



## Google Cloud에서 시작하십시오 Cloud Volumes ONTAP

NetApp  
July 11, 2022

# 목차

Google Cloud에서 시작하십시오 .....	1
Google Cloud에서 Cloud Volumes ONTAP를 빠르게 시작합니다 .....	1
Google Cloud에서 Cloud Volumes ONTAP 구성을 계획하십시오 .....	2
GCP의 Cloud Volumes ONTAP에 대한 네트워킹 요구 사항 .....	5
GCP에서 VPC 서비스 제어 계획 .....	15
데이터 계층화 및 백업을 위한 서비스 계정을 생성합니다 .....	17
Cloud Volumes ONTAP에서 고객이 관리하는 암호화 키 사용 .....	20
Google Cloud에서 Cloud Volumes ONTAP에 대한 라이선스를 설정합니다 .....	21
GCP에서 Cloud Volumes ONTAP를 시작합니다 .....	26

# Google Cloud에서 시작하십시오

## Google Cloud에서 Cloud Volumes ONTAP를 빠르게 시작합니다

몇 가지 단계를 통해 Cloud Volumes ONTAP for GCP를 시작해 보십시오.

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

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

Cloud Manager는 워크로드 요구사항에 맞게 사전 구성된 패키지를 제공하거나 자체 구성을 생성할 수 있습니다. 자신의 구성을 선택하는 경우 사용 가능한 옵션을 이해해야 합니다.

["구성 계획에 대해 자세히 알아보십시오"](#).

네트워크 설정

1. VPC와 서브넷이 커넥터와 Cloud Volumes ONTAP 간의 연결을 지원하는지 확인합니다.
2. 데이터 계층화를 사용할 계획이라면 ["개인 Google 액세스를 위한 Cloud Volumes ONTAP 서브넷을 구성합니다"](#).
3. HA 쌍을 구축하는 경우 각각 고유한 서브넷이 있는 4개의 VPC가 있는지 확인합니다.
4. 공유 VPC를 사용하는 경우 Connector 서비스 계정에 \_Compute Network User\_ 역할을 제공합니다.
5. 커넥터 및 Cloud Volumes ONTAP가 여러 엔드포인트에 연결할 수 있도록 타겟 VPC에서 아웃바운드 인터넷 액세스를 활성화합니다.

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

["네트워킹 요구 사항에 대해 자세히 알아보십시오"](#).

Cloud Volumes ONTAP를 사용하려면 Google Cloud 서비스 계정이 두 가지 용도로 필요합니다. 첫 번째는 를 활성화하는 것입니다 ["데이터 계층화"](#) Google Cloud에서 콜드 데이터를 저비용 오브젝트 스토리지로 계층화합니다. 두 번째는 를 활성화하는 것입니다 ["Cloud Backup Service"](#) 볼륨을 저렴한 오브젝트 스토리지에 백업

하나의 서비스 계정을 설정하고 두 가지 용도로 사용할 수 있습니다. 서비스 계정에는 \* 스토리지 관리자 \* 역할이 있어야 합니다.

["단계별 지침을 읽습니다"](#).

["프로젝트에서 다음 Google Cloud API를 활성화합니다"](#). 이러한 API는 Connector 및 Cloud Volumes ONTAP를 구축하는 데 필요합니다.

- Cloud Deployment Manager V2 API
- 클라우드 로깅 API

- Cloud Resource Manager API를 참조하십시오
- 컴퓨팅 엔진 API
- IAM(Identity and Access Management) API

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

관련 링크

- ["Cloud Manager에서 커넥터 생성"](#)
- ["Linux 호스트에 Connector 소프트웨어 설치"](#)
- ["Cloud Manager에서 GCP 권한으로 수행하는 권한입니다"](#)

## Google Cloud에서 Cloud Volumes ONTAP 구성을 계획하십시오

Google Cloud에 Cloud Volumes ONTAP를 배포할 때 워크로드 요구 사항에 맞는 사전 구성된 시스템을 선택하거나 자신만의 구성을 만들 수 있습니다. 자신의 구성을 선택하는 경우 가능한 옵션을 이해해야 합니다.

### Cloud Volumes ONTAP 라이선스를 선택합니다

Cloud Volumes ONTAP에는 몇 가지 라이선스 옵션이 있습니다. 각 옵션을 사용하여 요구사항에 맞는 소비 모델을 선택할 수 있습니다.

- ["Cloud Volumes ONTAP의 라이선스 옵션에 대해 자세히 알아보십시오"](#)
- ["라이선스 설정 방법에 대해 알아보십시오"](#)

### 지원되는 지역을 선택하십시오

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

### 지원되는 시스템 유형을 선택합니다

Cloud Volumes ONTAP는 선택한 라이선스 유형에 따라 여러 가지 시스템 유형을 지원합니다.

["GCP에서 Cloud Volumes ONTAP에 지원되는 구성입니다"](#)

### 스토리지 제한사항을 파악합니다

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

["GCP의 Cloud Volumes ONTAP에 대한 스토리지 제한입니다"](#)

### GCP에서 시스템 크기를 조정합니다

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

## 기계 유형

에서 지원되는 기계 유형을 확인합니다 "[Cloud Volumes ONTAP 릴리즈 노트](#)" 지원되는 각 시스템 유형에 대한 자세한 내용은 Google에서 확인하십시오. 워크로드 요구 사항을 시스템 유형에 대한 vCPU 및 메모리 수와 일치시킵니다. 각 CPU 코어는 네트워킹 성능을 향상시킵니다.

자세한 내용은 다음을 참조하십시오.

- "[Google Cloud 설명서: N1 표준 컴퓨터 유형](#)"
- "[Google Cloud 설명서: 성능](#)"

## GCP 디스크 유형입니다

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

- *Zonal SSD* 영구 디스크: SSD 영구 디스크는 높은 속도의 랜덤 IOPS가 필요한 워크로드에 가장 적합합니다.
- *Zonal Balanced* 영구 디스크 \_: 이 SSD는 GB당 더 낮은 IOPS를 제공하여 성능과 비용을 균형 있게 조정합니다.
- *Zonal Standard* 영구 디스크: 표준 영구 디스크는 경제적이며 순차적 읽기/쓰기 작업을 처리할 수 있습니다.

자세한 내용은 을 참조하십시오 "[Google Cloud 설명서: Zonal Persistent 디스크\(Standard 및 SSD\)](#)".

## GCP 디스크 크기입니다

Cloud Volumes ONTAP 시스템을 배포할 때 초기 디스크 크기를 선택해야 합니다. 그런 다음 Cloud Manager에서 시스템의 용량을 관리할 수 있지만, 애그리게이트를 직접 구축하려는 경우 다음 사항에 유의하십시오.

- Aggregate의 모든 디스크는 동일한 크기여야 합니다.
- 성능을 고려하면서 필요한 공간을 결정합니다.
- 영구 디스크의 성능은 디스크 크기와 시스템에서 사용할 수 있는 vCPU 수에 따라 자동으로 확장됩니다.

자세한 내용은 다음을 참조하십시오.

- "[Google Cloud 설명서: Zonal Persistent 디스크\(Standard 및 SSD\)](#)"
- "[Google Cloud 설명서: 영구 디스크 및 로컬 SSD 성능 최적화](#)"

## 기본 시스템 디스크를 봅니다

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

- "[Google Cloud에서 Cloud Volumes ONTAP 시스템 데이터에 대한 기본 디스크를 봅니다](#)".
- "[Google Cloud 문서: 리소스 할당량](#)"

Google Cloud Compute Engine은 리소스 사용량에 대해 할당량을 적용하므로 Cloud Volumes ONTAP를 배포하기 전에 한계에 도달하지 않았는지 확인해야 합니다.



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

## 네트워킹 정보를 수집합니다

GCP에서 Cloud Volumes ONTAP를 배포할 때 가상 네트워크에 대한 세부 정보를 지정해야 합니다. 워크시트를 사용하여 관리자로부터 정보를 수집할 수 있습니다.

- 단일 노드 시스템에 대한 네트워크 정보 \*

GCP 정보	귀사의 가치
지역	
Zone(영역)	
VPC 네트워크	
서브넷	
방화벽 정책(자체 사용 시)	

- 여러 존의 HA 쌍에 대한 네트워크 정보 \*

GCP 정보	귀사의 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 사용 시)	

- 단일 영역의 HA 쌍에 대한 네트워크 정보 \*

GCP 정보	귀사의 가치
지역	
Zone(영역)	
VPC-0 및 서브넷	
VPC-1 및 서브넷	
VPC-2 및 서브넷	
VPC-3 및 서브넷	
방화벽 정책(자체 사용 시)	

## 쓰기 속도를 선택합니다

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

## 볼륨 사용 프로필을 선택합니다

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

NetApp 스토리지 효율성 기능은 다음과 같은 이점을 제공합니다.

### 스핀 프로비저닝

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

### 중복 제거

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

### 압축

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

## GCP의 Cloud Volumes ONTAP에 대한 네트워킹 요구 사항

Cloud Volumes ONTAP 시스템이 올바르게 작동할 수 있도록 Google 클라우드 플랫폼 네트워킹을 설정합니다. 여기에는 커넥터 및 Cloud Volumes ONTAP에 대한 네트워킹이 포함됩니다.

