



네트워크 설정 Cloud Volumes ONTAP

NetApp
June 01, 2022

목차

| | |
|--|----|
| 네트워크 설정 | 1 |
| AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항 | 1 |
| 여러 AZs에서 HA 쌍에 대한 AWS 전송 게이트웨이 설정 | 8 |
| AWS의 보안 그룹 규칙 | 12 |

네트워크 설정

AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항

Cloud Manager는 IP 주소, 넷마스크, 경로 등과 같은 Cloud Volumes ONTAP용 네트워킹 구성 요소 설정을 처리합니다. 아웃바운드 인터넷 액세스를 사용할 수 있는지, 충분한 전용 IP 주소를 사용할 수 있는지, 올바른 연결이 있는지 등을 확인해야 합니다.

일반 요구 사항

AWS에서 다음 요구사항을 충족해야 합니다.

Cloud Volumes ONTAP 노드에 대한 아웃바운드 인터넷 액세스

Cloud Volumes ONTAP 노드를 사용하려면 스토리지 상태를 사전에 모니터링하는 NetApp AutoSupport에 메시지를 보내기 위해 아웃바운드 인터넷 액세스가 필요합니다.

라우팅 및 방화벽 정책은 Cloud Volumes ONTAP가 AutoSupport 메시지를 전송할 수 있도록 다음 엔드포인트로 AWS HTTP/HTTPS 트래픽을 허용해야 합니다.

- <https://support.netapp.com/aods/asupmessage> 으로 문의하십시오
- <https://support.netapp.com/asupprod/post/1.0/postAsup> 으로 문의하십시오

NAT 인스턴스가 있는 경우 개인 서브넷에서 인터넷으로 HTTPS 트래픽을 허용하는 인바운드 보안 그룹 규칙을 정의해야 합니다.

"AutoSupport 구성 방법을 알아보십시오".

HA 중재자를 위한 아웃바운드 인터넷 액세스

HA 중재자 인스턴스는 스토리지 페일오버를 지원할 수 있도록 AWS EC2 서비스에 대한 아웃바운드 연결이 있어야 합니다. 연결을 제공하기 위해 공용 IP 주소를 추가하거나 프록시 서버를 지정하거나 수동 옵션을 사용할 수 있습니다.

수동 옵션은 대상 서브넷에서 AWS EC2 서비스로 연결되는 NAT 게이트웨이 또는 인터페이스 VPC 엔드포인트일 수 있습니다. VPC 엔드포인트에 대한 자세한 내용은 을 참조하십시오 "[AWS 문서:인터페이스 VPC 엔드포인트\(AWS PrivateLink\)](#)".

전용 IP 주소

Cloud Manager는 필요한 수의 프라이빗 IP 주소를 Cloud Volumes ONTAP에 자동으로 할당합니다. 네트워킹에 사용 가능한 개인 IP 주소가 충분한지 확인해야 합니다.

Cloud Manager가 Cloud Volumes ONTAP에 할당하는 LIF 수는 단일 노드 시스템을 구축하든 HA 쌍을 구축하든 관계없이 달라집니다. LIF는 물리적 포트와 연결된 IP 주소입니다.

단일 노드 시스템의 IP 주소입니다

Cloud Manager는 단일 노드 시스템에 6개의 IP 주소를 할당합니다.

- 클러스터 관리 LIF
- 노드 관리 LIF
- 인터클러스터 LIF
- NAS 데이터 LIF
- iSCSI 데이터 LIF
- 스토리지 VM 관리 LIF

스토리지 VM 관리 LIF는 SnapCenter와 같은 관리 툴과 함께 사용됩니다.

HA 쌍의 IP 주소

HA Pair의 경우 단일 노드 시스템보다 더 많은 IP 주소가 필요합니다. 이러한 IP 주소는 다음 이미지와 같이 서로 다른 이더넷 인터페이스에 분산됩니다.



HA 쌍에 필요한 사설 IP 주소의 수는 선택한 구축 모델에 따라 다릅니다. AZ(Single_AWS Availability Zone)에 구축된 HA 쌍에는 15개의 프라이빗 IP 주소가 필요하고, _multiple_AZs에 구축된 HA 쌍에는 13개의 프라이빗 IP 주소가 필요합니다.

다음 표에는 각 프라이빗 IP 주소와 연결된 LIF에 대한 자세한 정보가 나와 있습니다.

