.
- 원격 가상 네트워크 피어링 링크 이름: 원격 VNET를 식별할 이름을 입력합니다.
- 모든 선택 항목을 기본값으로 유지합니다.
- 구독에서 구독을 선택합니다. 2.
- 가상 네트워크에서, 피어링을 설정할 서브스크립션 2의 가상 네트워크를 선택합니다.



5. 서브스크립션 2 VNET에서 동일한 단계를 수행하고 서브스크립션 1의 가입 및 원격 VNET 세부 정보를 지정합니다.

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

피어링 설정이 추가됩니다.

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



저장소 계정에 대한 개인 끝점을 만듭니다

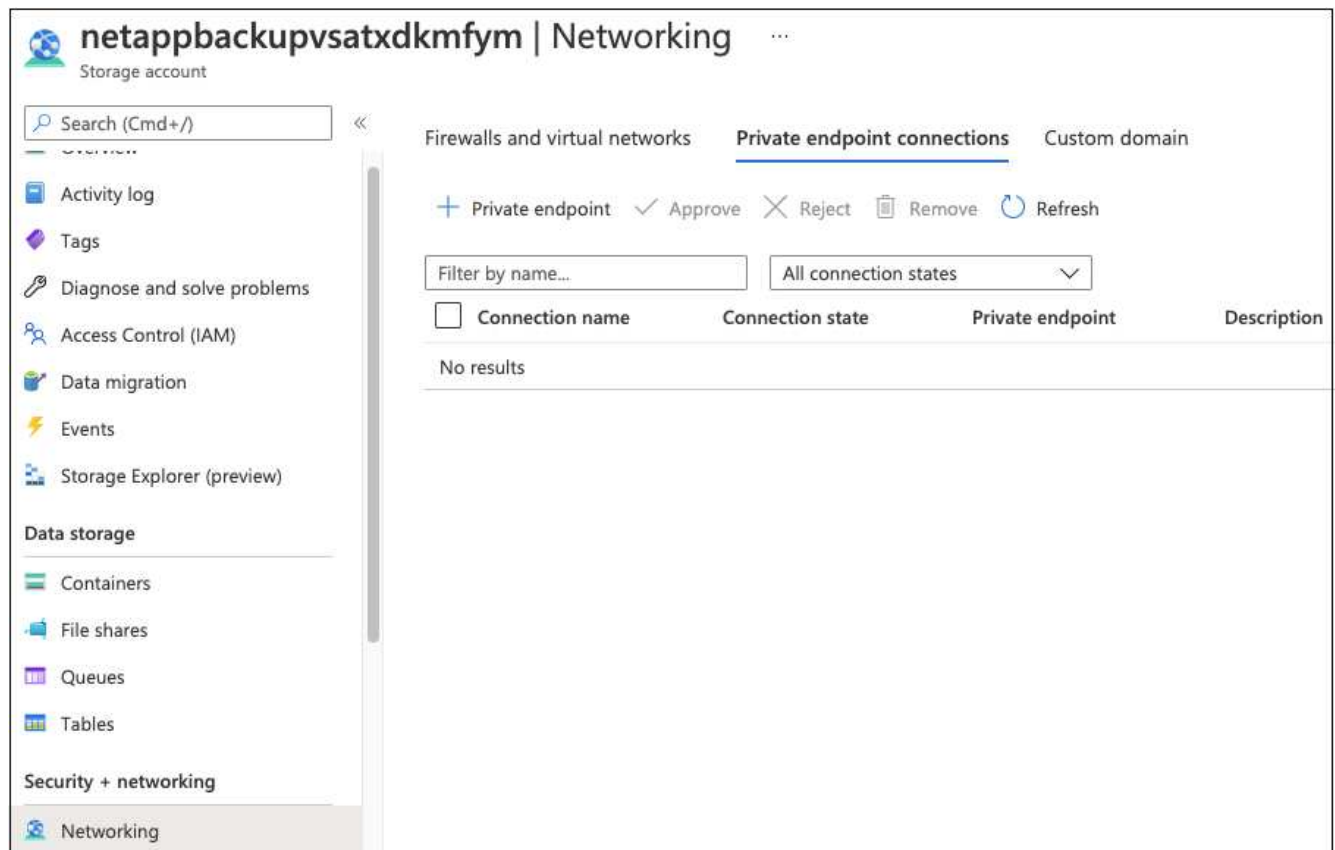
이제 저장소 계정에 대한 개인 끝점을 만들어야 합니다. 이 예에서는 스토리지 계정이 구독 1에 생성되고 Cloud Volumes ONTAP 시스템이 구독 2에서 실행되고 있습니다.



다음 작업을 수행하려면 네트워크 기여자 권한이 필요합니다.

```
{
  "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. 저장소 계정 > 네트워킹 > 개인 끝점 연결로 이동하고 \* + 개인 끝점 \* 을 클릭합니다.



2. 개인 Endpoint\_Basics\_페이지에서 다음을 수행합니다.

- 구독 2(Cloud Manager Connector와 Cloud Volumes ONTAP 시스템이 배포된 위치)와 리소스 그룹을 선택합니다.
- 끝점 이름을 입력합니다.
- 영역을 선택합니다.

### 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\_page에서 타겟 하위 리소스를 \* blob \* 로 선택합니다.

## 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. 구성 페이지에서 다음을 수행합니다.

- 가상 네트워크 및 서브넷을 선택합니다.
- 예 \* 라디오 버튼을 클릭하여 "사설 DNS 영역과 통합"하십시오.

## 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. Private DNS zone(개인 DNS 영역) 목록에서 올바른 지역에서 Private Zone(개인 영역)이 선택되어 있는지 확인하고 \* Review(검토) + Create(생성) \* 를 클릭합니다.

| 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>   |

이제 스토리지 계정(서브스크립션 1)은 서브스크립션 2에서 실행 중인 Cloud Volumes ONTAP 시스템에 액세스할 수 있습니다.

6. Cloud Volumes ONTAP 시스템에서 클라우드 백업을 다시 활성화해 보십시오. 이번에는 성공적으로 완료되어야 합니다.

## 저작권 정보

Copyright © 2022 NetApp, Inc. All rights reserved. 미국에서 인쇄된 본 문서의 어떤 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 그래픽, 전자적 또는 기계적 수단(사진 복사, 레코딩 등)으로도 저작권 소유자의 사전 서면 승인 없이 전자 검색 시스템에 저장 또는 저장.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지 사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 "있는 그대로" 제공되며 상품성 및 특정 목적에 대한 적합성에 대한 명시적 또는 묵시적 보증을 포함하여 이에 제한되지 않고, 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 또는 파생적 손해(소계 물품 또는 서비스의 조달, 사용 손실, 데이터 또는 수익 손실, 계약, 엄격한 책임 또는 불법 행위(과실 또는 그렇지 않은 경우)에 관계없이 어떠한 책임도 지지 않으며, 이는 이러한 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구입의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허 또는 해외 특허, 해외 특허, 해외 특허, 해외 특허, 해외 특허, 해외 특허, 해외 특허, 해외 특허, 미국 출원 중인 특허로 보호됩니다.

권리 제한 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.277-7103(1988년 10월) 및 FAR 52-227-19(1987년 6월)의 기술 데이터 및 컴퓨터 소프트웨어의 권리(Rights in Technical Data and Computer Software) 조항의 하위 조항 (c)(1)(ii)에 설명된 제한사항이 적용됩니다.

## 상표 정보

NETAPP, NETAPP 로고 및 에 나열된 마크는 NetApp에 있습니다 <http://www.netapp.com/TM> 는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.