네트워크 설정

Cloud Volumes ONTAP

NetApp
June 27, 2024

목차

네트워크 설정

AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항

BlueXP는 IP 주소, 넷마스크 및 라우트와 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 NetApp AutoSupport에 대한 아웃바운드 인터넷 액세스가 필요합니다. 사전 예방적으로 시스템의 상태를 모니터링하고 메시지를 NetApp 기술 지원으로 보냅니다.

라우팅 및 방화벽 정책은 Cloud Volumes ONTAP가 AutoSupport 메시지를 보낼 수 있도록 다음 엔드포인트에 대한 HTTP/HTTPS 트래픽을 허용해야 합니다.

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

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

AutoSupport 메시지를 보내는 데 아웃바운드 인터넷 연결을 사용할 수 없는 경우 BlueXP는 자동으로 Cloud Volumes ONTAP 시스템에서 커넥터를 프록시 서버로 사용하도록 구성합니다. 유일한 요구 사항은 커넥터의 보안 그룹이 포트 3128을 통한 _IN인바운드_연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

Cloud Volumes ONTAP에 대해 엄격한 아웃바운드 규칙을 정의한 경우 Cloud Volumes ONTAP 보안 그룹이 포트 3128을 통한 _outbound_connection을 허용하는지 확인해야 합니다.

아웃바운드 인터넷 액세스가 가능한지 확인한 후 AutoSupport를 테스트하여 메시지를 보낼 수 있는지 확인할 수 있습니다. 자세한 지침은 을 참조하십시오 "ONTAP 문서: AutoSupport 설정".

BlueXP에서 AutoSupport 메시지를 보낼 수 없다고 알리는 경우 "AutoSupport 구성 문제를 해결합니다".

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

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

BlueXP에서 Cloud Volumes ONTAP에 할당하는 LIF 수는 단일 노드 시스템을 배포할지 HA 쌍을 구축하는지에 따라 달라집니다. LIF는 물리적 포트와 연결된 IP 주소입니다.

단일 노드 시스템의 IP 주소입니다

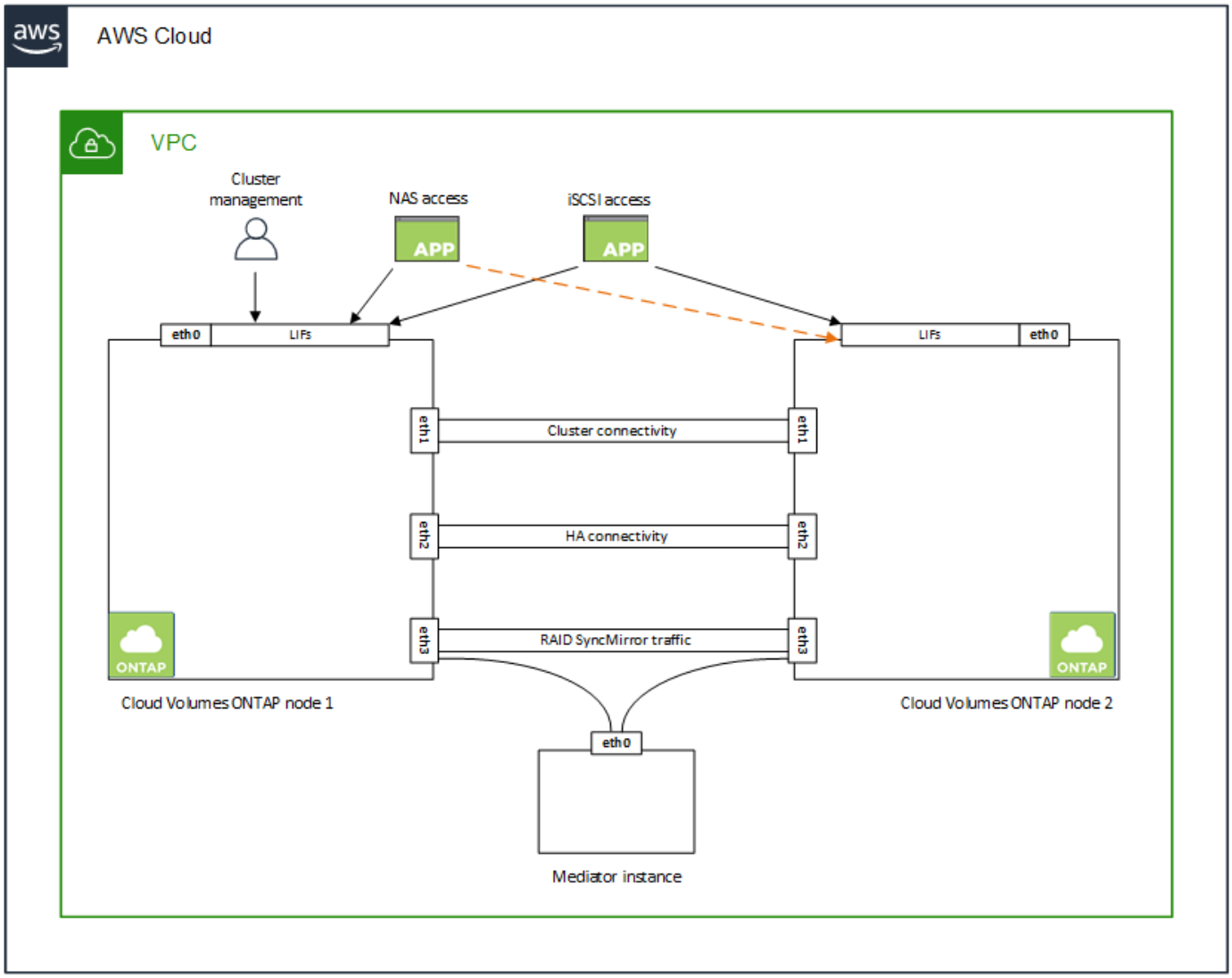
BlueXP는 단일 노드 시스템에 6개의 IP 주소를 할당합니다.