단일 AZ에서 HA 쌍을 지원하는 LIF

| LIF | 인터페이스 | 노드 | 목적 |
|------------------|-------|-------------|---|
| 클러스터 관리 | eth0 | 노드 1 | 전체 클러스터(HA 쌍)의 관리 |
| 노드 관리 | eth0 | 노드 1 및 노드 2 | 노드의 관리. |
| 인터클러스터 | eth0 | 노드 1 및 노드 2 | 클러스터 간 통신, 백업 및 복제 |
| NAS 데이터 | eth0 | 노드 1 | NAS 프로토콜을 통한 클라이언트 액세스 |
| iSCSI 데이터 | eth0 | 노드 1 및 노드 2 | iSCSI 프로토콜을 통한 클라이언트 액세스. |
| 클러스터 연결 | eth1 | 노드 1 및 노드 2 | 노드가 서로 통신하고 클러스터 내에서 데이터를 이동할 수 있도록 지원합니다. |
| HA 연결 | eth2 | 노드 1 및 노드 2 | 페일오버 시 두 노드 간의 통신. |
| RSM iSCSI 트래픽입니다 | eth3 | 노드 1 및 노드 2 | RAID SyncMirror iSCSI 트래픽과 두 Cloud Volumes ONTAP 노드 및 중재자 간의 통신 |
| 중재자 | eth0 | 중재자 | 스토리지 테이크오버 및 반환 프로세스를 지원하는 노드와 중재자 간의 통신 채널 |

여러 AZs의 HA 쌍에 대한 LIF

| LIF | 인터페이스 | 노드 | 목적 |
|------------------|-------|-------------|---|
| 노드 관리 | eth0 | 노드 1 및 노드 2 | 노드의 관리. |
| 인터클러스터 | eth0 | 노드 1 및 노드 2 | 클러스터 간 통신, 백업 및 복제 |
| iSCSI 데이터 | eth0 | 노드 1 및 노드 2 | iSCSI 프로토콜을 통한 클라이언트 액세스. 이 LIF는 노드 간 부동 IP 주소의 마이그레이션도 관리합니다. |
| 클러스터 연결 | eth1 | 노드 1 및 노드 2 | 노드가 서로 통신하고 클러스터 내에서 데이터를 이동할 수 있도록 지원합니다. |
| HA 연결 | eth2 | 노드 1 및 노드 2 | 페일오버 시 두 노드 간의 통신. |
| RSM iSCSI 트래픽입니다 | eth3 | 노드 1 및 노드 2 | RAID SyncMirror iSCSI 트래픽과 두 Cloud Volumes ONTAP 노드 및 중재자 간의 통신 |
| 중재자 | eth0 | 중재자 | 스토리지 테이크오버 및 반환 프로세스를 지원하는 노드와 중재자 간의 통신 채널 |



여러 가용성 영역에 구축된 경우 여러 LIF가 에 연결됩니다 "유동 IP 주소"이는 AWS 프라이빗 IP 제한에 계산되지 않습니다.

보안 그룹

Cloud Manager에서 보안 그룹을 생성할 수 있으므로 보안 그룹을 생성할 필요가 없습니다. 직접 사용해야 하는 경우 을 참조하십시오 "보안 그룹 규칙".

데이터 계층화를 위한 연결

EBS를 성능 계층으로 사용하고 AWS S3를 용량 계층으로 사용하려면 Cloud Volumes ONTAP이 S3에 연결되어 있는지 확인해야 합니다. 이 연결을 제공하는 가장 좋은 방법은 S3 서비스에 VPC 엔드포인트를 생성하는 것입니다. 자세한 내용은 [을 참조하십시오 "AWS 설명서: 게이트웨이 엔드포인트 생성"](#).

VPC 끝점을 만들 때 Cloud Volumes ONTAP 인스턴스에 해당하는 영역, VPC 및 라우팅 테이블을 선택해야 합니다. 또한 S3 엔드포인트에 대한 트래픽을 활성화하는 아웃바운드 HTTPS 규칙을 추가하려면 보안 그룹을 수정해야 합니다. 그렇지 않으면 Cloud Volumes ONTAP에서 S3 서비스에 연결할 수 없습니다.

문제가 발생하면 [을 참조하십시오 "AWS 지원 지식 센터: 게이트웨이 VPC 엔드포인트를 사용하여 S3 버킷에 연결할 수 없는 이유는 무엇입니까?"](#)

ONTAP 시스템에 대한 연결

AWS의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 AWS VPC와 회사 네트워크 같은 다른 네트워크 간에 VPN 연결을 설정해야 합니다. 자세한 내용은 [을 참조하십시오 "AWS 설명서: AWS VPN 연결 설정"](#).

CIFS용 DNS 및 Active Directory

CIFS 스토리지를 프로비저닝하려면 AWS에서 DNS 및 Active Directory를 설정하거나 사내 설정을 AWS로 확장해야 합니다.

DNS 서버는 Active Directory 환경에 대한 이름 확인 서비스를 제공해야 합니다. Active Directory 환경에서 사용되는 DNS 서버가 아니어야 하는 기본 EC2 DNS 서버를 사용하도록 DHCP 옵션 집합을 구성할 수 있습니다.

자세한 지침은 [을 참조하십시오 "AWS 설명서: AWS 클라우드의 Active Directory 도메인 서비스: 빠른 시작 참조 배포"](#).

