



Amazon Web Services에서 시작하십시오 Cloud Volumes ONTAP

NetApp
May 12, 2022

목차

Amazon Web Services에서 시작하십시오	1
AWS에서 Cloud Volumes ONTAP를 빠르게 시작합니다	1
AWS에서 Cloud Volumes ONTAP 구성 계획	2
네트워크 설정	6
AWS KMS 설정	25
AWS에서 Cloud Volumes ONTAP 실행	28
AWS C2S 환경에서 Cloud Volumes ONTAP를 시작하십시오	42

Amazon Web Services에서 시작하십시오

AWS에서 Cloud Volumes ONTAP를 빠르게 시작합니다

몇 가지 단계를 통해 AWS에서 Cloud Volumes ONTAP를 시작하십시오.

가 없는 경우 ["커넥터"](#) 그러나 계정 관리자는 계정을 만들어야 합니다. ["AWS에서 커넥터를 생성하는 방법에 대해 알아보십시오"](#).

첫 번째 Cloud Volumes ONTAP 작업 환경을 생성할 때 아직 커넥터가 없는 경우 Cloud Manager에서 커넥터를 배포할지 묻는 메시지를 표시합니다.

Cloud Manager는 워크로드 요구사항에 맞게 사전 구성된 패키지를 제공하거나 자체 구성을 생성할 수 있습니다. 자신의 구성을 선택하는 경우 사용 가능한 옵션을 이해해야 합니다. ["자세한 정보"](#).

네트워크 설정

1. VPC와 서브넷이 커넥터와 Cloud Volumes ONTAP 간의 연결을 지원하는지 확인합니다.
2. 커넥터 및 Cloud Volumes ONTAP가 여러 엔드포인트에 연결할 수 있도록 타겟 VPC에서 아웃바운드 인터넷 액세스를 활성화합니다.

이 단계는 커넥터가 아웃바운드 인터넷 액세스 없이 Cloud Volumes ONTAP를 관리할 수 없기 때문에 중요합니다. 아웃바운드 연결을 제한해야 하는 경우의 끝점 목록을 참조하십시오 ["커넥터 및 Cloud Volumes ONTAP"](#).

3. VPC 엔드포인트를 S3 서비스로 설정합니다.

Cloud Volumes ONTAP의 콜드 데이터를 저비용 오브젝트 스토리지로 계층화하려는 경우 VPC 엔드포인트가 필요합니다.

["네트워킹 요구 사항에 대해 자세히 알아보십시오"](#).

Cloud Volumes ONTAP에서 아마존 암호화를 사용하려면 활성 CMK(고객 마스터 키)가 있는지 확인해야 합니다. 또한 Connector에 대한 권한을 제공하는 IAM 역할을 _KEY_USER_로 추가하여 각 CMK에 대한 키 정책을 수정해야 합니다. ["자세한 정보"](#).

작업 환경 추가 * 를 클릭하고 배포할 시스템 유형을 선택한 다음 마법사의 단계를 완료합니다. ["단계별 지침을 읽습니다"](#).

관련 링크

- ["Cloud Manager에서 커넥터 생성"](#)
- ["AWS Marketplace에서 커넥터 실행"](#)
- ["Linux 호스트에 Connector 소프트웨어 설치"](#)
- ["Cloud Manager에서 AWS 권한을 통해 수행하는 것"](#)

AWS에서 Cloud Volumes ONTAP 구성 계획

AWS에 Cloud Volumes ONTAP를 구축할 때 워크로드 요구사항에 맞게 사전 구성된 시스템을 선택하거나 자체 구성을 생성할 수 있습니다. 자신의 구성을 선택하는 경우 사용 가능한 옵션을 이해해야 합니다.

지원되는 영역 보기

Cloud Volumes ONTAP는 대부분의 AWS 지역에서 지원됩니다. ["지원되는 영역의 전체 목록을 봅니다"](#).

해당 지역에서 리소스를 생성하고 관리하려면 먼저 새로운 AWS 영역을 활성화해야 합니다. ["지역 활성화 방법을 알아보십시오"](#).

라이선스 선택

Cloud Volumes ONTAP에는 몇 가지 라이선스 옵션이 있습니다. 각 옵션을 사용하여 요구사항에 맞는 소비 모델을 선택할 수 있습니다. ["Cloud Volumes ONTAP의 라이선스 옵션에 대해 자세히 알아보십시오"](#).

지원되는 인스턴스 선택

Cloud Volumes ONTAP는 선택한 라이선스 유형에 따라 여러 인스턴스 유형을 지원합니다.

["AWS에서 Cloud Volumes ONTAP가 지원되는 구성입니다"](#)

Flash Cache를 지원하는 구성 선택

AWS의 일부 Cloud Volumes ONTAP 구성에는 Cloud Volumes ONTAP이 성능 향상을 위해 _Flash Cache_로 사용하는 로컬 NVMe 스토리지가 포함됩니다. ["Flash Cache에 대해 자세히 알아보십시오"](#).

스토리지 제한 이해

Cloud Volumes ONTAP 시스템의 물리적 용량 제한은 라이선스에 연결되어 있습니다. 추가 제한은 애그리게이트 및 볼륨 크기에 영향을 줍니다. 구성을 계획할 때 이러한 제한 사항을 숙지해야 합니다.

["AWS의 Cloud Volumes ONTAP에 대한 스토리지 제한"](#)

AWS에서 시스템 사이징

Cloud Volumes ONTAP 시스템을 사이징하면 성능 및 용량 요구사항을 충족하는 데 도움이 될 수 있습니다. 인스턴스 유형, 디스크 유형 및 디스크 크기를 선택할 때 몇 가지 주요 사항을 알고 있어야 합니다.

인스턴스 유형

- 각 EC2 인스턴스 유형별 최대 처리량과 IOPS에 맞춰 워크로드 요구사항을 충족합니다.
- 여러 사용자가 동시에 시스템에 쓸 경우 요청을 관리할 CPU가 충분한 인스턴스 유형을 선택합니다.
- 대부분 읽혀지는 응용 프로그램이 있는 경우 충분한 RAM이 있는 시스템을 선택합니다.
 - ["AWS 문서: Amazon EC2 인스턴스 유형"](#)
 - ["AWS 문서: Amazon EBS – 최적화된 인스턴스"](#)

EBS 디스크 유형입니다

EBS 디스크 유형의 차이점은 다음과 같습니다. EBS 디스크의 사용 사례에 대한 자세한 내용은 [을 참조하십시오 "AWS 설명서:EBS 볼륨 유형"](#).

- **_GP3(General Purpose SSD)_**디스크는 광범위한 워크로드에 대해 비용과 성능의 균형을 유지하는 가장 저렴한 SSD입니다. 성능은 IOPS 및 처리량 측면에서 정의됩니다. GP3 디스크는 Cloud Volumes ONTAP 9.7 이상에서 지원됩니다.

GP3 디스크를 선택하면 Cloud Manager가 기본 IOPS 및 처리량 값을 채워 선택한 디스크 크기를 기준으로 GP2 디스크와 동일한 성능을 제공합니다. 더 높은 비용으로 더 나은 성능을 얻기 위해 값을 늘릴 수 있지만 성능이 저하될 수 있으므로 더 낮은 값을 지원하지 않습니다. 즉, 기본값을 그대로 사용하거나 값을 늘립니다. 낮추지 마십시오. ["GP3 디스크 및 성능에 대해 자세히 알아보십시오"](#).

- **_GP2(General Purpose SSD)_**디스크는 광범위한 워크로드에 대해 비용과 성능의 균형을 맞춥니다. 성능은 IOPS 측면에서 정의됩니다.
- **_provisioned IOPS ssd(i1)_disk**는 높은 비용으로 최고의 성능을 요구하는 중요한 응용 프로그램을 위한 것입니다.
- **_Throughput Optimized HDD(st1)_**디스크는 낮은 가격으로 빠르고 일관된 처리량을 필요로 하는 자주 액세스되는 워크로드에 적합합니다.



처리량 최적화 HDD(st1)를 사용하는 경우에는 데이터를 오브젝트 스토리지에 계층화하지 않는 것이 좋습니다.

EBS 디스크 크기입니다

Cloud Volumes ONTAP 시스템을 시작할 때 초기 디스크 크기를 선택해야 합니다. 그 이후에는 가능합니다 ["Cloud Manager로 시스템 용량을 관리할 수 있습니다"](#)하지만 원하는 경우 ["스스로 애그리게이트를 생성합니다"](#)다음 사항에 유의하십시오.