HA 쌍을 구축하려는 경우 "[GCP에서 HA Pair의 작동 방식에 대해 알아보십시오](#)".

## Cloud Volumes ONTAP에 대한 요구사항

GCP에서 다음 요구사항을 충족해야 합니다.

### 내부 로드 밸런서

Cloud Manager는 Cloud Volumes ONTAP HA 쌍에 대한 들어오는 트래픽을 관리하는 4개의 Google Cloud 내부 로드 밸런서(TCP/UDP)를 자동으로 생성합니다. 설정을 마칠 필요가 없습니다 이를 단순히 네트워크 트래픽을 알리고 보안 문제를 완화하기 위한 요구 사항으로 나열했습니다.

로드 밸런싱 장치 하나는 클러스터 관리이고, 하나는 SVM(스토리지 VM) 관리이고, 하나는 노드 1에 대한 NAS 트래픽이고, 나머지 하나는 노드 2에 대한 NAS 트래픽입니다.

각 부하 분산 장치에 대한 설정은 다음과 같습니다.

- 공유 개인 IP 주소 1개
- 글로벌 상태 점검 1회

기본적으로 상태 확인에 사용되는 포트는 63001, 63002 및 63003입니다.

- 지역 TCP 백엔드 서비스 1개
- 지역 UDP 백엔드 서비스 1개
- 하나의 TCP 전달 규칙
- UDP 포워딩 규칙 1개
- 전역 액세스가 비활성화되었습니다

전역 액세스는 기본적으로 해제되어 있지만 사후 배포를 사용하도록 설정하는 것이 지원됩니다. 지역 간 트래픽의 지연 시간이 훨씬 더 길기 때문에 이 기능을 비활성화했습니다. 우발적인 교차 부위 장착으로 인해 부정적인 경험을 하지 않으려 했습니다. 이 옵션의 활성화는 비즈니스 요구 사항에 따라 다릅니다.

### HA 쌍을 위한 하나 이상의 영역

여러 영역 또는 단일 영역에 HA 구성을 배포하여 데이터의고가용성을 보장할 수 있습니다. HA 쌍을 생성할 때 Cloud Manager에서 여러 존 또는 단일 존을 선택하라는 메시지를 표시합니다.

- 다중 영역(권장)

3개 존에 HA 구성을 구축하면 존 내에서 장애가 발생하더라도 지속적인 데이터 가용성을 보장할 수 있습니다. 쓰기 성능은 단일 존을 사용할 때보다 약간 낮지만, 이는 최소화됩니다.

- 단일 영역

단일 영역에 배포되면 Cloud Volumes ONTAP HA 구성에서 분산 배치 정책을 사용합니다. 이 정책은 별도의 존을 사용하여 장애를 격리하지 않고도 존 내의 단일 장애 지점으로부터 HA 구성을 보호합니다.

이 구축 모델은 구역 간 데이터 유출 비용이 없으므로 비용이 절감됩니다.

### HA 쌍을 위한 4가지 가상 프라이빗 클라우드

HA 구성을 위해서는 4개의 가상 프라이빗 클라우드(VPC)가 필요합니다. GCP가 각 네트워크 인터페이스가 별도의 VPC 네트워크에 상주하도록 요구하기 때문에 4개의 VPC가 필요합니다.

HA 쌍을 생성할 때 Cloud Manager에서 4개의 VPC를 선택하라는 메시지가 표시됩니다.

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





## HA 쌍을 위한 서브넷

각 VPC에 전용 서브넷이 필요합니다.

Connector를 VPC-0에 배치한 경우 서브넷에서 Private Google Access를 활성화하여 API에 액세스하고 데이터 계층화를 활성화해야 합니다.

이러한 VPC에 있는 서브넷에는 고유한 CIDR 범위가 있어야 합니다. CIDR 범위가 중복될 수 없습니다.

## 단일 노드 시스템을 위한 단일 가상 프라이빗 클라우드

단일 노드 시스템에는 VPC 1개가 필요합니다.

## 공유 VPC

Cloud Volumes ONTAP 및 Connector는 Google Cloud 공유 VPC 및 독립 실행형 VPC에서도 지원됩니다.

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

HA 쌍의 경우 4개의 VPC가 필요합니다. 각 VPC는 공유 또는 독립 실행형으로 사용할 수 있습니다. 예를 들어 VPC-0은 공유 VPC가 될 수 있고 VPC-1, VPC-2 및 VPC-3은 독립 실행형 VPC가 될 수 있습니다.

공유 VPC를 사용하면 여러 프로젝트에서 가상 네트워크를 구성하고 중앙에서 관리할 수 있습니다. `_host project_`에서 공유 VPC 네트워크를 설정하고 `_service project_`에서 Connector 및 Cloud Volumes ONTAP 가상

머신 인스턴스를 배포할 수 있습니다. "[Google Cloud 설명서: 공유 VPC 개요](#)".

"Connector 구축에서 적용되는 필수 공유 VPC 사용 권한을 검토합니다".

## VPC의 패킷 미러링

"패킷 미러링" Cloud Volumes ONTAP를 구축하는 Google Cloud VPC에서 비활성화되어야 합니다. 패킷 미러링이 활성화된 경우 Cloud Volumes ONTAP가 제대로 작동하지 않습니다.

## Cloud Volumes ONTAP에 대한 아웃바운드 인터넷 액세스

Cloud Volumes ONTAP에서 스토리지 상태를 능동적으로 모니터링하는 NetApp AutoSupport에 메시지를 보내려면 아웃바운드 인터넷 액세스가 필요합니다.

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

- <https://support.netapp.com/aods/asupmessage> 으로 문의하십시오
- <https://support.netapp.com/asupprod/post/1.0/postAsup> 으로 문의하십시오

"AutoSupport 확인 방법을 알아보십시오".



HA 쌍을 사용하는 경우 HA 중재자가 아웃바운드 인터넷 액세스를 요구하지 않습니다.

## 전용 IP 주소

Cloud Manager는 GCP의 Cloud Volumes ONTAP에 다음과 같은 수의 프라이빗 IP 주소를 할당합니다.

- \* 단일 노드 \*: 3개 또는 4개의 전용 IP 주소

API를 사용하여 Cloud Volumes ONTAP를 구축하고 다음 플래그를 지정한 경우 SVM(스토리지 VM) 관리 LIF의 생성을 건너뛸 수 있습니다.

'스킵스만트관리면: TRUE'

LIF는 물리적 포트와 연결된 IP 주소입니다. SnapCenter와 같은 관리 툴을 사용하려면 스토리지 VM(SVM) 관리 LIF가 필요합니다.

- \* HA 쌍 \*: 14 또는 15개의 전용 IP 주소

- VPC-0용 전용 IP 주소 7개 또는 8개

API를 사용하여 Cloud Volumes ONTAP를 구축하고 다음 플래그를 지정한 경우 SVM(스토리지 VM) 관리 LIF의 생성을 건너뛸 수 있습니다.

'스킵스만트관리면: TRUE'

- VPC-1용 사설 IP 주소 2개
- VPC-2용 사설 IP 주소 2개
- VPC-3용 사설 IP 주소 3개

## 방화벽 규칙

Cloud Manager에서 방화벽 규칙을 생성할 수 있으므로 이 규칙을 생성할 필요가 없습니다. 직접 사용해야 하는 경우 아래 나열된 방화벽 규칙을 참조하십시오.

HA 구성에는 두 가지 방화벽 규칙 세트가 필요합니다.

- VPC-0의 HA 구성 요소에 대한 하나의 규칙 세트 이러한 규칙을 통해 Cloud Volumes ONTAP에 대한 데이터 액세스가 가능합니다. [자세한 정보](#).
- VPC-1, VPC-2 및 VPC-3의 HA 구성 요소에 대한 또 다른 규칙 세트 이러한 규칙은 HA 구성 요소 간의 인바운드 및 아웃바운드 통신에 대해 개방됩니다. [자세한 정보](#).

## 데이터 계층화를 위해 Cloud Volumes ONTAP에서 Google 클라우드 스토리지로 연결

콜드 데이터를 Google 클라우드 스토리지 버킷에 계층화하려면 Cloud Volumes ONTAP가 상주하는 서버넷이 프라이빗 Google 액세스용으로 구성되어야 합니다(HA 쌍을 사용하는 경우 VPC-0의 서버넷임). 자세한 지침은 을 참조하십시오 ["Google Cloud 설명서: 개인 Google Access 구성"](#).

Cloud Manager에서 데이터 계층화를 설정하는 데 필요한 추가 단계는 를 참조하십시오 ["콜드 데이터를 저비용 오브젝트 스토리지로 계층화"](#).

## 다른 네트워크의 ONTAP 시스템에 대한 연결

GCP의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 VPC와 기업 네트워크 같은 다른 네트워크 간에 VPN 연결이 있어야 합니다.

자세한 지침은 을 참조하십시오 ["Google Cloud 설명서: Cloud VPN 개요"](#).

