시작하기
Cloud Volumes ONTAP

NetApp
February 17, 2026

목차

시작하기

Cloud Volumes ONTAP 에 대해 알아보세요

Cloud Volumes ONTAP 사용하면 데이터 보호, 보안 및 규정 준수를 강화하는 동시에 클라우드 스토리지 비용과 성능을 최적화할 수 있습니다.

Cloud Volumes ONTAP 클라우드에서 ONTAP 데이터 관리 소프트웨어를 실행하는 소프트웨어 전용 스토리지 어플라이언스입니다. 다음과 같은 주요 기능을 갖춘 엔터프라이즈급 스토리지를 제공합니다.

- 저장 효율성

  내장된 데이터 중복 제거, 데이터 압축, 씬 프로비저닝, 복제 기능을 활용하여 스토리지 비용을 최소화합니다.

- 고가용성

  클라우드 환경에서 장애가 발생하더라도 기업의 안정성과 지속적인 운영을 보장하세요.

- 데이터 보호

  Cloud Volumes ONTAP NetApp의 업계 최고 복제 기술인 SnapMirror 활용하여 온프레미스 데이터를 클라우드에 복제하므로 여러 사용 사례에 사용할 수 있는 보조 사본을 쉽게 확보할 수 있습니다.

  Cloud Volumes ONTAP NetApp Backup and Recovery 와 통합되어 클라우드 데이터의 보호 및 장기 보관을 위한 백업 및 복원 기능을 제공합니다.

  "백업 및 복구에 대해 자세히 알아보세요"

- 데이터 계층화

  애플리케이션을 오프라인으로 전환하지 않고도 필요에 따라 고성능 및 저성능 스토리지 풀을 전환할 수 있습니다.

- 애플리케이션 일관성

  NetApp SnapCenter 사용하여 NetApp Snapshot 복사본의 일관성을 보장합니다.

  "SnapCenter 에 대해 자세히 알아보세요"

- 데이터 보안

  Cloud Volumes ONTAP 데이터 암호화를 지원하고 바이러스 및 랜섬웨어로부터 보호합니다.

- 개인정보 보호 규정 준수 제어

  NetApp Data Classification 와의 통합을 통해 데이터 컨텍스트를 이해하고 중요한 데이터를 식별하는 데 도움이 됩니다.

  "데이터 분류에 대해 자세히 알아보세요"

ONTAP 기능 라이선스는 Cloud Volumes ONTAP 에 포함되어 있습니다.

"지원되는 Cloud Volumes ONTAP 구성 보기"

"Cloud Volumes ONTAP 에 대해 자세히 알아보세요"

Cloud Volumes ONTAP 배포에 지원되는 ONTAP 버전

NetApp Console 사용하면 Cloud Volumes ONTAP 시스템을 추가할 때 여러 가지 ONTAP 버전 중에서 선택할 수 있습니다.

여기에 나열된 버전 이외의 Cloud Volumes ONTAP 버전은 신규 배포에 사용할 수 없습니다. 릴리스에 표시된 패치 버전 또는 일반(General Availability) 버전은 배포에 사용할 수 있는 기본 버전을 나타냅니다. 사용 가능한 패치에 대한 자세한 내용은 각 릴리스의 "버전별 릴리스 노트"를 참조하십시오.

업그레이드에 대한 자세한 내용은 "지원되는 업그레이드 경로"을(를) 참조하십시오.

AWS

단일 노드

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

HA 쌍

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1

- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

하늘빛

단일 노드

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

HA 쌍

- 9.18.1
- 9.17.1 P1
- 9.16.1 P3
- 9.15.1 P10
- 9.14.1 P13
- 9.13.1 P16
- 9.12.1 P18

구글 클라우드

단일 노드

- 9.18.1
- 9.17.1 P1

- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

HA 쌍

- 9.18.1
- 9.17.1 P1
- 9.16.1
- 9.15.1
- 9.15.0 P1
- 9.14.1
- 9.14.1
- 9.14.0
- 9.13.1
- 9.12.1
- 9.12.1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

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. Amazon Simple Storage Service(Amazon 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.

> ⓘ Cloud Volumes ONTAP 시스템이 AWS Local Zone에 있는 경우 Amazon Simple Storage Service(Amazon S3)로의 데이터 계층화는 지원되지 않습니다. Local Zone 외부의 Amazon S3 버킷에 액세스하면 지연 시간이 길어지고 Cloud Volumes ONTAP 활동에 영향을 미치기 때문입니다.

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	

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

여러 AZ의 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

엔드포인트	적용 가능	목적	배포 모드	엔드포인트를 사용할 수 없는 경우의 영향
\ 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) • Amazon Simple Storage Service(S3)	AWS 서비스와의 통신.	표준 모드와 개인 모드.	Cloud Volumes ONTAP AWS 서비스와 통신하여 AWS에서 특정 작업을 수행할 수 없습니다.
AWS 서비스에 대한 정확한 정부 엔드포인트는 사용 중인 AWS 지역에 따라 달라집니다. 끝점에는 접미사가 붙습니다. `amazonaws.com` 그리고 `c2s.ic.gov` . 참조하다 "AWS SDK" 그리고 "AWS 문서" 자세한 내용은.	• 클라우드포메이션 • 탄력적 컴퓨팅 클라우드(EC2) • ID 및 액세스 관리(IAM) • 키 관리 서비스(KMS) • 보안 토큰 서비스(STS) • 간편 보관 서비스(S3)	AWS 서비스와의 통신.	제한 모드.	Cloud Volumes ONTAP AWS 서비스와 통신하여 AWS에서 특정 작업을 수행할 수 없습니다.

HA 중재자를 위한 아웃바운드 인터넷 액세스

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

수동 옵션은 대상 서브넷에서 AWS EC2 서비스로 연결되는 NAT 게이트웨이 또는 인터페이스 VPC 엔드포인트가 될 수 있습니다. VPC 엔드포인트에 대한 자세한 내용은 다음을 참조하세요. "AWS 설명서: VPC 엔드포인트 인터페이스(AWS PrivateLink)" .

NetApp Console 에이전트의 네트워크 프록시 구성

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

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

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

개인 **IP** 주소

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

Console에서 Cloud Volumes ONTAP에 할당하는 LIF 수는 단일 노드 시스템을 배포하는지 또는 HA 쌍을 배포하는지에 따라 달라집니다. LIF는 물리적 포트와 연결된 IP 주소입니다.

단일 노드 시스템의 **IP** 주소

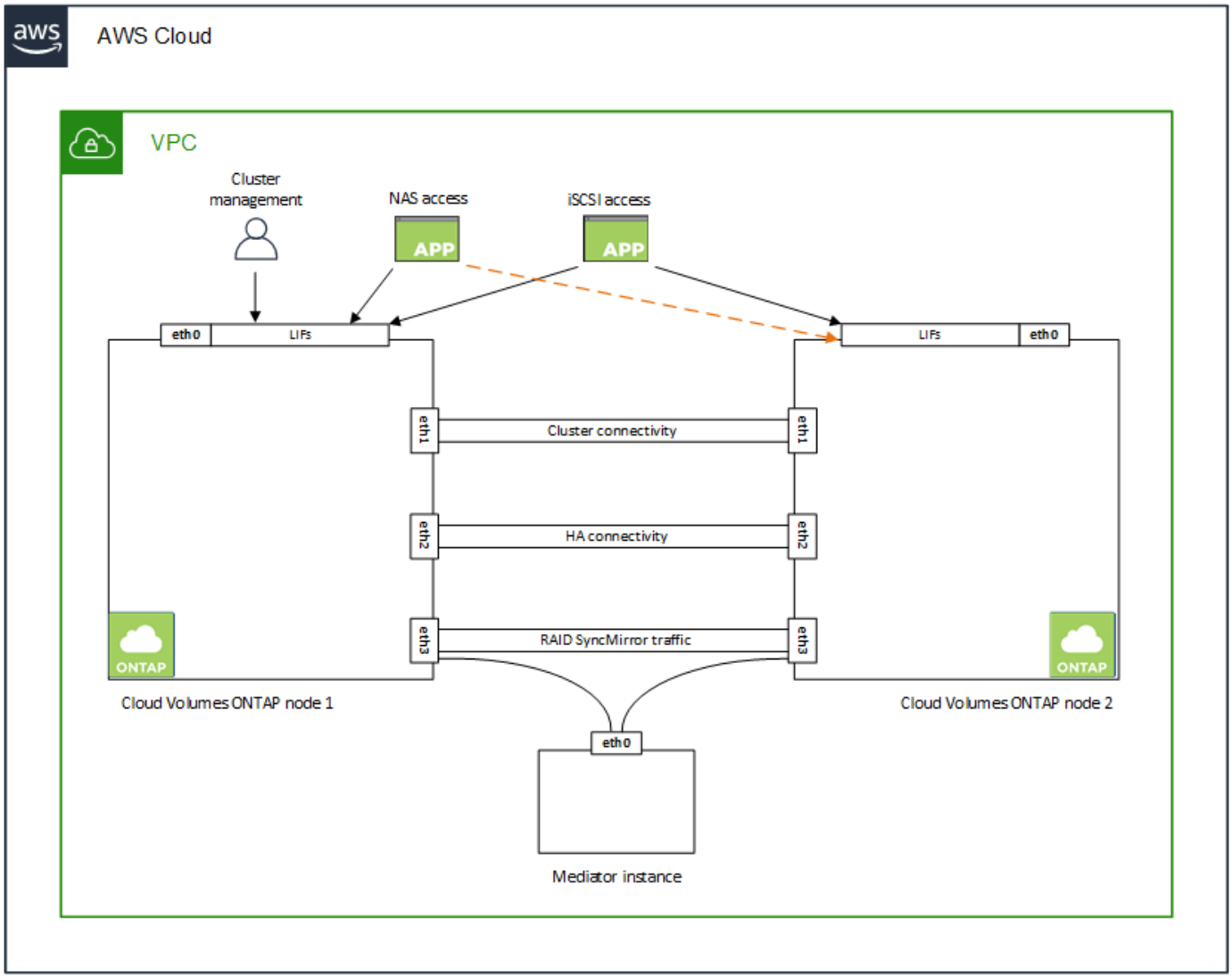
NetApp Console은 단일 노드 시스템에 6개의 IP 주소를 할당합니다.

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 쌍은 단일 노드 시스템보다 더 많은 IP 주소가 필요합니다. 이러한 IP 주소는 다음 이미지에 표시된 것처럼 여러 이더넷 인터페이스에 분산됩니다.



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, Amazon S3를 용량 계층으로 사용하려면 Cloud Volumes ONTAP이 S3에 연결되어 있어야 합니다. 이 연결을 제공하는 가장 좋은 방법은 S3 서비스에 대한 VPC 엔드포인트를 생성하는 것입니다. 지침은 "AWS 설명서: 게이트웨이 엔드포인트 생성"을 참조하십시오.

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

문제가 발생하면 다음을 참조하세요. "AWS 지원 지식 센터: 게이트웨이 VPC 엔드포인트를 사용하여 S3 버킷에 연결할 수 없는 이유는 무엇입니까?"

ONTAP 시스템에 대한 연결

AWS의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 AWS VPC와 다른 네트워크(예: 회사 네트워크) 간에 VPN 연결이 필요합니다. 지침은 다음을 참조하세요. "AWS 설명서: AWS VPN 연결 설정" .

CIFS용 **DNS** 및 **Active Directory**

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

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

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

VPC 공유

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

"공유 서브넷에 HA 쌍을 배포하는 방법을 알아보세요." .

여러 **AZ**의 **HA** 쌍에 대한 요구 사항

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

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

가용성 영역

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

각 가용성 영역에서 서브넷을 사용할 수 있어야 합니다.

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

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

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

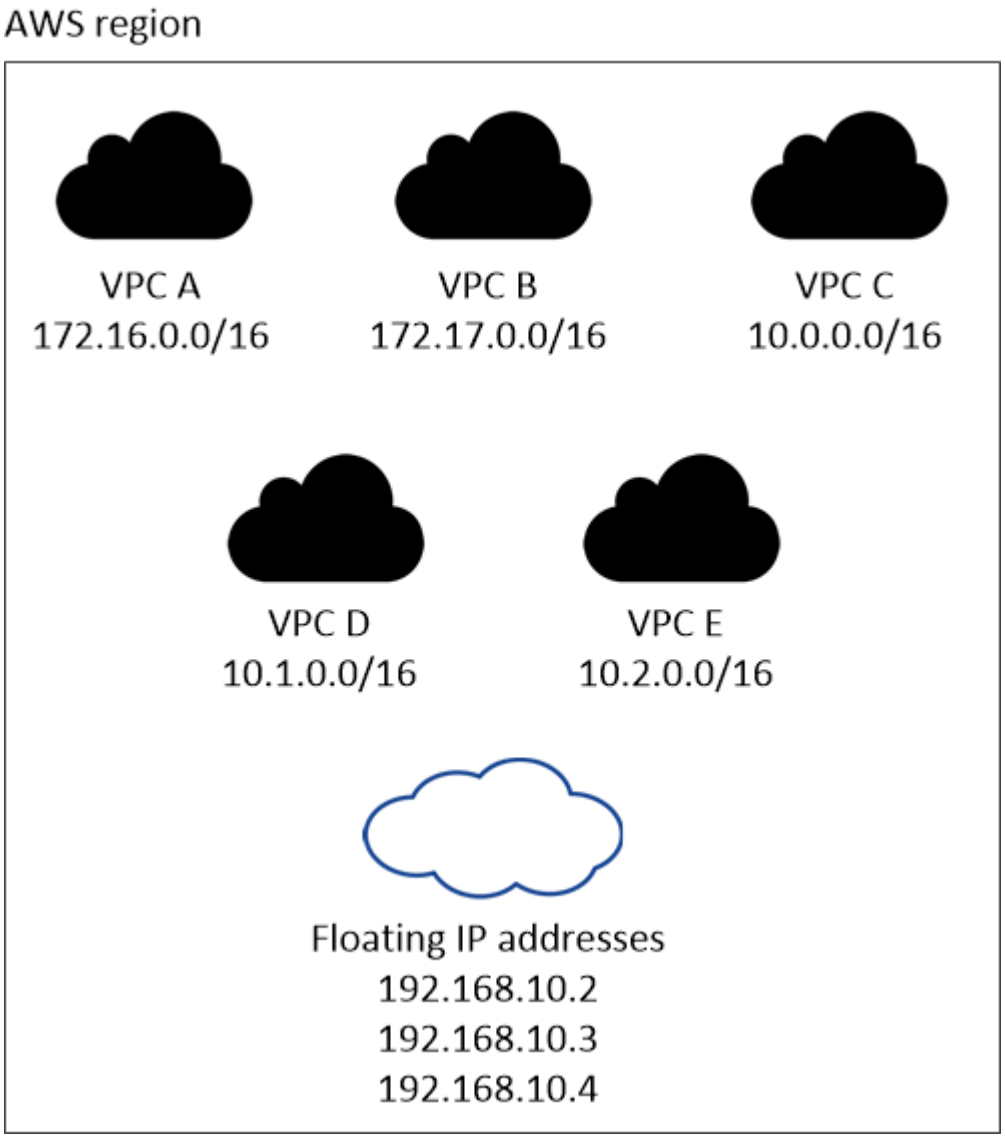
HA 쌍과 함께 Windows용 SnapDrive 또는 SnapCenter 사용하는 경우 SVM 관리 LIF에 부동 IP 주소가 필요합니다.

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

HA 구성을 배포하는 AWS 지역의 모든 VPC에 대한 CIDR 블록 외부에 부동 IP 주소가 있어야 합니다. 유동 IP

주소를 해당 지역의 VPC 외부에 있는 논리적 서브넷으로 생각해 보세요.

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



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

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

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

경로 테이블

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

VPC의 서브넷에 대한 경로 테이블이 하나뿐인 경우(기본 경로 테이블), 콘솔은 자동으로 해당 경로 테이블에 플로팅 IP 주소를 추가합니다. 두 개 이상의 경로 테이블이 있는 경우 HA 쌍을 시작할 때 올바른 경로 테이블을 선택하는 것이 매우 중요합니다. 그렇지 않으면 일부 클라이언트가 Cloud Volumes ONTAP 에 액세스하지 못할 수도

있습니다.

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

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

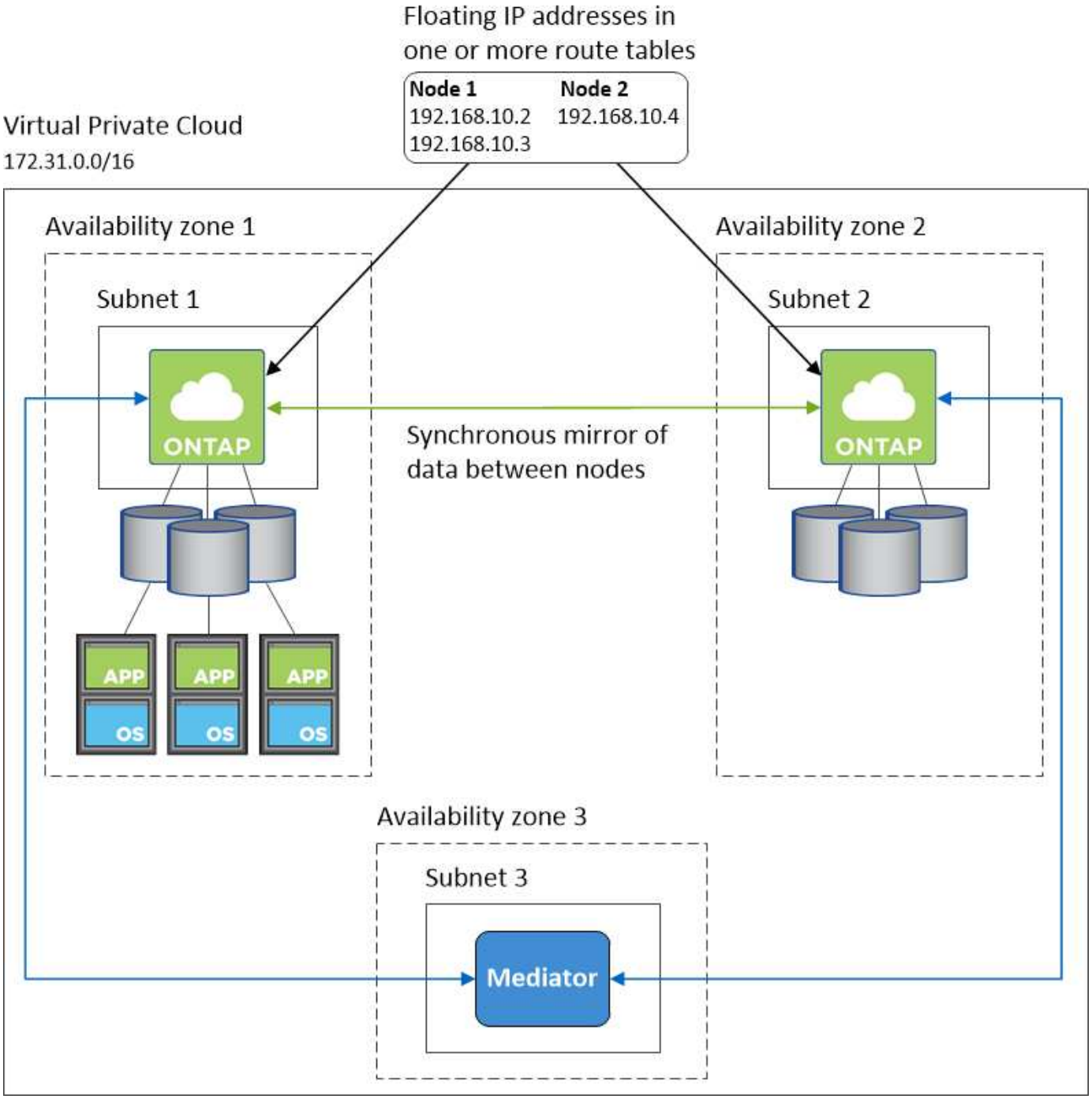
NetApp 관리 도구에 연결

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

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

HA 구성 예시

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



콘솔 에이전트에 대한 요구 사항

아직 콘솔 에이전트를 만들지 않았다면 네트워킹 요구 사항을 검토해야 합니다.

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

관련 주제

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

Cloud Volumes ONTAP HA 쌍에 대한 **AWS** 전송 게이트웨이 설정

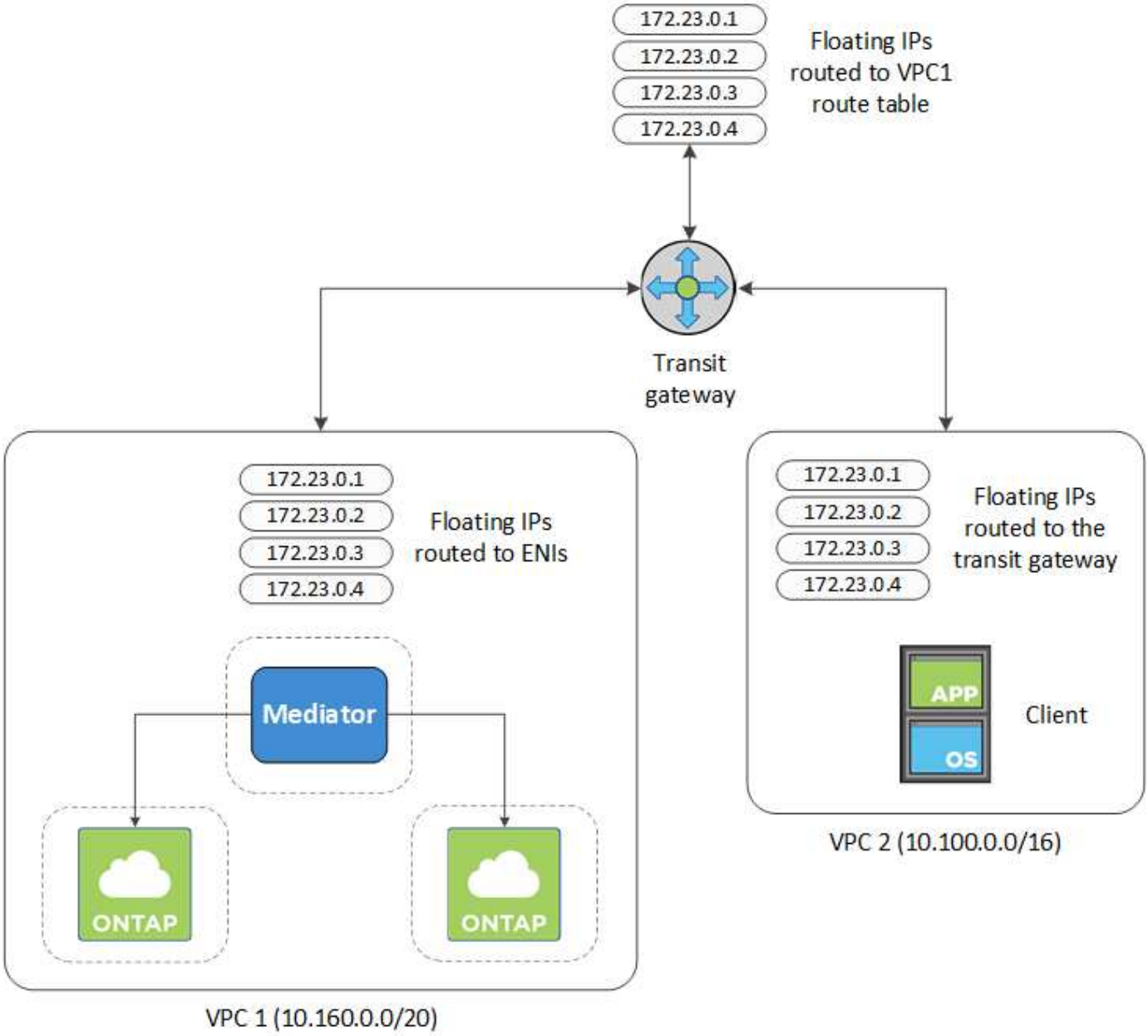
HA 쌍에 대한 액세스를 활성화하기 위해 AWS 전송 게이트웨이를 설정합니다."유동 IP 주소" HA 쌍이 있는 VPC 외부에서.

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

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

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

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

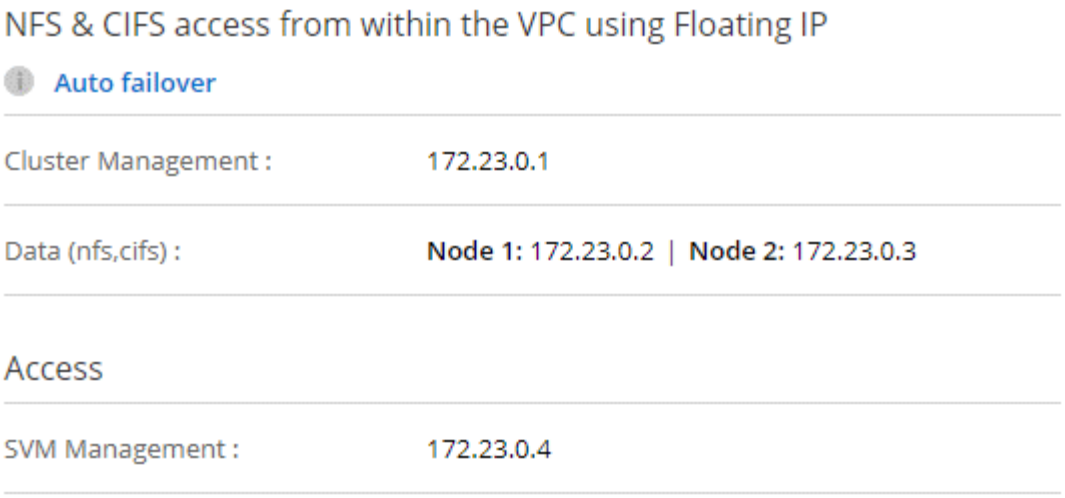


다음 단계에서는 비슷한 구성을 설정하는 방법을 보여줍니다.

단계

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

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



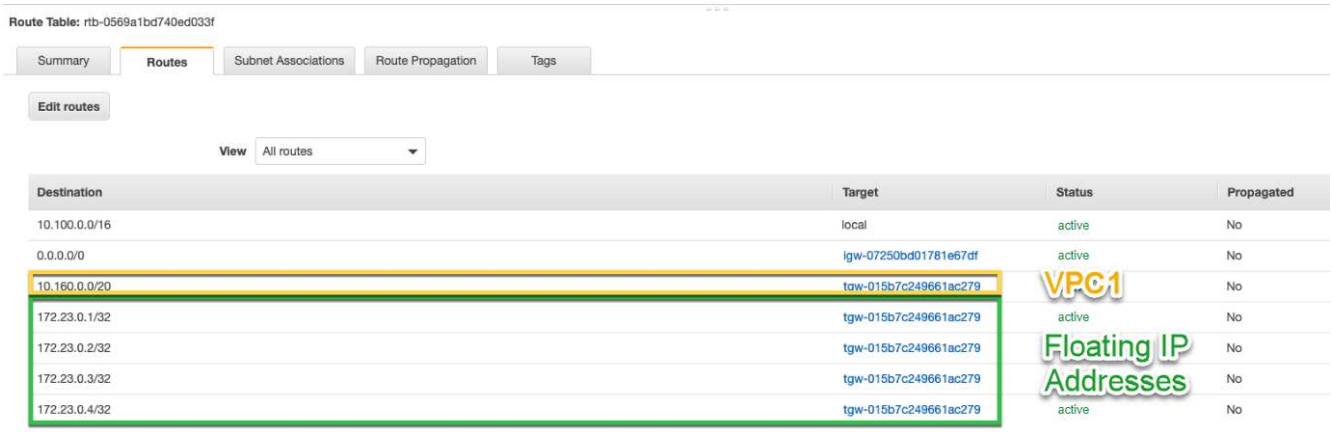
다음 샘플 이미지는 트랜짓 게이트웨이의 경로 테이블을 보여줍니다. 여기에는 Cloud Volumes ONTAP 에서 사용하는 두 개의 VPC의 CIDR 블록에 대한 경로와 4개의 플로팅 IP 주소가 포함됩니다.

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

   a. 플로팅 IP 주소에 경로 항목을 추가합니다.

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

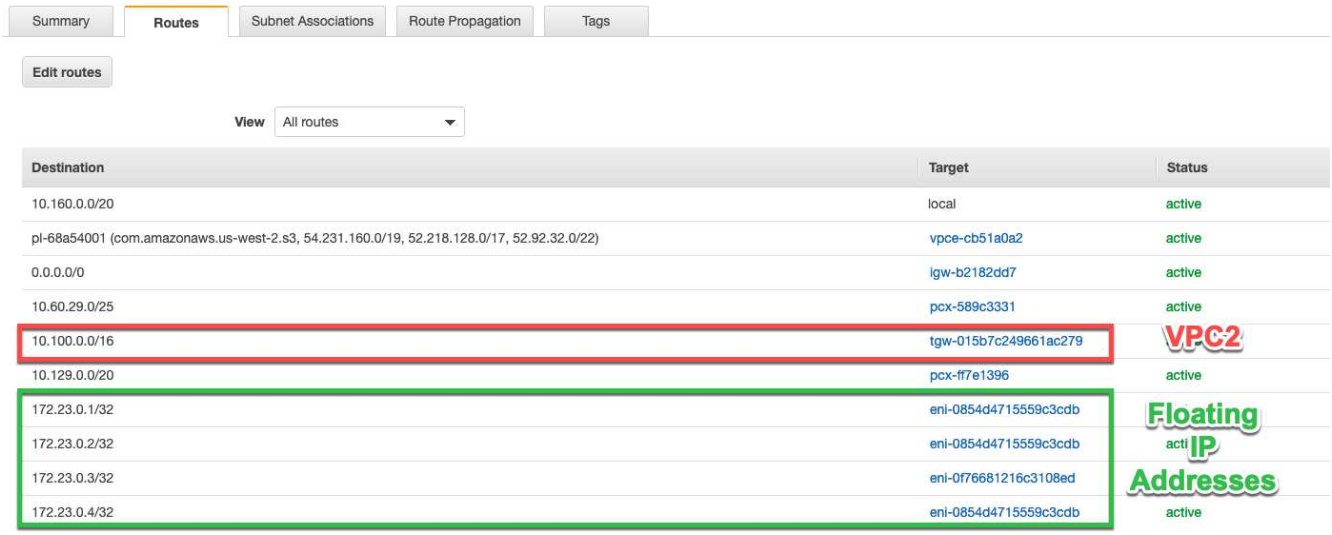
      다음 샘플 이미지는 VPC 1에 대한 경로와 플로팅 IP 주소를 포함하는 VPC 2의 경로 테이블을 보여줍니다.



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

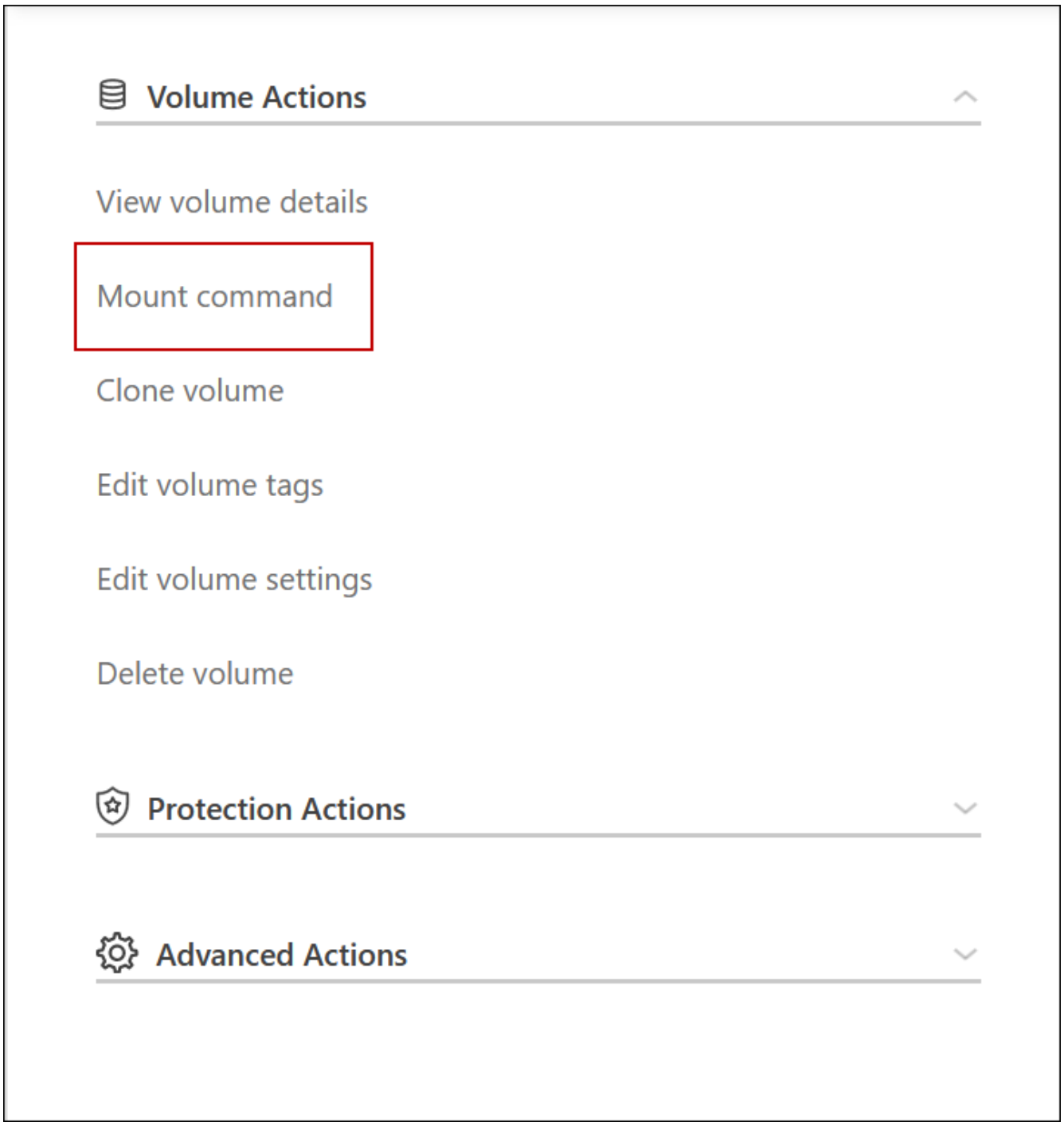
   이 단계는 VPC 간 라우팅을 완료하기 때문에 중요합니다.

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



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

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



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

   "볼륨을 편집하는 방법을 알아보세요" .