- Aggregate의 모든 디스크는 동일한 크기여야 합니다.
- EBS 디스크의 성능은 디스크 크기와 관련이 있습니다. 이 크기는 SSD 디스크의 기준 IOPS 및 최대 버스트 지속 시간과 HDD 디스크의 기준 및 버스트 처리량을 결정합니다.
- 궁극적으로 필요한 **_지속적인 성능_**을(를) 제공하는 디스크 크기를 선택해야 합니다.
- 더 큰 디스크(예: 4TiB 디스크 6개)를 선택하더라도 EC2 인스턴스가 대역폭 제한에 도달할 수 있으므로 모든 IOPS를 가져오지 못할 수 있습니다.

EBS 디스크 성능에 대한 자세한 내용은 [을 참조하십시오 "AWS 설명서:EBS 볼륨 유형"](#).

AWS에서 Cloud Volumes ONTAP 시스템 사이징에 대한 자세한 내용은 다음 비디오에서 확인하십시오.



기본 시스템 디스크를 봅니다

사용자 데이터를 위한 스토리지 외에, Cloud Manager는 Cloud Volumes ONTAP 시스템 데이터(부팅 데이터, 루트 데이터, 코어 데이터, NVRAM)를 위한 클라우드 스토리지도 구매합니다. 계획을 위해 Cloud Volumes ONTAP를 배포하기 전에 이러한 세부 정보를 검토하는 것이 도움이 될 수 있습니다.

"AWS에서 Cloud Volumes ONTAP 시스템 데이터의 기본 디스크를 봅니다".



커넥터에는 시스템 디스크도 필요합니다. ["커넥터의 기본 설정에 대한 세부 정보를 봅니다"](#).

AWS 아웃포스트에 Cloud Volumes ONTAP 구축 준비

AWS 아웃포스트가 있는 경우 작업 환경 마법사에서 아웃포스트 VPC를 선택하여 해당 아웃포스트에 Cloud Volumes ONTAP를 구축할 수 있습니다. 이러한 경험은 AWS에 상주하는 다른 VPC와 동일합니다. 먼저 AWS Outpost에 Connector를 구축해야 합니다.

몇 가지 제한 사항이 있습니다.

- 현재 단일 노드 Cloud Volumes ONTAP 시스템만 지원됩니다
- Cloud Volumes ONTAP와 함께 사용할 수 있는 EC2 인스턴스는 Outpost에서 사용할 수 있는 인스턴스로 제한됩니다
- 현재 GP2(범용 SSD)만 지원됩니다

AWS 네트워크 정보 워크시트

AWS에서 Cloud Volumes ONTAP를 시작할 때 VPC 네트워크에 대한 세부 정보를 지정해야 합니다. 워크시트를 사용하여 관리자로부터 정보를 수집할 수 있습니다.

Cloud Volumes ONTAP에 대한 네트워크 정보입니다

확인하십시오	귀사의 가치
지역	
VPC	
서브넷	
보안 그룹(자체 보안 그룹 사용 시)	

여러 AZs의 HA 쌍에 대한 네트워크 정보

확인하십시오	귀사의 가치
지역	
VPC	
보안 그룹(자체 보안 그룹 사용 시)	
노드 1 가용성 영역	
노드 1 서브넷	
노드 2 가용성 영역	
노드 2 서브넷	
중재자 가용성 영역	
중재자 서브넷	
중재자를 위한 키 쌍입니다	
클러스터 관리 포트의 부동 IP 주소입니다	
노드 1의 데이터에 대한 유동 IP 주소입니다	
노드 2의 데이터에 대한 유동 IP 주소입니다	
부동 IP 주소에 대한 라우팅 테이블	

쓰기 속도 선택

Cloud Manager를 사용하면 Cloud Volumes ONTAP의 쓰기 속도 설정을 선택할 수 있습니다. 쓰기 속도를 선택하기 전에 고속 쓰기 속도를 사용할 때 정상 및 높음 설정의 차이점과 위험 및 권장 사항을 이해해야 합니다. ["쓰기 속도에 대해 자세히 알아보십시오"](#).

볼륨 사용 프로파일 선택

ONTAP에는 필요한 총 스토리지 양을 줄일 수 있는 몇 가지 스토리지 효율성 기능이 포함되어 있습니다. Cloud Manager에서 볼륨을 생성할 때 이러한 기능을 사용하도록 설정하는 프로파일이나 기능을 사용하지 않도록 설정하는 프로파일을 선택할 수 있습니다. 사용할 프로파일을 결정하는 데 도움이 되도록 이러한 기능에 대해 자세히 알아 두어야 합니다.

NetApp 스토리지 효율성 기능은 다음과 같은 이점을 제공합니다.

씬 프로비저닝

에서는 실제 스토리지 풀에 있는 것보다 더 많은 논리적 스토리지를 호스트 또는 사용자에게 제공합니다. 스토리지 공간을 사전에 할당하는 대신 데이터가 기록될 때 스토리지 공간을 각 볼륨에 동적으로 할당합니다.

중복 제거

동일한 데이터 블록을 찾아 단일 공유 블록에 대한 참조로 대체하여 효율성을 향상시킵니다. 이 기술은 동일한 볼륨에 상주하는 중복된 데이터 블록을 제거하여 스토리지 용량 요구 사항을 줄여줍니다.

압축

1차, 2차 및 아카이브 스토리지의 볼륨 내에서 데이터를 압축하여 데이터를 저장하는 데 필요한 물리적 용량을 줄입니다.

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 [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.

LIF	인터페이스	노드	목적
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"는 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 **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 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 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

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://cloudmanagerinfraproduct.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 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

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	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)
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

AWS KMS 설정

Cloud Volumes ONTAP에서 Amazon 암호화를 사용하려면 AWS KMS(키 관리 서비스)를 설정해야 합니다.

단계

1. 활성 CMK(Customer Master Key)가 있는지 확인합니다.

CMK는 AWS로 관리되는 CMK 또는 고객이 관리하는 CMK가 될 수 있습니다. Cloud Manager 및 Cloud Volumes ONTAP와 동일한 AWS 계정 또는 다른 AWS 계정에 있을 수 있습니다.

["AWS 설명서:CMK\(Customer Master Key\)"](#)

2. Cloud Manager에 권한을 제공하는 IAM 역할을 _KEY_USER_로 추가하여 각 CMK에 대한 키 정책을 수정합니다.

IAM 역할을 주요 사용자로 추가하면 Cloud Manager에서 Cloud Volumes ONTAP와 함께 CMK를 사용할 수 있는 권한이 부여됩니다.

["AWS 설명서:키 편집"](#)

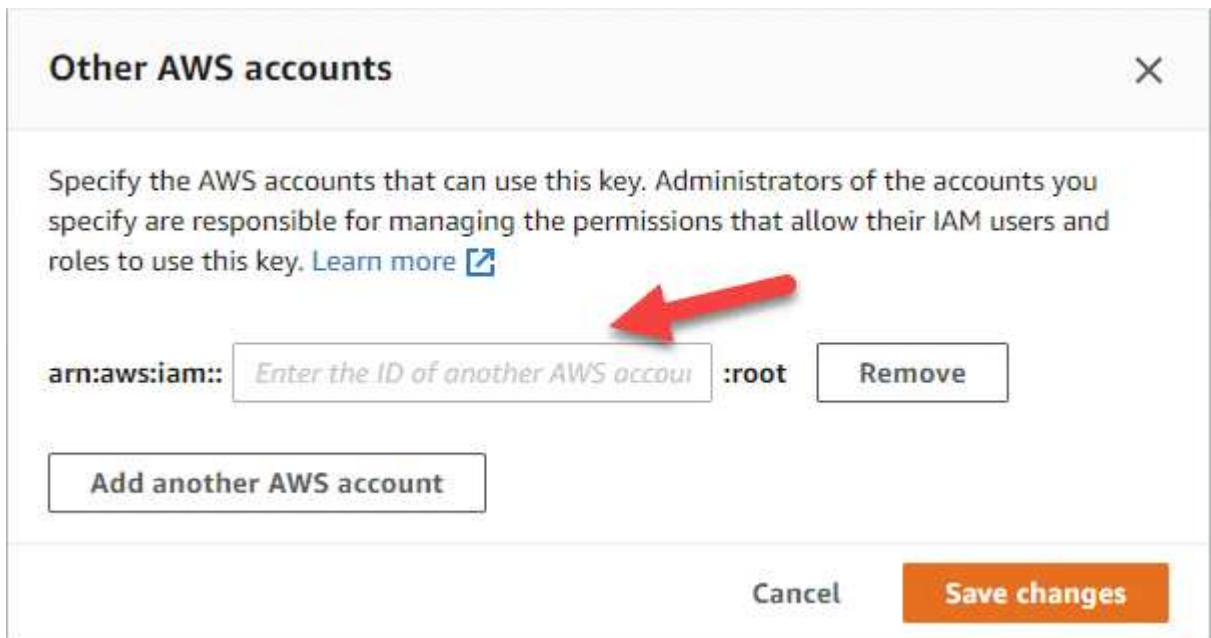
3. CMK가 다른 AWS 계정에 있는 경우 다음 단계를 수행하십시오.

