네트워킹을 설정하세요

Cloud Volumes ONTAP

NetApp
November 25, 2025

목차

네트워킹을 설정하세요

Cloud Volumes ONTAP 에 대한 AWS 네트워킹 설정

NetApp Console IP 주소, 넷마스크, 경로 등 Cloud Volumes ONTAP 의 네트워킹 구성 요소를 설정합니다. 아웃바운드 인터넷 접속이 가능한지, 충분한 개인 IP 주소가 사용 가능한지, 올바른 연결이 설정되어 있는지 등을 확인해야 합니다.

일반 요구 사항

AWS에서 다음 요구 사항을 충족했는지 확인하세요.

Cloud Volumes ONTAP 노드에 대한 아웃바운드 인터넷 액세스

Cloud Volumes ONTAP 시스템은 다양한 기능을 위해 외부 엔드포인트에 액세스하기 위해 아웃바운드 인터넷 액세스가 필요합니다. 엄격한 보안 요구 사항이 있는 환경에서 이러한 엔드포인트가 차단되면 Cloud Volumes ONTAP 제대로 작동할 수 없습니다.

콘솔 에이전트는 일상 업무를 위해 여러 엔드포인트에 연결합니다. 사용된 엔드포인트에 대한 정보는 다음을 참조하세요. "콘솔 에이전트에서 연결된 엔드포인트 보기" 그리고 "콘솔 사용을 위한 네트워킹 준비" .

Cloud Volumes ONTAP 엔드포인트

Cloud Volumes ONTAP 이러한 엔드포인트를 사용하여 다양한 서비스와 통신합니다.

엔드포인트	적용 가능	목적	배포 모드	엔드포인트를 사용할 수 없는 경우의 영향
\ https://netapp-cloud-account.auth0.com	입증	콘솔에서 인증에 사용됩니다.	표준 모드와 제한 모드.	사용자 인증에 실패하고 다음 서비스를 계속 사용할 수 없습니다. • Cloud Volumes ONTAP 서비스 • ONTAP 서비스 • 프로토콜 및 프록시 서비스
\ https://api.bluexp.netapp.com/tenancy	차용	콘솔에서 Cloud Volumes ONTAP 리소스를 검색하여 리소스와 사용자에게 권한을 부여하는 데 사용됩니다.	표준 모드와 제한 모드.	Cloud Volumes ONTAP 리소스와 사용자는 권한이 없습니다.

엔드포인트	적용 가능	목적	배포 모드	엔드포인트를 사용할 수 없는 경우의 영향
\ https://mysupport.netapp.com/aods/asupmessage \ https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	AutoSupport 원격 측정 데이터를 NetApp 지원팀으로 전송하는 데 사용됩니다.	표준 모드와 제한 모드.	AutoSupport 정보가 전달되지 않았습니다.
AWS 서비스의 정확한 상업적 종점(접미사 포함) `amazonaws.com`)는 사용하는 AWS 지역에 따라 다릅니다. 를 참조하세요 "자세한 내용은 AWS 설명서를 참조하세요." .	• 클라우드포메이션 • 탄력적 컴퓨팅 클라우드(EC2) • ID 및 액세스 관리(IAM) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • 간편 보관 서비스(S3)	AWS 서비스와의 통신.	표준 모드와 개인 모드.	Cloud Volumes ONTAP AWS 서비스와 통신하여 AWS에서 특정 작업을 수행할 수 없습니다.
AWS 서비스에 대한 정확한 정부 엔드포인트는 사용 중인 AWS 지역에 따라 달라집니다. 끝점에는 접미사가 붙습니다. `amazonaws.com` 그리고 `c2s.ic.gov` . 참조하다 "AWS SDK" 그리고 "AWS 문서" 자세한 내용은.	• 클라우드포메이션 • 탄력적 컴퓨팅 클라우드(EC2) • ID 및 액세스 관리(IAM) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • 간편 보관 서비스(S3)	AWS 서비스와의 통신.	제한 모드.	Cloud Volumes ONTAP AWS 서비스와 통신하여 AWS에서 특정 작업을 수행할 수 없습니다.

HA 중재자를 위한 아웃바운드 인터넷 액세스

HA 중재자 인스턴스는 스토리지 장애 조치를 지원할 수 있도록 AWS EC2 서비스에 대한 아웃바운드 연결이 있어야 합니다. 연결을 제공하려면 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 엔드포인트가 될 수 있습니다. VPC 엔드포인트에 대한 자세한 내용은 다음을 참조하세요. "AWS 설명서: VPC 엔드포인트 인터페이스(AWS PrivateLink)" .

NetApp Console 에이전트의 네트워크 프록시 구성

NetApp Console 에이전트의 프록시 서버 구성을 사용하여 Cloud Volumes ONTAP 에서 아웃바운드 인터넷 액세스를 활성화할 수 있습니다. 콘솔은 두 가지 유형의 프록시를 지원합니다.

- 명시적 프록시: Cloud Volumes ONTAP 의 아웃바운드 트래픽은 콘솔 에이전트의 프록시 구성 중에 지정된 프록시 서버의 HTTP 주소를 사용합니다. 관리자는 추가 인증을 위해 사용자 자격 증명과 루트 CA 인증서를 구성했을 수도 있습니다. 명시적 프록시에 대해 루트 CA 인증서를 사용할 수 있는 경우 다음을 사용하여 동일한 인증서를 Cloud Volumes ONTAP 시스템에 가져와 업로드해야 합니다. "ONTAP CLI: 보안 인증서 설치" 명령.
- 투명 프록시: 네트워크는 콘솔 에이전트의 프록시를 통해 Cloud Volumes ONTAP 에서 아웃바운드 트래픽을 자동으로 라우팅하도록 구성됩니다. 투명 프록시를 설정할 때 관리자는 프록시 서버의 HTTP 주소가 아닌 Cloud Volumes ONTAP 에서의 연결을 위한 루트 CA 인증서만 제공하면 됩니다. 다음을 사용하여 Cloud Volumes ONTAP 시스템에 동일한 루트 CA 인증서를 가져와 업로드해야 합니다. "ONTAP CLI: 보안 인증서 설치" 명령.

프록시 서버 구성에 대한 정보는 다음을 참조하세요. "프록시 서버를 사용하도록 콘솔 에이전트 구성" .

개인 IP 주소

콘솔은 필요한 수의 개인 IP 주소를 Cloud Volumes ONTAP 에 자동으로 할당합니다. 네트워크에 사용 가능한 개인 IP 주소가 충분한지 확인해야 합니다.

콘솔이 Cloud Volumes ONTAP 에 할당하는 LIF 수는 단일 노드 시스템을 배포하는지 아니면 HA 쌍을 배포하는지에 따라 달라집니다. LIF는 물리적 포트와 연결된 IP 주소입니다.

