Amazon Web Services에서 시작하세요

Cloud Volumes ONTAP

NetApp
December 10, 2025

목차

Amazon Web Services에서 시작하세요

AWS에서 Cloud Volumes ONTAP 빠르게 시작하세요

몇 단계만 거치면 AWS에서 Cloud Volumes ONTAP 시작할 수 있습니다.

1 콘솔 에이전트 만들기

만약 당신이 없다면 "콘솔 에이전트" 하지만, 하나는 만들어야 합니다. "AWS에서 콘솔 에이전트를 만드는 방법을 알아보세요" .

인터넷 접속이 불가능한 서브넷에 Cloud Volumes ONTAP 배포하려면 콘솔 에이전트를 수동으로 설치하고 해당 콘솔 에이전트에서 실행되는 NetApp Console 사용자 인터페이스에 액세스해야 합니다. "인터넷 접속이 불가능한 위치에 콘솔 에이전트를 수동으로 설치하는 방법을 알아보세요." .

2 구성을 계획하세요

콘솔은 사용자의 작업 부하 요구 사항에 맞는 미리 구성된 패키지를 제공하거나 사용자가 직접 구성을 만들 수도 있습니다. 원하는 구성을 선택하는 경우, 사용 가능한 옵션을 이해해야 합니다. "자세히 알아보기" .

3 네트워킹을 설정하세요

1. VPC와 서브넷이 콘솔 에이전트와 Cloud Volumes ONTAP 간의 연결을 지원하는지 확인하세요.
2. NetApp AutoSupport 에 대해 대상 VPC에서 아웃바운드 인터넷 액세스를 활성화합니다.

   인터넷 접속이 불가능한 위치에 Cloud Volumes ONTAP 배포하는 경우 이 단계는 필요하지 않습니다.
3. S3 서비스에 대한 VPC 엔드포인트를 설정합니다.

   Cloud Volumes ONTAP 에서 저비용 개체 스토리지로 콜드 데이터를 계층화하려면 VPC 엔드포인트가 필요합니다.

"네트워킹 요구 사항에 대해 자세히 알아보세요" .

4 **AWS KMS** 설정

Cloud Volumes ONTAP 과 함께 Amazon 암호화를 사용하려면 활성 고객 마스터 키(CMK)가 있는지 확인해야 합니다. 또한 콘솔 에이전트에 대한 권한을 제공하는 IAM 역할을 _키 사용자_로 추가하여 각 CMK에 대한 키 정책을 수정해야 합니다. "자세히 알아보기" .

5 콘솔을 사용하여 **Cloud Volumes ONTAP** 실행

*시스템 추가*를 클릭하고 배포하려는 시스템 유형을 선택한 다음 마법사의 단계를 완료합니다. "단계별 지침을 읽어보세요" .

관련 링크

- "AWS용 콘솔 에이전트 만들기"
- "AWS Marketplace에서 콘솔 에이전트 만들기"
- "온프레미스에 콘솔 에이전트 설치 및 설정"
- "콘솔 에이전트에 대한 AWS 권한"

AWS에서 Cloud Volumes ONTAP 구성을 계획하세요

AWS에 Cloud Volumes ONTAP 배포하는 경우 워크로드 요구 사항에 맞는 미리 구성된 시스템을 선택하거나 고유한 구성을 만들 수 있습니다. 원하는 구성을 선택하는 경우, 사용 가능한 옵션을 이해해야 합니다.

Cloud Volumes ONTAP 라이선스를 선택하세요

Cloud Volumes ONTAP 에는 여러 가지 라이선싱 옵션이 제공됩니다. 각 옵션을 통해 귀하의 필요에 맞는 소비 모델을 선택할 수 있습니다.

- "Cloud Volumes ONTAP 에 대한 라이선싱 옵션에 대해 알아보세요"
- "라이선싱 설정 방법 알아보기"

지원되는 지역을 선택하세요

Cloud Volumes ONTAP 대부분의 AWS 지역에서 지원됩니다. "지원되는 지역의 전체 목록 보기" .

새로운 AWS 지역은 해당 지역에서 리소스를 생성하고 관리하기 전에 활성화해야 합니다. "AWS 설명서: 리전을 활성화하는 방법 알아보기" .

지원되는 로컬 영역을 선택하세요

로컬 존을 선택하는 것은 선택 사항입니다. Cloud Volumes ONTAP 싱가포르를 포함한 일부 AWS 로컬 영역에서 지원됩니다. AWS의 Cloud Volumes ONTAP 단일 가용성 영역에서만 고가용성(HA) 모드를 지원합니다. 단일 노드 배포는 지원되지 않습니다.

> Cloud Volumes ONTAP AWS 로컬 영역에서 데이터 계층화 및 클라우드 계층화를 지원하지 않습니다. 또한, Cloud Volumes ONTAP 에 적합하지 않은 인스턴스가 있는 로컬 영역은 지원되지 않습니다. 이에 대한 예는 마이애미인데, 지원되지 않고 적격하지 않은 Gen6 인스턴스만 있기 때문에 로컬 영역으로 사용할 수 없습니다.

"AWS 문서: 로컬 영역 전체 목록 보기" . 로컬 영역을 활성화해야만 해당 영역에서 리소스를 만들고 관리할 수 있습니다.

"AWS 설명서: AWS 로컬 영역 시작하기" .

지원되는 인스턴스를 선택하세요

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

"AWS의 Cloud Volumes ONTAP 에 지원되는 구성"

저장 한도 이해하기

Cloud Volumes ONTAP 시스템의 원시 용량 제한은 라이선스에 따라 결정됩니다. 추가적인 제한은 골재와 부피의 크기에 영향을 미칩니다. 구성을 계획할 때 이러한 제한 사항을 알고 있어야 합니다.

"AWS의 Cloud Volumes ONTAP 대한 스토리지 한도"

AWS에서 시스템 크기 조정

Cloud Volumes ONTAP 시스템의 크기를 조정하면 성능 및 용량 요구 사항을 충족하는 데 도움이 될 수 있습니다. 인스턴스 유형, 디스크 유형 및 디스크 크기를 선택할 때 몇 가지 핵심 사항을 알아야 합니다.

인스턴스 유형

- 각 EC2 인스턴스 유형에 대한 최대 처리량 및 IOPS에 맞게 워크로드 요구 사항을 조정하세요.
- 여러 사용자가 동시에 시스템에 쓰는 경우 요청을 관리할 수 있는 충분한 CPU가 있는 인스턴스 유형을 선택하세요.
- 주로 읽기 작업을 하는 애플리케이션을 사용하는 경우, 충분한 RAM을 갖춘 시스템을 선택하세요.
  - "AWS 설명서: Amazon EC2 인스턴스 유형"
  - "AWS 설명서: Amazon EBS 최적화 인스턴스"

EBS 디스크 유형

높은 수준에서 EBS 디스크 유형 간의 차이점은 다음과 같습니다. EBS 디스크의 사용 사례에 대해 자세히 알아보려면 다음을 참조하세요. "AWS 문서: EBS 볼륨 유형" .

- 일반 용도 *SSD(gp3)* 디스크는 광범위한 작업 부하에 대해 비용과 성능의 균형을 맞춘 가장 저렴한 SSD입니다. 성능은 IOPS와 처리량으로 정의됩니다. gp3 디스크는 Cloud Volumes ONTAP 9.7 이상에서 지원됩니다.

  gp3 디스크를 선택하면 NetApp Console 선택한 디스크 크기를 기준으로 gp2 디스크와 동등한 성능을 제공하는 기본 IOPS 및 처리량 값을 입력합니다. 더 높은 비용으로 더 나은 성능을 얻으려면 값을 늘릴 수 있지만, 낮은 값은 성능이 저하될 수 있으므로 지원하지 않습니다. 간단히 말해, 기본값을 고수하거나 기본값을 늘리세요. 낮추지 마세요. "AWS 문서: gp3 디스크와 성능에 대해 자세히 알아보세요" .

  Cloud Volumes ONTAP gp3 디스크를 사용하는 Amazon EBS Elastic Volumes 기능을 지원합니다. "Elastic Volumes 지원에 대해 자세히 알아보세요" .

- 일반 용도 *SSD(gp2)* 디스크는 광범위한 작업 부하에 대해 비용과 성능의 균형을 맞춥니다. 성능은 IOPS로 정의됩니다.
- 프로비저닝된 *IOPS SSD(io1)* 디스크는 더 높은 비용으로 최고의 성능을 필요로 하는 중요한 애플리케이션을 위한 것입니다.

  Cloud Volumes ONTAP io1 디스크를 사용하여 Amazon EBS Elastic Volumes 기능을 지원합니다. "Elastic Volumes 지원에 대해 자세히 알아보세요" .

- 처리량 최적화 *HDD(st1)* 디스크는 저렴한 가격으로 빠르고 일관된 처리량이 필요한 자주 액세스되는 워크로드에 적합합니다.

  AWS 로컬 영역에서는 연결성이 부족하여 AWS S3에 대한 데이터 계층화를 사용할 수 없습니다.

EBS 디스크 크기

지원하지 않는 구성을 선택하는 경우"Amazon EBS Elastic Volumes 기능" , Cloud Volumes ONTAP 시스템을 시작할 때 초기 디스크 크기를 선택해야 합니다. 그 후에는 할 수 있습니다"콘솔이 시스템 용량을 관리하도록 하세요" , 하지만 당신이 원한다면"직접 집계를 생성하세요" 다음 사항을 주의하세요.

- 집계된 모든 디스크의 크기는 동일해야 합니다.
- EBS 디스크의 성능은 디스크 크기에 따라 달라집니다. 크기는 SSD 디스크의 기준 IOPS와 최대 버스트 지속 시간을 결정하고, HDD 디스크의 기준 및 버스트 처리량을 결정합니다.
- 궁극적으로, 필요한 _지속적인 성능_을 제공하는 디스크 크기를 선택해야 합니다.
- 더 큰 디스크(예: 4TiB 디스크 6개)를 선택하더라도 EC2 인스턴스가 대역폭 제한에 도달할 수 있으므로 모든 IOPS를 얻지 못할 수 있습니다.

  EBS 디스크 성능에 대한 자세한 내용은 다음을 참조하세요. "AWS 문서: EBS 볼륨 유형" .

  위에서 언급한 대로 Amazon EBS Elastic Volumes 기능을 지원하는 Cloud Volumes ONTAP 구성에서는 디스크 크기를 선택할 수 없습니다. "Elastic Volumes 지원에 대해 자세히 알아보세요" .

기본 시스템 디스크 보기

사용자 데이터 저장 외에도 콘솔은 Cloud Volumes ONTAP 시스템 데이터(부팅 데이터, 루트 데이터, 코어 데이터 및 NVRAM)를 위한 클라우드 스토리지도 구매합니다. 계획을 세우려면 Cloud Volumes ONTAP 배포하기 전에 이러한 세부 정보를 검토하는 것이 도움이 될 수 있습니다.

"AWS에서 Cloud Volumes ONTAP 시스템 데이터의 기본 디스크 보기" .

콘솔 에이전트에도 시스템 디스크가 필요합니다. "콘솔 에이전트의 기본 구성에 대한 세부 정보 보기" .

AWS Outpost에 Cloud Volumes ONTAP 배포 준비

AWS Outpost가 있는 경우 배포 프로세스 중에 Outpost VPC를 선택하여 해당 Outpost에 Cloud Volumes ONTAP 배포할 수 있습니다. 경험은 AWS에 있는 다른 VPC와 동일합니다. 먼저 AWS Outpost에 콘솔 에이전트를 배포해야 합니다.

지적해야 할 몇 가지 제한 사항이 있습니다.

- 현재 단일 노드 Cloud Volumes ONTAP 시스템만 지원됩니다.
- Cloud Volumes ONTAP 과 함께 사용할 수 있는 EC2 인스턴스는 Outpost에서 사용 가능한 인스턴스로 제한됩니다.
- 현재는 일반용 SSD(gp2)만 지원됩니다.

네트워킹 정보 수집

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

단일 **AZ**의 단일 노드 또는 **HA** 쌍

AWS 정보	당신의 가치
지역	
VPC	
서브넷	
보안 그룹(자체 보안 그룹을 사용하는 경우)	

여러 **AZ**의 **HA** 쌍

AWS 정보	당신의 가치
지역	
VPC	
보안 그룹(자체 보안 그룹을 사용하는 경우)	
노드 1 가용성 영역	
노드 1 서브넷	
노드 2 가용성 영역	
노드 2 서브넷	
중재자 가용성 영역	
중재자 서브넷	
중재자를 위한 키 쌍	
클러스터 관리 포트에 대한 유동 IP 주소	
노드 1의 데이터에 대한 유동 IP 주소	
노드 2의 데이터에 대한 플로팅 IP 주소	
플로팅 IP 주소에 대한 경로 테이블	

쓰기 속도를 선택하세요

콘솔을 사용하면 Cloud Volumes ONTAP 에 대한 쓰기 속도 설정을 선택할 수 있습니다. 쓰기 속도를 선택하기 전에 일반 설정과 높은 설정의 차이점, 높은 쓰기 속도를 사용할 때의 위험과 권장 사항을 이해해야 합니다. "쓰기 속도에 대해 자세히 알아보세요" .

볼륨 사용 프로필을 선택하세요

ONTAP 에는 필요한 총 저장 용량을 줄일 수 있는 여러 가지 저장 효율성 기능이 포함되어 있습니다. 콘솔에서 볼륨을 생성할 때 이러한 기능을 활성화하는 프로필이나 비활성화하는 프로필을 선택할 수 있습니다. 어떤 프로필을 사용할지

결정하는 데 도움이 되도록 이러한 기능에 대해 자세히 알아보세요.

NetApp 스토리지 효율성 기능은 다음과 같은 이점을 제공합니다.

씬 프로비저닝

실제 물리적 스토리지 풀에 있는 것보다 더 많은 논리적 스토리지를 호스트나 사용자에게 제공합니다. 저장 공간을 미리 할당하는 대신, 데이터가 기록됨에 따라 각 볼륨에 저장 공간이 동적으로 할당됩니다.

중복제거

동일한 데이터 블록을 찾아 단일 공유 블록에 대한 참조로 대체하여 효율성을 향상시킵니다. 이 기술은 동일한 볼륨에 있는 중복된 데이터 블록을 제거하여 저장 용량 요구 사항을 줄입니다.

압축

1차, 2차, 보관 저장소의 볼륨 내 데이터를 압축하여 데이터를 저장하는 데 필요한 물리적 용량을 줄입니다.

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.
\ 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.

엔드포인트	적용 가능	목적	배포 모드	엔드포인트를 사용할 수 없는 경우의 영향
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

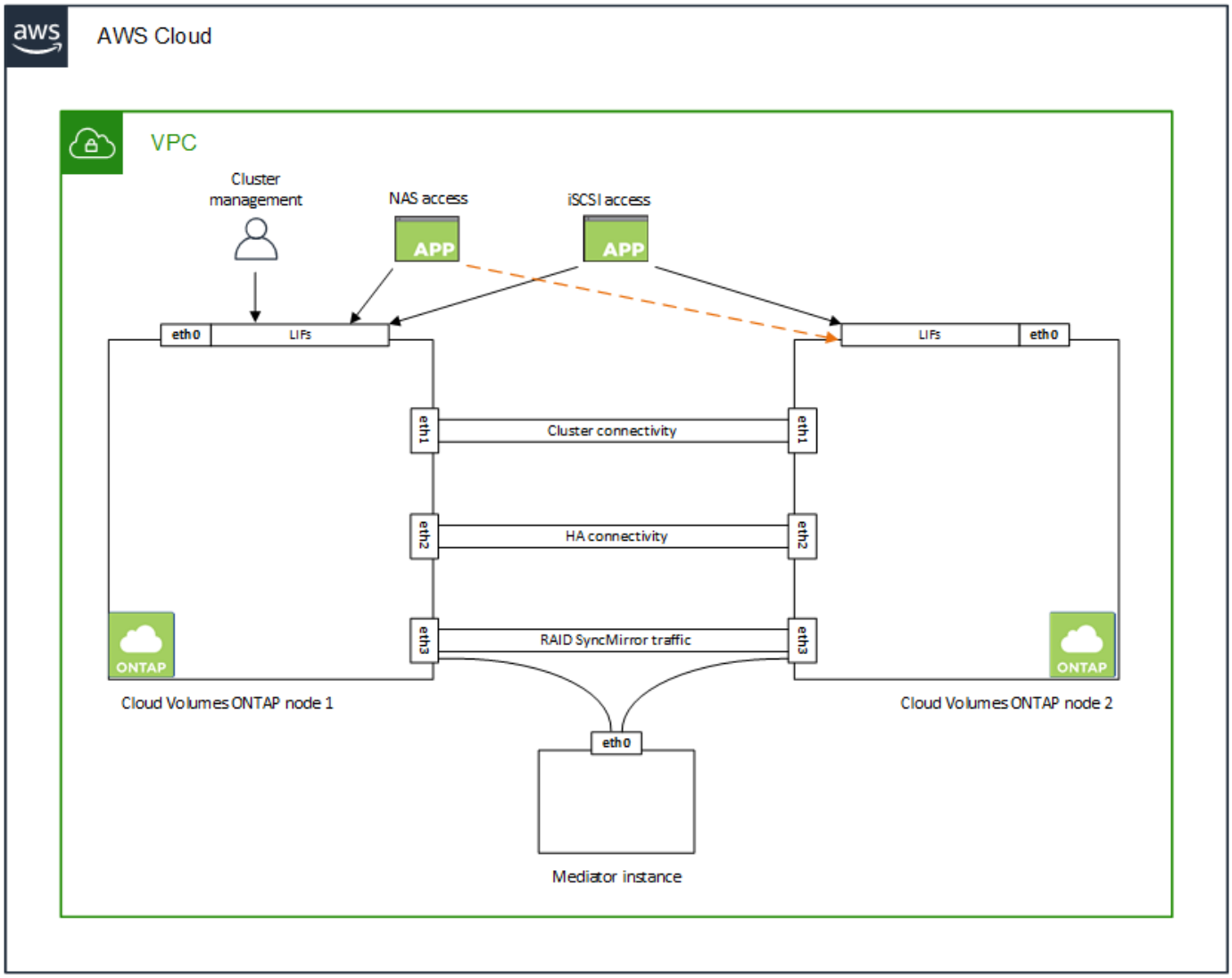
콘솔은 단일 노드 시스템에 6개의 IP 주소를 할당합니다.

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 AZ의 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.