## 커넥터 요구 사항

Connector가 공용 클라우드 환경 내에서 리소스와 프로세스를 관리할 수 있도록 네트워킹을 설정합니다. 가장 중요한 단계는 다양한 엔드포인트에 대한 아웃바운드 인터넷 액세스를 보장하는 것입니다.



네트워크에서 인터넷에 대한 모든 통신에 프록시 서버를 사용하는 경우 설정 페이지에서 프록시 서버를 지정할 수 있습니다. 을 참조하십시오 ["프록시 서버를 사용하도록 Connector 구성"](#).

## 대상 네트워크에 연결

커넥터를 사용하려면 Cloud Volumes ONTAP를 배포하려는 VPC에 대한 네트워크 연결이 필요합니다. HA 쌍을 구축하는 경우 Connector는 VPC-0에만 연결해야 합니다.

커넥터와 별도로 VPC에 Cloud Volumes ONTAP를 배포하려는 경우 VPC 네트워크 피어링을 설정해야 합니다. ["VPC 네트워크 피어링에 대해 자세히 알아보십시오"](#)

## 아웃바운드 인터넷 액세스

Connector를 사용하려면 공용 클라우드 환경 내의 리소스와 프로세스를 관리하기 위한 아웃바운드 인터넷 액세스가 필요합니다.

엔드포인트	목적
<a href="https://support.netapp.com">https://support.netapp.com</a> 으로 문의하십시오	라이선스 정보를 얻고 AutoSupport 메시지를 NetApp 지원 팀에 전송합니다.

엔드포인트	목적
<a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a> 으로 문의하십시오	Cloud Manager 내에서 SaaS 기능 및 서비스를 제공합니다.
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a> <a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a> 으로 문의하십시오	Connector 및 해당 Docker 구성 요소를 업그레이드합니다.

## Cloud Volumes ONTAP의 방화벽 규칙

Cloud Manager는 Cloud Volumes ONTAP이 성공적으로 운영하는 데 필요한 인바운드 및 아웃바운드 규칙을 포함하는 GCP 방화벽 규칙을 생성합니다. 테스트 목적으로 또는 자체 방화벽 규칙을 사용하려는 경우 포트를 참조할 수 있습니다.

Cloud Volumes ONTAP의 방화벽 규칙에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

HA 구성을 구축할 경우 VPC-0의 Cloud Volumes ONTAP에 대한 방화벽 규칙입니다.

### 인바운드 규칙

HA 쌍의 경우 사전 정의된 방화벽 정책의 인바운드 트래픽에 대한 소스 필터는 0.0.0.0/0입니다.

단일 노드 시스템의 경우 배포 중에 미리 정의된 방화벽 정책에 대한 소스 필터를 선택할 수 있습니다.

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

자체 방화벽 정책을 사용하는 경우 Cloud Volumes ONTAP와 통신해야 하는 모든 네트워크를 추가해야 하지만 내부 Google 로드 밸런서가 올바르게 작동할 수 있도록 두 주소 범위를 모두 추가해야 합니다. 이러한 주소는 130.211.0.0/22 및 35.191.0.0/16입니다. 자세한 내용은 ["Google Cloud 설명서: 부하 분산 방화벽 규칙"](#)을 참조하십시오.

프로토콜	포트	목적
모든 ICMP	모두	인스턴스에 Ping을 수행 중입니다
HTTP	80	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTP 액세스
HTTPS	443	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTPS 액세스
SSH를 클릭합니다	22	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다
TCP	111	NFS에 대한 원격 프로시저 호출
TCP	139	CIFS에 대한 NetBIOS 서비스 세션입니다
TCP	161-162	단순한 네트워크 관리 프로토콜
TCP	445	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
TCP	635	NFS 마운트
TCP	749	Kerberos

프로토콜	포트	목적
TCP	2049	NFS 서버 데몬
TCP	3260	iSCSI 데이터 LIF를 통한 iSCSI 액세스
TCP	4045	NFS 잠금 데몬
TCP	4046	NFS에 대한 네트워크 상태 모니터
TCP	10000입니다	NDMP를 사용한 백업
TCP	11104	SnapMirror에 대한 인터클러스터 통신 세션의 관리
TCP	11105	인터클러스터 LIF를 사용하여 SnapMirror 데이터 전송
TCP	63001-63050	로드 밸런싱 프로브 포트를 통해 어떤 노드가 정상 상태인지 확인(HA 쌍에만 필요)
UDP입니다	111	NFS에 대한 원격 프로시저 호출
UDP입니다	161-162	단순한 네트워크 관리 프로토콜
UDP입니다	635	NFS 마운트
UDP입니다	2049	NFS 서버 데몬
UDP입니다	4045	NFS 잠금 데몬
UDP입니다	4046	NFS에 대한 네트워크 상태 모니터
UDP입니다	4049	NFS rquotad 프로토콜

## 아웃바운드 규칙

Cloud Volumes ONTAP에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

### 기본 아웃바운드 규칙

Cloud Volumes ONTAP에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

프로토콜	포트	목적
모든 ICMP	모두	모든 아웃바운드 트래픽
모든 TCP	모두	모든 아웃바운드 트래픽
모든 UDP	모두	모든 아웃바운드 트래픽

### 고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Cloud Volumes ONTAP의 아웃바운드

통신에 필요한 포트만 열 수 있습니다.



소스는 Cloud Volumes ONTAP 시스템의 인터페이스(IP 주소)입니다.

서비스	프로토콜	포트	출처	목적지	목적
Active Directory 를 클릭합니 다	TCP	88	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니 다	137	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니 다	138	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
	TCP	139	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
	TCP 및 UDP	389	노드 관리 LIF	Active Directory 포리스트입니다	LDAP를 지원합니다
	TCP	445	노드 관리 LIF	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
	TCP	464	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	UDP입니 다	464	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos 키 관리
	TCP	749	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(RPCSEC_GSS)
	TCP	88	데이터 LIF(NFS, CIFS, iSCSI)	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니 다	137	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니 다	138	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
	TCP	139	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
	TCP 및 UDP	389	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	LDAP를 지원합니다
	TCP	445	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
	TCP	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	UDP입니 다	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos 키 관리
	TCP	749	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(RPCSEC_GSS)

서비스	프로토콜	포트	출처	목적지	목적
AutoSupport	HTTPS	443	노드 관리 LIF	support.netapp.com	AutoSupport(기본값은 HTTPS)
	HTTP	80	노드 관리 LIF	support.netapp.com	AutoSupport(전송 프로토콜이 HTTPS에서 HTTP로 변경된 경우에만 해당)
클러스터	모든 교통 정보	모든 교통 정보	모든 LIF가 하나의 노드에 있습니다	다른 노드의 모든 LIF	인터클러스터 통신(Cloud Volumes ONTAP HA에만 해당)
DHCP를 선택합니다	UDP입니다	68	노드 관리 LIF	DHCP를 선택합니다	처음으로 설정하는 DHCP 클라이언트
DHCPs	UDP입니다	67	노드 관리 LIF	DHCP를 선택합니다	DHCP 서버
DNS	UDP입니다	53	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
NDMP	TCP	1860-18699	노드 관리 LIF	대상 서버	NDMP 복제
SMTP	TCP	25	노드 관리 LIF	메일 서버	AutoSupport에 사용할 수 있는 SMTP 경고
SNMP를 선택합니다	TCP	161	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	UDP입니다	161	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	TCP	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	UDP입니다	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
SnapMirror를 참조하십시오	TCP	11104	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror에 대한 인터클러스터 통신 세션의 관리
	TCP	11105	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror 데이터 전송
Syslog를 클릭합니다	UDP입니다	514	노드 관리 LIF	Syslog 서버	Syslog 메시지를 전달합니다

## VPC-1, VPC-2 및 VPC-3의 방화벽 규칙

GCP에서 HA 구성은 네 대의 VPC에 구축됩니다. VPC-0의 HA 구성에 필요한 방화벽 규칙은 [입니 Cloud Volumes ONTAP에 대해 위에 나열되어 있습니다](#).

한편, Cloud Manager가 VPC-1, VPC-2 및 VPC-3의 인스턴스에 대해 생성하는 사전 정의된 방화벽 규칙은 `_ALL_PROTOCOLS` 및 `PORT`를 통한 수신 통신을 지원합니다. 이 규칙은 HA 노드 간 통신을 지원합니다.

HA 노드와 HA 중재자의 통신은 포트 3260(iSCSI)을 통해 이루어집니다.

## 커넥터의 방화벽 규칙

Connector의 방화벽 규칙에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

### 인바운드 규칙

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

### 아웃바운드 규칙

Connector에 대해 미리 정의된 방화벽 규칙은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

#### 기본 아웃바운드 규칙

Connector에 대해 미리 정의된 방화벽 규칙에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

프로토콜	포트	목적
모든 TCP	모두	모든 아웃바운드 트래픽
모든 UDP	모두	모든 아웃바운드 트래픽

#### 고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Connector의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.



소스 IP 주소는 커넥터 호스트입니다.

