



# Cloud Volumes ONTAP 설명서

## Cloud Volumes ONTAP

NetApp  
June 27, 2024

# 목차

Cloud Volumes ONTAP 설명서	1
릴리스 정보	2
새로운 기능	2
알려진 제한 사항	28
Cloud Volumes ONTAP 릴리즈 노트	29
시작하십시오	30
Cloud Volumes ONTAP에 대해 자세히 알아보십시오	30
새로운 배포에 지원되는 버전입니다	31
Amazon Web Services에서 시작하십시오	33
Microsoft Azure에서 시작하십시오	100
Google Cloud에서 시작하십시오	135
Cloud Volumes ONTAP를 사용합니다	186
라이선스 관리	186
볼륨 및 LUN 관리	200
통합 관리	226
스토리지 VM 관리	232
보안 및 데이터 암호화	267
시스템 관리	280
시스템 상태 및 이벤트입니다	312
개념	317
Cloud Volumes ONTAP 라이선스	317
스토리지	323
고가용성 쌍	345
보안	362
성능	364
노드 기반 BYOL의 라이선스 관리	365
AutoSupport 및 Active IQ 디지털 자문업체	368
Cloud Volumes ONTAP의 기본 구성입니다	369
지식 및 지원	373
지원을 위해 등록하십시오	373
도움을 받으십시오	377
법적 고지	383
저작권	383
상표	383
특허	383
개인 정보 보호 정책	383
오픈 소스	383

# Cloud Volumes ONTAP 설명서

# 릴리스 정보

## 새로운 기능

BlueXP에서 Cloud Volumes ONTAP 관리의 새로운 기능에 대해 알아보십시오.

이 페이지에 설명된 향상된 기능은 Cloud Volumes ONTAP 관리를 지원하는 BlueXP 기능에만 적용됩니다. Cloud Volumes ONTAP 소프트웨어 자체의 새로운 기능에 대해 알아보려면 ["Cloud Volumes ONTAP 릴리즈 노트 로 이동합니다"](#)

### 2023년 9월 10일

Connector 3.9.33 릴리스에서 다음과 같은 변경 사항이 적용되었습니다.

#### Azure에서 Lsv3 시리즈 VM 지원

이제 L48s\_v3 및 L64s\_v3 인스턴스 유형이 Azure의 Cloud Volumes ONTAP에서 지원되므로 9.13.1 릴리즈부터 단일 및 여러 가용 영역의 공유 관리 디스크를 사용한 단일 노드 및 고가용성 쌍 구축이 가능합니다. 이러한 인스턴스 유형은 Flash Cache를 지원합니다.

["Azure에서 Cloud Volumes ONTAP에 대해 지원되는 구성을 봅니다"](#)

["Azure에서 Cloud Volumes ONTAP의 스토리지 제한을 봅니다"](#)

### 2023년 7월 30일

다음 변경 사항은 커넥터의 3.9.32 릴리스에 도입되었습니다.

#### Flash Cache 및 Google Cloud의 고속 쓰기 지원

Google Cloud for Cloud Volumes ONTAP 9.13.1 이상에서는 Flash Cache 및 고속 쓰기 속도를 별도로 활성화할 수 있습니다. 지원되는 모든 인스턴스 유형에서 빠른 쓰기 속도를 사용할 수 있습니다. Flash Cache는 다음과 같은 인스턴스 유형에서 지원됩니다.

- N2-표준-16
- N2-표준-32
- N2-표준-48
- N2-표준-64

이러한 기능은 단일 노드 및 고가용성 쌍 구축 모두에서 개별적으로 또는 함께 사용할 수 있습니다.

["Google Cloud에서 Cloud Volumes ONTAP를 실행합니다"](#)

#### 사용 보고서 기능 향상

이제 사용 보고서 내에 표시되는 정보를 다양한 개선 사항을 사용할 수 있습니다. 다음은 사용 보고서의 향상된 기능입니다.

- 이제 TiB 단위는 컬럼 이름에 포함됩니다.

- 이제 일련 번호에 대한 새로운 "노드" 필드가 포함되었습니다.
- 이제 새로운 "워크로드 유형" 열이 스토리지 VM 사용량 보고서에 포함됩니다.
- 이제 스토리지 VM 및 볼륨 사용 보고서에 작업 환경 이름이 포함됩니다.
- 볼륨 유형 "파일"은 이제 "기본(읽기/쓰기)"으로 표시됩니다.
- 볼륨 유형 "보조"는 이제 "보조(DP)"로 표시됩니다.

사용 현황 보고서에 대한 자세한 내용은 을 참조하십시오 ["사용 보고서를 다운로드합니다"](#).

## 2023년 7월 26일

다음 변경 사항은 커넥터의 3.9.31 릴리스에 도입되었습니다.