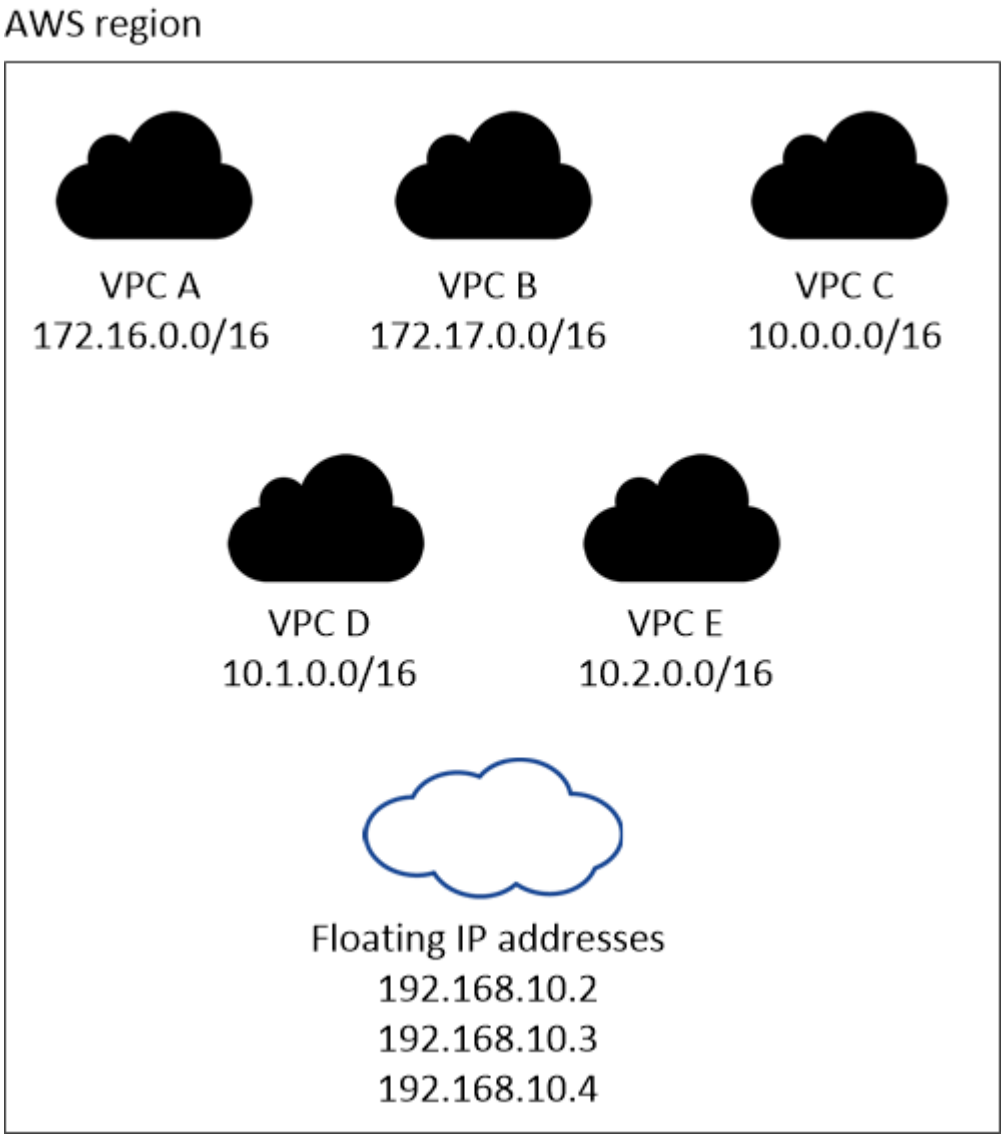
> ⓘ HA 쌍과 함께 Windows용 SnapDrive 또는 SnapCenter 사용하는 경우 SVM 관리 LIF에 부동 IP 주소가 필요합니다.

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" .

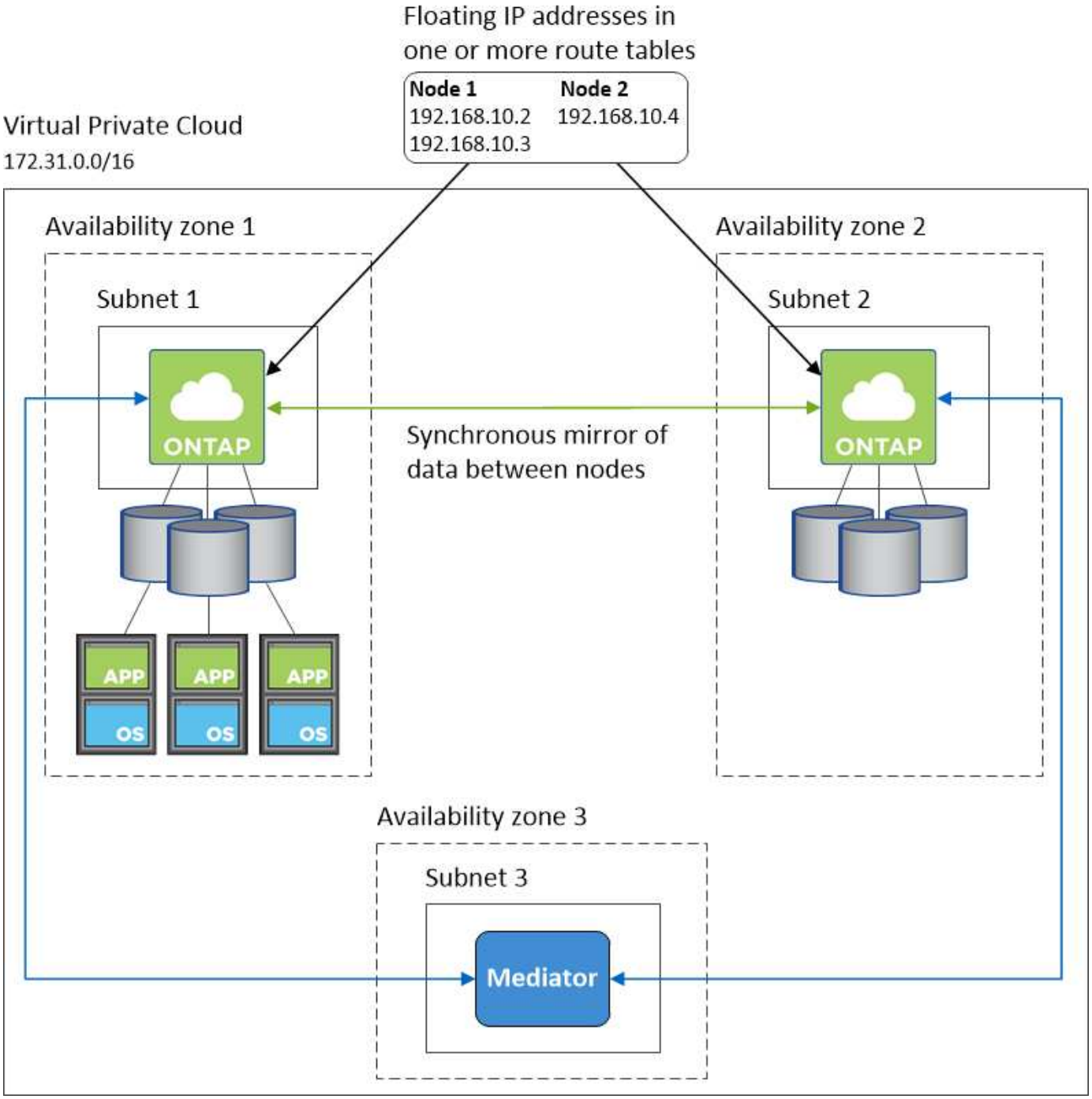
NetApp 관리 도구에 연결

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

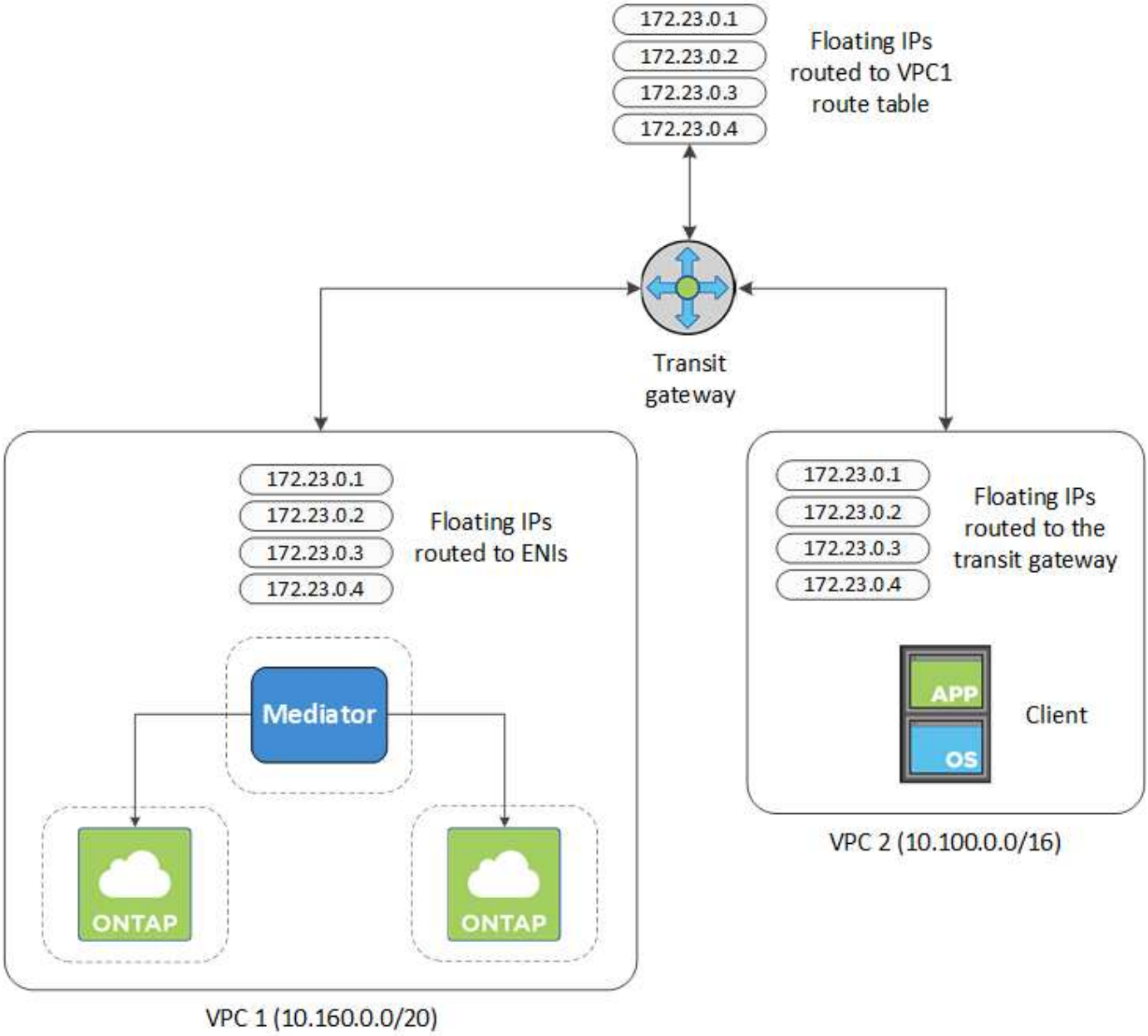
HA 쌍에 대한 액세스를 활성화하기 위해 AWS 전송 게이트웨이를 설정합니다."유동 IP 주소" HA 쌍이 있는 VPC 외부에서.

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.

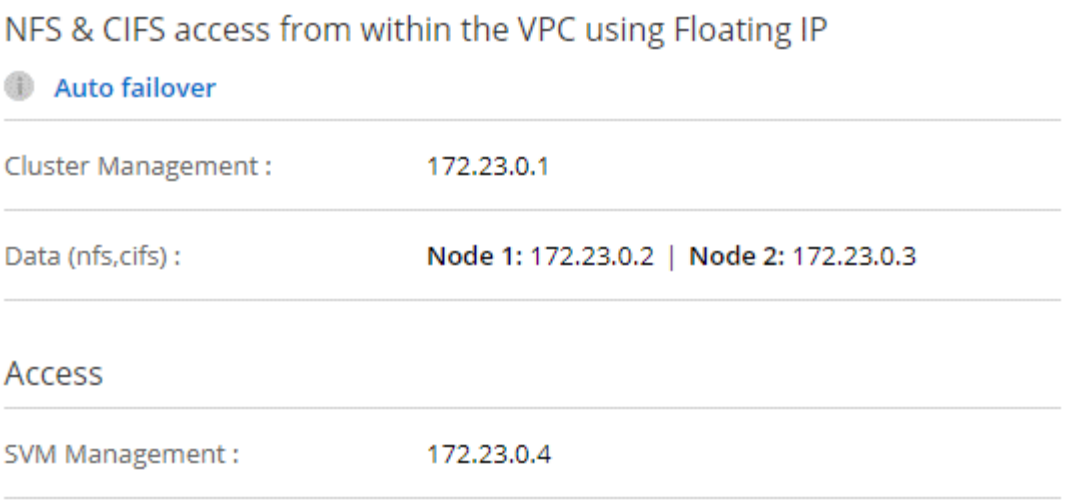


다음 단계에서는 비슷한 구성을 설정하는 방법을 보여줍니다.

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.



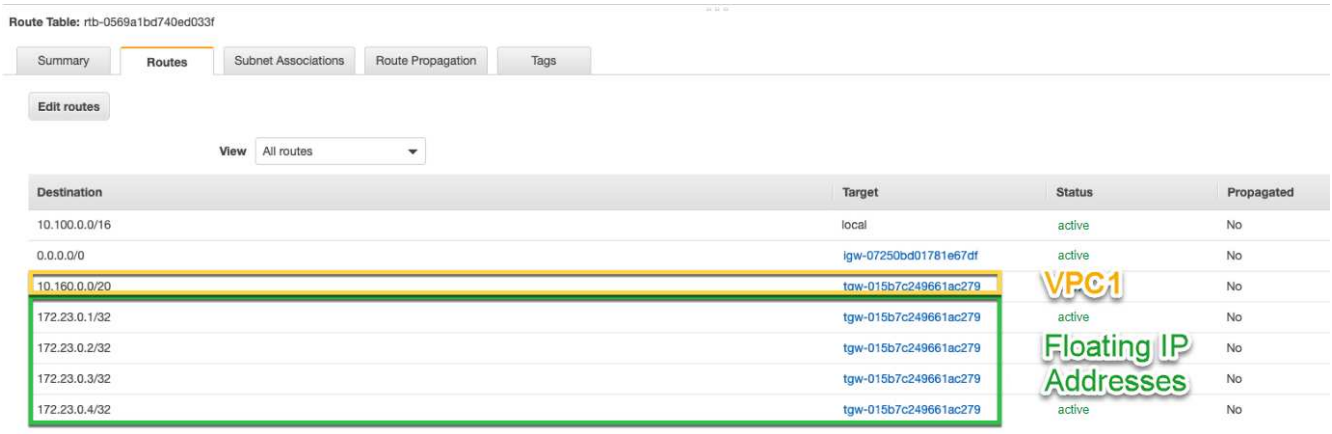
다음 샘플 이미지는 트랜짓 게이트웨이의 경로 테이블을 보여줍니다. 여기에는 Cloud Volumes ONTAP 에서 사용하는 두 개의 VPC의 CIDR 블록에 대한 경로와 4개의 플로팅 IP 주소가 포함됩니다.

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.

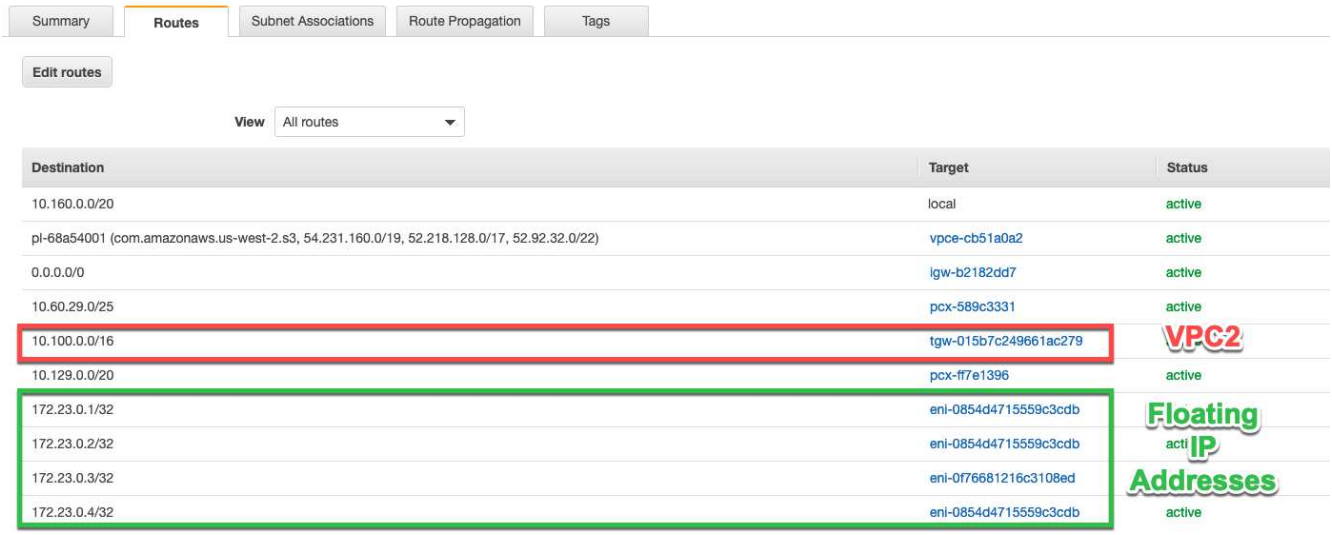
      다음 샘플 이미지는 VPC 1에 대한 경로와 플로팅 IP 주소를 포함하는 VPC 2의 경로 테이블을 보여줍니다.



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

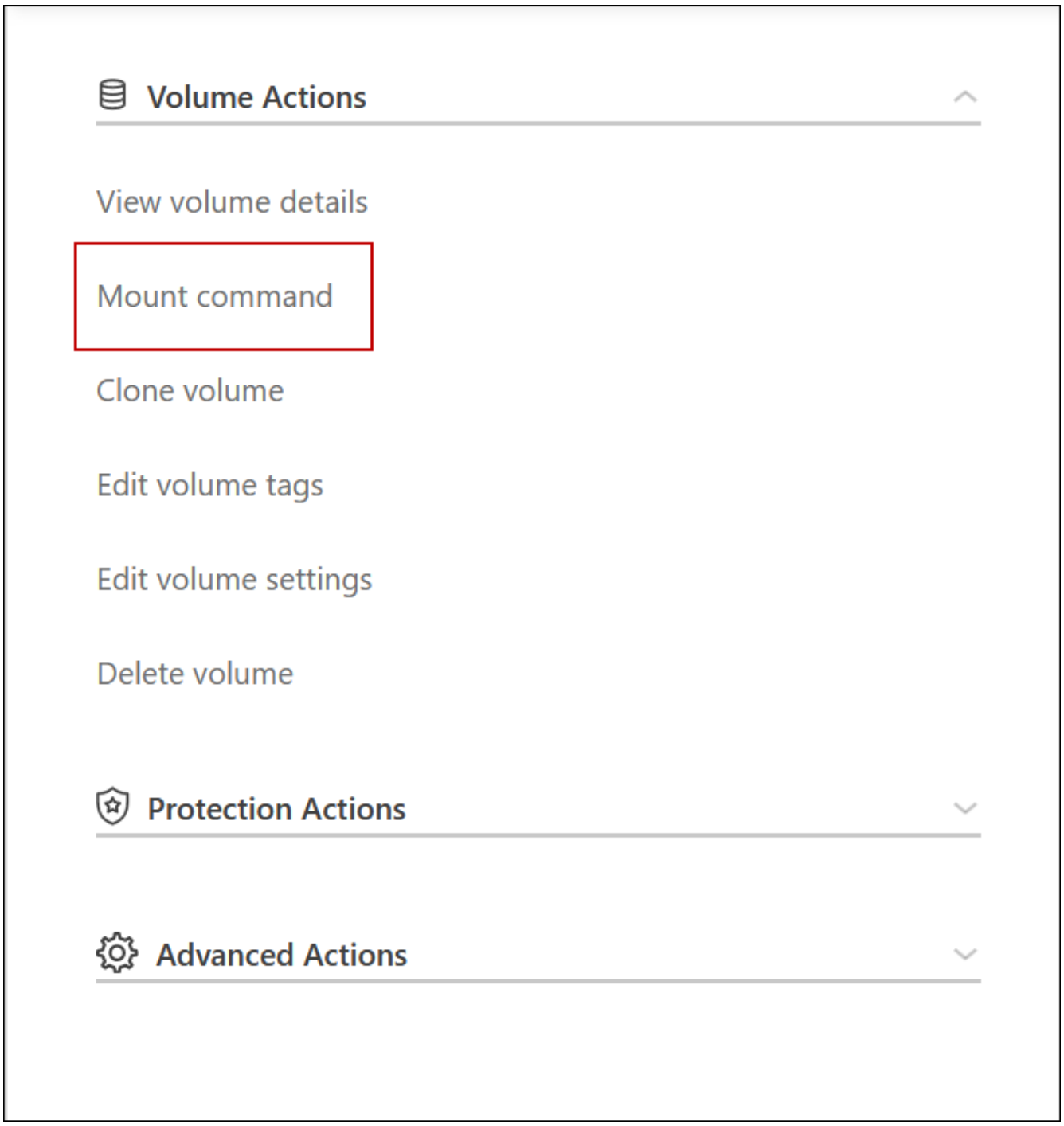
   이 단계는 VPC 간 라우팅을 완료하기 때문에 중요합니다.

