Google Cloud에서 시작하기

Cloud Volumes ONTAP

NetApp
December 10, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/storage-management-cloud-volumes-ontap/task-getting-started-gcp.html on December 10, 2025. Always check docs.netapp.com for the latest.

목차

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.

"GCP의 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.

"GCP의 Cloud Volumes ONTAP 대한 스토리지 한도"

GCP에서 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"

GCP 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)" .

GCP 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

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

단일 노드 시스템에 대한 네트워크 정보

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

여러 영역의 **HA** 쌍에 대한 네트워크 정보

GCP 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

GCP 정보	당신의 가치
지역	
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 특정 요구 사항

단일 노드 시스템을 배포하려면 네트워킹이 다음 요구 사항을 충족하는지 확인하세요.

하나의 VPC

단일 노드 시스템에는 하나의 가상 사설 클라우드(VPC)가 필요합니다.

개인 IP 주소

Google Cloud의 단일 노드 시스템의 경우 콘솔은 다음에 개인 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.

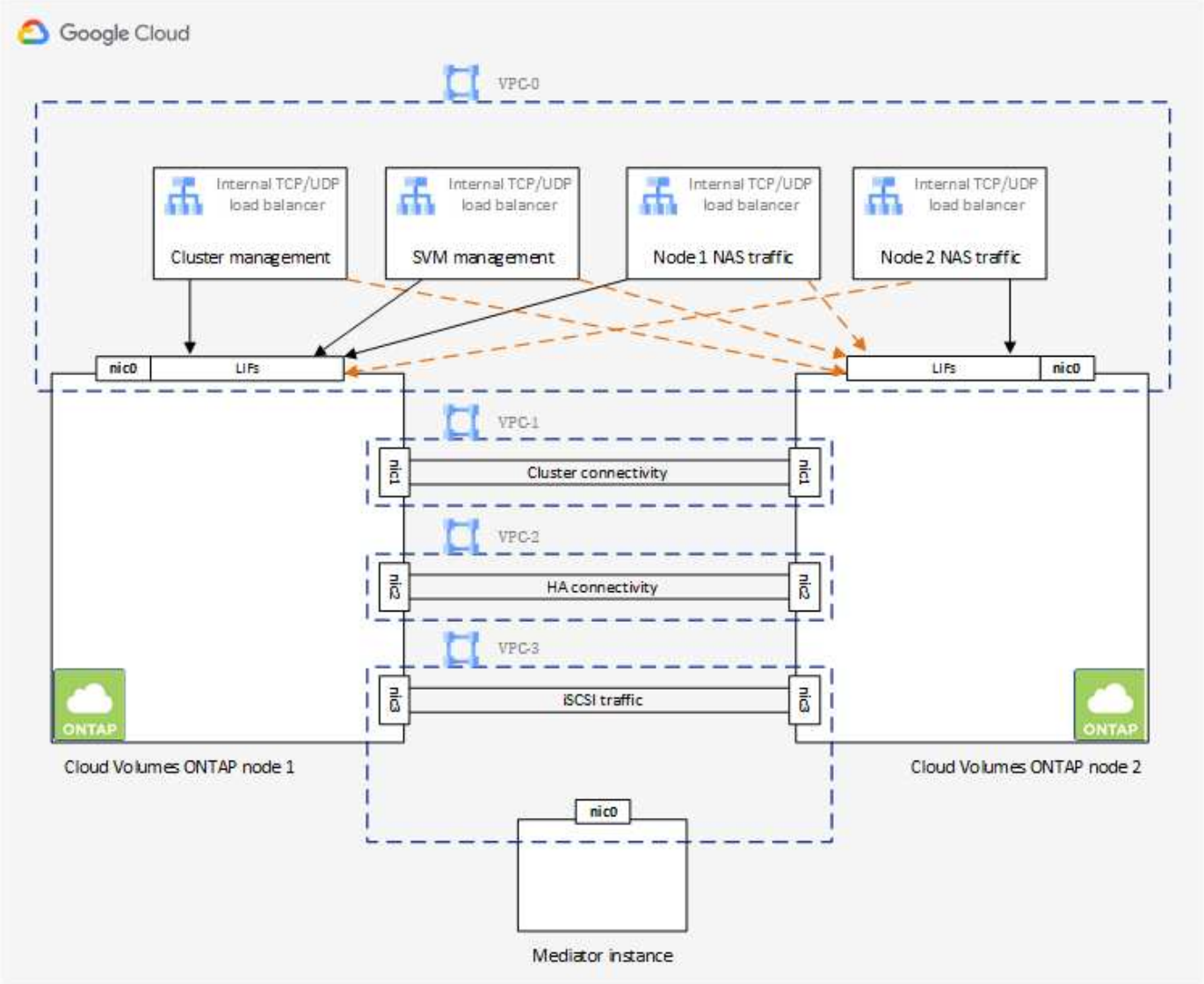
  이 배포 모델을 사용하면 영역 간에 데이터 유출 요금이 발생하지 않으므로 비용이 절감됩니다.

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 ONTAP 에 할당된 LIF 수는 단일 노드 시스템을 배포하는지 아니면 HA 쌍을 배포하는지에 따라 달라집니다. LIF는 물리적 포트와 연결된 IP 주소입니다. SnapCenter 와 같은 관리 도구에는 SVM 관리 LIF가 필요합니다.