관련 링크

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

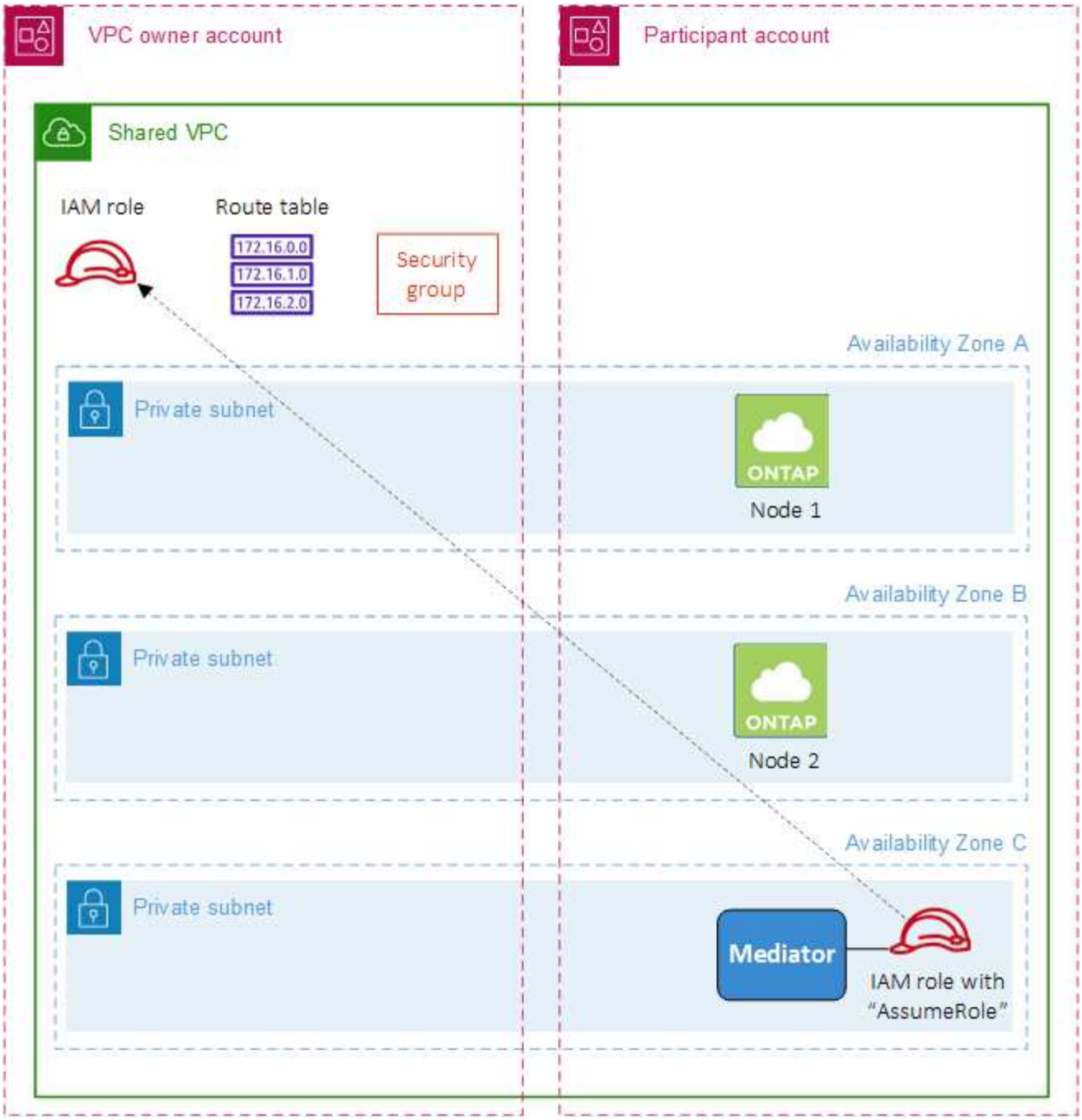
9.11.1 릴리스부터 VPC 공유를 통해 AWS에서 Cloud Volumes ONTAP HA 쌍이 지원됩니다. VPC 공유를 사용하면 조직에서 다른 AWS 계정과 서브넷을 공유할 수 있습니다. 이 구성을 사용하려면 AWS 환경을 설정한 다음 API를 사용하여 HA 쌍을 배포해야 합니다.

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 **AZ**에서 **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.

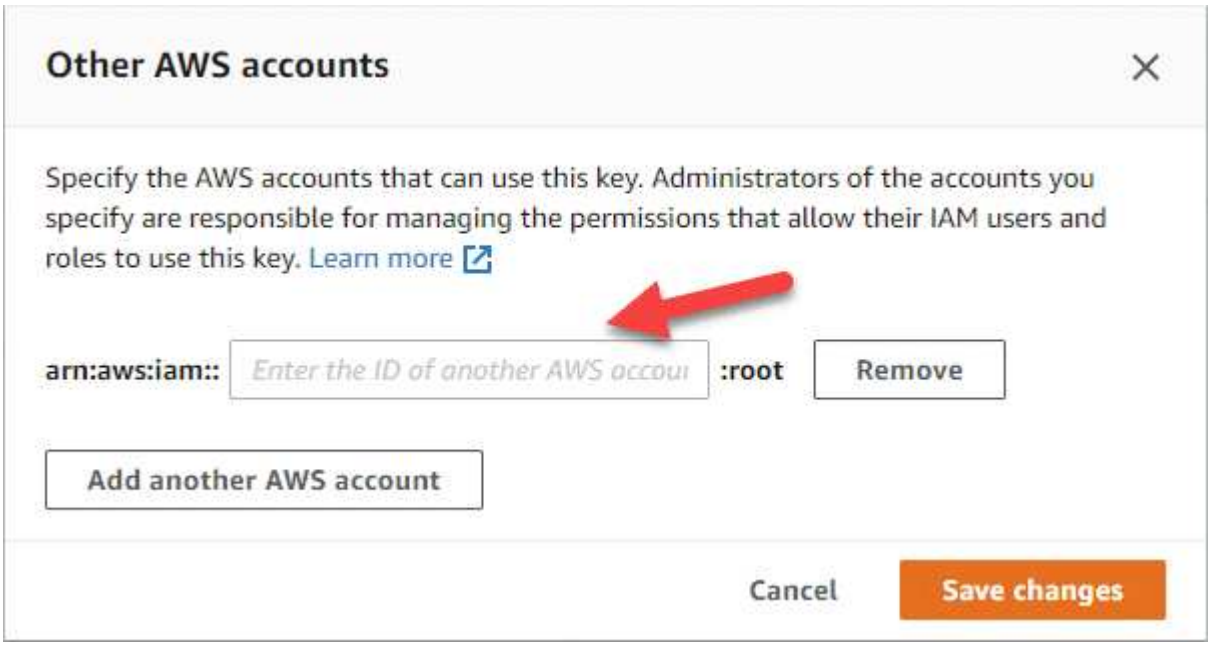
   b. 키를 선택하세요.

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.

이 단계는 Cloud Volumes ONTAP에서 데이터 계층화를 활성화했으며 Amazon Simple Storage Service(Amazon S3) 버킷에 저장된 데이터를 암호화하려는 경우에 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" .

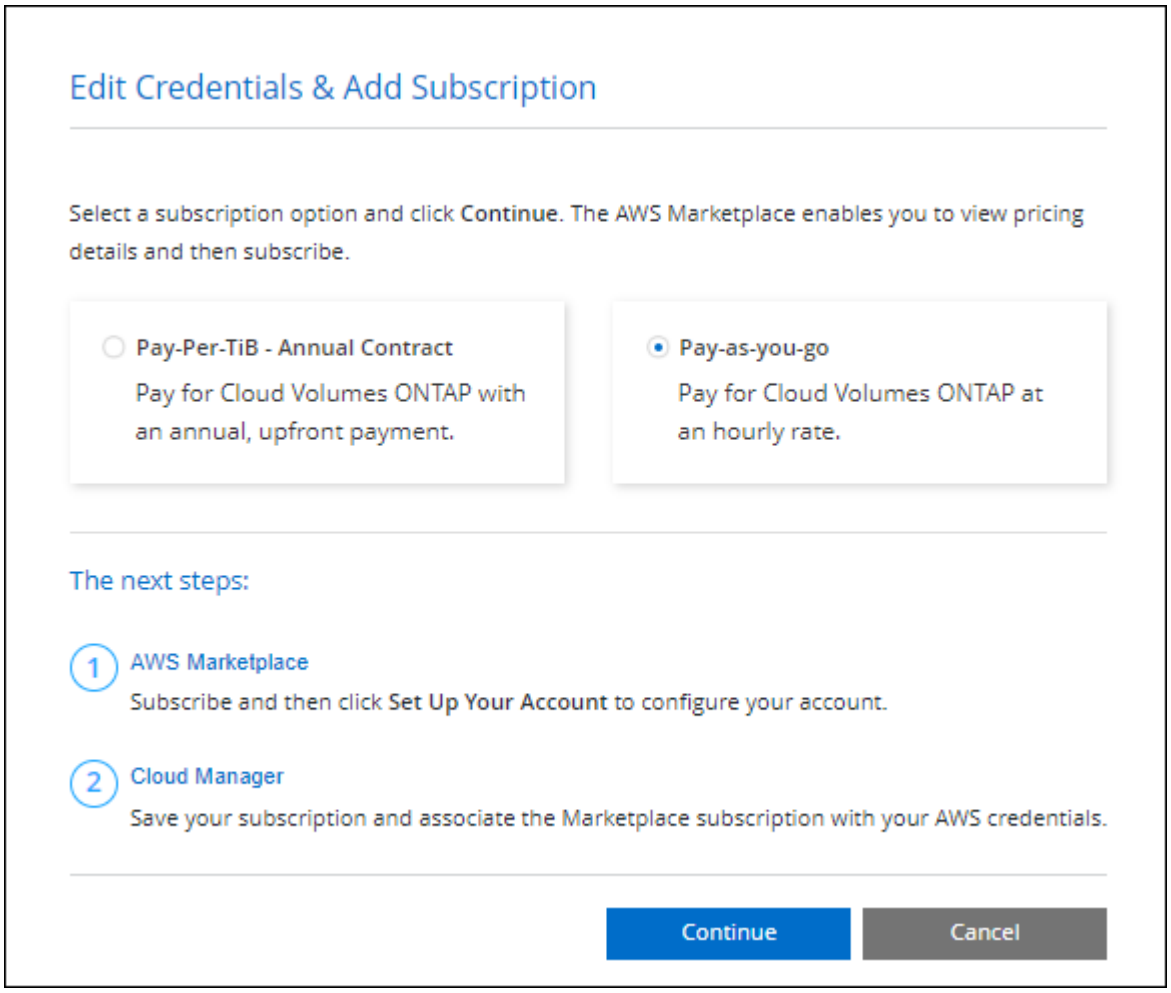
단계

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

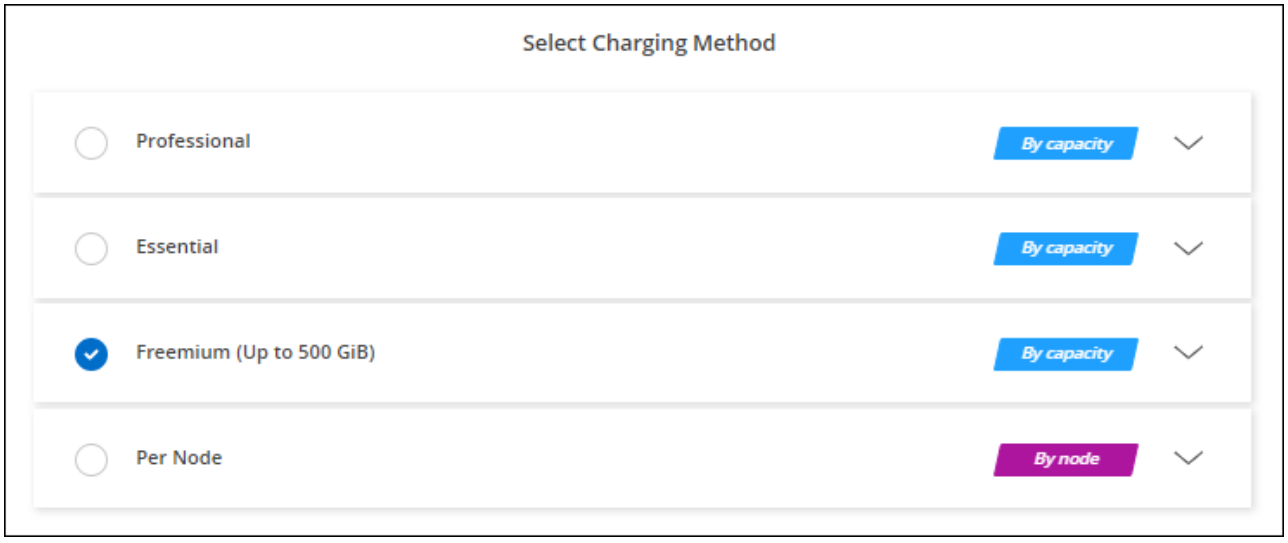
    a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 메시지에 따라 AWS

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"

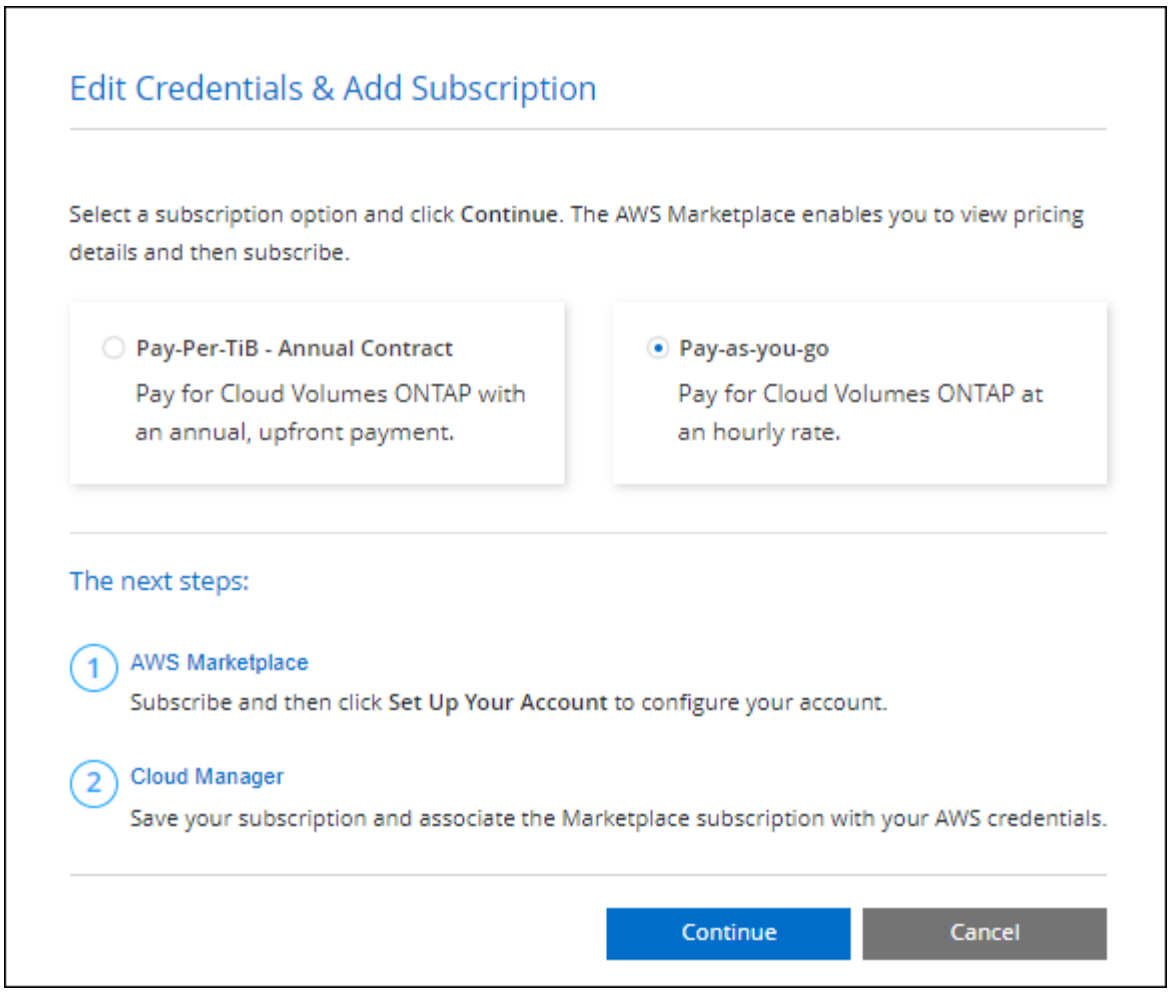
   콘솔은 NetApp 지원 사이트 계정과 연결된 라이선스에 대한 세부 정보를 얻기 위해 NetApp 라이선스 서비스에 자동으로 쿼리를 보냅니다. 오류가 없으면 콘솔이 자동으로 라이선스를 콘솔에 추가합니다.

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

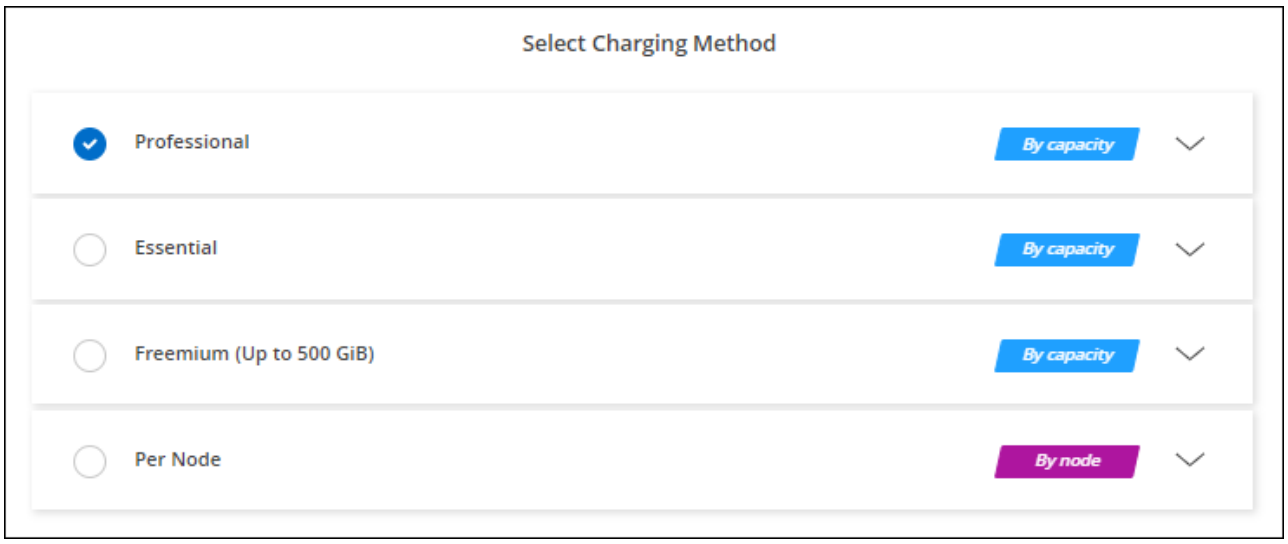
3. 콘솔의 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.

   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." .

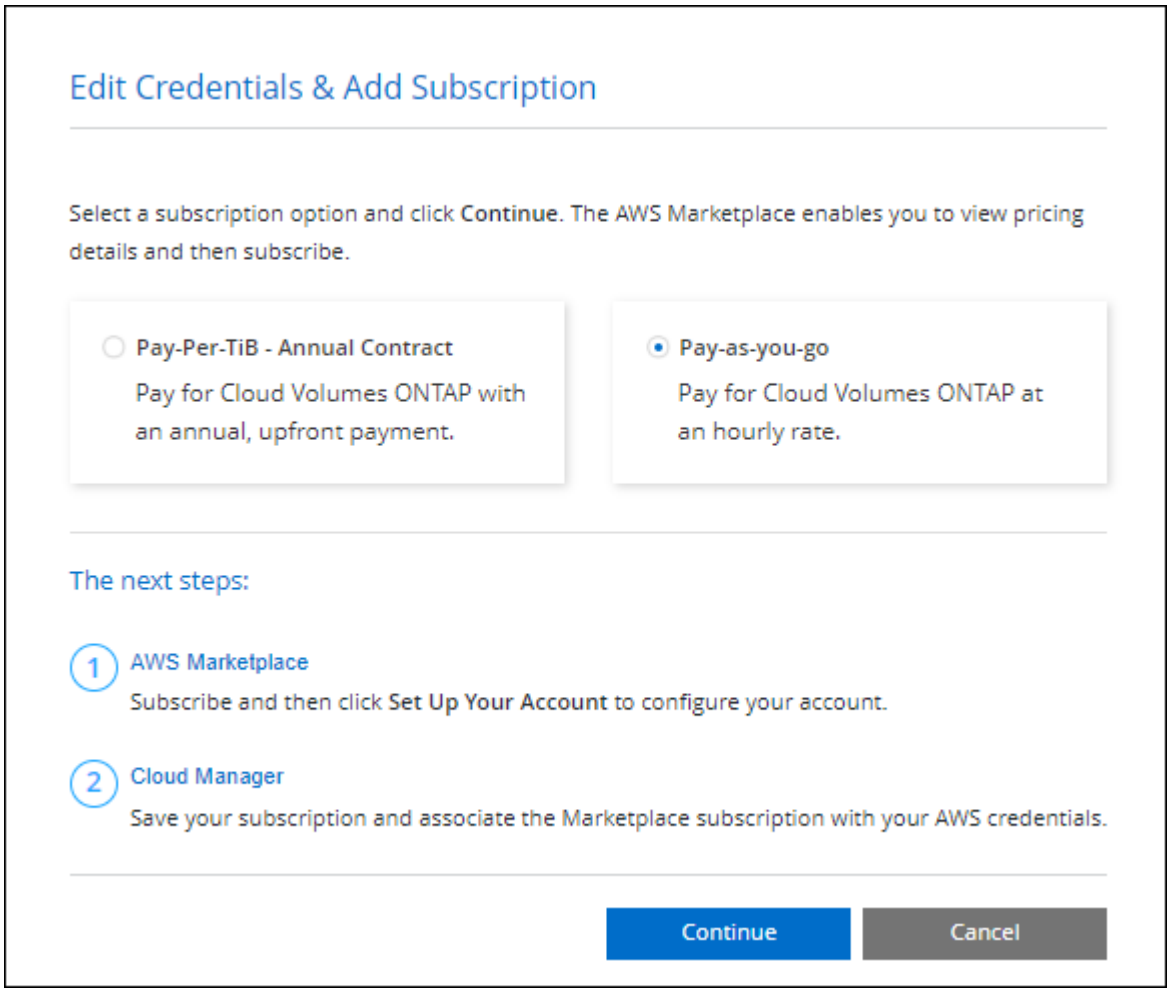
PAYGO 구독

클라우드 공급업체의 마켓플레이스에서 제공하는 혜택을 구독하여 시간당 요금을 지불하세요.

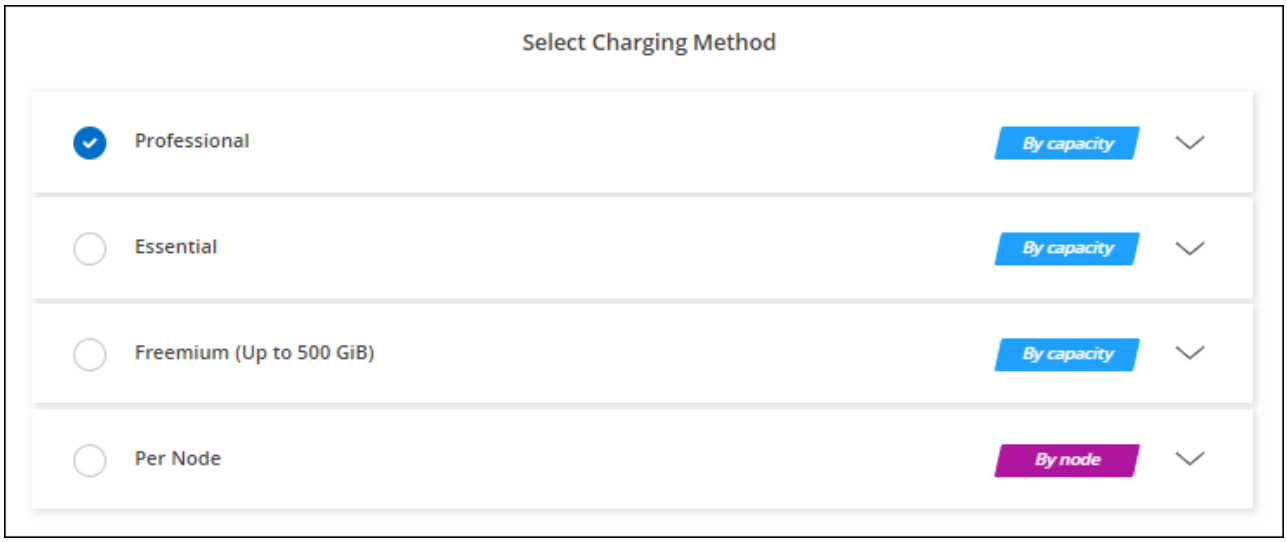
Cloud Volumes ONTAP 시스템을 생성하면 콘솔에서 AWS Marketplace에서 제공되는 계약에 가입하라는 메시지가 표시됩니다. 해당 구독은 요금 청구를 위해 시스템에 연결됩니다. 동일한 구독을 추가 Cloud Volumes ONTAP 시스템에도 사용할 수 있습니다.

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"

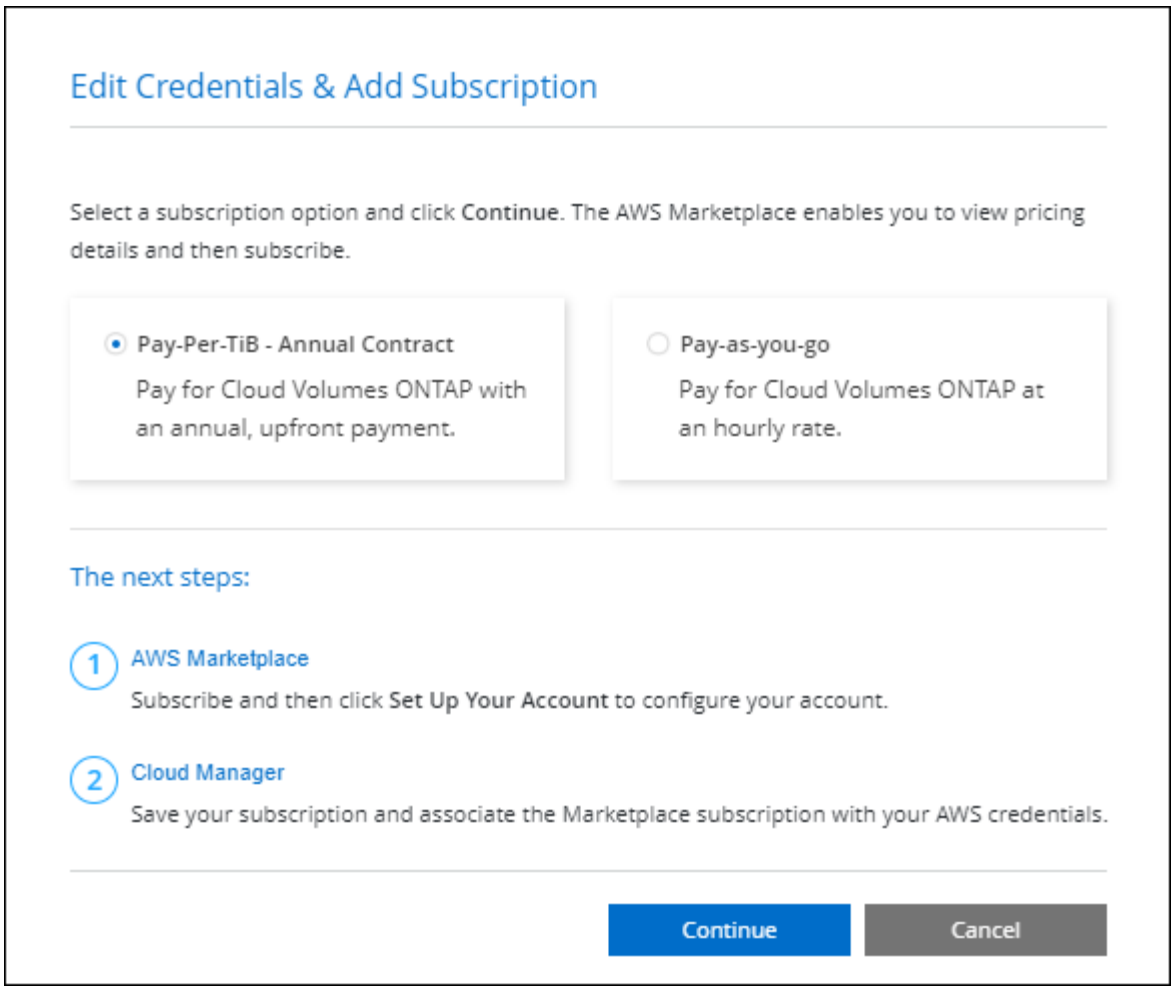
연간 계약

클라우드 공급업체의 마켓플레이스에서 연간 계약을 구매하여 연간으로 지불하세요.

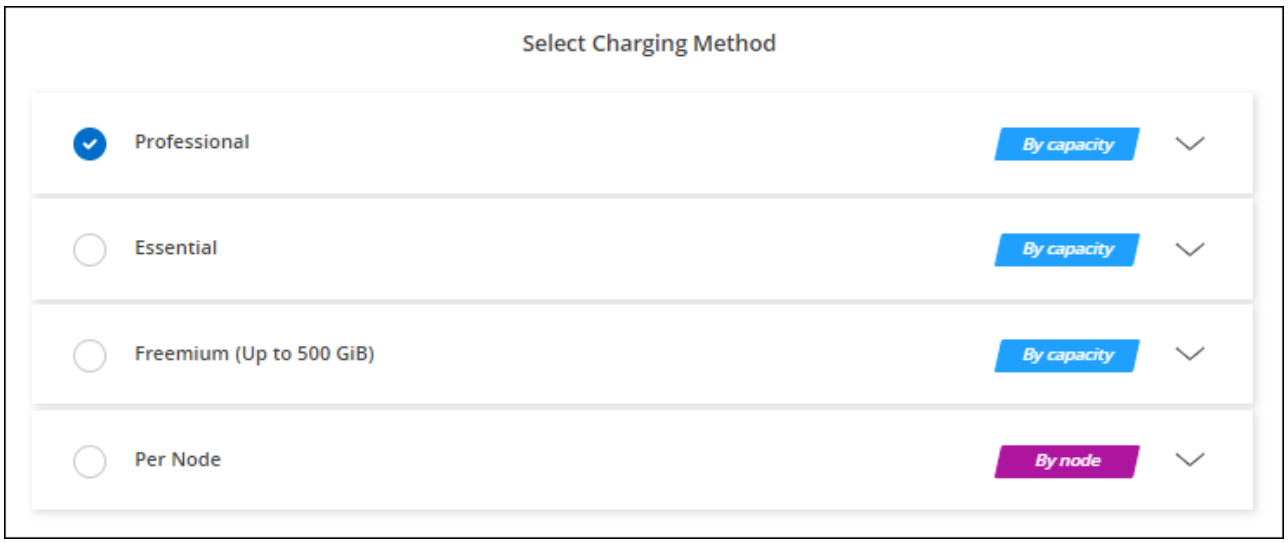
시간당 구독과 비슷하게, 콘솔에서는 AWS Marketplace에서 제공되는 연간 계약을 구독하라는 메시지가 표시됩니다.

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

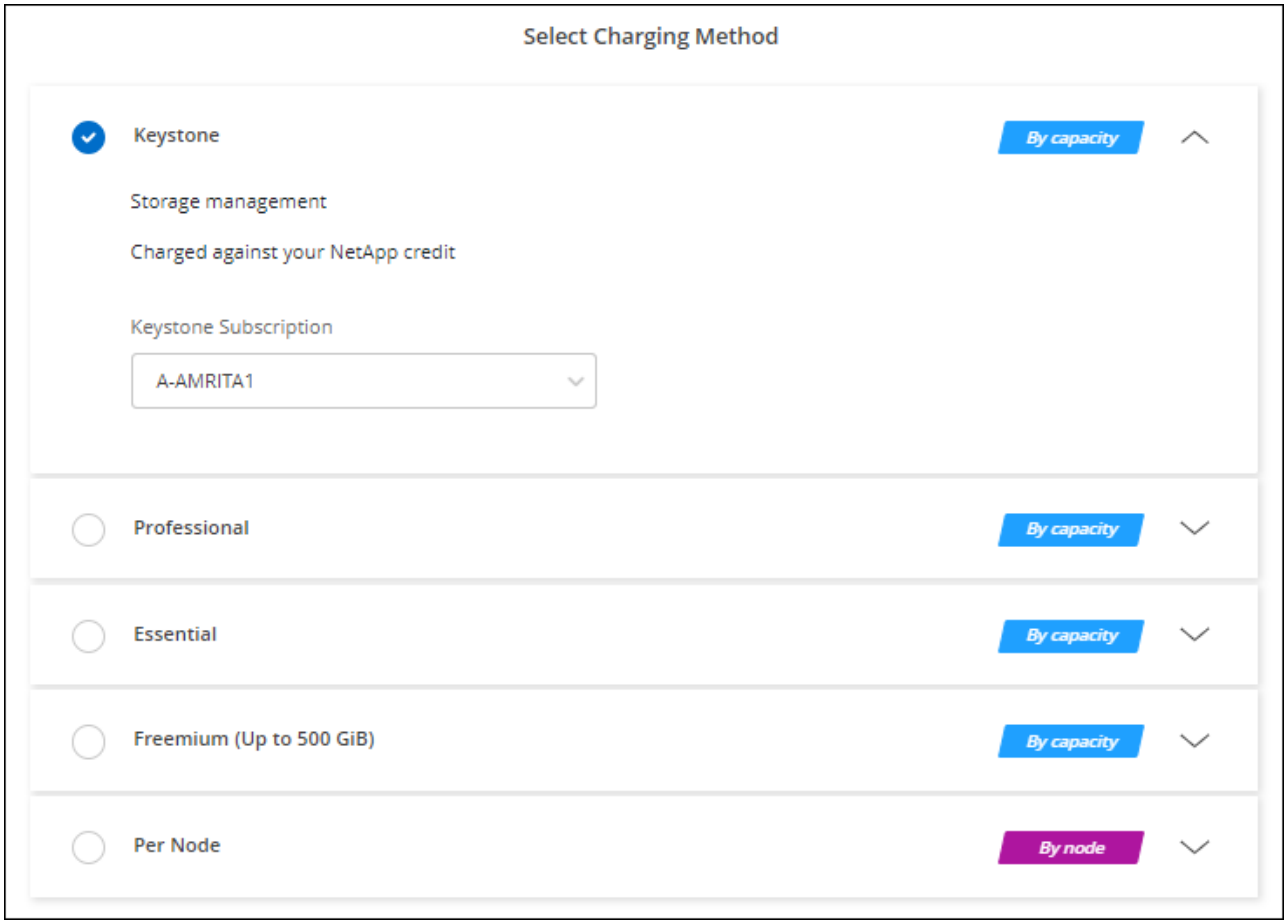
Keystone 구독은 사용량에 따라 비용을 지불하는 구독 기반 서비스입니다. "NetApp Keystone 구독에 대해 자세히

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 **AWS**에 **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.

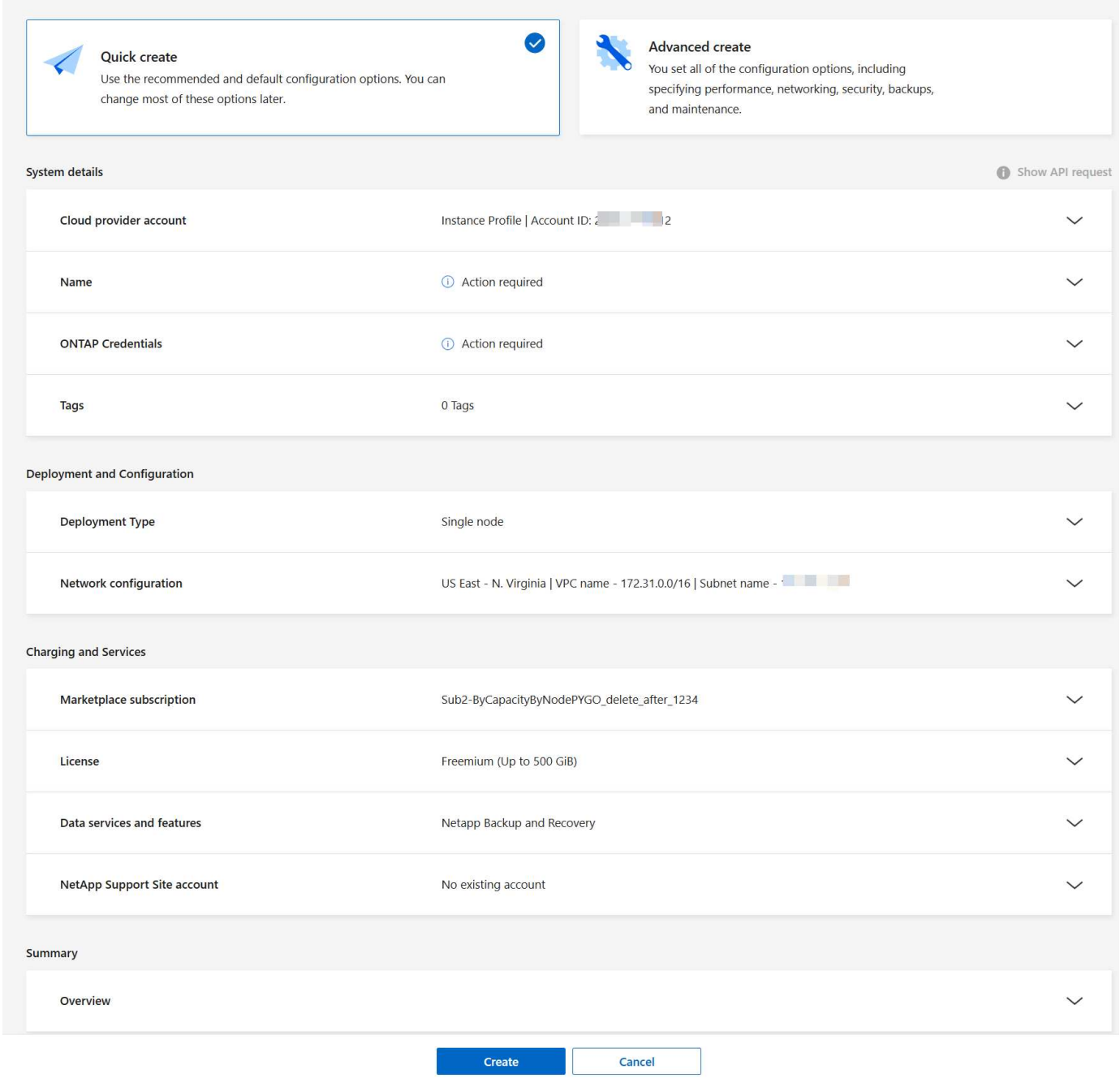
  자세한 내용은 다음을 참조하세요."AWS의 Cloud Volumes ONTAP 에 대한 네트워킹 요구 사항" .