   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

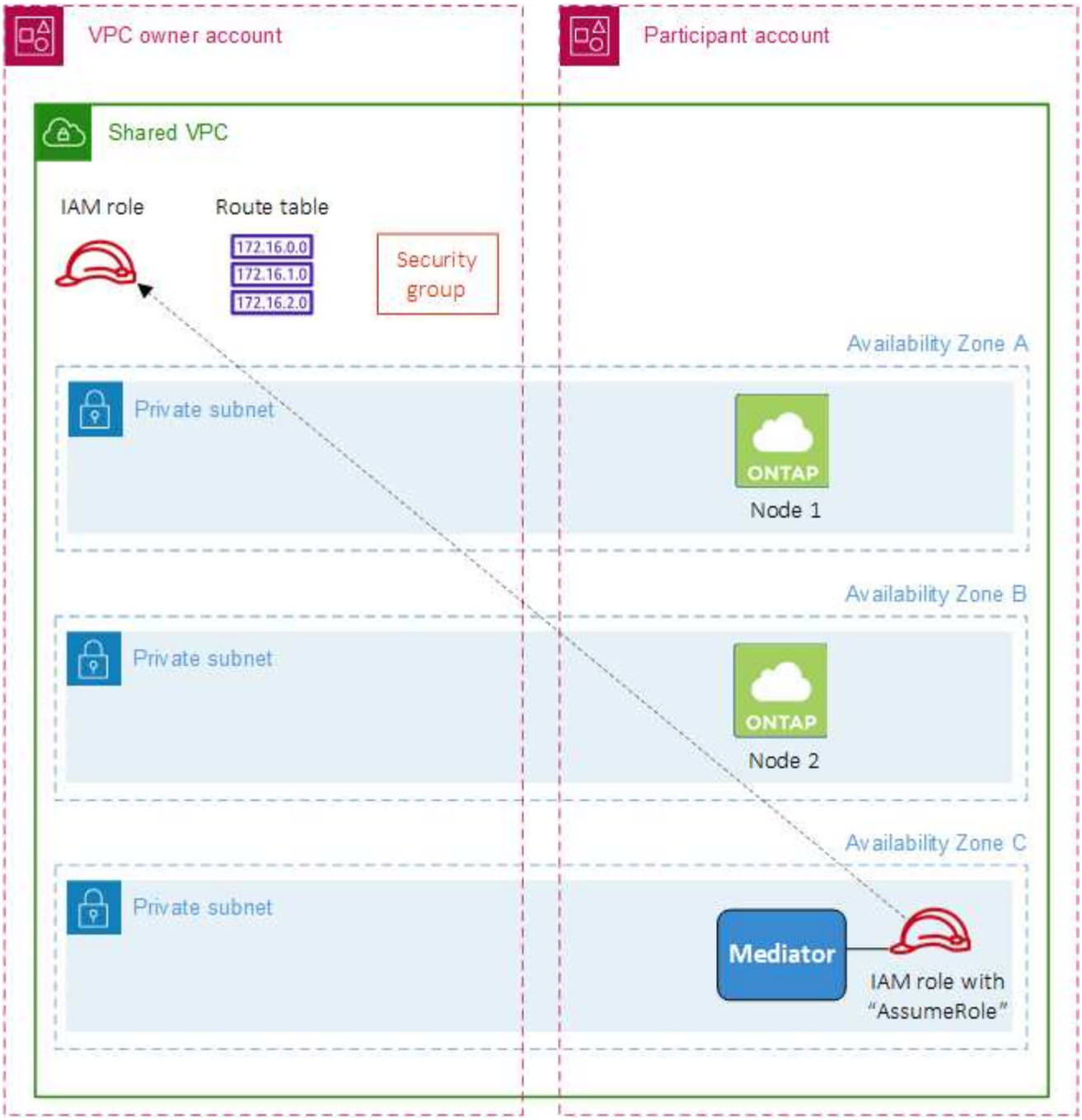
9.11.1 릴리스부터 VPC 공유를 통해 AWS에서 Cloud Volumes ONTAP HA 쌍이 지원됩니다. VPC 공유를 사용하면 조직에서 다른 AWS 계정과 서브넷을 공유할 수 있습니다. 이 구성을 사용하려면 AWS 환경을 설정한 다음 API를 사용하여 HA 쌍을 배포해야 합니다.

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

규약	포트	목적
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"

AWS에서 고객 관리 키를 사용하도록 Cloud Volumes ONTAP 설정

Cloud Volumes ONTAP 과 함께 Amazon 암호화를 사용하려면 AWS Key Management Service(KMS)를 설정해야 합니다.

단계

1. 활성 고객 마스터 키(CMK)가 있는지 확인하세요.

   CMK는 AWS 관리형 CMK이거나 고객 관리형 CMK일 수 있습니다. NetApp Console 및 Cloud Volumes ONTAP 과 동일한 AWS 계정에 있을 수도 있고 다른 AWS 계정에 있을 수도 있습니다.

   "AWS 문서: 고객 마스터 키(CMK)"

2. 콘솔에 대한 권한을 제공하는 IAM 역할을 _키 사용자_로 추가하여 각 CMK에 대한 키 정책을 수정합니다.

   IAM(Identity and Access Management) 역할을 주요 사용자로 추가하면 콘솔에서 Cloud Volumes ONTAP 과 함께 CMK를 사용할 수 있는 권한이 부여됩니다.

   "AWS 문서: 키 편집"

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

   a. CMK가 있는 계정에서 KMS 콘솔로 이동합니다.

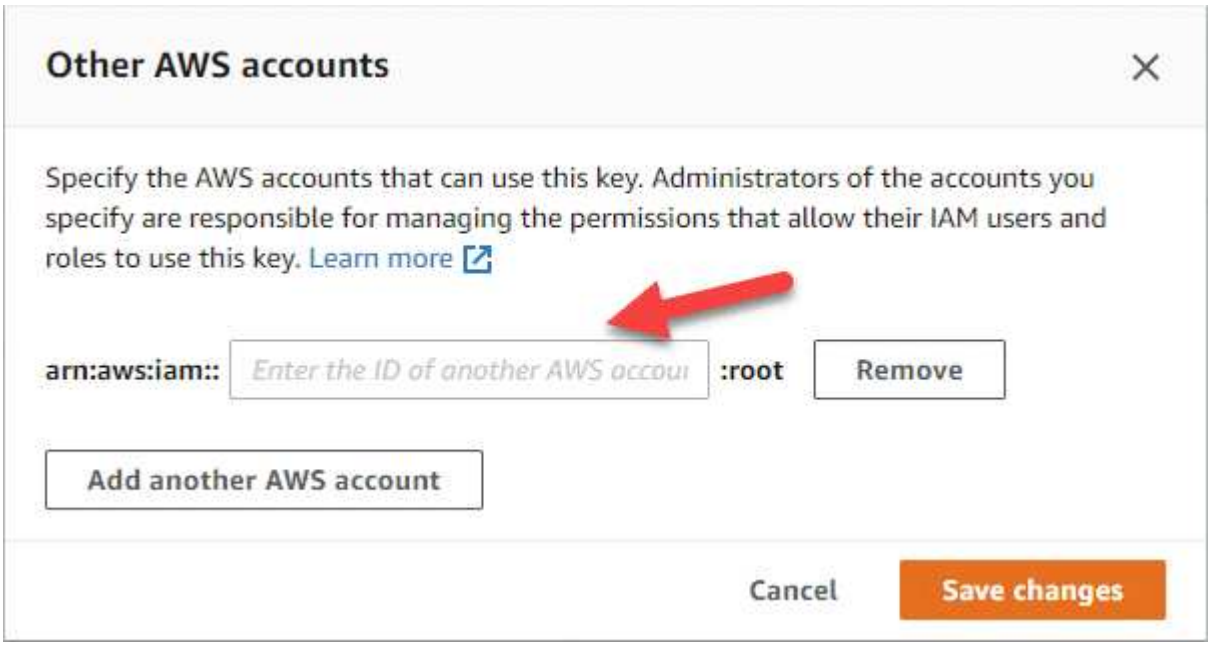
   b. 키를 선택하세요.

c. 일반 구성 창에서 키의 ARN을 복사합니다.

Cloud Volumes ONTAP 시스템을 생성할 때 콘솔에 ARN을 제공해야 합니다.

d. 다른 **AWS** 계정 창에서 콘솔에 권한을 제공하는 AWS 계정을 추가합니다.

일반적으로 이 계정에는 콘솔이 배포됩니다. AWS에 콘솔이 설치되어 있지 않은 경우 콘솔에 대한 AWS 액세스 키를 제공한 계정을 사용하세요.



e. 이제 콘솔에 권한을 제공하는 AWS 계정으로 전환하고 IAM 콘솔을 엽니다.

f. 아래 나열된 권한을 포함하는 IAM 정책을 만듭니다.

g. 콘솔에 대한 권한을 제공하는 IAM 역할이나 IAM 사용자에게 정책을 연결합니다.

다음 정책은 콘솔이 외부 AWS 계정에서 CMK를 사용하는 데 필요한 권한을 제공합니다. "리소스" 섹션에서 지역 및 계정 ID를 수정하세요.

```
{
    "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 추가 세부 사항은 다음을 참조하세요. "AWS 문서: 다른 계정의 사용자가 KMS 키를 사용하도록 허용" .

4. 고객 관리 CMK를 사용하는 경우 Cloud Volumes ONTAP IAM 역할을 _키 사용자_로 추가하여 CMK에 대한 키 정책을 수정합니다.

Cloud Volumes ONTAP 에서 데이터 계층화를 활성화하고 S3 버킷에 저장된 데이터를 암호화하려는 경우 이 단계가 필요합니다.

Cloud Volumes ONTAP 시스템을 생성할 때 IAM 역할이 생성되므로 Cloud Volumes ONTAP 배포한 후에 이 단계를 수행해야 합니다. (물론, 기존 Cloud Volumes ONTAP IAM 역할을 사용할 수도 있으므로 이 단계를 미리 수행할 수 있습니다.)

"AWS 문서: 키 편집"

Cloud Volumes ONTAP 노드에 대한 AWS IAM 역할 설정

필요한 권한이 있는 AWS Identity and Access Management(IAM) 역할은 각 Cloud Volumes ONTAP 노드에 연결되어야 합니다. HA 중재자의 경우도 마찬가지입니다. NetApp Console IAM 역할을 자동으로 생성하도록 하는 것이 가장 쉽지만, 사용자가 직접 역할을 지정할 수도 있습니다.

이 작업은 선택 사항입니다. Cloud Volumes ONTAP 시스템을 생성할 때 기본 옵션은 콘솔에서 IAM 역할을 생성하도록 하는 것입니다. 회사의 보안 정책에 따라 IAM 역할을 직접 만들어야 하는 경우 아래 단계를 따르세요.

AWS Secret Cloud에서는 고유한 IAM 역할을 제공해야 합니다. "C2S에 Cloud Volumes ONTAP 배포하는 방법을 알아보세요" .

단계

1. AWS IAM 콘솔로 이동합니다.
2. 다음 권한을 포함하는 IAM 정책을 만듭니다.
    - Cloud Volumes ONTAP 노드에 대한 기본 정책

표준 지역

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

GovCloud(미국) 지역

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

극비 지역