- 단일 노드 콘솔은 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 VPC이거나 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://www.googleapis.com/compute/v1/projects/ \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://www.googleapis.com/deploymentmanager/v2/projects \ https://compute.googleapis.com/compute/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
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

규약	포트	목적
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 콘솔에서 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 ONTAP 과 콘솔은 모두 NetApp 에서 관리하는 GCP 내 프로젝트의 이미지를 사용합니다. 조직 내에서 호스팅되지 않은 이미지 사용을 차단하는 정책이 있는 경우, 이는 콘솔 에이전트와 Cloud Volumes ONTAP 의 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

정책은 VPC 서비스 제어 규칙 세트에 대한 예외를 허용합니다. 정책에 대한 자세한 내용은 다음을 방문하세요. "GCP VPC 서비스 제어 정책 문서" .

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.

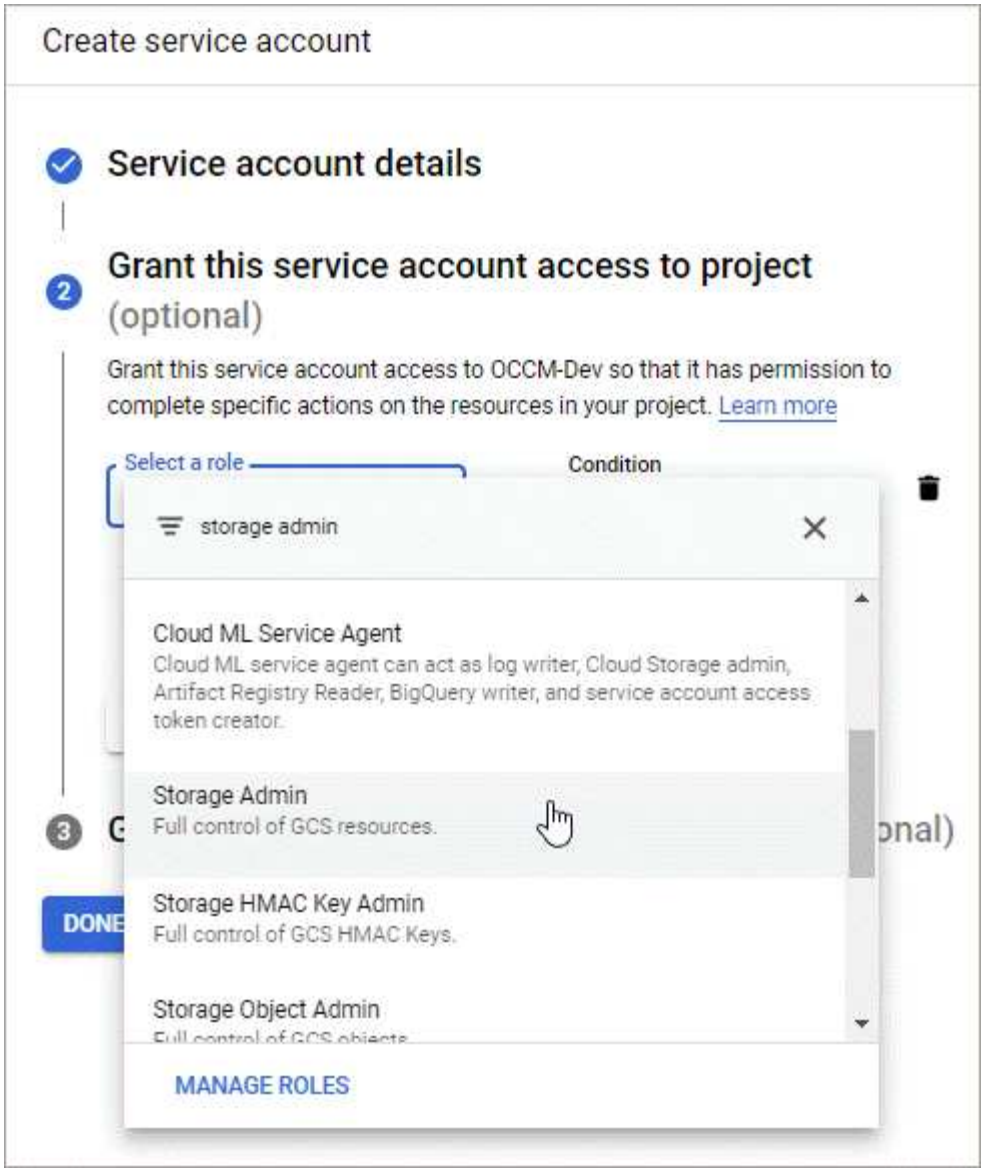
Cloud Volumes ONTAP 두 가지 목적으로 Google Cloud 서비스 계정이 필요합니다. 첫 번째는 활성화할 때입니다."데이터 계층화" Google Cloud의 저렴한 객체 스토리지에 콜드 데이터를 계층화합니다. 두 번째는 다음을 활성화할 때입니다. "NetApp Backup and Recovery" 저렴한 개체 스토리지에 볼륨을 백업합니다.

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.