서비스	프로토콜	포트	목적지	목적
API 호출 및 AutoSupport	HTTPS	443	아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF	API는 GCP 및 ONTAP, 클라우드 데이터 센스, 랜섬웨어 서비스 요청 및 AutoSupport 메시지를 NetApp에 전송합니다
DNS	UDP입니다	53	DNS	Cloud Manager에서 DNS Resolve에 사용됩니다



# GCP에서 VPC 서비스 제어 계획

VPC 서비스 제어를 통해 Google Cloud 환경을 잠그려면 Cloud Manager 및 Cloud Volumes ONTAP가 Google Cloud API와 상호 작용하는 방식과 Cloud Manager 및 Cloud Volumes ONTAP를 배포하기 위해 서비스 경계를 구성하는 방법을 이해해야 합니다.

VPC 서비스 제어를 사용하면 신뢰할 수 있는 경계 외부의 Google 관리 서비스에 대한 액세스를 제어하고, 신뢰할 수 없는 위치에서 데이터 액세스를 차단하고, 무단 데이터 전송 위험을 완화할 수 있습니다. "[Google Cloud VPC 서비스 컨트롤에 대해 자세히 알아보십시오](#)".

## NetApp 서비스가 VPC 서비스 제어와 통신하는 방법

Cloud Central 및 Cloud Manager와 같은 NetApp 서비스는 Google Cloud API와 직접 통신합니다. 이는 Google Cloud 외부의 외부 IP 주소(예: api.services.cloud.netapp.com) 또는 Cloud Manager Connector에 할당된 내부 주소에서 Google Cloud 내부에서 트리거됩니다.

Connector의 배포 스타일에 따라 서비스 경계에 대해 특정 예외가 발생할 수 있습니다.

## 이미지

Cloud Volumes ONTAP와 Cloud Manager는 모두 NetApp에서 관리하는 GCP 내 프로젝트의 이미지를 사용합니다. 조직 내에 호스팅되지 않은 이미지 사용을 차단하는 정책이 있는 경우 Cloud Manager Connector 및 Cloud Volumes ONTAP의 구축에 영향을 미칠 수 있습니다.

수동 설치 방법을 사용하여 커넥터를 수동으로 배포할 수도 있지만 Cloud Volumes ONTAP는 NetApp 프로젝트에서도 이미지를 가져와야 합니다. 커넥터 및 Cloud Volumes ONTAP를 배포하려면 허용 목록을 제공해야 합니다.

## 커넥터 배포

Connector를 배포하는 사용자는 ProjectID\_NetApp-cloudmanager\_에서 호스팅되는 이미지와 프로젝트 번호\_14190056516\_를 참조할 수 있어야 합니다.

## Cloud Volumes ONTAP 배포

- Cloud Manager 서비스 계정은 서비스 프로젝트에서 ProjectID\_NetApp-cloudmanager\_에 호스팅된 이미지와 프로젝트 번호\_14190056516\_에 호스팅된 이미지를 참조해야 합니다.
- 기본 Google API 서비스 에이전트의 서비스 계정은 ProjectID\_NetApp-cloudmanager\_에서 호스팅되는 이미지와 서비스 프로젝트의 \_14190056516\_프로젝트 번호를 참조해야 합니다.

VPC 서비스 제어를 사용하여 이러한 이미지를 가져오는 데 필요한 규칙의 예는 아래에 정의되어 있습니다.

## VPC 서비스는 경계 정책을 제어합니다

정책은 VPC 서비스 제어 규칙 집합에 대한 예외를 허용합니다. 정책에 대한 자세한 내용은 ["GCP VPC 서비스 제어 정책 문서"](#)를 참조하십시오.

Cloud Manager에 필요한 정책을 설정하려면 조직 내의 VPC 서비스 제어 경계로 이동하여 다음 정책을 추가합니다. 이 필드는 VPC 서비스 제어 정책 페이지에 제공된 옵션과 일치해야 합니다. 또한 \* 모든 \* 규칙이 필요하며 \* 또는 \* 매개 변수를 규칙 집합에 사용해야 합니다.