- a. CMK가 상주하는 계정에서 KMS 콘솔로 이동합니다.
- b. 키를 선택합니다.
- c. General configuration * 창에서 키의 ARN을 복사합니다.

Cloud Volumes ONTAP 시스템을 생성할 때 클라우드 관리자에게 ARN을 제공해야 합니다.

- d. 다른 AWS 계정 * 창에서 Cloud Manager에 사용 권한을 제공하는 AWS 계정을 추가합니다.

대부분의 경우 Cloud Manager가 상주하는 계정입니다. Cloud Manager가 AWS에 설치되어 있지 않으면, Cloud Manager에 AWS 액세스 키를 제공한 계정이 될 수 있습니다.



- e. 이제 Cloud Manager에 사용 권한을 제공하는 AWS 계정으로 전환하고 IAM 콘솔을 엽니다.
- f. 아래에 나열된 권한을 포함하는 IAM 정책을 생성합니다.
- g. Cloud Manager에 권한을 제공하는 IAM 역할 또는 IAM 사용자에게 정책을 연결합니다.

다음 정책은 Cloud Manager가 외부 AWS 계정에서 CMK를 사용하는 데 필요한 권한을 제공합니다. "리소스" 섹션에서 지역 및 계정 ID를 수정해야 합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUseOfTheKey",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:externalaccountid:key/externalkeyid"
      ]
    },
    {
      "Sid": "AllowAttachmentOfPersistentResources",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:externalaccountid:key/externalaccountid"
      ],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}

```

+

이 프로세스에 대한 자세한 내용은 을 참조하십시오 ["AWS 설명서: 다른 계정의 사용자가 KMS 키를 사용할 수 있도록 허용합니다"](#).

4. 고객이 관리하는 CMK를 사용하는 경우 Cloud Volumes ONTAP IAM 역할을 _KEY USER_로 추가하여 CMK에 대한 주요 정책을 수정합니다.

이 단계는 Cloud Volumes ONTAP에서 데이터 계층화를 활성화한 경우 S3 버킷에 저장된 데이터를 암호화하려는 경우에 필요합니다.

작업 환경을 생성할 때 IAM 역할이 생성되므로 이 단계는 _After_ Cloud Volumes ONTAP를 구축해야 합니다. (물론 기존 Cloud Volumes ONTAP IAM 역할을 사용할 수 있는 옵션이 있으므로 이 단계를 이전에 수행할 수 있습니다.)

["AWS 설명서:키 편집"](#)

AWS에서 Cloud Volumes ONTAP 실행

Cloud Volumes ONTAP는 단일 시스템 구성에서 실행하거나 AWS에서 HA 쌍으로 실행할 수 있습니다.

시작하기 전에

작업 환경을 만들려면 다음이 필요합니다.

- 실행 중인 커넥터입니다.
 - 가 있어야 합니다 ["작업 영역과 연결된 커넥터입니다"](#).
 - ["항상 Connector를 실행 상태로 둘 준비가 되어 있어야 합니다"](#).
- 사용하려는 구성에 대한 이해.

구성을 선택하고 관리자로부터 AWS 네트워킹 정보를 받아 준비해야 합니다. 자세한 내용은 [을 참조하십시오 "Cloud Volumes ONTAP 구성 계획"](#).

- CIFS 구성을 위한 DNS 및 Active Directory

자세한 내용은 [을 참조하십시오 "AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항"](#).

- 작업 환경 추가 마법사에서 특정 라이선스 옵션을 선택하는 데 필요한 사항을 이해합니다. ["Cloud Volumes ONTAP 라이선스에 대해 자세히 알아보십시오"](#).

라이선스 옵션	요구 사항	요구 사항을 충족하는 방법
프리모늄	마켓플레이스 구독 또는 NSS(NetApp Support Site) 계정이 필요합니다.	세부 정보 및 자격 증명 * 페이지에서 클라우드 공급자의 마켓플레이스를 구독할 수 있습니다. 충전 방법 및 NSS 계정 * 페이지에서 NSS 계정을 입력할 수 있습니다.
Professional 또는 Essential 패키지	BYOL(Marketplace Subscription 또는 용량 기반 라이선스)이 필요합니다. 계정에 유효한 용량 기반 라이선스가 없거나 프로비저닝된 용량이 라이선스 용량을 초과하는 경우 용량 기반 충전을 위해 Marketplace 구독을 사용하는 것이 좋습니다.	세부 정보 및 자격 증명 * 페이지에서 클라우드 공급자의 마켓플레이스를 구독할 수 있습니다. NetApp에서 구매한 용량 기반 라이선스(BYOL)를 사용하려면 먼저 * Digital Wallet * 에 추가해야 합니다. "용량 기반 BYOL 라이선스를 추가하는 방법에 대해 알아보십시오" .

라이선스 옵션	요구 사항	요구 사항을 충족하는 방법
유연한 Keystone 구독	계정이 인증되어야 하며 Cloud Volumes ONTAP에서 사용할 수 있도록 구독을 활성화해야 합니다.	<p>a. mailto:ng-keystone-success@netapp.com [Contact NetApp]: 하나 이상의 Keystone Flex 구독으로 Cloud Manager 사용자 계정을 인증하십시오.</p> <p>b. NetApp이 사용자 계정을 승인한 후 "Cloud Volumes ONTAP에서 사용할 수 있도록 구독을 연결합니다".</p> <p>c. Cloud Volumes ONTAP HA 쌍을 생성할 때 Keystone 유연한 구독 충전 방법을 선택하십시오.</p>
노드당 라이선스	Marketplace 구독이 필요하거나 BYOL(Bring Your Own License)을 사용해야 합니다. 이 옵션은 기존 구독 또는 기존 라이선스를 보유한 고객에게 제공됩니다. 신규 고객은 사용할 수 없습니다.	NetApp에서 구매한 노드 기반 라이선스(BYOL)를 사용하려면 먼저 * Digital Wallet * 에 추가해야 합니다. "노드 기반 BYOL 라이선스를 추가하는 방법에 대해 알아보십시오" . 충전 방법 및 NSS 계정 * 페이지에서 NSS 계정을 입력할 수 있습니다.

AWS에서 단일 노드 Cloud Volumes ONTAP 시스템 시작

AWS에서 Cloud Volumes ONTAP를 시작하려면 Cloud Manager에서 새로운 작업 환경을 만들어야 합니다.

작업 환경을 생성한 직후 Cloud Manager는 지정된 VPC에서 테스트 인스턴스를 시작하여 연결을 확인합니다. 성공하면 Cloud Manager가 즉시 인스턴스를 종료한 다음 Cloud Volumes ONTAP 시스템 구축을 시작합니다. Cloud Manager에서 연결을 확인할 수 없는 경우 작업 환경을 생성하지 못합니다. 테스트 인스턴스는 T2.nano(기본 VPC 테넌시의 경우) 또는 m3.medium(전용 VPC 테넌시의 경우)입니다.

단계

1. Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 화면의 지시를 따릅니다.
2. * 위치 선택 *: * 아마존 웹 서비스 * 및 * Cloud Volumes ONTAP 단일 노드 * 를 선택합니다.
3. 메시지가 표시되면 ["커넥터를 작성합니다"](#).
4. * 세부 정보 및 자격 증명 *: AWS 자격 증명과 구독을 선택적으로 변경하고, 작업 환경 이름을 입력하고, 필요한 경우 태그를 추가한 다음 암호를 입력합니다.

이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
작업 환경 이름	Cloud Manager에서는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Amazon EC2 인스턴스 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.

필드에 입력합니다	설명
태그 추가	AWS 태그는 AWS 리소스에 대한 메타데이터입니다. Cloud Manager에서 Cloud Volumes ONTAP 인스턴스와 해당 인스턴스에 연결된 각 AWS 리소스에 태그를 추가합니다. 작업 환경을 만들 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 생성된 후에는 더 많은 태그를 추가할 수 있습니다. API는 작업 환경을 생성할 때 태그를 4개로 제한하지 않습니다. 태그에 대한 자세한 내용은 을 참조하십시오 " AWS 문서: Amazon EC2 리소스에 태그 달기 ".
사용자 이름 및 암호	Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하여 System Manager 또는 CLI를 통해 Cloud Volumes ONTAP에 연결할 수 있습니다. default_admin_user 이름을 유지하거나 사용자 지정 사용자 이름으로 변경합니다.