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

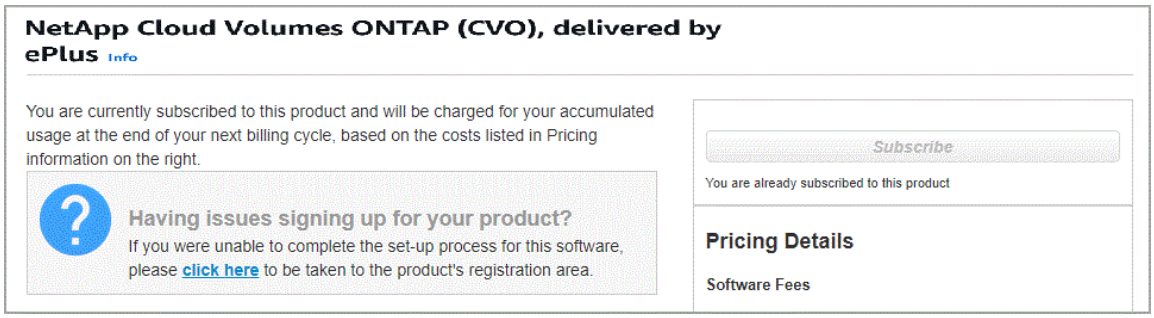
1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 안내를 따르세요.
3. *Amazon Web Services*와 * Cloud Volumes ONTAP Single Node*를 선택하세요.
4. 고급 만들기*를 선택하세요. 기본적으로 *빠른 생성 모드가 선택되어 있으므로 기본값에 대한 메시지가 표시될 수 있습니다. *계속*을 클릭하세요.
5. 메시지가 표시되면 "콘솔 에이전트 생성" .
6. 세부 정보 및 자격 증명: 선택적으로 AWS 자격 증명과 구독을 변경하고, 시스템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

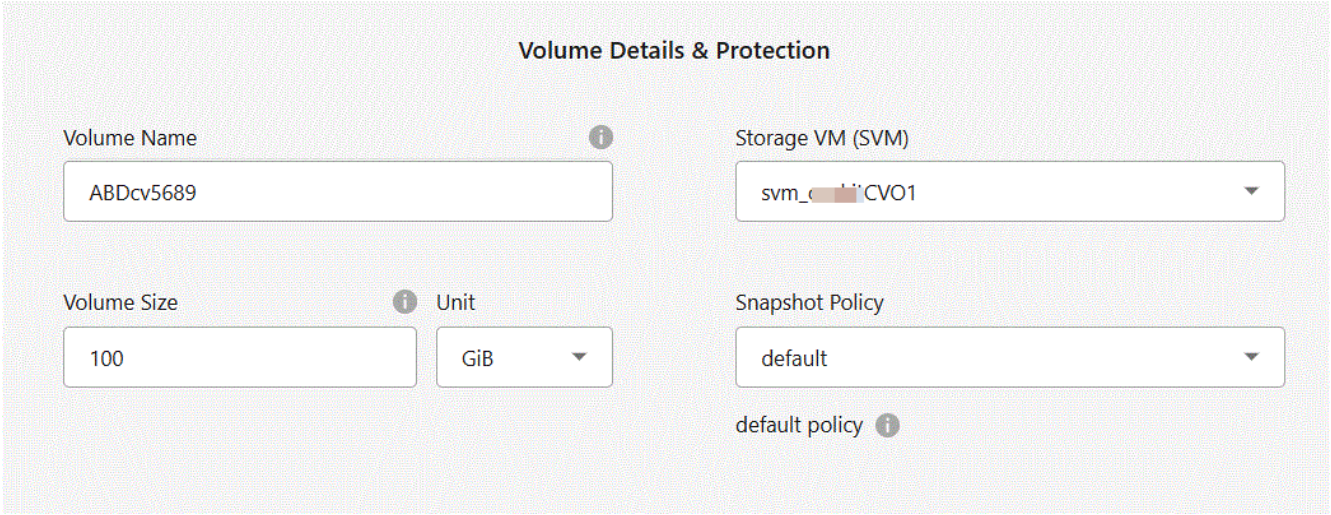
17. 볼륨 만들기: 새 볼륨에 대한 세부 정보를 입력하거나 *건너뛰기*를 클릭합니다.

"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.

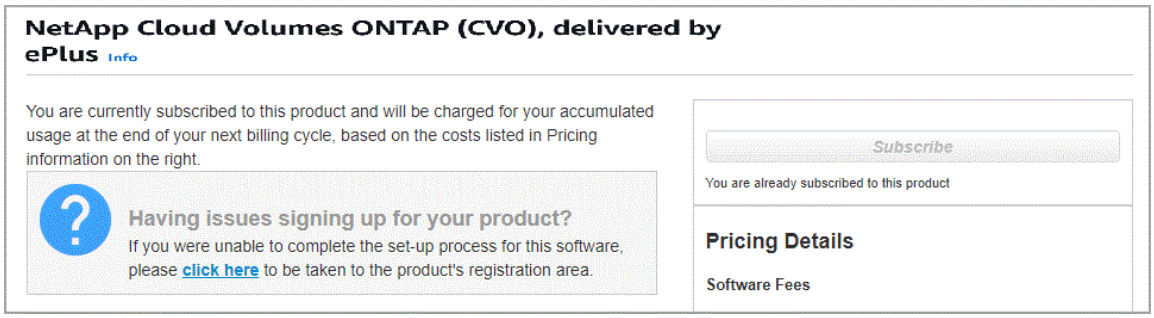
4. 세부 정보 및 자격 증명: 선택적으로 AWS 자격 증명과 구독을 변경하고, 시스템 이름을 입력하고, 필요한 경우 태그를 추가한 다음 비밀번호를 입력합니다.

   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.

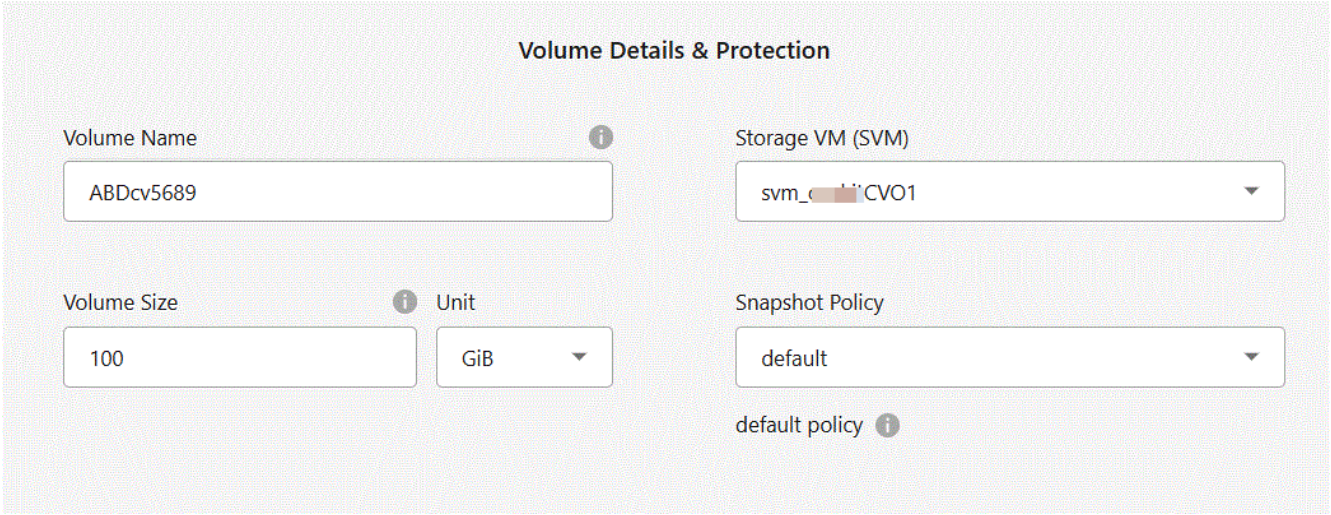
19. 볼륨 만들기: 새 볼륨에 대한 세부 정보를 입력하거나 *건너뛰기*를 클릭합니다.

"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. Amazon Simple Storage Service(Amazon 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>`

Microsoft Azure에서 시작하기

Azure에서 Cloud Volumes ONTAP 배포 옵션에 대해 알아보세요.

NetApp Azure에 Cloud Volumes ONTAP 배포하기 위한 두 가지 옵션을 제공합니다. Cloud Volumes ONTAP 전통적으로 배포 및 오케스트레이션을 위해 NetApp Console 사용합니다. Cloud Volumes ONTAP 9.16.1부터 Azure 마켓플레이스 직접 배포를 활용할 수 있습니다. 이는 제한적이지만 여전히 강력한 Cloud Volumes ONTAP 기능과 옵션에 대한 액세스를 제공하는 간소화된 프로세스입니다.

Azure Marketplace에서 직접 Cloud Volumes ONTAP 배포하는 경우 콘솔 에이전트를 설정하거나 콘솔을 통해 Cloud Volumes ONTAP 배포하는 데 필요한 다른 보안 및 온보딩 기준을 충족할 필요가 없습니다. Azure 마켓플레이스에서 몇 번의 클릭만으로 Cloud Volumes ONTAP 빠르게 배포하고 사용자 환경에서 핵심 기능과 성능을 살펴볼 수 있습니다.

Azure Marketplace에서 배포를 완료하면 콘솔에서 이러한 시스템을 검색할 수 있습니다. 발견 후에는 이를 Cloud Volumes ONTAP 시스템으로 관리하고 모든 콘솔 기능을 활용할 수 있습니다. "콘솔에서 배포된 시스템을 검색하세요" .

두 옵션의 기능을 비교한 내용은 다음과 같습니다. Azure 마켓플레이스를 통해 배포된 독립 실행형 인스턴스의 기능은 콘솔에서 검색될 때 변경됩니다.

	Azure 마켓플레이스	**NetApp Console**
온보딩	직접 배치에 필요한 준비가 최소화되어 더 짧고 쉽습니다.	콘솔 에이전트 설치를 포함한 더 긴 온보딩 프로세스
지원되는 가상 머신**(VM)** 유형	Eds_v5 및 Ls_v3 인스턴스 유형	다양한 VM 유형.https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html["Azure에서 지원되는 구성"^]

	Azure 마켓플레이스	NetApp Console
특허	무료 라이센스	모든 용량 기반 라이센스."Cloud Volumes ONTAP 라이선싱"
* NetApp 지원*	포함되지 않음	라이센스 유형에 따라 사용 가능
용량	최대 500GiB	구성에 따라 확장 가능
배포 모델	단일 가용성 영역(AZ)에 고가용성(HA) 모드 배포	단일 노드 및 HA 모드, 단일 및 다중 AZ 배포를 포함한 모든 지원 구성
지원되는 디스크 유형	프리미엄 SSD v2 관리 디스크	더 폭넓은 지원."Cloud Volumes ONTAP 의 기본 구성"
쓰기 속도(빠른 쓰기 모드)	지원되지 않음	구성에 따라 지원됩니다. "Cloud Volumes ONTAP 의 쓰기 속도에 대해 알아보세요" .
오케스트레이션 기능	사용할 수 없음	라이센스 유형에 따라 NetApp Console 통해 사용 가능
지원되는 스토리지 VM 수	배포당 하나	구성에 따라 여러 개의 스토리지 VM이 제공됩니다."지원되는 스토리지 VM 수"
인스턴스 유형 변경	지원되지 않음	지원됨
* FabricPool 계층화*	지원되지 않음	지원됨

관련 링크

- Azure 마켓플레이스 직접 배포:"Azure Marketplace에서 Cloud Volumes ONTAP 배포"
- 콘솔을 통한 배포:"Azure에서 Cloud Volumes ONTAP 대한 빠른 시작"
- "NetApp Console 설명서"

NetApp Console 에서 시작하기

Azure에서 **Cloud Volumes ONTAP** 대한 빠른 시작

몇 단계만 거치면 Azure용 Cloud Volumes ONTAP 시작할 수 있습니다.


콘솔 에이전트 만들기

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

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


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. 자세한 내용은 다음을 참조하세요. "Azure에서 Cloud Volumes ONTAP 구성 계획" .

3 네트워킹을 설정하세요

1. VNet과 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.

"네트워킹 요구 사항에 대해 자세히 알아보세요" .

4 **Cloud Volumes ONTAP** 출시

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

관련 링크

- "콘솔에서 콘솔 에이전트 만들기"
- "Azure Marketplace에서 콘솔 에이전트 만들기"
- "Linux 호스트에 콘솔 에이전트 소프트웨어 설치"
- "콘솔이 권한으로 수행하는 작업"

Azure에서 **Cloud Volumes ONTAP** 구성 계획

Azure에 Cloud Volumes ONTAP 배포할 때 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 Microsoft Azure 지역에서 지원됩니다. "지원되는 지역의 전체 목록 보기" .

지원되는 **VM** 유형을 선택하세요

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

"Azure의 Cloud Volumes ONTAP 에 지원되는 구성"

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.

"Azure의 Cloud Volumes ONTAP 에 대한 저장소 한도"

Azure에서 시스템 크기 조정

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

가상 머신 유형

지원되는 가상 머신 유형을 살펴보세요. "Cloud Volumes ONTAP 릴리스 노트" 그런 다음 지원되는 각 VM 유형에 대한 세부 정보를 검토합니다. 각 VM 유형은 특정 수의 데이터 디스크를 지원한다는 점을 알아두세요.

- "Azure 설명서: 범용 가상 머신 크기"
- "Azure 설명서: 메모리 최적화된 가상 머신 크기"

단일 노드 시스템의 **Azure** 디스크 유형

Cloud Volumes ONTAP 에 대한 볼륨을 생성할 때 Cloud Volumes ONTAP 디스크로 사용하는 기본 클라우드 스토리지를 선택해야 합니다.

단일 노드 시스템에서는 다음과 같은 유형의 Azure 관리 디스크를 사용할 수 있습니다.

- _프리미엄 SSD 관리 디스크_는 비용이 더 많이 들더라도 I/O 집약적 워크로드에 대해 높은 성능을 제공합니다.
- _프리미엄 SSD v2 관리형 디스크_는 프리미엄 SSD 관리형 디스크에 비해 더 낮은 비용으로 더 높은 성능과 더 낮은 지연 시간을 제공합니다.
- _표준 SSD 관리 디스크_는 낮은 IOPS가 필요한 작업 부하에 대해 일관된 성능을 제공합니다.
- _표준 HDD 관리 디스크_는 높은 IOPS가 필요하지 않고 비용을 절감하고 싶은 경우에 좋은 선택입니다.

이러한 디스크의 사용 사례에 대한 추가 세부 정보는 다음을 참조하세요. "Microsoft Azure 설명서: Azure에서 사용할 수 있는 디스크 유형은 무엇인가요?" .

HA 쌍이 있는 **Azure** 디스크 유형

HA 시스템은 비용이 더 많이 들더라도 I/O 집약적 워크로드에 대해 높은 성능을 제공하는 프리미엄 SSD 공유 관리 디스크를 사용합니다. 9.12.1 릴리스 이전에 생성된 HA 배포는 프리미엄 페이지 Blob을 사용합니다.

Azure 디스크 크기

Cloud Volumes ONTAP 인스턴스를 시작할 때 집계에 대한 기본 디스크 크기를 선택해야 합니다. NetApp Console 초기 집계에 이 디스크 크기를 사용하고, 간단한 프로비저닝 옵션을 사용할 때 생성하는 추가 집계에도 이 디스크 크기를 사용합니다. 기본값과 다른 디스크 크기를 사용하는 집계를 생성할 수 있습니다."고급 할당 옵션 사용" .

집계된 모든 디스크의 크기는 동일해야 합니다.

디스크 크기를 선택할 때는 여러 가지 요소를 고려해야 합니다. 디스크 크기는 스토리지 비용, 집계하여 생성할 수 있는 볼륨 크기, Cloud Volumes ONTAP 에서 사용할 수 있는 총 용량, 스토리지 성능에 영향을 미칩니다.

Azure Premium Storage의 성능은 디스크 크기에 따라 달라집니다. 더 큰 디스크는 더 높은 IOPS와 처리량을

제공합니다. 예를 들어, 1TiB 디스크를 선택하면 500GiB 디스크보다 비용이 더 많이 들더라도 더 나은 성능을 제공할 수 있습니다.

표준 저장소의 디스크 크기에는 성능 차이가 없습니다. 필요한 용량에 따라 디스크 크기를 선택해야 합니다.

디스크 크기별 IOPS 및 처리량은 Azure를 참조하세요.

- "Microsoft Azure: 관리 디스크 가격"
- "Microsoft Azure: 페이지 Blob 가격 책정"

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.

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

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

네트워킹 정보 수집

Azure에 Cloud Volumes ONTAP 배포하는 경우 가상 네트워크에 대한 세부 정보를 지정해야 합니다. 워크시트를 사용하여 관리자로부터 정보를 수집할 수 있습니다.

Azure 정보	당신의 가치
지역	
가상 네트워크(VNet)	
서브넷	
네트워크 보안 그룹(자체 그룹 사용 시)	

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.

Cloud Volumes ONTAP 에 대한 **Azure** 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.

Cloud Volumes ONTAP 요구 사항

Azure에서는 다음과 같은 네트워킹 요구 사항을 충족해야 합니다.

아웃바운드 인터넷 접속

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. 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	사용할 수 없는 경우 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://vault.azure.net	키 볼트	고객 관리 키(CMK)를 사용할 때 Azure Key Vault에서 클라이언트 비밀 키를 검색하는 데 사용됩니다.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP 서비스를 사용할 수 없습니다.

엔드포인트	적용 가능	목적	배포 모드	사용할 수 없는 경우 영향
\ 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.
\ https://management.azure.com \ https://login.microsoftonline.com \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://core.windows.net	공공 지역	Azure 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Azure 콘솔에서 특정 작업을 수행하기 위해 Azure 서비스와 통신할 수 없습니다.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	중국 지역	Azure 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Azure 콘솔에서 특정 작업을 수행하기 위해 Azure 서비스와 통신할 수 없습니다.
\ https://management.microsoftazure.de \ https://login.microsoftonline.de \ https://blob.core.cloudapi.de \ https://core.cloudapi.de	독일 지역	Azure 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Azure 콘솔에서 특정 작업을 수행하기 위해 Azure 서비스와 통신할 수 없습니다.

엔드포인트	적용 가능	목적	배포 모드	사용할 수 없는 경우 영향
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	정부 지역	Azure 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Azure 콘솔에서 특정 작업을 수행하기 위해 Azure 서비스와 통신할 수 없습니다.
\ https://management.azure.microsoft.scloud \ https://login.microsoftonline.microsoft.scloud \ https://blob.core.microsoft.scloud \ https://core.microsoft.scloud	정부 DoD 지역	Azure 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Azure 콘솔에서 특정 작업을 수행하기 위해 Azure 서비스와 통신할 수 없습니다.

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" .

IP 주소

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

Cloud Volumes ONTAP에 할당된 LIF 수는 단일 노드 시스템을 배포하는지 또는 HA 쌍을 배포하는지에 따라 달라집니다. LIF는 물리적 포트와 연결된 IP 주소입니다. SVM 관리 LIF는 SnapCenter와 같은 관리 툴에 필요합니다.

iSCSI LIF는 iSCSI 프로토콜을 통해 클라이언트 액세스를 제공하며 시스템에서 다른 중요한 네트워킹 워크플로에 사용됩니다. 이러한 LIF는 필수이므로 삭제하면 안 됩니다.

단일 노드 시스템의 **IP** 주소

NetApp Console은 단일 노드 시스템에 5개 또는 6개의 IP 주소를 할당합니다.

- 클러스터 관리 IP
- 노드 관리 IP
- SnapMirror 용 클러스터 간 IP
- NFS/CIFS IP
- iSCSI IP

> iSCSI IP는 iSCSI 프로토콜을 통해 클라이언트 액세스를 제공합니다. 또한 시스템에서 다른 중요한 네트워킹 워크플로에도 사용됩니다. 이 LIF는 필수이므로 삭제하면 안 됩니다.

- SVM 관리(선택 사항 - 기본적으로 구성되지 않음)

HA 쌍의 **IP** 주소

콘솔은 배포 중에 노드당 4개의 NIC에 IP 주소를 할당합니다.

참고로 Console은 HA 쌍에 대해서는 SVM 관리 LIF를 생성하지만, Azure의 단일 노드 시스템에 대해서는 생성하지 않습니다.

NIC0

- 노드 관리 IP
- 클러스터 간 IP
- iSCSI IP

> iSCSI IP는 iSCSI 프로토콜을 통해 클라이언트 액세스를 제공합니다. 또한 시스템에서 다른 중요한 네트워킹 워크플로에도 사용됩니다. 이 LIF는 필수이므로 삭제하면 안 됩니다.

NIC1

- 클러스터 네트워크 IP

NIC2

- 클러스터 상호 연결 IP(HA IC)

NIC3

- Pageblob NIC IP(디스크 액세스)

> NIC3는 페이지 Blob 스토리지를 사용하는 HA 배포에만 적용할 수 있습니다.

위의 IP 주소는 장애 조치 이벤트 시 마이그레이션되지 않습니다.

또한 4개의 프런트엔드 IP(FIP)가 장애 조치 이벤트 시 마이그레이션되도록 구성됩니다. 이러한 프런트엔드 IP는 로드

밸런서에 있습니다.

- 클러스터 관리 IP
- NodeA 데이터 IP(NFS/CIFS)
- NodeB 데이터 IP(NFS/CIFS)
- SVM 관리 IP

Azure 서비스에 대한 보안 연결

기본적으로 콘솔은 Cloud Volumes ONTAP 과 Azure 페이지 Blob 스토리지 계정 간의 연결을 위해 Azure Private Link를 활성화합니다.

대부분의 경우 사용자가 해야 할 일은 없습니다. 콘솔이 사용자를 대신하여 Azure Private Link를 관리해 줍니다. 하지만 Azure Private DNS를 사용하는 경우 구성 파일을 편집해야 합니다. Azure에서 콘솔 에이전트의 위치에 대한 요구 사항도 알고 있어야 합니다.

비즈니스 요구 사항에 따라 Private Link 연결을 비활성화할 수도 있습니다. 링크를 비활성화하면 콘솔은 Cloud Volumes ONTAP 대신 서비스 엔드포인트를 사용하도록 구성합니다.

"Cloud Volumes ONTAP 에서 Azure Private Links 또는 서비스 엔드포인트를 사용하는 방법에 대해 자세히 알아보세요." .

Azure VNet 암호화를 위한 네트워킹

Cloud Volumes ONTAP는 VNet 내부 또는 피어링된 VNet 간의 VM 간 트래픽 "Azure Virtual Network(VNet) 암호화"을 지원합니다. 이 기능은 Azure VNet 계층에서 구성되며 Cloud Volumes ONTAP 토폴로지(단일 노드 또는 HA)와는 무관합니다.

VM의 NIC에서 가속 네트워킹이 활성화되어 있는지 확인하고 Azure VNet 암호화 요구 사항 및 제한 사항을 검토한 후 해당 기능을 활성화하면 됩니다. NetApp 관리형 로드 밸런서 개체는 수정해서는 안 됩니다.

"Azure 설명서: VNet 암호화 및 가속 네트워킹".

다른 **ONTAP** 시스템에 대한 연결

Azure의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 Azure VNet과 다른 네트워크(예: 회사 네트워크) 간에 VPN 연결이 필요합니다.

지침은 다음을 참조하세요. "Microsoft Azure 설명서: Azure Portal에서 사이트 간 연결 만들기" .

HA 상호 연결을 위한 포트

Cloud Volumes ONTAP HA 쌍에는 HA 상호 연결이 포함되어 있어 각 노드가 파트너가 제대로 작동하는지 지속적으로 확인하고 다른 노드의 비휘발성 메모리에 대한 로그 데이터를 미러링할 수 있습니다. HA 상호 연결은 통신을 위해 TCP 포트 10006을 사용합니다.

기본적으로 HA 상호 연결 LIF 간 통신은 열려 있으며 이 포트에 대한 보안 그룹 규칙은 없습니다. 하지만 HA 상호 연결 LIF 사이에 방화벽을 만드는 경우 HA 쌍이 제대로 작동할 수 있도록 포트 10006에 대한 TCP 트래픽이 열려 있는지 확인해야 합니다.

Azure 리소스 그룹에는 **HA** 쌍이 하나만 있습니다**.**

Azure에 배포하는 각 Cloud Volumes ONTAP HA 쌍에 대해 전용 리소스 그룹을 사용해야 합니다. 리소스 그룹에서는 HA 쌍을 하나만 지원합니다.

Azure 리소스 그룹에 두 번째 Cloud Volumes ONTAP HA 쌍을 배포하려고 하면 콘솔에서 연결 문제가 발생합니다.

보안 그룹 규칙

콘솔은 Cloud Volumes ONTAP 성공적으로 작동할 수 있도록 인바운드 및 아웃바운드 규칙을 포함하는 Azure 보안 그룹을 만듭니다. "콘솔 에이전트에 대한 보안 그룹 규칙 보기" .

Cloud Volumes ONTAP 용 Azure 보안 그룹에는 노드 간 내부 통신을 위해 적절한 포트가 열려 있어야 합니다. "ONTAP 내부 포트에 대해 알아보세요" .

미리 정의된 보안 그룹을 수정하거나 사용자 지정 보안 그룹을 사용하는 것은 권장하지 않습니다. 하지만 반드시 그렇게 해야 하는 경우 배포 프로세스에서 Cloud Volumes ONTAP 시스템이 자체 서브넷 내에서 전체 액세스 권한을 가져야 한다는 점에 유의하세요. 배포가 완료된 후 네트워크 보안 그룹을 수정하기로 결정한 경우 클러스터 포트와 HA 네트워크 포트를 열어 두세요. 이를 통해 Cloud Volumes ONTAP 클러스터 내에서 원활한 통신(노드 간 모든 통신)이 보장됩니다.

단일 노드 시스템에 대한 인바운드 규칙

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

- 선택된 **VNet**만 해당: 인바운드 트래픽의 소스는 Cloud Volumes ONTAP 시스템의 VNet 서브넷 범위와 콘솔 에이전트가 있는 VNet의 서브넷 범위입니다. 이것은 권장되는 옵션입니다.
- 모든 **VNet**: 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
- 비활성화: 이 옵션은 스토리지 계정에 대한 공용 네트워크 액세스를 제한하고 Cloud Volumes ONTAP 시스템의 데이터 계층화를 비활성화합니다. 보안 규정 및 정책으로 인해 동일한 VNet 내에서도 개인 IP 주소가 노출되어서는 안 되는 경우 이 옵션을 사용하는 것이 좋습니다.

우선순위와 이름	포트 및 프로토콜	출발지와 목적지	설명
1000 인바운드_ssh	22 TCP	어떤 것으로든	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 대한 SSH 액세스
1001 인바운드_http	80 TCP	어떤 것으로든	클러스터 관리 LIF의 IP 주소를 사용하여 ONTAP System Manager 웹 콘솔에 대한 HTTP 액세스
1002 inbound_111_tcp	111 TCP	어떤 것으로든	NFS에 대한 원격 프로시저 호출
1003 inbound_111_udp	111 UDP	어떤 것으로든	NFS에 대한 원격 프로시저 호출
1004 inbound_139	139 TCP	어떤 것으로든	CIFS용 NetBIOS 서비스 세션
1005 인바운드_161-162_tcp	161-162 TCP	어떤 것으로든	간단한 네트워크 관리 프로토콜

우선순위와 이름	포트 및 프로토콜	출발지와 목적지	설명
1006 인바운드_161-162_udp	161-162 UDP	어떤 것으로든	간단한 네트워크 관리 프로토콜
1007 inbound_443	443 TCP	어떤 것으로든	클러스터 관리 LIF의 IP 주소를 사용하여 콘솔 에이전트와 ONTAP System Manager 웹 콘솔에 대한 HTTPS 액세스 연결
1008 inbound_445	445 TCP	어떤 것으로든	NetBIOS 프레이밍을 통한 TCP를 통한 Microsoft SMB/CIFS
1009 inbound_635_tcp	635 TCP	어떤 것으로든	NFS 마운트
1010 inbound_635_udp	635 UDP	어떤 것으로든	NFS 마운트
1011 inbound_749	749 TCP	어떤 것으로든	케르베로스
1012 inbound_2049_tcp	2049 TCP	어떤 것으로든	NFS 서버 데몬
1013 inbound_2049_udp	2049 UDP	어떤 것으로든	NFS 서버 데몬
1014 inbound_3260	3260 TCP	어떤 것으로든	iSCSI 데이터 LIF를 통한 iSCSI 액세스
1015 인바운드_4045-4046_tcp	4045-4046 TCP	어떤 것으로든	NFS 잠금 데몬 및 네트워크 상태 모니터
1016 인바운드_4045-4046_udp	4045-4046 UDP	어떤 것으로든	NFS 잠금 데몬 및 네트워크 상태 모니터
1017 inbound_10000	10000 TCP	어떤 것으로든	NDMP를 사용한 백업
1018 인바운드_11104-11105	11104-11105 TCP	어떤 것으로든	SnapMirror 데이터 전송
3000 인바운드_거부_모든_tcp	모든 포트 TCP	어떤 것으로든	다른 모든 TCP 인바운드 트래픽 차단
3001 인바운드_거부_모든_udp	모든 포트 UDP	어떤 것으로든	다른 모든 UDP 인바운드 트래픽 차단
65000 AllowVnetInBound	모든 포트 모든 프로토콜	VirtualNetwork에서 VirtualNetwork로	VNet 내부에서 들어오는 트래픽
65001 AllowAzureLoadBalancerInBound	모든 포트 모든 프로토콜	AzureLoadBalancer를 Any로	Azure Standard Load Balancer의 데이터 트래픽
65500 DenyAllInBound	모든 포트 모든 프로토콜	어떤 것으로든	다른 모든 인바운드 트래픽 차단

HA 시스템에 대한 인바운드 규칙

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

- 선택된 **VNet**만 해당: 인바운드 트래픽의 소스는 Cloud Volumes ONTAP 시스템의 VNet 서브넷 범위와 콘솔

에이전트가 있는 VNet의 서브넷 범위입니다. 이것은 권장되는 옵션입니다.

- 모든 **VNet**: 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.

> HA 시스템은 인바운드 데이터 트래픽이 Azure Standard Load Balancer를 통과하기 때문에 단일 노드 시스템보다 인바운드 규칙이 적습니다. 따라서 "AllowAzureLoadBalancerInBound" 규칙에 표시된 것처럼 Load Balancer에서 들어오는 트래픽은 허용되어야 합니다.

- 비활성화: 이 옵션은 스토리지 계정에 대한 공용 네트워크 액세스를 제한하고 Cloud Volumes ONTAP 시스템의 데이터 계층화를 비활성화합니다. 보안 규정 및 정책으로 인해 동일한 VNet 내에서도 개인 IP 주소가 노출되어서는 안 되는 경우 이 옵션을 사용하는 것이 좋습니다.

우선순위와 이름	포트 및 프로토콜	출발지와 목적지	설명
100 inbound_443	443 모든 프로토콜	어떤 것으로든	클러스터 관리 LIF의 IP 주소를 사용하여 콘솔 에이전트와 ONTAP System Manager 웹 콘솔에 대한 HTTPS 액세스 연결
101 inbound_111_tcp	111 모든 프로토콜	어떤 것으로든	NFS에 대한 원격 프로시저 호출
102 inbound_2049_tcp	2049 모든 프로토콜	어떤 것으로든	NFS 서버 데몬
111 인바운드_ssh	22 모든 프로토콜	어떤 것으로든	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 대한 SSH 액세스
121 inbound_53	53 모든 프로토콜	어떤 것으로든	DNS와 CIFS
65000 AllowVnetInBound	모든 포트 모든 프로토콜	VirtualNetwork에서 VirtualNetwork로	VNet 내부에서 들어오는 트래픽
65001 AllowAzureLoad BalancerInBound	모든 포트 모든 프로토콜	AzureLoadBalancer를 Any로	Azure Standard Load Balancer의 데이터 트래픽
65500 DenyAllInBound	모든 포트 모든 프로토콜	어떤 것으로든	다른 모든 인바운드 트래픽 차단

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.

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

서비스	포트	규약	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
구성 백업	HTTP	80	노드 관리 LIF	http://<콘솔 에이전트 IP 주소>/occm/offboxconfig	구성 백업을 콘솔 에이전트로 보냅니다. "ONTAP 문서" .
DHCP	68	UDP	노드 관리 LIF	DHCP	최초 설정을 위한 DHCP 클라이언트
DHCPS	67	UDP	노드 관리 LIF	DHCP	DHCP 서버
DNS	53	UDP	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
NDMP	18600년–18699년	TCP	노드 관리 LIF	대상 서버	NDMP 사본
SMTP	25	TCP	노드 관리 LIF	메일 서버	SMTP 알림은 AutoSupport 에 사용할 수 있습니다.
SNMP	161	TCP	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	161	UDP	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	162	TCP	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
	162	UDP	노드 관리 LIF	모니터 서버	SNMP 트랩을 통한 모니터링
SnapMirror	11104	TCP	클러스터 간 LIF	ONTAP 클러스터 간 LIF	SnapMirror 위한 클러스터 간 통신 세션 관리
	11105	TCP	클러스터 간 LIF	ONTAP 클러스터 간 LIF	SnapMirror 데이터 전송
시스템 로그	514	UDP	노드 관리 LIF	시스템 로그 서버	Syslog 전달 메시지

콘솔 에이전트에 대한 요구 사항

아직 콘솔 에이전트를 만들지 않았다면 콘솔 에이전트에 대한 네트워킹 요구 사항도 검토해야 합니다.

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

관련 주제

- "Cloud Volumes ONTAP 에 대한 AutoSupport 설정 확인"

- "ONTAP 내부 포트에 대해 알아보세요" .

Azure에서 고객 관리 키를 사용하도록 **Cloud Volumes ONTAP** 설정

Azure의 Cloud Volumes ONTAP 에서는 Microsoft에서 관리하는 키를 사용하여 Azure Storage Service Encryption을 사용하여 데이터가 자동으로 암호화됩니다. 하지만 이 페이지의 단계에 따라 자신의 암호화 키를 대신 사용할 수 있습니다.

데이터 암호화 개요

Cloud Volumes ONTAP 데이터는 Azure에서 자동으로 암호화됩니다. "Azure Storage 서비스 암호화" . 기본 구현에서는 Microsoft에서 관리하는 키를 사용합니다. 설정이 필요하지 않습니다.

Cloud Volumes ONTAP 에서 고객 관리 키를 사용하려면 다음 단계를 완료해야 합니다.

1. Azure에서 키 자격 증명 모음을 만든 다음 해당 자격 증명 모음에서 키를 생성합니다.
2. NetApp Console 에서 API를 사용하여 키를 사용하는 Cloud Volumes ONTAP 시스템을 만듭니다.

데이터 암호화 방법

콘솔은 디스크 암호화 세트를 사용하는데, 이를 통해 페이지 블롭이 아닌 관리형 디스크에서 암호화 키를 관리할 수 있습니다. 새로운 데이터 디스크도 동일한 디스크 암호화 세트를 사용합니다. 하위 버전에서는 고객 관리 키 대신 Microsoft 관리 키를 사용합니다.

고객 관리 키를 사용하도록 구성된 Cloud Volumes ONTAP 시스템을 생성한 후 Cloud Volumes ONTAP 데이터는 다음과 같이 암호화됩니다.