여러 대의 AZs에서 HA 쌍에 대한 요구 사항

추가 AWS 네트워킹 요구사항은 ZS(Multiple Availability Zones)를 사용하는 Cloud Volumes ONTAP HA 구성에 적용됩니다. 작업 환경을 생성할 때 Cloud Manager에 네트워킹 세부 정보를 입력해야 하므로 HA 쌍을 실행하기 전에 이러한 요구사항을 검토해야 합니다.

HA 쌍의 작동 방식을 이해하려면 [를 참조하십시오 "고가용성 쌍"](#).

가용성 영역

이 HA 구축 모델은 여러 대의 AZs를 사용하여 데이터의 고가용성을 보장합니다. 각 Cloud Volumes ONTAP 인스턴스와 중재자 인스턴스에 전용 AZ를 사용해야 하며 HA 쌍 간의 통신 채널을 제공합니다.

각 가용성 영역에서 서브넷을 사용할 수 있어야 합니다.

NAS 데이터 및 클러스터/SVM 관리를 위한 부동 IP 주소

여러 AZs의 HA 구성에서는 장애가 발생할 경우 노드 간에 이동하는 부동 IP 주소를 사용합니다. 고객이 아니라면 VPC 외부에서 기본적으로 액세스할 수 없습니다 ["AWS 전송 게이트웨이를 설정합니다"](#).

하나의 부동 IP 주소는 클러스터 관리용, 하나는 노드 1의 NFS/CIFS 데이터용으로, 다른 하나는 노드 2의 NFS/CIFS 데이터용으로 사용됩니다. SVM 관리를 위한 네 번째 유동 IP 주소는 선택 사항입니다.



Windows용 SnapDrive 또는 HA 쌍을 지원하는 SnapCenter를 사용하는 경우 SVM 관리 LIF에는 부동 IP 주소가 필요합니다.

Cloud Volumes ONTAP HA 작업 환경을 생성할 때 Cloud Manager에 부동 IP 주소를 입력해야 합니다. Cloud Manager는 시스템을 시작할 때 HA 쌍에 IP 주소를 할당합니다.

부동 IP 주소는 HA 구성을 배포하는 AWS 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 합니다. 유동 IP 주소를 해당 지역의 VPC 외부에 있는 논리적 서브넷으로 생각해 보십시오.

다음 예에서는 AWS 영역에 있는 VPC와 유동 IP 주소 간의 관계를 보여 줍니다. 부동 IP 주소는 모든 VPC에 대한 CIDR 블록 외부에 있지만 라우팅 테이블을 통해 서브넷으로 라우팅할 수 있습니다.

AWS region



Cloud Manager는 VPC 외부의 클라이언트에서 iSCSI 액세스 및 NAS 액세스를 위한 정적 IP 주소를 자동으로 생성합니다. 이러한 유형의 IP 주소에 대한 요구 사항을 충족할 필요는 없습니다.

VPC 외부에서 유동 IP 액세스를 지원하는 전송 게이트웨이

필요한 경우 ["AWS 전송 게이트웨이를 설정합니다"](#) HA 쌍이 상주하는 VPC 외부에서 HA 쌍의 부동 IP 주소에 액세스할 수 있도록 합니다.

배관 테이블

Cloud Manager에서 부동 IP 주소를 지정한 후 부동 IP 주소에 대한 라우트를 포함해야 하는 라우팅 테이블을 선택하라는 메시지가 표시됩니다. 이렇게 하면 클라이언트가 HA 쌍에 액세스할 수 있습니다.

VPC(기본 경로 테이블)에 있는 서브넷에 대해 하나의 라우팅 테이블만 있는 경우 Cloud Manager는 해당 라우팅 테이블에 부동 IP 주소를 자동으로 추가합니다. 둘 이상의 라우팅 테이블이 있는 경우 HA 쌍을 시작할 때 올바른 라우팅 테이블을 선택하는 것이 매우 중요합니다. 그렇지 않으면 일부 클라이언트가 Cloud Volumes ONTAP에 액세스하지 못할 수 있습니다.

예를 들어, 서로 다른 라우팅 테이블에 연결된 두 개의 서브넷이 있을 수 있습니다. 라우팅 테이블 A를 선택했지만 라우팅 테이블 B는 선택하지 않은 경우, 라우팅 테이블 A와 연결된 서브넷에 있는 클라이언트는 HA 쌍에 액세스할 수 있지만, 라우팅 테이블 B와 연결된 서브넷에 있는 클라이언트는 액세스할 수 없습니다.

라우팅 테이블에 대한 자세한 내용은 [AWS 설명서: 경로 테이블](#)을 참조하십시오.

NetApp 관리 톨에 연결

여러 AZs에 있는 HA 구성에서 NetApp 관리 톨을 사용하려면 다음 두 가지 연결 옵션을 사용할 수 있습니다.