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

LIF	목적
클러스터 관리	전체 클러스터(HA 쌍)의 관리
노드 관리	노드의 관리.
인터클러스터	클러스터 간 통신, 백업 및 복제
NAS 데이터	NAS 프로토콜을 통한 클라이언트 액세스
iSCSI 데이터	iSCSI 프로토콜을 통한 클라이언트 액세스. 또한 시스템에서 다른 중요한 네트워킹 워크플로우에 사용됩니다. 이 LIF는 필수 항목이므로 삭제할 수 없습니다.
스토리지 VM 관리	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 **AZ**에서 **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. 또한 시스템에서 다른 중요한 네트워킹 워크플로우에 사용됩니다. 이러한 LIF는 필수 항목이므로 삭제할 수 없습니다.

LIF	인터페이스	노드	목적
클러스터 연결	eth1	노드 1 및 노드 2	노드가 서로 통신하고 클러스터 내에서 데이터를 이동할 수 있도록 지원합니다.
HA 연결	윤리2	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 **AZs**의 **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. 이러한 LIF는 노드 간 부동 IP 주소의 마이그레이션도 관리합니다. 이러한 LIF는 필수 항목이므로 삭제할 수 없습니다.
클러스터 연결	eth1	노드 1 및 노드 2	노드가 서로 통신하고 클러스터 내에서 데이터를 이동할 수 있도록 지원합니다.
HA 연결	윤리2	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

BlueXP에서는 보안 그룹을 만들 필요가 없습니다. 직접 사용해야 하는 경우 을 참조하십시오 "보안 그룹 규칙".

커넥터에 대한 정보를 찾고 계십니까? "Connector에 대한 보안 그룹 규칙을 봅니다"

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".

VPC 공유

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

"공유 서브넷에 HA 쌍을 구축하는 방법을 알아보십시오".

여러 대의 **AZs**에서 **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 BlueXP에 네트워킹 세부 정보를 입력해야 하므로 HA 쌍을 실행하기 전에 이러한 요구 사항을 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".

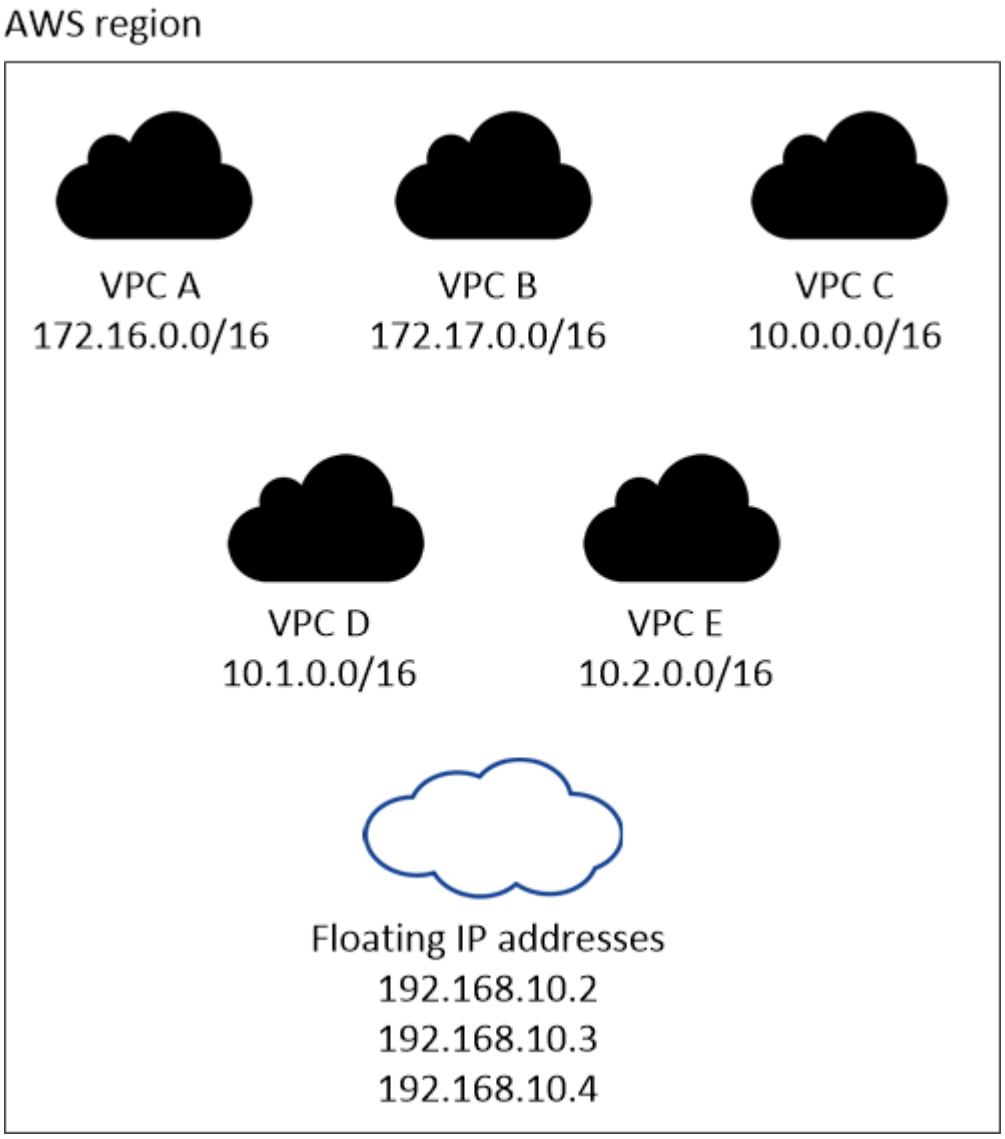
하나의 부동 IP 주소는 클러스터 관리용, 하나는 노드 1의 NFS/CIFS 데이터용으로, 다른 하나는 노드 2의 NFS/CIFS 데이터용으로 사용됩니다. SVM 관리를 위한 네 번째 유동 IP 주소는 선택 사항입니다.