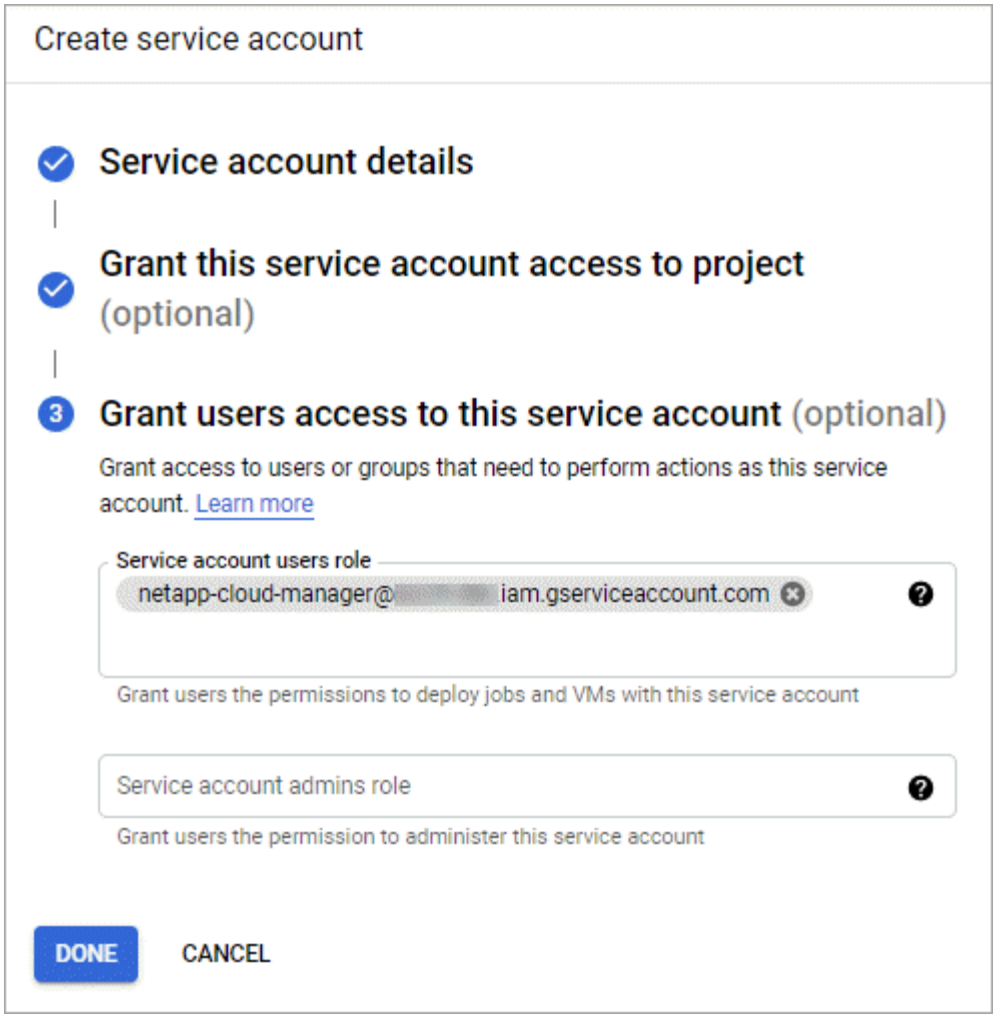
단계

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.



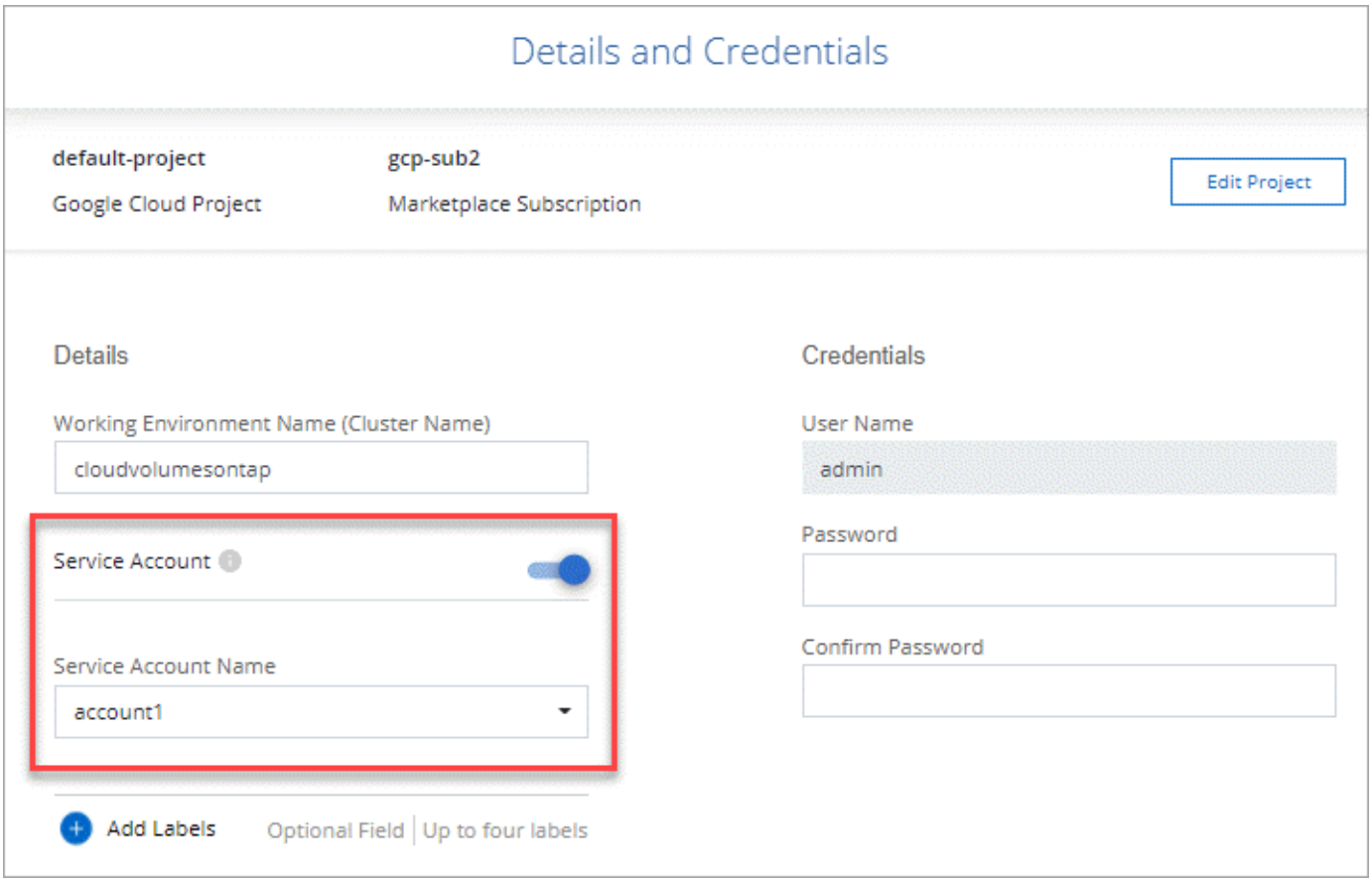
c. 사용자에게 이 서비스 계정에 대한 액세스 권한 부여: 이 새로운 서비스 계정에 콘솔 에이전트 서비스 계정을 _서비스 계정 사용자_로 추가합니다.