1. NetApp 관리 톨을 다른 VPC 및 에 구축할 수 있습니다 ["AWS 전송 게이트웨이를 설정합니다"](#). 게이트웨이를 사용하면 VPC 외부에서 클러스터 관리 인터페이스의 부동 IP 주소에 액세스할 수 있습니다.
2. NAS 클라이언트와 비슷한 라우팅 구성을 사용하여 동일한 VPC에 NetApp 관리 톨을 구축합니다.

HA 구성의 예

다음 그림에서는 여러 AZs의 HA 쌍, 즉 가용성 영역 3개, 서브넷 3개, 부동 IP 주소 및 라우팅 테이블과 같은 네트워크 구성 요소를 보여 줍니다.



커넥터 요구 사항

Connector가 공용 클라우드 환경 내에서 리소스와 프로세스를 관리할 수 있도록 네트워킹을 설정합니다. 가장 중요한 단계는 다양한 엔드포인트에 대한 아웃바운드 인터넷 액세스를 보장하는 것입니다.



네트워크에서 인터넷에 대한 모든 통신에 프록시 서버를 사용하는 경우 설정 페이지에서 프록시 서버를 지정할 수 있습니다. 을 참조하십시오 ["프록시 서버를 사용하도록 Connector 구성"](#).

대상 네트워크에 연결

커넥터를 사용하려면 Cloud Volumes ONTAP를 배포할 VPC 및 VNet에 대한 네트워크 연결이 필요합니다.

예를 들어 회사 네트워크에 커넥터를 설치하는 경우 Cloud Volumes ONTAP를 실행하는 VPC 또는 VNET에 대한 VPN 연결을 설정해야 합니다.

아웃바운드 인터넷 액세스

Connector를 사용하려면 공용 클라우드 환경 내의 리소스와 프로세스를 관리하기 위한 아웃바운드 인터넷 액세스가 필요합니다.

| 엔드포인트 | 목적 |
|--|--|
| https://support.netapp.com 으로 문의하십시오 | 라이선스 정보를 얻고 AutoSupport 메시지를 NetApp 지원 팀에 전송합니다. |
| https://*.cloudmanager.cloud.netapp.com 으로 문의하십시오 | Cloud Manager 내에서 SaaS 기능 및 서비스를 제공합니다. |
| https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net 으로 문의하십시오 | Connector 및 해당 Docker 구성 요소를 업그레이드합니다. |

여러 AZs에서 HA 쌍에 대한 AWS 전송 게이트웨이 설정

HA 쌍에 대한 액세스를 지원하는 AWS 전송 게이트웨이를 설정합니다 "유동 IP 주소" HA 쌍이 상주하는 VPC 외부에서

Cloud Volumes ONTAP HA 구성이 여러 AWS 가용성 영역에 분산되면 VPC 내에서 NAS 데이터 액세스에 유동 IP 주소가 필요합니다. 이러한 부동 IP 주소는 장애가 발생할 때 노드 간에 마이그레이션할 수 있지만 VPC 외부에서 기본적으로 액세스할 수 없습니다. 별도의 프라이빗 IP 주소를 통해 VPC 외부에서 데이터에 액세스할 수 있지만 자동 페일오버를 제공하지 않습니다.

클러스터 관리 인터페이스와 선택적 SVM 관리 LIF에도 부동 IP 주소가 필요합니다.

AWS 전송 게이트웨이를 설정한 경우 HA 쌍이 상주하는 VPC 외부의 유동 IP 주소에 액세스할 수 있습니다. 즉, VPC 외부에 있는 NAS 클라이언트와 NetApp 관리 툴이 유동 IP에 액세스할 수 있습니다.

다음은 전송 게이트웨이에 의해 연결된 두 대의 VPC를 보여 주는 예입니다. HA 시스템은 VPC 하나에 상주하고 클라이언트는 다른 VPC에 상주합니다. 그런 다음 부동 IP 주소를 사용하여 클라이언트에 NAS 볼륨을 마운트할 수 있습니다.



다음 단계에서는 유사한 구성을 설정하는 방법을 보여 줍니다.

단계

1. "전송 게이트웨이를 만들고 VPC를 게이트웨이에 연결합니다".
2. VPC를 전송 게이트웨이 경로 테이블에 연결합니다.
 - a. VPC * 서비스에서 * Transit Gateway Route Tables * 를 클릭합니다.
 - b. 라우팅 테이블을 선택합니다.
 - c. 연결 * 을 클릭한 다음 * 연결 생성 * 을 선택합니다.
 - d. 연결할 첨부 파일(VPC)을 선택한 다음 * 연결 생성 * 을 클릭합니다.
3. HA 쌍의 부동 IP 주소를 지정하여 전송 게이트웨이의 라우팅 테이블에서 경로를 만듭니다.