## 수신 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
```

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



위에 요약된 프로젝트 번호는 Cloud Volumes ONTAP용 커넥터 및 이미지를 저장하는 데 사용되는 PROJECT\_NetApp-cloudmanager\_입니다.

## 데이터 계층화 및 백업을 위한 서비스 계정을 생성합니다

Cloud Volumes ONTAP를 사용하려면 Google Cloud 서비스 계정이 두 가지 용도로 필요합니다. 첫 번째는 를 활성화하는 것입니다 **"데이터 계층화"** Google Cloud에서 콜드 데이터를 저비용 오브젝트 스토리지로 계층화합니다. 두 번째는 를 활성화하는 것입니다 **"Cloud Backup Service"** 볼륨을 저렴한 오브젝트 스토리지에 백업

Cloud Volumes ONTAP는 서비스 계정을 사용하여 계층화된 데이터에 대한 하나의 버킷과 백업을 위한 다른 버킷에 액세스하고 관리합니다.

하나의 서비스 계정을 설정하고 두 가지 용도로 사용할 수 있습니다. 서비스 계정에는 \* 스토리지 관리자 \* 역할이 있어야 합니다.

### 단계

1. Google Cloud 콘솔에서 **"서비스 계정 페이지로 이동합니다"**.
2. 프로젝트를 선택합니다.
3. 서비스 계정 생성 \* 을 클릭하고 필요한 정보를 입력합니다.
  - a. \* 서비스 계정 세부 정보 \*: 이름과 설명을 입력합니다.
  - b. \* 프로젝트에 대한 이 서비스 계정 액세스 권한 부여 \*: \* 스토리지 관리자 \* 역할을 선택합니다.



- c. 이 서비스 계정에 대한 사용자 액세스 허용 \*: Connector 서비스 계정을 이 새 서비스 계정에 \_ 서비스 계정 사용자로 추가 \_.

이 단계는 데이터 계층화에만 필요합니다. Cloud Backup Service에는 필요하지 않습니다.

Create service account

✓ Service account details

✓ Grant this service account access to project (optional)

3 Grant users access to this service account (optional)  
Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role

netapp-cloud-manager@iam.gserviceaccount.com ✕ ?

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role ?

Grant users the permission to administer this service account

DONE

CANCEL

Cloud Volumes ONTAP 작업 환경을 생성할 때 나중에 서비스 계정을 선택해야 합니다.

## Details and Credentials

**default-project**  
Google Cloud Project

**gcp-sub2**  
Marketplace Subscription

[Edit Project](#)

**Details**

Working Environment Name (Cluster Name)

cloudvolumesontap

**Service Account** ⓘ

☒

Service Account Name

account1

+ Add Labels    Optional Field | Up to four labels

**Credentials**

User Name

admin

Password

Confirm Password

## Cloud Volumes ONTAP에서 고객이 관리하는 암호화 키 사용

Google 클라우드 스토리지는 디스크에 데이터를 쓰기 전에 항상 데이터를 암호화하지만, Cloud Manager API를 사용하여 고객이 관리하는 암호화 키를 사용하는 Cloud Volumes ONTAP 시스템을 생성할 수 있습니다. 클라우드 키 관리 서비스를 사용하여 GCP에서 생성하고 관리하는 키입니다.

단계

1. 키가 저장된 프로젝트의 Cloud Manager Connector 서비스 계정에 프로젝트 수준에서 올바른 권한이 있는지 확인합니다.

권한은 에서 제공합니다 ["Cloud Manager YAML 파일"](#) 기본적으로 클라우드 키 관리 서비스에 대체 프로젝트를 사용하는 경우에는 적용되지 않을 수 있습니다.

사용 권한은 다음과 같습니다.

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

2. 에 대한 서비스 계정이 있는지 확인합니다 ["Google Compute Engine 서비스 에이전트입니다"](#) Cloud KMS Encrypter/Decrypter 권한이 키에 있습니다.

서비스 계정 이름은 "service-[service\_project\_number]@compute-system.iam.gserviceaccount.com" 형식을 사용합니다.

"Google Cloud 설명서: IAM을 Cloud KMS-Granting 역할과 함께 리소스에 사용"

3. "/GCP/VSA/metadata/GCP-encryption-keys" API 호출에 대한 get 명령을 호출하거나 GCP 콘솔의 키에 있는 "Copy Resource Name"을 선택하여 키의 "id"를 얻습니다.
4. 고객이 관리하는 암호화 키를 사용하고 데이터를 오브젝트 스토리지에 계층화하는 경우 Cloud Manager는 영구 디스크를 암호화하는 데 사용된 것과 동일한 키를 사용하려 합니다. 하지만 먼저 Google Cloud Storage 버킷을 활성화하여 키를 사용해야 합니다.
  - a. 예 따라 Google Cloud Storage 서비스 에이전트를 찾습니다 "Google Cloud 설명서: 클라우드 스토리지 서비스 에이전트 얻기".
  - b. 암호화 키로 이동하여 Cloud KMS Encrypter/Decrypter 권한이 있는 Google Cloud Storage 서비스 에이전트를 할당합니다.

자세한 내용은 을 참조하십시오 "Google Cloud 설명서: 고객이 관리하는 암호화 키 사용"

5. 작업 환경을 만들 때 API 요청과 함께 "GcpEncryption" 매개 변수를 사용합니다.

◦ 예 \*

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

을 참조하십시오 "Cloud Manager 자동화 문서" "GcpEncryption" 매개 변수 사용에 대한 자세한 내용은 를 참조하십시오.

## Google Cloud에서 Cloud Volumes ONTAP에 대한 라이선스를 설정합니다

Cloud Volumes ONTAP에서 사용할 라이선스 옵션을 결정한 후에는 몇 가지 단계를 거쳐 새 작업 환경을 만들 때 해당 라이선스 옵션을 선택해야 합니다.

### 프리모늄

최대 500GiB의 용량을 제공하는 Cloud Volumes ONTAP를 무료로 사용할 수 있는 Freemium 오퍼링을 선택하십시오. "Freemium 제품에 대해 자세히 알아보십시오".

### 단계

1. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 Cloud Manager의 단계를 따릅니다.
  - a. 상세 정보 및 자격 증명 \* 페이지에서 \* 자격 증명 편집 > 구독 추가 \* 를 클릭한 다음 화면의 지시에 따라 Google Cloud Marketplace에서 선불 종량제 서비스를 구독합니다.

프로비저닝된 용량 500GiB를 초과하지 않는 한, 마켓플레이스 구독을 통해 비용이 청구되지 않으며, 이 경우 시스템이 으로 자동으로 변환됩니다 "Essentials 패키지를 선택합니다".

b. Cloud Manager로 돌아간 후 충전 방법 페이지에 도달하면 \* Freemium \* 을 선택합니다.



The screenshot shows a 'Select Charging Method' dialog box with four radio button options. The 'Freemium (Up to 500 GiB)' option is selected, indicated by a blue checkmark. To the right of each option is a button labeled 'By capacity' (for Professional, Essential, and Freemium) or 'By node' (for Per Node), followed by a downward arrow. The buttons for Professional, Essential, and Freemium are blue, while the button for Per Node is purple.

"Google Cloud에서 Cloud Volumes ONTAP를 실행하기 위한 단계별 지침을 확인하십시오".

## 용량 기반 라이선스

용량 기반 라이선스를 통해 Cloud Volumes ONTAP 1TiB 용량 단위로 비용을 지불할 수 있습니다. 용량 기반 라이선스는 Essentials 패키지 또는 Professional 패키지 형태로 제공됩니다.

Essentials 및 Professional 패키지는 다음 소비 모델과 함께 제공됩니다.

- NetApp에서 구입한 라이선스(BYOL)
- Google Cloud Marketplace에서 PAYGO(pay-as-you-go) 방식으로 구독을 지원합니다
- 연간 계약입니다

"용량 기반 라이선스에 대해 자세히 알아보십시오".

다음 섹션에서는 이러한 각 소비 모델을 시작하는 방법을 설명합니다.

### BYOL

NetApp에서 BYOL(License)을 구매하여 모든 클라우드 공급자를 통해 Cloud Volumes ONTAP 시스템 구축

단계

1. "라이선스를 획득하려면 NetApp 세일즈 팀에 문의하십시오"
2. "Cloud Manager에 NetApp Support 사이트 계정을 추가합니다"

Cloud Manager에서 NetApp의 라이선스 서비스에 대해 자동으로 쿼리하여 NetApp Support 사이트 계정과 연결된 라이선스에 대한 자세한 정보를 가져옵니다. 오류가 없는 경우 Cloud Manager는 디지털 지갑에 라이선스를 자동으로 추가합니다.

Cloud Volumes ONTAP에서 사용하기 전에 디지털 지갑에서 라이선스를 사용할 수 있어야 합니다. 필요한 경우, 할 수 있습니다 "디지털 지갑에 라이선스를 수동으로 추가합니다".



3. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 Cloud Manager의 단계를 따릅니다.

- a. 상세 정보 및 자격 증명 \* 페이지에서 \* 자격 증명 편집 > 구독 추가 \* 를 클릭한 다음 화면의 지시에 따라 Google Cloud Marketplace에서 선불 종량제 서비스를 구독합니다.

NetApp에서 구매한 라이선스는 항상 먼저 부과되지만, 라이선스 용량을 초과하거나 라이선스 기간이 만료되면 마켓플레이스의 시간당 요금으로 비용이 청구됩니다.

- b. Cloud Manager로 돌아간 후 충전 방법 페이지가 표시되면 용량 기반 패키지를 선택합니다.

The screenshot shows a 'Select Charging Method' dialog box with four options:

- ☒ Professional: By capacity (blue button)
- ☐ Essential: By capacity (blue button)
- ☐ Freemium (Up to 500 GiB): By capacity (blue button)
- ☐ Per Node: By node (purple button)

"Google Cloud에서 Cloud Volumes ONTAP를 실행하기 위한 단계별 지침을 확인하십시오".

## PAYGO 구독

클라우드 공급자 마켓플레이스의 서비스에 가입하여 시간별 비용 지불

Cloud Volumes ONTAP 작업 환경을 생성할 때 Cloud Manager에서 Google Cloud Marketplace에서 사용 가능한 계약을 구독하라는 메시지를 표시합니다. 그러면 해당 구독이 충전을 위한 작업 환경과 연결됩니다. 추가 작업 환경에 동일한 서브스크립션을 사용할 수 있습니다.

## 단계

1. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 Cloud Manager의 단계를 따릅니다.

- a. 상세 정보 및 자격 증명 \* 페이지에서 \* 자격 증명 편집 > 구독 추가 \* 를 클릭한 다음 화면의 지시에 따라 Google Cloud Marketplace에서 선불 종량제 서비스를 구독합니다.

- b. Cloud Manager로 돌아간 후 충전 방법 페이지가 표시되면 용량 기반 패키지를 선택합니다.

Select Charging Method

<input checked="" type="radio"/> Professional	By capacity	▼
<input type="radio"/> Essential	By capacity	▼