### Cloud Volumes ONTAP 9.13.1 GA

BlueXP는 이제 AWS, Azure 및 Google Cloud에서 Cloud Volumes ONTAP 9.13.1 일반 가용성 릴리스를 배포하고 관리할 수 있습니다.

["이 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 자세히 알아보십시오"](#).

## 2023년 7월 2일

다음 변경 사항은 커넥터의 3.9.31 릴리스에 도입되었습니다.

### Azure에서 HA 다중 가용성 영역 구축 지원

Azure의 Japan East 및 Korea Central은 현재 Cloud Volumes ONTAP 9.12.1 GA 이상의 HA 다중 가용성 영역 배포를 지원합니다.

여러 가용 영역을 지원하는 모든 지역 목록은 를 참조하십시오 ["Azure 아래의 글로벌 지역 지도"](#).

### 자율주행 랜섬웨어 보호 지원

Cloud Volumes ONTAP에서는 자율 ARP(랜섬웨어 보호)가 현재 지원됩니다. ARP 지원은 Cloud Volumes ONTAP 버전 9.12.1 이상에서 사용할 수 있습니다.

Cloud Volumes ONTAP의 ARP에 대한 자세한 내용은 를 참조하십시오 ["자율 랜섬웨어 보호"](#).

## 2023년 6월 26일

다음 변경은 커넥터의 3.9.30 릴리스에 도입되었습니다.

### Cloud Volumes ONTAP 9.13.1 RC1

이제 BlueXP는 AWS, Azure 및 Google Cloud에서 Cloud Volumes ONTAP 9.13.1 을 배포하고 관리할 수 있습니다.

["이 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 자세히 알아보십시오"](#).

## 2023년 6월 4일

다음 변경은 커넥터의 3.9.30 릴리스에 도입되었습니다.

### Cloud Volumes ONTAP 업그레이드 버전 선택기 업데이트

Cloud Volumes ONTAP 업그레이드 페이지를 통해 최신 버전의 Cloud Volumes ONTAP 또는 이전 버전으로 업그레이드할 수 있습니다.

BlueXP를 통한 Cloud Volumes ONTAP 업그레이드에 대한 자세한 내용은 [을 참조하십시오 "Cloud Volumes ONTAP를 업그레이드합니다"](#).

## 2023년 5월 7일

Connector 3.9.29 릴리스에서 다음과 같은 변경 사항이 적용되었습니다.

### Qatar 지역이 이제 Google Cloud에서 지원됩니다

Qatar 지역은 현재 Google Cloud for Cloud Volumes ONTAP 및 Connector for Cloud Volumes ONTAP 9.12.1 GA 이상에서 지원됩니다.

이제 스웨덴 중앙 지역이 **Azure**에서 지원됩니다

이제 스웨덴 중앙 지역은 Azure for Cloud Volumes ONTAP 및 Cloud Volumes ONTAP 9.12.1 GA 이상의 커넥터에서 지원됩니다.

### Azure Australia East에서 HA 다중 가용성 영역 구축 지원

Azure의 오스트레일리아 동부 지역은 현재 Cloud Volumes ONTAP 9.12.1 GA 이상을 위한 HA 다중 가용성 영역 구축을 지원합니다.

충전 사용 내역이 없습니다

이제 용량 기반 라이선스를 구독할 때 부과되는 요금을 확인할 수 있습니다. BlueXP의 디지털 지갑에서 다음 유형의 사용 보고서를 다운로드할 수 있습니다. 사용 현황 보고서는 구독의 용량 세부 정보를 제공하고 Cloud Volumes ONTAP 구독에 포함된 리소스에 대한 비용 청구 방식을 알려줍니다. 다운로드할 수 있는 보고서는 다른 사용자와 쉽게 공유할 수 있습니다.

- Cloud Volumes ONTAP 패키지 사용
- 높은 수준의 사용
- 스토리지 VM 사용량
- 볼륨 사용량

자세한 내용은 [을 참조하십시오 "용량 기반 라이선스 관리"](#).

마켓플레이스 가입 없이 **BlueXP**에 액세스할 때 알림 메시지가 표시됩니다

이제 시장에 가입하지 않고 BlueXP에서 Cloud Volumes ONTAP에 액세스할 때마다 알림이 표시됩니다. 알림에는 "이 작업 환경에 대한 마켓플레이스 가입이 Cloud Volumes ONTAP 약관을 준수해야 합니다."라고 나와 있습니다.

## 2023년 4월 4일

Cloud Volumes ONTAP 9.12.1 GA부터 중국 지역이 다음과 같이 AWS에서 지원됩니다.

- 단일 노드 시스템이 지원됩니다.
- NetApp에서 직접 구매한 라이선스가 지원됩니다.

지역별 이용 가능 여부는 를 참조하십시오 ["Cloud Volumes ONTAP를 위한 글로벌 지역 맵"](#).