   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 요청과 함께 "GcpEncryption" 매개변수를 사용하세요.

   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

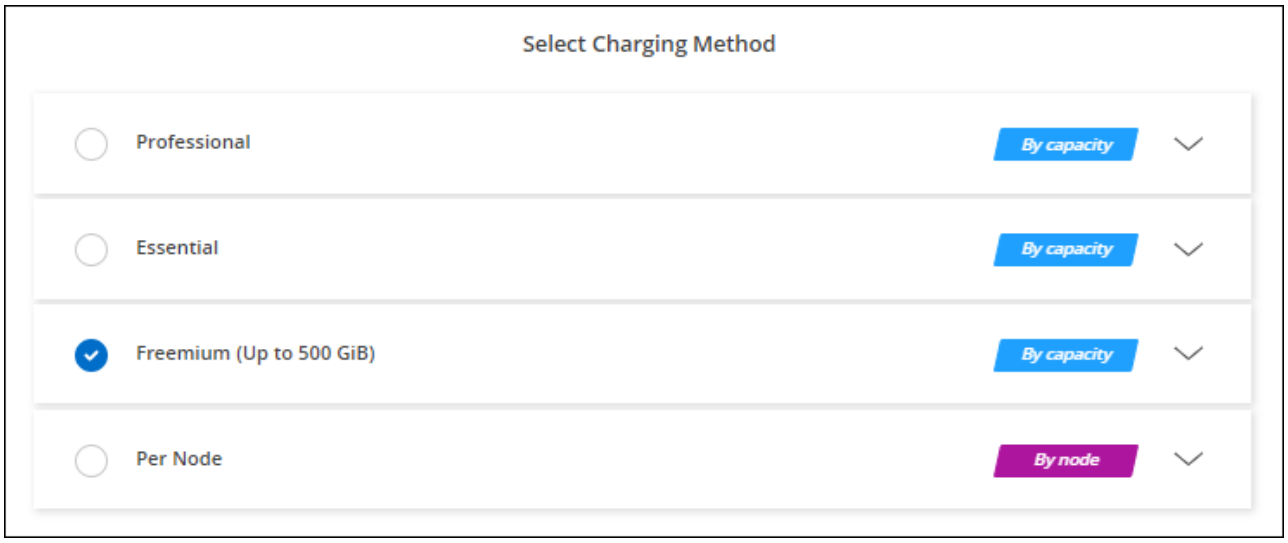
1. 왼쪽 탐색 메뉴에서 *저장소 > 관리*를 선택합니다.
2. 시스템 페이지에서 *시스템 추가*를 클릭하고 NetApp Console 의 단계를 따릅니다.

   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"

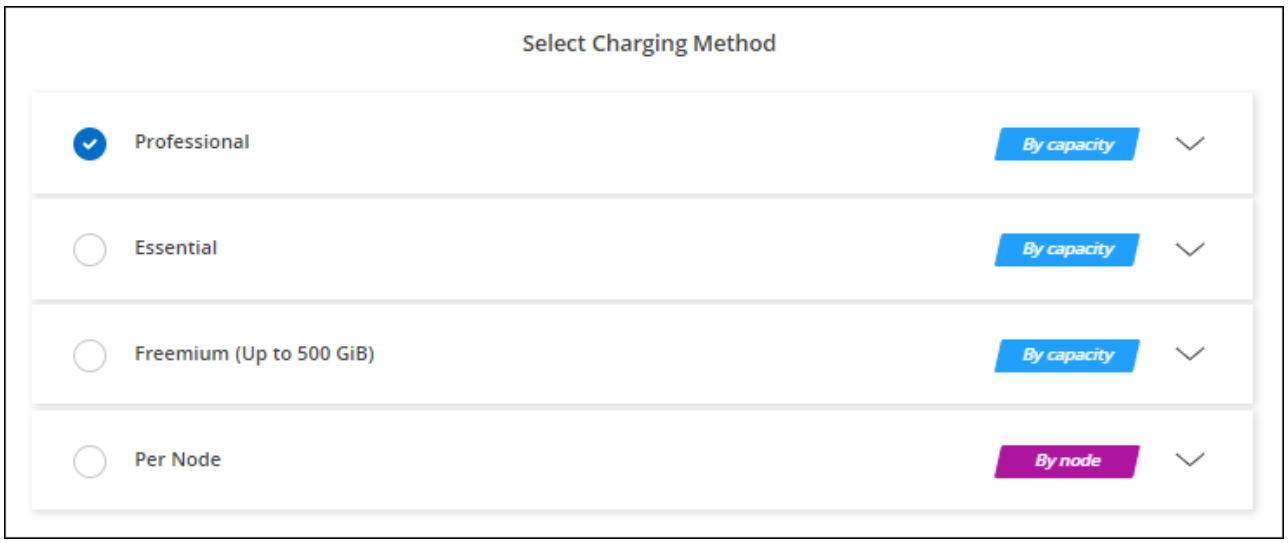
콘솔은 NetApp 지원 사이트 계정과 연결된 라이선스에 대한 세부 정보를 얻기 위해 NetApp 라이선스 서비스에 자동으로 쿼리를 보냅니다. 오류가 없으면 콘솔이 라이선스를 추가합니다.