단일 노드 시스템의 IP 주소

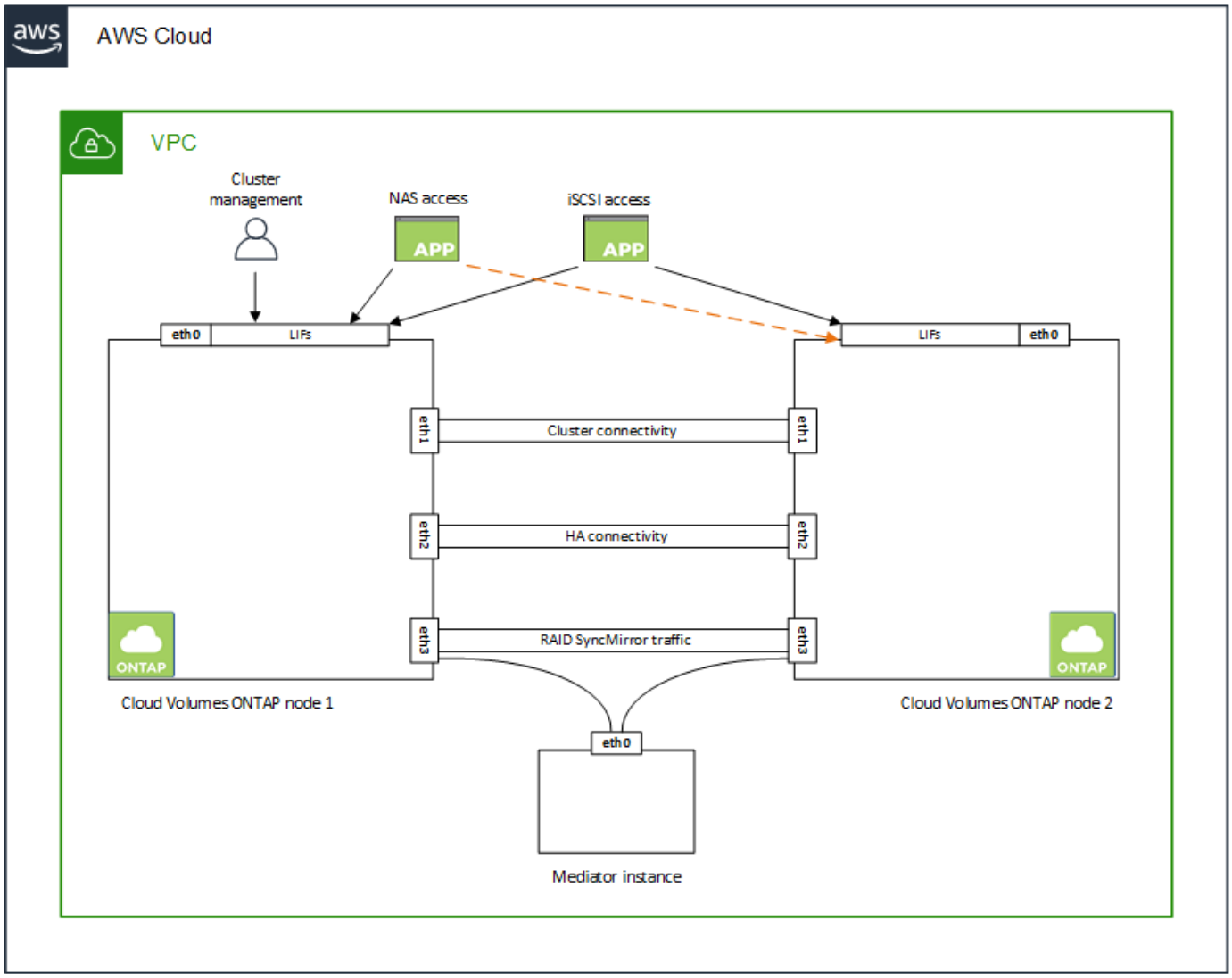
콘솔은 단일 노드 시스템에 6개의 IP 주소를 할당합니다.

다음 표는 각 개인 IP 주소와 연결된 LIF에 대한 세부 정보를 제공합니다.

라이프	목적
클러스터 관리	전체 클러스터(HA 쌍)의 관리.
노드 관리	노드의 관리.
클러스터 간	클러스터 간 통신, 백업 및 복제.
NAS 데이터	NAS 프로토콜을 통한 클라이언트 접근.
iSCSI 데이터	iSCSI 프로토콜을 통한 클라이언트 액세스. 또한 시스템에서 다른 중요한 네트워킹 워크플로우에도 사용됩니다. 이 LIF는 필수이므로 삭제하면 안 됩니다.
스토리지 VM 관리	스토리지 VM 관리 LIF는 SnapCenter 와 같은 관리 도구와 함께 사용됩니다.

HA 쌍의 IP 주소

HA 쌍에는 단일 노드 시스템보다 더 많은 IP 주소가 필요합니다. 이러한 IP 주소는 다음 이미지에서 볼 수 있듯이 다양한 이더넷 인터페이스에 분산되어 있습니다.



HA 쌍에 필요한 개인 IP 주소 수는 선택한 배포 모델에 따라 달라집니다. 단일 AWS 가용성 영역(AZ)에 배포된 HA 쌍에는 15개의 개인 IP 주소가 필요하고, 여러 AZ에 배포된 HA 쌍에는 13개의 개인 IP 주소가 필요합니다.

다음 표에서는 각 개인 IP 주소와 연결된 LIF에 대한 세부 정보를 제공합니다.

라이프	인터페이스	마디	목적
클러스터 관리	eth0	노드 1	전체 클러스터(HA 쌍)의 관리.
노드 관리	eth0	노드 1과 노드 2	노드의 관리.
클러스터 간	eth0	노드 1과 노드 2	클러스터 간 통신, 백업 및 복제.
NAS 데이터	eth0	노드 1	NAS 프로토콜을 통한 클라이언트 접근.
iSCSI 데이터	eth0	노드 1과 노드 2	iSCSI 프로토콜을 통한 클라이언트 액세스. 또한 시스템에서 다른 중요한 네트워킹 워크플로우에도 사용됩니다. 이러한 LIF는 필수이므로 삭제하면 안 됩니다.
클러스터 연결성	eth1	노드 1과 노드 2	클러스터 내에서 노드가 서로 통신하고 데이터를 이동할 수 있도록 합니다.
HA 연결	eth2	노드 1과 노드 2	장애 조치 시 두 노드 간의 통신.

라이프	인터페이스	마디	목적
RSM iSCSI 트래픽	eth3	노드 1과 노드 2	RAID SyncMirror iSCSI 트래픽과 두 Cloud Volumes ONTAP 노드와 중재자 간의 통신입니다.
중재인	eth0	중재인	저장소 인수 및 반환 프로세스를 지원하기 위한 노드와 중재자 간의 통신 채널입니다.

라이프	인터페이스	마디	목적
노드 관리	eth0	노드 1과 노드 2	노드의 관리.
클러스터 간	eth0	노드 1과 노드 2	클러스터 간 통신, 백업 및 복제.
iSCSI 데이터	eth0	노드 1과 노드 2	iSCSI 프로토콜을 통한 클라이언트 액세스. 이러한 LIF는 노드 간의 플로팅 IP 주소 마이그레이션도 관리합니다. 이러한 LIF는 필수이므로 삭제하면 안 됩니다.
클러스터 연결성	eth1	노드 1과 노드 2	클러스터 내에서 노드가 서로 통신하고 데이터를 이동할 수 있도록 합니다.
HA 연결	eth2	노드 1과 노드 2	장애 조치 시 두 노드 간의 통신.
RSM iSCSI 트래픽	eth3	노드 1과 노드 2	RAID SyncMirror iSCSI 트래픽과 두 Cloud Volumes ONTAP 노드와 중재자 간의 통신입니다.
중재인	eth0	중재인	저장소 인수 및 반환 프로세스를 지원하기 위한 노드와 중재자 간의 통신 채널입니다.

여러 가용성 영역에 배포되는 경우 여러 LIF가 연결됩니다."유동 IP 주소" AWS 개인 IP 제한에 포함되지 않습니다.

보안 그룹

콘솔이 보안 그룹을 자동으로 생성하므로 직접 보안 그룹을 만들 필요가 없습니다. 자신의 것을 사용해야 하는 경우 다음을 참조하세요."보안 그룹 규칙" .

콘솔 에이전트에 대한 정보를 찾고 계신가요? "콘솔 에이전트에 대한 보안 그룹 규칙 보기"

데이터 계층화를 위한 연결

EBS를 성능 계층으로 사용하고 AWS S3를 용량 계층으로 사용하려면 Cloud Volumes ONTAP S3에 연결되어 있는지 확인해야 합니다. 해당 연결을 제공하는 가장 좋은 방법은 S3 서비스에 대한 VPC 엔드포인트를 만드는 것입니다. 지침은 다음을 참조하세요. "AWS 설명서: 게이트웨이 엔드포인트 생성" .

VPC 엔드포인트를 생성할 때 Cloud Volumes ONTAP 인스턴스에 해당하는 지역, VPC 및 경로 테이블을 선택해야 합니다. 또한 S3 엔드포인트로의 트래픽을 활성화하는 아웃바운드 HTTPS 규칙을 추가하려면 보안 그룹을 수정해야 합니다. 그렇지 않으면 Cloud Volumes ONTAP 이 S3 서비스에 연결할 수 없습니다.

문제가 발생하면 다음을 참조하세요. "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 다른 네트워크(예: 회사 네트워크) 간에 VPN 연결이 필요합니다. 지침은 다음을 참조하세요. "AWS 설명서: AWS VPN 연결 설정" .

CIFS용 **DNS** 및 **Active Directory**

CIFS 스토리지를 프로비저닝하려면 AWS에서 DNS와 Active Directory를 설정하거나 온프레미스 설정을 AWS로 확장해야 합니다.

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

지침은 다음을 참조하세요. "AWS 설명서: AWS 클라우드의 Active Directory 도메인 서비스: 빠른 시작 참조 배포" .