Cloud Manager의 작업 환경 정보 페이지에서 부동 IP 주소를 찾을 수 있습니다. 예를 들면 다음과 같습니다.

NFS & CIFS access from within the VPC using Floating IP

Auto failover

Cluster Management : 172.23.0.1

Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

Access

SVM Management : 172.23.0.4

다음 샘플 이미지는 전송 게이트웨이의 라우트 테이블을 보여 줍니다. 여기에는 2개의 VPC의 CIDR 블록에 대한 경로와 Cloud Volumes ONTAP에서 사용하는 4개의 부동 IP 주소가 포함됩니다.

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aedd3

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

| <input type="checkbox"/> | CIDR | Attachment | Resource type | Route type | Route state |
|--------------------------|---------------|--|---------------|------------|-------------|
| <input type="checkbox"/> | 10.100.0.0/16 | tgw-attach-05e77bd34e2ff91f8 vpc-0b2bc30e0dc8e0db1 | VPC2 | propagated | active |
| <input type="checkbox"/> | 10.160.0.0/20 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | VPC1 | propagated | active |
| <input type="checkbox"/> | 172.23.0.1/32 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | VPC | static | active |
| <input type="checkbox"/> | 172.23.0.2/32 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | Floating IP | static | active |
| <input type="checkbox"/> | 172.23.0.3/32 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | Floating IP | static | active |
| <input type="checkbox"/> | 172.23.0.4/32 | tgw-attach-00eba3eac3250d7db vpc-673ae603 | Floating IP | static | active |

4. 부동 IP 주소에 액세스해야 하는 VPC의 라우팅 테이블을 수정합니다.

a. 부동 IP 주소에 라우트 항목을 추가합니다.

b. HA 쌍이 상주하는 VPC의 CIDR 블록에 경로 항목을 추가합니다.

다음 샘플 이미지는 VPC 1에 대한 라우트 및 부동 IP 주소를 포함하는 VPC 2용 라우팅 테이블을 보여 줍니다.

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

| Destination | Target | Status | Propagated |
|---------------|-----------------------|--------|------------|
| 10.100.0.0/16 | local | active | No |
| 0.0.0.0/0 | lgw-07250bd01781e67df | active | No |
| 10.160.0.0/20 | tgw-015b7c249661ac279 | active | No |
| 172.23.0.1/32 | tgw-015b7c249661ac279 | active | No |
| 172.23.0.2/32 | tgw-015b7c249661ac279 | active | No |
| 172.23.0.3/32 | tgw-015b7c249661ac279 | active | No |
| 172.23.0.4/32 | tgw-015b7c249661ac279 | active | No |

VPC1
Floating IP
Addresses

5. 유동 IP 주소에 액세스해야 하는 VPC에 경로를 추가하여 HA 쌍 VPC의 경로 테이블을 수정합니다.

이 단계는 VPC 간 라우팅을 완료하기 때문에 중요합니다.

다음 샘플 이미지는 VPC 1의 라우트 테이블을 보여 줍니다. 여기에는 부동 IP 주소 및 클라이언트가 있는 VPC 2로의 라우트가 포함됩니다. Cloud Manager에서 HA 쌍을 구축하면 라우팅 테이블에 유동 IP가 자동으로 추가됩니다.

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

| Destination | Target | Status |
|---|-----------------------|--------|
| 10.160.0.0/20 | local | active |
| pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22) | vpce-cb51a0a2 | active |
| 0.0.0.0/0 | lgw-b2182dd7 | active |
| 10.60.29.0/25 | pcx-589c3331 | active |
| 10.100.0.0/16 | tgw-015b7c249661ac279 | active |
| 10.129.0.0/20 | pcx-f7e1396 | active |
| 172.23.0.1/32 | eni-0854d4715559c3cdb | active |
| 172.23.0.2/32 | eni-0854d4715559c3cdb | active |
| 172.23.0.3/32 | eni-0f76681216c3108ed | active |
| 172.23.0.4/32 | eni-0854d4715559c3cdb | active |

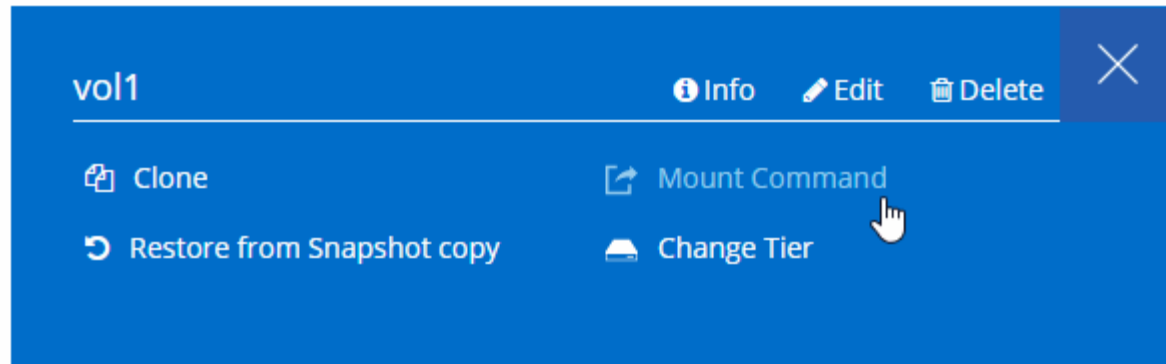
VPC2
Floating
IP
Addresses

6. 부동 IP 주소를 사용하여 클라이언트에 볼륨을 마운트합니다.