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." .

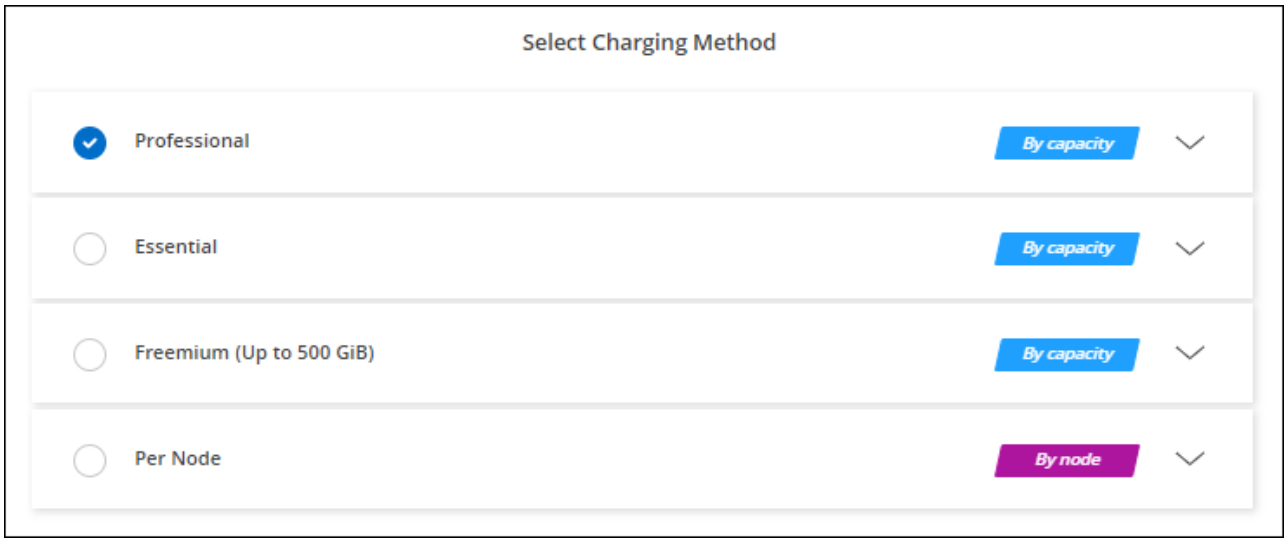
PAYGO 구독

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.

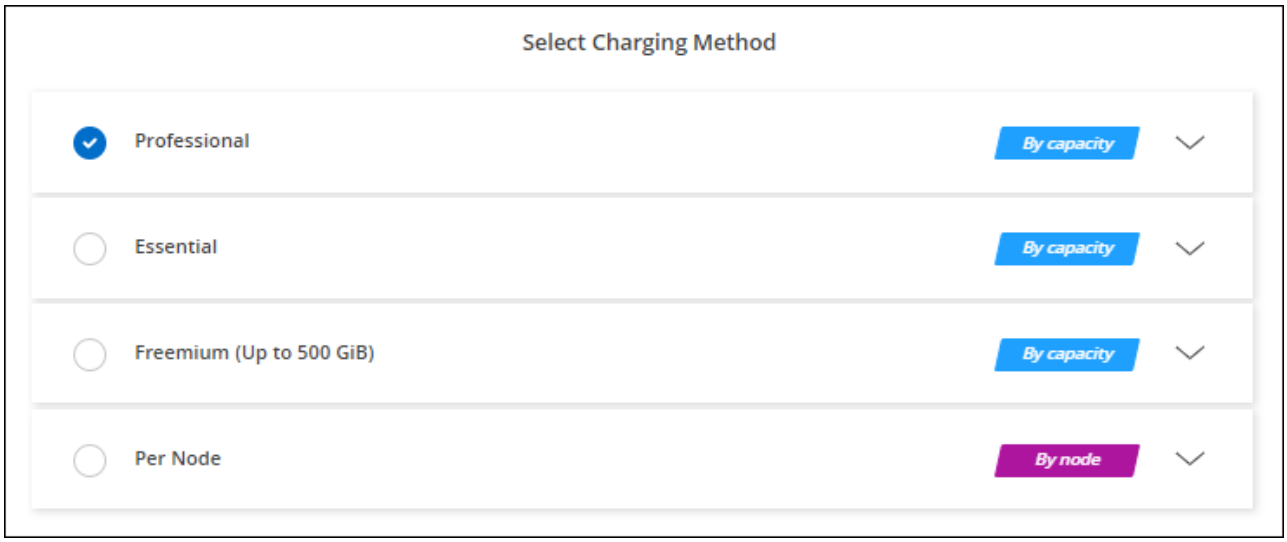
단계

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." .