Cloud Volumes ONTAP 구성	키 암호화에 사용되는 시스템 디스크	키 암호화에 사용되는 데이터 디스크
단일 노드	• 부팅 • 핵심 • NVRAM	• 뿌리 • 데이터
페이지 Blob이 있는 Azure HA 단일 가용성 영역	• 부팅 • 핵심 • NVRAM	None
공유 관리 디스크가 있는 Azure HA 단일 가용성 영역	• 부팅 • 핵심 • NVRAM	• 뿌리 • 데이터
공유 관리 디스크를 사용한 Azure HA 다중 가용성 영역	• 부팅 • 핵심 • NVRAM	• 뿌리 • 데이터

Cloud Volumes ONTAP 의 모든 Azure 스토리지 계정은 고객 관리 키를 사용하여 암호화됩니다. 스토리지 계정을 생성하는 동안 암호화하려면 Cloud Volumes ONTAP 생성 요청에서 리소스 ID를 생성하고 제공해야 합니다. 이는 모든 유형의 배포에 적용됩니다. 해당 정보를 제공하지 않으면 저장소 계정은 여전히 암호화되지만 콘솔은 먼저 Microsoft에서 관리하는 키 암호화를 사용하여 저장소 계정을 만든 다음, 저장소 계정을 업데이트하여 고객이 관리하는 키를 사용합니다.

Cloud Volumes ONTAP 의 키 회전

암호화 키를 구성할 때 Azure Portal을 사용하여 자동 키 순환을 설정하고 활성화해야 합니다. 암호화 키의 새로운 버전을 만들고 활성화하면 Cloud Volumes ONTAP 암호화에 최신 키 버전을 자동으로 감지하고 사용할 수 있으므로 수동 개입 없이도 데이터가 안전하게 유지됩니다.

키 구성 및 키 순환 설정에 대한 자세한 내용은 다음 Microsoft Azure 설명서 항목을 참조하세요.

- "Azure Key Vault에서 암호화 키 자동 순환 구성"
- "Azure PowerShell - 고객 관리 키 사용"

> 키를 구성한 후 다음을 선택했는지 확인하십시오. "자동 회전 활성화" 이를 통해 Cloud Volumes ONTAP 이전 키가 만료되면 새 키를 사용할 수 있습니다. Azure Portal에서 이 옵션을 활성화하지 않으면 Cloud Volumes ONTAP 새 키를 자동으로 감지하지 못하여 스토리지 프로비저닝에 문제가 발생할 수 있습니다.

사용자가 할당한 관리 ID 만들기

사용자 지정 관리 ID라는 리소스를 만들 수 있는 옵션이 있습니다. 이렇게 하면 Cloud Volumes ONTAP 시스템을 생성할 때 스토리지 계정을 암호화할 수 있습니다. 키 보관소를 만들고 키를 생성하기 전에 이 리소스를 만드는 것이 좋습니다.

리소스의 ID는 다음과 같습니다. `userassignedidentity` .

단계

1. Azure에서 Azure 서비스로 이동하여 *관리 ID*를 선택합니다.
2. *만들기*를 클릭하세요.
3. 다음 세부 정보를 제공하세요.
    - 구독: 구독을 선택하세요. 콘솔 에이전트 구독과 동일한 구독을 선택하는 것이 좋습니다.
    - 리소스 그룹: 기존 리소스 그룹을 사용하거나 새 리소스 그룹을 만듭니다.
    - 지역: 선택적으로 콘솔 에이전트와 동일한 지역을 선택합니다.
    - 이름: 리소스의 이름을 입력하세요.
4. 선택적으로 태그를 추가합니다.
5. *만들기*를 클릭하세요.

키 볼트를 생성하고 키를 생성합니다.

키 보관소는 Cloud Volumes ONTAP 시스템을 만들려는 동일한 Azure 구독 및 지역에 있어야 합니다.

만약 당신이라면사용자가 할당한 관리 ID를 생성했습니다. 키 보관소를 생성하는 동안 키 보관소에 대한 액세스 정책도 생성해야 합니다.

단계

1. "Azure 구독에서 키 자격 증명 모음 만들기" .

   키 보관소에 대한 다음 요구 사항을 참고하세요.

   - 키 볼트는 Cloud Volumes ONTAP 시스템과 동일한 지역에 있어야 합니다.
   - 다음 옵션을 활성화해야 합니다.
     - 소프트 삭제 (이 옵션은 기본적으로 활성화되어 있지만 비활성화해서는 안 됩니다)
     - 퍼지 보호
     - 볼륨 암호화를 위한 **Azure Disk Encryption** (단일 노드 시스템, 여러 영역의 HA 쌍 및 HA 단일 AZ 배포용)

       Azure 고객 관리 암호화 키를 사용하려면 키 자격 증명 모음에 Azure Disk 암호화가 활성화되어 있어야 합니다.

   - 사용자가 할당한 관리 ID를 생성한 경우 다음 옵션을 활성화해야 합니다.
     - 금고 접근 정책
2. Vault 액세스 정책을 선택한 경우 만들기를 클릭하여 키 볼트에 대한 액세스 정책을 만듭니다. 그렇지 않은 경우 3단계로 넘어가세요.
   a. 다음 권한을 선택하세요.
      - 얻다
      - 목록
      - 해독하다
      - 암호화하다
      - 열쇠를 풀다
      - 랩 키
      - 확인하다
      - 징후
   b. 사용자가 할당한 관리 ID(리소스)를 주체로 선택합니다.
   c. 액세스 정책을 검토하고 생성합니다.
3. "키 보관소에서 키 생성" .

   키에 대한 다음 요구 사항을 참고하세요.

   - 키 유형은 *RSA*여야 합니다.
   - 권장되는 RSA 키 크기는 *2048*이지만 다른 크기도 지원됩니다.

암호화 키를 사용하는 시스템을 만듭니다.

키 볼트를 만들고 암호화 키를 생성한 후에는 해당 키를 사용하도록 구성된 새 Cloud Volumes ONTAP 시스템을 만들 수 있습니다. 이러한 단계는 API를 사용하여 지원됩니다.

필요한 권한

단일 노드 Cloud Volumes ONTAP 시스템에서 고객 관리 키를 사용하려면 콘솔 에이전트에 다음 권한이 있는지 확인하세요.

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"최신 권한 목록 보기"

단계

1. 다음 API 호출을 사용하여 Azure 구독의 주요 자격 증명 모음 목록을 가져옵니다.

   HA 쌍의 경우: `GET /azure/ha/metadata/vaults`

   단일 노드의 경우: `GET /azure/vsa/metadata/vaults`

   *이름*과 *리소스그룹*을 기록해 두세요. 다음 단계에서 해당 값을 지정해야 합니다.

   "이 API 호출에 대해 자세히 알아보세요" .

2. 다음 API 호출을 사용하여 볼트 내의 키 목록을 가져옵니다.

   HA 쌍의 경우: `GET /azure/ha/metadata/keys-vault`

   단일 노드의 경우: `GET /azure/vsa/metadata/keys-vault`

   *keyName*을 기록해 두세요. 다음 단계에서는 해당 값(볼트 이름과 함께)을 지정해야 합니다.

   "이 API 호출에 대해 자세히 알아보세요" .

3. 다음 API 호출을 사용하여 Cloud Volumes ONTAP 시스템을 만듭니다.

   a. HA 쌍의 경우:

      `POST /azure/ha/working-environments`

      요청 본문에는 다음 필드가 포함되어야 합니다.

      ```
      "azureEncryptionParameters": {
                    "key": "keyName",
                    "vaultName": "vaultName"
      }
      ```

포함하다 "userAssignedIdentity": " userAssignedIdentityId" 저장소 계정 암호화에 사용할 리소스를 만든 경우 필드입니다.

"이 API 호출에 대해 자세히 알아보세요" .

b. 단일 노드 시스템의 경우:

```
POST /azure/vsa/working-environments
```

요청 본문에는 다음 필드가 포함되어야 합니다.

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

포함하다 "userAssignedIdentity": " userAssignedIdentityId" 저장소 계정 암호화에 사용할 리소스를 만든 경우 필드입니다.

"이 API 호출에 대해 자세히 알아보세요" .

결과

데이터 암호화를 위해 고객 관리 키를 사용하도록 구성된 새로운 Cloud Volumes ONTAP 시스템이 있습니다.

Azure에서 **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

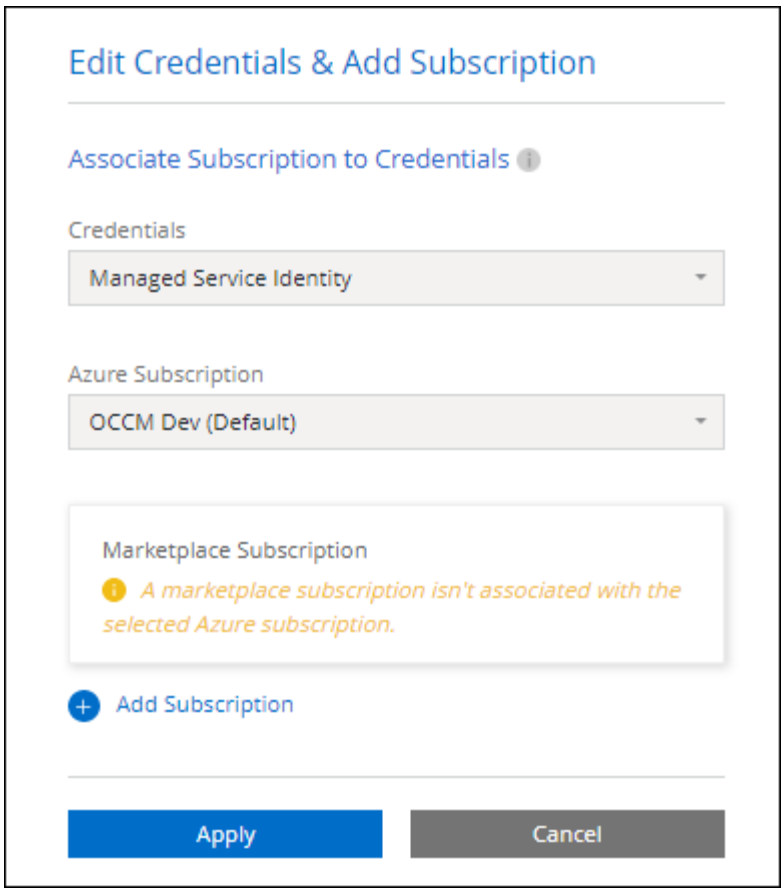
최대 500GiB의 프로비저닝 용량을 제공하는 Cloud Volumes ONTAP 무료로 사용하려면 Freemium 옵션을 선택하세요. "Freemium 제공에 대해 자세히 알아보세요" .

단계

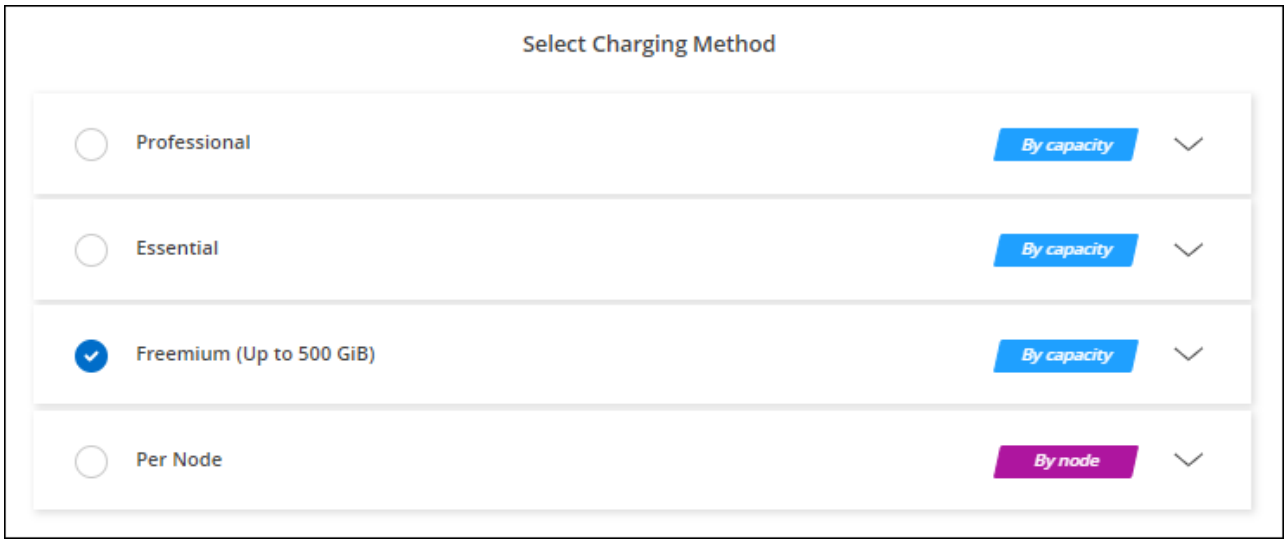
1. NetApp Console 의 왼쪽 탐색 메뉴에서 *스토리지 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.

   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 화면의 지시에 따라 Azure Marketplace에서 종량제 상품을 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.



"Azure에서 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))
- Azure Marketplace의 시간당, 사용량에 따라 지불(PAYGO) 구독
- 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"

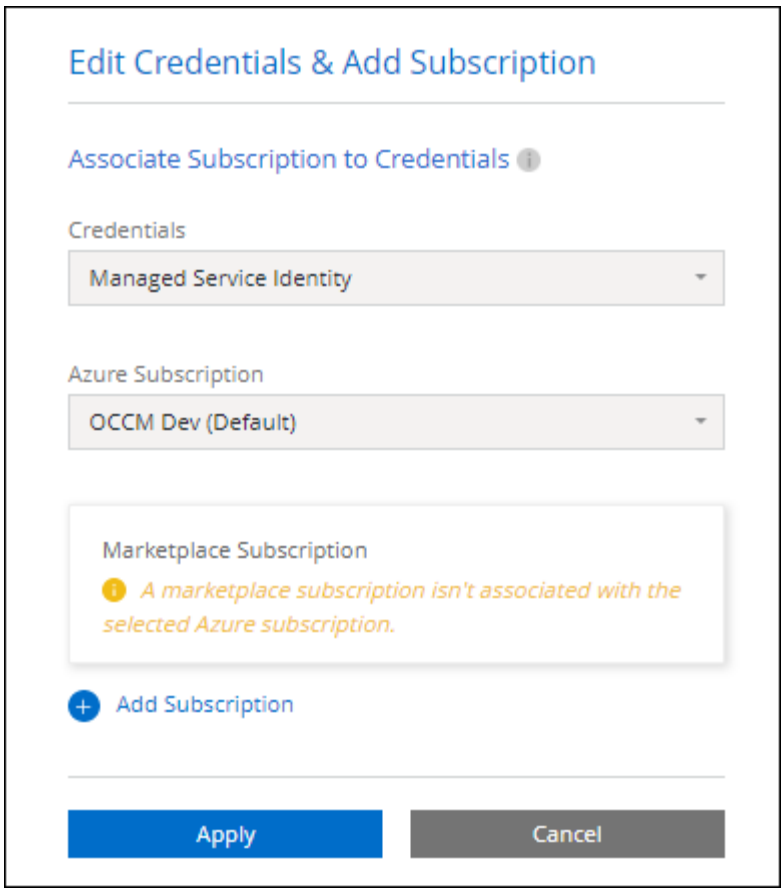
   콘솔은 NetApp 지원 사이트 계정과 연결된 라이선스에 대한 세부 정보를 얻기 위해 NetApp 라이선스 서비스에 자동으로 쿼리를 보냅니다. 오류가 없으면 콘솔이 자동으로 라이선스를 콘솔에 추가합니다.

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

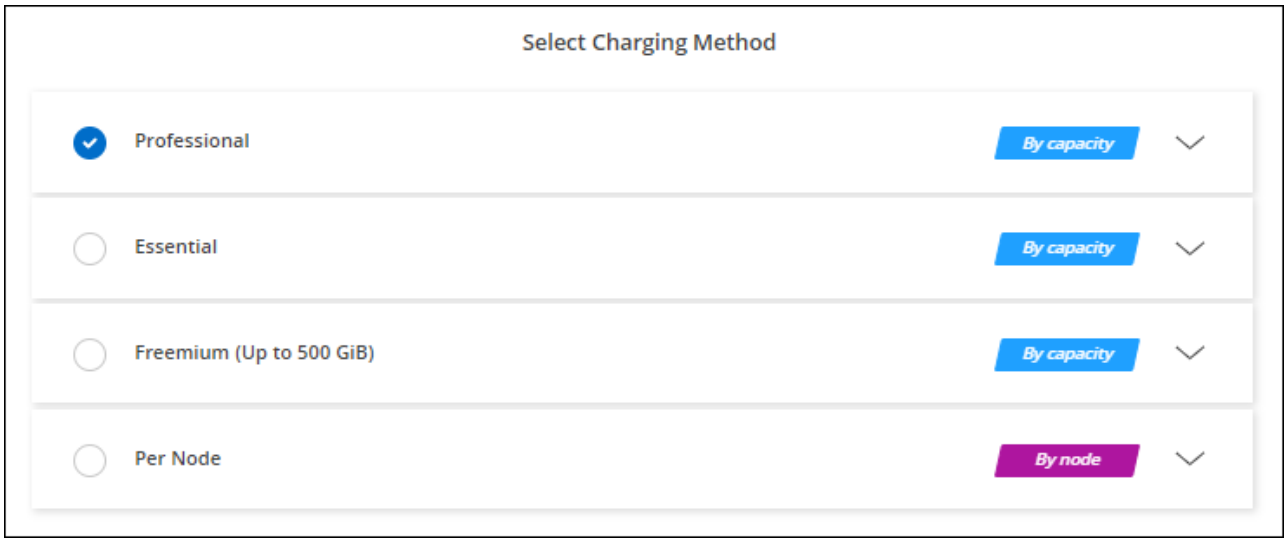
3. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.

   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 화면의 지시에 따라 Azure Marketplace에서 종량제 상품을 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.



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

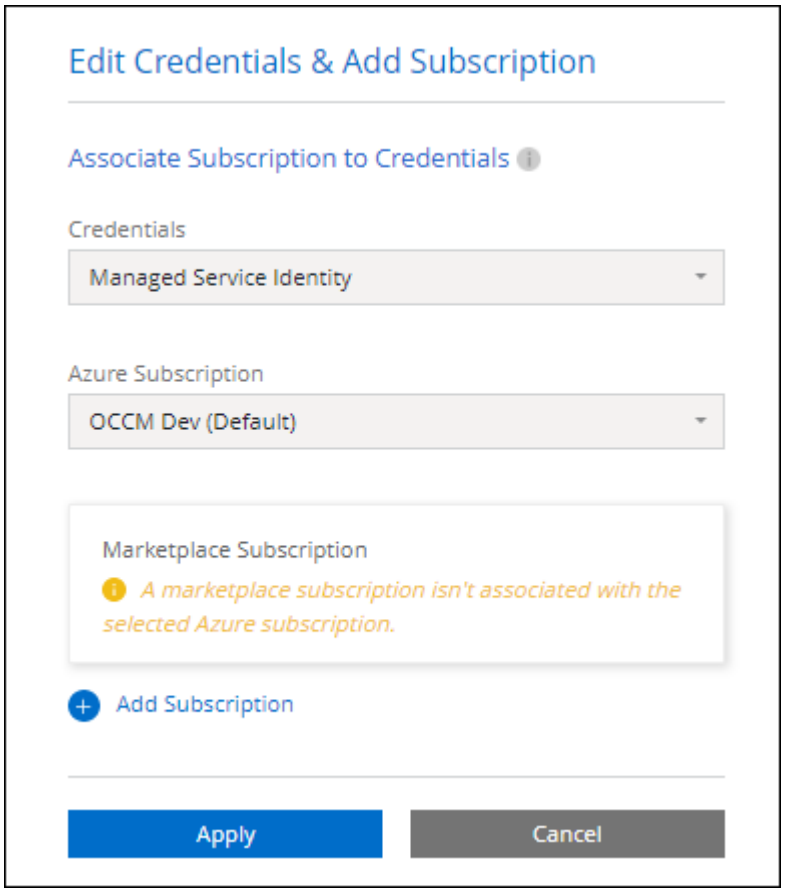
PAYGO 구독

클라우드 공급업체의 마켓플레이스에서 제공하는 혜택을 구독하여 시간당 요금을 지불하세요.

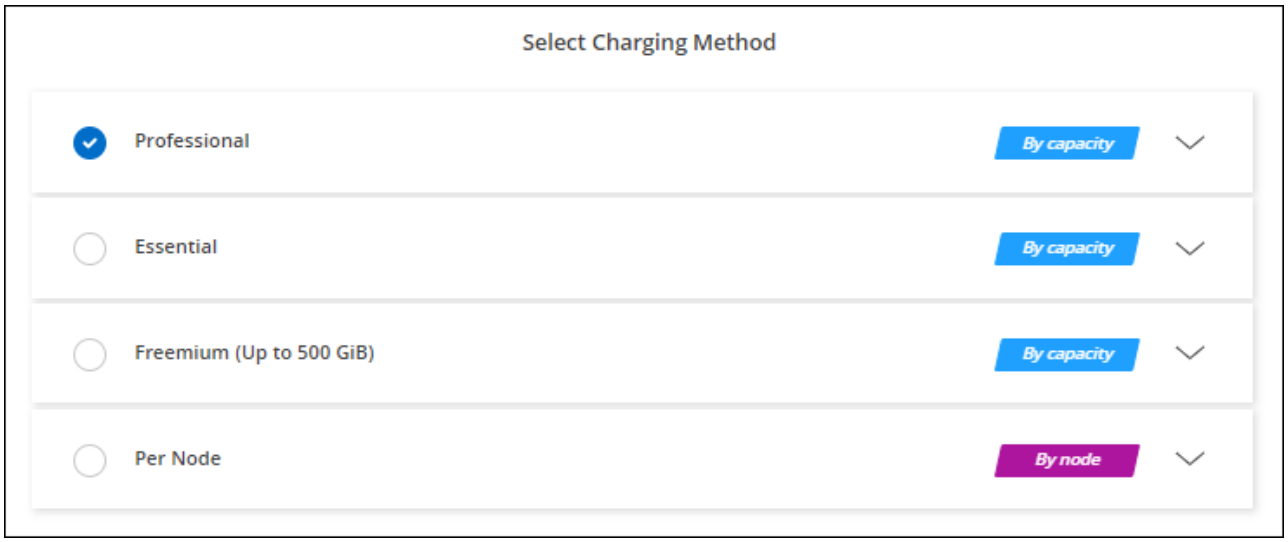
Cloud Volumes ONTAP 시스템을 만들면 콘솔에서 Azure Marketplace에서 제공되는 계약에 가입하라는 메시지가 표시됩니다. 해당 구독은 요금 청구를 위해 시스템에 연결됩니다. 동일한 구독을 추가 시스템에도 사용할 수 있습니다.

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, 화면의 지시에 따라 Azure Marketplace에서 종량제 상품을 구독하세요.



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



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

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

연간 계약

연간 계약을 구매하여 매년 Cloud Volumes ONTAP 에 대한 비용을 지불하세요.

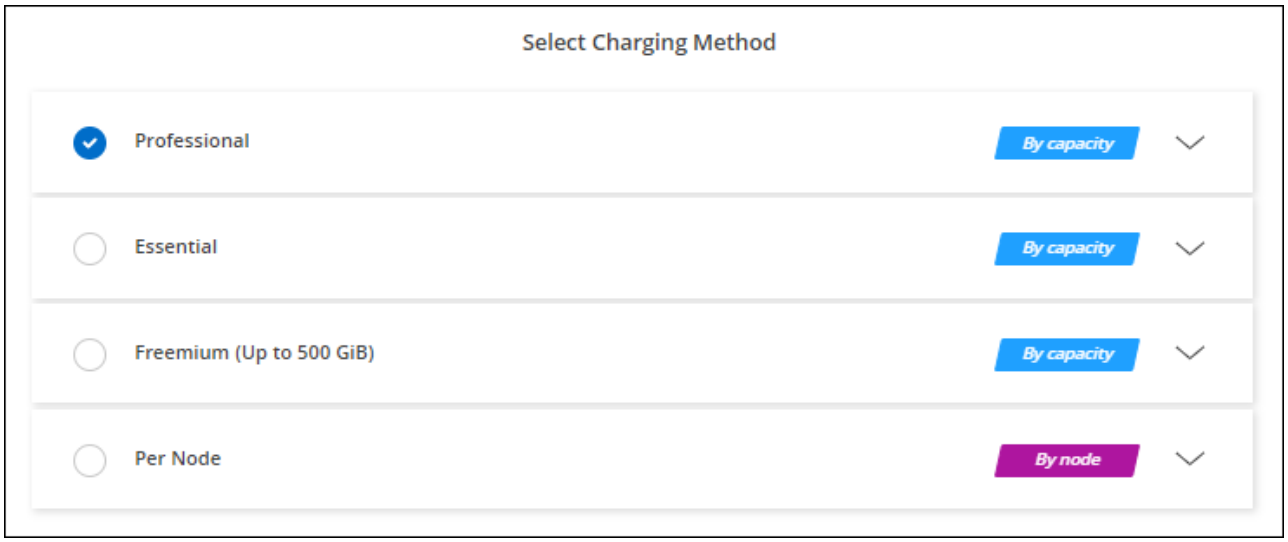
단계

1. 연간 계약을 구매하려면 NetApp 영업 담당자에게 문의하세요.

   해당 계약은 Azure Marketplace에서 비공개 제안으로 제공됩니다.

   NetApp 에서 비공개 제안을 공유한 후, 시스템을 만드는 동안 Azure Marketplace에서 구독할 때 연간 요금제를 선택할 수 있습니다.

2. 시스템 페이지에서 *시스템 추가*를 클릭하고 단계를 따르세요.
   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가 > 계속*을 클릭합니다.
   b. Azure Portal에서 Azure 계정과 공유된 연간 플랜을 선택한 다음 *구독*을 클릭합니다.
   c. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



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

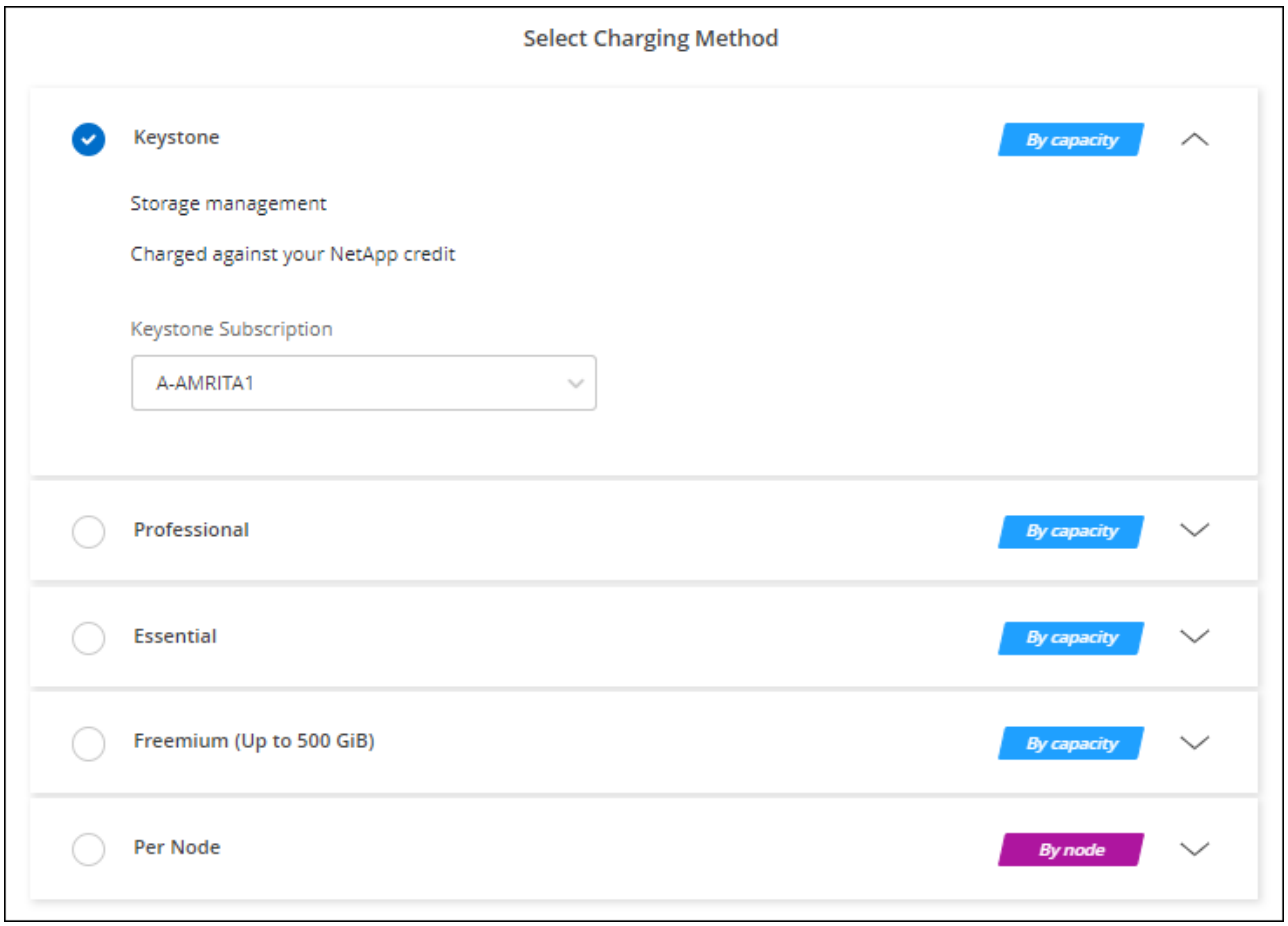
Keystone 구독

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. 콘솔에서 하나 이상의 Keystone 구독으로 사용자 계정을 인증하려면 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.



"Azure에서 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"

Azure에서 **Cloud Volumes ONTAP** 에 대해 고가용성 모드 활성화

예기치 않은 장애 조치 시간을 줄이고 Cloud Volumes ONTAP에 대한 NFSv4 지원을 활성화하려면 Microsoft Azure의 고가용성(HA) 모드를 활성화해야 합니다. 이 모드를 활성화하면 Cloud Volumes ONTAP HA 노드는 CIFS 및 NFSv4 클라이언트에 대한 예기치 않은 장애 조치 시 낮은(60초) 복구 시간 목표(RTO)를 달성할 수 있습니다.

Cloud Volumes ONTAP 9.10.1부터 Microsoft Azure에서 실행되는 Cloud Volumes ONTAP HA 쌍에 대한 계획되지 않은 장애 조치 시간을 줄이고 NFSv4에 대한 지원을 추가했습니다. 이러한 향상된 기능을 Cloud Volumes ONTAP 에

적용하려면 Azure 구독에서 고가용성 기능을 활성화해야 합니다.

이 작업에 관하여

NetApp Console은 Azure 구독에서 해당 기능을 활성화해야 할 때 다음과 같은 세부 정보를 표시합니다. 다음 사항에 유의하십시오.

- Cloud Volumes ONTAP HA 쌍의 고가용성에는 문제가 없습니다. 이 Azure 기능은 ONTAP 과 함께 작동하여 계획되지 않은 장애 조치 이벤트로 인해 NFS 프로토콜에 대한 클라이언트 관찰 애플리케이션 중단 시간을 줄입니다.
- 이 기능을 활성화해도 Cloud Volumes ONTAP HA 쌍은 중단되지 않습니다.
- Azure 구독에서 이 기능을 활성화해도 다른 VM에는 문제가 발생하지 않습니다.
- Cloud Volumes ONTAP CIFS 및 NFS 클라이언트에서 클러스터 및 SVM 관리 LIF의 장애 조치 중에 내부 Azure Load Balancer를 사용합니다.
- HA 모드가 활성화되면 콘솔은 12시간마다 시스템을 검사하여 내부 Azure Load Balancer 규칙을 업데이트합니다.

단계

소유자 권한이 있는 Azure 사용자는 Azure CLI에서 해당 기능을 활성화할 수 있습니다.

1. "Azure Portal에서 Azure Cloud Shell에 액세스"
2. 고가용성 모드 기능을 등록하세요:

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. 선택적으로 해당 기능이 등록되었는지 확인하세요.

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Azure CLI는 다음과 유사한 결과를 반환해야 합니다.

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

관련 링크

1. "Microsoft Azure 설명서: 고가용성 포트 개요"
2. "Microsoft Azure 설명서: Azure CLI 시작하기"

Azure에서 **Cloud Volumes ONTAP** 에 **VMOrchestratorZonalMultiFD** 사용

로컬 중복 스토리지(LRS) 단일 가용성 영역(AZ)에 VM 인스턴스를 배포하려면 Microsoft를 활성화해야 합니다. `Microsoft.Compute/VMOrchestratorZonalMultiFD` 귀하의 구독에 대한 기능입니다. 고가용성(HA) 모드에서 이 기능은 동일한 가용성 영역 내의 별도의 장애 도메인에 노드를 배포하는 것을 용이하게 합니다.

이 기능을 활성화하지 않으면 영역별 배포가 발생하지 않으며, 이전 LRS 비영역별 배포가 적용됩니다.

단일 가용성 영역에 VM을 배포하는 방법에 대한 자세한 내용은 다음을 참조하세요."Azure의 고가용성 쌍" .

"소유자" 권한이 있는 사용자로 다음 단계를 수행하세요.

단계

1. Azure Portal에서 Azure Cloud Shell에 액세스합니다. 자세한 내용은 다음을 참조하세요. "Microsoft Azure 설명서: Azure Cloud Shell 시작하기" .
2. 등록하세요 `Microsoft.Compute/VMOrchestratorZonalMultiFD` 다음 명령을 실행하여 기능을 추가하세요.

   az 계정 설정 -s <*Azure_subscription_name_or_ID*> az 기능 등록 --name VMOrchestratorZonalMultiFD --namespace Microsoft.Compute

3. 등록 상태와 출력 샘플을 확인하세요.

   az 기능 표시 -n VMOrchestratorZonalMultiFD --네임스페이스 Microsoft.Compute { "id": "/subscriptions/<*ID*>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestratorZonalMultiFD", "name": "Microsoft.Compute/VMOrchestratorZonalMultiFD", "properties": { "state": "등록됨" }, "type": "Microsoft.Features/providers/features" }

Azure에서 **Cloud Volumes ONTAP** 실행

NetApp Console에서 Cloud Volumes ONTAP 시스템을 생성하여 Azure에서 단일 노드 시스템 또는 HA 쌍을 시작할 수 있습니다.

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 계획해야 하며, 관리자로부터 필요한 Azure 네트워킹 세부 정보를 받아야 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" .

이 작업에 관하여

콘솔이 Azure에 Cloud Volumes ONTAP 시스템을 만들면 리소스 그룹, 네트워크 인터페이스, 스토리지 계정 등 여러 Azure 개체가 만들어집니다. 마법사가 끝나면 리소스 요약을 검토할 수 있습니다.

> 데이터 손실 가능성
>
> 가장 좋은 방법은 각 Cloud Volumes ONTAP 시스템에 대해 새로운 전용 리소스 그룹을 사용하는 것입니다.
>
> 데이터 손실 위험 때문에 기존의 공유 리소스 그룹에 Cloud Volumes ONTAP 배포하는 것은 권장되지 않습니다. 배포 실패 또는 삭제 시 콘솔에서 공유 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거할 수 있지만, Azure 사용자가 실수로 공유 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 삭제할 수도 있습니다.

Azure에서 단일 노드 **Cloud Volumes ONTAP** 시스템 실행

Azure에서 단일 노드 Cloud Volumes ONTAP 시스템을 시작하려면 Console에서 단일 노드 시스템을 생성해야 합니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 안내를 따르세요.
3. 위치 선택: *Microsoft Azure*와 * Cloud Volumes ONTAP 단일 노드*를 선택하세요.
4. 메시지가 표시되면 "콘솔 에이전트 생성" .
5. 세부 정보 및 자격 증명: 필요에 따라 Azure 자격 증명과 구독을 변경하고, 클러스터 이름을 지정하고, 필요한 경우 태그를 추가한 다음 자격 증명을 지정합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
시스템 이름	콘솔은 시스템 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Azure 가상 머신의 이름을 지정합니다. 해당 옵션을 선택하면 사전 정의된 보안 그룹의 접두사로도 이름이 사용됩니다.
리소스 그룹 태그	태그는 Azure 리소스에 대한 메타데이터입니다. 이 필드에 태그를 입력하면 콘솔이 Cloud Volumes ONTAP 시스템과 연결된 리소스 그룹에 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. "Microsoft Azure 설명서: 태그를 사용하여 Azure 리소스 구성" .