볼륨을 선택하고 * 탑재 명령 * 을 클릭하여 Cloud Manager에서 올바른 IP 주소를 찾을 수 있습니다.

Volumes

2 Volumes | 0.22 TB Allocated | < 0.01 TB Used (0 TB in S3)



7. NFS 볼륨을 마운트하는 경우 클라이언트 VPC의 서브넷에 일치하도록 익스포트 정책을 구성합니다.

"볼륨을 편집하는 방법에 대해 알아봅니다".

- 관련 링크 *
- "AWS의 고가용성 쌍"
- "AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항"

AWS의 보안 그룹 규칙

Cloud Manager는 Connector와 Cloud Volumes ONTAP가 성공적으로 운영하는 데 필요한 인바운드 및 아웃바운드 규칙을 포함하는 AWS 보안 그룹을 생성합니다. 테스트 목적으로 또는 자체 보안 그룹을 사용하려는 경우 포트를 참조할 수 있습니다.

Cloud Volumes ONTAP 규칙

Cloud Volumes ONTAP의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

인바운드 규칙

미리 정의된 보안 그룹의 인바운드 규칙 소스는 0.0.0.0/0입니다.

| 프로토콜 | 포트 | 목적 |
|------------|-----|--|
| 모든 ICMP | 모두 | 인스턴스에 Ping을 수행 중입니다 |
| HTTP | 80 | 클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTP 액세스 |
| HTTPS | 443 | 클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTPS 액세스 |
| SSH를 클릭합니다 | 22 | 클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다 |

| 프로토콜 | 포트 | 목적 |
|--------|----------|---|
| TCP | 111 | NFS에 대한 원격 프로시저 호출 |
| TCP | 139 | CIFS에 대한 NetBIOS 서비스 세션입니다 |
| TCP | 161-162 | 단순한 네트워크 관리 프로토콜 |
| TCP | 445 | Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임 |
| TCP | 635 | NFS 마운트 |
| TCP | 749 | Kerberos |
| TCP | 2049 | NFS 서버 데몬 |
| TCP | 3260 | iSCSI 데이터 LIF를 통한 iSCSI 액세스 |
| TCP | 4045 | NFS 잠금 데몬 |
| TCP | 4046 | NFS에 대한 네트워크 상태 모니터 |
| TCP | 10000입니다 | NDMP를 사용한 백업 |
| TCP | 11104 | SnapMirror에 대한 인터클러스터 통신 세션의 관리 |
| TCP | 11105 | 인터클러스터 LIF를 사용하여 SnapMirror 데이터 전송 |
| UDP입니다 | 111 | NFS에 대한 원격 프로시저 호출 |
| UDP입니다 | 161-162 | 단순한 네트워크 관리 프로토콜 |
| UDP입니다 | 635 | NFS 마운트 |
| UDP입니다 | 2049 | NFS 서버 데몬 |
| UDP입니다 | 4045 | NFS 잠금 데몬 |
| UDP입니다 | 4046 | NFS에 대한 네트워크 상태 모니터 |
| UDP입니다 | 4049 | NFS quotad 프로토콜 |

아웃바운드 규칙

Cloud Volumes ONTAP에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

기본 아웃바운드 규칙

Cloud Volumes ONTAP에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

| 프로토콜 | 포트 | 목적 |
|---------|----|--------------|
| 모든 ICMP | 모두 | 모든 아웃바운드 트래픽 |

| 프로토콜 | 포트 | 목적 |
|--------|----|--------------|
| 모든 TCP | 모두 | 모든 아웃바운드 트래픽 |
| 모든 UDP | 모두 | 모든 아웃바운드 트래픽 |

고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Cloud Volumes ONTAP의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.