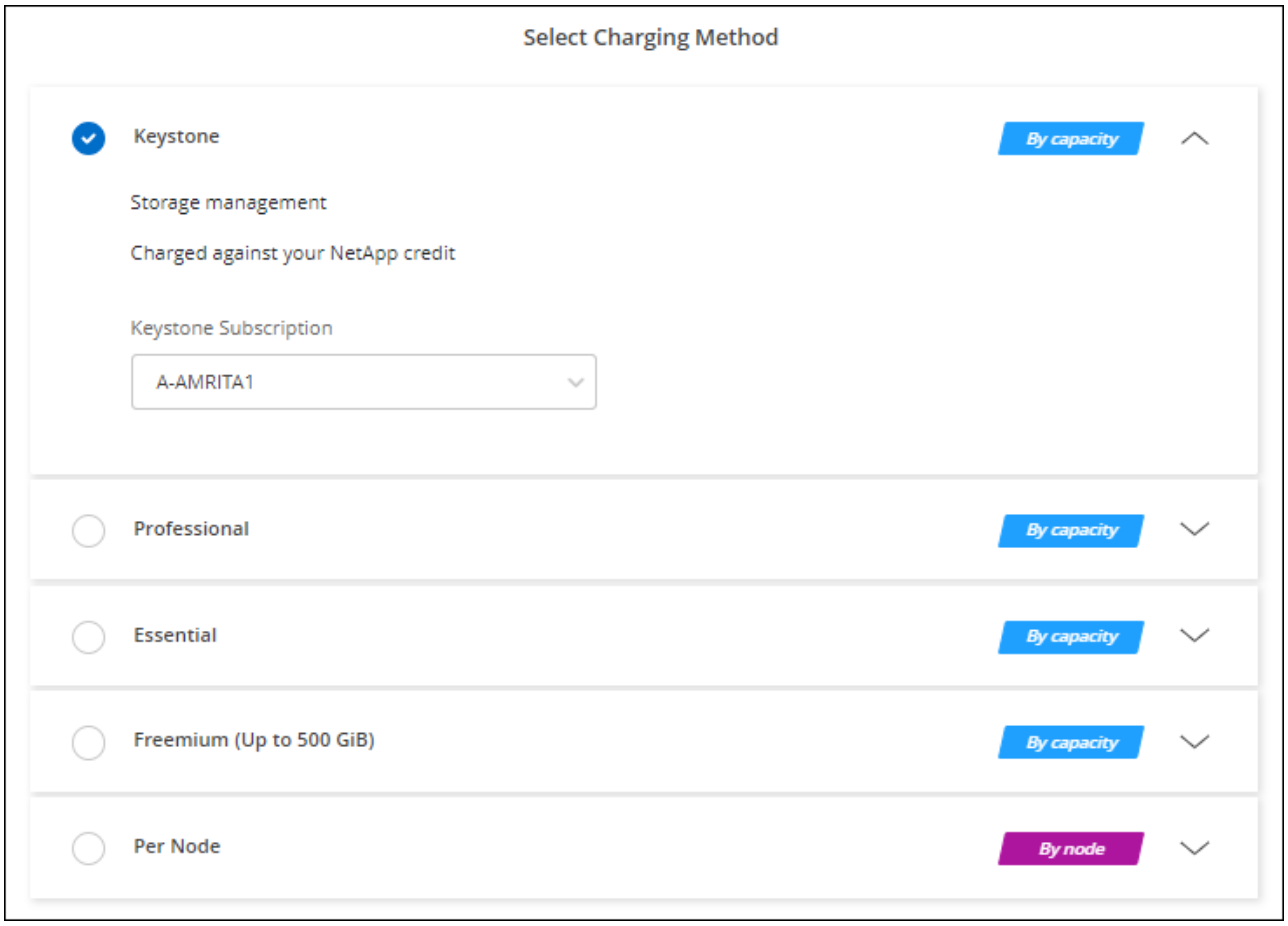
Keystone 구독

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.

- 이미 실행 중인 콘솔 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 보이지 않으면 아직 서비스 계정을 다른 프로젝트와 연결하지 않은 것입니다. Google Cloud 콘솔로 이동하여 IAM 서비스를 열고 프로젝트를 선택합니다. 콘솔에 사용하는 역할이 있는 서비스 계정을 해당 프로젝트에 추가합니다. 각 프로젝트마다 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: 위치를 선택하고, 방화벽 정책을 선택하고, 데이터 계층화를 위해 Google Cloud Storage에 대한 네트워크 연결을 확인하세요.

   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: 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. 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. 원하는 경우 *플래시 캐시*를 활성화하세요.

       Cloud Volumes ONTAP 9.13.1부터 _Flash Cache_는 n2-standard-16, n2-standard-32, n2-standard-48 및 n2-standard-64 인스턴스 유형에서 지원됩니다. 배포 후에는 Flash Cache를 비활성화할 수 없습니다.

    b. 원하는 경우 보통 또는 높음 쓰기 속도를 선택하세요.