VPC 공유

9.11.1 릴리스부터 VPC 공유를 통해 AWS에서 Cloud Volumes ONTAP HA 쌍이 지원됩니다. VPC 공유를 사용하면 조직에서 다른 AWS 계정과 서브넷을 공유할 수 있습니다. 이 구성을 사용하려면 AWS 환경을 설정한 다음 API를 사용하여 HA 쌍을 배포해야 합니다.

"공유 서브넷에 HA 쌍을 배포하는 방법을 알아보세요." .

여러 **AZ**의 **HA** 쌍에 대한 요구 사항

여러 가용성 영역(AZ)을 사용하는 Cloud Volumes ONTAP HA 구성에는 추가 AWS 네트워킹 요구 사항이 적용됩니다. Cloud Volumes ONTAP 시스템을 추가할 때 콘솔에 네트워킹 세부 정보를 입력해야 하므로 HA 쌍을 시작하기 전에 이러한 요구 사항을 검토해야 합니다.

HA 쌍이 어떻게 작동하는지 이해하려면 다음을 참조하세요."고가용성 쌍" .

가용성 영역

이 HA 배포 모델은 여러 AZ를 사용하여 데이터의 높은 가용성을 보장합니다. HA 쌍 간의 통신 채널을 제공하는 각 Cloud Volumes ONTAP 인스턴스와 중재자 인스턴스에 대해 전용 AZ를 사용해야 합니다.

각 가용성 영역에서 서브넷을 사용할 수 있어야 합니다.

NAS 데이터 및 클러스터**/SVM** 관리를 위한 유동 **IP** 주소

여러 AZ의 HA 구성은 장애가 발생할 경우 노드 간에 마이그레이션되는 부동 IP 주소를 사용합니다. VPC 외부에서는 기본적으로 액세스할 수 없습니다."AWS 전송 게이트웨이 설정" .

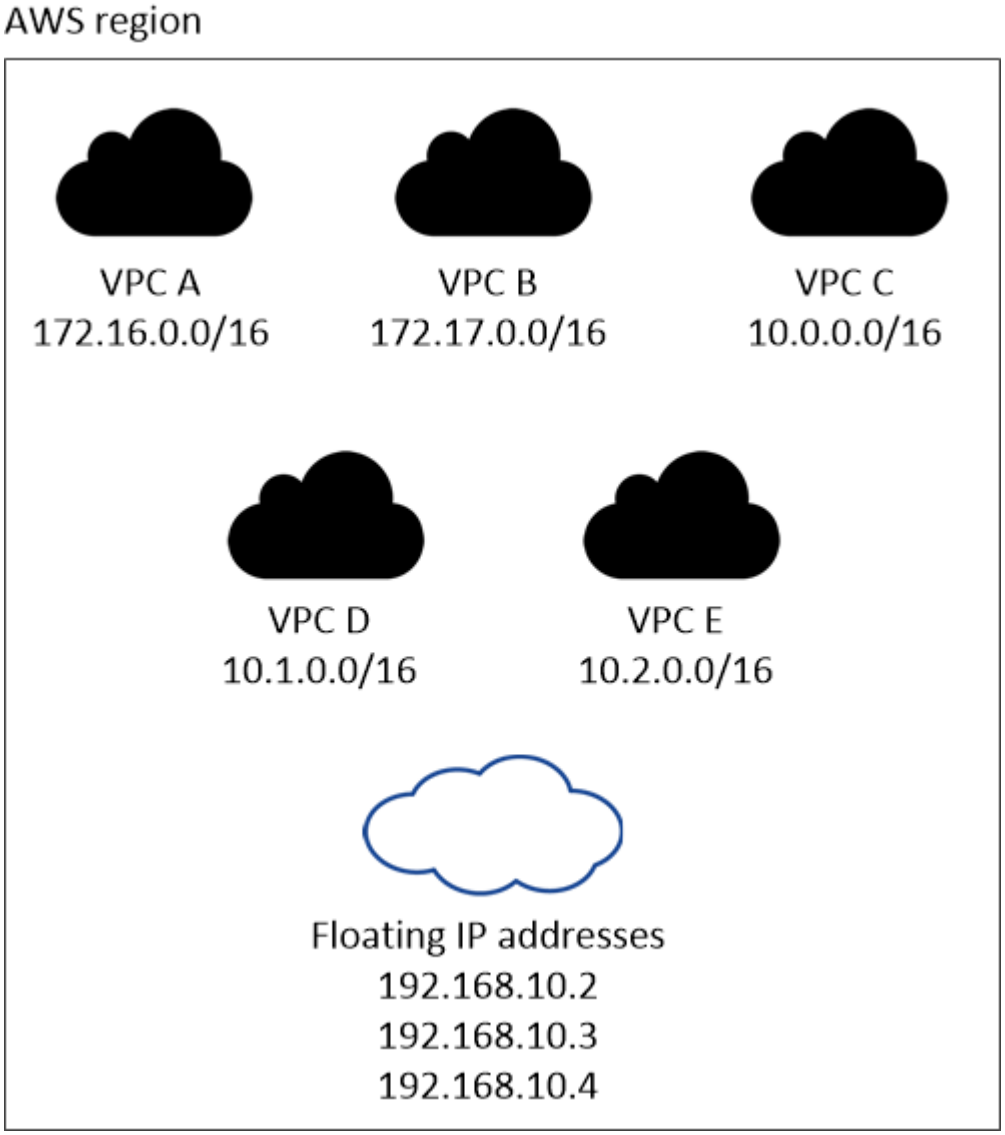
하나의 부동 IP 주소는 클러스터 관리용이고, 하나는 노드 1의 NFS/CIFS 데이터용이고, 다른 하나는 노드 2의 NFS/CIFS 데이터용입니다. SVM 관리를 위한 네 번째 유동 IP 주소는 선택 사항입니다.

HA 쌍과 함께 Windows용 SnapDrive 또는 SnapCenter 사용하는 경우 SVM 관리 LIF에 부동 IP 주소가 필요합니다.

Cloud Volumes ONTAP HA 시스템을 추가하는 경우 유동 IP 주소를 입력해야 합니다. 콘솔은 시스템을 시작할 때 HA 쌍에 IP 주소를 할당합니다.

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

다음 예에서는 AWS 지역의 VPC와 플로팅 IP 주소 간의 관계를 보여줍니다. 플로팅 IP 주소는 모든 VPC의 CIDR 블록 외부에 있지만, 경로 테이블을 통해 서브넷으로 라우팅할 수 있습니다.



콘솔은 VPC 외부의 클라이언트에서 iSCSI 액세스와 NAS 액세스를 위해 정적 IP 주소를 자동으로 생성합니다. 이러한 유형의 IP 주소에 대해서는 어떠한 요구 사항도 충족할 필요가 없습니다.

VPC 외부에서 플로팅 **IP** 액세스를 가능하게 하는 트랜짓 게이트웨이

필요한 경우,"AWS 전송 게이트웨이 설정" HA 쌍이 있는 VPC 외부에서 HA 쌍의 부동 IP 주소에 액세스할 수 있도록 합니다.

경로 테이블

유동 IP 주소를 지정한 후에는 유동 IP 주소에 대한 경로를 포함할 경로 테이블을 선택하라는 메시지가 표시됩니다. 이를 통해 클라이언트가 HA 쌍에 액세스할 수 있습니다.

VPC의 서브넷에 대한 경로 테이블이 하나뿐인 경우(기본 경로 테이블), 콘솔은 자동으로 해당 경로 테이블에 플로팅 IP 주소를 추가합니다. 두 개 이상의 경로 테이블이 있는 경우 HA 쌍을 시작할 때 올바른 경로 테이블을 선택하는

것이 매우 중요합니다. 그렇지 않으면 일부 클라이언트가 Cloud Volumes ONTAP 에 액세스하지 못할 수도 있습니다.

예를 들어, 서로 다른 경로 테이블과 연결된 두 개의 서브넷이 있을 수 있습니다. 경로 테이블 A를 선택했지만 경로 테이블 B는 선택하지 않은 경우, 경로 테이블 A에 연결된 서브넷의 클라이언트는 HA 쌍에 액세스할 수 있지만 경로 테이블 B에 연결된 서브넷의 클라이언트는 액세스할 수 없습니다.

경로 테이블에 대한 자세한 내용은 다음을 참조하세요. "AWS 문서: 라우팅 테이블" .