자격 증명 편집	이 시스템을 구축할 계정과 연결된 AWS 자격 증명을 선택합니다. AWS Marketplace 구독을 연결하여 이 Cloud Volumes ONTAP 시스템에 사용할 수도 있습니다. 선택한 자격 증명을 새 AWS Marketplace 구독에 연결하려면 * Add Subscription * 을 클릭합니다. 이 구독은 연간 계약을 기준으로 하거나 시간당 요금로 Cloud Volumes ONTAP에 대한 비용을 지불할 수 있습니다. https://docs.netapp.com/us-en/cloud-manager-setup-admin/task-adding-aws-accounts.html ["Cloud Manager에 AWS 자격 증명을 추가하는 방법에 대해 알아보십시오"^].

다음 비디오에서는 용량제 마켓플레이스 구독을 AWS 자격 증명에 연결하는 방법을 보여줍니다.

▶ https://docs.netapp.com/ko-kr/cloud-manager-cloud-volumes-ontap//media/video_subscribing_aws.mp4

(video)

여러 IAM 사용자가 동일한 AWS 계정으로 작업하는 경우 각 사용자는 가입해야 합니다. 첫 번째 사용자가 구독한 후 AWS Marketplace는 아래 이미지에 표시된 것처럼 후속 사용자에게 이미 구독했음을 알립니다. AWS_ACCOUNT에 가입되어 있는 동안 각 IAM 사용자는 자신을 해당 구독과 연결해야 합니다. 아래 메시지가 표시되면 *여기를 클릭* 링크를 클릭하여 Cloud Central로 이동하여 프로세스를 완료하십시오



Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

Having issues signing up for your product?

If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

[Subscribe](#)

You are already subscribed to this product

Pricing Details

Software Fees

5. * 서비스 *: Cloud Volumes ONTAP에서 사용하지 않을 개별 서비스를 활성화 또는 비활성화합니다.

- "클라우드 데이터 센스에 대해 자세히 알아보십시오".
- "Cloud Backup에 대해 자세히 알아보십시오".
- "모니터링에 대해 자세히 알아보십시오".

6. * 위치 및 연결 *: 에 기록한 네트워크 정보를 입력합니다 "AWS 워크시트".

AWS 아웃포스트가 있는 경우 아웃포스트 VPC를 선택하여 해당 아웃포스트에 단일 노드 Cloud Volumes ONTAP 시스템을 구축할 수 있습니다. 이러한 경험은 AWS에 상주하는 다른 VPC와 동일합니다.

다음 이미지는 페이지가 채워진 상태를 보여줍니다.

Location	Connectivity
AWS Region US West Oregon	Security Group <input checked="" type="radio"/> Generated security group <input type="radio"/> Use existing security group
VPC vpc-3a01e05f - 172.31.0.0/16	SSH Authentication Method <input checked="" type="radio"/> Password <input type="radio"/> Key Pair
Subnet 172.31.5.0/24 (OCCM subnet)	

7. * 데이터 암호화 *: 데이터 암호화 또는 AWS로 관리되는 암호화를 선택하지 않습니다.

AWS로 관리되는 암호화의 경우 사용자 계정 또는 다른 AWS 계정에서 다른 CMK(Customer Master Key)를 선택할 수 있습니다.



Cloud Volumes ONTAP 시스템을 생성한 후에는 AWS 데이터 암호화 방법을 변경할 수 없습니다.

"Cloud Volumes ONTAP용 AWS KMS를 설정하는 방법에 대해 알아보십시오".

"지원되는 암호화 기술에 대해 자세히 알아보십시오".

8. * 충전 방법 및 NSS 계정 *: 이 시스템에서 사용할 충전 옵션을 지정한 다음 NetApp Support 사이트 계정을 지정합니다.

- "이러한 충전 방법에 대해 자세히 알아보십시오".
- "마법사에서 사용하려는 라이선스 방법에 필요한 사항을 알아봅니다."

9. * Cloud Volumes ONTAP 구성 * (연간 AWS 마켓플레이스 계약만 해당): 기본 구성을 검토하고 * 계속 * 을 클릭하거나 * 구성 변경 * 을 클릭하여 원하는 구성을 선택합니다.

기본 구성을 유지하는 경우 볼륨을 지정한 다음 구성을 검토 및 승인하기만 하면 됩니다.

10. * 사전 구성된 패키지 * (시간별 또는 BYOL 전용): Cloud Volumes ONTAP를 빠르게 시작하려면 패키지 중 하나를 선택하고, 원하는 구성을 선택하려면 * 구성 변경 * 을 클릭합니다.

패키지 중 하나를 선택하는 경우 볼륨을 지정한 다음 구성을 검토 및 승인하기만 하면 됩니다.

11. * IAM Role *: Cloud Manager가 역할을 생성할 수 있도록 기본 옵션을 유지하는 것이 가장 좋습니다.

자체 정책을 사용하려면 이 정책이 충족해야 합니다 "Cloud Volumes ONTAP 노드의 정책 요구사항".

12. * 라이선스 *: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 라이선스, 인스턴스 유형 및 인스턴스 테넌시를 선택합니다.

인스턴스를 시작한 후 필요한 사항이 변경되면 나중에 라이선스 또는 인스턴스 유형을 수정할 수 있습니다.



선택한 버전에 대해 새로운 출시 후보, 일반 가용성 또는 패치 릴리스를 사용할 수 있는 경우, Cloud Manager는 작업 환경을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.6 RC1 및 9.6 GA를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리즈에서 다른 릴리즈로 발생하지 않습니다(예: 9.6에서 9.7로).

13. * 기본 스토리지 리소스 *: 초기 애그리게이트의 설정(디스크 유형, 각 디스크의 크기, 데이터 계층화 활성화 여부)을 선택합니다.

다음 사항에 유의하십시오.

- 디스크 유형은 초기 볼륨입니다. 이후 볼륨에 대해 다른 디스크 유형을 선택할 수 있습니다.
- 디스크 크기는 초기 애그리게이트의 모든 디스크와 단순 프로비저닝 옵션을 사용할 때 Cloud Manager가 생성하는 추가 애그리게이트의 경우 모두 사용됩니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.

디스크 유형과 크기를 선택하는 방법은 을 참조하십시오 ["AWS에서 시스템 사이징"](#).

- 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
- 데이터 계층화를 사용하지 않는 경우, 후속 애그리게이트에서 이 기능을 사용하도록 설정할 수 있습니다.

["데이터 계층화의 작동 방식에 대해 알아보십시오"](#).

14. * 쓰기 속도 및 WORM *: * 일반 * 또는 * 고속 * 쓰기 속도를 선택하고 필요한 경우 WORM(Write Once, Read Many) 스토리지를 활성화합니다.

["쓰기 속도에 대해 자세히 알아보십시오"](#).

Cloud Backup이 활성화되었거나 데이터 계층화가 활성화된 경우 WORM을 설정할 수 없습니다.

["WORM 스토리지에 대해 자세히 알아보십시오"](#).

15. * 볼륨 생성 *: 새 볼륨에 대한 세부 정보를 입력하거나 * 건너뛰기 * 를 클릭합니다.

["지원되는 클라이언트 프로토콜 및 버전에 대해 알아보십시오"](#).

이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
크기	입력할 수 있는 최대 크기는 썬 프로비저닝의 사용 여부에 따라 크게 달라집니다. 이를 통해 현재 사용 가능한 물리적 스토리지보다 더 큰 볼륨을 생성할 수 있습니다.
액세스 제어(NFS에만 해당)	엑스포트 정책은 볼륨에 액세스할 수 있는 서버넷의 클라이언트를 정의합니다. 기본적으로 Cloud Manager는 서버넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS 전용)	이러한 필드를 사용하면 사용자 및 그룹의 공유에 대한 액세스 수준(액세스 제어 목록 또는 ACL라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자 또는 그룹, UNIX 사용자 또는 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자의 도메인을 포함해야 합니다.
스냅샷 정책	스냅샷 복사본 정책은 자동으로 생성되는 NetApp 스냅샷 복사본의 수와 빈도를 지정합니다. NetApp 스냅샷 복사본은 성능 영향이 없고 최소한의 스토리지가 필요한 시점 파일 시스템 이미지입니다. 기본 정책을 선택하거나 선택하지 않을 수 있습니다. Microsoft SQL Server의 tempdb와 같이 임시 데이터에 대해 없음을 선택할 수 있습니다.