       "쓰기 속도에 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" .

c. 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 비활성화하면 이후 집계에서 활성화할 수 있지만, 시스템을 끄고 Google Cloud 콘솔에서 서비스 계정을 추가해야 합니다.

"데이터 계층화에 대해 자세히 알아보세요" .

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

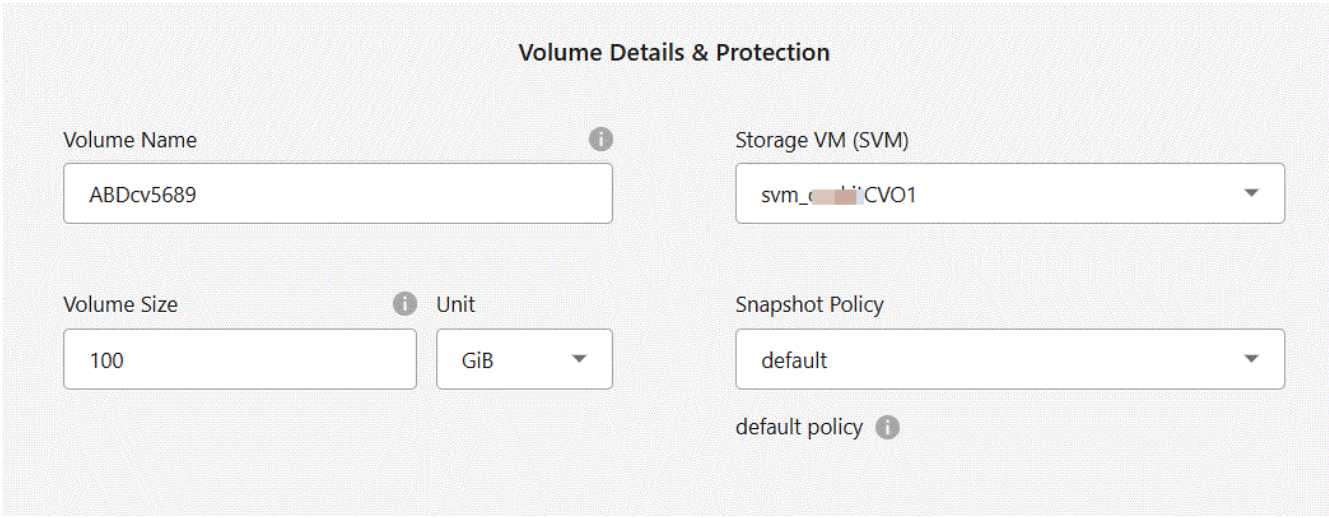
"지원되는 클라이언트 프로토콜 및 버전에 대해 알아보세요" .

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" .

배포 프로세스가 완료된 후에는 Google Cloud 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.

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 보이지 않으면 아직 서비스 계정을 다른 프로젝트와 연결하지 않은 것입니다. Google Cloud 콘솔로 이동하여 IAM 서비스를 열고 프로젝트를 선택합니다. 콘솔에 사용하는 역할이 있는 서비스 계정을 해당 프로젝트에 추가합니다. 각 프로젝트마다 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 구성을 위해 여러 개의 영역(권장) 또는 단일 영역을 선택합니다. 그런 다음 지역과 구역을 선택하세요.

   "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. 원하는 경우 *플래시 캐시*를 활성화하세요.

       Cloud Volumes ONTAP 9.13.1부터 _Flash Cache_는 n2-standard-16, n2-standard-32, n2-standard-48 및 n2-standard-64 인스턴스 유형에서 지원됩니다. 배포 후에는 Flash Cache를 비활성화할 수 없습니다.

    b. 원하는 경우 보통 또는 높음 쓰기 속도를 선택하세요.

       "쓰기 속도에 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" .

    c. 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 비활성화하면 이후 집계에서 활성화할 수 있지만, 시스템을 끄고 Google Cloud 콘솔에서 서비스 계정을 추가해야 합니다.

      "데이터 계층화에 대해 자세히 알아보세요" .

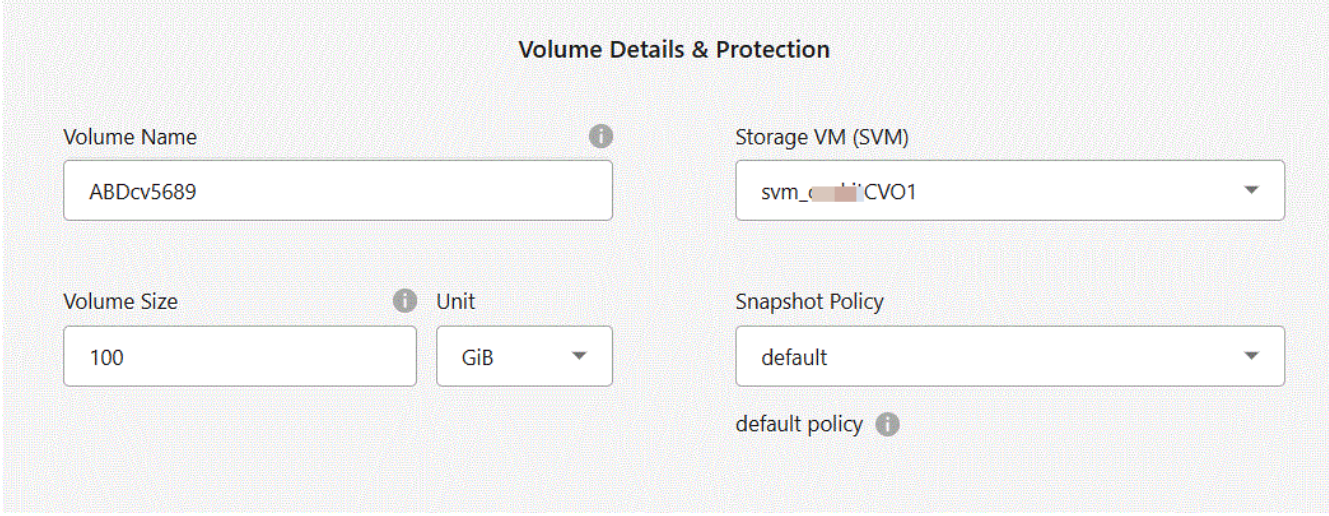
14. 볼륨 만들기: 새 볼륨에 대한 세부 정보를 입력하거나 *건너뛰기*를 클릭합니다.