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity	▼
<input type="radio"/> Per Node	By node	▼

"Google Cloud에서 Cloud Volumes ONTAP를 실행하기 위한 단계별 지침을 확인하십시오".



설정 > 자격 증명 페이지에서 계정과 연결된 Google Cloud Marketplace 구독을 관리할 수 있습니다.  
["Google Cloud 자격 증명 및 구독을 관리하는 방법을 알아보십시오"](#)

## 연간 계약

연간 계약을 구매하여 매년 Cloud Volumes ONTAP에 대한 비용을 지불합니다.

## 단계

1. 연간 계약을 구입하려면 NetApp 세일즈 담당자에게 문의하십시오.

이 계약은 Google Cloud Marketplace에서 `_private_Offer`로 제공됩니다.

NetApp이 프라이빗 오퍼를 공유하면 근무 환경을 생성하는 동안 Google Cloud Marketplace에서 가입할 때 연간 계획을 선택할 수 있습니다.

2. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 Cloud Manager의 단계를 따릅니다.
  - a. 세부 정보 및 자격 증명 \* 페이지에서 \* 자격 증명 편집 > 구독 추가 \* 를 클릭한 다음 표시되는 메시지에 따라 Google Cloud Marketplace에서 연간 계획을 구독합니다.
  - b. Google Cloud에서 계정과 공유된 연간 계획을 선택한 다음 \* 구독 \* 을 클릭합니다.
  - c. Cloud Manager로 돌아간 후 충전 방법 페이지가 표시되면 용량 기반 패키지를 선택합니다.

### Select Charging Method

<input checked="" type="radio"/> Professional	<span style="background-color: #007bff; color: white; padding: 2px 5px;">By capacity</span> <span style="font-size: 1.2em;">▼</span>
<input type="radio"/> Essential	<span style="background-color: #007bff; color: white; padding: 2px 5px;">By capacity</span> <span style="font-size: 1.2em;">▼</span>
<input type="radio"/> Freemium (Up to 500 GiB)	<span style="background-color: #007bff; color: white; padding: 2px 5px;">By capacity</span> <span style="font-size: 1.2em;">▼</span>
<input type="radio"/> Per Node	<span style="background-color: #6f42c1; color: white; padding: 2px 5px;">By node</span> <span style="font-size: 1.2em;">▼</span>

"Google Cloud에서 Cloud Volumes ONTAP를 실행하기 위한 단계별 지침을 확인하십시오".

## 유연한 **Keystone** 구독

Keystone Flex 가입은 종량제 구독 기반 서비스입니다. "[Keystone Flex 구독에 대해 자세히 알아보십시오](#)".

단계

1. 아직 구독이 없는 경우 "[NetApp에 문의하십시오](#)"
2. <mailto:ng-keystone-success@netapp.com> [Contact NetApp]: 하나 이상의 Keystone Flex 구독으로 Cloud Manager 사용자 계정을 인증하십시오.
3. NetApp이 사용자 계정을 승인한 후 "[Cloud Volumes ONTAP에서 사용할 수 있도록 구독을 연결합니다](#)".
4. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 Cloud Manager의 단계를 따릅니다.
  - a. 충전 방법을 선택하라는 메시지가 표시되면 Keystone Flex 가입 충전 방법을 선택합니다.

"Google Cloud에서 Cloud Volumes ONTAP를 실행하기 위한 단계별 지침을 확인하십시오".

## GCP에서 Cloud Volumes ONTAP를 시작합니다

단일 노드 구성에서 Cloud Volumes ONTAP를 실행하거나 Google 클라우드 플랫폼에서 HA 쌍으로 실행할 수 있습니다.

### 시작하기 전에

작업 환경을 만들려면 다음이 필요합니다.

- 실행 중인 커넥터입니다.
  - 가 있어야 합니다 "작업 영역과 연결된 커넥터입니다".
  - "항상 Connector를 실행 상태로 둘 준비가 되어 있어야 합니다".
  - Connector와 연결된 서비스 계정입니다 "최신 권한이 있어야 합니다".
- 사용하려는 구성에 대한 이해.

구성을 선택하고 관리자로부터 GCP 네트워킹 정보를 받아 준비해야 합니다. 자세한 내용은 을 참조하십시오 "Cloud Volumes ONTAP 구성 계획".

- Cloud Volumes ONTAP에 대한 라이선스 설정에 필요한 사항을 이해합니다.

"라이선스 설정 방법에 대해 알아보십시오".

- Google Cloud API는입니다 **"프로젝트에서 활성화됩니다"**:
  - Cloud Deployment Manager V2 API
  - 클라우드 로깅 API
  - Cloud Resource Manager API를 참조하십시오
  - 컴퓨팅 엔진 API
  - IAM(Identity and Access Management) API

## GCP에서 단일 노드 시스템 시작

Cloud Manager에서 작업 환경을 생성하여 GCP에서 Cloud Volumes ONTAP를 실행합니다.

단계

1. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 화면의 지시를 따릅니다.
2. \* 위치 선택 \*: \* Google Cloud \* 및 \* Cloud Volumes ONTAP \* 를 선택합니다.
3. 메시지가 표시되면 **"커넥터를 작성합니다"**.
4. \* 세부 정보 및 자격 증명 \*: 프로젝트를 선택하고 클러스터 이름을 지정한 다음 서비스 계정을 선택하고 선택적으로 레이블을 추가한 다음 자격 증명을 지정합니다.

다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
작업 환경 이름	Cloud Manager에서는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 GCP VM 인스턴스 모두에 이름을 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.
서비스 계정 이름입니다	를 사용할 계획인 경우 <b>"데이터 계층화"</b> 또는 <b>"클라우드 백업"</b> Cloud Volumes ONTAP를 사용하는 경우 * 서비스 계정 * 을 활성화하고 사전 정의된 스토리지 관리 역할이 있는 서비스 계정을 선택해야 합니다. <b>"서비스 계정을 만드는 방법에 대해 알아보십시오"</b> .
레이블 추가	레이블은 GCP 리소스에 대한 메타데이터입니다. Cloud Manager는 시스템에 연결된 Cloud Volumes ONTAP 시스템 및 GCP 리소스에 레이블을 추가합니다. 작업 환경을 만들 때 사용자 인터페이스에서 최대 4개의 레이블을 추가할 수 있으며, 그런 다음 만든 후에 레이블을 더 추가할 수 있습니다. API는 작업 환경을 만들 때 레이블을 네 개로 제한하지 않습니다. 레이블에 대한 자세한 내용은 을 참조하십시오 <b>"Google Cloud 설명서: 라벨 리소스"</b> .
사용자 이름 및 암호	Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하여 System Manager 또는 CLI를 통해 Cloud Volumes ONTAP에 연결할 수 있습니다. default_admin_user 이름을 유지하거나 사용자 지정 사용자 이름으로 변경합니다.

필드에 입력합니다	설명
프로젝트 편집	<p>Cloud Volumes ONTAP가 상주할 프로젝트를 선택합니다. 기본 프로젝트는 Cloud Manager가 상주하는 프로젝트입니다.</p> <p>드롭다운 목록에 추가 프로젝트가 표시되지 않으면 Cloud Manager 서비스 계정을 다른 프로젝트와 연결하지 않은 것입니다. Google Cloud 콘솔로 이동하여 IAM 서비스를 열고 프로젝트를 선택합니다. Cloud Manager 역할이 있는 서비스 계정을 해당 프로젝트에 추가합니다. 각 프로젝트에 대해 이 단계를 반복해야 합니다.</p> <div>  <p>Cloud Manager에 대해 설정한 서비스 계정입니다. <a href="#">"이 페이지에 설명되어 있습니다"</a>.</p> </div> <p>선택한 자격 증명을 구독과 연결하려면 * 구독 추가 * 를 클릭합니다.</p> <p>용량제 Cloud Volumes ONTAP 시스템을 생성하려면 GCP 마켓플레이스에서 Cloud Volumes ONTAP 서브스크립션과 연관된 GCP 프로젝트를 선택해야 합니다.</p>

다음 비디오에서는 용량제 마켓플레이스 서브스크립션을 GCP 프로젝트에 연결하는 방법을 보여줍니다. 또는 에 있는 구독 단계를 따릅니다 ["Marketplace 구독을 GCP 자격 증명과 연결합니다"](#) 섹션을 참조하십시오.

▶ [https://docs.netapp.com/ko-kr/cloud-manager-cloud-volumes-ontap//media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/ko-kr/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4)

(video)

5. \* 서비스 \*: 이 시스템에서 사용할 서비스를 선택합니다. Cloud Backup을 선택하거나 Tiering을 사용하려면 3단계에서 서비스 계정을 지정해야 합니다.
6. \* 위치 및 연결 \*: 위치를 선택하고 방화벽 정책을 선택한 다음 데이터 계층화를 위해 Google Cloud 스토리지에 대한 네트워크 연결을 확인합니다.

다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
연결 검증	콜드 데이터를 Google 클라우드 스토리지 버킷에 계층화하려면 Cloud Volumes ONTAP가 상주하는 서버넷을 프라이빗 Google 액세스용으로 구성해야 합니다. 자세한 지침은 을 참조하십시오 " <a href="#">Google Cloud 설명서: 개인 Google Access 구성</a> ".
방화벽 정책을 생성했습니다	Cloud Manager에서 방화벽 정책을 생성하도록 허용할 경우 트래픽을 허용하는 방법을 선택해야 합니다. <ul style="list-style-type: none"><li>• 선택한 VPC 전용 * 을 선택한 경우 인바운드 트래픽에 대한 소스 필터는 선택한 VPC의 서버넷 범위와 커넥터가 있는 VPC의 서버넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다.</li><li>• 모든 VPC * 를 선택한 경우 인바운드 트래픽의 소스 필터는 0.0.0.0/0 IP 범위입니다.</li></ul>
기존 방화벽 정책을 사용합니다	기존 방화벽 정책을 사용하는 경우 필수 규칙이 포함되어 있는지 확인합니다. " <a href="#">Cloud Volumes ONTAP의 방화벽 규칙에 대해 알아보십시오</a> ".

7. \* 충전 방법 및 NSS 계정 \*: 이 시스템에서 사용할 충전 옵션을 지정한 다음 NetApp Support 사이트 계정을 지정합니다.
  - "[Cloud Volumes ONTAP의 라이선스 옵션에 대해 자세히 알아보십시오](#)".
  - "[라이선스 설정 방법에 대해 알아보십시오](#)".
8. \* 사전 구성된 패키지 \*: 패키지 중 하나를 선택하여 Cloud Volumes ONTAP 시스템을 신속하게 배포하거나 \* 고유한 구성 만들기 \* 를 클릭합니다.

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

9. \* 라이선스 \*: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 시스템 유형을 선택합니다.



선택한 버전에 대해 새로운 출시 후보, 일반 가용성 또는 패치 릴리스를 사용할 수 있는 경우, Cloud Manager는 작업 환경을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.10.1 및 9.10.1 P4를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리즈에서 다른 릴리즈로 발생하지 않습니다(예: 9.6에서 9.7로).

10. \* 기본 스토리지 리소스 \*: 초기 집계에 대한 설정(디스크 유형 및 각 디스크의 크기)을 선택합니다.