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

Cloud Volumes ONTAP HA 작업 환경을 생성할 때 BlueXP에서 부동 IP 주소를 입력해야 합니다. BlueXP는 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.



BlueXP는 VPC 외부의 클라이언트에서 iSCSI 액세스 및 NAS 액세스를 위해 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

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

VPC(주 경로 테이블)에 있는 서브넷을 위한 경로 테이블이 하나만 있는 경우 BlueXP는 해당 라우팅 테이블에 부동 IP 주소를 자동으로 추가합니다. 둘 이상의 라우트 테이블이 있는 경우 HA 쌍을 시작할 때 올바른 라우트 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. 라우트 테이블 A를 선택했지만 라우트 테이블 B는 선택하지 않은 경우, 라우트 테이블 A와 연결된 서브넷에 있는 클라이언트는 HA 쌍에 액세스할 수 있지만, 라우트 테이블 B와 연결된 서브넷에 있는 클라이언트는 액세스할 수 없습니다.

라우팅 테이블에 대한 자세한 내용은 을 참조하십시오 "AWS 설명서: 경로 테이블".

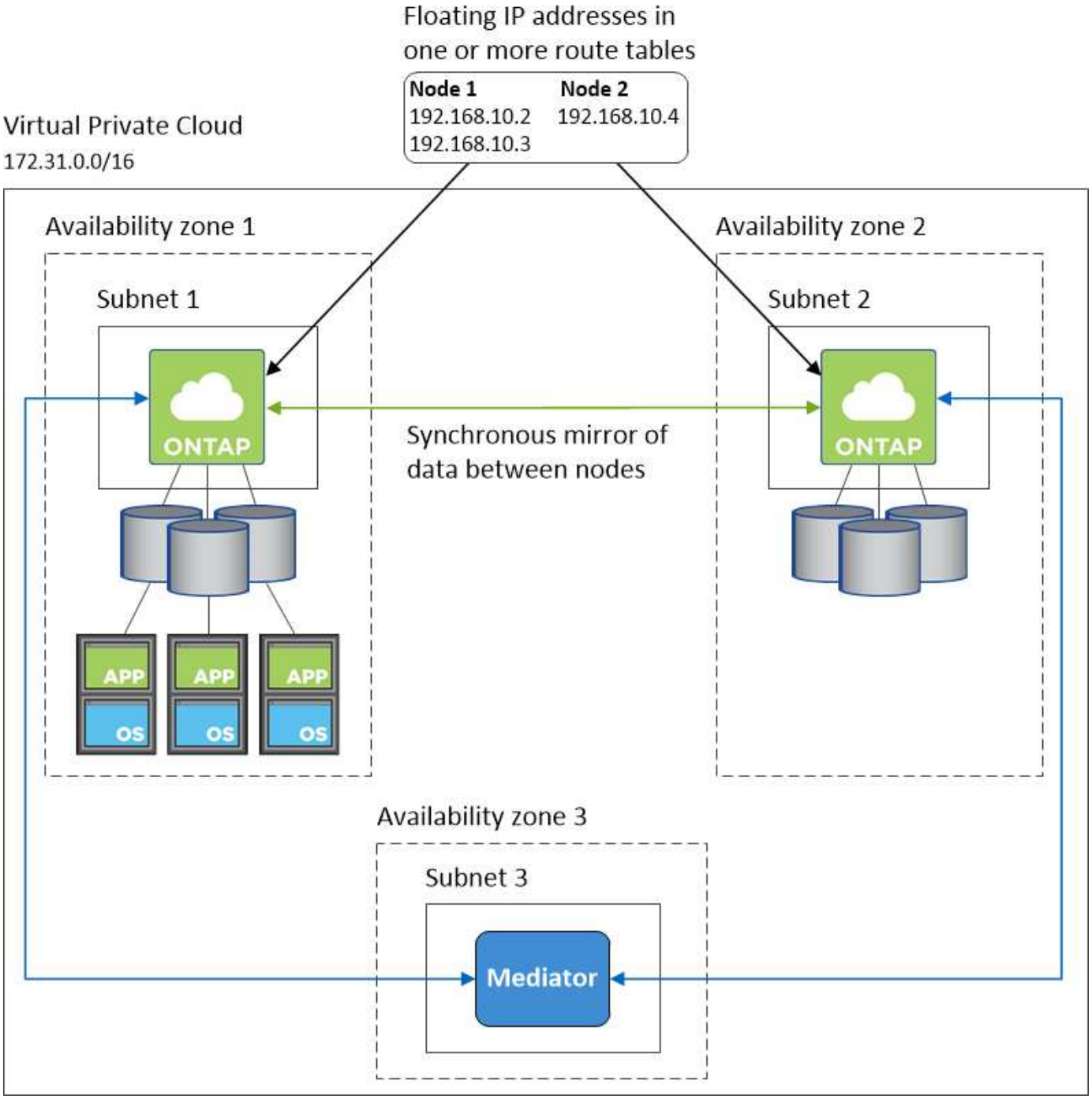
NetApp 관리 툴에 연결

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

1. NetApp 관리 툴을 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 툴을 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

아직 Connector를 만들지 않은 경우 Connector에 대한 네트워킹 요구 사항도 검토해야 합니다.

- "커넥터에 대한 네트워킹 요구 사항을 봅니다"
- "AWS의 보안 그룹 규칙"

여러 **AZs**에서 **HA** 쌍에 대한 **AWS** 전송 게이트웨이 설정

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

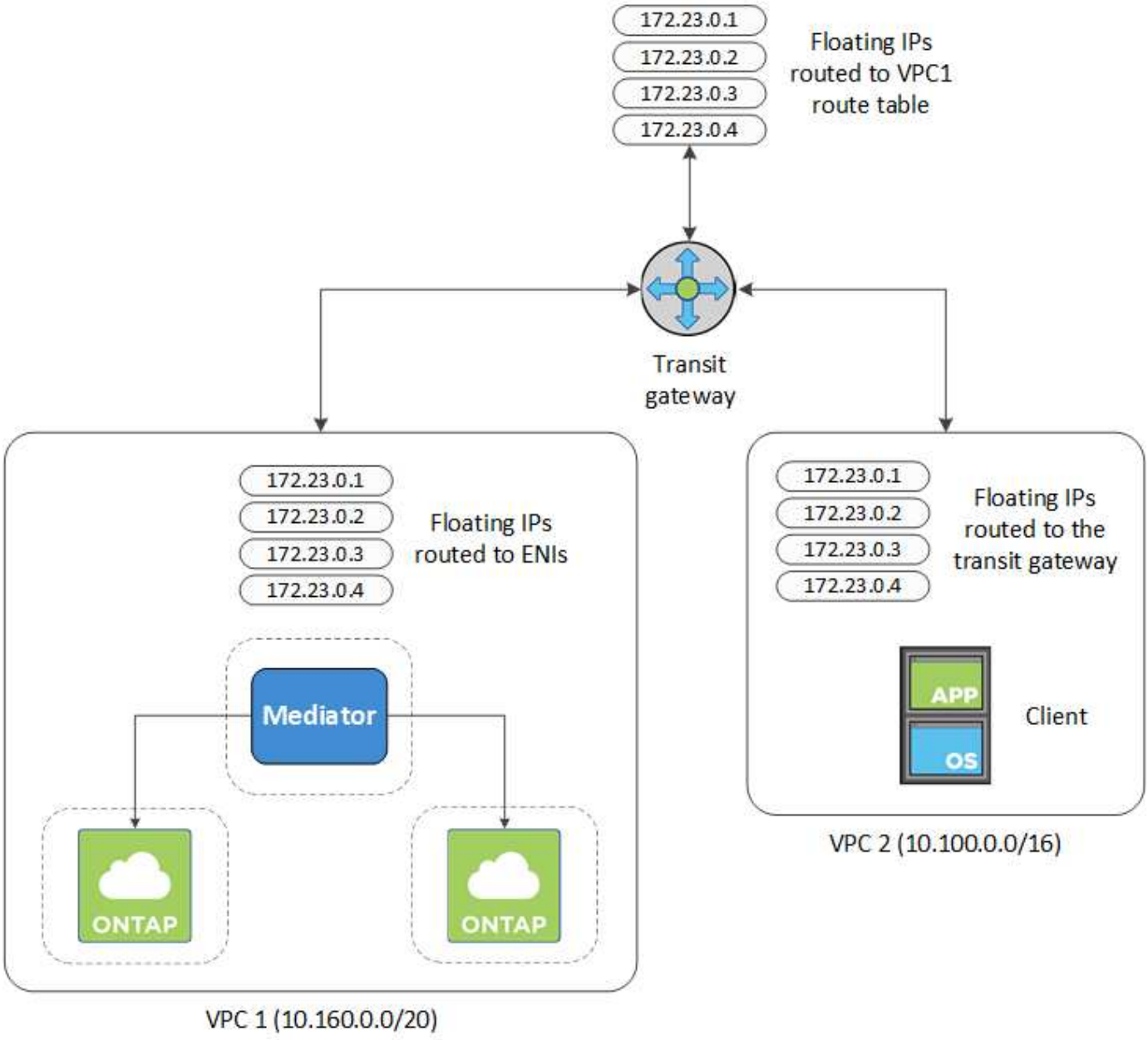
상주하는 VPC 외부에서

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.