```
{
    "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"
    }]
}
```

비밀 지역

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

- Cloud Volumes ONTAP 노드에 대한 백업 정책

  Cloud Volumes ONTAP 시스템과 함께 NetApp Backup and Recovery 사용하려는 경우 노드의 IAM 역할에 아래에 표시된 두 번째 정책이 포함되어야 합니다.

표준 지역

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud(미국) 지역

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

극비 지역

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

비밀 지역

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso-b:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- HA 중재자

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

3. IAM 역할을 만들고 해당 역할에 만든 정책을 연결합니다.

결과

이제 새로운 Cloud Volumes ONTAP 시스템을 생성할 때 선택할 수 있는 IAM 역할이 생겼습니다.

더 많은 정보

- "AWS 설명서: IAM 정책 생성"
- "AWS 설명서: IAM 역할 생성"

AWS에서 Cloud Volumes ONTAP 에 대한 라이선싱 설정

Cloud Volumes ONTAP 에서 사용할 라이선싱 옵션을 결정한 후에는 새 시스템을 만들 때 해당 라이선싱 옵션을 선택하기 전에 몇 가지 단계를 거쳐야 합니다.

프리미엄

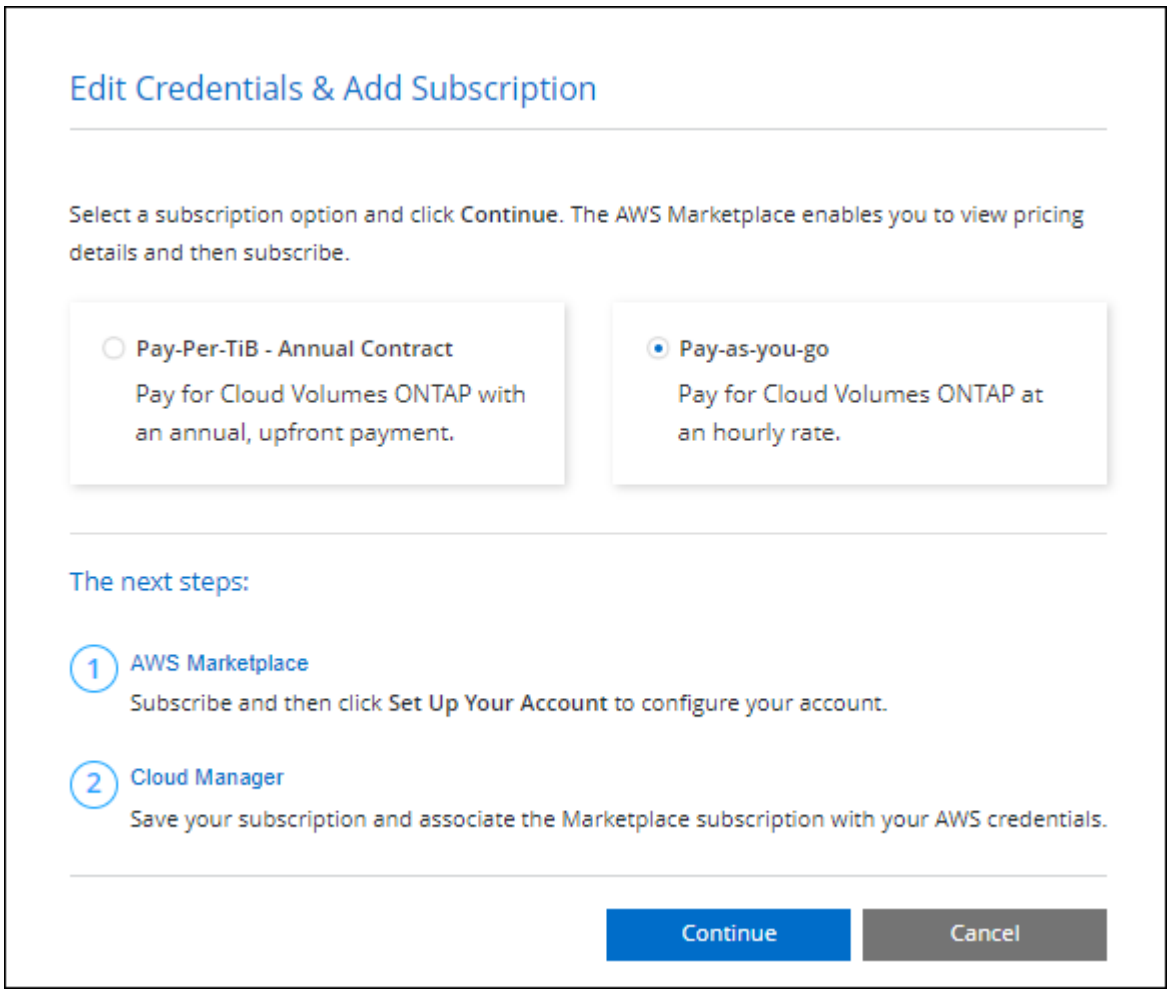
최대 500GiB의 프로비저닝 용량을 제공하는 Cloud Volumes ONTAP 무료로 사용하려면 Freemium 옵션을 선택하세요. "Freemium 제공에 대해 자세히 알아보세요" .

단계

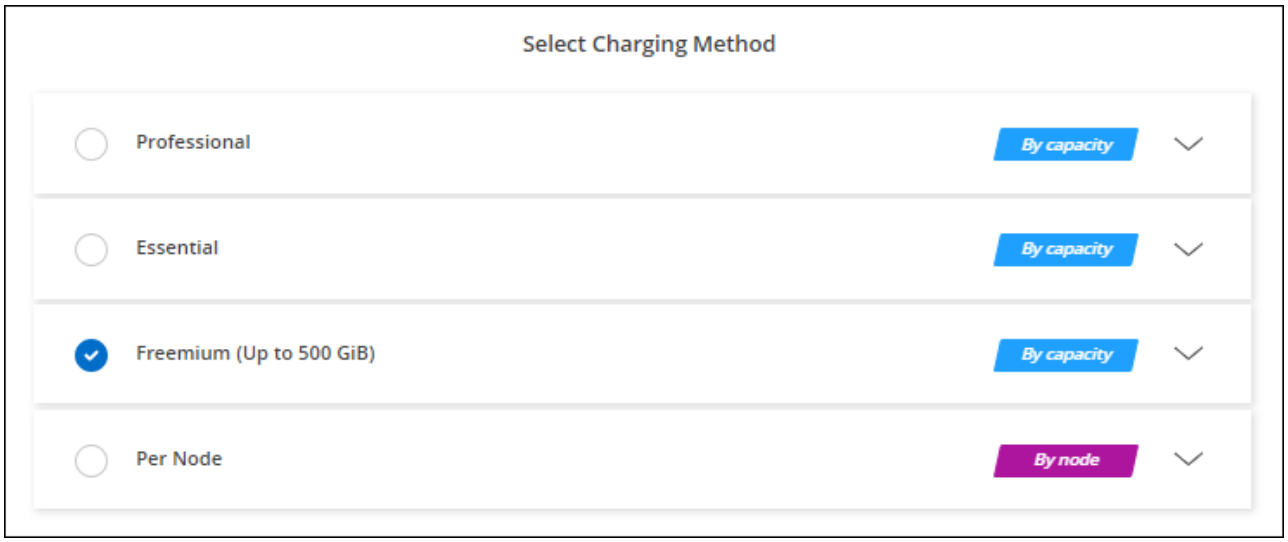
1. NetApp Console 의 왼쪽 탐색 메뉴에서 *스토리지 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.

a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 메시지에 따라 AWS Marketplace에서 사용량에 따라 지불하는 서비스를 구독하세요.

   프로비저닝된 용량이 500GiB를 초과하지 않는 한 마켓플레이스 구독을 통해 요금이 청구되지 않습니다. 초과 시 시스템은 자동으로 다음 용량으로 변환됩니다."필수 패키지" .



a. 콘솔로 돌아와서 요금 청구 방법 페이지에서 *프리미엄*을 선택하세요.



"AWS에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

용량 기반 라이센스

용량 기반 라이선싱을 사용하면 TiB 용량당 Cloud Volumes ONTAP 비용을 지불할 수 있습니다. 용량 기반 라이선싱은 패키지 형태로 제공됩니다. 패키지에는 Essentials 패키지와 Professional 패키지가 있습니다.

Essentials 및 Professional 패키지는 다음과 같은 소비 모델 또는 구매 옵션으로 이용 가능합니다.

- NetApp 에서 구매한 라이선스(BYOL(Bring Your Own License))
- AWS Marketplace의 시간당 결제(PAYGO) 구독
- AWS Marketplace의 연간 계약

"용량 기반 라이선싱에 대해 자세히 알아보세요" .

다음 섹션에서는 각 소비 모델을 시작하는 방법을 설명합니다.

바이올

NetApp 에서 라이선스(BYOL)를 구매하여 선불로 지불하면 모든 클라우드 공급자에 Cloud Volumes ONTAP 시스템을 배포할 수 있습니다.

NetApp BYOL 라이선스 구매, 연장 및 갱신을 제한하고 있습니다. 자세한 내용은 다음을 참조하세요. "Cloud Volumes ONTAP 에 대한 BYOL 라이선싱의 제한된 가용성" .

단계

1. "라이센스를 얻으려면 NetApp Sales에 문의하세요."
2. "콘솔에 NetApp 지원 사이트 계정 추가"

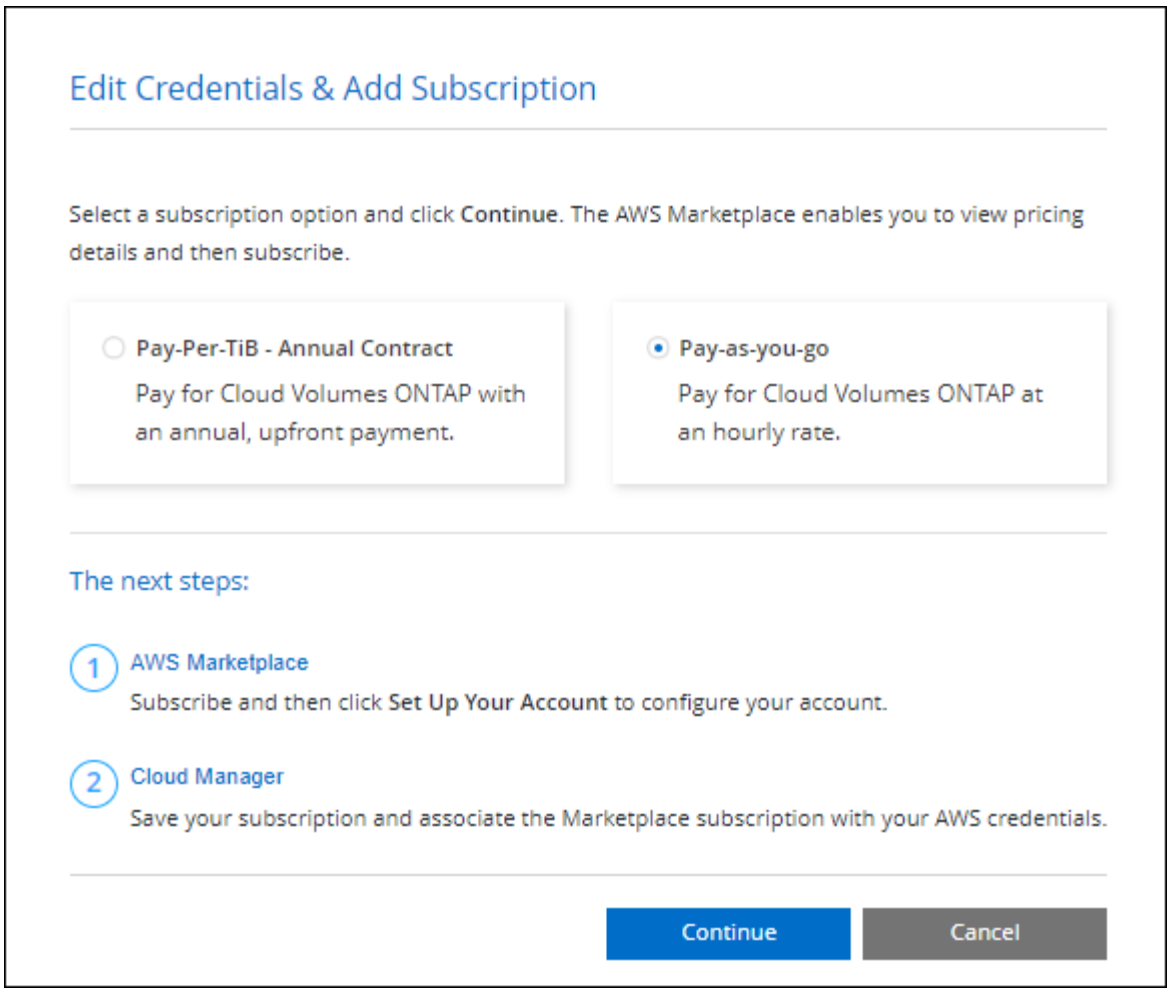
   콘솔은 NetApp 지원 사이트 계정과 연결된 라이선스에 대한 세부 정보를 얻기 위해 NetApp 라이선스 서비스에 자동으로 쿼리를 보냅니다. 오류가 없으면 콘솔이 자동으로 라이선스를 콘솔에 추가합니다.

   Cloud Volumes ONTAP 에서 라이선스를 사용하려면 먼저 콘솔에서 라이선스를 사용할 수 있어야 합니다. 필요한 경우 다음을 수행할 수 있습니다."콘솔에 라이센스를 수동으로 추가합니다." .

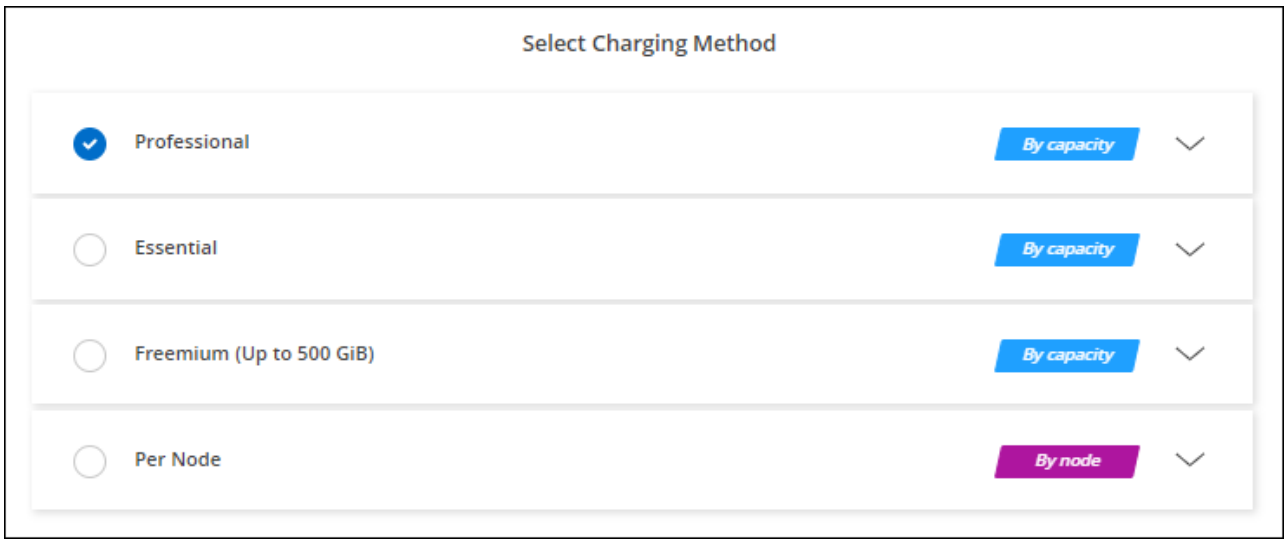
3. 콘솔의 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.

   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 메시지에 따라 AWS Marketplace에서 사용량에 따라 지불하는 서비스를 구독하세요.

      NetApp 에서 구매한 라이선스는 항상 먼저 청구되지만, 라이선스 용량을 초과하거나 라이선스 기간이 만료되면 마켓플레이스의 시간당 요금으로 청구됩니다.



a. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



"AWS에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

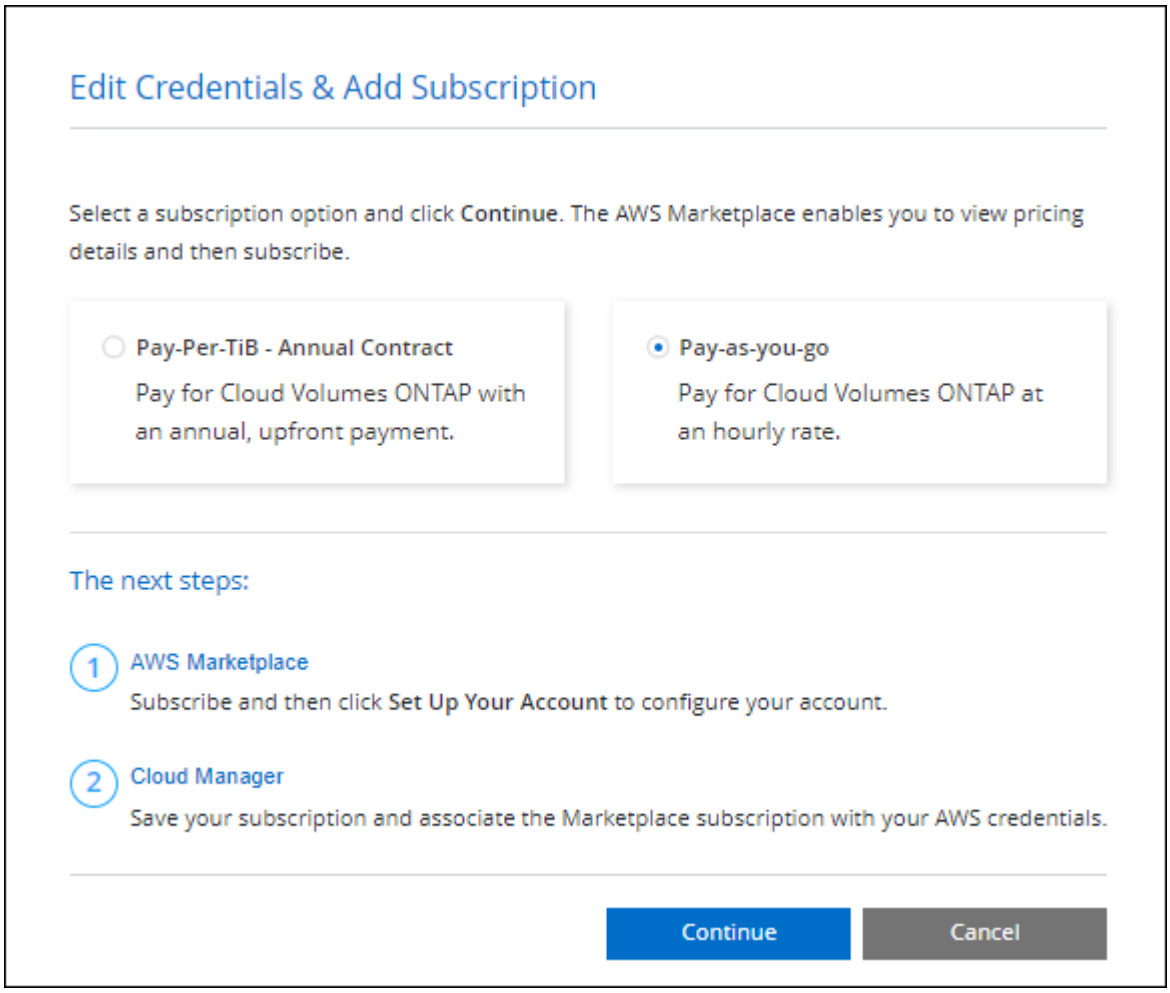
PAYGO 구독

클라우드 공급업체의 마켓플레이스에서 제공하는 혜택을 구독하여 시간당 요금을 지불하세요.

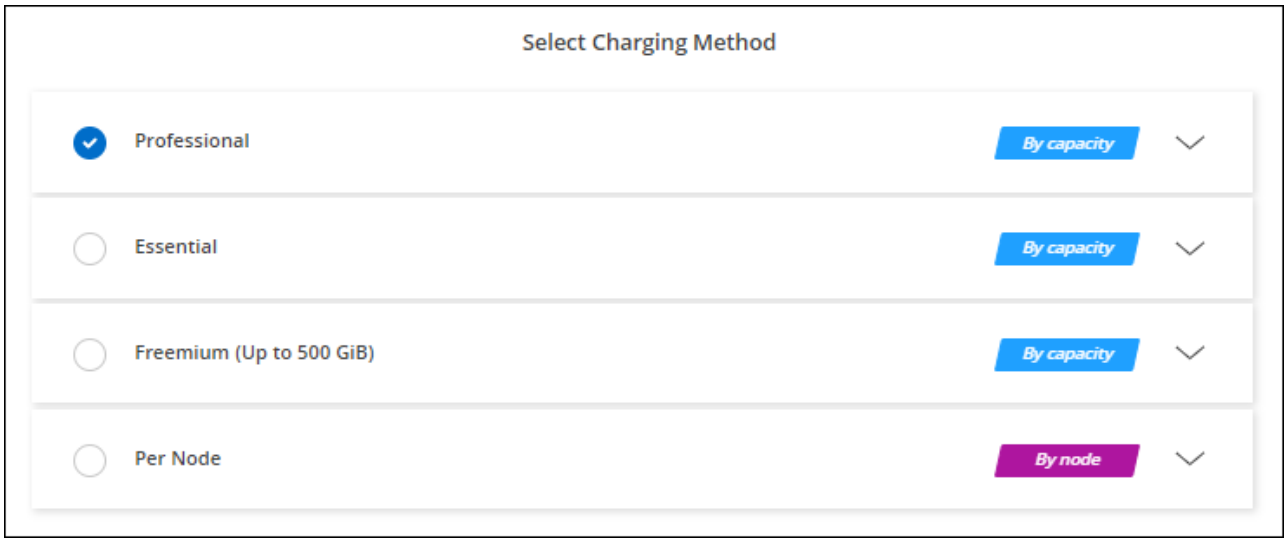
Cloud Volumes ONTAP 시스템을 생성하면 콘솔에서 AWS Marketplace에서 제공되는 계약에 가입하라는 메시지가 표시됩니다. 해당 구독은 요금 청구를 위해 시스템에 연결됩니다. 동일한 구독을 추가 Cloud Volumes ONTAP 시스템에도 사용할 수 있습니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.
   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음 프롬프트에 따라 AWS Marketplace에서 사용량에 따라 지불하는 서비스를 구독합니다.



   b. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



"AWS에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

설정 > 자격 증명 페이지에서 AWS 계정과 연결된 AWS Marketplace 구독을 관리할 수 있습니다. "AWS 계정 및 구독을 관리하는 방법을 알아보세요"

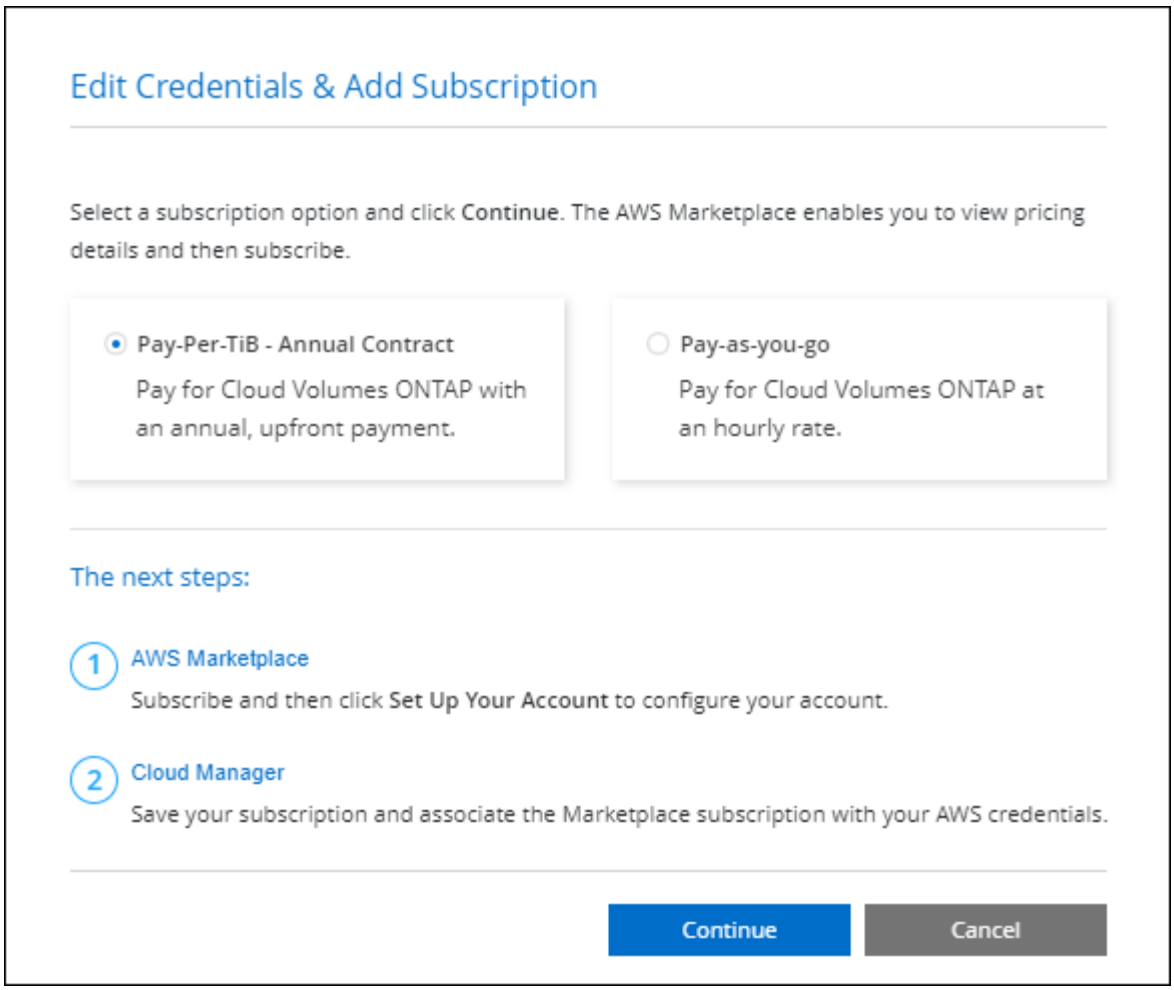
연간 계약

클라우드 공급업체의 마켓플레이스에서 연간 계약을 구매하여 연간으로 지불하세요.

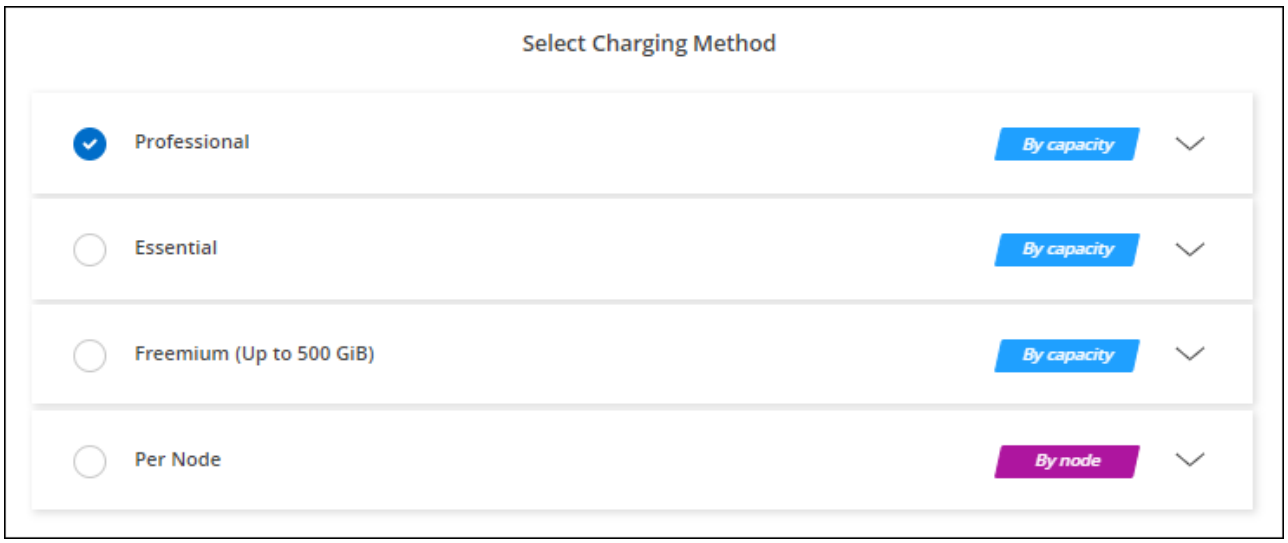
시간당 구독과 비슷하게, 콘솔에서는 AWS Marketplace에서 제공되는 연간 계약을 구독하라는 메시지가 표시됩니다.

단계

1. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.
   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 메시지에 따라 AWS Marketplace에서 연간 계약을 구독하세요.



b. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



"AWS에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

Keystone 구독

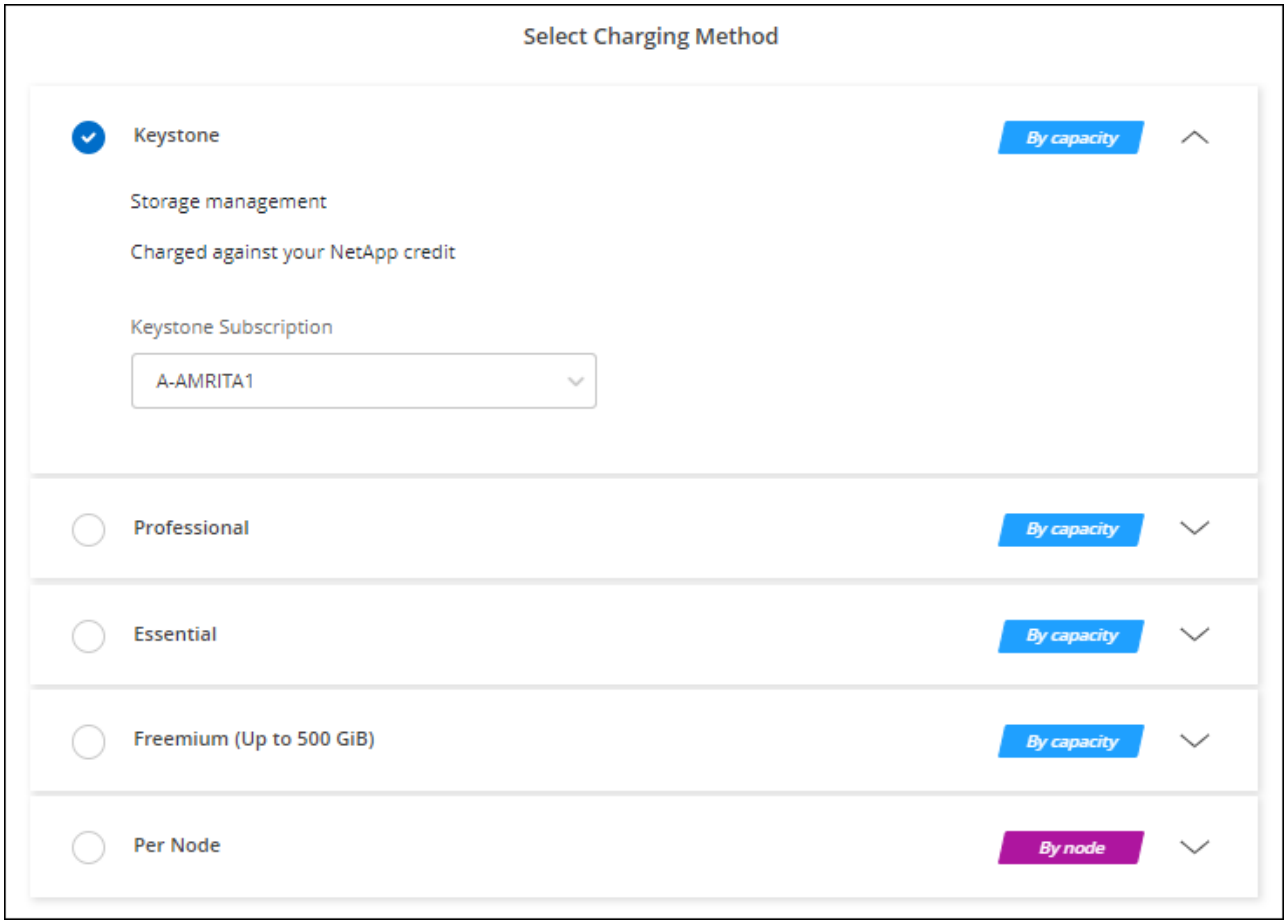
Keystone 구독은 사용량에 따라 비용을 지불하는 구독 기반 서비스입니다. "NetApp Keystone 구독에 대해 자세히

알아보세요" .

단계

1. 아직 구독이 없으신 경우, "NetApp 에 문의하세요"
2. 사용자 계정에 하나 이상의 Keystone 구독을 승인하려면 NetApp 에 문의으로 이메일을 보내주세요.
3. NetApp 귀하의 계정을 승인한 후,"Cloud Volumes ONTAP 과 함께 사용할 구독을 연결하세요" .
4. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.

    a. 청구 방법을 선택하라는 메시지가 표시되면 Keystone 구독 청구 방법을 선택하세요.



"AWS에서 Cloud Volumes ONTAP 시작하기 위한 단계별 지침을 확인하세요." .

노드 기반 라이센스

노드 기반 라이선스는 Cloud Volumes ONTAP 의 이전 세대 라이선스입니다. 노드 기반 라이선스는 NetApp (BYOL)에서 구매할 수 있으며, 특정 경우에만 라이선스를 갱신할 수 있습니다. 자세한 내용은 다음을 참조하세요.

- "노드 기반 라이선스의 가용성 종료"
- "노드 기반 라이선스 제공 종료"
- "노드 기반 라이선스를 용량 기반 라이선스로 변환"

빠른 배포를 사용하여 AWS에 Cloud Volumes ONTAP 배포

단일 노드와 고가용성(HA) 구성 모두에 대해 빠른 배포 방법을 사용하여 AWS에 Cloud Volumes ONTAP 배포할 수 있습니다. 이 간소화된 프로세스는 고급 방법에 비해 배포 단계를 줄여줍니다. 또한 단일 페이지에 기본값을 자동으로 설정하고 탐색을 최소화하여 작업 흐름을 더 명확하게 해줍니다.

시작하기 전에

NetApp Console 에서 AWS에 Cloud Volumes ONTAP 시스템을 추가하려면 다음이 필요합니다.

- 이미 실행 중인 콘솔 에이전트입니다.
  - 당신은 ~을 가져야합니다 "프로젝트 또는 작업 공간과 연결된 콘솔 에이전트" .
  - "항상 콘솔 에이전트를 실행 상태로 두어야 합니다." .
- 사용하려는 구성에 대한 이해.

  구성을 선택하고 관리자로부터 AWS 네트워킹 정보를 얻어서 준비했어야 합니다. 자세한 내용은 다음을 참조하세요."Cloud Volumes ONTAP 구성 계획" .
- Cloud Volumes ONTAP 에 대한 라이선싱을 설정하는 데 필요한 사항에 대한 이해.

  "라이선싱 설정 방법 알아보기" .
- CIFS 구성을 위한 DNS 및 Active Directory.

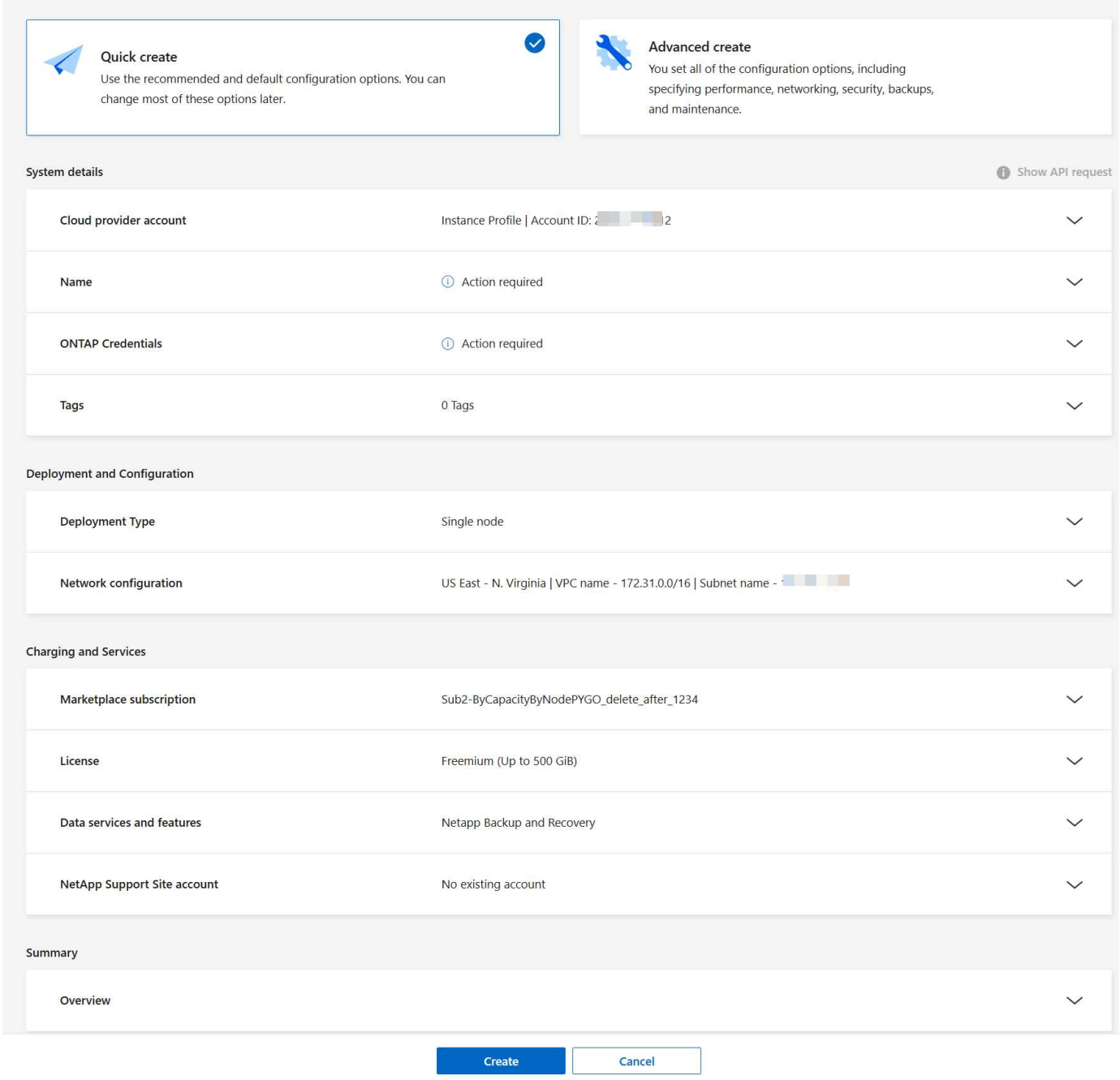
  자세한 내용은 다음을 참조하세요."AWS의 Cloud Volumes ONTAP 에 대한 네트워킹 요구 사항" .

이 작업에 관하여

Cloud Volumes ONTAP 시스템을 생성한 직후, NetApp Console 지정된 VPC에서 테스트 인스턴스를 시작하여 연결을 확인합니다. 성공하면 콘솔은 즉시 인스턴스를 종료한 다음 시스템 배포를 시작합니다. 콘솔에서 연결을 확인할 수 없는 경우 시스템 생성이 실패합니다. 테스트 인스턴스는 다음 중 하나입니다. `t2.nano` (기본 VPC 테넌시의 경우) 또는 `m3.medium` (전용 VPC 테넌시용).

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 캔버스 페이지에서 *시스템 추가*를 클릭하고 안내를 따르세요.
3. **Amazon Web Services** > * Cloud Volumes ONTAP* > 새로 추가*를 선택합니다. 기본적으로 *빠른 생성 옵션이 선택되어 있습니다.



시스템 세부 정보

1. 클라우드 공급자 계정: 선택한 콘솔 에이전트에 따라 계정 세부 정보가 자동으로 채워집니다. 여러 계정이 있는 경우 사용할 계정을 선택하세요. 콘솔 에이전트를 사용할 수 없는 경우 다음 메시지가 표시됩니다. "콘솔 에이전트 생성" .
2. 이름: 시스템 이름입니다. 콘솔은 시스템(클러스터) 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Amazon EC2 인스턴스의 이름을 지정합니다. 해당 옵션을 선택하면 사전 정의된 보안 그룹의 접두사로도 이름이 사용됩니다.
3. * ONTAP 자격 증명* 이는 Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하면 ONTAP System Manager나 ONTAP CLI를 통해 Cloud Volumes ONTAP 에 연결할 수 있습니다. 기본 *admin* 사용자 이름을 유지하거나 사용자 지정 사용자 이름으로 변경할 수 있습니다.
4. 태그 AWS 태그는 AWS 리소스에 대한 메타데이터입니다. 콘솔은 Cloud Volumes ONTAP 인스턴스와 인스턴스에 연결된 각 AWS 리소스에 태그를 추가합니다. Cloud Volumes ONTAP 시스템을 생성할 때 사용자 인터페이스에서 최대 15개의 태그를 추가할 수 있으며, 시스템을 생성한 후에 태그를 더 추가할 수 있습니다. API는 시스템을 생성할

때 태그를 4개로 제한하지 않습니다. 태그에 대한 정보는 다음을 참조하세요. "AWS 설명서: Amazon EC2 리소스 태그 지정" .

배포 및 구성

1. 배포 유형: 사용할 배포 유형을 선택합니다. 단일 노드, 단일 가용성 영역(AZ)의 고가용성(HA), 여러 AZ의 HA입니다.
2. 네트워크 구성 : 기록해 두신 네트워크 정보를 입력하세요. "AWS 워크시트" .
   a. **AWS** 지역: 기본적으로 서브넷 리소스가 있는 VPC가 있는 연결된 클라우드 계정의 지역이 선택됩니다.
   b. **VPC**: 서브넷이 있는 AWS 지역의 VPC를 입력하세요. 서브넷이 없으면 VPC의 기본값이 선택됩니다.