디스크 유형은 초기 볼륨입니다. 이후 볼륨에 대해 다른 디스크 유형을 선택할 수 있습니다.

디스크 크기는 초기 애그리게이트의 모든 디스크와 단순 프로비저닝 옵션을 사용할 때 Cloud Manager가 생성하는 추가 애그리게이트의 경우 모두 사용됩니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.

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

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

쓰기 속도 선택은 단일 노드 시스템에서만 지원됩니다.

["쓰기 속도에 대해 자세히 알아보십시오"](#).

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

["WORM 스토리지에 대해 자세히 알아보십시오"](#).

12. \* Google Cloud Platform의 데이터 계층화 \*: 초기 애그리게이트에서 데이터 계층화를 사용할지 여부를 선택하고, 계층형 데이터에 대한 스토리지 클래스를 선택한 다음 사전 정의된 스토리지 관리 역할이 있는 서비스 계정을 선택합니다(Cloud Volumes ONTAP 9.7 이상에 필요). 또는 GCP 계정(Cloud Volumes ONTAP 9.6의 경우 필수)을 선택합니다.

다음 사항에 유의하십시오.

- Cloud Manager는 Cloud Volumes ONTAP 인스턴스에서 서비스 계정을 설정합니다. 이 서비스 계정은 Google Cloud Storage 버킷에 대한 데이터 계층화 권한을 제공합니다. Connector 서비스 계정을 계층화 서비스 계정의 사용자로 추가해야 합니다. 그렇지 않으면 Cloud Manager에서 선택할 수 없습니다.
- GCP 계정 추가에 대한 자세한 내용은 을 참조하십시오 ["9.6으로 데이터 계층화를 위해 GCP 계정 설정 및 추가"](#).
- 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
- 데이터 계층화를 사용하지 않는 경우, 후속 애그리게이트에서 사용하도록 설정할 수 있지만 시스템을 끄고 GCP 콘솔에서 서비스 계정을 추가해야 합니다.

["데이터 계층화에 대해 자세히 알아보십시오"](#).

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

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

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

필드에 입력합니다	설명
크기	입력할 수 있는 최대 크기는 씬 프로비저닝의 사용 여부에 따라 크게 달라집니다. 이를 통해 현재 사용 가능한 물리적 스토리지보다 더 큰 볼륨을 생성할 수 있습니다.
액세스 제어(NFS에만 해당)	엑스포트 정책은 볼륨에 액세스할 수 있는 서버넷의 클라이언트를 정의합니다. 기본적으로 Cloud Manager는 서버넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS 전용)	이러한 필드를 사용하면 사용자 및 그룹의 공유에 대한 액세스 수준(액세스 제어 목록 또는 ACL라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자 또는 그룹, UNIX 사용자 또는 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자의 도메인을 포함해야 합니다.



필드에 입력합니다	설명
스냅샷 정책	스냅샷 복사본 정책은 자동으로 생성되는 NetApp 스냅샷 복사본의 수와 빈도를 지정합니다. NetApp 스냅샷 복사본은 성능 영향이 없고 최소한의 스토리지가 필요한 시점 파일 시스템 이미지입니다. 기본 정책을 선택하거나 선택하지 않을 수 있습니다. Microsoft SQL Server의 tempdb와 같이 임시 데이터에 대해 없음을 선택할 수 있습니다.
고급 옵션(NFS에만 해당)	볼륨의 NFS 버전 선택: NFSv3 또는 NFSv4
이니시에이터 그룹 및 IQN(iSCSI 전용)	iSCSI 스토리지 타겟을 LUN(논리 유닛)이라고 하며 호스트에 표준 블록 디바이스로 표시됩니다. 이니시에이터 그룹은 iSCSI 호스트 노드 이름의 테이블이며 어떤 이니시에이터가 어떤 LUN을 액세스할 수 있는지 제어합니다. iSCSI 대상은 표준 이더넷 네트워크 어댑터(NIC), 소프트웨어 이니시에이터가 있는 TCP 오프로드 엔진(TOE) 카드, 통합 네트워크 어댑터(CNA) 또는 전용 호스트 파스트 어댑터(HBA)를 통해 네트워크에 연결되며 iSCSI 공인 이름(IQN)으로 식별됩니다. iSCSI 볼륨을 생성할 때 Cloud Manager에서 자동으로 LUN을 생성합니다. 볼륨 당 하나의 LUN만 생성하므로 관리가 필요 없습니다. 볼륨을 생성한 후 <b>"IQN을 사용하여 호스트에서 LUN에 연결합니다"</b> .

다음 이미지는 CIFS 프로토콜에 대해 작성된 볼륨 페이지를 보여 줍니다.

**Volume Details, Protection & Protocol**

Details & Protection	Protocol
<div style="display: flex; justify-content: space-between;"> <div> <b>Volume Name:</b>  <input style="width: 150px;" type="text" value="vol"/> </div> <div> <b>Size (GB):</b> ⓘ  <input style="width: 80px;" type="text" value="250"/> </div> </div> <div style="margin-top: 10px;"> <b>Snapshot Policy:</b>  <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> <span>default</span> <span style="font-size: 0.8em;">▼</span> </div> <div style="margin-top: 5px; font-size: 0.8em;">             ⓘ Default Policy           </div> </div>	<div style="display: flex; justify-content: space-around; border-bottom: 1px solid #ccc; padding-bottom: 5px;"> <span>NFS</span> <span style="border-bottom: 2px solid #0070C0;">CIFS</span> <span>iSCSI</span> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div> <b>Share name:</b>  <input style="width: 100px;" type="text" value="vol_share"/> </div> <div> <b>Permissions:</b>  <div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> <span>Full Control</span> <span style="font-size: 0.8em;">▼</span> </div> </div> </div> <div style="margin-top: 10px;"> <b>Users / Groups:</b>  <input style="width: 150px;" type="text" value="engineering"/> <div style="font-size: 0.8em; margin-top: 5px;">Valid users and groups separated by a semicolon</div> </div>

14. \* CIFS 설정 \*: CIFS 프로토콜을 선택한 경우 CIFS 서버를 설정합니다.

필드에 입력합니다	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다. Google Managed Active Directory를 구성하는 경우 기본적으로 169.254.169.254 IP 주소를 사용하여 AD에 액세스할 수 있습니다.
연결할 Active Directory 도메인입니다	CIFS 서버를 연결할 AD(Active Directory) 도메인의 FQDN입니다.
도메인에 가입하도록 승인된 자격 증명입니다	AD 도메인 내의 지정된 OU(조직 구성 단위)에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름 및 암호입니다.

필드에 입력합니다	설명
CIFS 서버 NetBIOS 이름입니다	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 구성 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. Google 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 * OU=Computers, OU=Cloud * 를 입력합니다. <a href="https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units">https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units</a> ["Google 클라우드 문서: Google Managed Microsoft AD의 조직 단위"]]
DNS 도메인	SVM(Cloud Volumes ONTAP 스토리지 가상 머신)용 DNS 도메인 대부분의 경우 도메인은 AD 도메인과 동일합니다.
NTP 서버	Active Directory DNS를 사용하여 NTP 서버를 구성하려면 * Active Directory 도메인 사용 * 을 선택합니다. 다른 주소를 사용하여 NTP 서버를 구성해야 하는 경우 API를 사용해야 합니다. 를 참조하십시오 <a href="#">"Cloud Manager 자동화 문서"</a> 를 참조하십시오. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 생성한 후에는 구성할 수 없습니다.

15. \* Usage Profile, Disk Type, Tiering Policy \*: 스토리지 효율성 기능을 사용하도록 설정하고 필요한 경우 볼륨 계층화 정책을 변경할 것인지 선택합니다.

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

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

Cloud Manager는 Cloud Volumes ONTAP 시스템을 구축합니다. 타임라인에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 시스템을 배포하는 데 문제가 있으면 오류 메시지를 검토합니다. 작업 환경을 선택하고 \* 환경 다시 작성 \* 을 클릭할 수도 있습니다.

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

작업을 마친 후

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

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

## GCP에서 HA 쌍 시작

Cloud Manager에서 작업 환경을 생성하여 GCP에서 Cloud Volumes ONTAP를 실행합니다.

단계

1. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 화면의 지시를 따릅니다.
2. \* 위치 선택 \*: \* Google Cloud \* 및 \* Cloud Volumes ONTAP HA \* 를 선택합니다.
3. \* 세부 정보 및 자격 증명 \*: 프로젝트를 선택하고 클러스터 이름을 지정한 다음 서비스 계정을 선택하고 선택적으로 레이블을 추가한 다음 자격 증명을 지정합니다.

다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
작업 환경 이름	Cloud Manager에서는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 GCP VM 인스턴스 모두에 이름을 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.
서비스 계정 이름입니다	를 사용할 계획인 경우 "계층화" 또는 "클라우드 백업" 서비스를 사용하려면 * 서비스 계정 * 스위치를 활성화한 다음 미리 정의된 스토리지 관리자 역할이 있는 서비스 계정을 선택해야 합니다.
레이블 추가	레이블은 GCP 리소스에 대한 메타데이터입니다. Cloud Manager는 시스템에 연결된 Cloud Volumes ONTAP 시스템 및 GCP 리소스에 레이블을 추가합니다. 작업 환경을 만들 때 사용자 인터페이스에서 최대 4개의 레이블을 추가할 수 있으며, 그런 다음 만든 후에 레이블을 더 추가할 수 있습니다. API는 작업 환경을 만들 때 레이블을 네 개로 제한하지 않습니다. 레이블에 대한 자세한 내용은 을 참조하십시오 "Google Cloud 설명서: 라벨 리소스".