필드	설명
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 시스템에서는 다양한 Azure 자격 증명과 Azure 구독을 선택하여 사용할 수 있습니다. 사용량에 따라 지불하는 Cloud Volumes ONTAP 시스템을 배포하려면 선택한 Azure 구독과 Azure Marketplace 구독을 연결해야 합니다. "자격 증명을 추가하는 방법을 알아보세요" .

6. 서비스: Cloud Volumes ONTAP 과 함께 사용하거나 사용하지 않을 개별 서비스를 활성화하거나 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.

7. 위치: 지역, 가용성 영역, VNet 및 서브넷을 선택한 다음 확인란을 선택하여 콘솔 에이전트와 대상 위치 간의 네트워크 연결을 확인합니다.

   중국 지역의 경우 단일 노드 배포는 Cloud Volumes ONTAP 9.12.1 GA 및 9.13.0 GA에서만 지원됩니다. 이러한 버전을 Cloud Volumes ONTAP 의 최신 패치 및 릴리스로 업그레이드할 수 있습니다."Azure에서 지원됨" . 중국 지역에 이후 Cloud Volumes ONTAP 버전을 배포하려면 NetApp 지원팀에 문의하세요. 중국 지역에서는 NetApp 에서 직접 구매한 라이선스만 지원되며, 마켓플레이스 구독은 이용할 수 없습니다.

8. 연결성: 새 리소스 그룹이나 기존 리소스 그룹을 선택한 다음, 미리 정의된 보안 그룹을 사용할지 아니면 사용자 고유의 보안 그룹을 사용할지 선택합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
리소스 그룹	Cloud Volumes ONTAP 에 대한 새 리소스 그룹을 만들거나 기존 리소스 그룹을 사용하세요. 가장 좋은 방법은 Cloud Volumes ONTAP 에 대해 새로운 전용 리소스 그룹을 사용하는 것입니다. 기존의 공유 리소스 그룹에 Cloud Volumes ONTAP 배포하는 것은 가능하지만 데이터 손실 위험 때문에 권장하지는 않습니다. 자세한 내용은 위의 경고를 참조하세요. 사용 중인 Azure 계정에 다음이 있는 경우 "필요한 권한" 배포 실패 또는 삭제 시 콘솔은 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거합니다.

필드	설명
생성된 보안 그룹	콘솔에서 보안 그룹을 생성하도록 허용하는 경우 트래픽 허용 방법을 선택해야 합니다. • *선택한 VNet만*을 선택하는 경우 인바운드 트래픽의 소스는 선택한 VNet의 서브넷 범위와 콘솔 에이전트가 있는 VNet의 서브넷 범위입니다. 이것은 권장되는 옵션입니다. • *모든 VNet*을 선택하면 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
기존 사용	기존 보안 그룹을 선택하는 경우 Cloud Volumes ONTAP 요구 사항을 충족해야 합니다. "기본 보안 그룹 보기" .

9. 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" .
10. 사전 구성된 패키지: Cloud Volumes ONTAP 시스템을 빠르게 배포하려면 패키지 중 하나를 선택하거나 *내 구성 만들기*를 클릭하세요.

    패키지 중 하나를 선택하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.
11. 라이선스: 필요한 경우 Cloud Volumes ONTAP 버전을 변경하고 가상 머신 유형을 선택합니다.

    선택한 버전에 대해 최신 릴리스 후보, 일반 출시 버전 또는 패치 릴리스가 제공되는 경우 BlueXP 작업 환경을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.16.1 P3를 선택하고 9.16.1 P4를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리스에서 다른 릴리스로 전달되지 않습니다(예: 9.15에서 9.16로 전달).
12. **Azure Marketplace**에서 구독: 콘솔에서 Cloud Volumes ONTAP 의 프로그래밍 방식 배포를 활성화할 수 없는 경우 이 페이지가 표시됩니다. 화면에 나열된 단계를 따르세요. "마켓플레이스 제품의 프로그래밍 방식 배포" 자세한 내용은.
13. 기본 스토리지 리소스: 초기 집계에 대한 설정을 선택합니다. 디스크 유형, 각 디스크의 크기, Blob 스토리지에 대한 데이터 계층화를 활성화할지 여부입니다.

    다음 사항에 유의하세요.
    - VNet 내에서 스토리지 계정에 대한 공용 액세스가 비활성화된 경우 Cloud Volumes ONTAP 시스템에서 데이터 계층화를 활성화할 수 없습니다. 자세한 내용은 다음을 참조하세요."보안 그룹 규칙" .
    - 디스크 유형은 초기 볼륨을 위한 것입니다. 이후 볼륨에는 다른 디스크 유형을 선택할 수 있습니다.
    - 디스크 크기는 초기 집계의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 콘솔이 생성하는 모든 추가 집계에 적용됩니다. 고급 할당 옵션을 사용하면 다른 디스크 크기를 사용하는 집계를 만들 수 있습니다.

      디스크 유형 및 크기 선택에 대한 도움말은 다음을 참조하세요."Azure에서 시스템 크기 조정" .
    - 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
    - 데이터 계층화를 비활성화하면 이후 집계에서 활성화할 수 있습니다.

      "데이터 계층화에 대해 자세히 알아보세요" .

14. 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.

       이 옵션은 특정 VM 유형에만 사용할 수 있습니다. 지원되는 VM 유형을 알아보려면 다음을 참조하세요."HA 쌍에 대한 라이선스별 지원 구성" .

       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.

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

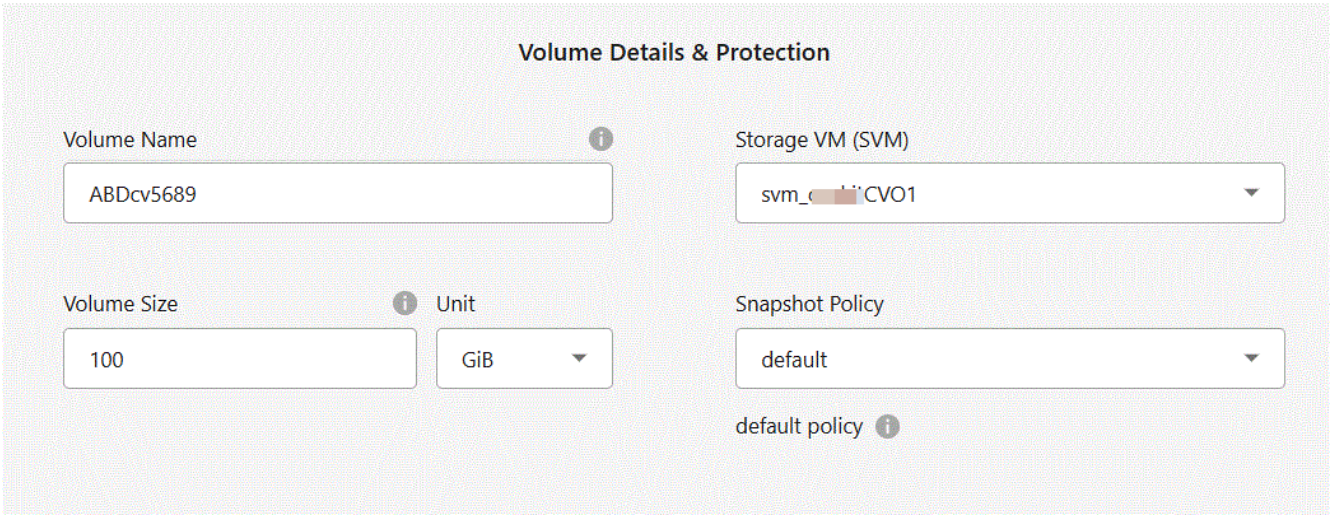
    "지원되는 클라이언트 프로토콜 및 버전에 대해 알아보세요" .

    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.

필드	설명
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.



16. **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 Azure AD Domain Services를 구성하려면 이 필드에 **OU=AADDC Computers** 또는 *OU=AADDC Users*를 입력해야 합니다.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 설명서: Azure AD Domain Services 관리 도메인에서 OU(조직 단위) 만들기"^]
DNS 도메인	Cloud Volumes ONTAP 스토리지 가상 머신(SVM)의 DNS 도메인입니다. 대부분의 경우 도메인은 AD 도메인과 동일합니다.

필드	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 참조하세요 "NetApp Console 자동화 문서" 자세한 내용은. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 만든 후에는 구성할 수 없습니다.

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

    자세한 내용은 다음을 참조하세요."볼륨 사용 프로필 이해" 그리고"데이터 계층화 개요" .

18. 검토 및 승인: 선택 사항을 검토하고 확인합니다.
    a. 구성에 대한 세부 정보를 검토하세요.
    b. *자세한 정보*를 클릭하여 콘솔에서 구매할 지원 및 Azure 리소스에 대한 세부 정보를 검토하세요.
    c. 이해합니다... 확인란을 선택하세요.
    d. *이동*을 클릭하세요.

결과

콘솔은 Cloud Volumes ONTAP 시스템을 배포합니다. 감사 페이지에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 시스템 배포 중 문제가 발생하면 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 Azure Portal에서 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.

Azure에서 Cloud Volumes ONTAP HA 쌍 시작

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

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 안내를 따르세요.
3. 메시지가 표시되면 "콘솔 에이전트 생성" .

4. 세부 정보 및 자격 증명: 필요에 따라 Azure 자격 증명과 구독을 변경하고, 클러스터 이름을 지정하고, 필요한 경우 태그를 추가한 다음 자격 증명을 지정합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
시스템 이름	콘솔은 시스템 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Azure 가상 머신의 이름을 지정합니다. 해당 옵션을 선택하면 사전 정의된 보안 그룹의 접두사로도 이름이 사용됩니다.
리소스 그룹 태그	태그는 Azure 리소스에 대한 메타데이터입니다. 이 필드에 태그를 입력하면 콘솔이 Cloud Volumes ONTAP 시스템과 연결된 리소스 그룹에 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. "Microsoft Azure 설명서: 태그를 사용하여 Azure 리소스 구성" .
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 시스템에서는 다양한 Azure 자격 증명과 Azure 구독을 선택하여 사용할 수 있습니다. 사용량에 따라 지불하는 Cloud Volumes ONTAP 시스템을 배포하려면 선택한 Azure 구독과 Azure Marketplace 구독을 연결해야 합니다. "자격 증명을 추가하는 방법을 알아보세요" .

5. 서비스: Cloud Volumes ONTAP 과 함께 사용할지 여부에 따라 개별 서비스를 활성화하거나 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.

6. **HA** 배포 모델:
   a. 단일 가용 영역 또는 *다중 가용 영역*을 선택하세요.
      - 단일 가용성 영역의 경우 Azure 지역, 가용성 영역, VNet 및 서브넷을 선택합니다.

        Cloud Volumes ONTAP 9.15.1부터 Azure의 단일 가용성 영역(AZ)에 HA 모드로 가상 머신(VM) 인스턴스를 배포할 수 있습니다. 이 배포를 지원하는 영역과 지역을 선택해야 합니다. 해당 영역이나 지역이 영역별 배포를 지원하지 않는 경우 LRS에 대한 이전 비영역별 배포 모드가 따릅니다. 공유 관리 디스크에 대해 지원되는 구성을 이해하려면 다음을 참조하세요."공유 관리 디스크를 사용한 HA 단일 가용성 영역 구성" .

      - 여러 가용성 영역의 경우 노드 1에 대한 지역, VNet, 서브넷, 영역, 노드 2에 대한 영역을 선택합니다.

   b. 네트워크 연결을 확인했습니다**...** 확인란을 선택하세요.

7. 연결성: 새 리소스 그룹이나 기존 리소스 그룹을 선택한 다음, 미리 정의된 보안 그룹을 사용할지 아니면 사용자 고유의 보안 그룹을 사용할지 선택합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
리소스 그룹	Cloud Volumes ONTAP 에 대한 새 리소스 그룹을 만들거나 기존 리소스 그룹을 사용하세요. 가장 좋은 방법은 Cloud Volumes ONTAP 에 대해 새로운 전용 리소스 그룹을 사용하는 것입니다. 기존의 공유 리소스 그룹에 Cloud Volumes ONTAP 배포하는 것은 가능하지만 데이터 손실 위험 때문에 권장하지는 않습니다. 자세한 내용은 위의 경고를 참조하세요. Azure에 배포하는 각 Cloud Volumes ONTAP HA 쌍에 대해 전용 리소스 그룹을 사용해야 합니다. 리소스 그룹에서는 HA 쌍을 하나만 지원합니다. Azure 리소스 그룹에서 두 번째 Cloud Volumes ONTAP HA 쌍을 배포하려고 하면 콘솔에서 연결 문제가 발생합니다. 사용 중인 Azure 계정에 다음이 있는 경우 "필요한 권한" 배포 실패 또는 삭제 시 콘솔은 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거합니다.
생성된 보안 그룹	콘솔에서 보안 그룹을 생성하도록 허용하는 경우 트래픽 허용 방법을 선택해야 합니다. • *선택한 VNet만*을 선택하는 경우 인바운드 트래픽의 소스는 선택한 VNet의 서브넷 범위와 콘솔 에이전트가 있는 VNet의 서브넷 범위입니다. 이것은 권장되는 옵션입니다. • *모든 VNet*을 선택하면 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.
기존 사용	기존 보안 그룹을 선택하는 경우 Cloud Volumes ONTAP 요구 사항을 충족해야 합니다. "기본 보안 그룹 보기" .

8. 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" .
9. 사전 구성된 패키지: Cloud Volumes ONTAP 시스템을 빠르게 배포하려면 패키지 중 하나를 선택하거나 *구성 변경*을 클릭하세요.

   패키지 중 하나를 선택하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.
10. 라이선스: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 가상 머신 유형을 선택합니다.

    선택한 버전에 대해 최신 릴리스 후보, 일반 공급 또는 패치 릴리스가 제공되는 경우 콘솔은 버전을 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. 예를 들어, 9.13에서 9.14로 전달되지 않습니다.
11. **Azure Marketplace**에서 구독: 콘솔에서 Cloud Volumes ONTAP 의 프로그래밍 방식 배포를 활성화할 수 없는 경우 다음 단계를 따르세요.
12. 기본 스토리지 리소스: 초기 집계에 대한 설정을 선택합니다. 디스크 유형, 각 디스크의 크기, Blob 스토리지에 대한 데이터 계층화를 활성화할지 여부입니다.

    다음 사항에 유의하세요.

- 디스크 크기는 초기 집계의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 콘솔이 생성하는 모든 추가 집계에 적용됩니다. 고급 할당 옵션을 사용하면 다른 디스크 크기를 사용하는 집계를 만들 수 있습니다.

  디스크 크기 선택에 대한 도움말은 다음을 참조하세요."Azure에서 시스템 크기 조정" .

- VNet 내에서 스토리지 계정에 대한 공용 액세스가 비활성화된 경우 Cloud Volumes ONTAP 시스템에서 데이터 계층화를 활성화할 수 없습니다. 자세한 내용은 다음을 참조하세요."보안 그룹 규칙" .
- 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
- 데이터 계층화를 비활성화하면 이후 집계에서 활성화할 수 있습니다.

  "데이터 계층화에 대해 자세히 알아보세요" .

- Cloud Volumes ONTAP 9.15.0P1부터 새로운 고가용성 쌍 배포에 대해 Azure 페이지 Blob이 더 이상 지원되지 않습니다. 현재 기존 고가용성 쌍 배포에서 Azure 페이지 Blob을 사용하는 경우 Edsv4 시리즈 VM 및 Edsv5 시리즈 VM에서 최신 VM 인스턴스 유형으로 마이그레이션할 수 있습니다.

  "Azure에서 지원되는 구성에 대해 자세히 알아보세요." .

13. 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.

       이 옵션은 특정 VM 유형에만 사용할 수 있습니다. 지원되는 VM 유형을 알아보려면 다음을 참조하세요."HA 쌍에 대한 라이선스별 지원 구성" .

       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.

14. 저장소 및 **WORM**에 대한 보안 통신: Azure 저장소 계정에 HTTPS 연결을 사용할지 여부를 선택하고, 필요한 경우 WORM(한 번 쓰고 여러 번 읽기) 저장소를 활성화합니다.

    HTTPS 연결은 Cloud Volumes ONTAP 9.7 HA 쌍에서 Azure 페이지 Blob 스토리지 계정으로 이루어집니다. 이 옵션을 활성화하면 쓰기 성능에 영향을 줄 수 있습니다. 시스템을 만든 후에는 설정을 변경할 수 없습니다.

    "WORM 스토리지에 대해 자세히 알아보세요" .

    데이터 계층화가 활성화된 경우 WORM을 활성화할 수 없습니다.

    "WORM 스토리지에 대해 자세히 알아보세요" .

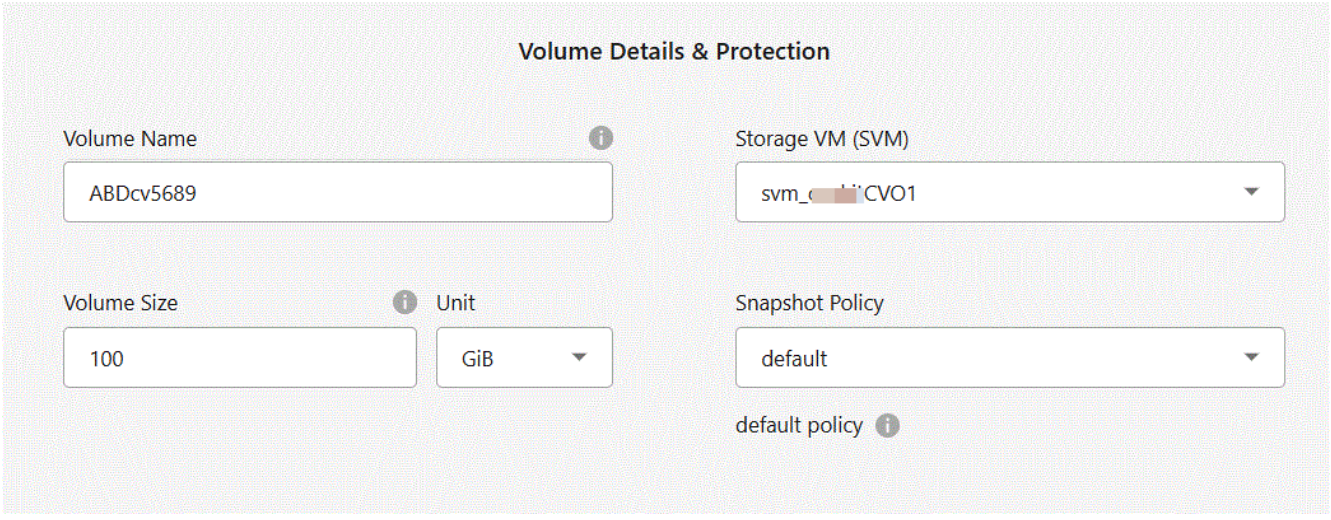
15. 볼륨 만들기: 새 볼륨에 대한 세부 정보를 입력하거나 *건너뛰기*를 클릭합니다.

    "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.



16. **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 Azure AD Domain Services를 구성하려면 이 필드에 **OU=AADDC Computers** 또는 *OU=AADDC Users*를 입력해야 합니다.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure 설명서: Azure AD Domain Services 관리 도메인에서 OU(조직 단위) 만들기"^]
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.

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

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

18. 검토 및 승인: 선택 사항을 검토하고 확인합니다.
    a. 구성에 대한 세부 정보를 검토하세요.
    b. *자세한 정보*를 클릭하여 콘솔에서 구매할 지원 및 Azure 리소스에 대한 세부 정보를 검토하세요.
    c. 이해합니다... 확인란을 선택하세요.
    d. *이동*을 클릭하세요.

결과

콘솔은 Cloud Volumes ONTAP 시스템을 배포합니다. 감사 페이지에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 시스템 배포 중 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 Azure Portal에서 시스템 생성 Cloud Volumes ONTAP 구성, 특히 시스템 태그를 수정하지 마세요. 이러한 구성을 변경하면 예기치 않은 동작이나 데이터 손실이 발생할 수 있습니다.

관련 링크

*"Azure에서 Cloud Volumes ONTAP 구성 계획" *"Azure Marketplace에서 Azure에 Cloud Volumes ONTAP 배포"

Azure 플랫폼 이미지 확인

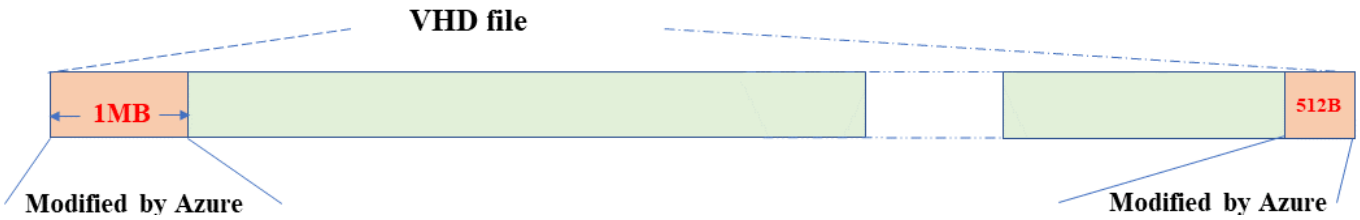
Cloud Volumes ONTAP 에 대한 Azure 마켓플레이스 이미지 검증

Azure 이미지 검증은 향상된 NetApp 보안 요구 사항을 준수합니다. 이미지 파일을 검증하는 것은 간단한 과정입니다. 그러나 Azure 이미지 서명 검증에는 Azure VHD 이미지 파일에 대한 특정 고려 사항이 필요합니다. Azure VHD 이미지 파일은 Azure Marketplace에서 변경되기 때문입니다.

> Azure 이미지 검증은 Cloud Volumes ONTAP 9.15.0 이상에서 지원됩니다.

Azure에서 게시된 VHD 파일 변경

VHD 파일의 시작 부분인 1MB(1048576바이트)와 끝 부분인 512바이트는 Azure에 의해 수정됩니다. NetApp 나머지 VHD 파일에 서명합니다.



이 예에서 VHD 파일의 크기는 10GB입니다. NetApp 에서 서명한 부분은 녹색으로 표시되어 있습니다(10GB - 1MB - 512바이트).

관련 링크

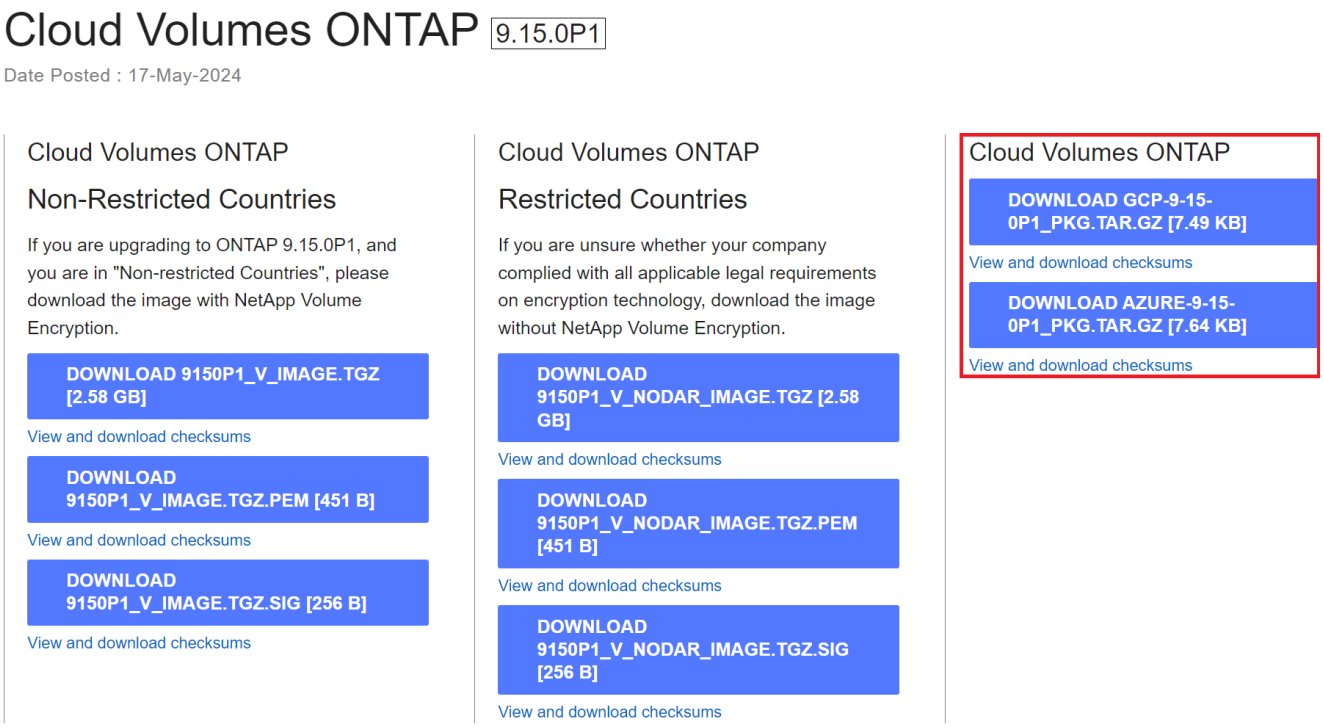
- "페이지 폴트 블로그: OpenSSL을 사용하여 서명하고 확인하는 방법"
- "Azure Marketplace 이미지를 사용하여 Azure Stack Edge Pro GPU용 VM 이미지 만들기 | Microsoft Learn"
- "Azure CLI를 사용하여 관리 디스크를 저장소 계정으로 내보내기/복사 | Microsoft Learn"
- "Azure Cloud Shell 빠른 시작 - Bash | Microsoft Learn"
- "Azure CLI 설치 방법 | Microsoft Learn"
- "az 스토리지 BLOB 복사 | Microsoft Learn"
- "Azure CLI로 Sign in - 로그인 및 인증 | Microsoft Learn"

Azure 이미지 파일은 다음에서 다운로드할 수 있습니다. "NetApp 지원 사이트" .

tar.gz 파일에는 이미지 서명 검증에 필요한 파일이 포함되어 있습니다. *tar.gz* 파일과 함께 이미지에 대한 *checksum* 파일도 다운로드해야 합니다. 체크섬 파일에는 다음이 포함됩니다. `md5` 그리고 `sha256` *tar.gz* 파일의 체크섬.

단계

1. 로 가다 "NetApp 지원 사이트의 Cloud Volumes ONTAP 제품 페이지" 다운로드 섹션에서 필요한 소프트웨어 버전을 다운로드하세요.
2. Cloud Volumes ONTAP 다운로드 페이지에서 Azure 이미지에 대한 다운로드 가능한 파일을 클릭하고 *tar.gz* 파일을 다운로드합니다.



3. Linux에서 실행 `md5sum AZURE-<version>_PKG.TAR.GZ` .

   macOS에서는 다음을 실행합니다. `sha256sum AZURE-<version>_PKG.TAR.GZ` .

4. 다음을 확인하십시오. `md5sum` 그리고 `sha256sum` 값이 다운로드한 Azure 이미지의 값과 일치합니다.
5. Linux 및 macOS에서는 다음을 사용하여 *tar.gz* 파일을 추출합니다. `tar -xzf` 명령.

   추출된 *tar.gz* 파일에는 다이제스트(*.sig*) 파일, 공개 키 인증서(*.pem*) 파일, 체인 인증서(*.pem*) 파일이 포함되어 있습니다.

   tar.gz 파일을 추출한 후의 출력 예**:**

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

Azure Marketplace에서 Cloud Volumes ONTAP 용 VHD 이미지 내보내기

VHD 이미지가 Azure 클라우드에 게시되면 더 이상 NetApp 에서 관리되지 않습니다. 대신, 게시된 이미지는 Azure Marketplace에 배치됩니다. 이미지가 Azure 마켓플레이스에 스테이징되어 게시되면 Azure는 VHD의 시작 부분에서 1MB, 끝 부분에서 512바이트를 수정합니다. VHD 파일의 서명을 확인하려면 Azure 마켓플레이스에서 Azure가 수정한 VHD 이미지를 내보내야 합니다.

시작하기 전에

시스템에 Azure CLI가 설치되어 있는지, 아니면 Azure Portal을 통해 Azure Cloud Shell을 사용할 수 있는지 확인하세요. Azure CLI를 설치하는 방법에 대한 자세한 내용은 다음을 참조하세요. "Microsoft 설명서: Azure CLI 설치 방법" .

단계

1. *version_readme* 파일의 내용을 사용하여 시스템의 Cloud Volumes ONTAP 버전을 Azure Marketplace 이미지 버전에 매핑합니다. Cloud Volumes ONTAP 버전은 다음과 같이 표현됩니다. `buildname` Azure Marketplace 이미지 버전은 다음과 같이 표현됩니다. `version` 버전 매핑에서.

   다음 예에서는 Cloud Volumes ONTAP 버전 `9.15.0P1` Azure Marketplace 이미지 버전에 매핑됨 `9150.01000024.05090105` . 이 Azure 마켓플레이스 이미지 버전은 나중에 이미지 URN을 설정하는 데 사용됩니다.

   ```
   [
    "buildname": "9.15.0P1",
       "publisher": "netapp",
        "version": "9150.01000024.05090105"

   ]
   ```

2. VM을 만들려는 지역을 식별합니다. 지역 이름은 값으로 사용됩니다. `locName` 마켓플레이스 이미지의 URN을 설정할 때 변수입니다. 사용 가능한 지역을 나열하려면 다음 명령을 실행하세요.

   ```
   az account list-locations -o table
   ```

   이 표에서는 지역 이름이 다음과 같이 나타납니다. `Name` 필드.

```
$ az account list-locations -o table
DisplayName               Name                 RegionalDisplayName
------------------------  -------------------
-------------------------------------
East US                   eastus               (US) East US
East US 2                 eastus2              (US) East US 2
South Central US          southcentralus       (US) South Central US
...
```

3. 아래 표에서 해당 Cloud Volumes ONTAP 버전과 VM 배포 유형에 대한 SKU 이름을 검토하세요. SKU 이름은 값으로 사용됩니다. `skuName` 마켓플레이스 이미지의 URN을 설정할 때 변수입니다.

   예를 들어, Cloud Volumes ONTAP 9.15.0을 사용한 모든 단일 노드 배포는 다음을 사용해야 합니다. `ontap_cloud_byol` SKU 이름으로.

* Cloud Volumes ONTAP 버전*	**VM** 배포를 통해	**SKU** 이름
9.17.1 이상	Azure 마켓플레이스	ontap_cloud_direct_gen2
9.17.1 이상	NetApp Console	ontap_cloud_gen2
9.16.1	Azure 마켓플레이스	온탭_클라우드_다이렉트
9.16.1	콘솔	온탭_클라우드
9.15.1	콘솔	온탭_클라우드
9.15.0	콘솔, 단일 노드 배포	온탭_클라우드_바이올
9.15.0	콘솔, 고가용성(HA) 배포	온탑_클라우드_비올_하

4. ONTAP 버전과 Azure 마켓플레이스 이미지를 매핑한 후 Azure Cloud Shell 또는 Azure CLI를 사용하여 Azure 마켓플레이스에서 VHD 파일을 내보냅니다.

Linux에서 **Azure Cloud Shell**을 사용하여 **VHD** 파일 내보내기

Azure Cloud Shell에서 마켓플레이스 이미지를 VHD 파일(예: *9150.01000024.05090105.vhd*)로 내보내고 로컬 Linux 시스템에 다운로드합니다. Azure Marketplace에서 VHD 이미지를 가져오려면 다음 단계를 수행하세요.

단계

1. 마켓플레이스 이미지의 URN 및 기타 매개변수를 설정합니다. URN 형식은 다음과 같습니다. `<publisher>:<offer>:<sku>:<version>` . 선택적으로 NetApp 마켓플레이스 이미지를 나열하여 올바른 이미지 버전을 확인할 수 있습니다.

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. 일치하는 이미지 버전으로 마켓플레이스 이미지에서 새 관리 디스크를 만듭니다.

```
PS /home/user1> $diskName = “9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = “fnf1”
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
```

3. 관리 디스크에서 Azure Storage로 VHD 파일을 내보냅니다. 적절한 액세스 수준으로 컨테이너를 만듭니다. 이 예에서 우리는 다음과 같은 이름의 컨테이너를 사용했습니다. `vm-images` ~와 함께 `Container` 접근 수준. Azure Portal에서 저장소 계정 액세스 키를 가져옵니다. 저장소 계정 **> *examplesaname* >** 액세스 키 **> *key1* > *key* >** 표시 **> <복사>**

```
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container $containerName
–Context $destContext -Blob $destBlobName
```

4. 생성된 이미지를 Linux 시스템에 다운로드합니다. 사용하다 `wget` VHD 파일을 다운로드하는 명령:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

URL은 표준 형식을 따릅니다. 자동화를 위해 아래와 같이 URL 문자열을 파생시킬 수 있습니다. 또는 Azure CLI를 사용할 수 있습니다. `az` URL을 가져오는 명령입니다. URL 예시:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. 관리되는 디스크 정리

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Linux에서 **Azure CLI**를 사용하여 **VHD** 파일 내보내기

로컬 Linux 시스템에서 Azure CLI를 사용하여 마켓플레이스 이미지를 VHD 파일로 내보냅니다.

단계

1. Azure CLI에 로그인하고 마켓플레이스 이미지를 나열합니다.

```
% az login --use-device-code
```

2. 로그인하려면 웹 브라우저를 사용하여 페이지를 엽니다. https://microsoft.com/devicelogin 인증코드를 입력하세요.

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...
```

3. 마켓플레이스 이미지에서 일치하는 이미지 버전으로 새로운 관리 디스크를 만듭니다.

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
```

프로세스를 자동화하려면 표준 출력에서 SAS를 추출해야 합니다. 자세한 내용은 해당 문서를 참조하세요.

4. 관리 디스크에서 VHD 파일을 내보냅니다.

   a. 적절한 액세스 수준으로 컨테이너를 만듭니다. 이 예에서는 컨테이너라는 이름이 있습니다. `vm-images` ~와 함께 `Container` 접근 수준이 사용됩니다.

   b. Azure Portal에서 저장소 계정 액세스 키를 가져옵니다. 저장소 계정 **> *examplesaname* >** 액세스 키 **> *key1* > *key* >** 표시 **> <복사>**

      또한 다음을 사용할 수도 있습니다. `az` 이 단계에 대한 명령입니다.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
-container $containerName --account-name $storageAccountName --account
-key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Blob 복사본의 상태를 확인하세요.

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. 생성된 이미지를 Linux 서버로 다운로드합니다.

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

URL은 표준 형식을 따릅니다. 자동화를 위해 아래와 같이 URL 문자열을 파생시킬 수 있습니다. 또는 Azure CLI를 사용할 수 있습니다. `az` URL을 가져오는 명령입니다. URL 예시:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. 관리되는 디스크 정리

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

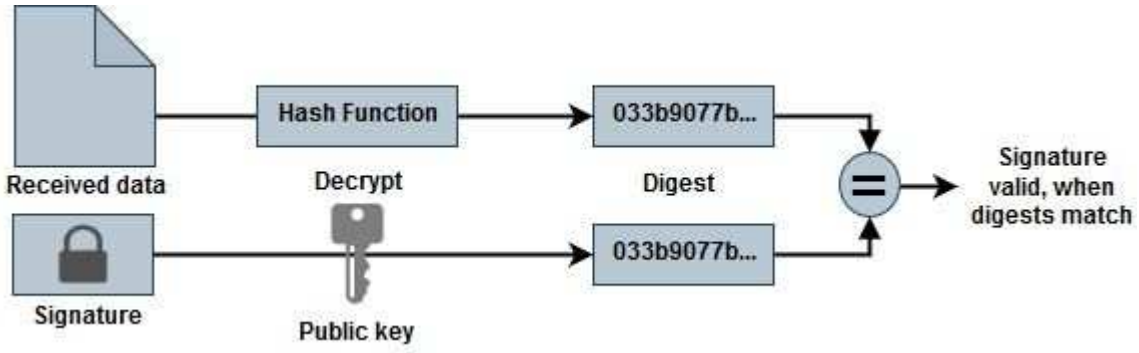
파일 서명 확인

Cloud Volumes ONTAP 에 대한 **Azure** 마켓플레이스 이미지 서명 확인

Azure 이미지 검증 프로세스는 VHD 파일의 시작 부분에서 1MB, 끝 부분에서 512바이트를 제거한 다음 해시 함수를 적용하여 다이제스트 파일을 생성합니다. 서명 절차를 일치시키기 위해 해싱에는 _sha256_이 사용됩니다.