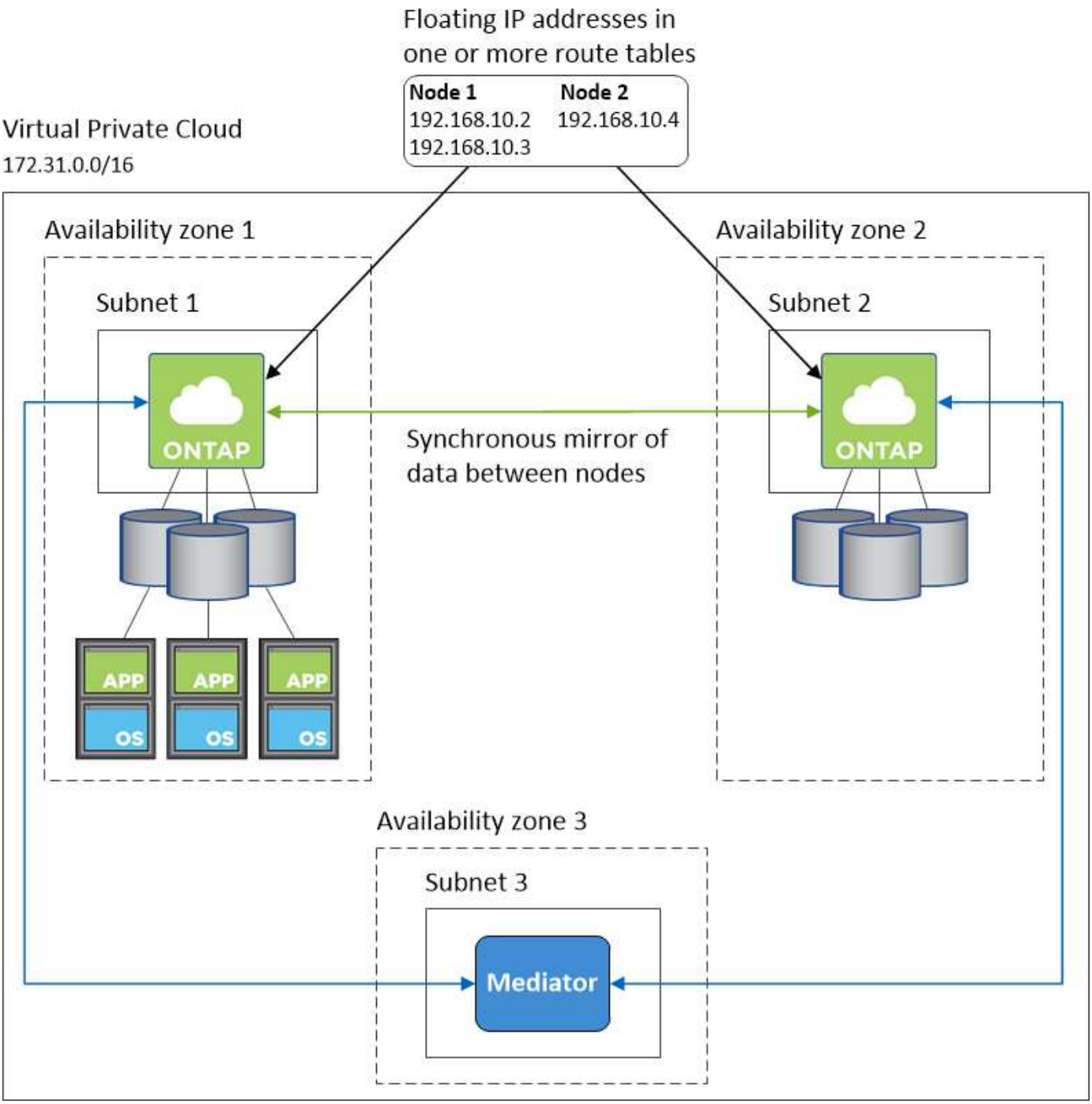
NetApp 관리 도구에 연결

여러 AZ에 있는 HA 구성에서 NetApp 관리 도구를 사용하려면 두 가지 연결 옵션이 있습니다.

1. 다른 VPC에 NetApp 관리 도구를 배포합니다."AWS 전송 게이트웨이 설정" . 게이트웨이를 사용하면 VPC 외부에서 클러스터 관리 인터페이스의 플로팅 IP 주소에 액세스할 수 있습니다.
2. NAS 클라이언트와 유사한 라우팅 구성을 사용하여 동일한 VPC에 NetApp 관리 도구를 배포합니다.

HA 구성 예시

다음 이미지는 여러 AZ의 HA 쌍에 특정한 네트워킹 구성 요소를 보여줍니다. 즉, 3개의 가용성 영역, 3개의 서브넷, 부동 IP 주소 및 경로 테이블입니다.



콘솔 에이전트에 대한 요구 사항

아직 콘솔 에이전트를 만들지 않았다면 네트워킹 요구 사항을 검토해야 합니다.

- "콘솔 에이전트에 대한 네트워킹 요구 사항 보기"
- "AWS의 보안 그룹 규칙"

관련 주제

- "Cloud Volumes ONTAP 에 대한 AutoSupport 설정 확인"
- "ONTAP 내부 포트에 대해 알아보세요" .

Cloud Volumes ONTAP HA 쌍에 대한 AWS 전송 게이트웨이 설정

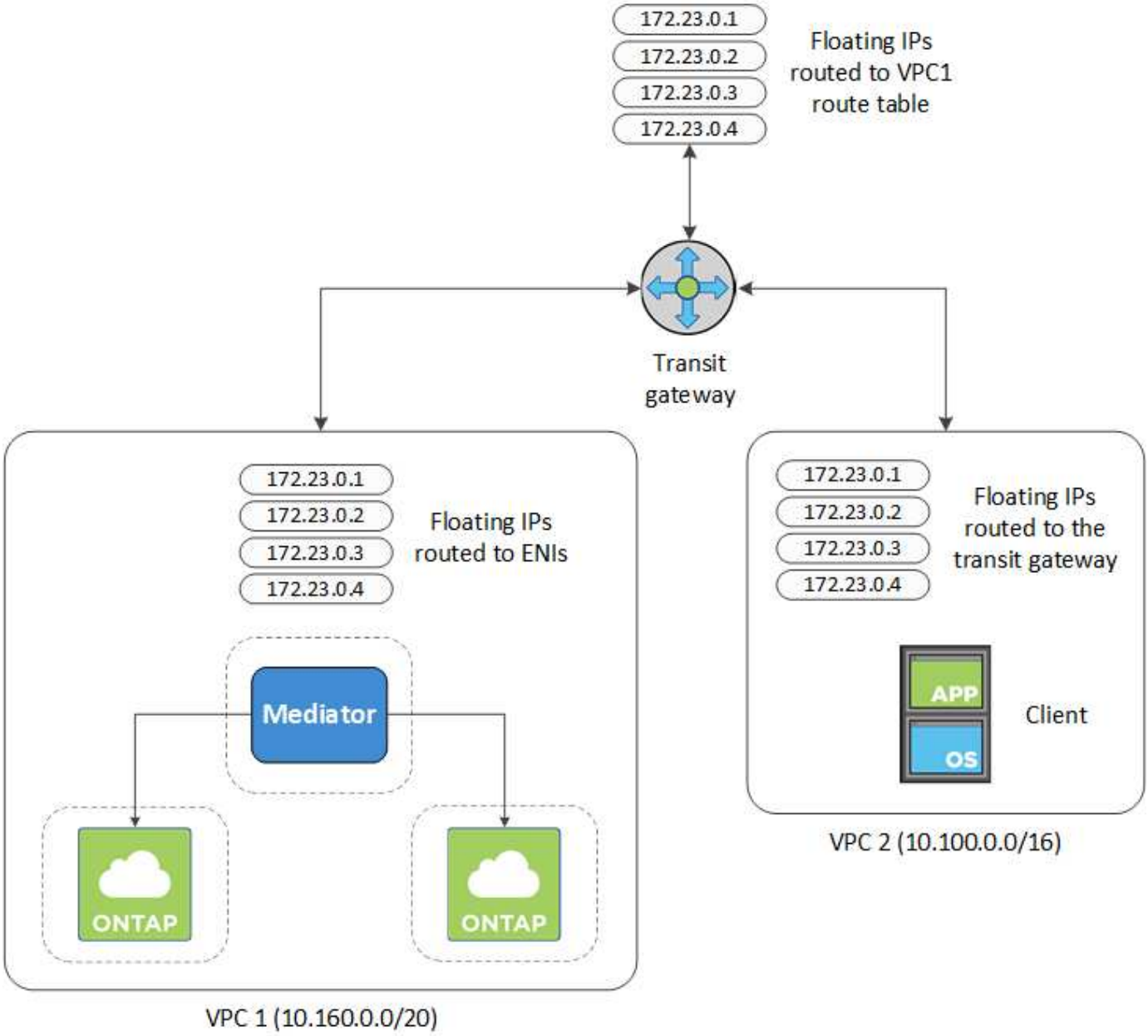
HA 쌍에 대한 액세스를 활성화하기 위해 AWS 전송 게이트웨이를 설정합니다."유동 IP 주소" HA 쌍이 있는 VPC 외부에서.