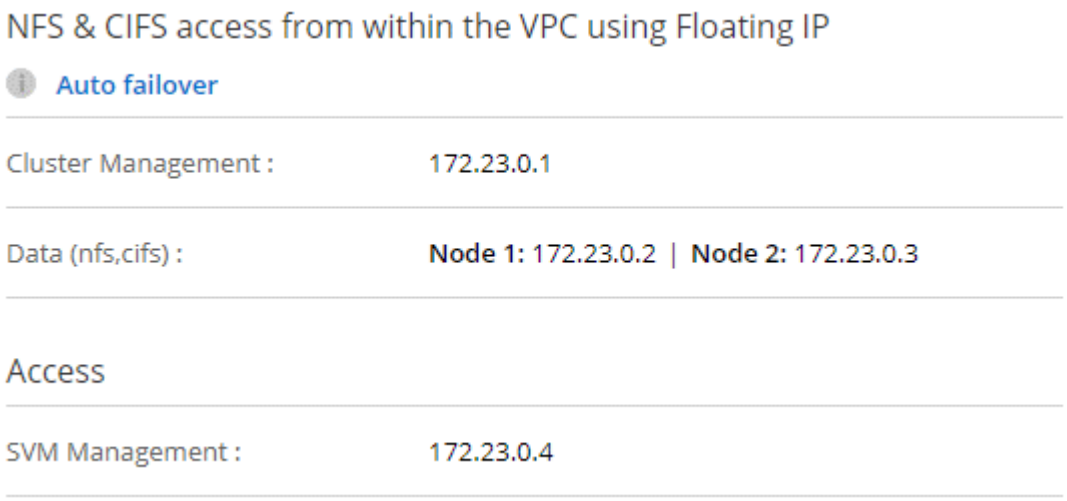


다음 단계에서는 유사한 구성을 설정하는 방법을 보여 줍니다.

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.

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



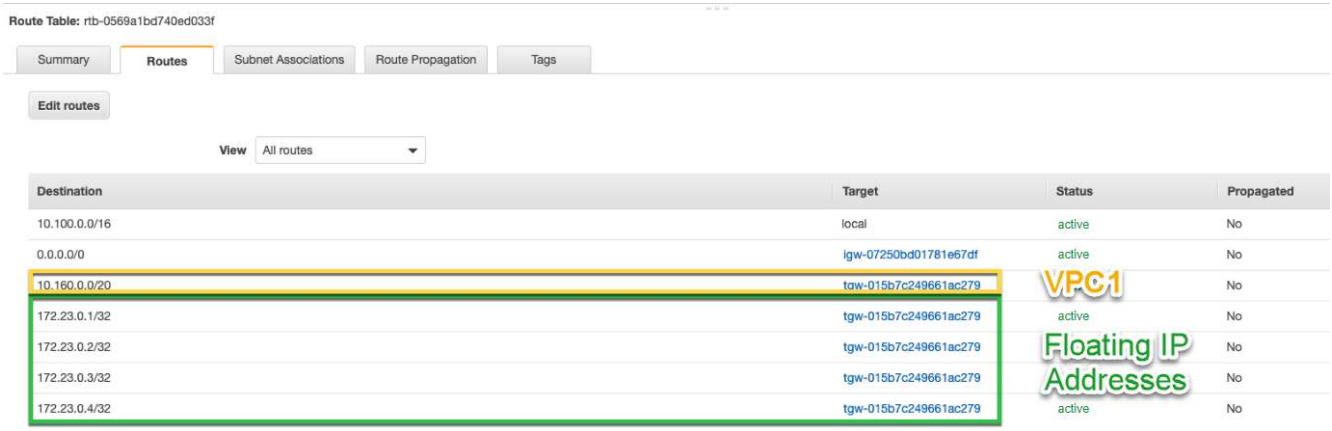
   다음 샘플 이미지는 전송 게이트웨이의 라우트 테이블을 보여 줍니다. 여기에는 2개의 VPC의 CIDR 블록에 대한 경로와 Cloud Volumes ONTAP에서 사용하는 4개의 부동 IP 주소가 포함됩니다.

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.