파일 서명 검증 워크플로 요약

다음은 파일 서명 검증 워크플로 프로세스에 대한 개요입니다.



- Azure 이미지를 다운로드합니다. "NetApp 지원 사이트" 그리고 다이제스트(.sig) 파일, 공개 키 인증서(.pem) 파일, 체인 인증서(.pem) 파일을 추출합니다. . "Azure 이미지 다이제스트 파일 다운로드" 자세한 내용은.
- 신뢰 사슬의 검증.
- 공개 키 인증서(.pem)에서 공개 키(.pub)를 추출합니다.
- 추출된 공개 키를 사용하여 다이제스트 파일을 해독합니다.
- 이미지 파일에서 시작 부분 1MB와 끝 부분 512바이트를 제거한 후 생성된 임시 파일의 새로 생성된 다이제스트와 결과를 비교합니다. 이 단계는 OpenSSL 명령줄 도구를 사용하여 수행됩니다. OpenSSL CLI 도구는 파일 일치에 성공하거나 실패할 경우 적절한 메시지를 표시합니다.

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

Linux에서 **Cloud Volumes ONTAP** 에 대한 **Azure** 마켓플레이스 이미지 서명 확인

Linux에서 내보낸 VHD 파일 서명을 검증하는 작업에는 신뢰 체인 검증, 파일 편집, 서명 검증이 포함됩니다.

단계

1. Azure 이미지 파일을 다운로드하세요. "NetApp 지원 사이트" 그리고 다이제스트(.sig) 파일, 공개 키 인증서(.pem) 파일, 체인 인증서(.pem) 파일을 추출합니다.

   참조하다 "Azure 이미지 다이제스트 파일 다운로드" 자세한 내용은.

2. 신뢰 사슬을 확인하세요.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. VHD 파일의 시작 부분에서 1MB(1,048,576바이트)를 제거하고 끝 부분에서 512바이트를 제거합니다. 사용시 `tail` , 그 `-c +K` 이 옵션은 파일의 K번째 바이트에서 바이트를 생성합니다. 따라서 1048577을 전달합니다. `tail -c` .

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. OpenSSL을 사용하여 인증서에서 공개 키를 추출하고, 스트립된 파일(sign.tmp)을 서명 파일과 공개 키로 검증합니다.

   명령 프롬프트는 검증 결과에 따라 성공 또는 실패를 나타내는 메시지를 표시합니다.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 작업 공간을 정리하세요.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

macOS에서 **Cloud Volumes ONTAP** 대한 **Azure** 마켓플레이스 이미지 서명 확인

Linux에서 내보낸 VHD 파일 서명을 검증하는 작업에는 신뢰 체인 검증, 파일 편집, 서명 검증이 포함됩니다.

단계

1. Azure 이미지 파일을 다운로드하세요. "NetApp 지원 사이트" 그리고 다이제스트(.sig) 파일, 공개 키 인증서(.pem) 파일, 체인 인증서(.pem) 파일을 추출합니다.

   참조하다 "Azure 이미지 다이제스트 파일 다운로드" 자세한 내용은.

2. 신뢰 사슬을 확인하세요.

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. VHD 파일의 시작 부분에서 1MB(1,048,576바이트)를 제거하고 끝 부분에서 512바이트를 제거합니다. 사용시 `tail` , 그 `-c +K` 이 옵션은 파일의 K번째 바이트에서 바이트를 생성합니다. 따라서 1048577을 전달합니다. `tail -c` . macOS에서는 tail 명령을 완료하는 데 약 10분이 걸릴 수 있습니다.

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. OpenSSL을 사용하여 인증서에서 공개 키를 추출하고, 스트립된 파일(sign.tmp)을 서명 파일과 공개 키로 검증합니다. 명령 프롬프트는 검증 결과에 따라 성공 또는 실패를 나타내는 메시지를 표시합니다.

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 작업 공간을 정리하세요.

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Azure Marketplace에서 Cloud Volumes ONTAP 배포

Azure Marketplace 직접 배포를 사용하면 Cloud Volumes ONTAP 빠르고 쉽게 배포할 수 있습니다. Azure 마켓플레이스에서 몇 번의 클릭만으로 Cloud Volumes ONTAP 빠르게 배포하고 사용자 환경에서 핵심 기능과 성능을 살펴볼 수 있습니다.

이 제안에 대한 자세한 내용은 다음을 참조하세요."NetApp Console 과 마켓플레이스에서 Cloud Volumes ONTAP 제품에 대해 알아보세요." .

이 작업에 관하여

Azure Marketplace 직접 배포를 사용하여 배포된 Cloud Volumes ONTAP 시스템은 다음과 같은 속성을 갖습니다. Azure 마켓플레이스를 통해 배포된 독립 실행형 인스턴스의 기능은 NetApp Console 에서 검색될 때 변경됩니다.

- 최신 Cloud Volumes ONTAP 버전(9.16.1 이상).
- 프로비저닝 용량이 500GiB로 제한된 Cloud Volumes ONTAP 의 무료 라이선스입니다. 이 라이선스에는 NetApp 지원이 포함되지 않으며 만료 날짜도 없습니다.
- 단일 가용성 영역(AZ)에서 고가용성(HA) 모드로 구성된 두 개의 노드는 기본 일련 번호로 제공됩니다. 스토리지 가상 머신(스토리지 VM)은 다음에 배포됩니다."유연한 오케스트레이션 모드" .
- 기본적으로 생성된 인스턴스에 대한 집계입니다.
- 500GiB 프로비저닝 용량의 프리미엄 SSD v2 관리 디스크와 루트 디스크, 데이터 디스크.
- NFS, CIFS, iSCSI 및 NVMe/TCP 데이터 서비스를 갖춘 하나의 데이터 저장 VM이 배포되었습니다. 추가 데이터 저장소 VM을 추가할 수 없습니다.
- NFS, CIFS(SMB), iSCSI, Autonomous Ransomware Protection(ARP), SnapLock 및 SnapMirror 대한 라이센스가 설치되었습니다.
- "ONTAP 온도 민감 저장 효율성(TSSE)", 볼륨 암호화 및 외부 키 관리가 기본적으로 활성화되어 있습니다.
- 다음 기능은 지원되지 않습니다.

- FabricPool 계층화
- 스토리지 VM 유형 변경
- 빠른 쓰기 모드

시작하기 전에

- 유효한 Azure Marketplace 구독이 있는지 확인하세요.
- 네트워킹 요구 사항을 충족하는지 확인하세요."단일 AZ에 HA 배포" Azure에서. "Cloud Volumes ONTAP 에 대한 Azure 네트워킹 설정" .
- Cloud Volumes ONTAP 배포하려면 다음 Azure 역할 중 하나가 할당되어야 합니다.
  - 그만큼 `contributor` 기본 권한이 있는 역할입니다. 자세한 내용은 다음을 참조하세요. "Microsoft Azure 설명서: Azure 기본 제공 역할" .
  - 다음 권한이 있는 사용자 지정 RBAC 역할입니다. 자세한 내용은 다음을 참조하세요. "Azure 설명서: Azure 사용자 지정 역할" .

```
"사용 권한": [ { "작업": [ "Microsoft.AAD/등록/작업", "Microsoft.Resources/구독/리소스그룹/쓰기",
"Microsoft.Network/로드밸런서/쓰기", "Microsoft.ClassicCompute/virtualMachines/쓰기",
"Microsoft.Compute/capacityReservationGroups/배포/작업",
"Microsoft.ClassicCompute/virtualMachines/네트워크인터페이스/연관된네트워크보안그룹/쓰기",
"Microsoft.Network/네트워크인터페이스/쓰기", "Microsoft.Compute/virtualMachines/쓰기",
"Microsoft.Compute/virtualMachines/확장/쓰기", "Microsoft.Resources/배포/검증/작업",
"Microsoft.Resources/구독/리소스그룹/읽기", "Microsoft.Network/virtualNetworks/쓰기",
"Microsoft.Network/virtualNetworks/read", "Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Compute/disks/write",
"Microsoft.Compute/virtualMachineScaleSets/write", "Microsoft.Resources/deployments/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/subnets/write" ], "notActions": [], "dataActions": [],
"notDataActions": [] } ]
```

> 구독에 리소스 공급자 "Microsoft.storage"를 등록한 경우에는 필요하지 않습니다. `Microsoft.AAD/register/action` 허가. 자세한 내용은 다음을 참조하세요. "Azure 설명서: 저장소에 대한 Azure 권한" .

단계

1. Azure Marketplace 사이트에서 NetApp 제품을 검색합니다.
2. * NetApp Cloud Volumes ONTAP 직접*을 선택하세요.
3. *만들기*를 클릭하여 배포 마법사를 시작합니다.
4. 플랜을 선택하세요. 계획 목록에는 일반적으로 Cloud Volumes ONTAP 의 최신 릴리스가 표시됩니다.
5. 기본 탭에서 다음 세부 정보를 제공합니다.
   - 구독: 구독을 선택하세요. 배포는 구독 번호에 연결됩니다.
   - 리소스 그룹: 기존 리소스 그룹을 사용하거나 새 리소스 그룹을 만듭니다. 리소스 그룹은 Cloud Volumes ONTAP 시스템의 단일 그룹 내에서 디스크 및 스토리지 VM과 같은 모든 리소스를 할당하는 데 도움이 됩니다.
   - 지역: 단일 AZ에서 Azure HA 배포를 지원하는 지역을 선택하세요. 목록에서는 사용 가능한 지역만 볼 수 있습니다.

- 크기: 지원되는 Premium SSD v2 관리 디스크에 대한 스토리지 VM 크기를 선택하세요.
- 지역: 선택한 지역의 지역을 선택하세요.
- 관리자 비밀번호: 비밀번호를 설정하세요. 배포 후 이 관리자 비밀번호를 사용하여 시스템에 로그인합니다.
- 비밀번호 확인: 확인을 위해 동일한 비밀번호를 다시 입력하세요.
  - 네트워크 탭에서 가상 네트워크와 서브넷을 추가하거나 목록에서 선택합니다.

    Microsoft Azure 제한 사항을 준수하려면 새 가상 네트워크를 설정할 때 새 서브넷을 만들어야 합니다. 마찬가지로, 기존 네트워크를 선택하는 경우 기존 서브넷을 선택해야 합니다.

  - 미리 정의된 네트워크 보안 그룹을 선택하려면 *예*를 선택하세요. 미리 정의된 Azure 네트워크 보안 그룹에 필요한 트래픽 규칙을 할당하려면 *아니요*를 선택합니다. 자세한 내용은 다음을 참조하세요. "Azure에 대한 보안 그룹 규칙" .
  - 고급 탭에서 이 배포에 필요한 두 가지 Azure 기능이 설정되었는지 확인합니다. 참조하다"Cloud Volumes ONTAP 단일 AZ 배포를 위한 Azure 기능 활성화" 그리고"Azure에서 Cloud Volumes ONTAP 에 대해 고가용성 모드 활성화" .
  - 태그 탭에서 리소스 또는 리소스 그룹에 대한 이름과 값 쌍을 정의할 수 있습니다.
  - 검토 + 생성 탭에서 세부 정보를 검토하고 배포를 시작합니다.

당신이 완료한 후

배포 진행 상황을 보려면 알림 아이콘을 선택하세요. Cloud Volumes ONTAP 이 배포되면 작업을 위해 나열된 스토리지 VM을 볼 수 있습니다.

접근이 가능해지면 ONTAP System Manager나 ONTAP CLI를 사용하여 설정한 관리자 자격 증명으로 스토리지 VM에 로그인합니다. 그 후에는 볼륨, LUN 또는 공유를 생성하고 Cloud Volumes ONTAP 의 스토리지 기능을 활용할 수 있습니다.

배포 문제 해결

Azure 마켓플레이스를 통해 직접 배포된 Cloud Volumes ONTAP 시스템에는 NetApp 의 지원이 포함되지 않습니다. 배포 중에 문제가 발생하면 독립적으로 문제를 해결하고 해결할 수 있습니다.

단계

1. Azure Marketplace 사이트에서 *부팅 진단 > 직렬 로그*로 이동합니다.
2. 직렬 로그를 다운로드하고 조사하세요.
3. 문제 해결을 위해서는 제품 설명서와 지식 기반(KB) 문서를 참조하세요.
   - "Azure 마켓플레이스 문서"
   - "NetApp 문서"
   - "NetApp KB 문서"

콘솔에서 배포된 시스템을 찾아보세요

Azure Marketplace 직접 배포를 사용하여 배포한 Cloud Volumes ONTAP 시스템을 검색하고 콘솔의 시스템 페이지에서 관리할 수 있습니다. 콘솔 에이전트는 시스템을 검색하고, 시스템을 추가하고, 필요한 라이선스를 적용하고, 이러한 시스템에 대해 콘솔의 모든 기능을 잠금 해제합니다. PSSD v2 관리형 디스크가 있는 단일 AZ의 원래 HA

구성은 유지되며, 시스템은 원래 배포와 동일한 Azure 구독 및 리소스 그룹에 등록됩니다.

이 작업에 관하여

Azure Marketplace 직접 배포를 사용하여 배포된 Cloud Volumes ONTAP 시스템을 검색하면 콘솔 에이전트는 다음 작업을 수행합니다.

- 발견된 시스템의 무료 라이센스를 일반적인 용량 기반으로 대체합니다."프리미엄 라이선스" .
- 배포된 시스템의 기존 기능을 유지하고, 데이터 보호, 데이터 관리, 보안 기능 등 콘솔의 추가 기능을 추가합니다.
- 노드에 설치된 라이선스를 NFS, CIFS(SMB), iSCSI, ARP, SnapLock 및 SnapMirror 에 대한 새로운 ONTAP 라이선스로 교체합니다.
- 일반 노드 일련 번호를 고유한 일련 번호로 변환합니다.
- 필요에 따라 리소스에 새로운 시스템 태그를 할당합니다.
- 인스턴스의 동적 IP 주소를 정적 IP 주소로 변환합니다.
- 기능을 활성화합니다"FabricPool 계층화" ,"AutoSupport" , 그리고"한 번 쓰고 여러 번 읽기" 배포된 시스템에 (WORM) 저장소를 설치합니다. 필요할 때 콘솔에서 이러한 기능을 활성화할 수 있습니다.
- 인스턴스를 검색하는 데 사용된 NSS 계정에 인스턴스를 등록합니다.
- 용량 관리 기능을 활성화합니다."자동 및 수동 모드" 발견된 시스템에 대해서.

시작하기 전에

Azure Marketplace에서 배포가 완료되었는지 확인하세요. 콘솔 에이전트는 배포가 완료되고 검색이 가능한 경우에만 시스템을 검색할 수 있습니다.

단계

콘솔에서는 기존 시스템을 검색하기 위한 표준 절차를 따릅니다. "콘솔에 기존 Cloud Volumes ONTAP 시스템 추가" .

검색하는 동안 실패 메시지가 표시될 수 있지만 검색 프로세스가 완료될 때까지 무시할 수 있습니다. 검색 중에는 Azure Marketplace 포털에서 시스템 생성 Cloud Volumes ONTAP 구성, 특히 시스템 태그를 수정하지 마세요. 이러한 구성을 변경하면 예상치 못한 시스템 동작이 발생할 수 있습니다.

당신이 완료한 후

검색이 완료되면 콘솔의 시스템 페이지에 나열된 시스템을 볼 수 있습니다. 다음과 같은 다양한 관리 작업을 수행할 수 있습니다."집계 확장" ,"볼륨 추가" ,"추가 스토리지 VM 프로비저닝" , 그리고"인스턴스 유형 변경" .

관련 링크

저장소 생성에 대한 자세한 내용은 ONTAP 설명서를 참조하세요.

- "NFS용 볼륨 생성"
- "iSCSI에 대한 LUN 생성"
- "CIFS에 대한 공유 생성"

Google Cloud에서 시작하기

Google Cloud에서 Cloud Volumes ONTAP 빠르게 시작하세요

몇 단계만 거치면 Google Cloud에서 Cloud Volumes ONTAP 시작할 수 있습니다.

1 콘솔 에이전트 만들기

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

인터넷 접속이 불가능한 서브넷에 Cloud Volumes ONTAP 배포하려면 콘솔 에이전트를 수동으로 설치하고 해당 콘솔 에이전트에서 실행 중인 NetApp Console 에 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.

"구성 계획에 대해 자세히 알아보세요" .

3 네트워킹을 설정하세요

1. VPC와 서브넷이 콘솔 에이전트와 Cloud Volumes ONTAP 간의 연결을 지원하는지 확인하세요.
2. 데이터 계층화를 활성화하려는 경우 "Private Google Access를 위해 Cloud Volumes ONTAP 서브넷을 구성합니다." .
3. HA 쌍을 배포하는 경우 각각 자체 서브넷이 있는 4개의 VPC가 있는지 확인하세요.
4. 공유 VPC를 사용하는 경우 콘솔 에이전트 서비스 계정에 *Compute Network User* 역할을 제공합니다.
5. NetApp AutoSupport 에 대해 대상 VPC에서 아웃바운드 인터넷 액세스를 활성화합니다.

   인터넷 접속이 불가능한 위치에 Cloud Volumes ONTAP 배포하는 경우 이 단계는 필요하지 않습니다.

"네트워킹 요구 사항에 대해 자세히 알아보세요" .

4 서비스 계정 설정

Cloud Volumes ONTAP 두 가지 목적으로 Google Cloud 서비스 계정이 필요합니다. 첫 번째는 활성화할 때입니다. "데이터 계층화" Google Cloud의 저렴한 객체 스토리지에 콜드 데이터를 계층화합니다. 두 번째는 다음을 활성화할 때입니다. "NetApp Backup and Recovery" 저렴한 개체 스토리지에 볼륨을 백업합니다.

하나의 서비스 계정을 설정하여 두 가지 목적으로 모두 사용할 수 있습니다. 서비스 계정에는 저장소 관리자 역할이 있어야 합니다.

"단계별 지침을 읽어보세요" .

5 Google Cloud API 활성화

"프로젝트에서 다음 Google Cloud API를 활성화하세요." . 이러한 API는 Console 에이전트와 Cloud Volumes ONTAP 배포하는 데 필요합니다.

- 클라우드 배포 관리자 V2 API
- 클라우드 로깅 API
- 클라우드 리소스 관리자 API
- 컴퓨트 엔진 API
- ID 및 액세스 관리(IAM) API

6 콘솔을 사용하여 **Cloud Volumes ONTAP** 실행

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

관련 링크

- "콘솔 에이전트 생성"
- "Linux 호스트에 콘솔 에이전트 소프트웨어 설치"
- "콘솔 에이전트에 대한 Google Cloud 권한"

Google Cloud에서 Cloud Volumes ONTAP 구성을 계획하세요.

Google Cloud에 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 Google Cloud 지역에서 지원됩니다. "지원되는 지역의 전체 목록 보기" .

지원되는 머신 유형을 선택하세요

Cloud Volumes ONTAP 선택한 라이선스 유형에 따라 여러 가지 머신 유형을 지원합니다.

"Google Cloud에서 Cloud Volumes ONTAP에 대해 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.

"Google Cloud의 Cloud Volumes ONTAP 스토리지 제한 사항"

Google Cloud에서 시스템 크기 조정

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

기계 유형

지원되는 기계 유형을 확인하세요. "Cloud Volumes ONTAP 릴리스 노트" 그런 다음 Google에서 지원되는 각 기기 유형에 대한 세부 정보를 검토합니다. 머신 유형에 맞는 vCPU 수와 메모리에 맞게 워크로드 요구 사항을 조정하세요. 각 CPU 코어가 네트워킹 성능을 향상시킨다는 점에 유의하세요.

자세한 내용은 다음을 참조하세요.

- "Google Cloud 문서: N1 표준 머신 유형"
- "Google Cloud 문서: 성능"

디스크 유형

Cloud Volumes ONTAP 에 대한 볼륨을 생성할 때 Cloud Volumes ONTAP 디스크에 사용하는 기본 클라우드 스토리지를 선택해야 합니다. 디스크 유형은 다음 중 하나일 수 있습니다.

- 영역별 *SSD* 영구 디스크: SSD 영구 디스크는 높은 속도의 무작위 IOPS가 필요한 워크로드에 가장 적합합니다.
- 영역별 균형 지속 디스크: 이러한 SSD는 GB당 더 낮은 IOPS를 제공하여 성능과 비용의 균형을 맞춥니다.
- 영역별 표준 영구 디스크 : 표준 영구 디스크는 경제적이며 순차적 읽기/쓰기 작업을 처리할 수 있습니다.

  자세한 내용은 다음을 참조하세요. "Google Cloud 문서: 영역별 영구 디스크(표준 및 SSD)" .

디스크 크기

Cloud Volumes ONTAP 시스템을 배포할 때 초기 디스크 크기를 선택해야 합니다. 그 후에는 NetApp Console 사용하여 시스템 용량을 관리할 수 있지만 직접 집계를 구축하려는 경우 다음 사항에 유의하세요.

- 집계된 모든 디스크의 크기는 동일해야 합니다.
- 성능을 고려하면서 필요한 공간을 결정하세요.
- 영구 디스크의 성능은 디스크 크기와 시스템에서 사용 가능한 vCPU 수에 따라 자동으로 확장됩니다.

  자세한 내용은 다음을 참조하세요.

  - "Google Cloud 문서: 영역별 영구 디스크(표준 및 SSD)"
  - "Google Cloud 설명서: 영구 디스크 및 로컬 SSD 성능 최적화"

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.

- "Google Cloud에서 Cloud Volumes ONTAP 시스템 데이터의 기본 디스크 보기" .
- "Google Cloud 문서: Cloud Quotas 개요"

  Google Cloud Compute Engine은 리소스 사용에 할당량을 적용하므로 Cloud Volumes ONTAP 배포하기 전에 한도에 도달하지 않았는지 확인해야 합니다.

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

네트워킹 정보 수집

Google Cloud에 Cloud Volumes ONTAP을 배포할 때 가상 네트워크에 대한 세부 정보를 지정해야 합니다. 워크시트를 사용하여 관리자로부터 정보를 수집할 수 있습니다.

단일 노드 시스템에 대한 네트워크 정보

Google Cloud 정보	당신의 가치
지역	
존	
VPC 네트워크	
서브넷	
방화벽 정책(자체 방화벽 정책을 사용하는 경우)	

여러 영역의 **HA** 쌍에 대한 네트워크 정보

Google Cloud 정보	당신의 가치
지역	
노드 1의 영역	
노드 2의 영역	
중재자를 위한 구역	
VPC-0 및 서브넷	
VPC-1 및 서브넷	
VPC-2 및 서브넷	
VPC-3 및 서브넷	
방화벽 정책(자체 방화벽 정책을 사용하는 경우)	

단일 존의 **HA** 쌍에 대한 네트워크 정보

Google Cloud 정보	당신의 가치
지역	

Google Cloud 정보	당신의 가치
존	
VPC-0 및 서브넷	
VPC-1 및 서브넷	
VPC-2 및 서브넷	
VPC-3 및 서브넷	
방화벽 정책(자체 방화벽 정책을 사용하는 경우)	

쓰기 속도를 선택하세요

콘솔을 사용하면 Google Cloud의 고가용성(HA) 쌍을 제외하고 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.

Cloud Volumes ONTAP 에 대한 Google Cloud 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.

HA 쌍을 배포하려면 다음을 수행해야 합니다."Google Cloud에서 HA 쌍이 작동하는 방식 알아보기" .

Cloud Volumes ONTAP 요구 사항

Google Cloud에서는 다음 요구 사항을 충족해야 합니다.

단일 노드 시스템에 대한 요구 사항

단일 노드 시스템을 구축하려면 네트워킹이 다음 요구 사항을 충족하는지 확인하십시오.

하나의 **VPC**

단일 노드 시스템에는 하나의 Virtual Private Cloud(VPC)가 필요합니다.

개인 **IP** 주소

Google Cloud의 단일 노드 시스템의 경우 Console은 다음에 프라이빗 IP 주소를 할당합니다.

- 마디
- 무리
- 스토리지 VM
- 데이터 NAS LIF
- 데이터 iSCSI LIF

API를 사용하여 Cloud Volumes ONTAP 배포하고 다음 플래그를 지정하면 스토리지 VM(SVM) 관리 LIF 생성을 건너뛸 수 있습니다.

```
skipSvmManagementLif: true
```

LIF는 물리적 포트와 연결된 IP 주소입니다. SnapCenter 와 같은 관리 도구에는 스토리지 VM(SVM) 관리 LIF가 필요합니다.

HA 쌍에 대한 특정 요구 사항

HA 쌍을 배포하려면 네트워킹이 다음 요구 사항을 충족하는지 확인하세요.

하나 또는 여러 개의 구역

여러 영역이나 단일 영역에 HA 구성을 배포하면 데이터의 높은 가용성을 보장할 수 있습니다. HA 쌍을 생성할 때 콘솔에서는 여러 영역이나 단일 영역을 선택하라는 메시지가 표시됩니다.

- 여러 구역(권장)

  3개 영역에 걸쳐 HA 구성을 배포하면 영역 내에서 장애가 발생하더라도 지속적인 데이터 가용성이 보장됩니다. 단일 영역을 사용하는 것에 비해 쓰기 성능은 약간 낮지만 최소한입니다.

- 단일 구역

  단일 영역에 배포되는 경우 Cloud Volumes ONTAP HA 구성은 확산 배치 정책을 사용합니다. 이 정책은 오류 격리를 위해 별도의 영역을 사용하지 않고도 영역 내의 단일 장애 지점으로부터 HA 구성이 보호되도록 보장합니다.

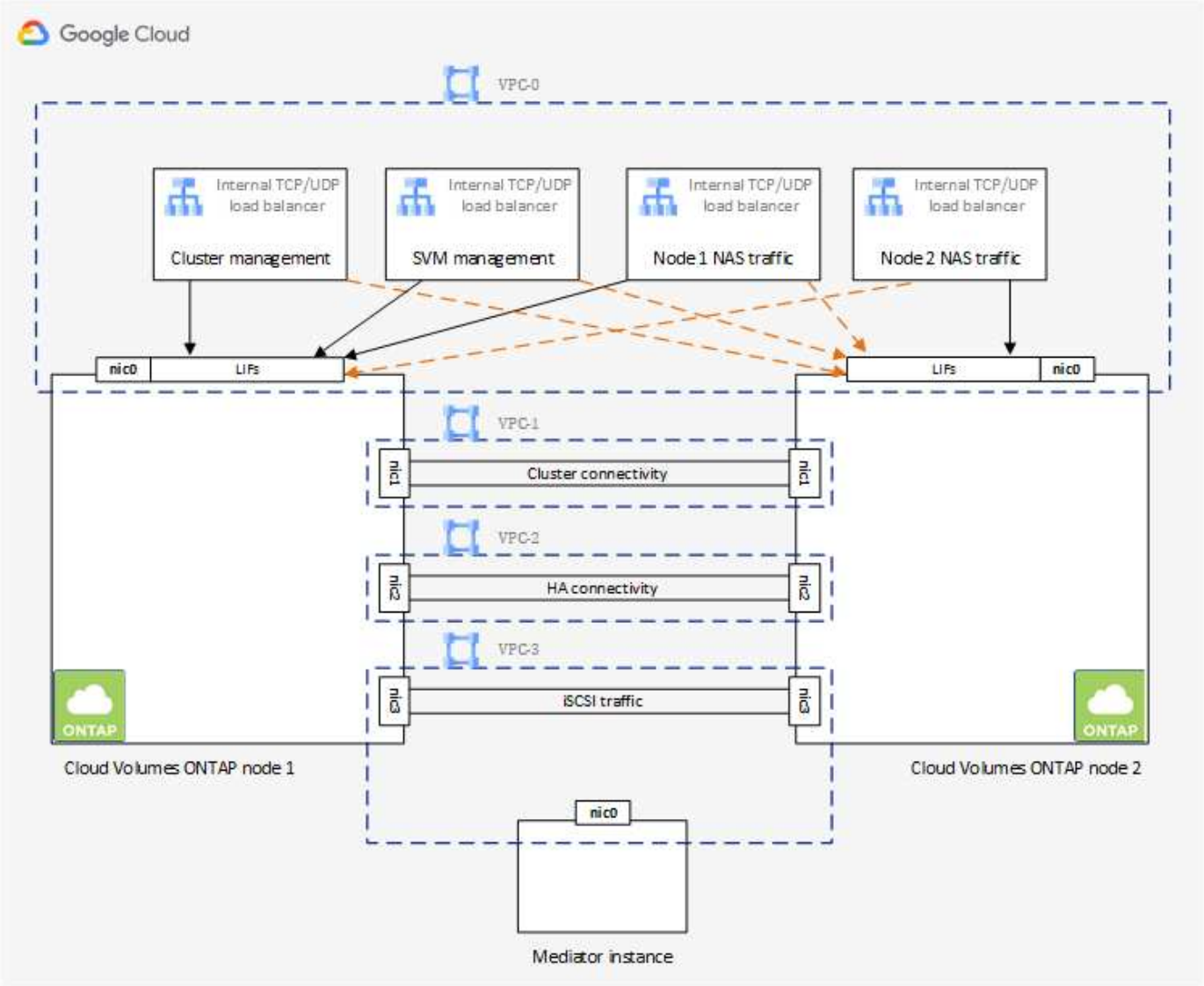
  이 배포 모델을 사용하면 영역 간에 데이터 유출 요금이 발생하지 않으므로 비용이 절감됩니다.

4개의 가상 사설 클라우드

HA 구성에는 4개의 가상 사설 클라우드(VPC)가 필요합니다. Google Cloud에서는 각 네트워크 인터페이스가 별도의 VPC 네트워크에 있어야 하므로 4개의 VPC가 필요합니다.

HA 쌍을 생성할 때 콘솔에서는 4개의 VPC를 선택하라는 메시지가 표시됩니다.

- 데이터 및 노드에 대한 인바운드 연결을 위한 VPC-0
- 노드와 HA 중재자 간 내부 통신을 위한 VPC-1, VPC-2 및 VPC-3



서브넷

각 VPC에는 개인 서브넷이 필요합니다.

VPC-0에 콘솔 에이전트를 배치하는 경우 API에 액세스하고 데이터 계층화를 활성화하려면 서브넷에서 Private Google Access를 활성화해야 합니다.

이러한 VPC의 서브넷에는 서로 다른 CIDR 범위가 있어야 합니다. CIDR 범위가 겹칠 수 없습니다.

개인 IP 주소

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

Cloud Volumes ONTAP에 할당된 LIF 수는 단일 노드 시스템을 배포하는지 또는 HA 쌍을 배포하는지에 따라 달라집니다. LIF는 물리적 포트와 연결된 IP 주소입니다. SVM 관리 LIF는 SnapCenter와 같은 관리 툴에 필요합니다.

- 단일 노드 NetApp Console은 단일 노드 시스템에 4개의 IP 주소를 할당합니다.
  - 노드 관리 LIF
  - 클러스터 관리 LIF
  - iSCSI 데이터 LIF

    iSCSI LIF는 iSCSI 프로토콜을 통해 클라이언트 액세스를 제공하며 시스템에서 다른 중요한 네트워킹 워크플로에 사용됩니다. 이러한 LIF는 필수이므로 삭제하면 안 됩니다.

  - 나스 라이프

    API를 사용하여 Cloud Volumes ONTAP 배포하고 다음 플래그를 지정하면 스토리지 VM(SVM) 관리 LIF 생성을 건너뛸 수 있습니다.

```
skipSvmManagementLif: true
```

- **HA** 쌍 콘솔은 HA 쌍에 12-13개의 IP 주소를 할당합니다.
  - 2개의 노드 관리 LIF(e0a)
  - 1 클러스터 관리 LIF(e0a)
  - 2개의 iSCSI LIF(e0a)

    iSCSI LIF는 iSCSI 프로토콜을 통해 클라이언트 액세스를 제공하며 시스템에서 다른 중요한 네트워킹 워크플로에 사용됩니다. 이러한 LIF는 필수이므로 삭제하면 안 됩니다.

  - 1개 또는 2개의 NAS LIF(e0a)
  - 2개의 클러스터 LIF(e0b)
  - 2개의 HA 상호 연결 IP 주소(e0c)
  - 2개의 RSM iSCSI IP 주소(e0d)

    API를 사용하여 Cloud Volumes ONTAP 배포하고 다음 플래그를 지정하면 스토리지 VM(SVM) 관리 LIF 생성을 건너뛸 수 있습니다.

```
skipSvmManagementLif: true
```

내부 로드 밸런서

콘솔은 Cloud Volumes ONTAP HA 쌍으로 들어오는 트래픽을 관리하는 4개의 Google Cloud 내부 부하 분산 장치(TCP/UDP)를 생성합니다. 귀하 측에서는 아무런 설정이 필요하지 않습니다. 우리는 네트워크 트래픽에 대해 알려드리고 보안 문제를 완화하기 위해 이를 필수 사항으로 나열했습니다.

한 로드 밸런서는 클러스터 관리용이고, 다른 하나는 스토리지 VM(SVM) 관리용이며, 다른 하나는 노드 1로의 NAS 트래픽용이고, 마지막 하나는 노드 2로의 NAS 트래픽용입니다.

각 로드 밸런서의 설정은 다음과 같습니다.

- 공유된 개인 IP 주소 하나
- 글로벌 건강 검진 한 번

  기본적으로 상태 점검에 사용되는 포트는 63001, 63002, 63003입니다.

- 하나의 지역 TCP 백엔드 서비스
- 하나의 지역 UDP 백엔드 서비스
- 하나의 TCP 전달 규칙
- UDP 전달 규칙 1개
- 글로벌 접근이 비활성화되었습니다

  기본적으로 글로벌 액세스는 비활성화되어 있지만 배포 후에 활성화하는 것이 지원됩니다. 지역 간 트래픽의 지연 시간이 상당히 길어지기 때문에 이 기능을 비활성화했습니다. 우리는 여러분이 우연히 다른 지역의 탈것을 타고 부정적인 경험을 하지 않도록 하려고 했습니다. 이 옵션을 활성화하는 것은 귀하의 비즈니스 요구 사항에 맞게 결정됩니다.

공유 **VPC**

Cloud Volumes ONTAP 과 콘솔 에이전트는 Google Cloud 공유 VPC와 독립형 VPC에서 지원됩니다.

단일 노드 시스템의 경우 VPC는 공유 VPC 또는 독립형 VPC일 수 있습니다.

HA 쌍의 경우 4개의 VPC가 필요합니다. 각 VPC는 공유형이거나 독립형일 수 있습니다. 예를 들어, VPC-0은 공유 VPC가 될 수 있고, VPC-1, VPC-2, VPC-3은 독립형 VPC가 될 수 있습니다.

공유 VPC를 사용하면 여러 프로젝트에서 가상 네트워크를 구성하고 중앙에서 관리할 수 있습니다. _호스트 프로젝트_에서 공유 VPC 네트워크를 설정하고 _서비스 프로젝트_에서 콘솔 에이전트와 Cloud Volumes ONTAP 가상 머신 인스턴스를 배포할 수 있습니다.

"Google Cloud 문서: 공유 VPC 개요" .

"콘솔 에이전트 배포에서 다루는 필수 공유 VPC 권한을 검토하세요."

VPC에서의 패킷 미러링

"패킷 미러링"Cloud Volumes ONTAP 배포하는 Google Cloud 서브넷에서 비활성화해야 합니다.

아웃바운드 인터넷 접속

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. 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.

엔드포인트	적용 가능	목적	배포 모드	엔드포인트를 사용할 수 없는 경우의 영향
https://cloudbuild.googleapis.com/v1 (개인 모드 배포 전용) https://cloudkms.googleapis.com/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://compute.googleapis.com/compute/v1 https://www.googleapis.com/compute/beta https://www.googleapis.com/compute/v1/projects/ https://www.googleapis.com/deploymentmanager/v2/projects https://www.googleapis.com/storage/v1 https://www.googleapis.com/upload/storage/v1 https://config.googleapis.com/v1 https://iam.googleapis.com/v1 https://storage.googleapis.com/storage/v1	Google Cloud(상업적 사용).	Google Cloud 서비스와의 통신.	표준, 제한, 비공개 모드.	Cloud Volumes ONTAP Google Cloud 서비스와 통신하여 Google Cloud의 콘솔에 대한 특정 작업을 수행할 수 없습니다.