고급 옵션(NFS에만 해당)	볼륨의 NFS 버전 선택: NFSv3 또는 NFSv4

필드에 입력합니다	설명
이니시에이터 그룹 및 IQN(iSCSI 전용)	iSCSI 스토리지 타겟을 LUN(논리 유닛)이라고 하며 호스트에 표준 블록 디바이스로 표시됩니다. 이니시에이터 그룹은 iSCSI 호스트 노드 이름의 테이블이며 어떤 이니시에이터가 어떤 LUN을 액세스할 수 있는지 제어합니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 통합 네트워크 어댑터(CNA) 또는 전용 호스트 파스트 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 공인 이름(IQN)으로 식별됩니다. iSCSI 볼륨을 생성할 때 Cloud Manager에서 자동으로 LUN을 생성합니다. 볼륨 당 하나의 LUN만 생성하므로 관리가 필요 없습니다. 볼륨을 생성한 후 "IQN을 사용하여 호스트에서 LUN에 연결합니다" .

다음 이미지는 CIFS 프로토콜에 대해 작성된 볼륨 페이지를 보여 줍니다.

Volume Details, Protection & Protocol

Details & Protection

Volume Name:

Size (GB):

Snapshot Policy:

default

Default Policy

Protocol

NFS
CIFS
iSCSI

Share name:

Permissions:

Full Control

Users / Groups:

Valid users and groups separated by a semicolon

16. * CIFS 설정 *: CIFS 프로토콜을 선택한 경우 CIFS 서버를 설정합니다.

필드에 입력합니다	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
연결할 Active Directory 도메인입니다	CIFS 서버를 연결할 AD(Active Directory) 도메인의 FQDN입니다.
도메인에 가입하도록 승인된 자격 증명입니다	AD 도메인 내의 지정된 OU(조직 구성 단위)에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름 및 암호입니다.
CIFS 서버 NetBIOS 이름입니다	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 구성 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. AWS 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하는 경우 이 필드에 * OU=Computers, OU=Corp * 를 입력해야 합니다.
DNS 도메인	SVM(Cloud Volumes ONTAP 스토리지 가상 머신)용 DNS 도메인 대부분의 경우 도메인은 AD 도메인과 동일합니다.

필드에 입력합니다	설명
NTP 서버	Active Directory DNS를 사용하여 NTP 서버를 구성하려면 * Active Directory 도메인 사용 * 을 선택합니다. 다른 주소를 사용하여 NTP 서버를 구성해야 하는 경우 API를 사용해야 합니다. 를 참조하십시오 "Cloud Manager 자동화 문서" 를 참조하십시오. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 생성한 후에는 구성할 수 없습니다.

17. * Usage Profile, Disk Type 및 Tiering Policy *: 스토리지 효율성 기능을 사용하도록 설정하고 필요한 경우 볼륨 계층화 정책을 편집할지 여부를 선택합니다.

자세한 내용은 을 참조하십시오 ["볼륨 사용 프로필 이해"](#) 및 ["데이터 계층화 개요"](#).

18. * 검토 및 승인 *: 선택 사항을 검토 및 확인합니다.
- 구성에 대한 세부 정보를 검토합니다.
 - Cloud Manager가 구매할 지원 및 AWS 리소스에 대한 세부 정보를 검토하려면 * 자세한 정보 * 를 클릭합니다.
 - 이해함... * 확인란을 선택합니다.
 - Go * 를 클릭합니다.

Cloud Manager가 Cloud Volumes ONTAP 인스턴스를 시작합니다. 타임라인에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 인스턴스를 시작하는 데 문제가 있는 경우 실패 메시지를 검토합니다. 작업 환경을 선택하고 환경 다시 생성 을 클릭할 수도 있습니다.

자세한 내용은 를 참조하십시오 ["NetApp Cloud Volumes ONTAP 지원"](#).

작업을 마친 후

- CIFS 공유를 프로비저닝한 경우 파일 및 폴더에 대한 사용자 또는 그룹 권한을 제공하고 해당 사용자가 공유를 액세스하고 파일을 생성할 수 있는지 확인합니다.
- 볼륨에 할당량을 적용하려면 System Manager 또는 CLI를 사용하십시오.

할당량을 사용하면 사용자, 그룹 또는 qtree가 사용하는 파일 수와 디스크 공간을 제한하거나 추적할 수 있습니다.

AWS에서 Cloud Volumes ONTAP HA 쌍 시작

AWS에서 Cloud Volumes ONTAP HA 쌍을 실행하려면 Cloud Manager에서 HA 작업 환경을 만들어야 합니다.

현재 HA 쌍은 AWS 아웃포스트에서 지원되지 않습니다.

작업 환경을 생성한 직후 Cloud Manager는 지정된 VPC에서 테스트 인스턴스를 시작하여 연결을 확인합니다. 성공하면 Cloud Manager가 즉시 인스턴스를 종료한 다음 Cloud Volumes ONTAP 시스템 구축을 시작합니다. Cloud Manager에서 연결을 확인할 수 없는 경우 작업 환경을 생성하지 못합니다. 테스트 인스턴스는 T2.nano(기본 VPC 테넌시의 경우) 또는 m3.medium(전용 VPC 테넌시의 경우)입니다.

단계

- Canvas 페이지에서 * 작업 환경 추가 * 를 클릭하고 화면의 지시를 따릅니다.
- * 위치 선택 *: * 아마존 웹 서비스 * 및 * Cloud Volumes ONTAP 단일 노드 * 를 선택합니다.
- * 세부 정보 및 자격 증명 *: AWS 자격 증명과 구독을 선택적으로 변경하고, 작업 환경 이름을 입력하고, 필요한

경우 태그를 추가한 다음 암호를 입력합니다.

이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
작업 환경 이름	Cloud Manager에서는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Amazon EC2 인스턴스 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.
태그 추가	AWS 태그는 AWS 리소스에 대한 메타데이터입니다. Cloud Manager에서 Cloud Volumes ONTAP 인스턴스와 해당 인스턴스에 연결된 각 AWS 리소스에 태그를 추가합니다. 작업 환경을 만들 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 생성된 후에는 더 많은 태그를 추가할 수 있습니다. API는 작업 환경을 생성할 때 태그를 4개로 제한하지 않습니다. 태그에 대한 자세한 내용은 을 참조하십시오 " AWS 문서: Amazon EC2 리소스에 태그 달기 ".
사용자 이름 및 암호	Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하여 System Manager 또는 CLI를 통해 Cloud Volumes ONTAP에 연결할 수 있습니다. default_admin_user 이름을 유지하거나 사용자 지정 사용자 이름으로 변경합니다.
자격 증명 편집	이 Cloud Volumes ONTAP 시스템에서 사용할 AWS 자격 증명과 마켓플레이스 구독을 선택하십시오. 선택한 자격 증명을 새 AWS Marketplace 구독에 연결하려면 * Add Subscription * 을 클릭합니다. 이 구독은 연간 계약을 기준으로 하거나 시간당 요금으로 Cloud Volumes ONTAP에 대한 비용을 지불할 수 있습니다. NetApp(BYOL)에서 직접 라이선스를 구입한 경우에는 AWS 가입이 필요하지 않습니다. https://docs.netapp.com/us-en/cloud-manager-setup-admin/task-adding-aws-accounts.html ["Cloud Manager에 AWS 자격 증명을 추가하는 방법에 대해 알아보십시오"]].

다음 비디오에서는 용량제 마켓플레이스 구독을 AWS 자격 증명에 연결하는 방법을 보여줍니다.

► https://docs.netapp.com/ko-kr/cloud-manager-cloud-volumes-ontap//media/video_subscribing_aws.mp4

(video)

여러 IAM 사용자가 동일한 AWS 계정으로 작업하는 경우 각 사용자는 가입해야 합니다. 첫 번째 사용자가 구독한 후 AWS Marketplace는 아래 이미지에 표시된 것처럼 후속 사용자에게 이미 구독했음을 알립니다. AWS_ACCOUNT에 가입되어 있는 동안 각 IAM 사용자는 자신을 해당 구독과 연결해야 합니다. 아래 메시지가 표시되면 *여기를 클릭* 링크를 클릭하여 Cloud Central로 이동하여 프로세스를 완료하십시오