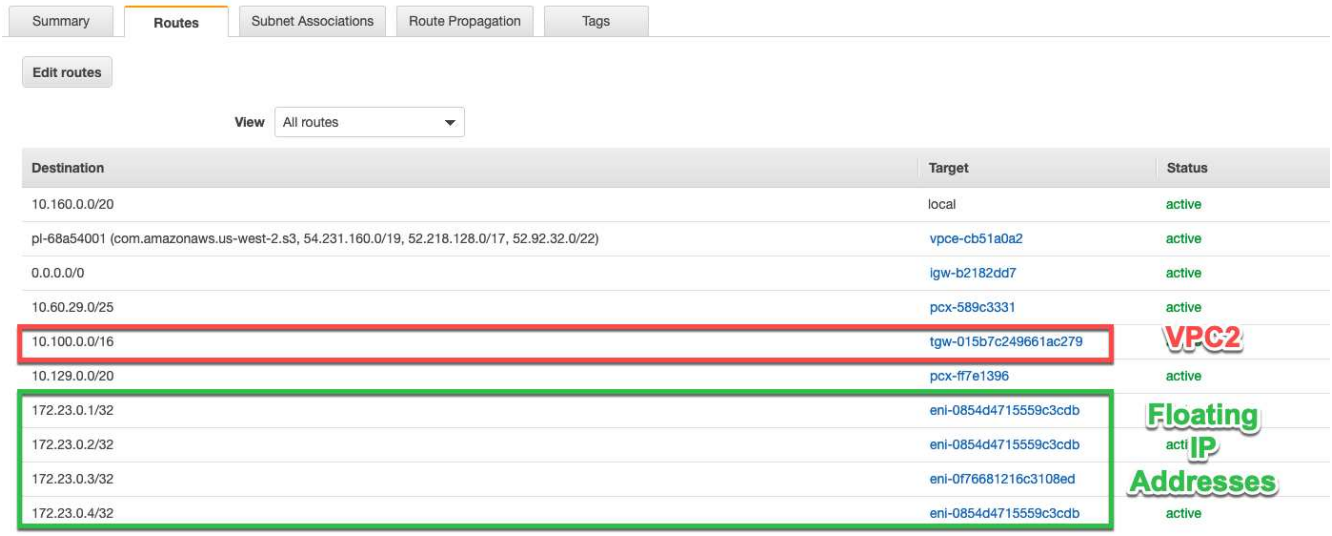
다음 샘플 이미지는 VPC 1에 대한 라우트 및 부동 IP 주소를 포함하는 VPC 2용 라우팅 테이블을 보여 줍니다.



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

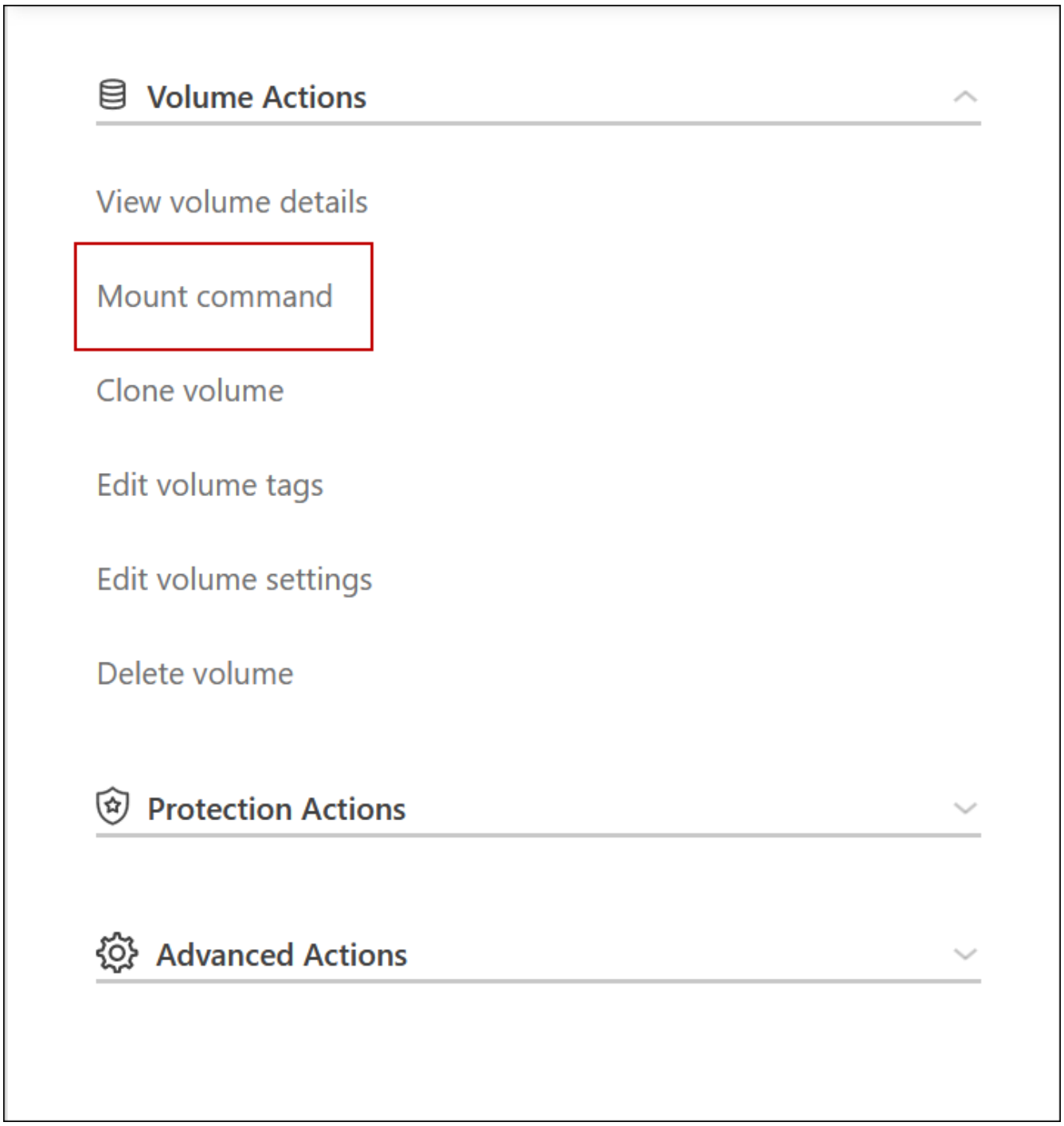
이 단계는 VPC 간 라우팅을 완료하기 때문에 중요합니다.