다른 네트워크의 **ONTAP** 시스템에 대한 연결

Google Cloud의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 VPC와 다른 네트워크(예: 회사 네트워크) 간에 VPN 연결이 필요합니다.

"Google Cloud 문서: Cloud VPN 개요" .

방화벽 규칙

콘솔은 Cloud Volumes ONTAP 성공적으로 작동하는 데 필요한 인바운드 및 아웃바운드 규칙을 포함하는 Google Cloud 방화벽 규칙을 생성합니다. 테스트 목적으로 포트를 참조하거나 자체 방화벽 규칙을 사용하려는 경우 포트를 참조할 수 있습니다.

Cloud Volumes ONTAP 의 방화벽 규칙에는 인바운드 규칙과 아웃바운드 규칙이 모두 필요합니다. HA 구성을 배포하는 경우 VPC-0의 Cloud Volumes ONTAP 에 대한 방화벽 규칙은 다음과 같습니다.

HA 구성에는 두 세트의 방화벽 규칙이 필요합니다.

- VPC-0의 HA 구성 요소에 대한 한 세트의 규칙입니다. 이러한 규칙은 Cloud Volumes ONTAP 에 대한 데이터 액세스를 가능하게 합니다.
- VPC-1, VPC-2, VPC-3의 HA 구성 요소에 대한 또 다른 규칙 세트입니다. 이러한 규칙은 HA 구성 요소 간의 인바운드 및 아웃바운드 통신에 적용됩니다. 자세히 알아보기 .

콘솔 에이전트에 대한 정보를 찾고 계신가요? "콘솔 에이전트에 대한 방화벽 규칙 보기"

인바운드 규칙

Cloud Volumes ONTAP 시스템을 추가하면 배포 중에 미리 정의된 방화벽 정책에 대한 소스 필터를 선택할 수 있습니다.

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

자체 방화벽 정책을 사용하는 경우 Cloud Volumes ONTAP 과 통신해야 하는 모든 네트워크를 추가해야 하지만, 내부 Google Load Balancer가 올바르게 작동할 수 있도록 두 주소 범위도 추가해야 합니다. 이 주소는 130.211.0.0/22와 35.191.0.0/16입니다. 자세한 내용은 다음을 참조하세요. "Google Cloud 문서: 로드 밸런서 방화벽 규칙" .

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

규약	포트	목적
TCP	63001-63050	어느 노드가 정상인지 확인하기 위한 로드 밸런싱 프로브 포트(HA 쌍에만 필요)
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. Cloud Volumes ONTAP 클러스터는 노드 트래픽을 조절하기 위해 다음 포트를 사용합니다.

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
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
시스템 로그	UDP	514	노드 관리 LIF	시스템 로그 서버	Syslog 전달 메시지

VPC-1, VPC-2 및 **VPC-3**에 대한 규칙

Google Cloud에서는 HA 구성이 4개의 VPC에 배포됩니다. VPC-0의 HA 구성에 필요한 방화벽 규칙은 다음과 같습니다.위에 나열된 Cloud Volumes ONTAP .

한편, VPC-1, VPC-2, VPC-3의 인스턴스에 대해 미리 정의된 방화벽 규칙은 모든 프로토콜과 포트를 통한 수신 통신을 활성화합니다. 이러한 규칙은 HA 노드 간의 통신을 가능하게 합니다.

HA 노드에서 HA 중재자로의 통신은 포트 3260(iSCSI)을 통해 이루어집니다.

새로운 Google Cloud HA 쌍 배포에 대해 높은 쓰기 속도를 구현하려면 VPC-1, VPC-2, VPC-3에 최소 8,896바이트의 최대 전송 단위(MTU)가 필요합니다. 기존 VPC-1, VPC-2, VPC-3을 8,896바이트의 MTU로 업그레이드하기로 선택한 경우 구성 프로세스 중에 이러한 VPC를 사용하는 모든 기존 HA 시스템을 종료해야 합니다.

콘솔 에이전트에 대한 요구 사항

아직 콘솔 에이전트를 만들지 않았다면 네트워킹 요구 사항을 검토해야 합니다.

- "콘솔 에이전트에 대한 네트워킹 요구 사항 보기"
- "Google Cloud의 방화벽 규칙"

콘솔 에이전트 프록시를 지원하는 네트워크 구성

콘솔 에이전트에 구성된 프록시 서버를 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 에이전트 프록시 구성 중에 지정된 프록시 서버의 HTTP 주소를 사용합니다. 콘솔 에이전트 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 에이전트 프록시를 통해 Cloud Volumes ONTAP 에서 아웃바운드 트래픽을 자동으로 라우팅하도록 구성됩니다. 투명 프록시를 설정할 때 콘솔 에이전트 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.

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

Google Cloud에서 **Cloud Volumes ONTAP** 에 대한 네트워크 태그 구성

콘솔 에이전트의 투명 프록시 구성 중에 관리자는 Google Cloud에 대한 네트워크 태그를 추가합니다. Cloud Volumes ONTAP 구성에 대해 동일한 네트워크 태그를 얻어 수동으로 추가해야 합니다. 이 태그는 프록시 서버가 올바르게 작동하는 데 필요합니다.

1. Google Cloud Console에서 Cloud Volumes ONTAP 시스템을 찾습니다.
2. *세부정보 > 네트워킹 > 네트워크 태그*로 이동합니다.
3. 콘솔 에이전트에 사용된 태그를 추가하고 구성을 저장합니다.

관련 주제

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

Google Cloud에 **Cloud Volumes ONTAP** 배포하기 위한 **VPC** 서비스 제어 설정

VPC 서비스 제어를 사용하여 Google Cloud 환경을 잠그기로 선택하는 경우 NetApp Console 과 Cloud Volumes ONTAP Google Cloud API와 상호 작용하는 방식과 Console과 Cloud Volumes ONTAP 배포하기 위해 서비스 경계를 구성하는 방법을 이해해야 합니다.

VPC 서비스 제어를 사용하면 신뢰할 수 있는 경계 외부에서 Google 관리 서비스에 대한 액세스를 제어하고, 신뢰할 수 없는 위치에서의 데이터 액세스를 차단하고, 승인되지 않은 데이터 전송 위험을 완화할 수 있습니다. "Google Cloud VPC 서비스 제어에 대해 자세히 알아보세요" .

NetApp 서비스가 VPC 서비스 제어와 통신하는 방법

콘솔은 Google Cloud API와 직접 통신합니다. 이는 Google Cloud 외부의 외부 IP 주소(예: api.services.cloud.netapp.com)에서 트리거되거나, Google Cloud 내에서 Console 에이전트에 할당된 내부 주소에서 트리거됩니다.

콘솔 에이전트의 배포 스타일에 따라 서비스 경계에 대한 특정 예외를 만들어야 할 수도 있습니다.

이미지

Cloud Volumes ONTAP과 Console은 모두 NetApp에서 관리하는 Google Cloud 내 프로젝트의 이미지를 사용합니다. 조직에서 조직 내에 호스팅되지 않은 이미지 사용을 차단하는 정책이 있는 경우 Console 에이전트 및 Cloud Volumes ONTAP 배포에 영향을 미칠 수 있습니다.

수동 설치 방법을 사용하여 콘솔 에이전트를 수동으로 배포할 수 있지만 Cloud Volumes ONTAP 도 NetApp 프로젝트에서 이미지를 가져와야 합니다. 콘솔 에이전트와 Cloud Volumes ONTAP 배포하려면 허용 목록을 제공해야 합니다.

콘솔 에이전트 배포

콘솔 에이전트를 배포하는 사용자는 프로젝트 ID _netapp-cloudmanager_와 프로젝트 번호 _14190056516_에 호스팅된 이미지를 참조할 수 있어야 합니다.

Cloud Volumes ONTAP 배포

- 콘솔 서비스 계정은 서비스 프로젝트의 프로젝트 ID _netapp-cloudmanager_와 프로젝트 번호 _14190056516_에 호스팅된 이미지를 참조해야 합니다.
- 기본 Google API 서비스 에이전트의 서비스 계정은 서비스 프로젝트의 프로젝트 ID _netapp-cloudmanager_와 프로젝트 번호 _14190056516_에 호스팅된 이미지를 참조해야 합니다.

VPC 서비스 제어를 사용하여 이러한 이미지를 가져오는 데 필요한 규칙의 예는 아래와 같습니다.

VPC 서비스 제어 경계 정책

정책을 사용하면 VPC Service Controls 규칙 집합에 대한 예외를 허용할 수 있습니다. 정책에 대한 자세한 내용은 해당 페이지를 참조하십시오 "Google Cloud VPC Service Controls 정책 설명서".

콘솔에 필요한 정책을 설정하려면 조직 내의 VPC 서비스 제어 경계로 이동하여 다음 정책을 추가하세요. 필드는 VPC 서비스 제어 정책 페이지에 제공된 옵션과 일치해야 합니다. 또한 모든 규칙이 필수이며 규칙 세트에서는 **OR** 매개변수를 사용해야 합니다.

Ingress 규칙

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

또는

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

또는

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

탈출 규칙

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

위에 설명된 프로젝트 번호는 NetApp 에서 콘솔 에이전트와 Cloud Volumes ONTAP 의 이미지를 저장하는 데 사용되는 프로젝트 _netapp-cloudmanager_입니다.

Cloud Volumes ONTAP 에 대한 Google Cloud 서비스 계정을 만듭니다.

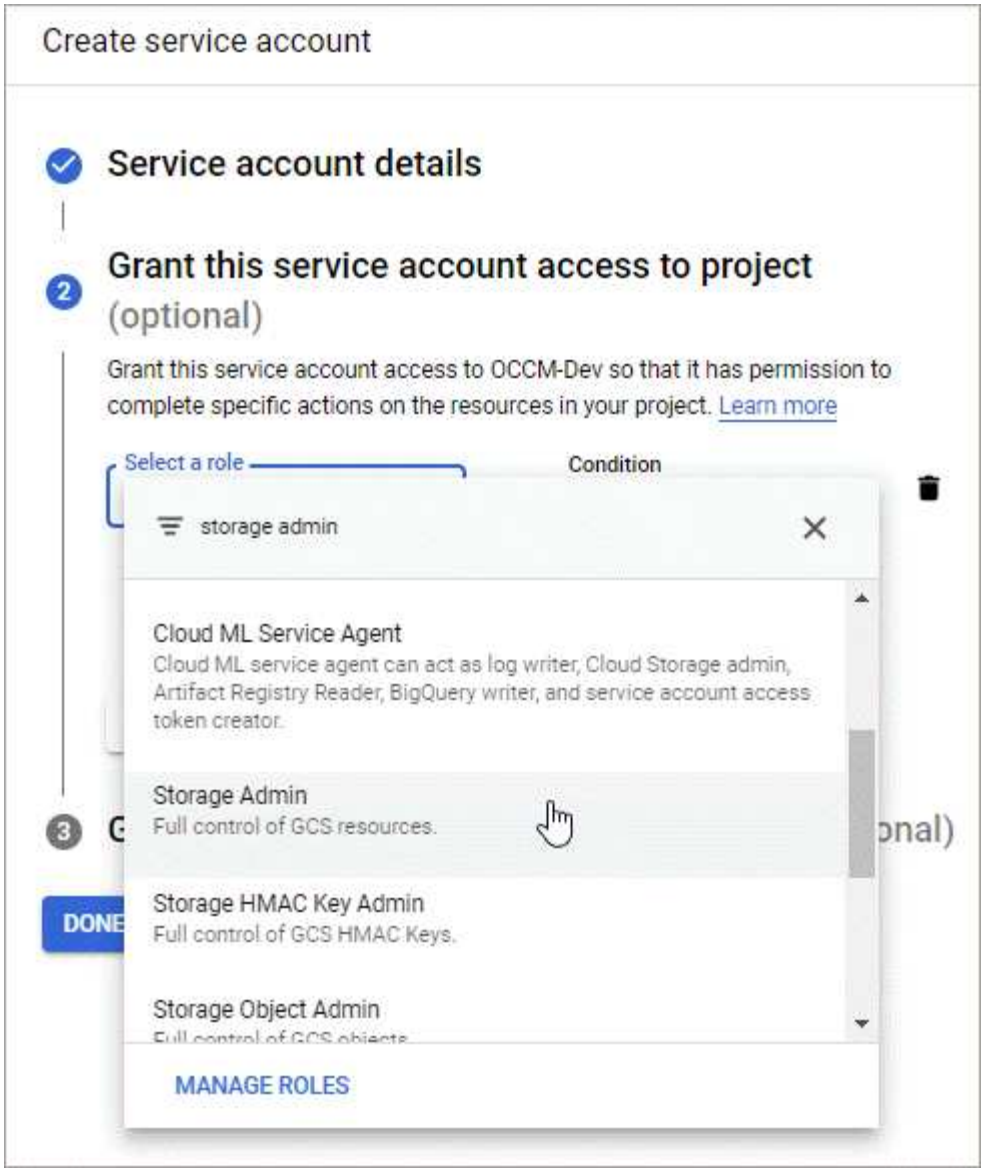
Cloud Volumes ONTAP 두 가지 목적으로 Google Cloud 서비스 계정이 필요합니다. 첫 번째는 활성화할 때입니다."데이터 계층화" Google Cloud의 저렴한 객체 스토리지에 콜드 데이터를 계층화합니다. 두 번째는 다음을 활성화할 때입니다. "NetApp Backup and Recovery" 저렴한 개체 스토리지에 볼륨을 백업합니다.

Cloud Volumes ONTAP 서비스 계정을 사용하여 계층화된 데이터용 버킷 하나와 백업용 버킷 하나에 액세스하고 관리합니다.

하나의 서비스 계정을 설정하여 두 가지 목적으로 모두 사용할 수 있습니다. 서비스 계정에는 저장소 관리자 역할이 있어야 합니다.

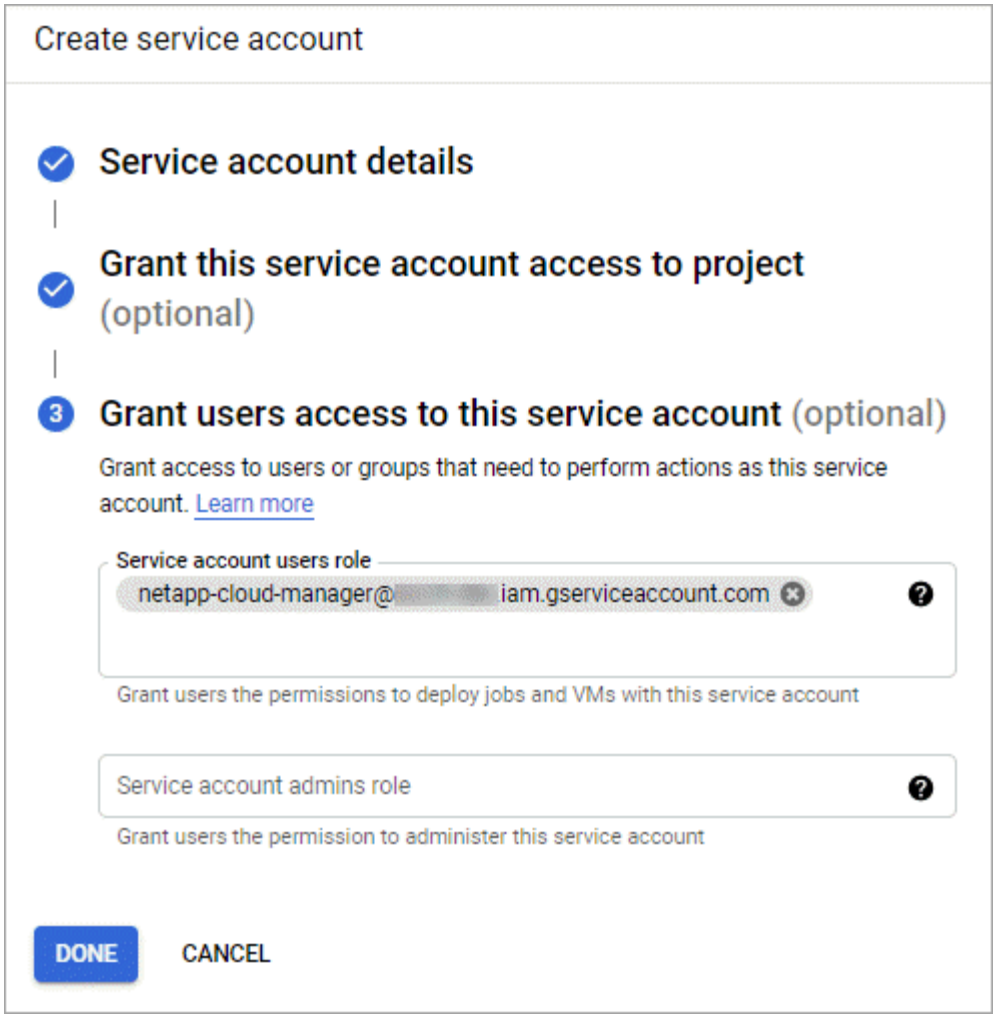
단계

1. Google Cloud 콘솔에서 "서비스 계정 페이지로 이동".
2. 프로젝트를 선택하세요.
3. *서비스 계정 만들기*를 클릭하고 필요한 정보를 입력하세요.
    a. 서비스 계정 세부 정보: 이름과 설명을 입력하세요.
    b. 이 서비스 계정에 프로젝트에 대한 액세스 권한 부여: 저장소 관리자 역할을 선택합니다.



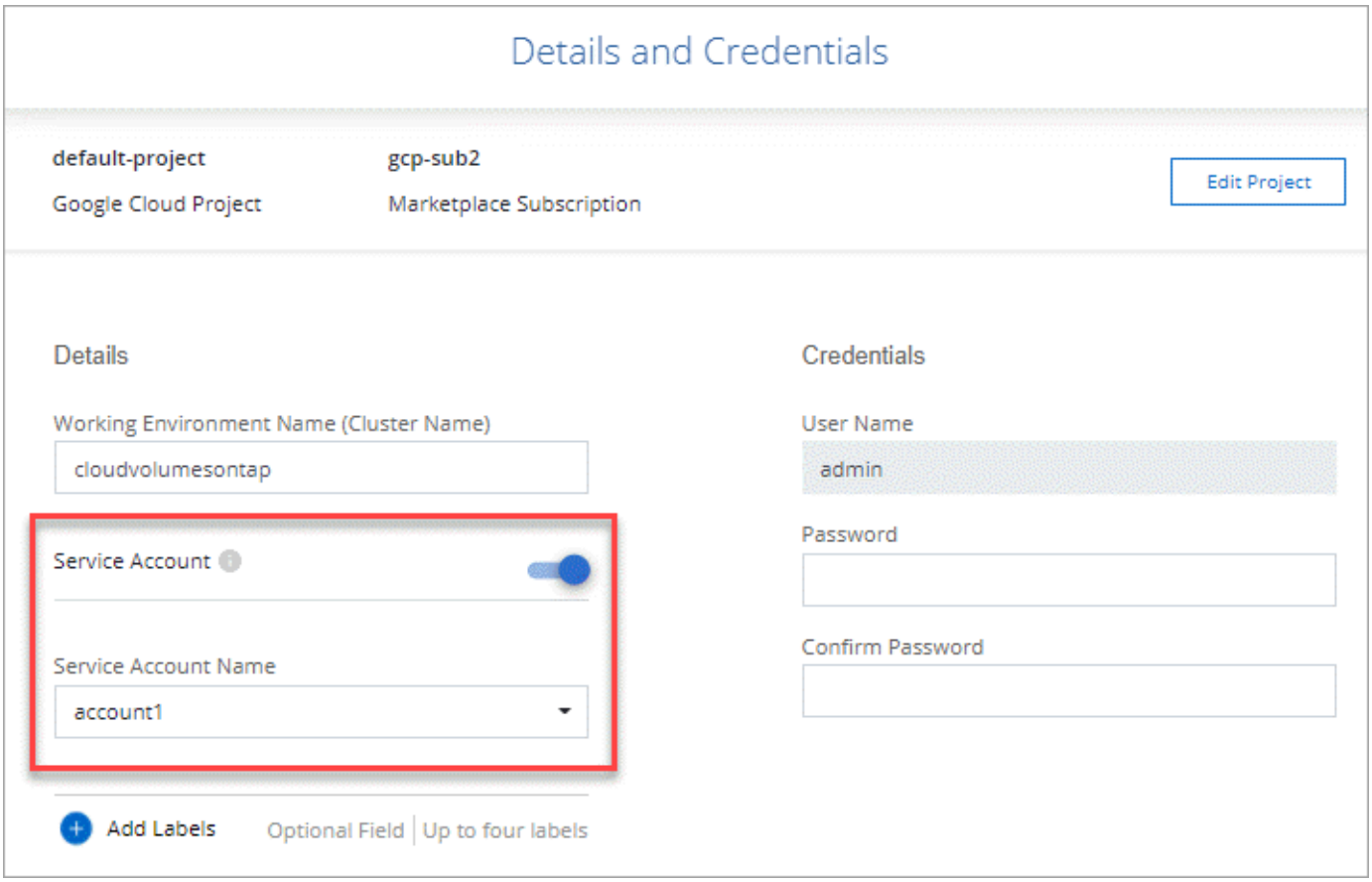
c. 사용자에게 이 서비스 계정에 대한 액세스 권한 부여: 이 새로운 서비스 계정에 콘솔 에이전트 서비스 계정을 _서비스 계정 사용자_로 추가합니다.

   이 단계는 데이터 계층화에만 필요합니다. 백업 및 복구에는 필요하지 않습니다.



다음은 무엇인가요?

나중에 Cloud Volumes ONTAP 시스템을 생성할 때 서비스 계정을 선택해야 합니다.



Cloud Volumes ONTAP 에서 고객 관리 암호화 키 사용

Google Cloud Storage는 디스크에 쓰기 전에 항상 데이터를 암호화하지만, API를 사용하면 _고객 관리 암호화 키_를 사용하는 Cloud Volumes ONTAP 시스템을 만들 수 있습니다. 이러한 키는 Cloud Key Management Service를 사용하여 GCP에서 생성하고 관리하는 키입니다.

단계

1. 키가 저장된 프로젝트에서 콘솔 에이전트 서비스 계정에 프로젝트 수준에서 올바른 권한이 있는지 확인하세요.

   권한은 다음에서 제공됩니다. "기본적으로 서비스 계정 권한" 하지만 Cloud Key Management Service에 대한 대체 프로젝트를 사용하는 경우에는 적용되지 않을 수 있습니다.

   권한은 다음과 같습니다.

   ```
   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list
   ```

2. 서비스 계정이 다음인지 확인하세요. "Google Compute Engine 서비스 에이전트" 키에 Cloud KMS 암호화/복호화 권한이 있습니다.

   서비스 계정의 이름은 "service-[service_project_number]@compute-system.iam.gserviceaccount.com" 형식을 사용합니다.

"Google Cloud 문서: Cloud KMS와 함께 IAM 사용 - 리소스에 대한 역할 부여"

3. get 명령을 호출하여 키의 "id"를 얻으십시오. `/gcp/vsa/metadata/gcp-encryption-keys` API 호출 또는 GCP 콘솔의 키에서 "리소스 이름 복사"를 선택합니다.
4. 고객 관리 암호화 키를 사용하고 데이터를 개체 스토리지로 계층화하는 경우 NetApp Console 영구 디스크를 암호화하는 데 사용되는 것과 동일한 키를 활용하려고 시도합니다. 하지만 먼저 Google Cloud Storage 버킷을 활성화하여 키를 사용해야 합니다.

   a. 다음을 따라 Google Cloud Storage 서비스 에이전트를 찾으세요. "Google Cloud 문서: Cloud Storage 서비스 에이전트 가져오기" .

   b. 암호화 키로 이동하여 Google Cloud Storage 서비스 에이전트에 Cloud KMS 암호화/복호화 권한을 할당합니다.

   자세한 내용은 다음을 참조하세요. "Google Cloud 문서: 고객 관리 암호화 키 사용"

5. 시스템을 생성할 때 API 요청에 "gcpEncryption" 매개변수를 사용하십시오.