    "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 시스템 생성 Cloud Volumes ONTAP 구성, 특히 시스템 태그를 수정하지 마세요. 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

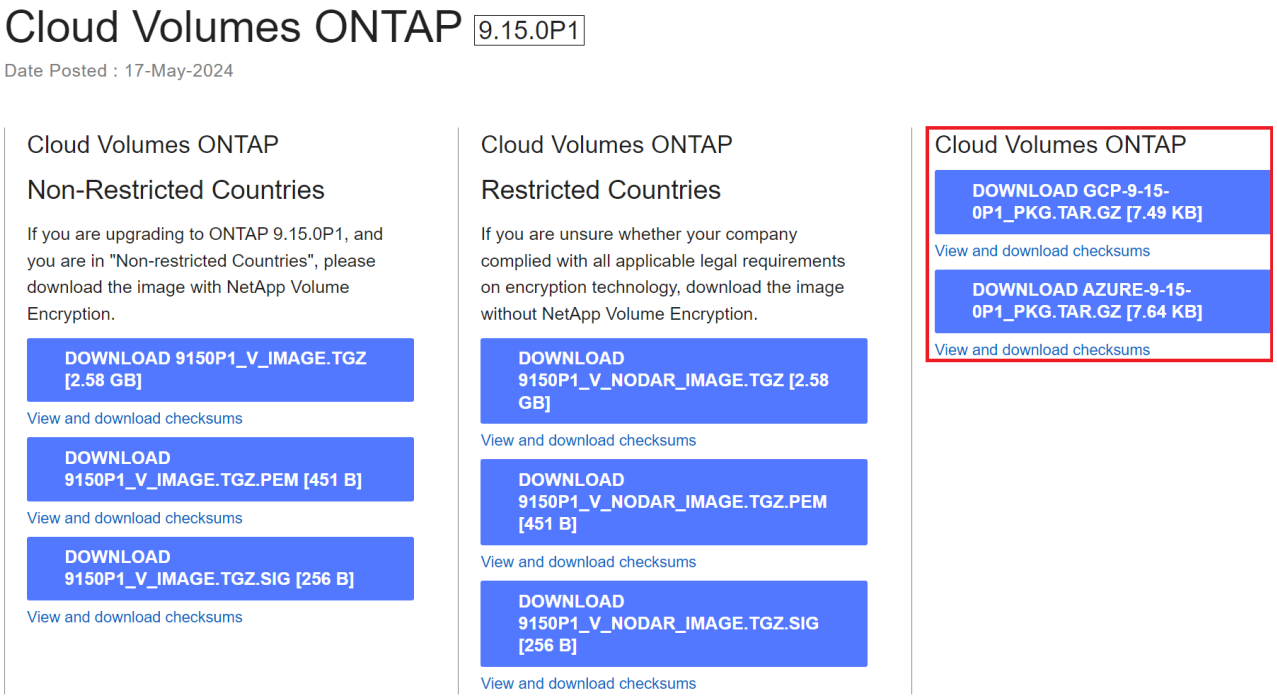
Cloud Volumes ONTAP 에 대한 **Google Cloud** 이미지 서명 확인

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

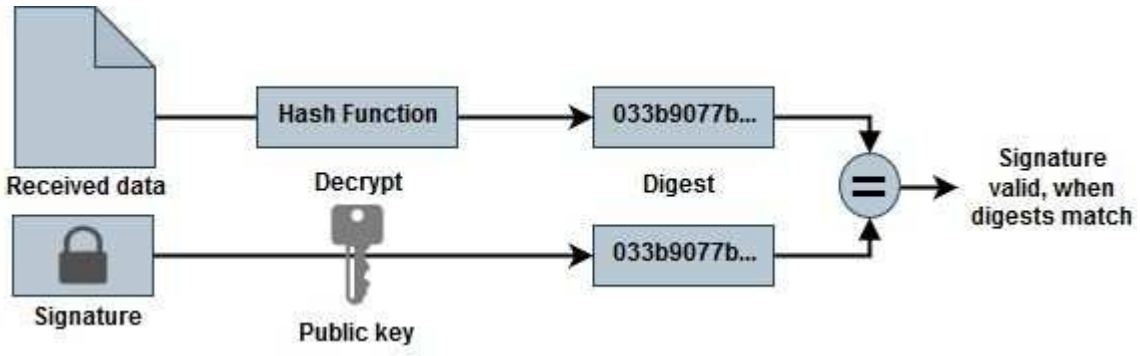
서명된 이미지 검증 워크플로 요약

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
```

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.