Cloud Volumes ONTAP HA 구성이 여러 AWS 가용성 영역에 걸쳐 분산된 경우 VPC 내에서 NAS 데이터에 액세스하려면 플로팅 IP 주소가 필요합니다. 이러한 유동 IP 주소는 장애 발생 시 노드 간에 마이그레이션될 수 있지만 기본적으로 VPC 외부에서 액세스할 수는 없습니다. 별도의 개인 IP 주소는 VPC 외부에서 데이터에 액세스할 수 있도록 하지만 자동 장애 조치는 제공하지 않습니다.

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

AWS 전송 게이트웨이를 설정하면 HA 쌍이 있는 VPC 외부에서 플로팅 IP 주소에 액세스할 수 있습니다. 즉, VPC 외부의 NAS 클라이언트와 NetApp 관리 도구가 플로팅 IP에 액세스할 수 있습니다.

다음은 두 개의 VPC가 트랜짓 게이트웨이로 연결된 것을 보여주는 예입니다. HA 시스템은 한 VPC에 있고, 클라이언트는 다른 VPC에 있습니다. 그런 다음 부동 IP 주소를 사용하여 클라이언트에 NAS 볼륨을 마운트할 수 있습니다.

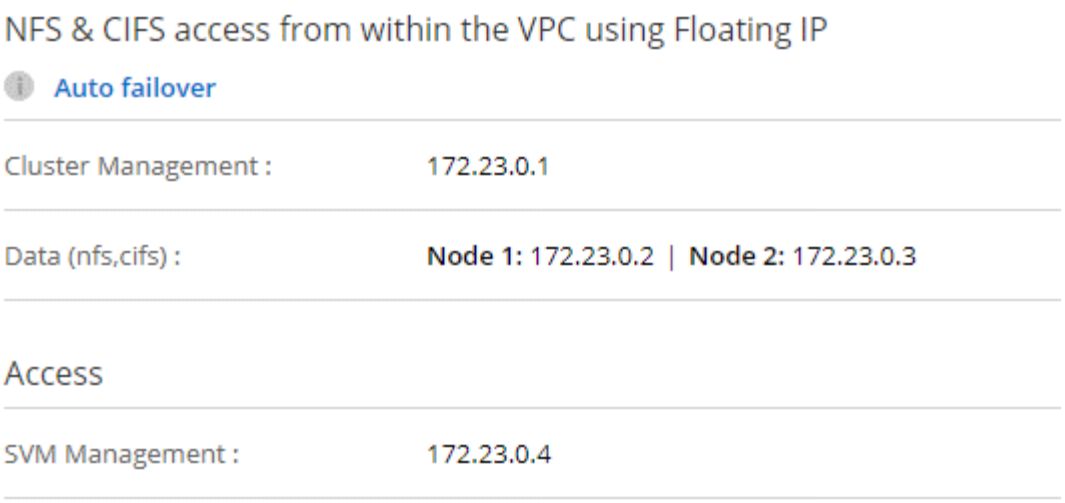


다음 단계에서는 비슷한 구성을 설정하는 방법을 보여줍니다.

단계

1. "트랜짓 게이트웨이를 생성하고 VPC를 게이트웨이에 연결합니다." .
2. VPC를 전송 게이트웨이 경로 테이블과 연결합니다.
   a. **VPC** 서비스에서 *전송 게이트웨이 경로 테이블*을 클릭합니다.
   b. 경로 테이블을 선택하세요.
   c. *협회*를 클릭한 다음 *협회 만들기*를 선택합니다.
   d. 연결할 첨부 파일(VPC)을 선택한 다음 *연결 만들기*를 클릭합니다.
3. HA 쌍의 플로팅 IP 주소를 지정하여 트랜짓 게이트웨이의 경로 테이블에 경로를 생성합니다.

   NetApp Console 의 시스템 정보 페이지에서 부동 IP 주소를 찾을 수 있습니다. 예를 들면 다음과 같습니다.



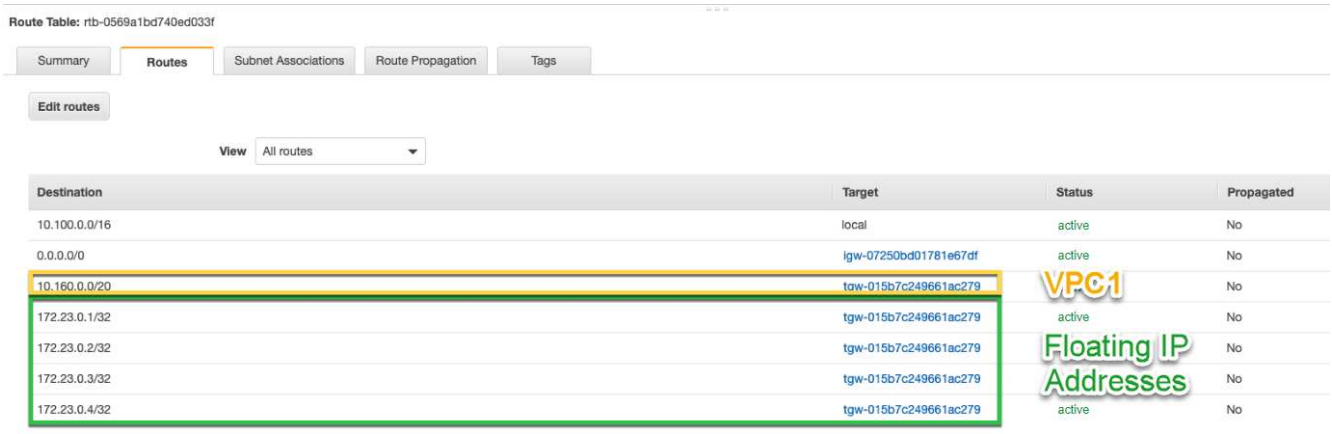
다음 샘플 이미지는 트랜짓 게이트웨이의 경로 테이블을 보여줍니다. 여기에는 Cloud Volumes ONTAP 에서 사용하는 두 개의 VPC의 CIDR 블록에 대한 경로와 4개의 플로팅 IP 주소가 포함됩니다.

4. 플로팅 IP 주소에 액세스해야 하는 VPC의 경로 테이블을 수정합니다.

   a. 플로팅 IP 주소에 경로 항목을 추가합니다.