다음 샘플 이미지는 VPC 1의 라우트 테이블을 보여 줍니다. 여기에는 부동 IP 주소 및 클라이언트가 있는 VPC 2로의 라우트가 포함됩니다. BlueXP는 HA 쌍을 배포할 때 라우팅 테이블에 유동 IP를 자동으로 추가했습니다.



6. 부동 IP 주소를 사용하여 클라이언트에 볼륨을 마운트합니다.

BlueXP의 볼륨 관리 패널의 * 탑재 명령 * 옵션을 통해 BlueXP에서 올바른 IP 주소를 찾을 수 있습니다.



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

   "볼륨을 편집하는 방법에 대해 알아봅니다".

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

공유 서브넷에 **HA** 쌍 구축

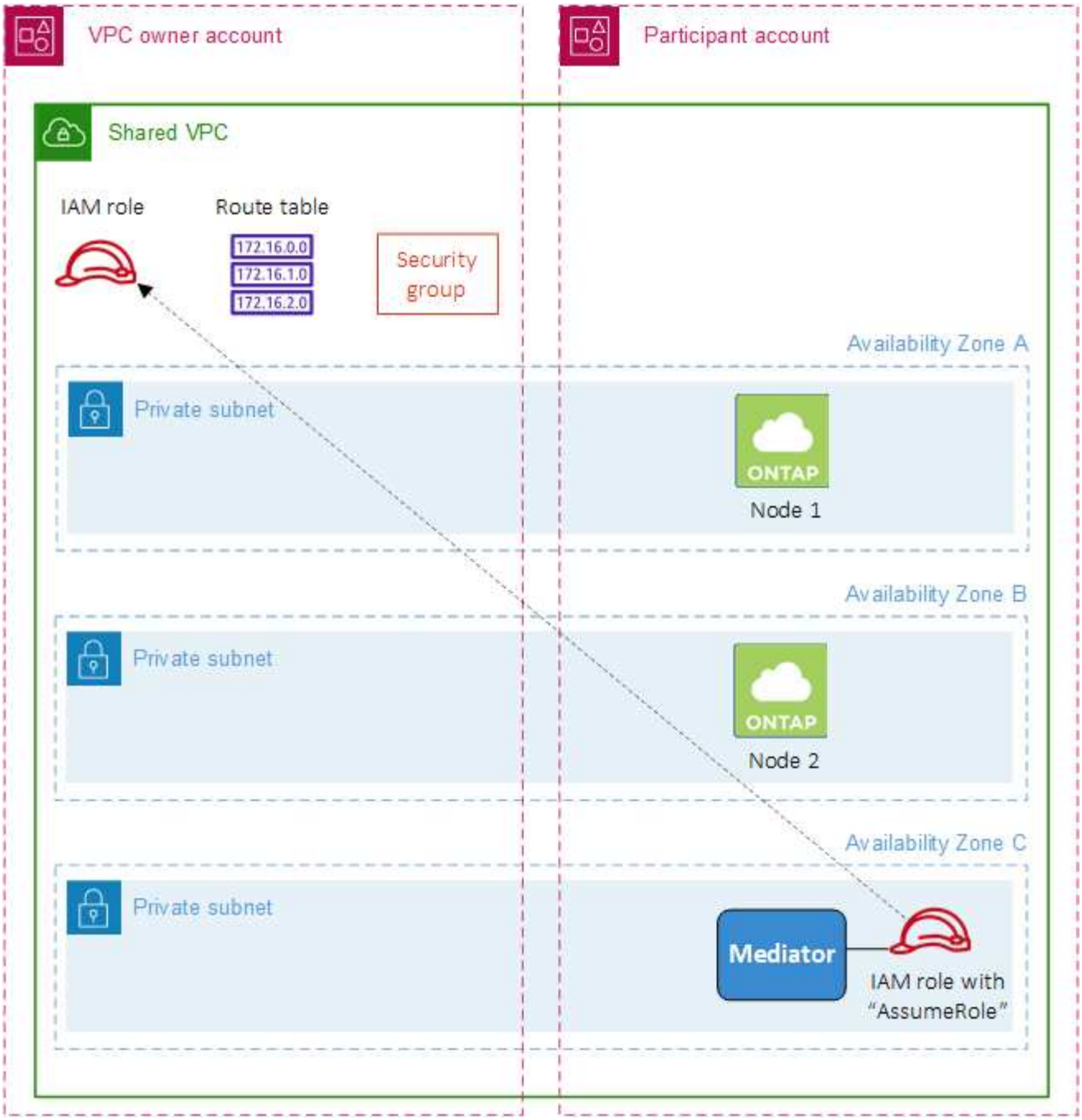
9.11.1 릴리즈부터 VPC 공유를 지원하는 AWS에서 Cloud Volumes ONTAP HA 쌍이 지원됩니다. VPC 공유를 사용하면 서브넷을 다른 AWS 계정과 공유할 수 있습니다. 이 구성을 사용하려면 AWS 환경을 설정한 다음 API를 사용하여 HA 쌍을 구축해야 합니다.

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

- 네트워킹을 소유하는 VPC 소유자 계정(VPC, 서브넷, 라우팅 테이블 및 Cloud Volumes ONTAP 보안 그룹)
- 참가자 계정으로, EC2 인스턴스가 공유 서브넷에 구축됩니다(여기에는 2개의 HA 노드와 중재자가 포함됨).