   c. 서브넷: 단일 노드 배포 또는 단일 AZ의 HA 배포에 대해서만 VPC에 대한 서브넷을 선택할 수 있습니다.

고가용성

HA 구성을 선택한 경우 다음 정보를 입력하세요.

단일 **AZ**의 **HA**

1. 중재자 접근: 중재자 접근 정보를 지정합니다. 중재자는 HA 쌍의 상태를 모니터링하고 장애 발생 시 쿼럼을 제공하는 별도의 인스턴스입니다. AWS EC2 서비스에 연결할 수 있도록 중재자 인스턴스에 키 쌍 이름을 제공하고 연결 방법을 선택합니다.

여러 **AZ**의 **HA**

1. 가용성 영역 및 중재자: 각 노드와 중재자에 대한 가용성 영역(AZ)과 Cloud Volumes ONTAP HA 쌍을 배포하려는 해당 서브넷을 선택합니다.
2. 유동 **IP**: 여러 AZ를 선택한 경우 NFS 및 CIFS 서비스와 클러스터 및 SVM 관리를 위한 유동 IP 주소를 지정합니다. IP 주소는 해당 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 합니다. 추가 세부 사항은 다음을 참조하세요."여러 AZ에서 Cloud Volumes ONTAP HA에 대한 AWS 네트워킹 요구 사항" .
3. 중재자 접근: 중재자 접근 정보를 지정합니다. 중재자는 HA 쌍의 상태를 모니터링하고 장애 발생 시 쿼럼을 제공하는 별도의 인스턴스입니다. AWS EC2 서비스에 연결할 수 있도록 중재자 인스턴스에 키 쌍 이름을 제공하고 연결 방법을 선택합니다.
4. 경로 테이블: 여러 AZ를 선택한 경우, 플로팅 IP 주소에 대한 경로가 포함된 경로 테이블을 선택합니다. 두 개 이상의 경로 테이블이 있는 경우 올바른 경로 테이블을 선택하는 것이 중요합니다. 그렇지 않으면 일부 클라이언트가 Cloud Volumes ONTAP HA 쌍에 액세스하지 못할 수도 있습니다. 경로 테이블에 대한 자세한 내용은 다음을 참조하세요. "AWS 문서: 라우팅 테이블" .

충전 및 서비스

1. 마켓플레이스 구독: 이 Cloud Volumes ONTAP 시스템과 함께 사용할 AWS 마켓플레이스 구독을 선택하세요.
2. 라이선스: 이 Cloud Volumes ONTAP 시스템에 사용할 라이선스 유형을 선택하세요. Professional, Essential, Premium 라이선스 중에서 선택할 수 있습니다. 다양한 라이센스에 대한 정보는 다음을 참조하세요."Cloud Volumes ONTAP 라이선스에 대해 알아보세요" .
3. 데이터 서비스 및 기능: Cloud Volumes ONTAP 에서 사용하지 않으려는 서비스를 활성화 상태로 유지하거나 비활성화합니다.
   - "NetApp 분류에 대해 자세히 알아보세요"
   - "NetApp Backup and Recovery 에 대해 자세히 알아보세요"
   - "Cloud Volumes ONTAP 의 WORM 스토리지에 대해 알아보세요"

WORM 및 데이터 계층화를 활용하려면 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 시스템을 배포해야 합니다.

- * NetApp 지원 사이트 계정*: 계정이 여러 개인 경우 사용할 계정을 선택하세요.

요약

입력한 세부 정보를 확인하거나 편집한 다음 *만들기*를 클릭하세요.

배포 프로세스가 완료된 후에는 AWS 클라우드 포털에서 시스템 생성 Cloud Volumes ONTAP 구성, 특히 시스템 태그를 수정하지 마세요. 이러한 구성을 변경하면 예기치 않은 동작이나 데이터 손실이 발생할 수 있습니다.

관련 링크

- "Cloud Volumes ONTAP 구성 계획"
- "고급 배포를 사용하여 AWS에 Cloud Volumes ONTAP 배포"

AWS에서 Cloud Volumes ONTAP 실행

AWS에서 단일 시스템 구성이나 HA 쌍으로 Cloud Volumes ONTAP 시작할 수 있습니다. 이 방법은 빠른 배포 방법보다 더 많은 구성 옵션과 유연성을 제공하는 고급 배포 환경을 제공합니다.

시작하기 전에

시작하기 전에 다음 사항이 필요합니다.

- 이미 실행 중인 콘솔 에이전트입니다.
  - 당신은 ~을 가져야합니다 "시스템과 연결된 콘솔 에이전트" .
  - "항상 콘솔 에이전트를 실행 상태로 두어야 합니다." .
- 사용하려는 구성에 대한 이해.

  구성을 선택하고 관리자로부터 AWS 네트워킹 정보를 얻어서 준비했어야 합니다. 자세한 내용은 다음을 참조하세요."Cloud Volumes ONTAP 구성 계획" .

- Cloud Volumes ONTAP 에 대한 라이선싱을 설정하는 데 필요한 사항에 대한 이해.

  "라이선싱 설정 방법 알아보기" .

- CIFS 구성을 위한 DNS 및 Active Directory.

  자세한 내용은 다음을 참조하세요."AWS의 Cloud Volumes ONTAP 에 대한 네트워킹 요구 사항" .

AWS에서 단일 노드 Cloud Volumes ONTAP 시스템 실행

AWS에서 Cloud Volumes ONTAP 시작하려면 NetApp Console 에서 새 시스템을 만들어야 합니다.

이 작업에 관하여

시스템을 생성한 직후, 콘솔은 지정된 VPC에서 테스트 인스턴스를 시작하여 연결을 확인합니다. 성공하면 콘솔은 즉시 인스턴스를 종료한 다음 Cloud Volumes ONTAP 시스템 배포를 시작합니다. 연결성을 검증할 수 없으면 시스템 생성이 실패합니다. 테스트 인스턴스는 다음 중 하나입니다. `t2.nano` (기본 VPC 테넌시의 경우) 또는 `m3.medium` (전용 VPC 테넌시용).

단계

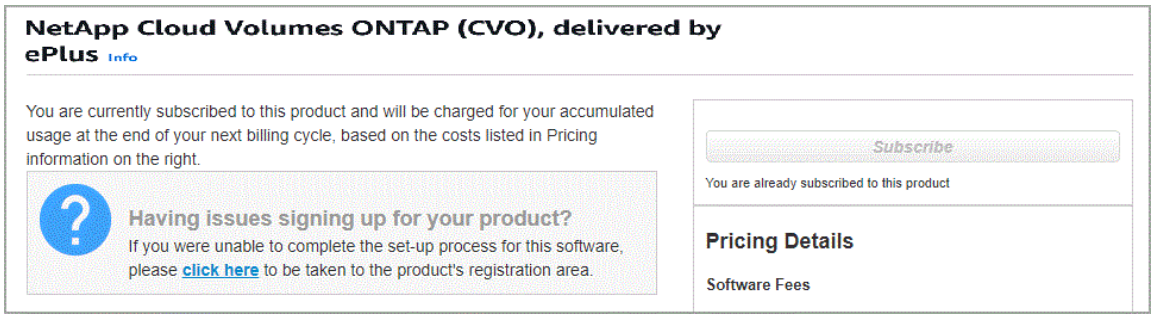
1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 안내를 따르세요.
3. *Amazon Web Services*와 * Cloud Volumes ONTAP Single Node*를 선택하세요.
4. 고급 만들기*를 선택하세요. 기본적으로 *빠른 생성 모드가 선택되어 있으므로 기본값에 대한 메시지가 표시될 수 있습니다. *계속*을 클릭하세요.
5. 메시지가 표시되면 "콘솔 에이전트 생성" .
6. 세부 정보 및 자격 증명: 선택적으로 AWS 자격 증명과 구독을 변경하고, 시스템 이름을 입력하고, 필요한 경우 태그를 추가한 다음 비밀번호를 입력합니다.

   이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
시스템 이름	콘솔은 시스템 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Amazon EC2 인스턴스의 이름을 지정합니다. 해당 옵션을 선택하면 사전 정의된 보안 그룹의 접두사로도 이름이 사용됩니다.
태그 추가	AWS 태그는 AWS 리소스에 대한 메타데이터입니다. 콘솔은 Cloud Volumes ONTAP 인스턴스와 인스턴스에 연결된 각 AWS 리소스에 태그를 추가합니다. 시스템을 생성할 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 시스템을 생성한 후에 태그를 더 추가할 수 있습니다. API는 시스템을 생성할 때 태그를 4개로 제한하지 않습니다. 태그에 대한 정보는 다음을 참조하세요. "AWS 설명서: Amazon EC2 리소스 태그 지정" .
사용자 이름과 비밀번호	이는 Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하면 ONTAP System Manager나 ONTAP CLI를 통해 Cloud Volumes ONTAP 에 연결할 수 있습니다. 기본 *admin* 사용자 이름을 유지하거나 사용자 지정 사용자 이름으로 변경하세요.
자격 증명 편집	이 시스템을 배포하려는 계정과 연결된 AWS 자격 증명을 선택하세요. AWS 마켓플레이스 구독을 연결하여 이 Cloud Volumes ONTAP 시스템과 함께 사용할 수도 있습니다. 선택한 자격 증명을 새 AWS 마켓플레이스 구독과 연결하려면 *구독 추가*를 클릭하세요. 구독은 연간 계약 또는 시간당 요금으로 Cloud Volumes ONTAP 결제할 수 있습니다. "NetApp Console 에 추가 AWS 자격 증명을 추가하는 방법을 알아보세요." .

여러 IAM 사용자가 동일한 AWS 계정에서 작업하는 경우 각 사용자는 구독해야 합니다. 첫 번째 사용자가 구독한 후, AWS 마켓플레이스는 다음 사용자에게 이미 구독되었음을 알립니다(아래 이미지 참조). AWS 계정에 대한 구독이 있는 동안 각 IAM 사용자는 해당 구독에 자신을 연결해야 합니다. 아래에 표시된 메시지가 나타나면 여기를 클릭 링크를 클릭하여 콘솔 웹사이트로 이동하여 프로세스를 완료하세요

.



7. 서비스: Cloud Volumes ONTAP 에서 사용하지 않으려는 서비스를 활성화 상태로 유지하거나 개별 서비스를 비활성화합니다.
   - "NetApp Data Classification 에 대해 자세히 알아보세요"
   - "NetApp Backup and Recovery 에 대해 자세히 알아보세요"

   WORM 및 데이터 계층화를 활용하려면 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 시스템을 배포해야 합니다.

8. 위치 및 연결: 기록한 네트워크 정보를 입력하세요. "AWS 워크시트" .

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
VPC	AWS Outpost가 있는 경우 Outpost VPC를 선택하여 해당 Outpost에 단일 노드 Cloud Volumes ONTAP 시스템을 배포할 수 있습니다. 경험은 AWS에 있는 다른 VPC와 동일합니다.
생성된 보안 그룹	콘솔에서 보안 그룹을 생성하도록 허용하는 경우 트래픽 허용 방법을 선택해야 합니다. • *선택한 VPC만*을 선택하는 경우 인바운드 트래픽의 소스는 선택한 VPC의 서브넷 범위와 콘솔 에이전트가 있는 VPC의 서브넷 범위입니다. 이것은 권장되는 옵션입니다. • *모든 VPC*를 선택하면 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
기존 보안 그룹 사용	기존 방화벽 정책을 사용하는 경우 필요한 규칙이 포함되어 있는지 확인하세요. "Cloud Volumes ONTAP 의 방화벽 규칙에 대해 알아보세요" .

9. 데이터 암호화: 데이터 암호화를 사용하지 않거나 AWS에서 관리하는 암호화를 선택합니다.

   AWS 관리 암호화의 경우, 귀하의 계정이나 다른 AWS 계정에서 다른 고객 마스터 키(CMK)를 선택할 수 있습니다.

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

"Cloud Volumes ONTAP 에 AWS KMS를 설정하는 방법을 알아보세요." .

"지원되는 암호화 기술에 대해 자세히 알아보세요" .

10. 청구 방법 및 **NSS** 계정: 이 시스템에서 사용할 청구 옵션을 지정한 다음 NetApp 지원 사이트 계정을 지정하세요.
    - "Cloud Volumes ONTAP 에 대한 라이선싱 옵션에 대해 알아보세요" .
    - "라이선싱 설정 방법 알아보기" .
11. * Cloud Volumes ONTAP 구성* (연간 AWS 마켓플레이스 계약에만 해당): 기본 구성을 검토하고 *계속*을 클릭하거나 *구성 변경*을 클릭하여 원하는 구성을 선택합니다.

    기본 구성을 유지하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.

12. 사전 구성된 패키지: Cloud Volumes ONTAP 빠르게 시작하려면 패키지 중 하나를 선택하거나, *구성 변경*을 클릭하여 원하는 구성을 선택하세요.

    패키지 중 하나를 선택하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.

13. **IAM** 역할: 콘솔에서 역할을 자동으로 생성하도록 기본 옵션을 유지하는 것이 가장 좋습니다.

    자체 정책을 사용하려면 다음 사항을 충족해야 합니다."Cloud Volumes ONTAP 노드에 대한 정책 요구 사항" .

14. 라이선스: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 인스턴스 유형과 인스턴스 테넌시를 선택합니다.

    선택한 버전에 대해 최신 릴리스 후보, 일반 공급 또는 패치 릴리스가 제공되는 경우 콘솔은 시스템을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.13.1을 선택하고 9.13.1 P4를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리스에서 다른 릴리스로 전달되지 않습니다(예: 9.13에서 9.14로 전달).

15. 기본 스토리지 리소스: 디스크 유형을 선택하고, 기본 스토리지를 구성하고, 데이터 계층화를 계속 사용할지 여부를 선택합니다.

    다음 사항에 유의하세요.

    - 디스크 유형은 초기 볼륨(및 집계)을 위한 것입니다. 이후 볼륨(및 집계)에 대해 다른 디스크 유형을 선택할 수 있습니다.
    - gp3 또는 io1 디스크를 선택하면 콘솔은 AWS의 Elastic Volumes 기능을 사용하여 필요에 따라 기본 스토리지 디스크 용량을 자동으로 늘립니다. 스토리지 요구 사항에 따라 초기 용량을 선택하고 Cloud Volumes ONTAP 배포한 후 수정할 수 있습니다. "AWS에서 Elastic Volumes 지원에 대해 자세히 알아보세요" .
    - gp2 또는 st1 디스크를 선택하는 경우 초기 집계의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 콘솔에서 생성하는 추가 집계에 대한 디스크 크기를 선택할 수 있습니다. 고급 할당 옵션을 사용하면 다른 디스크 크기를 사용하는 집계를 만들 수 있습니다.
    - 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
    - 데이터 계층화를 비활성화하면 이후 집계에서 활성화할 수 있습니다.

      "데이터 계층화 작동 방식 알아보기" .

16. 쓰기 속도 및 **WORM**:

    a. 원하는 경우 보통 또는 높음 쓰기 속도를 선택하세요.

"쓰기 속도에 대해 자세히 알아보세요" .

b. 원하는 경우 WORM(한 번 쓰고 여러 번 읽기) 저장소를 활성화합니다.

Cloud Volumes ONTAP 버전 9.7 이하에서 데이터 계층화가 활성화된 경우 WORM을 활성화할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로 되돌리거나 다운그레이드하는 것이 차단됩니다.

"WORM 스토리지에 대해 자세히 알아보세요" .

a. WORM 저장소를 활성화하는 경우 보존 기간을 선택하세요.

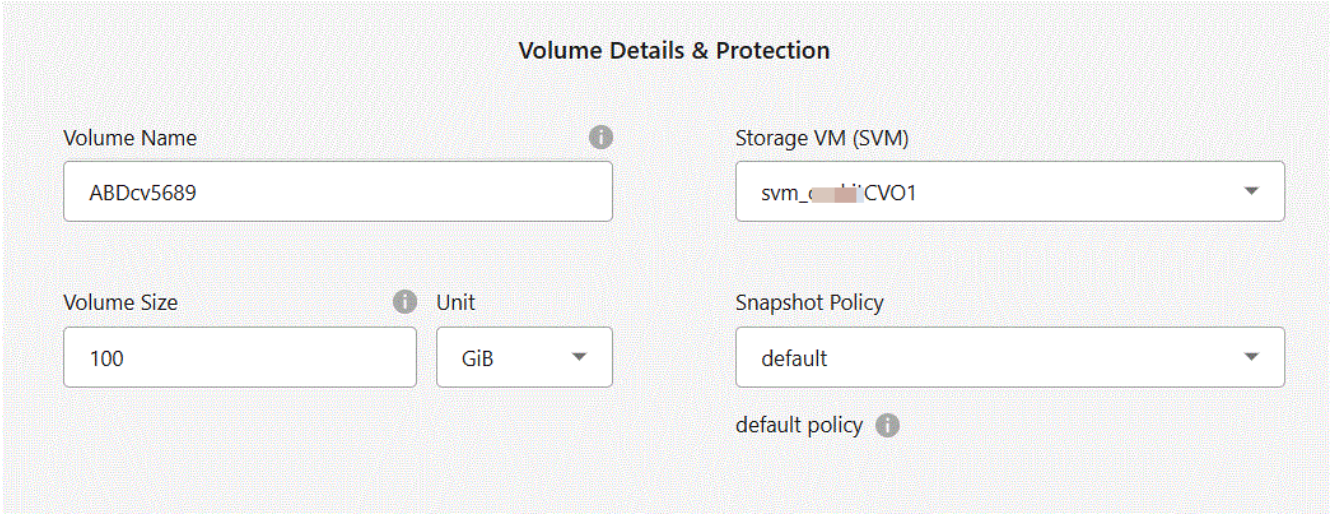
17. 볼륨 만들기: 새 볼륨에 대한 세부 정보를 입력하거나 *건너뛰기*를 클릭합니다.

"지원되는 클라이언트 프로토콜 및 버전에 대해 알아보세요" .

이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝을 활성화하는지 여부에 따라 크게 달라집니다. 씬 프로비저닝을 활성화하면 현재 사용 가능한 물리적 저장소보다 큰 볼륨을 만들 수 있습니다.
액세스 제어(NFS에만 해당)	내보내기 정책은 볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 콘솔은 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS에만 해당)	이러한 필드를 사용하면 사용자 및 그룹의 공유 액세스 수준(액세스 제어 목록 또는 ACL이라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자나 그룹, 또는 UNIX 사용자나 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자 도메인을 포함해야 합니다.
스냅샷 정책	스냅샷 복사 정책은 NetApp 스냅샷 복사본이 자동으로 생성되는 빈도와 수를 지정합니다. NetApp 스냅샷 복사본은 성능에 영향을 미치지 않고 최소한의 저장 공간만 필요한 특정 시점의 파일 시스템 이미지입니다. 기본 정책을 선택하거나 아무것도 선택하지 않을 수 있습니다. 일시적인 데이터의 경우 '없음'을 선택할 수 있습니다. 예를 들어 Microsoft SQL Server의 경우 tempdb를 선택합니다.
고급 옵션(NFS에만 해당)	볼륨에 대한 NFS 버전을 선택합니다: NFSv3 또는 NFSv4.
이니시에이터 그룹 및 IQN(iSCSI에만 해당)	iSCSI 스토리지 대상은 LUN(논리 단위)이라고 하며 호스트에 표준 블록 장치로 표시됩니다. 이니시에이터 그룹은 iSCSI 호스트 노드 이름 테이블이며, 어떤 이니시에이터가 어떤 LUN에 액세스할 수 있는지 제어합니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 컨버지드 네트워크 어댑터(CNA) 또는 전용 호스트 버스 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 정규화된 이름(IQN)으로 식별됩니다. iSCSI 볼륨을 생성하면 콘솔이 자동으로 LUN을 생성합니다. 볼륨당 LUN을 하나만 만들어서 간편하게 관리할 수 있도록 했습니다. 볼륨을 생성한 후, "IQN을 사용하여 호스트에서 LUN에 연결합니다." .

다음 이미지는 볼륨 생성 마법사의 첫 번째 페이지를 보여줍니다.



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

필드	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 가입할 도메인의 Active Directory LDAP 서버와 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
가입할 Active Directory 도메인	CIFS 서버에 가입하려는 Active Directory(AD) 도메인의 FQDN입니다.
도메인에 가입할 수 있는 권한이 있는 자격 증명	AD 도메인 내의 지정된 조직 단위(OU)에 컴퓨터를 추가할 수 있는 권한이 있는 Windows 계정의 이름과 비밀번호입니다.
CIFS 서버 NetBIOS 이름	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. Cloud Volumes ONTAP 의 AD 서버로 AWS Managed Microsoft AD를 구성하는 경우 이 필드에 *OU=Computers,OU=corp*를 입력해야 합니다.
DNS 도메인	Cloud Volumes ONTAP 스토리지 가상 머신(SVM)의 DNS 도메인입니다. 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 참조하세요 "NetApp Console 자동화 문서" 자세한 내용은. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 만든 후에는 구성할 수 없습니다.

19. 사용 프로필, 디스크 유형 및 계층화 정책: 스토리지 효율성 기능을 활성화할지 여부를 선택하고 필요한 경우 볼륨 계층화 정책을 편집합니다.

    자세한 내용은 다음을 참조하세요."볼륨 사용 프로필 이해" ,"데이터 계층화 개요" , 그리고 "KB: CVO에서는 어떤 인라인 스토리지 효율성 기능이 지원되나요?"

20. 검토 및 승인: 선택 사항을 검토하고 확인합니다.

    a. 구성에 대한 세부 정보를 검토하세요.

    b. *자세한 정보*를 클릭하면 콘솔에서 구매할 지원 및 AWS 리소스에 대한 세부 정보를 검토할 수 있습니다.

c. 이해합니다... 확인란을 선택하세요.

d. *이동*을 클릭하세요.

결과

콘솔은 Cloud Volumes ONTAP 인스턴스를 시작합니다. 감사 페이지에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 인스턴스를 시작하는 데 문제가 있는 경우 실패 메시지를 검토하세요. 시스템을 선택하고 *환경 다시 만들기*를 클릭할 수도 있습니다.

추가 도움말을 보려면 다음으로 이동하세요. "NetApp Cloud Volumes ONTAP 지원" .

배포 프로세스가 완료된 후에는 AWS 클라우드 포털에서 시스템 생성 Cloud Volumes ONTAP 구성, 특히 시스템 태그를 수정하지 마세요. 이러한 구성을 변경하면 예기치 않은 동작이나 데이터 손실이 발생할 수 있습니다.

당신이 완료한 후

- CIFS 공유를 프로비저닝한 경우 사용자 또는 그룹에 파일과 폴더에 대한 권한을 부여하고 해당 사용자가 공유에 액세스하여 파일을 만들 수 있는지 확인합니다.
- 볼륨에 할당량을 적용하려면 ONTAP 시스템 관리자나 ONTAP CLI를 사용하세요.

  할당량을 사용하면 사용자, 그룹 또는 Qtree에서 사용하는 디스크 공간과 파일 수를 제한하거나 추적할 수 있습니다.

AWS에서 Cloud Volumes ONTAP HA 쌍 실행

AWS에서 Cloud Volumes ONTAP HA 쌍을 시작하려면 콘솔에서 HA 시스템을 만들어야 합니다.

한정

현재 AWS Outposts에서는 HA 쌍이 지원되지 않습니다.

이 작업에 관하여

Cloud Volumes ONTAP 시스템을 생성한 직후, 콘솔은 지정된 VPC에서 테스트 인스턴스를 시작하여 연결을 확인합니다. 성공하면 콘솔은 즉시 인스턴스를 종료한 다음 Cloud Volumes ONTAP 시스템 배포를 시작합니다. 연결성을 검증할 수 없으면 시스템 생성이 실패합니다. 테스트 인스턴스는 다음 중 하나입니다. `t2.nano` (기본 VPC 테넌시의 경우) 또는 `m3.medium` (전용 VPC 테넌시용).

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 화면의 지시를 따르세요.
3. *Amazon Web Services*와 * Cloud Volumes ONTAP HA*를 선택하세요.

   일부 AWS 로컬 영역을 사용할 수 있습니다.

   AWS 로컬 영역을 사용하려면 먼저 로컬 영역을 활성화하고 AWS 계정의 로컬 영역에 서브넷을 생성해야 합니다. AWS 로컬 영역에 가입하기* 및 Amazon VPC를 로컬 영역으로 확장하기* 단계를 따르세요."AWS 튜토리얼 "AWS 로컬 영역을 사용하여 저지연 애플리케이션 배포 시작하기"" .

   콘솔 에이전트 3.9.36 이하를 실행 중인 경우 다음을 추가해야 합니다. `DescribeAvailabilityZones` AWS

EC2 콘솔에서 AWS 역할에 대한 권한.

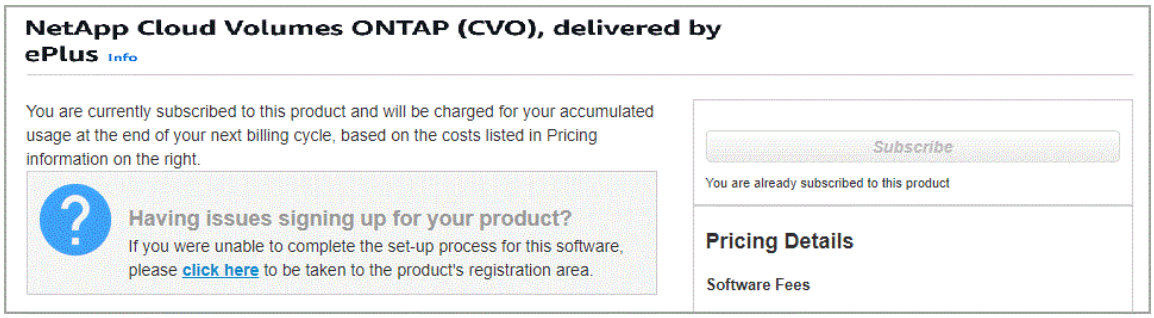
4. 세부 정보 및 자격 증명: 선택적으로 AWS 자격 증명과 구독을 변경하고, 시스템 이름을 입력하고, 필요한 경우 태그를 추가한 다음 비밀번호를 입력합니다.

   이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
시스템 이름	콘솔은 시스템 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Amazon EC2 인스턴스의 이름을 지정합니다. 해당 옵션을 선택하면 사전 정의된 보안 그룹의 접두사로도 이름이 사용됩니다.
태그 추가	AWS 태그는 AWS 리소스에 대한 메타데이터입니다. 콘솔은 Cloud Volumes ONTAP 인스턴스와 인스턴스에 연결된 각 AWS 리소스에 태그를 추가합니다. 시스템을 생성할 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 시스템을 생성한 후에 태그를 더 추가할 수 있습니다. API는 시스템을 생성할 때 태그를 4개로 제한하지 않습니다. 태그에 대한 정보는 다음을 참조하세요. "AWS 설명서: Amazon EC2 리소스 태그 지정" .
사용자 이름과 비밀번호	이는 Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하면 ONTAP System Manager나 ONTAP CLI를 통해 Cloud Volumes ONTAP 에 연결할 수 있습니다. 기본 *admin* 사용자 이름을 유지하거나 사용자 지정 사용자 이름으로 변경하세요.
자격 증명 편집	이 Cloud Volumes ONTAP 시스템에 사용할 AWS 자격 증명과 마켓플레이스 구독을 선택하세요. 선택한 자격 증명을 새 AWS 마켓플레이스 구독과 연결하려면 *구독 추가*를 클릭하세요. 구독은 연간 계약 또는 시간당 요금으로 Cloud Volumes ONTAP 결제할 수 있습니다. NetApp 에서 직접 라이선스를 구매한 경우(BYOL(Bring Your Own License)), AWS 구독은 필요하지 않습니다. NetApp BYOL 라이선스 구매, 연장 및 갱신을 제한하고 있습니다. 자세한 내용은 다음을 참조하세요. "Cloud Volumes ONTAP 에 대한 BYOL 라이선싱의 제한된 가용성" . "콘솔에 추가 AWS 자격 증명을 추가하는 방법을 알아보세요." .

여러 IAM 사용자가 동일한 AWS 계정에서 작업하는 경우 각 사용자는 구독해야 합니다. 첫 번째 사용자가 구독한 후, AWS 마켓플레이스는 아래 이미지에서 볼 수 있듯이 후속 사용자에게 이미 구독되었음을 알립니다. AWS 계정에 대한 구독이 있는 동안 각 IAM 사용자는 해당 구독에 자신을 연결해야 합니다. 아래에 표시된 메시지가 나타나면 여기를 클릭 링크를 클릭하여 콘솔 웹사이트로 이동하여 프로세스를 완료하세요

.



5. 서비스: 해당 Cloud Volumes ONTAP 시스템에서 사용하지 않으려는 서비스를 활성화 상태로 유지하거나 개별 서비스를 비활성화합니다.

   - "NetApp Data Classification 에 대해 자세히 알아보세요"

◦ "백업 및 복구에 대해 자세히 알아보세요"

WORM 및 데이터 계층화를 활용하려면 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 시스템을 배포해야 합니다.

6. **HA** 배포 모델: HA 구성을 선택하세요.

   배포 모델 개요는 다음을 참조하세요."AWS용 Cloud Volumes ONTAP HA" .

7. 위치 및 연결(단일 가용성 영역(AZ)) 또는 지역 및 **VPC**(여러 AZ): AWS 워크시트에 기록한 네트워크 정보를 입력합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
생성된 보안 그룹	콘솔에서 보안 그룹을 생성하도록 허용하는 경우 트래픽 허용 방법을 선택해야 합니다. • *선택한 VPC만*을 선택하는 경우 인바운드 트래픽의 소스는 선택한 VPC의 서브넷 범위와 콘솔 에이전트가 있는 VPC의 서브넷 범위입니다. 이것은 권장되는 옵션입니다. • *모든 VPC*를 선택하면 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
기존 보안 그룹 사용	기존 방화벽 정책을 사용하는 경우 필요한 규칙이 포함되어 있는지 확인하세요. "Cloud Volumes ONTAP 의 방화벽 규칙에 대해 알아보세요" .

8. 연결 및 **SSH** 인증: HA 쌍과 중재자에 대한 연결 방법을 선택합니다.
9. 유동 **IP**: 여러 AZ를 선택한 경우 유동 IP 주소를 지정하세요.

   IP 주소는 해당 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 합니다. 추가 세부 사항은 다음을 참조하세요. "여러 AZ에서 Cloud Volumes ONTAP HA에 대한 AWS 네트워킹 요구 사항" .

10. 경로 테이블: 여러 AZ를 선택한 경우, 플로팅 IP 주소에 대한 경로를 포함해야 하는 경로 테이블을 선택합니다.

    두 개 이상의 경로 테이블이 있는 경우 올바른 경로 테이블을 선택하는 것이 매우 중요합니다. 그렇지 않으면 일부 클라이언트가 Cloud Volumes ONTAP HA 쌍에 액세스하지 못할 수도 있습니다. 경로 테이블에 대한 자세한 내용은 다음을 참조하세요. "AWS 문서: 라우팅 테이블" .

11. 데이터 암호화: 데이터 암호화를 사용하지 않거나 AWS에서 관리하는 암호화를 선택합니다.