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

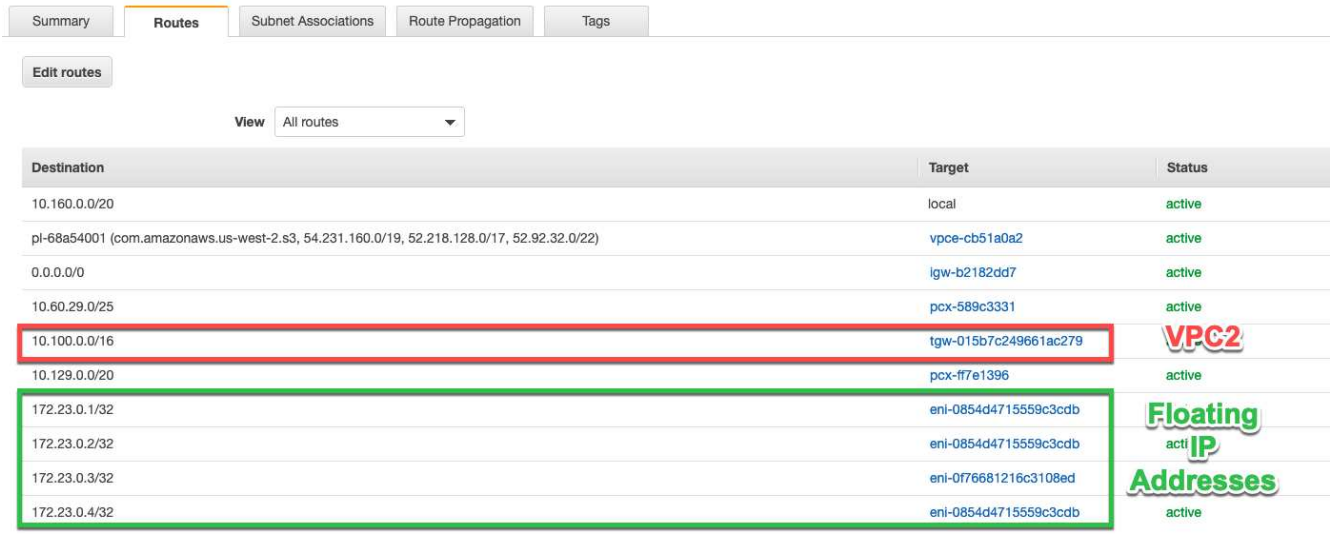
      다음 샘플 이미지는 VPC 1에 대한 경로와 플로팅 IP 주소를 포함하는 VPC 2의 경로 테이블을 보여줍니다.



5. 부동 IP 주소에 액세스해야 하는 VPC에 경로를 추가하여 HA 쌍의 VPC에 대한 경로 테이블을 수정합니다.

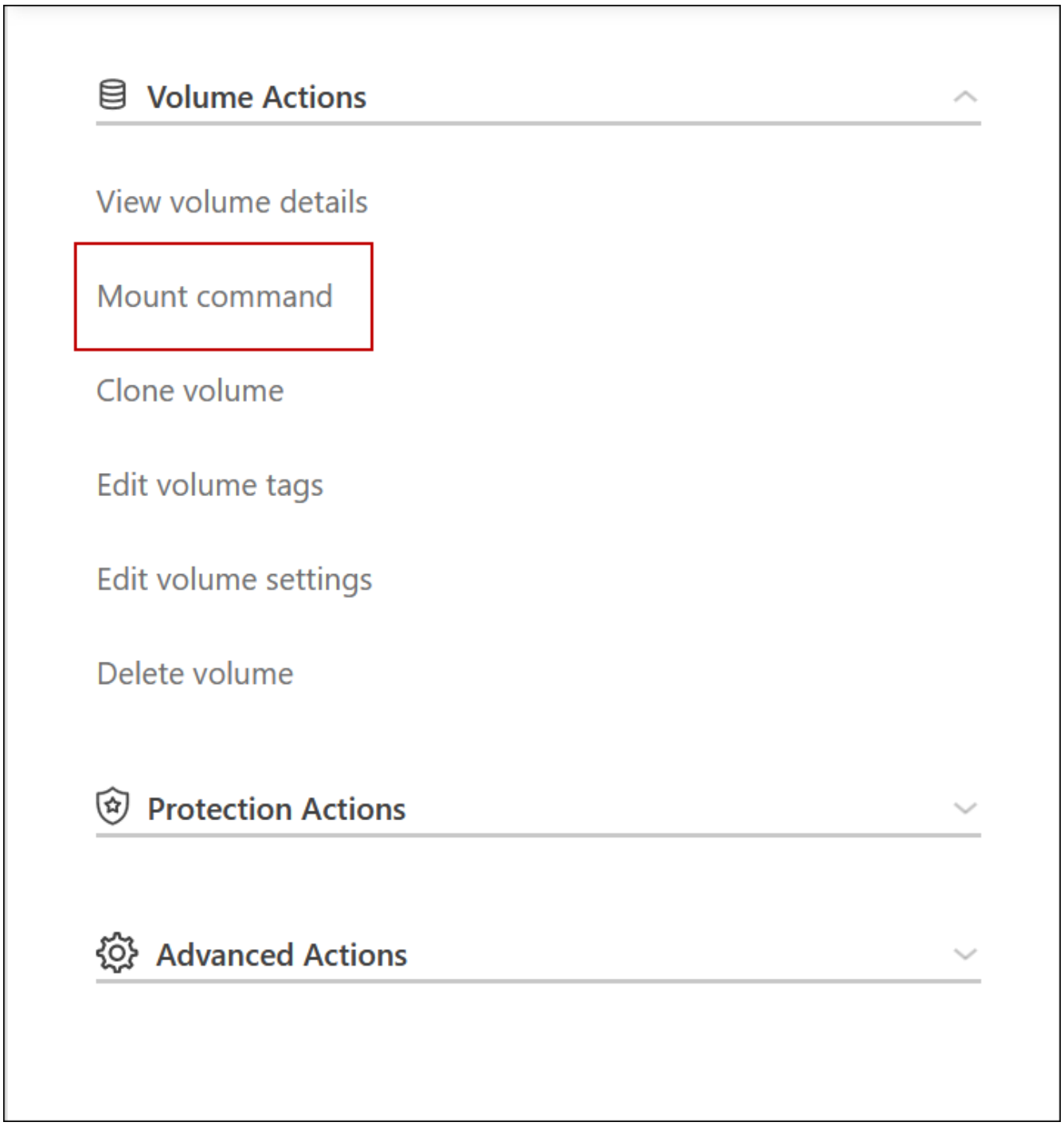
   이 단계는 VPC 간 라우팅을 완료하기 때문에 중요합니다.

   다음 샘플 이미지는 VPC 1의 경로 테이블을 보여줍니다. 여기에는 부동 IP 주소와 클라이언트가 있는 VPC 2에 대한 경로가 포함됩니다. 콘솔은 HA 쌍을 배포할 때 자동으로 플로팅 IP를 경로 테이블에 추가했습니다.



6. VPC에 대한 모든 트래픽에 대한 보안 그룹 설정을 업데이트합니다.
   a. 가상 사설 클라우드에서 *서브넷*을 클릭합니다.
   b. 경로 테이블 탭을 클릭하고 HA 쌍의 부동 IP 주소 중 하나에 대한 원하는 환경을 선택합니다.
   c. *보안 그룹*을 클릭하세요.
   d. *인바운드 규칙 편집*을 선택합니다.
   e. *규칙 추가*를 클릭합니다.
   f. 유형에서 *모든 트래픽*을 선택한 다음 VPC IP 주소를 선택합니다.
   g. 변경 사항을 적용하려면 *규칙 저장*을 클릭하세요.
7. 플로팅 IP 주소를 사용하여 클라이언트에 볼륨을 마운트합니다.

   콘솔의 볼륨 관리 패널에서 마운트 명령 옵션을 통해 콘솔에서 올바른 IP 주소를 찾을 수 있습니다.



8. NFS 볼륨을 마운트하는 경우 클라이언트 VPC의 서브넷과 일치하도록 내보내기 정책을 구성합니다.

   "볼륨을 편집하는 방법을 알아보세요" .

관련 링크

- "AWS의 고가용성 쌍"
- "AWS의 Cloud Volumes ONTAP 에 대한 네트워킹 요구 사항"