   예

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-
1/cryptoKeys/generatedkey1"
  }
```

를 참조하세요 "NetApp Console 자동화 문서" "GcpEncryption" 매개변수 사용에 대한 자세한 내용은 다음을 참조하세요.

Google Cloud에서 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" .

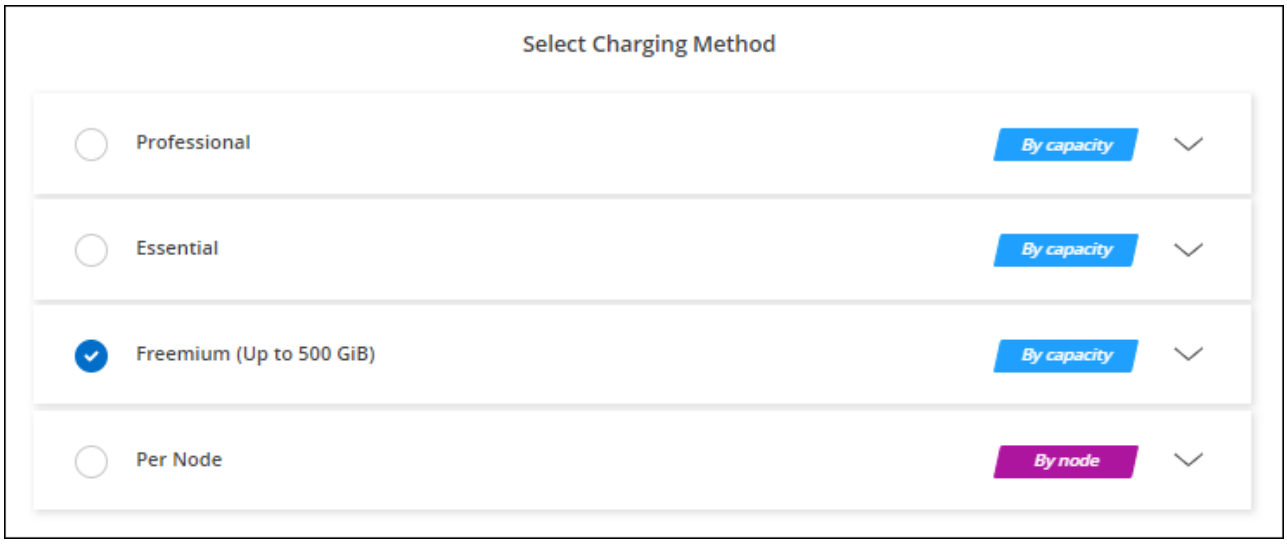
단계

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

   a. 세부 정보 및 자격 증명 페이지에서 *자격 증명 편집 > 구독 추가*를 클릭한 다음, 메시지에 따라 Google Cloud 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" .

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



"Google Cloud에서 Cloud Volumes ONTAP 시작하는 단계별 지침을 확인하세요." .

용량 기반 라이센스

용량 기반 라이선싱을 사용하면 TiB 용량당 Cloud Volumes ONTAP 비용을 지불할 수 있습니다. 용량 기반 라이선싱은 패키지(Essentials 또는 Professional 패키지) 형태로 제공됩니다.

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

- NetApp 에서 구매한 라이선스(BYOL(Bring Your Own License))
- Google Cloud Marketplace의 시간당 결제(PAYGO) 구독
- 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. "NetApp Console 에 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 라이선스를 추가합니다.

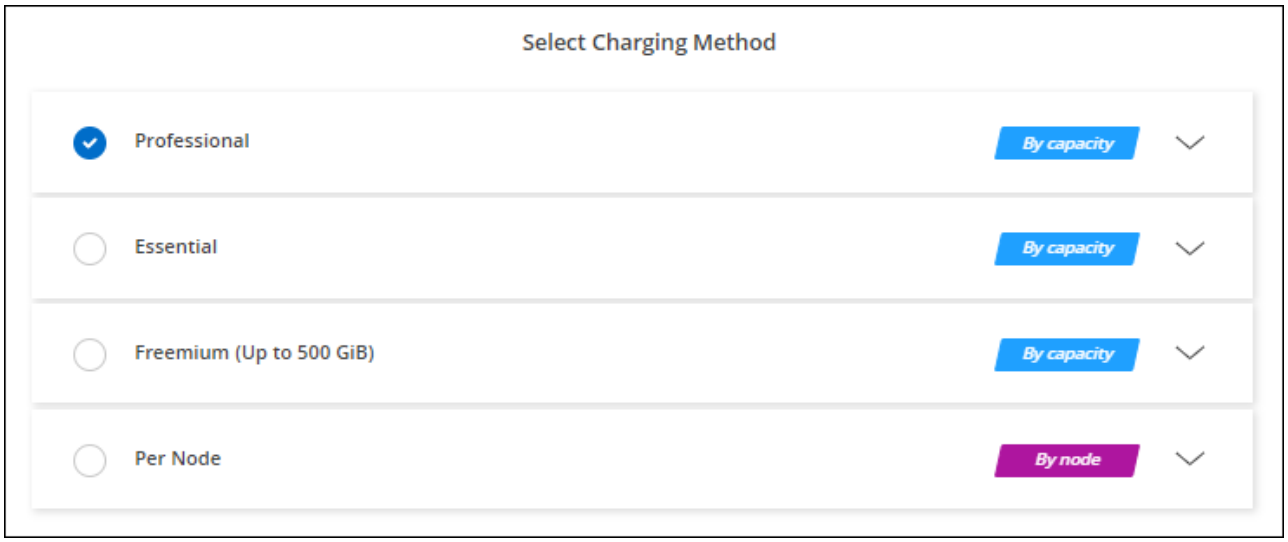
   Cloud Volumes ONTAP 에서 라이선스를 사용하려면 먼저 콘솔에서 라이선스를 사용할 수 있어야 합니다. 필요한 경우 다음을 수행할 수 있습니다."콘솔에 라이센스를 수동으로 추가합니다." .

3. 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 Google Cloud Marketplace에서 사용량에 따라 지불하는 서비스를 구독하세요.

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

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



"Google Cloud에서 Cloud Volumes ONTAP 시작하는 단계별 지침을 확인하세요." .

PAYGO 구독

클라우드 공급업체의 마켓플레이스에서 제공하는 혜택을 구독하여 시간당 요금을 지불하세요.

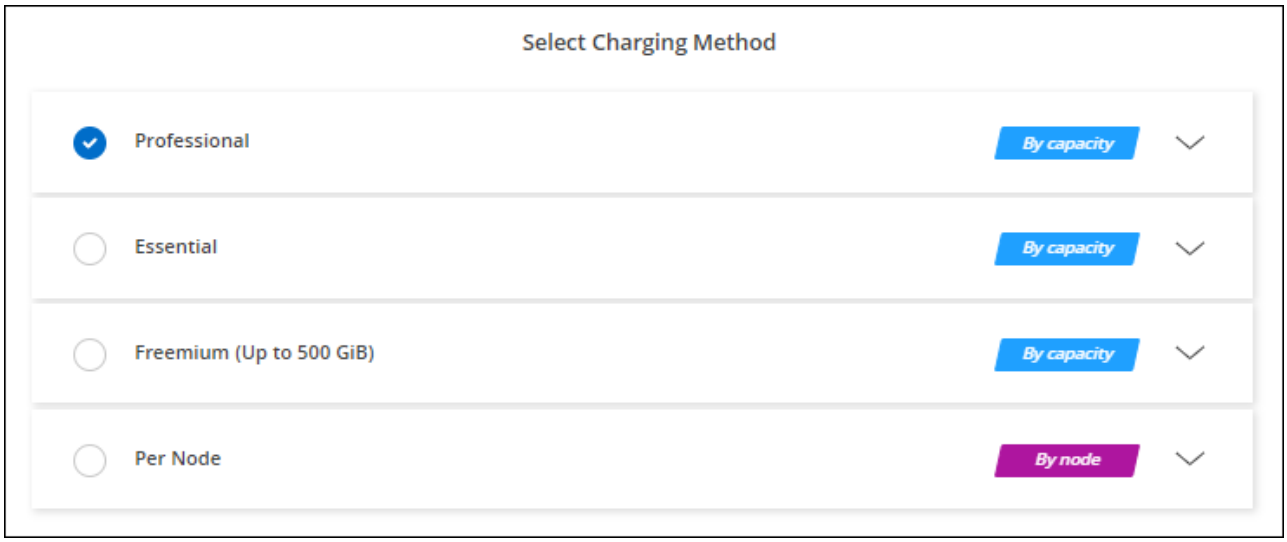
Cloud Volumes ONTAP 시스템을 만들면 콘솔에서 Google Cloud Marketplace에서 제공되는 계약에 가입하라는 메시지가 표시됩니다. 해당 구독은 요금 청구를 위해 시스템에 연결됩니다. 동일한 구독을 추가 시스템에도 사용할 수 있습니다.

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, 메시지에 따라 Google Cloud Marketplace에서 사용량에 따라 지불하는 서비스를 구독하세요.

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



"Google Cloud에서 Cloud Volumes ONTAP 시작하는 단계별 지침을 확인하세요." .

설정 > 사용자 인증 정보 페이지에서 계정과 연결된 Google Cloud Marketplace 구독을 관리할 수 있습니다. "Google Cloud 자격 증명 및 구독을 관리하는 방법을 알아보세요."

연간 계약

연간 계약을 구매하여 매년 Cloud Volumes ONTAP 에 대한 비용을 지불하세요.

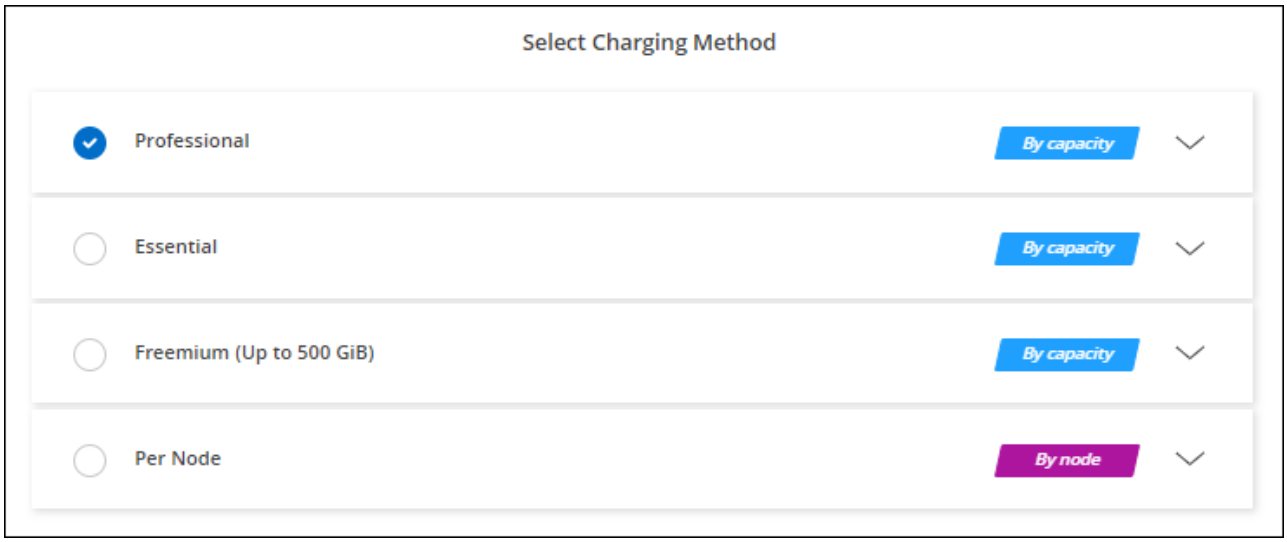
단계

1. 연간 계약을 구매하려면 NetApp 영업 담당자에게 문의하세요.

   해당 계약은 Google Cloud Marketplace에서 비공개 제안으로 제공됩니다.

   NetApp 에서 비공개 제안을 공유한 후, 시스템을 생성하는 동안 Google Cloud Marketplace에서 구독할 때 연간 요금제를 선택할 수 있습니다.

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 Google Cloud Marketplace에서 연간 요금제를 구독하세요.
   b. Google Cloud에서 계정과 공유된 연간 요금제를 선택한 다음 *구독*을 클릭합니다.
   c. 콘솔로 돌아온 후, 청구 방법 페이지가 나타나면 용량 기반 패키지를 선택하세요.



"Google Cloud에서 Cloud Volumes ONTAP 시작하는 단계별 지침을 확인하세요." .

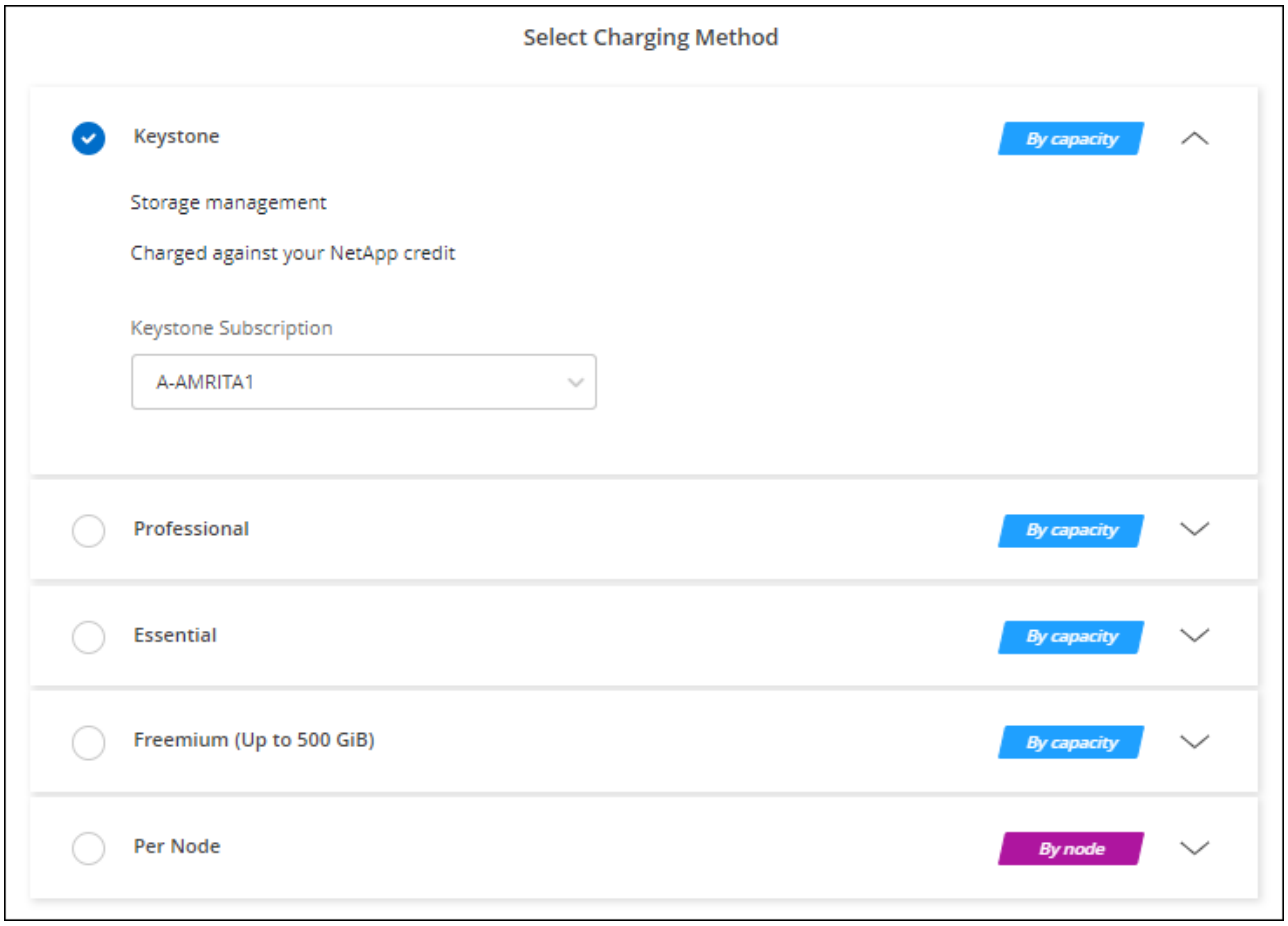
Keystone 구독

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. 콘솔 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.



"Google Cloud에서 Cloud Volumes ONTAP 시작하는 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"

Google Cloud에서 Cloud Volumes ONTAP 실행

Google Cloud에서 단일 노드 구성이나 HA 쌍으로 Cloud Volumes ONTAP 실행할 수 있습니다.

시작하기 전에

시작하기 전에 다음 사항이 필요합니다.

- 정상적으로 실행 중인 NetApp Console 에이전트입니다.
  - 당신은 ~을 가져야합니다 "시스템과 연결된 콘솔 에이전트" .

- "항상 콘솔 에이전트를 실행 상태로 두어야 합니다." .
- 콘솔 에이전트와 연결된 서비스 계정 "필요한 권한이 있어야 합니다"

- 사용하려는 구성에 대한 이해.

  구성을 선택하고 관리자로부터 Google Cloud 네트워킹 정보를 얻어서 준비해야 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" .

- Google Cloud API는 다음과 같아야 합니다. "프로젝트에서 활성화됨" :
  - 클라우드 배포 관리자 V2 API
  - 클라우드 로깅 API
  - 클라우드 리소스 관리자 API
  - 컴퓨트 엔진 API
  - ID 및 액세스 관리(IAM) API

Google Cloud에서 단일 노드 시스템 출시

NetApp Console 에서 시스템을 만들어 Google Cloud에서 Cloud Volumes ONTAP 시작합니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 안내를 따르세요.
3. 위치 선택: *Google Cloud*와 * Cloud Volumes ONTAP*을 선택하세요.
4. 메시지가 표시되면 "콘솔 에이전트 생성" .
5. 세부 정보 및 자격 증명: 프로젝트를 선택하고, 클러스터 이름을 지정하고, 선택적으로 서비스 계정을 선택하고, 선택적으로 레이블을 추가한 다음 자격 증명을 지정합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
시스템 이름	콘솔은 시스템 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Google Cloud VM 인스턴스의 이름을 지정합니다. 해당 옵션을 선택하면 사전 정의된 보안 그룹의 접두사로도 이름이 사용됩니다.
서비스 계정 이름	사용할 계획이라면"데이터 계층화" 또는 "NetApp Backup and Recovery" Cloud Volumes ONTAP 사용하는 경우 *서비스 계정*을 활성화하고 사전 정의된 스토리지 관리자 역할이 있는 서비스 계정을 선택해야 합니다. "서비스 계정을 만드는 방법을 알아보세요" .

필드	설명
라벨 추가	라벨은 Google Cloud 리소스에 대한 메타데이터입니다. 콘솔은 Cloud Volumes ONTAP 시스템 및 해당 시스템과 연결된 Google Cloud 리소스에 레이블을 추가합니다. 시스템을 생성할 때 사용자 인터페이스에서 최대 4개의 라벨을 추가할 수 있으며, 시스템을 생성한 후에 라벨을 더 추가할 수 있습니다. API는 시스템을 생성할 때 레이블을 4개로 제한하지 않습니다. 라벨에 대한 정보는 다음을 참조하세요. "Google Cloud 문서: 리소스 레이블 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.
프로젝트 편집	Cloud Volumes ONTAP 저장할 프로젝트를 선택하세요. 기본 프로젝트는 콘솔의 프로젝트입니다. 드롭다운 목록에 추가 프로젝트가 표시되지 않으면 아직 서비스 계정을 다른 프로젝트와 연결하지 않은 것입니다. Google Cloud Console로 이동하여 IAM 서비스를 열고 해당 프로젝트를 선택하세요. Console에서 사용하는 역할로 서비스 계정을 해당 프로젝트에 추가합니다. 각 프로젝트에 대해 이 단계를 반복해야 합니다. 이는 콘솔에 대해 설정한 서비스 계정입니다."이 페이지에 설명된 대로" . *구독 추가*를 클릭하여 선택한 자격 증명을 구독과 연결합니다. 사용량에 따라 요금을 지불하는 Cloud Volumes ONTAP 시스템을 만들려면 Google Cloud 마켓플레이스에서 Cloud Volumes ONTAP 구독과 연결된 Google Cloud 프로젝트를 선택해야 합니다. 참조하다 "Google Cloud 자격 증명과 마켓플레이스 구독 연결" .

6. 서비스: 이 시스템에서 사용할 서비스를 선택하세요. 백업 및 복구를 선택하거나 NetApp Cloud Tiering 사용하려면 3단계에서 서비스 계정을 지정해야 합니다.

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

7. 위치 및 연결: 시스템에 사용할 Google Cloud 지역 및 영역을 선택하고, 방화벽 정책을 선택한 다음, 데이터 계층화를 위해 Google Cloud 스토리지에 대한 네트워크 연결을 확인하십시오.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
연결성 검증	콜드 데이터를 Google Cloud Storage 버킷에 계층화하려면 Cloud Volumes ONTAP 이 있는 서브넷을 비공개 Google 액세스로 구성해야 합니다. 지침은 다음을 참조하세요. "Google Cloud 문서: 비공개 Google 액세스 구성" .

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

8. 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"
9. 사전 구성된 패키지: 패키지 중 하나를 선택하여 Cloud Volumes ONTAP 시스템을 빠르게 배포하거나 *나만의 구성 생성*을 클릭하십시오. 사전 구성된 패키지는 선택한 Cloud Volumes ONTAP 버전에 따라 다릅니다. 예를 들어 Cloud Volumes ONTAP 9.18.1 이상 버전의 경우 NetApp Console에 Hyperdisk Balanced 디스크를 포함한 C3 VM이 포함된 패키지가 표시됩니다. 워크로드 요구 사항에 따라 IOPS 및 처리량 매개변수와 같은 구성을 수정할 수 있습니다.

   패키지 중 하나를 선택하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.
10. 라이선스: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 머신 유형을 선택합니다.

    선택한 버전에 대해 최신 릴리스 후보, 일반 공급 또는 패치 릴리스가 제공되는 경우 콘솔은 버전을 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. 예를 들어, 9.13에서 9.14로 전달되지 않습니다.
11. 기본 스토리지 리소스: 초기 집계에 대한 설정을 선택합니다. 디스크 유형과 각 디스크의 크기입니다.

    디스크 유형은 초기 볼륨을 위한 것입니다. 이후 볼륨에는 다른 디스크 유형을 선택할 수 있습니다.

    디스크 크기는 초기 집계의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 콘솔이 생성하는 모든 추가 집계에 적용됩니다. 고급 할당 옵션을 사용하면 다른 디스크 크기를 사용하는 집계를 만들 수 있습니다.

    디스크 유형 및 크기 선택에 대한 도움말은 다음을 참조하세요."Google Cloud에서 시스템 크기 조정" .
12. 플래시 캐시, 쓰기 속도 및 **WORM**:
    a. 필요한 경우 **Flash Cache***를 활성화하거나 ***Normal** 또는 **High** 쓰기 속도를 선택하십시오.

    ```
    https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-gcp.html#flash-cache-support["Flash Cache"^]와 xref:{relative_path}concept-write-speed.html["쓰기 속도"]에 대해 자세히 알아보세요.
    ```

높은 쓰기 속도 옵션을 통해 높은 쓰기 속도와 8,896바이트의 더 높은 최대 전송 단위(MTU)를 사용할 수 있습니다. 또한, 8,896의 더 높은 MTU는 배포를 위해 VPC-1, VPC-2, VPC-3을 선택해야 합니다. VPC-1, VPC-2 및 VPC-3에 대한 자세한 내용은 다음을 참조하세요. "VPC-1, VPC-2 및 VPC-3에 대한 규칙" .

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.

13. **Google Cloud Platform**의 데이터 계층화: 초기 집계에서 데이터 계층화를 활성화할지 여부를 선택하고, 계층화된 데이터에 대한 스토리지 클래스를 선택한 다음, 사전 정의된 스토리지 관리자 역할(Cloud Volumes ONTAP 9.7 이상에 필요)이 있는 서비스 계정을 선택하거나, Google Cloud 계정(Cloud Volumes ONTAP 9.6에 필요)을 선택합니다.

다음 사항에 유의하세요.

- 콘솔은 Cloud Volumes ONTAP 인스턴스에 서비스 계정을 설정합니다. 이 서비스 계정은 Google Cloud Storage 버킷에 대한 데이터 계층화 권한을 제공합니다. 계층화 서비스 계정의 사용자로 콘솔 에이전트 서비스 계정을 반드시 추가해야 합니다. 그렇지 않으면 콘솔에서 해당 계정을 선택할 수 없습니다.
- Google Cloud 계정 추가에 대한 도움말은 다음을 참조하세요. "9.6을 사용하여 데이터 계층화를 위한 Google Cloud 계정 설정 및 추가" .
- 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
- 데이터 계층화를 비활성화한 경우 후속 애그리게이트에서 다시 활성화할 수 있지만, 시스템을 종료하고 Google Cloud Console에서 서비스 계정을 추가해야 합니다.

"데이터 계층화에 대해 자세히 알아보세요" .

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

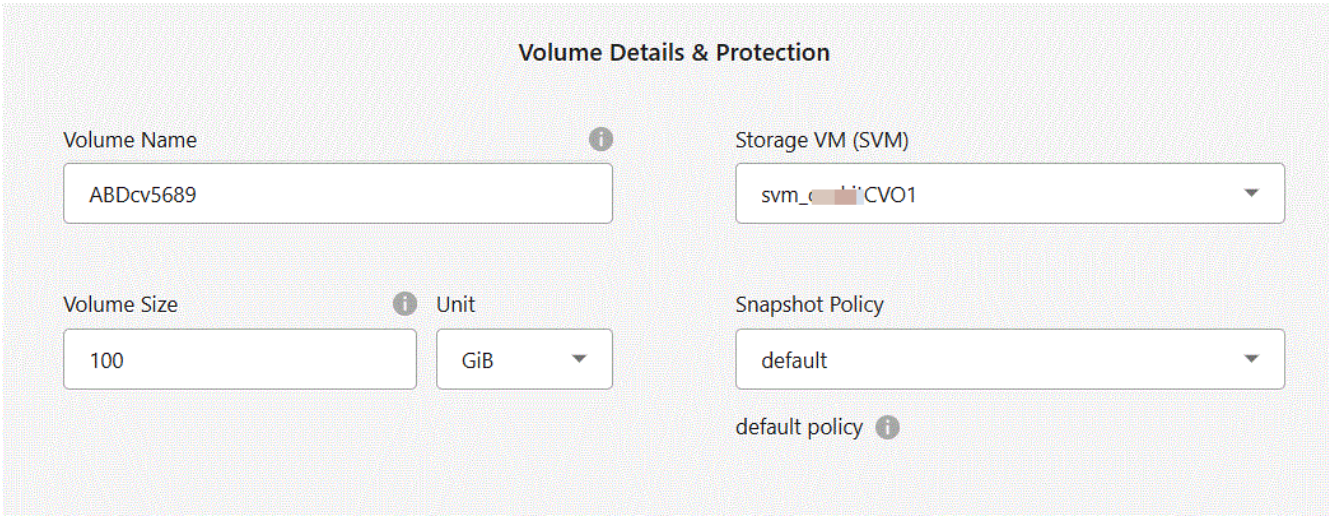
"지원되는 클라이언트 프로토콜 및 버전에 대해 알아보세요" .

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.

필드	설명
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.



15. **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. Google Managed Active Directory를 구성하는 경우 기본적으로 169.254.169.254 IP 주소를 사용하여 AD에 액세스할 수 있습니다.
가입할 Active Directory 도메인	CIFS 서버에 가입하려는 Active Directory(AD) 도메인의 FQDN입니다.

필드	설명
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 Google Managed Microsoft AD를 구성하려면 이 필드에 *OU=Computers,OU=Cloud*를 입력합니다.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud 문서: Google Managed Microsoft AD의 조직 단위"^]
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. 자세한 내용은 다음을 참조하세요. "NetApp Console 자동화 문서" 자세한 내용은. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 만든 후에는 구성할 수 없습니다.

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

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

17. 검토 및 승인: 선택 사항을 검토하고 확인합니다.

    a. 구성에 대한 세부 정보를 검토하세요.

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

    c. 이해합니다... 확인란을 선택하세요.

    d. *이동*을 클릭하세요.

결과

콘솔은 Cloud Volumes ONTAP 시스템을 배포합니다. 감사 페이지에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 시스템 배포 중 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 Google Cloud 포털에서 시스템에서 생성된 Cloud Volumes ONTAP 구성(예: 시스템 태그 및 Google Cloud 리소스에 설정된 레이블)을 수정하지 마십시오. 이러한 구성을 변경하면 예기치 않은 동작이나 데이터 손실이 발생할 수 있습니다.

Google Cloud에서 HA 쌍 시작

Google Cloud에서 Cloud Volumes ONTAP 시작하기 위한 시스템을 콘솔에서 만듭니다.

단계

1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *저장소 > 시스템*을 클릭하고 화면의 지시를 따르세요.
3. 위치 선택: *Google Cloud*와 * Cloud Volumes ONTAP HA*를 선택합니다.
4. 세부 정보 및 자격 증명: 프로젝트를 선택하고, 클러스터 이름을 지정하고, 선택적으로 서비스 계정을 선택하고, 선택적으로 레이블을 추가한 다음 자격 증명을 지정합니다.

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

필드	설명
시스템 이름	콘솔은 시스템 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Google Cloud VM 인스턴스의 이름을 지정합니다. 해당 옵션을 선택하면 사전 정의된 보안 그룹의 접두사로도 이름이 사용됩니다.
서비스 계정 이름	사용할 계획이라면"NetApp Cloud Tiering" 또는 "백업 및 복구" 서비스를 사용하려면 서비스 계정 스위치를 활성화한 다음 미리 정의된 스토리지 관리자 역할이 있는 서비스 계정을 선택해야 합니다.
라벨 추가	라벨은 Google Cloud 리소스에 대한 메타데이터입니다. 콘솔은 Cloud Volumes ONTAP 시스템 및 해당 시스템과 연결된 Google Cloud 리소스에 레이블을 추가합니다. 시스템을 생성할 때 사용자 인터페이스에서 최대 4개의 라벨을 추가할 수 있으며, 시스템을 생성한 후에 라벨을 더 추가할 수 있습니다. API는 시스템을 생성할 때 레이블을 4개로 제한하지 않습니다. 라벨에 대한 정보는 다음을 참조하세요. "Google Cloud 문서: 리소스 레이블 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.

필드	설명
프로젝트 편집	Cloud Volumes ONTAP 저장할 프로젝트를 선택하세요. 기본 프로젝트는 콘솔 프로젝트입니다. 드롭다운 목록에 추가 프로젝트가 표시되지 않으면 아직 서비스 계정을 다른 프로젝트와 연결하지 않은 것입니다. Google Cloud Console로 이동하여 IAM 서비스를 열고 해당 프로젝트를 선택하세요. Console에서 사용하는 역할로 서비스 계정을 해당 프로젝트에 추가합니다. 각 프로젝트에 대해 이 단계를 반복해야 합니다. 이는 콘솔에 대해 설정한 서비스 계정입니다."이 페이지에 설명된 대로" . *구독 추가*를 클릭하여 선택한 자격 증명을 구독과 연결합니다. 사용량에 따라 요금을 지불하는 Cloud Volumes ONTAP 시스템을 만들려면 Google Cloud Marketplace에서 Cloud Volumes ONTAP 구독과 연결된 Google Cloud 프로젝트를 선택해야 합니다. 참조하다 "Google Cloud 자격 증명과 마켓플레이스 구독 연결" .

5. 서비스: 이 시스템에서 사용할 서비스를 선택하세요. 백업 및 복구를 선택하거나 NetApp Cloud Tiering 사용하려면 3단계에서 서비스 계정을 지정해야 합니다.

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

6. **HA** 배포 모델: HA 구성에 대해 여러 영역(권장) 또는 단일 영역을 선택합니다. 그런 다음 지역과 영역을 선택합니다.

   "HA 배포 모델에 대해 자세히 알아보세요" .

7. 연결성: HA 구성을 위해 4개의 다른 VPC를 선택하고, 각 VPC에 서브넷을 선택한 다음 방화벽 정책을 선택합니다.

   "네트워킹 요구 사항에 대해 자세히 알아보세요" .

   다음 표에서는 지침이 필요할 수 있는 필드를 설명합니다.

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

8. 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" .
9. 사전 구성된 패키지: Cloud Volumes ONTAP 시스템을 빠르게 배포하려면 패키지 중 하나를 선택하거나 *내 구성 만들기*를 클릭하세요.

   패키지 중 하나를 선택하는 경우 볼륨만 지정하고 구성을 검토하여 승인하기만 하면 됩니다.
10. 라이선스: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 머신 유형을 선택합니다.

    선택한 버전에 대해 최신 릴리스 후보, 일반 공급 또는 패치 릴리스가 제공되는 경우 콘솔은 버전을 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).
11. 기본 스토리지 리소스: 초기 집계에 대한 설정을 선택합니다. 디스크 유형과 각 디스크의 크기입니다.

    디스크 유형은 초기 볼륨을 위한 것입니다. 이후 볼륨에는 다른 디스크 유형을 선택할 수 있습니다.

    디스크 크기는 초기 집계의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 콘솔이 생성하는 모든 추가 집계에 적용됩니다. 고급 할당 옵션을 사용하면 다른 디스크 크기를 사용하는 집계를 만들 수 있습니다.

    디스크 유형 및 크기 선택에 대한 도움말은 다음을 참조하세요."Google Cloud에서 시스템 크기 조정" .
12. 플래시 캐시, 쓰기 속도 및 **WORM**:
    a. 필요한 경우 **Flash Cache***를 활성화하거나 ***Normal** 또는 **High** 쓰기 속도를 선택하십시오.

    ```
    https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-gcp.html#flash-cache-support["Flash Cache"^]와 xref:{relative_path}concept-write-speed.html["쓰기 속도"]에 대해 자세히 알아보세요.
    ```

    높음 쓰기 속도 옵션을 사용하면 n2-standard-16, n2-standard-32, n2-standard-48 및 n2-standard-64 인스턴스 유형에서 높은 쓰기 속도와 8,896바이트의 더 높은 최대 전송 단위(MTU)를 사용할 수 있습니다. 또한, 8,896의 더 높은 MTU는 배포를 위해 VPC-1, VPC-2, VPC-3을 선택해야 합니다. 높은 쓰기 속도와 8,896의 MTU는 기능에 따라 달라지며 구성된 인스턴스 내에서 개별적으로 비활성화할 수 없습니다. VPC-1, VPC-2 및 VPC-3에 대한 자세한 내용은 다음을 참조하세요. "VPC-1, VPC-2 및 VPC-3에 대한 규칙" .

    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.

13. **Google Cloud**의 데이터 계층화: 초기 집계에서 데이터 계층화를 활성화할지 여부를 선택하고, 계층화된 데이터에 대한 스토리지 클래스를 선택한 다음, 사전 정의된 스토리지 관리자 역할이 있는 서비스 계정을 선택합니다.

    다음 사항에 유의하세요.

    - 콘솔은 Cloud Volumes ONTAP 인스턴스에 서비스 계정을 설정합니다. 이 서비스 계정은 Google Cloud Storage 버킷에 대한 데이터 계층화 권한을 제공합니다. 계층화 서비스 계정의 사용자로 콘솔 에이전트 서비스 계정을 반드시 추가해야 합니다. 그렇지 않으면 콘솔에서 해당 계정을 선택할 수 없습니다.
    - 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
    - 데이터 계층화를 비활성화한 경우 후속 애그리게이트에서 다시 활성화할 수 있지만, 시스템을 종료하고 Google Cloud Console에서 서비스 계정을 추가해야 합니다.

      "데이터 계층화에 대해 자세히 알아보세요" .

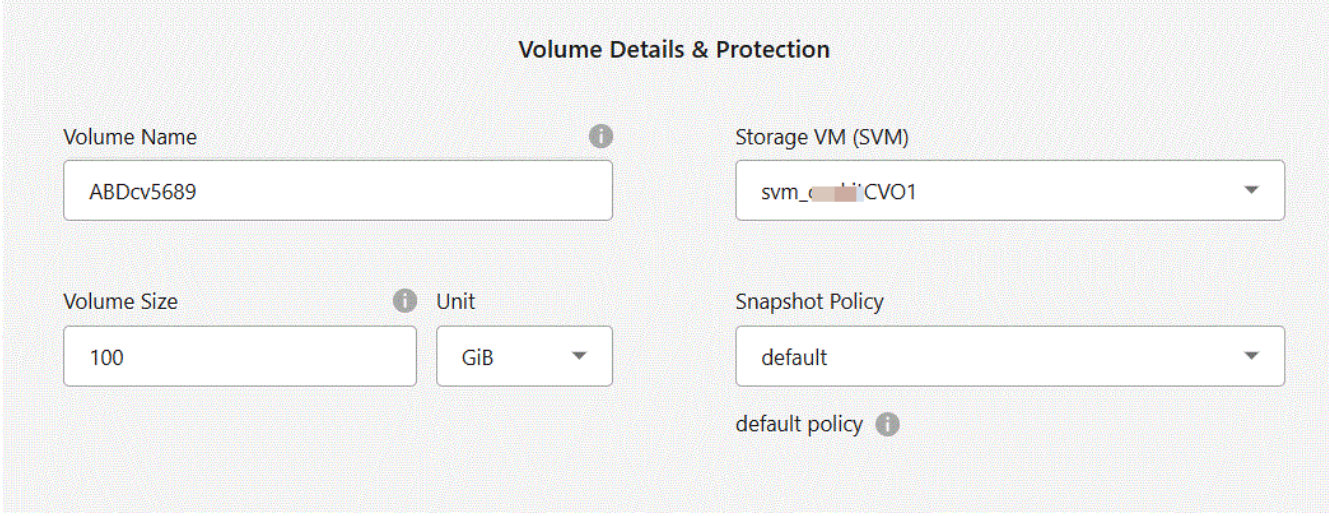
14. 볼륨 만들기: 새 볼륨에 대한 세부 정보를 입력하거나 *건너뛰기*를 클릭합니다.

    "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.



15. **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. Google Managed Active Directory를 구성하는 경우 기본적으로 169.254.169.254 IP 주소를 사용하여 AD에 액세스할 수 있습니다.
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 Google Managed Microsoft AD를 구성하려면 이 필드에 *OU=Computers,OU=Cloud*를 입력합니다.https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud 문서: Google Managed Microsoft AD의 조직 단위"^]
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.

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

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

17. 검토 및 승인: 선택 사항을 검토하고 확인합니다.

    a. 구성에 대한 세부 정보를 검토하세요.

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

    c. 이해합니다... 확인란을 선택하세요.

    d. *이동*을 클릭하세요.

결과

콘솔은 Cloud Volumes ONTAP 시스템을 배포합니다. 감사 페이지에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 시스템 배포 중 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 Google Cloud 포털에서 시스템에서 생성된 Cloud Volumes ONTAP 구성(예: 시스템 태그 및 Google Cloud 리소스에 설정된 레이블)을 수정하지 마십시오. 이러한 구성을 변경하면 예기치 않은 동작이나 데이터 손실이 발생할 수 있습니다.

관련 링크

- "Google Cloud에서 Cloud Volumes ONTAP 구성 계획"

Google Cloud Platform 이미지 검증

Cloud Volumes ONTAP 에서 **Google Cloud** 이미지가 검증되는 방식을 알아보세요**.**

Google Cloud 이미지 검증은 향상된 NetApp 보안 요구 사항을 준수합니다. 이 작업을 위해 특별히 생성된 개인 키를 사용하여 이미지에 서명하는 방식으로 이미지를 생성하는 스크립트가 변경되었습니다. Google Cloud 이미지의 무결성은 다음을 통해 다운로드할 수 있는 서명된 다이제스트 및 Google Cloud 공개 인증서를 사용하여 확인할 수 있습니다. "NSS" 특정 릴리스에 대한.

Google Cloud 이미지 검증은 Cloud Volumes ONTAP 소프트웨어 버전 9.13.0 이상에서 지원됩니다.

Google Cloud 이미지를 **Cloud Volumes ONTAP** 용 **RAW** 포맷으로 변환

새로운 인스턴스, 업그레이드를 배포하는 데 사용되는 이미지 또는 기존 이미지에서 사용되는

이미지는 다음을 통해 클라이언트와 공유됩니다. "NetApp 지원 사이트(NSS)" . 서명된 다이제스트와 인증서는 NSS 포털을 통해 다운로드할 수 있습니다. NetApp 지원팀에서 공유한 이미지에 해당하는 올바른 릴리스에 대한 다이제스트와 인증서를 다운로드하고 있는지 확인하세요. 예를 들어, 9.13.0 이미지에는 9.13.0 서명된 다이제스트와 NSS에서 사용할 수 있는 인증서가 포함됩니다.

왜 이 단계가 필요한가요?

Google Cloud의 이미지는 직접 다운로드할 수 없습니다. 서명된 다이제스트와 인증서에 대해 이미지를 검증하려면 두 파일을 비교하고 이미지를 다운로드할 수 있는 메커니즘이 필요합니다. 이를 위해서는 이미지를 disk.raw 형식으로 내보내거나 변환하고 그 결과를 Google Cloud의 스토리지 버킷에 저장해야 합니다. disk.raw 파일은 이 과정에서 tar와 gzip으로 압축됩니다.

사용자/서비스 계정에는 다음을 수행할 수 있는 권한이 필요합니다.

- Google 스토리지 버킷에 액세스
- Google Storage 버킷에 쓰기
- 클라우드 빌드 작업 생성(내보내기 프로세스 중 사용)
- 원하는 이미지에 접근
- 이미지 내보내기 작업 만들기

이미지를 확인하려면 disk.raw 형식으로 변환한 다음 다운로드해야 합니다.

Google Cloud 명령줄을 사용하여 **Google Cloud** 이미지를 내보냅니다.

이미지를 Cloud Storage로 내보내는 가장 좋은 방법은 다음을 사용하는 것입니다. "gcloud compute 이미지 내보내기 명령" . 이 명령은 제공된 이미지를 가져와서 tar와 gzip으로 압축된 disk.raw 파일로 변환합니다. 생성된 파일은 대상 URL에 저장되며, 확인을 위해 다운로드할 수 있습니다.

이 작업을 실행하려면 사용자/계정에 원하는 버킷에 액세스하고 쓰기 권한이 있어야 하며, 이미지를 내보내고, 클라우드 빌드(Google에서 이미지를 내보내는 데 사용)에 대한 권한이 있어야 합니다.

gcloud를 사용하여 **Google Cloud** 이미지 내보내기

클릭하여 표시

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

압축 파일 추출

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

Google Cloud를 통해 이미지를 내보내는 방법에 대한 자세한 내용은 다음을 참조하세요. "이미지 내보내기에 대한 Google Cloud 문서" .

이미지 서명 검증

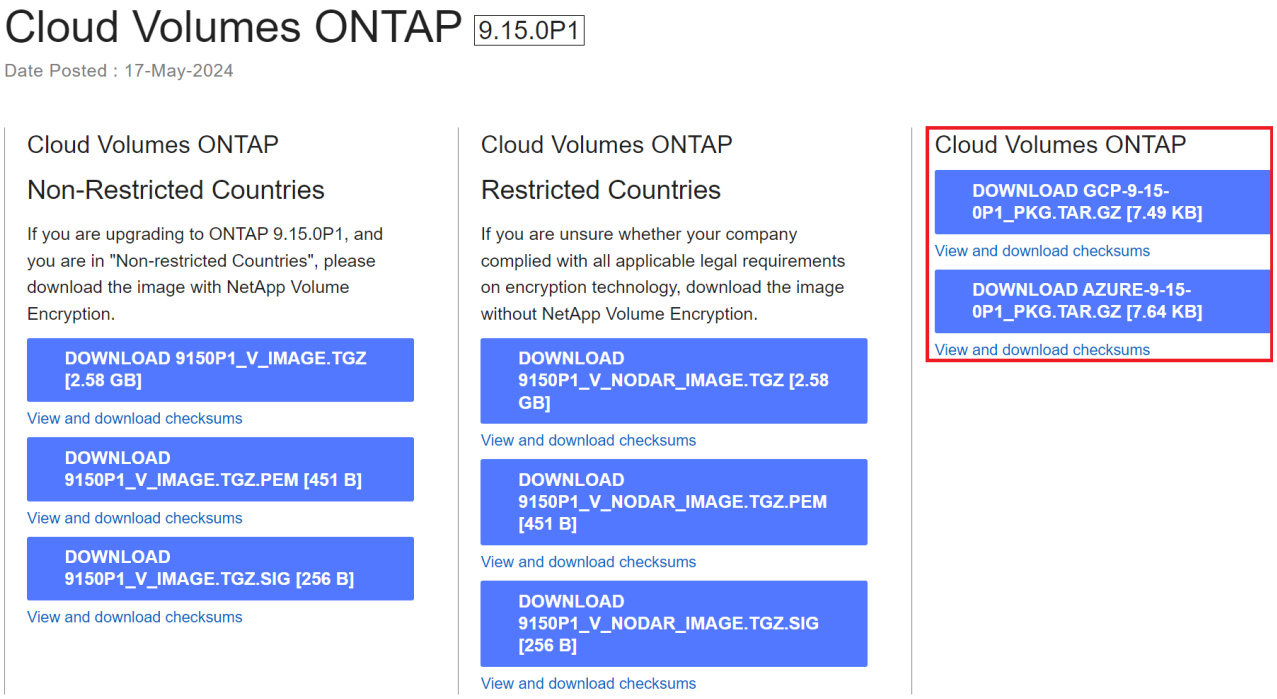
Cloud Volumes ONTAP 에 대한 **Google Cloud** 이미지 서명 확인

내보낸 Google Cloud 서명 이미지를 확인하려면 NSS에서 이미지 다이제스트 파일을 다운로드하여 disk.raw 파일과 다이제스트 파일 내용을 검증해야 합니다.

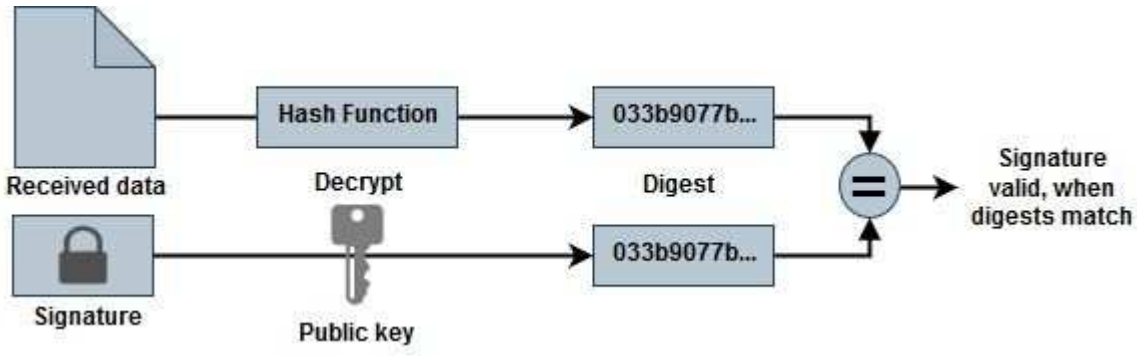
서명된 이미지 검증 워크플로 요약

다음은 Google Cloud 서명 이미지 검증 워크플로 프로세스에 대한 개요입니다.

- 에서 "NSS" 다음 파일이 포함된 Google Cloud 보관 파일을 다운로드하세요.
  - 서명된 다이제스트(.sig)
  - 공개 키(.pem)를 포함하는 인증서
  - 인증서 체인(.pem)



- 변환된 disk.raw 파일을 다운로드하세요
- 인증서 체인을 사용하여 인증서 검증
- 공개 키가 포함된 인증서를 사용하여 서명된 다이제스트를 검증합니다.
  - 공개 키를 사용하여 서명된 다이제스트를 복호화하여 이미지 파일의 다이제스트를 추출합니다.
  - 다운로드한 disk.raw 파일의 다이제스트를 만듭니다.
  - 검증을 위해 두 개의 다이제스트 파일을 비교합니다.



OpenSSL을 사용하여 **Cloud Volumes ONTAP** 에 대한 **Google Cloud** 이미지 **disk.raw** 파일을 확인합니다**.**

Google Cloud에서 다운로드한 disk.raw 파일을 다이제스트 파일 콘텐츠와 비교하여 확인할 수 있습니다. "NSS" OpenSSL을 사용합니다.

이미지를 검증하는 OpenSSL 명령은 Linux, macOS, Windows 시스템과 호환됩니다.

단계

1. OpenSSL을 사용하여 인증서를 확인합니다.

클릭하여 표시

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
          e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
          22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
          38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
          fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
          bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. 다운로드한 disk.raw 파일, 서명, 인증서를 디렉토리에 넣습니다.
3. OpenSSL을 사용하여 인증서에서 공개 키를 추출합니다.
4. 추출된 공개 키를 사용하여 서명을 복호화하고 다운로드한 disk.raw 파일의 내용을 확인합니다.

클릭하여 표시

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```