Cloud Manager (for Cloud Volumes ONTAP)

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.



Having issues signing up for your product?

If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

Subscribe

You are already subscribed to this product

Pricing Details

Software Fees

4. * 서비스 *: 이 Cloud Volumes ONTAP 시스템에서 사용하지 않을 개별 서비스를 활성화 또는 비활성화합니다.

- "클라우드 데이터 센스에 대해 자세히 알아보십시오".
- "Cloud Backup에 대해 자세히 알아보십시오".
- "모니터링에 대해 자세히 알아보십시오".

5. * HA 배포 모델 *: HA 구성을 선택합니다.

배포 모델에 대한 개요는 을 참조하십시오 "AWS용 Cloud Volumes ONTAP HA".

6. * 지역 및 VPC *: AWS 워크시트에 기록한 네트워크 정보를 입력합니다.

다음 이미지는 다중 AZ 구성에 대해 작성된 페이지를 보여줍니다.

Region & VPC

AWS Region

US East | N. Virginia

VPC

vpc-a76d91c2 - 172.31.0.0/16

Security group

Use a generated security group

Node 1:

Availability Zone

us-east-1a

Subnet

172.31.8.0/24

Node 2:

Availability Zone

us-east-1b

Subnet

172.31.9.0/24

Mediator:

Availability Zone

us-east-1c

Subnet

172.31.2.0/24

7. * 연결 및 SSH 인증 *: HA 쌍선 및 중재자의 연결 방법을 선택합니다.

8. * 부동 IP *: 여러 AZs를 선택한 경우 부동 IP 주소를 지정합니다.

IP 주소는 해당 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 합니다. 자세한 내용은 을 참조하십시오 ["여러 AZs에서 Cloud Volumes ONTAP HA를 위한 AWS 네트워킹 요구사항"](#).

9. * 루트 테이블 *: 여러 AZs를 선택한 경우 부동 IP 주소에 대한 라우트를 포함해야 하는 라우팅 테이블을 선택합니다.

둘 이상의 라우팅 테이블이 있는 경우 올바른 라우팅 테이블을 선택하는 것이 매우 중요합니다. 그렇지 않으면 일부 클라이언트가 Cloud Volumes ONTAP HA 쌍에 액세스하지 못할 수 있습니다. 라우팅 테이블에 대한 자세한 내용은 을 참조하십시오 ["AWS 설명서: 경로 테이블"](#).

10. * 데이터 암호화 *: 데이터 암호화 또는 AWS로 관리되는 암호화를 선택하지 않습니다.

AWS로 관리되는 암호화의 경우 사용자 계정 또는 다른 AWS 계정에서 다른 CMK(Customer Master Key)를 선택할 수 있습니다.



Cloud Volumes ONTAP 시스템을 생성한 후에는 AWS 데이터 암호화 방법을 변경할 수 없습니다.

["Cloud Volumes ONTAP용 AWS KMS를 설정하는 방법에 대해 알아보십시오"](#).

["지원되는 암호화 기술에 대해 자세히 알아보십시오"](#).

11. * 충전 방법 및 NSS 계정 *: 이 시스템에서 사용할 충전 옵션을 지정한 다음 NetApp Support 사이트 계정을 지정합니다.

◦ ["이러한 충전 방법에 대해 자세히 알아보십시오"](#).

◦ ["마법사에서 사용하려는 라이선스 방법에 필요한 사항을 알아봅니다"](#).

12. * Cloud Volumes ONTAP 구성 * (연간 AWS 마켓플레이스 계약만 해당): 기본 구성을 검토하고 * 계속 * 을 클릭하거나 * 구성 변경 * 을 클릭하여 원하는 구성을 선택합니다.

기본 구성을 유지하는 경우 볼륨을 지정한 다음 구성을 검토 및 승인하기만 하면 됩니다.

13. * 사전 구성된 패키지 * (시간별 또는 BYOL 전용): Cloud Volumes ONTAP를 빠르게 시작하려면 패키지 중 하나를 선택하고, 원하는 구성을 선택하려면 * 구성 변경 * 을 클릭합니다.

패키지 중 하나를 선택하는 경우 볼륨을 지정한 다음 구성을 검토 및 승인하기만 하면 됩니다.

14. * IAM Role *: Cloud Manager가 역할을 생성할 수 있도록 기본 옵션을 유지하는 것이 가장 좋습니다.

자체 정책을 사용하려면 이 정책이 충족해야 합니다 ["Cloud Volumes ONTAP 노드 및 HA 중재자의 정책 요구사항"](#).

15. * 라이선스 *: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 라이선스, 인스턴스 유형 및 인스턴스 테넌시를 선택합니다.



인스턴스를 시작한 후 요구 사항이 변경되는 경우 나중에 라이선스 또는 인스턴스 유형을 수정할 수 있습니다.



선택한 버전에 대해 새로운 출시 후보, 일반 가용성 또는 패치 릴리스를 사용할 수 있는 경우, Cloud Manager는 작업 환경을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.6 RC1 및 9.6 GA를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리즈에서 다른 릴리즈로 발생하지 않습니다(예: 9.6에서 9.7로).

16. * 기본 스토리지 리소스 *: 초기 애그리게이트의 설정(디스크 유형, 각 디스크의 크기, 데이터 계층화 활성화 여부)을 선택합니다.

다음 사항에 유의하십시오.

- 디스크 유형은 초기 볼륨입니다. 이후 볼륨에 대해 다른 디스크 유형을 선택할 수 있습니다.
- 디스크 크기는 초기 애그리게이트의 모든 디스크와 단순 프로비저닝 옵션을 사용할 때 Cloud Manager가 생성하는 추가 애그리게이트의 경우 모두 사용됩니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.

디스크 유형과 크기를 선택하는 방법은 을 참조하십시오 ["AWS에서 시스템 사이징"](#).

- 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
- 데이터 계층화를 사용하지 않는 경우, 후속 애그리게이트에서 이 기능을 사용하도록 설정할 수 있습니다.

["데이터 계층화의 작동 방식에 대해 알아보십시오"](#).

17. * 쓰기 속도 및 WORM *: * 일반 * 또는 * 고속 * 쓰기 속도를 선택하고 필요한 경우 WORM(Write Once, Read Many) 스토리지를 활성화합니다.

["쓰기 속도에 대해 자세히 알아보십시오"](#).

Cloud Backup이 활성화되었거나 데이터 계층화가 활성화된 경우 WORM을 설정할 수 없습니다.

["WORM 스토리지에 대해 자세히 알아보십시오"](#).

18. * 볼륨 생성 *: 새 볼륨에 대한 세부 정보를 입력하거나 * 건너뛰기 * 를 클릭합니다.

["지원되는 클라이언트 프로토콜 및 버전에 대해 알아보십시오"](#).

이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
크기	입력할 수 있는 최대 크기는 썸 프로비저닝의 사용 여부에 따라 크게 달라집니다. 이를 통해 현재 사용 가능한 물리적 스토리지보다 더 큰 볼륨을 생성할 수 있습니다.
액세스 제어(NFS에만 해당)	엑스포트 정책은 볼륨에 액세스할 수 있는 서버넷의 클라이언트를 정의합니다. 기본적으로 Cloud Manager는 서버넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS 전용)	이러한 필드를 사용하면 사용자 및 그룹의 공유에 대한 액세스 수준(액세스 제어 목록 또는 ACL라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자 또는 그룹, UNIX 사용자 또는 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자의 도메인을 포함해야 합니다.
스냅샷 정책	스냅샷 복사본 정책은 자동으로 생성되는 NetApp 스냅샷 복사본의 수와 빈도를 지정합니다. NetApp 스냅샷 복사본은 성능 영향이 없고 최소한의 스토리지가 필요한 시점 파일 시스템 이미지입니다. 기본 정책을 선택하거나 선택하지 않을 수 있습니다. Microsoft SQL Server의 tempdb와 같이 임시 데이터에 대해 없음을 선택할 수 있습니다.
고급 옵션(NFS에만 해당)	볼륨의 NFS 버전 선택: NFSv3 또는 NFSv4