    AWS 관리 암호화의 경우, 귀하의 계정이나 다른 AWS 계정에서 다른 고객 마스터 키(CMK)를 선택할 수 있습니다.

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

    "Cloud Volumes ONTAP 에 AWS KMS를 설정하는 방법을 알아보세요." .

    "지원되는 암호화 기술에 대해 자세히 알아보세요" .

12. 청구 방법 및 **NSS** 계정: 이 시스템에서 사용할 청구 옵션을 지정한 다음 NetApp 지원 사이트 계정을 지정하세요.

- "Cloud Volumes ONTAP 에 대한 라이선싱 옵션에 대해 알아보세요" .
- "라이선싱 설정 방법 알아보기" .

13. * Cloud Volumes ONTAP 구성* (연간 AWS Marketplace 계약에만 해당): 기본 구성을 검토하고 *계속*을 클릭하거나 *구성 변경*을 클릭하여 원하는 구성을 선택합니다.

    기본 구성을 유지하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.

14. 사전 구성된 패키지(시간별 또는 BYOL만 해당): Cloud Volumes ONTAP 빠르게 시작하려면 패키지 중 하나를 선택하거나, *구성 변경*을 클릭하여 원하는 구성을 선택하세요.

    패키지 중 하나를 선택하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.

15. **IAM** 역할: 콘솔에서 역할을 자동으로 생성하도록 기본 옵션을 유지하는 것이 가장 좋습니다.

    자체 정책을 사용하려면 다음 사항을 충족해야 합니다."Cloud Volumes ONTAP 노드 및 HA 중재자에 대한 정책 요구 사항" .

16. 라이선스: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 인스턴스 유형과 인스턴스 테넌시를 선택합니다.

    선택한 버전에 대해 최신 릴리스 후보, 일반 공급 또는 패치 릴리스가 제공되는 경우 콘솔은 시스템을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.13.1을 선택하고 9.13.1 P4를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리스에서 다른 릴리스로 전달되지 않습니다(예: 9.13에서 9.14로 전달).

17. 기본 스토리지 리소스: 디스크 유형을 선택하고, 기본 스토리지를 구성하고, 데이터 계층화를 계속 사용할지 여부를 선택합니다.

    다음 사항에 유의하세요.

    - 디스크 유형은 초기 볼륨(및 집계)을 위한 것입니다. 이후 볼륨(및 집계)에 대해 다른 디스크 유형을 선택할 수 있습니다.
    - gp3 또는 io1 디스크를 선택하면 콘솔은 AWS의 Elastic Volumes 기능을 사용하여 필요에 따라 기본 스토리지 디스크 용량을 자동으로 늘립니다. 스토리지 요구 사항에 따라 초기 용량을 선택하고 Cloud Volumes ONTAP 배포한 후 수정할 수 있습니다. "AWS에서 Elastic Volumes 지원에 대해 자세히 알아보세요" .
    - gp2 또는 st1 디스크를 선택하는 경우 초기 집계의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 콘솔에서 생성하는 추가 집계에 대한 디스크 크기를 선택할 수 있습니다. 고급 할당 옵션을 사용하면 다른 디스크 크기를 사용하는 집계를 만들 수 있습니다.
    - 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
    - 데이터 계층화를 비활성화하면 이후 집계에서 활성화할 수 있습니다.

      "데이터 계층화 작동 방식 알아보기" .

18. 쓰기 속도 및 **WORM**:

    a. 원하는 경우 보통 또는 높음 쓰기 속도를 선택하세요.

       "쓰기 속도에 대해 자세히 알아보세요" .

    b. 원하는 경우 WORM(한 번 쓰고 여러 번 읽기) 저장소를 활성화합니다.

Cloud Volumes ONTAP 버전 9.7 이하에서 데이터 계층화가 활성화된 경우 WORM을 활성화할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로 되돌리거나 다운그레이드하는 것이 차단됩니다.

"WORM 스토리지에 대해 자세히 알아보세요" .

a. WORM 저장소를 활성화하는 경우 보존 기간을 선택하세요.

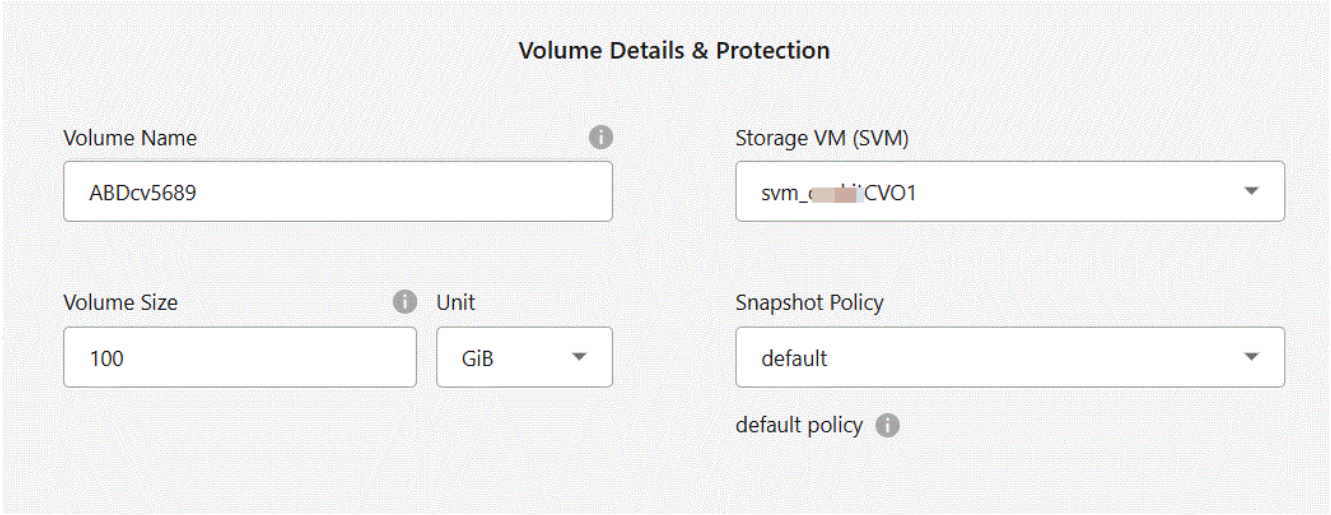
19. 볼륨 만들기: 새 볼륨에 대한 세부 정보를 입력하거나 *건너뛰기*를 클릭합니다.

"지원되는 클라이언트 프로토콜 및 버전에 대해 알아보세요" .

이 페이지의 일부 필드는 설명이 필요 없습니다. 다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝을 활성화하는지 여부에 따라 크게 달라집니다. 씬 프로비저닝을 활성화하면 현재 사용 가능한 물리적 저장소보다 큰 볼륨을 만들 수 있습니다.
액세스 제어(NFS에만 해당)	내보내기 정책은 볼륨에 액세스할 수 있는 서브넷의 클라이언트를 정의합니다. 기본적으로 콘솔은 서브넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS에만 해당)	이러한 필드를 사용하면 사용자 및 그룹의 공유 액세스 수준(액세스 제어 목록 또는 ACL이라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자나 그룹, 또는 UNIX 사용자나 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자 도메인을 포함해야 합니다.
스냅샷 정책	스냅샷 복사 정책은 NetApp 스냅샷 복사본이 자동으로 생성되는 빈도와 수를 지정합니다. NetApp 스냅샷 복사본은 성능에 영향을 미치지 않고 최소한의 저장 공간만 필요한 특정 시점의 파일 시스템 이미지입니다. 기본 정책을 선택하거나 아무것도 선택하지 않을 수 있습니다. 일시적인 데이터의 경우 '없음'을 선택할 수 있습니다. 예를 들어 Microsoft SQL Server의 경우 tempdb를 선택합니다.
고급 옵션(NFS에만 해당)	볼륨에 대한 NFS 버전을 선택합니다: NFSv3 또는 NFSv4.
이니시에이터 그룹 및 IQN(iSCSI에만 해당)	iSCSI 스토리지 대상은 LUN(논리 단위)이라고 하며 호스트에 표준 블록 장치로 표시됩니다. 이니시에이터 그룹은 iSCSI 호스트 노드 이름 테이블이며, 어떤 이니시에이터가 어떤 LUN에 액세스할 수 있는지 제어합니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 컨버지드 네트워크 어댑터(CNA) 또는 전용 호스트 버스 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 정규화된 이름(IQN)으로 식별됩니다. iSCSI 볼륨을 생성하면 콘솔이 자동으로 LUN을 생성합니다. 볼륨당 LUN을 하나만 만들어서 간편하게 관리할 수 있도록 했습니다. 볼륨을 생성한 후, "IQN을 사용하여 호스트에서 LUN에 연결합니다." .

다음 이미지는 볼륨 생성 마법사의 첫 번째 페이지를 보여줍니다.



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

필드	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 가입할 도메인의 Active Directory LDAP 서버와 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
가입할 Active Directory 도메인	CIFS 서버에 가입하려는 Active Directory(AD) 도메인의 FQDN입니다.
도메인에 가입할 수 있는 권한이 있는 자격 증명	AD 도메인 내의 지정된 조직 단위(OU)에 컴퓨터를 추가할 수 있는 권한이 있는 Windows 계정의 이름과 비밀번호입니다.
CIFS 서버 NetBIOS 이름	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. Cloud Volumes ONTAP 의 AD 서버로 AWS Managed Microsoft AD를 구성하는 경우 이 필드에 *OU=Computers,OU=corp*를 입력해야 합니다.
DNS 도메인	Cloud Volumes ONTAP 스토리지 가상 머신(SVM)의 DNS 도메인입니다. 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 참조하세요 "NetApp Console 자동화 문서" 자세한 내용은. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 만든 후에는 구성할 수 없습니다.

21. 사용 프로필, 디스크 유형 및 계층화 정책: 스토리지 효율성 기능을 활성화할지 여부를 선택하고 필요한 경우 볼륨 계층화 정책을 편집합니다.

    자세한 내용은 다음을 참조하세요."볼륨 사용 프로필을 선택하세요" 그리고"데이터 계층화 개요" .

22. 검토 및 승인: 선택 사항을 검토하고 확인합니다.

    a. 구성에 대한 세부 정보를 검토하세요.

    b. *자세한 정보*를 클릭하면 콘솔에서 구매할 지원 및 AWS 리소스에 대한 세부 정보를 검토할 수 있습니다.

    c. 이해합니다... 확인란을 선택하세요.

d. *이동*을 클릭하세요.

결과

콘솔은 Cloud Volumes ONTAP HA 쌍을 시작합니다. 감사 페이지에서 진행 상황을 추적할 수 있습니다.

HA 쌍을 시작하는 데 문제가 발생하면 실패 메시지를 검토하세요. 시스템을 선택하고 '환경 다시 만들기'를 클릭할 수도 있습니다.

추가 도움말을 보려면 다음으로 이동하세요. "NetApp Cloud Volumes ONTAP 지원" .

당신이 완료한 후

- CIFS 공유를 프로비저닝한 경우 사용자 또는 그룹에 파일과 폴더에 대한 권한을 부여하고 해당 사용자가 공유에 액세스하여 파일을 만들 수 있는지 확인합니다.
- 볼륨에 할당량을 적용하려면 ONTAP 시스템 관리자나 ONTAP CLI를 사용하세요.

  할당량을 사용하면 사용자, 그룹 또는 Qtree에서 사용하는 디스크 공간과 파일 수를 제한하거나 추적할 수 있습니다.

> 배포 프로세스가 완료된 후에는 AWS 클라우드 포털에서 시스템 생성 Cloud Volumes ONTAP 구성, 특히 시스템 태그를 수정하지 마세요. 이러한 구성을 변경하면 예기치 않은 동작이나 데이터 손실이 발생할 수 있습니다.

관련 링크

- "Cloud Volumes ONTAP 구성 계획"
- "빠른 배포를 사용하여 AWS에 Cloud Volumes ONTAP 배포"

AWS Secret Cloud 또는 AWS Top Secret Cloud에 Cloud Volumes ONTAP 배포

표준 AWS 지역과 유사하게 NetApp Console 사용할 수 있습니다."AWS 시크릿 클라우드" 그리고"AWS 최고 비밀 클라우드" 클라우드 스토리지에 엔터프라이즈급 기능을 제공하는 Cloud Volumes ONTAP 구축하세요. AWS Secret Cloud와 Top Secret Cloud는 미국 정보 커뮤니티에 한정된 폐쇄된 지역입니다. 이 페이지의 지침은 AWS Secret Cloud와 Top Secret Cloud 지역 사용자에게만 적용됩니다.

시작하기 전에

시작하기 전에 AWS Secret Cloud와 Top Secret Cloud에서 지원되는 버전을 검토하고 콘솔에서 비공개 모드에 대해 알아보세요.

- AWS Secret Cloud 및 Top Secret Cloud에서 지원되는 다음 버전을 검토하세요.
  - Cloud Volumes ONTAP 9.12.1 P2
  - 콘솔 에이전트 버전 3.9.32

    AWS에서 Cloud Volumes ONTAP 배포하고 관리하려면 콘솔 에이전트가 필요합니다. 콘솔 에이전트 인스턴스에 설치된 소프트웨어에서 콘솔에 로그인합니다. AWS Secret Cloud 및 Top Secret Cloud에서는 콘솔용 SaaS 웹사이트가 지원되지 않습니다.

- 개인 모드에 대해 알아보세요

  AWS Secret Cloud와 Top Secret Cloud에서는 콘솔이 _비공개 모드_로 작동합니다. 개인 모드에서는 콘솔에서 SaaS 계층에 연결할 수 없습니다. 콘솔 에이전트에 액세스할 수 있는 로컬 웹 기반 애플리케이션을 통해 콘솔에 액세스할 수 있습니다.

  개인 모드의 작동 방식에 대해 자세히 알아보려면 다음을 참조하세요."콘솔의 개인 배포 모드" .

1단계: 네트워킹 설정

Cloud Volumes ONTAP 제대로 작동할 수 있도록 AWS 네트워킹을 설정하세요.

단계

1. 콘솔 에이전트와 Cloud Volumes ONTAP 인스턴스의 인스턴스를 시작할 VPC와 서브넷을 선택합니다.
2. VPC와 서브넷이 콘솔 에이전트와 Cloud Volumes ONTAP 간의 연결을 지원하는지 확인하세요.
3. S3 서비스에 대한 VPC 엔드포인트를 설정합니다.

   Cloud Volumes ONTAP 에서 저비용 개체 스토리지로 콜드 데이터를 계층화하려면 VPC 엔드포인트가 필요합니다.

2단계: 권한 설정

AWS Secret Cloud 또는 Top Secret Cloud에서 작업을 수행하는 데 필요한 권한을 Console 에이전트와 Cloud Volumes ONTAP 에 제공하는 IAM 정책과 역할을 설정합니다.

다음 각각에 대해 IAM 정책과 IAM 역할이 필요합니다.

- 콘솔 에이전트의 인스턴스
- Cloud Volumes ONTAP 인스턴스
- HA 쌍의 경우 Cloud Volumes ONTAP HA 중재자 인스턴스(HA 쌍을 배포하려는 경우)

단계

1. AWS IAM 콘솔로 가서 *정책*을 클릭합니다.
2. 콘솔 에이전트 인스턴스에 대한 정책을 만듭니다.

AWS 환경에서 S3 버킷을 지원하기 위해 이러한 정책을 생성합니다. 나중에 버킷을 생성할 때 버킷 이름 앞에 접두사가 있는지 확인하십시오. `fabric-pool-` . 이 요구 사항은 AWS Secret Cloud 및 Top Secret Cloud 지역 모두에 적용됩니다.

비밀 지역