소스는 Cloud Volumes ONTAP 시스템의 인터페이스(IP 주소)입니다.

| 서비스 | 프로토콜 | 포트 | 출처 | 목적지 | 목적 |
|------------------------------------|--------------|-----|------------------------------|-----------------------------|---|
| Active Directory 를 클릭합니 다 | TCP | 88 | 노드 관리 LIF | Active Directory 포리스트입니다 | Kerberos V 인증 |
| | UDP입니 다 | 137 | 노드 관리 LIF | Active Directory 포리스트입니다 | NetBIOS 이름 서비스입니다 |
| | UDP입니 다 | 138 | 노드 관리 LIF | Active Directory 포리스트입니다 | NetBIOS 데이터그램 서비스 |
| | TCP | 139 | 노드 관리 LIF | Active Directory 포리스트입니다 | NetBIOS 서비스 세션입니다 |
| | TCP 및 UDP | 389 | 노드 관리 LIF | Active Directory 포리스트입니다 | LDAP를 지원합니다 |
| | TCP | 445 | 노드 관리 LIF | Active Directory 포리스트입니다 | Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임 |
| | TCP | 464 | 노드 관리 LIF | Active Directory 포리스트입니다 | Kerberos V 변경 및 암호 설정(set_change) |
| | UDP입니 다 | 464 | 노드 관리 LIF | Active Directory 포리스트입니다 | Kerberos 키 관리 |
| | TCP | 749 | 노드 관리 LIF | Active Directory 포리스트입니다 | Kerberos V 변경 및 암호 설정(RPCSEC_GSS) |
| | TCP | 88 | 데이터 LIF(NFS, CIFS, iSCSI) | Active Directory 포리스트입니다 | Kerberos V 인증 |
| | UDP입니 다 | 137 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | NetBIOS 이름 서비스입니다 |
| | UDP입니 다 | 138 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | NetBIOS 데이터그램 서비스 |
| | TCP | 139 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | NetBIOS 서비스 세션입니다 |
| | TCP 및 UDP | 389 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | LDAP를 지원합니다 |
| | TCP | 445 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임 |
| | TCP | 464 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | Kerberos V 변경 및 암호 설정(set_change) |
| | UDP입니 다 | 464 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | Kerberos 키 관리 |
| | TCP | 749 | 데이터 LIF(NFS, CIFS) | Active Directory 포리스트입니다 | Kerberos V 변경 및 암호 설정(RPCSEC_GSS) |
| AutoSupp ort | HTTPS | 443 | 노드 관리 LIF | support.netapp.com | AutoSupport(기본값은 HTTPS) |
| | HTTP | 80 | 노드 관리 LIF | support.netapp.com | AutoSupport(전송 프로토콜이 HTTPS에서 HTTP로 변경된 경우에만 해당) |

| 서비스 | 프로토콜 | 포트 | 출처 | 목적지 | 목적 |
|--------------------|----------|------------|--------------------------------|------------------|--|
| S3로 백업 | TCP | 5010 | 인터클러스터 LIF | 엔드포인트 백업 또는 복원 | S3로 백업 기능의 백업 및 복원 작업 |
| 클러스터 | 모든 교통 정보 | 모든 교통 정보 | 모든 LIF가 하나의 노드에 있습니다 | 다른 노드의 모든 LIF | 인터클러스터 통신(Cloud Volumes ONTAP HA에만 해당) |
| | TCP | 3000 입니다 | 노드 관리 LIF | HA 중재자 | ZAPI 호출(Cloud Volumes ONTAP HA 전용) |
| | ICMP | 1 | 노드 관리 LIF | HA 중재자 | 활성 상태 유지(Cloud Volumes ONTAP HA만 해당) |
| DHCP를 선택합니다 | UDP입니다 | 68 | 노드 관리 LIF | DHCP를 선택합니다 | 처음으로 설정하는 DHCP 클라이언트 |
| DHCPs | UDP입니다 | 67 | 노드 관리 LIF | DHCP를 선택합니다 | DHCP 서버 |
| DNS | UDP입니다 | 53 | 노드 관리 LIF 및 데이터 LIF(NFS, CIFS) | DNS | DNS |
| NDMP | TCP | 1860-18699 | 노드 관리 LIF | 대상 서버 | NDMP 복제 |
| SMTP | TCP | 25 | 노드 관리 LIF | 메일 서버 | AutoSupport에 사용할 수 있는 SMTP 경고 |
| SNMP를 선택합니다 | TCP | 161 | 노드 관리 LIF | 서버 모니터링 | SNMP 트랩으로 모니터링 |
| | UDP입니다 | 161 | 노드 관리 LIF | 서버 모니터링 | SNMP 트랩으로 모니터링 |
| | TCP | 162 | 노드 관리 LIF | 서버 모니터링 | SNMP 트랩으로 모니터링 |
| | UDP입니다 | 162 | 노드 관리 LIF | 서버 모니터링 | SNMP 트랩으로 모니터링 |
| SnapMirror를 참조하십시오 | TCP | 11104 | 인터클러스터 LIF | ONTAP 인터클러스터 LIF | SnapMirror에 대한 인터클러스터 통신 세션의 관리 |
| | TCP | 11105 | 인터클러스터 LIF | ONTAP 인터클러스터 LIF | SnapMirror 데이터 전송 |
| Syslog를 클릭합니다 | UDP입니다 | 514 | 노드 관리 LIF | Syslog 서버 | Syslog 메시지를 전달합니다 |

외부 보안 그룹의 HA 중재자를 위한 규칙

Cloud Volumes ONTAP HA 중재자를 위해 미리 정의된 외부 보안 그룹에는 다음과 같은 인바운드 및 아웃바운드 규칙이 포함됩니다.