이니시에이터 그룹 및 IQN(iSCSI 전용)	iSCSI 스토리지 타겟을 LUN(논리 유닛)이라고 하며 호스트에 표준 블록 디바이스로 표시됩니다. 이니시에이터 그룹은 iSCSI 호스트 노드 이름의 테이블이며 어떤 이니시에이터가 어떤 LUN을 액세스할 수 있는지 제어합니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 통합 네트워크 어댑터(CNA) 또는 전용 호스트 파스트 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 공인 이름(IQN)으로 식별됩니다. iSCSI 볼륨을 생성할 때 Cloud Manager에서 자동으로 LUN을 생성합니다. 볼륨 당 하나의 LUN만 생성하므로 관리가 필요 없습니다. 볼륨을 생성한 후 "IQN을 사용하여 호스트에서 LUN에 연결합니다" .

다음 이미지는 CIFS 프로토콜에 대해 작성된 볼륨 페이지를 보여 줍니다.

Volume Details, Protection & Protocol

Details & Protection

Volume Name: Size (GB):

Snapshot Policy:

Default Policy

Protocol

NFS **CIFS** iSCSI

Share name: Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

19. * CIFS 설정 *: CIFS 프로토콜을 선택한 경우 CIFS 서버를 설정합니다.

필드에 입력합니다	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
연결할 Active Directory 도메인입니다	CIFS 서버를 연결할 AD(Active Directory) 도메인의 FQDN입니다.
도메인에 가입하도록 승인된 자격 증명입니다	AD 도메인 내의 지정된 OU(조직 구성 단위)에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름 및 암호입니다.
CIFS 서버 NetBIOS 이름입니다	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 구성 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. AWS 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하는 경우 이 필드에 * OU=Computers, OU=Corp * 를 입력해야 합니다.
DNS 도메인	SVM(Cloud Volumes ONTAP 스토리지 가상 머신)용 DNS 도메인 대부분의 경우 도메인은 AD 도메인과 동일합니다.
NTP 서버	Active Directory DNS를 사용하여 NTP 서버를 구성하려면 * Active Directory 도메인 사용 * 을 선택합니다. 다른 주소를 사용하여 NTP 서버를 구성해야 하는 경우 API를 사용해야 합니다. 를 참조하십시오 "Cloud Manager 자동화 문서" 를 참조하십시오. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 생성한 후에는 구성할 수 없습니다.

20. * Usage Profile, Disk Type 및 Tiering Policy *: 스토리지 효율성 기능을 사용하도록 설정하고 필요한 경우 볼륨 계층화 정책을 편집할지 여부를 선택합니다.

자세한 내용은 을 참조하십시오 ["볼륨 사용 프로필 이해"](#) 및 ["데이터 계층화 개요"](#).

21. * 검토 및 승인 *: 선택 사항을 검토 및 확인합니다.
- 구성에 대한 세부 정보를 검토합니다.
 - Cloud Manager가 구매할 지원 및 AWS 리소스에 대한 세부 정보를 검토하려면 * 자세한 정보 * 를 클릭합니다.
 - 이해함... * 확인란을 선택합니다.
 - Go * 를 클릭합니다.

Cloud Manager가 Cloud Volumes ONTAP HA 쌍을 시작합니다. 타임라인에서 진행 상황을 추적할 수 있습니다.

HA 쌍 실행에 문제가 있는 경우 장애 메시지를 검토하십시오. 작업 환경을 선택하고 환경 다시 생성 을 클릭할 수도 있습니다.

자세한 내용은 를 참조하십시오 ["NetApp Cloud Volumes ONTAP 지원"](#).

작업을 마친 후

- CIFS 공유를 프로비저닝한 경우 파일 및 폴더에 대한 사용자 또는 그룹 권한을 제공하고 해당 사용자가 공유를 액세스하고 파일을 생성할 수 있는지 확인합니다.
- 볼륨에 할당량을 적용하려면 System Manager 또는 CLI를 사용하십시오.

할당량을 사용하면 사용자, 그룹 또는 qtree가 사용하는 파일 수와 디스크 공간을 제한하거나 추적할 수 있습니다.

AWS C2S 환경에서 Cloud Volumes ONTAP를 시작하십시오

표준 AWS 지역과 마찬가지로, 에서 Cloud Manager를 사용할 수 있습니다 "[AWS C2S\(Commercial Cloud Services\)](#)" 구축할 환경: 클라우드 스토리지에 엔터프라이즈급 기능을 제공하는 Cloud Volumes ONTAP AWS C2S는 미국 고유의 폐쇄된 지역입니다 Intelligence Community - 이 페이지의 지침은 AWS C2S 지역 사용자에게만 적용됩니다.

C2S에서 지원되는 기능

C2S 환경의 Cloud Manager에서 사용할 수 있는 기능은 다음과 같습니다.

- Cloud Volumes ONTAP
- 데이터 복제
- 감사 시간 표시 막대입니다

Cloud Volumes ONTAP의 경우 단일 노드 시스템 또는 HA 쌍을 생성할 수 있습니다. 두 가지 라이선스 옵션 모두 사용 가능: 용량제 및 BYOL(Bring Your Own License)

C2S의 Cloud Volumes ONTAP에서는 S3에 대한 데이터 계층화도 지원됩니다.

제한 사항

Cloud Manager에서 제공되는 NetApp 클라우드 서비스가 없습니다.

C2S 환경에는 인터넷 액세스가 없으므로 다음 기능을 사용할 수 없습니다.

- NetApp Cloud Central과 통합
- Cloud Manager에서 소프트웨어 업그레이드 자동화
- NetApp AutoSupport를 참조하십시오
- Cloud Volumes ONTAP 리소스에 대한 AWS 비용 정보입니다

구축 개요

C2S에서 Cloud Volumes ONTAP 시작하기에는 몇 가지 단계가 포함되어 있습니다.

1. AWS 환경 준비

여기에는 네트워킹 설정, Cloud Volumes ONTAP 가입, 권한 설정 및 AWS KMS 설정 옵션이 포함됩니다.

2. Connector 설치 및 Cloud Manager 설정

Cloud Manager를 사용하여 Cloud Volumes ONTAP를 구축하기 전에 _Connector_를 작성해야 합니다. Connector를 사용하면 Cloud Manager에서 퍼블릭 클라우드 환경(Cloud Volumes ONTAP 포함)의 리소스와 프로세스를 관리할 수 있습니다.

Connector 인스턴스에 설치되는 소프트웨어에서 Cloud Manager에 로그인합니다.

3. Cloud Manager에서 Cloud Volumes ONTAP 실행:

이러한 각 단계는 아래에 설명되어 있습니다.

AWS 환경을 준비하십시오

AWS 환경은 몇 가지 요구사항을 충족해야 합니다.

네트워크 설정

Cloud Volumes ONTAP가 제대로 작동할 수 있도록 AWS 네트워킹을 설정합니다.

단계

1. 커넥터 인스턴스 및 Cloud Volumes ONTAP 인스턴스를 시작할 VPC 및 서브넷을 선택합니다.
2. VPC와 서브넷이 커넥터와 Cloud Volumes ONTAP 간의 연결을 지원하는지 확인합니다.
3. VPC 엔드포인트를 S3 서비스로 설정합니다.

Cloud Volumes ONTAP의 콜드 데이터를 저비용 오브젝트 스토리지로 계층화하려는 경우 VPC 엔드포인트가 필요합니다.

Cloud Volumes ONTAP에 가입하십시오

Cloud Manager에서 Cloud Volumes ONTAP를 구축하려면 Marketplace에 가입해야 합니다.

단계

1. AWS 인텔리전스 커뮤니티 마켓플레이스로 이동하여 Cloud Volumes ONTAP를 검색합니다.
2. 구축할 오퍼링을 선택합니다.
3. 약관을 검토하고 * Accept * (수락 *)를 클릭합니다.
4. 다른 서비스를 배포하려는 경우 해당 서비스에 대해 이 단계를 반복합니다.

Cloud Volumes ONTAP 인스턴스를 시작하려면 Cloud Manager를 사용해야 합니다. EC2 콘솔에서 Cloud Volumes ONTAP 인스턴스를 시작하면 안 됩니다.

권한 설정

AWS 상용 클라우드 서비스 환경에서 작업을 수행하는 데 필요한 권한을 Cloud Manager 및 Cloud Volumes ONTAP에 제공하는 IAM 정책 및 역할을 설정합니다.

다음 각 항목에 대해 IAM 정책 및 IAM 역할이 필요합니다.

- 커넥터 인스턴스
- Cloud Volumes ONTAP 인스턴스
- Cloud Volumes ONTAP HA 중재자 인스턴스(HA 쌍을 구축하려는 경우)

단계

1. AWS IAM 콘솔로 이동하여 * Policies * 를 클릭합니다.
2. Connector 인스턴스에 대한 정책을 만듭니다.