사용자 이름 및 암호	Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하여 System Manager 또는 CLI를 통해 Cloud Volumes ONTAP에 연결할 수 있습니다. default_admin_user 이름을 유지하거나 사용자 지정 사용자 이름으로 변경합니다.
프로젝트 편집	<p>Cloud Volumes ONTAP가 상주할 프로젝트를 선택합니다. 기본 프로젝트는 Cloud Manager가 상주하는 프로젝트입니다.</p> <p>드롭다운 목록에 추가 프로젝트가 표시되지 않으면 Cloud Manager 서비스 계정을 다른 프로젝트와 연결하지 않은 것입니다. Google Cloud 콘솔로 이동하여 IAM 서비스를 열고 프로젝트를 선택합니다. Cloud Manager 역할이 있는 서비스 계정을 해당 프로젝트에 추가합니다. 각 프로젝트에 대해 이 단계를 반복해야 합니다.</p> <div>  <p>Cloud Manager에 대해 설정한 서비스 계정입니다. <a href="#">"이 페이지에 설명되어 있습니다"</a>.</p> </div> <p>선택한 자격 증명을 구독과 연결하려면 * 구독 추가 * 를 클릭합니다.</p> <p>용량제 Cloud Volumes ONTAP 시스템을 생성하려면 GCP 마켓플레이스에서 Cloud Volumes ONTAP 서브스크립션과 연관된 GCP 프로젝트를 선택해야 합니다.</p>

다음 비디오에서는 용량제 마켓플레이스 서브스크립션을 GCP 프로젝트에 연결하는 방법을 보여줍니다. 또는 에 있는 구독 단계를 따릅니다 ["Marketplace 구독을 GCP 자격 증명과 연결합니다"](#) 섹션을 참조하십시오.

▶ [https://docs.netapp.com/ko-kr/cloud-manager-cloud-volumes-ontap//media/video\\_subscribing\\_gcp.mp4](https://docs.netapp.com/ko-kr/cloud-manager-cloud-volumes-ontap//media/video_subscribing_gcp.mp4)

(video)

4. \* 서비스 \*: 이 시스템에서 사용할 서비스를 선택합니다. Cloud Backup을 선택하거나 Tiering을 사용하려면 3단계에서 서비스 계정을 지정해야 합니다.
5. \* HA 배포 모델 \*: HA 구성에 대해 여러 영역(권장) 또는 단일 영역을 선택합니다. 그런 다음 지역 및 구역을 선택합니다.

["HA 구축 모델에 대해 자세히 알아보십시오"](#).

6. \* 연결 \*: HA 구성을 위한 4개의 서로 다른 VPC, 각 VPC의 서브넷을 선택한 다음 방화벽 정책을 선택합니다.

["네트워킹 요구 사항에 대해 자세히 알아보십시오"](#).

7. \* 충전 방법 및 NSS 계정 \*: 이 시스템에서 사용할 충전 옵션을 지정한 다음 NetApp Support 사이트 계정을 지정합니다.
  - ["Cloud Volumes ONTAP의 라이선스 옵션에 대해 자세히 알아보십시오"](#).
  - ["라이선스 설정 방법에 대해 알아보십시오"](#).
8. \* 사전 구성된 패키지 \*: 패키지 중 하나를 선택하여 Cloud Volumes ONTAP 시스템을 신속하게 배포하거나 \* 고유한 구성 만들기 \* 를 클릭합니다.

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

9. \* 라이선스 \*: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 시스템 유형을 선택합니다.



선택한 버전에 대해 새로운 출시 후보, 일반 가용성 또는 패치 릴리스를 사용할 수 있는 경우, Cloud Manager는 작업 환경을 생성할 때 시스템을 해당 버전으로 업데이트합니다. 예를 들어, Cloud Volumes ONTAP 9.10.1 및 9.10.1 P4를 사용할 수 있는 경우 업데이트가 발생합니다. 업데이트는 한 릴리즈에서 다른 릴리즈로 발생하지 않습니다(예: 9.6에서 9.7로).

10. \* 기본 스토리지 리소스 \*: 초기 집계에 대한 설정(디스크 유형 및 각 디스크의 크기)을 선택합니다.

디스크 유형은 초기 볼륨입니다. 이후 볼륨에 대해 다른 디스크 유형을 선택할 수 있습니다.

디스크 크기는 초기 애그리게이트의 모든 디스크와 단순 프로비저닝 옵션을 사용할 때 Cloud Manager가 생성하는 추가 애그리게이트의 경우 모두 사용됩니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.

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

11. \* WORM \*: 필요한 경우 WORM(Write Once, Read Many) 스토리지를 활성화합니다.

데이터 계층화가 설정된 경우 WORM을 설정할 수 없습니다. ["WORM 스토리지에 대해 자세히 알아보십시오"](#).

12. \* Google Cloud Platform \* 의 데이터 계층화: 초기 애그리게이트에 데이터 계층화를 사용할 것인지, 계층형 데이터에 대한 스토리지 클래스를 선택한 다음 사전 정의된 스토리지 관리 역할이 있는 서비스 계정을 선택합니다.

다음 사항에 유의하십시오.

- Cloud Manager는 Cloud Volumes ONTAP 인스턴스에서 서비스 계정을 설정합니다. 이 서비스 계정은 Google Cloud Storage 버킷에 대한 데이터 계층화 권한을 제공합니다. Connector 서비스 계정을 계층화 서비스 계정의 사용자로 추가해야 합니다. 그렇지 않으면 Cloud Manager에서 선택할 수 없습니다.

- 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
- 데이터 계층화를 사용하지 않는 경우, 후속 애그리게이트에서 사용하도록 설정할 수 있지만 시스템을 끄고 GCP 콘솔에서 서비스 계정을 추가해야 합니다.

"데이터 계층화에 대해 자세히 알아보십시오".

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

"지원되는 클라이언트 프로토콜 및 버전에 대해 알아보십시오".

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

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

다음 이미지는 CIFS 프로토콜에 대해 작성된 볼륨 페이지를 보여 줍니다.

Volume Details, Protection & Protocol

### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy: default

Default Policy

### Protocol

NFS **CIFS** iSCSI

Share name:  Permissions: Full Control

Users / Groups:

Valid users and groups separated by a semicolon

14. \* CIFS 설정 \*: CIFS 프로토콜을 선택한 경우 CIFS 서버를 설정합니다.

필드에 입력합니다	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다. Google Managed Active Directory를 구성하는 경우 기본적으로 169.254.169.254 IP 주소를 사용하여 AD에 액세스할 수 있습니다.
연결할 Active Directory 도메인입니다	CIFS 서버를 연결할 AD(Active Directory) 도메인의 FQDN입니다.
도메인에 가입하도록 승인된 자격 증명입니다	AD 도메인 내의 지정된 OU(조직 구성 단위)에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름 및 암호입니다.
CIFS 서버 NetBIOS 이름입니다	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 구성 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다. Google 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 * OU=Computers, OU=Cloud * 를 입력합니다. <a href="https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units">https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units</a> ["Google 클라우드 문서: Google Managed Microsoft AD의 조직 단위"]
DNS 도메인	SVM(Cloud Volumes ONTAP 스토리지 가상 머신)용 DNS 도메인 대부분의 경우 도메인은 AD 도메인과 동일합니다.
NTP 서버	Active Directory DNS를 사용하여 NTP 서버를 구성하려면 * Active Directory 도메인 사용 * 을 선택합니다. 다른 주소를 사용하여 NTP 서버를 구성해야 하는 경우 API를 사용해야 합니다. 를 참조하십시오 <a href="#">"Cloud Manager 자동화 문서"</a> 를 참조하십시오. CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 생성한 후에는 구성할 수 없습니다.

15. \* Usage Profile, Disk Type, Tiering Policy \*: 스토리지 효율성 기능을 사용하도록 설정하고 필요한 경우 볼륨 계층화 정책을 변경할 것인지 선택합니다.

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

16. \* 검토 및 승인 \*: 선택 사항을 검토 및 확인합니다.

- a. 구성에 대한 세부 정보를 검토합니다.
- b. Cloud Manager가 구매할 지원 및 GCP 리소스에 대한 세부 정보를 검토하려면 \* 자세히 정보 \* 를 클릭합니다.
- c. 이해함... \* 확인란을 선택합니다.
- d. Go \* 를 클릭합니다.

Cloud Manager는 Cloud Volumes ONTAP 시스템을 구축합니다. 타임라인에서 진행 상황을 추적할 수 있습니다.

Cloud Volumes ONTAP 시스템을 배포하는 데 문제가 있으면 오류 메시지를 검토합니다. 작업 환경을 선택하고 \* 환경 다시 작성 \* 을 클릭할 수도 있습니다.

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

작업을 마친 후

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

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

## 저작권 정보

Copyright © 2022 NetApp, Inc. All rights reserved. 미국에서 인쇄된 본 문서의 어떤 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 그래픽, 전자적 또는 기계적 수단(사진 복사, 레코딩 등)으로도 저작권 소유자의 사전 서면 승인 없이 전자 검색 시스템에 저장 또는 저장.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지 사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 "있는 그대로" 제공되며 상품성 및 특정 목적에 대한 적합성에 대한 명시적 또는 묵시적 보증을 포함하여 이에 제한되지 않고, 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 또는 파생적 손해(소계 물품 또는 서비스의 조달, 사용 손실, 데이터 또는 수익 손실, 계약, 엄격한 책임 또는 불법 행위(과실 또는 그렇지 않은 경우)에 관계없이 어떠한 책임도 지지 않으며, 이는 이러한 손해의 가능성을 사전에 알고 있던 경우에도 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 구입의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

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

권리 제한 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.277-7103(1988년 10월) 및 FAR 52-227-19(1987년 6월)의 기술 데이터 및 컴퓨터 소프트웨어의 권리(Rights in Technical Data and Computer Software) 조항의 하위 조항 (c)(1)(ii)에 설명된 제한사항이 적용됩니다.

## 상표 정보

NETAPP, NETAPP 로고 및 에 나열된 마크는 NetApp에 있습니다 <http://www.netapp.com/TM> 는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.