인바운드 규칙

인바운드 규칙의 소스는 0.0.0.0/0입니다.

| 프로토콜 | 포트 | 목적 |
|------------|---------|-----------------------------|
| SSH를 클릭합니다 | 22 | HA 중재자로 SSH 연결 |
| TCP | 3000입니다 | Connector에서 Restful API 액세스 |

아웃바운드 규칙

HA 중재자를 위한 사전 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

기본 아웃바운드 규칙

HA 중재자를 위해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

| 프로토콜 | 포트 | 목적 |
|--------|----|--------------|
| 모든 TCP | 모두 | 모든 아웃바운드 트래픽 |
| 모든 UDP | 모두 | 모든 아웃바운드 트래픽 |

고급 아웃바운드 규칙

아웃바운드 트래픽에 대한 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 HA 중재자의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

| 프로토콜 | 포트 | 목적지 | 목적 |
|--------|-----|--------------|--------------------|
| HTTP | 80 | 커넥터 IP 주소입니다 | 중재자를 위한 업그레이드 다운로드 |
| HTTPS | 443 | AWS API 서비스 | 스토리지 페일오버 지원 |
| UDP입니다 | 53 | AWS API 서비스 | 스토리지 페일오버 지원 |



포트 443과 53을 열지 않고 타겟 서브넷에서 AWS EC2 서비스로 인터페이스 VPC 엔드포인트를 생성할 수 있습니다.

HA 구성 내부 보안 그룹에 대한 규칙입니다

Cloud Volumes ONTAP HA 구성에 대해 미리 정의된 내부 보안 그룹에는 다음 규칙이 포함됩니다. 이 보안 그룹은 HA 노드와 중재자 및 노드 간의 통신을 지원합니다.

Cloud Manager는 항상 이 보안 그룹을 생성합니다. 자신의 을(를) 사용할 수 있는 옵션이 없습니다.

인바운드 규칙

미리 정의된 보안 그룹에는 다음과 같은 인바운드 규칙이 포함됩니다.

| 프로토콜 | 포트 | 목적 |
|----------|----|---------------------|
| 모든 교통 정보 | 모두 | HA 중재자 및 HA 노드 간 통신 |

아웃바운드 규칙

미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

| 프로토콜 | 포트 | 목적 |
|----------|----|---------------------|
| 모든 교통 정보 | 모두 | HA 중재자 및 HA 노드 간 통신 |

커넥터 규칙

Connector의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

인바운드 규칙

| 프로토콜 | 포트 | 목적 |
|-------------------|------|--|
| SSH를 클릭합니 다 | 22 | 커넥터 호스트에 대한 SSH 액세스를 제공합니다 |
| HTTP | 80 | 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공하고 Cloud Data Sense에서 연결을 제공합니다 |
| HTTPS | 443 | 클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTPS 액세스를 제공합니다 |
| TCP | 3128 | AWS 네트워크에서 NAT 또는 프록시를 사용하지 않는 경우 인터넷 액세스가 가능한 클라우드 데이터 감지 인스턴스를 제공합니다 |

아웃바운드 규칙

Connector에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

기본 아웃바운드 규칙

Connector에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

| 프로토콜 | 포트 | 목적 |
|--------|----|--------------|
| 모든 TCP | 모두 | 모든 아웃바운드 트래픽 |
| 모든 UDP | 모두 | 모든 아웃바운드 트래픽 |

고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Connector의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.



소스 IP 주소는 커넥터 호스트입니다.

| 서비스 | 프로토콜 | 포트 | 목적지 | 목적 |
|----------------------|--------|---------|-------------------------------|--|
| API 호출 및 AutoSupport | HTTPS | 443 | 아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF | API는 AWS 및 ONTAP, 클라우드 데이터 감지, 랜섬웨어 서비스 요청, AutoSupport 메시지를 NetApp에 전송합니다 |
| API 호출 | TCP | 3000입니다 | ONTAP HA 중재자 | ONTAP HA 중재인과의 커뮤니케이션 |
| | TCP | 8088 | S3로 백업 | API에서 S3로 백업을 호출합니다 |
| DNS | UDP입니다 | 53 | DNS | Cloud Manager에서 DNS Resolve에 사용됩니다 |
| 클라우드 데이터 감지 | HTTP | 80 | 클라우드 데이터 감지 인스턴스 | Cloud Volumes ONTAP에 대한 클라우드 데이터 감지 |

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.