```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:DescribeRouteTables",
      "ec2:DescribeImages",
      "ec2:CreateTags",
      "ec2:CreateVolume",
      "ec2:DescribeVolumes",
      "ec2:ModifyVolumeAttribute",
      "ec2>DeleteVolume",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2>DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeDhcpOptions",
      "ec2:CreateSnapshot",
      "ec2>DeleteSnapshot",
      "ec2:DescribeSnapshots",
      "ec2:GetConsoleOutput",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeRegions",
      "ec2>DeleteTags",
      "ec2:DescribeTags",
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents",
      "cloudformation:ValidateTemplate",
      "iam:PassRole",
      "iam:CreateRole",
      "iam>DeleteRole",

```

```

        "iam:PutRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "kms:List*",
        "kms:Describe*",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2>DeletePlacementGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
    ],
    "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],

```

```

        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Resource": [
            "arn:aws-iso:ec2:*:*:instance/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws-iso:ec2:*:*:volume/*"
        ]
    }
]
}

```

3. Cloud Volumes ONTAP에 대한 정책을 생성합니다.


```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-iso:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}

```

4. Cloud Volumes ONTAP HA 쌍을 구축하려는 경우 HA 종재자를 위한 정책을 생성합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AssignPrivateIpAddresses",
      "ec2:CreateRoute",
      "ec2>DeleteRoute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeVpcs",
      "ec2:ReplaceRoute",
      "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource": "*"
  }]
}

```

5. Amazon EC2 역할 유형으로 IAM 역할을 생성하고 이전 단계에서 생성한 정책을 첨부합니다.

정책과 마찬가지로, Connector에 IAM 역할 1개, Cloud Volumes ONTAP 노드에 대해 1개, HA 중재자를 위한 IAM 역할 1개가 있어야 합니다(HA 쌍을 구축하려는 경우).

Connector 인스턴스를 실행할 때 Connector IAM 역할을 선택해야 합니다.

Cloud Manager에서 Cloud Volumes ONTAP 작업 환경을 생성할 때 Cloud Volumes ONTAP의 IAM 역할과 HA 중재자를 선택할 수 있습니다.

AWS KMS를 설정합니다

Cloud Volumes ONTAP에서 Amazon 암호화를 사용하려면 AWS 키 관리 서비스에 대한 요구 사항이 충족되는지 확인합니다.

단계

1. 사용자 계정 또는 다른 AWS 계정에 활성 CMK(Customer Master Key)가 있는지 확인합니다.

CMK는 AWS로 관리되는 CMK 또는 고객이 관리하는 CMK가 될 수 있습니다.

2. CMK가 Cloud Volumes ONTAP를 배포할 계정과 별도로 AWS 계정에 있는 경우 해당 키의 ARN을 얻어야 합니다.

Cloud Volumes ONTAP 시스템을 생성할 때 클라우드 관리자에게 ARN을 제공해야 합니다.

3. Cloud Manager 인스턴스의 IAM 역할을 CMK의 주요 사용자 목록에 추가합니다.

이렇게 하면 Cloud Volumes ONTAP에서 CMK를 사용할 수 있는 클라우드 관리자 권한이 부여됩니다.

Cloud Manager 설치 및 설정

AWS에서 Cloud Volumes ONTAP 시스템을 시작하려면 먼저 AWS Marketplace에서 Connector 인스턴스를 시작한 다음 로그인하고 Cloud Manager를 설정해야 합니다.

단계

1. PEM(Privacy Enhanced Mail) Base-64로 인코딩된 X.509 형식으로 CA(인증 기관)에서 서명한 루트 인증서를 받습니다. 인증서를 얻으려면 조직의 정책 및 절차를 참조하십시오.

설치 프로세스 중에 인증서를 업로드해야 합니다. Cloud Manager는 HTTPS를 통해 AWS로 요청을 보낼 때 신뢰할 수 있는 인증서를 사용합니다.

2. 커넥터 인스턴스를 시작합니다.

- a. Cloud Manager의 AWS Intelligence Community Marketplace 페이지로 이동합니다.
- b. Custom Launch 탭에서 EC2 콘솔에서 인스턴스를 시작하는 옵션을 선택합니다.
- c. 프롬프트에 따라 인스턴스를 구성합니다.

인스턴스를 구성할 때 다음 사항에 유의하십시오.

- T3.xLarge를 권장합니다.

- AWS 환경을 준비할 때 생성한 IAM 역할을 선택해야 합니다.
 - 기본 스토리지 옵션을 유지해야 합니다.
 - Connector에 필요한 연결 방법은 SSH, HTTP, HTTPS입니다.
3. Connector 인스턴스에 연결된 호스트에서 Cloud Manager를 설정합니다.
 - a. 웹 브라우저를 열고 다음 URL을 입력합니다. <http://ipaddress:80>
 - b. AWS 서비스 연결을 위한 프록시 서버를 지정합니다.
 - c. 1단계에서 얻은 인증서를 업로드합니다.
 - d. 설정 마법사의 단계를 완료하여 Cloud Manager를 설정합니다.
 - * 시스템 세부 정보 *: 이 Cloud Manager 인스턴스의 이름을 입력하고 회사 이름을 입력합니다.
 - * 사용자 생성 *: Cloud Manager 관리에 사용할 관리자 사용자를 생성합니다.
 - * 검토 *: 세부 정보를 검토하고 최종 사용자 사용권 계약을 승인합니다.
 - e. CA 서명 인증서의 설치를 완료하려면 EC2 콘솔에서 Connector 인스턴스를 다시 시작합니다.
 4. Connector가 다시 시작된 후 설치 마법사에서 만든 관리자 사용자 계정을 사용하여 로그인합니다.

Cloud Volumes ONTAP를 시작합니다

Cloud Manager에서 새로운 작업 환경을 생성하여 AWS 상용 클라우드 서비스 환경에서 Cloud Volumes ONTAP 인스턴스를 시작할 수 있습니다.

무엇을 '필요로 할거야

- 라이선스를 구입한 경우 NetApp에서 받은 라이선스 파일이 있어야 합니다. 라이선스 파일은 JSON 형식의 .NLF 파일입니다.
- HA 중재자가 키 기반 SSH 인증을 사용할 수 있도록 키 쌍이 필요합니다.

단계

1. 작업 환경 페이지에서 * 작업 환경 추가 * 를 클릭합니다.
2. 생성 아래에서 Cloud Volumes ONTAP 또는 Cloud Volumes ONTAP HA를 선택합니다.
3. 마법사의 단계를 완료하여 Cloud Volumes ONTAP 시스템을 시작합니다.

마법사를 완료하면 다음 사항에 유의하십시오.

- 여러 가용성 영역에 Cloud Volumes ONTAP HA를 배포하려는 경우 게시 시점에 AWS 상용 클라우드 서비스 환경에서 AZs를 두 개만 사용할 수 있으므로 다음과 같이 구성을 구축합니다.
 - 노드 1: 가용성 영역 A
 - 노드 2: 가용성 영역 B
 - 중재자: 가용성 영역 A 또는 B
- 생성된 보안 그룹을 사용하려면 기본 옵션을 그대로 두어야 합니다.

미리 정의된 보안 그룹에는 Cloud Volumes ONTAP가 제대로 작동하는 데 필요한 규칙이 포함됩니다. 사용자 고유의 사용이 필요한 경우 아래의 보안 그룹 섹션을 참조할 수 있습니다.

- AWS 환경을 준비할 때 생성한 IAM 역할을 선택해야 합니다.
- 기본 AWS 디스크 유형은 초기 Cloud Volumes ONTAP 볼륨에 사용됩니다.

이후 볼륨에 대해 다른 디스크 유형을 선택할 수 있습니다.

- AWS 디스크의 성능은 디스크 크기와 관련이 있습니다.

필요한 일관된 성능을 제공하는 디스크 크기를 선택해야 합니다. EBS 성능에 대한 자세한 내용은 AWS 설명서를 참조하십시오.

- 디스크 크기는 시스템의 모든 디스크에 대한 기본 크기입니다.



나중에 다른 크기가 필요한 경우 고급 할당 옵션을 사용하여 특정 크기의 디스크를 사용하는 Aggregate를 생성할 수 있습니다.

- 스토리지 효율성 기능을 사용하면 스토리지 활용률을 개선하고 필요한 총 스토리지 양을 줄일 수 있습니다.

Cloud Manager가 Cloud Volumes ONTAP 인스턴스를 시작합니다. 타임라인에서 진행 상황을 추적할 수 있습니다.

보안 그룹 규칙

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

커넥터의 보안 그룹

Connector의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

인바운드 규칙

프로토콜	포트	목적
SSH를 클릭합니다	22	커넥터 호스트에 대한 SSH 액세스를 제공합니다
HTTP	80	클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공합니다
HTTPS	443	클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTPS 액세스를 제공합니다

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

Cloud Volumes ONTAP의 보안 그룹입니다

Cloud Volumes ONTAP 노드의 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
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

프로토콜	포트	목적
UDP입니다	4046	NFS에 대한 네트워크 상태 모니터
UDP입니다	4049	NFS rquotad 프로토콜

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

HA 중재자를 위한 외부 보안 그룹

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

인바운드 규칙

인바운드 규칙의 소스는 Connector가 상주하는 VPC의 트래픽입니다.

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

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

HA 중재자를 위한 내부 보안 그룹

Cloud Volumes ONTAP HA 중재자를 위해 미리 정의된 내부 보안 그룹에는 다음 규칙이 포함됩니다. Cloud Manager는 항상 이 보안 그룹을 생성합니다. 자체 옵션을 사용할 수 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

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.