```
{
    "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-b: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-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

극비 지역

```
{
    "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 ONTAP 에 대한 정책을 만듭니다.

비밀 지역

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

극비 지역

```
{
    "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"
    }]
}
```

HA 쌍의 경우 Cloud Volumes ONTAP HA 쌍을 배포할 계획이라면 HA 중재자에 대한 정책을 만듭니다.

```
{
    "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": "*"
        }
    ]
}
```

4. 역할 유형이 Amazon EC2인 IAM 역할을 만들고 이전 단계에서 만든 정책을 연결합니다.

   역할을 만듭니다.

   정책과 마찬가지로 콘솔 에이전트에 대한 IAM 역할 하나와 Cloud Volumes ONTAP 노드에 대한 IAM 역할 하나가 있어야 합니다. HA 쌍의 경우: 정책과 마찬가지로 콘솔 에이전트에 대한 IAM 역할 하나, Cloud Volumes ONTAP 노드에 대한 IAM 역할 하나, HA 중재자(HA 쌍을 배포하려는 경우)에 대한 IAM 역할 하나가 있어야 합니다.

   역할을 선택하세요:

   콘솔 에이전트 인스턴스를 시작할 때 콘솔 에이전트 IAM 역할을 선택해야 합니다. 콘솔에서 Cloud Volumes ONTAP 시스템을 생성할 때 Cloud Volumes ONTAP 에 대한 IAM 역할을 선택할 수 있습니다. HA 쌍의 경우 Cloud Volumes ONTAP 시스템을 생성할 때 Cloud Volumes ONTAP 및 HA 중재자에 대한 IAM 역할을 선택할 수 있습니다.

3단계: AWS KMS 설정

Cloud Volumes ONTAP 과 함께 Amazon 암호화를 사용하려면 AWS Key Management Service(KMS)에 대한 요구 사항이 충족되는지 확인하세요.

단계

1. 귀하의 계정이나 다른 AWS 계정에 활성 고객 마스터 키(CMK)가 있는지 확인하세요.

   CMK는 AWS 관리형 CMK이거나 고객 관리형 CMK일 수 있습니다.

2. CMK가 Cloud Volumes ONTAP 배포하려는 계정과 별도의 AWS 계정에 있는 경우 해당 키의 ARN을 얻어야 합니다.

   Cloud Volumes ONTAP 시스템을 생성할 때 콘솔에 ARN을 제공해야 합니다.

3. CMK의 주요 사용자 목록에 인스턴스의 IAM 역할을 추가합니다.

   이렇게 하면 콘솔에서 Cloud Volumes ONTAP 과 함께 CMK를 사용할 수 있는 권한이 부여됩니다.

4단계: 콘솔 에이전트 설치 및 콘솔 설정

AWS에서 Cloud Volumes ONTAP 배포하기 위해 콘솔을 사용하려면 먼저 콘솔 에이전트를 설치하고 설정해야 합니다. 콘솔을 통해 퍼블릭 클라우드 환경(여기에는 Cloud Volumes ONTAP 포함됨) 내의 리소스와 프로세스를 관리할 수 있습니다.

단계

1. 인증 기관(CA)에서 서명한 루트 인증서를 PEM(Privacy Enhanced Mail) Base-64 인코딩된 X.509 형식으로 얻습니다. 인증서를 취득하기 위해서는 귀하의 조직의 정책과 절차를 참조하세요.

   AWS Secret Cloud 지역의 경우 다음을 업로드해야 합니다. `NSS Root CA 2` 인증서 및 Top Secret Cloud의 경우 `Amazon Root CA 4` 자격증. 전체 체인이 아닌 해당 인증서만 업로드해야 합니다. 인증서 체인 파일이 커서 업로드가 실패할 수 있습니다. 추가 인증서가 있는 경우 다음 단계에 설명된 대로 나중에 업로드할 수 있습니다.

   설정 과정에서 인증서를 업로드해야 합니다. 콘솔은 HTTPS를 통해 AWS에 요청을 보낼 때 신뢰할 수 있는 인증서를 사용합니다.

2. 콘솔 에이전트 인스턴스를 시작합니다.
   a. 콘솔의 AWS Intelligence Community Marketplace 페이지로 이동합니다.
   b. 사용자 지정 시작 탭에서 EC2 콘솔에서 인스턴스를 시작하는 옵션을 선택합니다.
   c. 프롬프트에 따라 인스턴스를 구성합니다.

      인스턴스를 구성할 때 다음 사항에 유의하세요.

      - t3.xlarge을 권장합니다.
      - 권한을 설정할 때 생성한 IAM 역할을 선택해야 합니다.
      - 기본 저장 옵션을 유지해야 합니다.
      - 콘솔 에이전트에 필요한 연결 방법은 다음과 같습니다: SSH, HTTP, HTTPS.
3. 인스턴스에 연결된 호스트에서 콘솔을 설정합니다.
   a. 웹 브라우저를 열고 입력하세요 https://ipaddress 여기서 _ipaddress_는 콘솔 에이전트를 설치한 Linux 호스트의 IP 주소입니다.
   b. AWS 서비스에 연결하기 위한 프록시 서버를 지정합니다.
   c. 1단계에서 얻은 인증서를 업로드하세요.
   d. 화면의 지시에 따라 새로운 시스템을 설정하세요.
      - 시스템 세부 정보: 콘솔 에이전트의 이름과 회사 이름을 입력하세요.
      - 관리자 사용자 만들기: 시스템의 관리자 사용자를 만듭니다.

        이 사용자 계정은 시스템에서 로컬로 실행됩니다. 콘솔을 통해 auth0 서비스에 연결할 수 없습니다.

- 검토: 세부 정보를 검토하고, 라이선스 계약에 동의한 후 *설정*을 선택합니다.

e. CA 서명 인증서 설치를 완료하려면 EC2 콘솔에서 콘솔 에이전트 인스턴스를 다시 시작합니다.

4. 콘솔 에이전트가 다시 시작된 후 설치 마법사에서 만든 관리자 사용자 계정을 사용하여 로그인합니다.

5단계: (선택 사항) 개인 모드 인증서 설치

이 단계는 AWS Secret Cloud 및 Top Secret Cloud 지역의 경우 선택 사항이며, 이전 단계에서 설치한 루트 인증서 외에 추가 인증서가 있는 경우에만 필요합니다.

단계

1. 기존에 설치된 인증서를 나열합니다.

   a. occm 컨테이너 docker ID(식별된 이름 "ds-occm-1")를 수집하려면 다음 명령을 실행하세요.

   ```
   docker ps
   ```

   b. occm 컨테이너 안으로 들어가려면 다음 명령을 실행하세요.

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   c. "TRUST_STORE_PASSWORD" 환경 변수에서 비밀번호를 수집하려면 다음 명령을 실행하세요.

   ```
   env
   ```

   d. 신뢰 저장소에 설치된 모든 인증서를 나열하려면 다음 명령을 실행하고 이전 단계에서 수집한 비밀번호를 사용하세요.

   ```
   keytool -list -v -keystore occm.truststore
   ```

2. 인증서를 추가합니다.

   a. occm 컨테이너 docker ID(식별된 이름 "ds-occm-1")를 수집하려면 다음 명령을 실행하세요.

   ```
   docker ps
   ```

   b. occm 컨테이너 안으로 들어가려면 다음 명령을 실행하세요.

   ```
   docker exec -it <docker-id> /bin/sh
   ```

   새로운 인증서 파일을 내부에 저장합니다.

   c. "TRUST_STORE_PASSWORD" 환경 변수에서 비밀번호를 수집하려면 다음 명령을 실행하세요.

```
env
```

d. 인증서를 신뢰 저장소에 추가하려면 다음 명령을 실행하고 이전 단계의 비밀번호를 사용하세요.

```
keytool -import -alias <alias-name> -file <certificate-file-name>
-keystore occm.truststore
```

e. 인증서가 설치되었는지 확인하려면 다음 명령을 실행하세요.

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

f. occm 컨테이너를 종료하려면 다음 명령을 실행하세요.

```
exit
```

g. occm 컨테이너를 재설정하려면 다음 명령을 실행하세요.

```
docker restart <docker-id>
```

6단계: 콘솔에 라이선스 추가

NetApp 에서 라이선스를 구매한 경우 콘솔에 라이선스를 추가해야 새 Cloud Volumes ONTAP 시스템을 생성할 때 라이선스를 선택할 수 있습니다. 이러한 라이선스는 새 Cloud Volumes ONTAP 시스템과 연결할 때까지 할당되지 않은 상태로 유지됩니다.

단계

1. 왼쪽 탐색 메뉴에서 * Licenses and subscriptions*을 선택하세요.
2. * Cloud Volumes ONTAP* 패널에서 *보기*를 선택합니다.
3. * Cloud Volumes ONTAP* 탭에서 *라이선스 > 노드 기반 라이선스*를 선택합니다.
4. *할당되지 않음*을 클릭합니다.
5. *할당되지 않은 라이선스 추가*를 클릭합니다.
6. 라이선스의 일련번호를 입력하거나 라이선스 파일을 업로드하세요.
7. 아직 라이선스 파일이 없으면 netapp.com에서 라이선스 파일을 수동으로 업로드해야 합니다.
   a. 로 가다"NetApp 라이선스 파일 생성기" NetApp 지원 사이트 자격 증명을 사용하여 로그인하세요.
   b. 비밀번호를 입력하고, 제품을 선택하고, 일련번호를 입력하고, 개인정보 보호정책을 읽고 동의함을 확인한 후 *제출*을 클릭하세요.
   c. serialnumber.NLF JSON 파일을 이메일로 받을지, 아니면 직접 다운로드할지 선택하세요.

8. *라이선스 추가*를 클릭하세요.

결과

콘솔은 새 Cloud Volumes ONTAP 시스템과 연결할 때까지 라이선스를 미할당으로 추가합니다. 라이선스는 왼쪽 탐색 메뉴의 * Licenses and subscriptions > Cloud Volumes ONTAP > 보기 > 라이선스*에서 확인할 수 있습니다.

7단계: 콘솔에서 Cloud Volumes ONTAP 실행

콘솔에서 새로운 시스템을 생성하여 AWS Secret Cloud 및 Top Secret Cloud에서 Cloud Volumes ONTAP 인스턴스를 시작할 수 있습니다.

시작하기 전에

HA 쌍의 경우 HA 중재자에 대한 키 기반 SSH 인증을 활성화하려면 키 쌍이 필요합니다.

단계

1. 시스템 페이지에서 *시스템 추가*를 클릭합니다.
2. *만들기*에서 Cloud Volumes ONTAP 선택합니다.

   HA의 경우: *만들기*에서 Cloud Volumes ONTAP 또는 Cloud Volumes ONTAP HA를 선택합니다.

3. 마법사의 단계를 완료하여 Cloud Volumes ONTAP 시스템을 시작합니다.

> 마법사를 통해 선택하는 동안 *서비스*에서 *데이터 감지 및 규정 준수*와 *클라우드에 백업*을 선택하지 마세요. *사전 구성된 패키지*에서 *구성 변경*만 선택하고 다른 옵션은 선택하지 않았는지 확인하세요. 사전 구성된 패키지는 AWS Secret Cloud 및 Top Secret Cloud 지역에서는 지원되지 않으며, 이를 선택하면 배포가 실패합니다.

여러 가용성 영역에 **Cloud Volumes ONTAP HA**를 배포하기 위한 참고 사항

HA 쌍에 대한 마법사를 완료할 때 다음 사항에 유의하세요.

- 여러 가용성 영역(AZ)에 Cloud Volumes ONTAP HA를 배포하는 경우 전송 게이트웨이를 구성해야 합니다. 지침은 다음을 참조하세요."AWS 전송 게이트웨이 설정" .
- AWS Top Secret Cloud가 게시될 당시에는 사용 가능한 AZ가 두 개뿐이었으므로 다음과 같이 구성을 배포합니다.
  - 노드 1: 가용성 영역 A
  - 노드 2: 가용성 영역 B
  - 중재자: 가용성 영역 A 또는 B

단일 및 **HA** 노드 모두에 **Cloud Volumes ONTAP** 배포하기 위한 참고 사항

마법사를 완료할 때 다음 사항에 유의하세요.

- 생성된 보안 그룹을 사용하려면 기본 옵션을 그대로 두어야 합니다.

  미리 정의된 보안 그룹에는 Cloud Volumes ONTAP 성공적으로 작동하는 데 필요한 규칙이 포함되어 있습니다. 자체 보안 그룹이 필요한 경우 아래 보안 그룹 섹션을 참조하세요.

- AWS 환경을 준비할 때 생성한 IAM 역할을 선택해야 합니다.

- 기본 AWS 디스크 유형은 초기 Cloud Volumes ONTAP 볼륨을 위한 것입니다.

  이후 볼륨에는 다른 디스크 유형을 선택할 수 있습니다.

- AWS 디스크의 성능은 디스크 크기에 따라 달라집니다.

  지속적으로 필요한 성능을 제공하는 디스크 크기를 선택해야 합니다. EBS 성능에 대한 자세한 내용은 AWS 설명서를 참조하세요.

- 디스크 크기는 시스템의 모든 디스크에 대한 기본 크기입니다.

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

결과

Cloud Volumes ONTAP 인스턴스가 시작됩니다. 감사 페이지에서 진행 상황을 추적할 수 있습니다.

8단계: 데이터 계층화를 위한 보안 인증서 설치

AWS Secret Cloud 및 Top Secret Cloud 지역에서 데이터 계층화를 활성화하려면 보안 인증서를 수동으로 설치해야 합니다.

시작하기 전에

1. S3 버킷을 생성합니다.

   버킷 이름 앞에 접두사가 있는지 확인하십시오. `fabric-pool-`. 예를 들어 `fabric-pool-testbucket` .

2. 설치한 루트 인증서를 유지하세요. `step 4` 능숙한.

단계

1. 설치한 루트 인증서에서 텍스트를 복사하세요. `step 4` .
2. CLI를 사용하여 Cloud Volumes ONTAP 시스템에 안전하게 연결합니다.
3. 루트 인증서를 설치합니다. 당신은 눌러야 할 수도 있습니다 `ENTER` 키를 여러 번 누르세요:

   ```
   security certificate install -type server-ca -cert-name <certificate-name>
   ```

4. 메시지가 표시되면 다음을 포함하여 복사된 전체 텍스트를 입력하십시오. `----- BEGIN CERTIFICATE -----` 에게 `----- END CERTIFICATE -----` .
5. 나중에 참조할 수 있도록 CA 서명 디지털 인증서 사본을 보관하세요.
6. CA 이름과 인증서 일련번호를 보관하세요.
7. AWS Secret Cloud 및 Top Secret Cloud 지역에 대한 개체 저장소를 구성합니다. `set -privilege advanced -confirmations off`

8. 이 명령을 실행하여 개체 저장소를 구성합니다.

> 모든 Amazon 리소스 이름(ARN)에는 다음 접미사가 붙어야 합니다. `-iso-b` , 와 같은 `arn:aws-iso-b` . 예를 들어 리소스에 지역이 포함된 ARN이 필요한 경우 Top Secret Cloud의 경우 다음과 같은 명명 규칙을 사용합니다. `us-iso-b` 를 위해 `-server` 깃발. AWS Secret Cloud의 경우 다음을 사용하세요. `us-iso-b-1` .

```
storage aggregate object-store config create -object-store-name
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl
-enabled true -port 443
```

9. 개체 저장소가 성공적으로 생성되었는지 확인하세요. `storage aggregate object-store show -instance`
10. 개체 저장소를 집계에 연결합니다. 이것은 모든 새로운 집계에 대해 반복되어야 합니다. `storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>`