AWS 공유 서브넷에 Cloud Volumes ONTAP HA 쌍 배포

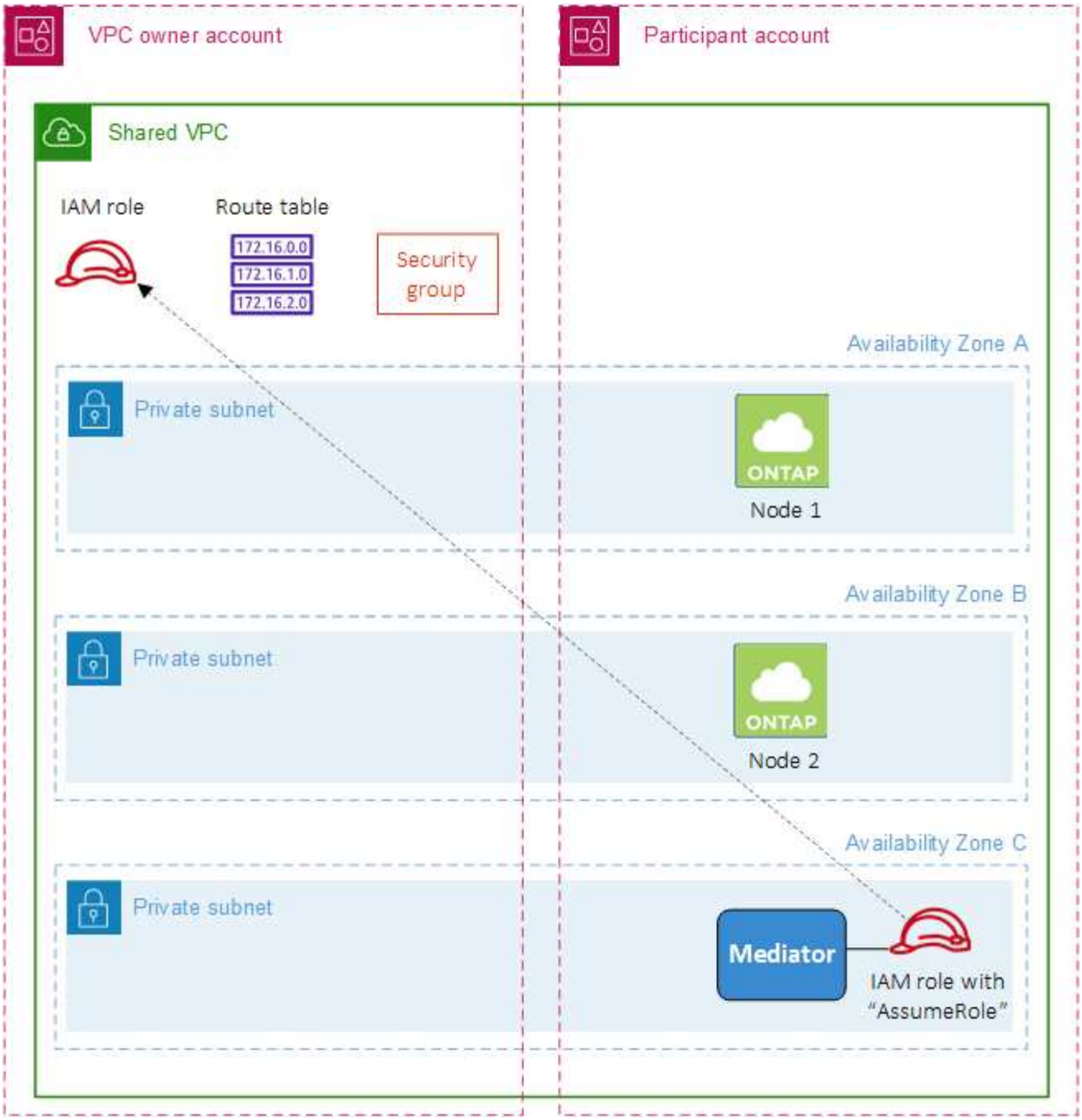
9.11.1 릴리스부터 VPC 공유를 통해 AWS에서 Cloud Volumes ONTAP HA 쌍이 지원됩니다. VPC 공유를 사용하면 조직에서 다른 AWS 계정과 서브넷을 공유할 수 있습니다. 이 구성을 사용하려면 AWS 환경을 설정한 다음 API를 사용하여 HA 쌍을 배포해야 합니다.

와 함께 "VPC 공유" Cloud Volumes ONTAP HA 구성은 두 계정에 분산됩니다.

- 네트워킹(VPC, 서브넷, 경로 테이블 및 Cloud Volumes ONTAP 보안 그룹)을 소유한 VPC 소유자 계정
- EC2 인스턴스가 공유 서브넷에 배포되는 참여자 계정(여기에는 두 개의 HA 노드와 중재자가 포함됨)

여러 가용성 영역에 배포된 Cloud Volumes ONTAP HA 구성의 경우, HA 중재자에게 VPC 소유자 계정의 경로 테이블에 쓰기 위한 특정 권한이 필요합니다. 중재자가 맡을 수 있는 IAM 역할을 설정하여 해당 권한을 제공해야 합니다.

다음 이미지는 이 배포에 포함된 구성 요소를 보여줍니다.



아래 단계에 설명된 대로 참여자 계정과 서브넷을 공유한 다음 VPC 소유자 계정에서 IAM 역할과 보안 그룹을 만들어야 합니다.

Cloud Volumes ONTAP 시스템을 생성하면 NetApp Console 자동으로 IAM 역할을 생성하여 중재자에 연결합니다. 이 역할은 HA 쌍과 관련된 경로 테이블을 변경하기 위해 VPC 소유자 계정에서 생성한 IAM 역할을 수행합니다.

단계

1. VPC 소유자 계정의 서브넷을 참여자 계정과 공유합니다.

   이 단계는 공유 서브넷에 HA 쌍을 배포하는 데 필요합니다.

   "AWS 설명서: 서브넷 공유"

2. VPC 소유자 계정에서 Cloud Volumes ONTAP 에 대한 보안 그룹을 만듭니다.

   "Cloud Volumes ONTAP 에 대한 보안 그룹 규칙을 참조하세요." . HA 중재자에 대한 보안 그룹을 만들 필요는 없습니다. 콘솔이 그 일을 대신해 줍니다.

3. VPC 소유자 계정에서 다음 권한이 포함된 IAM 역할을 만듭니다.

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. API를 사용하여 새로운 Cloud Volumes ONTAP 시스템을 만듭니다.

   다음 필드를 지정해야 합니다.

   - "보안그룹ID"

     "securityGroupId" 필드는 VPC 소유자 계정에서 생성한 보안 그룹을 지정해야 합니다(위의 2단계 참조).

   - "haParams" 객체의 "assumeRoleArn"

     "assumeRoleArn" 필드에는 VPC 소유자 계정에서 생성한 IAM 역할의 ARN이 포함되어야 합니다(위의 3단계 참조).

     예를 들어:

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

   +
   "Cloud Volumes ONTAP API에 대해 알아보세요"

AWS 단일 AZ에서 Cloud Volumes ONTAP HA 쌍에 대한 배치 그룹 생성 구성

AWS 단일 가용성 영역(AZ)에 있는 Cloud Volumes ONTAP 고가용성(HA) 배포는 배치 그룹 생성에 실패하면 실패하고 롤백될 수 있습니다. Cloud Volumes ONTAP 노드와 중재자

인스턴스를 사용할 수 없는 경우 배치 그룹 생성도 실패하고 배포가 롤백됩니다. 이를 방지하려면 배치 그룹 생성에 실패하더라도 배포가 완료되도록 구성을 수정할 수 있습니다.

롤백 프로세스를 우회하면 Cloud Volumes ONTAP 배포 프로세스가 성공적으로 완료되고 배치 그룹 생성이 완료되지 않았음을 알립니다.

단계

1. SSH를 사용하여 NetApp Console 에이전트 호스트에 연결하고 로그인합니다.
2. 로 이동 `/opt/application/netapp/cloudmanager/docker_occm/data` .
3. 편집하다 `app.conf` 값을 변경하여 `rollback-on-placement-group-failure` 매개변수 `false` . 이 매개변수의 기본값은 다음과 같습니다. `true` .

```
{
    "occm" : {
        "aws" : {
            "rollback-on-placement-group-failure" : false
        }
    }
}
```

4. 파일을 저장하고 콘솔 에이전트에서 로그오프합니다. 콘솔 에이전트를 다시 시작할 필요가 없습니다.

Cloud Volumes ONTAP 에 대한 AWS 보안 그룹 인바운드 및 아웃바운드 규칙

NetApp Console Cloud Volumes ONTAP 성공적으로 작동하는 데 필요한 인바운드 및 아웃바운드 규칙을 포함하는 AWS 보안 그룹을 생성합니다. 테스트 목적으로 포트를 참조하거나 자체 보안 그룹을 사용하려는 경우 포트를 참조할 수 있습니다.

Cloud Volumes ONTAP 규칙

Cloud Volumes ONTAP 의 보안 그룹에는 인바운드 규칙과 아웃바운드 규칙이 모두 필요합니다.

인바운드 규칙

Cloud Volumes ONTAP 시스템을 추가하고 미리 정의된 보안 그룹을 선택하면 다음 중 하나 내에서 트래픽을 허용하도록 선택할 수 있습니다.

- 선택된 **VPC**만 해당: 인바운드 트래픽의 소스는 Cloud Volumes ONTAP 시스템의 VPC 서브넷 범위와 콘솔 에이전트가 있는 VPC의 서브넷 범위입니다. 이것은 권장되는 옵션입니다.
- 모든 **VPC**: 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.