여러 가용성 영역에 배포된 Cloud Volumes ONTAP HA 구성의 경우 HA 중재자가 VPC 소유자 계정의 라우트 테이블에 쓸 수 있는 특정 권한이 필요합니다. 중재자가 추정할 수 있는 IAM 역할을 설정하여 이러한 권한을 제공해야 합니다.

다음 이미지는 이 구축과 관련된 구성 요소를 보여줍니다.



아래 단계에 설명된 대로 참가자 계정과 서브넷을 공유하고 VPC 소유자 계정에서 IAM 역할 및 보안 그룹을 만들어야 합니다.

Cloud Volumes ONTAP 작업 환경을 만들면 BlueXP는 자동으로 IAM 역할을 생성하여 중재자에 연결합니다. 이 역할은 HA 쌍과 연결된 경로 테이블을 변경하기 위해 VPC 소유자 계정에서 생성한 IAM 역할을 가정합니다.

단계

1. VPC 소유자 계정의 서브넷을 참가자 계정과 공유합니다.

   이 단계는 공유 서브넷에 HA 쌍을 구축하는 데 필요합니다.

   "AWS 설명서: 서브넷을 공유합니다"

2. VPC 소유자 계정에서 Cloud Volumes ONTAP용 보안 그룹을 생성합니다.

   "Cloud Volumes ONTAP의 보안 그룹 규칙을 참조하십시오". HA 중재자를 위한 보안 그룹을 만들 필요는 없습니다. BlueXP가 이러한 작업을 수행합니다.

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

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

4. BlueXP API를 사용하여 새로운 Cloud Volumes ONTAP 작업 환경을 만듭니다.

   다음 필드를 지정해야 합니다.

   - "보안 그룹 ID"

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

   - "haParams" 개체의 "assumeRoleArn

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

     예를 들면 다음과 같습니다.

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

+
"Cloud Volumes ONTAP API에 대해 자세히 알아보십시오"

AWS의 보안 그룹 규칙

BlueXP는 Cloud Volumes ONTAP의 성공적인 운영에 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

작업 환경을 만들고 미리 정의된 보안 그룹을 선택할 때 다음 중 한 가지 내에서 트래픽을 허용하도록 선택할 수 있습니다.

- * 선택한 VPC만 해당 *: 인바운드 트래픽의 소스는 Cloud Volumes ONTAP 시스템용 VPC의 서브넷 범위와 커넥터가 상주하는 VPC의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다.
- * 모든 VPC *: 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.

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 커넥터 및 HTTPS 액세스와의 연결
SSH를 클릭합니다	22	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다
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	2049년	NFS 서버 데몬
TCP	3260입니다	iSCSI 데이터 LIF를 통한 iSCSI 액세스
TCP	4045로 문의하십시오	NFS 잠금 데몬
TCP	4046으로 문의하십시오	NFS에 대한 네트워크 상태 모니터
TCP	10000	NDMP를 사용한 백업
TCP	11104를 참조하십시오	SnapMirror에 대한 인터클러스터 통신 세션의 관리
TCP	11105를 참조하십시오	인터클러스터 LIF를 사용하여 SnapMirror 데이터 전송

프로토콜	포트	목적
UDP입니다	111	NFS에 대한 원격 프로시저 호출
UDP입니다	161-162	단순한 네트워크 관리 프로토콜
UDP입니다	635	NFS 마운트
UDP입니다	2049년	NFS 서버 데몬
UDP입니다	4045로 문의하십시오	NFS 잠금 데몬
UDP입니다	4046으로 문의하십시오	NFS에 대한 네트워크 상태 모니터
UDP입니다	4049입니다	NFS rquotad 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
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 Directory를 클릭합니다	TCP	88을 참조하십시오	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니다	137입니다	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니다	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)
	UDP입니다	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	88을 참조하십시오	데이터 LIF(NFS, CIFS, iSCSI)	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니다	137입니다	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니다	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)
	UDP입니다	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)

서비스	프로토콜	포트	출처	목적지	목적
AutoSupport	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)
	TCP	3128	노드 관리 LIF	커넥터	아웃바운드 인터넷 연결을 사용할 수 없는 경우 커넥터의 프록시 서버를 통해 AutoSupport 메시지 보내기
S3로 백업	TCP	5010입니다	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	3000입니다	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)
구성 백업	HTTP	80	노드 관리 LIF	http://<connector-IP-address>/occm/offboxconfig입니다	Connector로 구성 백업을 보냅니다. "구성 백업 파일에 대해 자세히 알아보십시오".
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	18600–18699	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

서비스	프로토콜	포트	출처	목적지	목적
SnapMirror를 참조하십시오	TCP	11104를 참조하십시오	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror에 대한 인터클러스터 통신 세션의 관리
	TCP	11105를 참조하십시오	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

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

프로토콜	포트	출처	목적
TCP	3000입니다	커넥터의 CIDR	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	AWS EC2 인스턴스에 있는 Connector의 IP 주소입니다	중재자를 위한 업그레이드 다운로드

프로토콜	포트	목적지	목적
HTTPS	443	ec2.amazonaws.com	스토리지 페일오버 지원
UDP입니다	53	ec2.amazonaws.com	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.

BlueXP는 항상 이 보안 그룹을 만듭니다. 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

"Connector에 대한 보안 그룹 규칙을 봅니다"