규약	포트	목적
모든 ICMP	모두	인스턴스에 ping을 보냅니다.
HTTP	80	클러스터 관리 LIF의 IP 주소를 사용하여 ONTAP System Manager 웹 콘솔에 대한 HTTP 액세스
HTTPS	443	클러스터 관리 LIF의 IP 주소를 사용하여 콘솔 에이전트와 ONTAP System Manager 웹 콘솔에 대한 HTTPS 액세스 연결
SSH	22	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 대한 SSH 액세스
TCP	111	NFS에 대한 원격 프로시저 호출
TCP	139	CIFS용 NetBIOS 서비스 세션
TCP	161-162	간단한 네트워크 관리 프로토콜
TCP	445	NetBIOS 프레이밍을 통한 TCP를 통한 Microsoft SMB/CIFS
TCP	635	NFS 마운트
TCP	749	케르베로스
TCP	2049	NFS 서버 데몬
TCP	3260	iSCSI 데이터 LIF를 통한 iSCSI 액세스
TCP	4045	NFS 잠금 데몬
TCP	4046	NFS용 네트워크 상태 모니터
TCP	10000	NDMP를 사용한 백업
TCP	11104	SnapMirror 위한 클러스터 간 통신 세션 관리
TCP	11105	클러스터 간 LIF를 사용한 SnapMirror 데이터 전송
UDP	111	NFS에 대한 원격 프로시저 호출
UDP	161-162	간단한 네트워크 관리 프로토콜
UDP	635	NFS 마운트
UDP	2049	NFS 서버 데몬
UDP	4045	NFS 잠금 데몬
UDP	4046	NFS용 네트워크 상태 모니터
UDP	4049	NFS rquotad 프로토콜

아웃바운드 규칙

Cloud Volumes ONTAP 의 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 개방합니다. 이것이 허용된다면, 기본적인 아웃바운드 규칙을 따르세요. 더욱 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용하세요.

기본 아웃바운드 규칙

Cloud Volumes ONTAP 의 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함되어 있습니다.

규약	포트	목적
모든 ICMP	모두	모든 아웃바운드 트래픽
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 Cloud Volumes ONTAP 의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

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

서비스	규약	포트	원천	목적지	목적
액티브 디렉토리	TCP	88	노드 관리 LIF	Active Directory 포리스트	Kerberos V 인증
	UDP	137	노드 관리 LIF	Active Directory 포리스트	NetBIOS 이름 서비스
	UDP	138	노드 관리 LIF	Active Directory 포리스트	NetBIOS 데이터그램 서비스
	TCP	139	노드 관리 LIF	Active Directory 포리스트	NetBIOS 서비스 세션
	TCP 및 UDP	389	노드 관리 LIF	Active Directory 포리스트	LDAP
	TCP	445	노드 관리 LIF	Active Directory 포리스트	NetBIOS 프레이밍을 통한 TCP를 통한 Microsoft SMB/CIFS
	TCP	464	노드 관리 LIF	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(SET_CHANGE)
	UDP	464	노드 관리 LIF	Active Directory 포리스트	Kerberos 키 관리
	TCP	749	노드 관리 LIF	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(RPCSEC_GSS)
	TCP	88	데이터 LIF(NFS, CIFS, iSCSI)	Active Directory 포리스트	Kerberos V 인증
	UDP	137	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 이름 서비스
	UDP	138	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 데이터그램 서비스
	TCP	139	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 서비스 세션
	TCP 및 UDP	389	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	LDAP
	TCP	445	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	NetBIOS 프레이밍을 통한 TCP를 통한 Microsoft SMB/CIFS
	TCP	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(SET_CHANGE)
	UDP	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	Kerberos 키 관리
	TCP	749	데이터 LIF(NFS, CIFS)	Active Directory 포리스트	Kerberos V 비밀번호 변경 및 설정(RPCSEC_GSS)

서비스	규약	포트	원천	목적지	목적
AutoSupport	HTTPS	443	노드 관리 LIF	mysupport.netapp.com	AutoSupport (HTTPS가 기본값)
	HTTP	80	노드 관리 LIF	mysupport.netapp.com	AutoSupport (전송 프로토콜이 HTTPS에서 HTTP로 변경된 경우에만)
	TCP	3128	노드 관리 LIF	콘솔 에이전트	아웃바운드 인터넷 연결이 불가능한 경우 콘솔 에이전트의 프록시 서버를 통해 AutoSupport 메시지 보내기
S3에 백업	TCP	5010	클러스터 간 LIF	백업 엔드포인트 또는 복원 엔드포인트	S3 백업 기능에 대한 백업 및 복원 작업
무리	모든 트래픽	모든 트래픽	한 노드의 모든 LIF	다른 노드의 모든 LIF	클러스터 간 통신(Cloud Volumes ONTAP HA만 해당)
	TCP	3000	노드 관리 LIF	HA 중재자	ZAPI 호출(Cloud Volumes ONTAP HA만 해당)
	ICMP	1	노드 관리 LIF	HA 중재자	유지(Cloud Volumes ONTAP HA만 해당)
구성 백업	HTTP	80	노드 관리 LIF	http://<콘솔 에이전트 IP 주소>/occm/offboxconfig	구성 백업을 콘솔 에이전트로 보냅니다 ."ONTAP 문서"
DHCP	UDP	68	노드 관리 LIF	DHCP	최초 설정을 위한 DHCP 클라이언트
DHCPS	UDP	67	노드 관리 LIF	DHCP	DHCP 서버
DNS	UDP	53	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
NDMP	TCP	18600년–18699년	노드 관리 LIF	대상 서버	NDMP 사본
SMTP	TCP	25	노드 관리 LIF	메일 서버	SMTP 알림은 AutoSupport 에 사용할 수 있습니다.
SNMP	TCP	161	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	UDP	161	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	TCP	162	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	UDP	162	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
SnapMirror	TCP	11104	클러스터 간 LIF	ONTAP 클러스터 간 LIF	SnapMirror 위한 클러스터 간 통신 세션 관리
	TCP	11105	클러스터 간 LIF	ONTAP 클러스터 간 LIF	SnapMirror 데이터 전송

서비스	규약	포트	원천	목적지	목적
시스템 로그	UDP	514	노드 관리 LIF	시스템 로그 서버	Syslog 전달 메시지

HA 중재자 외부 보안 그룹에 대한 규칙

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

인바운드 규칙

HA 중재자에 대한 미리 정의된 보안 그룹에는 다음과 같은 인바운드 규칙이 포함됩니다.

규약	포트	원천	목적
TCP	3000	콘솔 에이전트의 CIDR	콘솔 에이전트에서 RESTful API 액세스

아웃바운드 규칙

HA 중재자에 대한 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 개방합니다. 이것이 허용된다면, 기본적인 아웃바운드 규칙을 따르세요. 더욱 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용하세요.

기본 아웃바운드 규칙

HA 중재자에 대한 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

규약	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.

규약	포트	목적지	목적
HTTP	80	AWS EC2 인스턴스의 콘솔 에이전트의 IP 주소	중재자용 업그레이드 다운로드
HTTPS	443	ec2.amazonaws.com	스토리지 장애 조치 지원
UDP	53	ec2.amazonaws.com	스토리지 장애 조치 지원

포트 443과 53을 여는 대신 대상 서브넷에서 AWS EC2 서비스로 인터페이스 VPC 엔드포인트를 만들 수 있습니다.

HA 구성 내부 보안 그룹에 대한 규칙

Cloud Volumes ONTAP HA 구성을 위한 미리 정의된 내부 보안 그룹에는 다음 규칙이 포함됩니다. 이 보안 그룹은 HA 노드 간, 중재자와 노드 간 통신을 가능하게 합니다.

콘솔은 항상 이 보안 그룹을 생성합니다. 귀하 자신의 것을 사용할 수 있는 옵션이 없습니다.

인바운드 규칙

미리 정의된 보안 그룹에는 다음과 같은 인바운드 규칙이 포함됩니다.

규약	포트	목적
모든 트래픽	모두	HA 중재자와 HA 노드 간 통신

아웃바운드 규칙

미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

규약	포트	목적
모든 트래픽	모두	HA 중재자와 HA 노드 간 통신

콘솔 에이전트에 대한 규칙

"콘솔 에이전트에 대한 보안 그룹 규칙 보기"