## 2023년 4월 3일

Connector 3.9.28 릴리스에서 다음과 같은 변경 사항이 도입되었습니다.

**Turin** 지역이 이제 **Google Cloud**에서 지원됩니다

Turin 지역은 현재 Google Cloud for Cloud Volumes ONTAP 및 Connector for Cloud Volumes ONTAP 9.12.1 GA 이상에서 지원됩니다.

**BlueXP** 디지털 지갑 기능 향상

이제 BlueXP 디지털 지갑에 시장 프라이빗 오퍼와 함께 구입한 라이선스 용량이 표시됩니다.

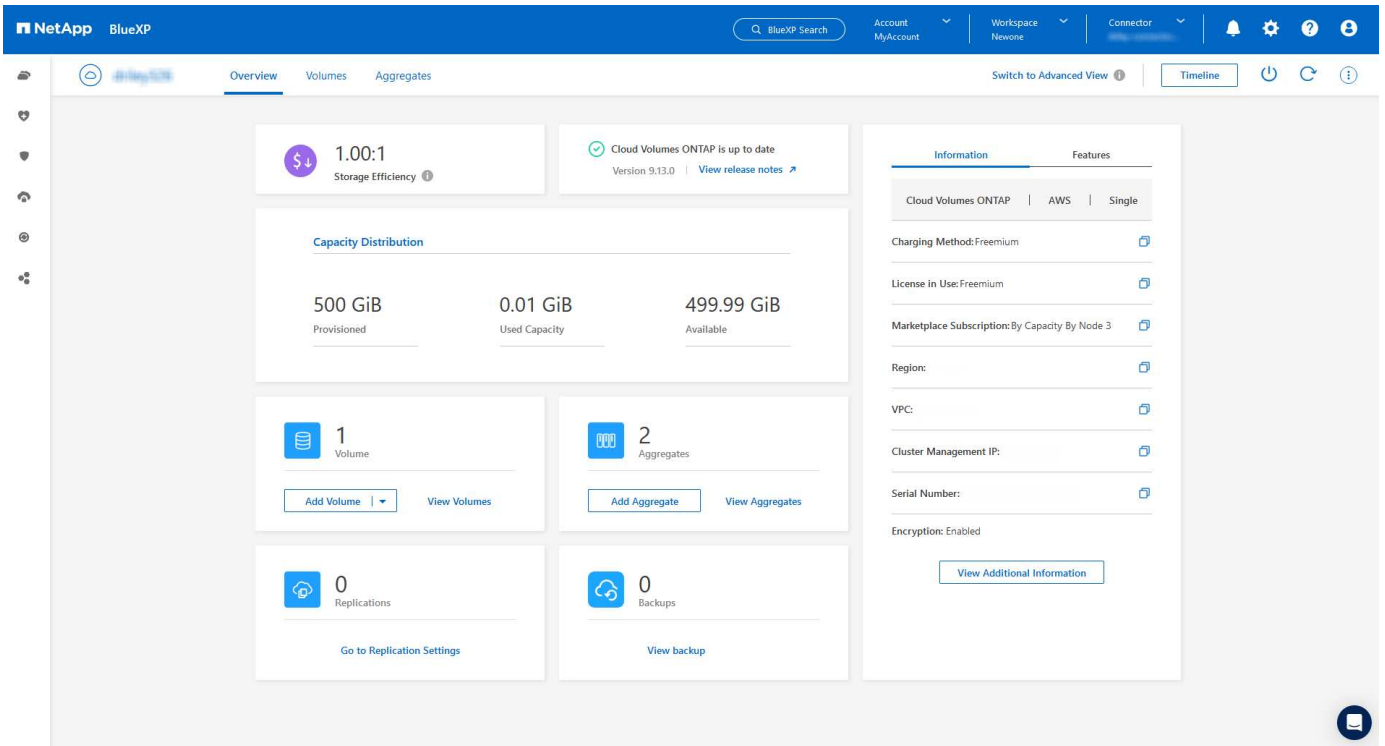
["계정에서 사용된 용량을 확인하는 방법에 대해 알아봅니다"](#).

볼륨 생성 중 주석 지원

이 릴리즈를 사용하면 API를 사용할 때 Cloud Volumes ONTAP FlexGroup 볼륨 또는 FlexVol 볼륨을 생성할 때 주석을 작성할 수 있습니다.

**Cloud Volumes ONTAP** 개요, 볼륨 및 집계 페이지를 위한 **BlueXP** 사용자 인터페이스 재설계

BlueXP는 이제 Cloud Volumes ONTAP 개요, 볼륨 및 집계 페이지에 대한 사용자 인터페이스를 새롭게 설계했습니다. 타일 기반 디자인은 각 타일에 보다 포괄적인 정보를 제공하여 사용자 경험을 향상시킬 수 있습니다.

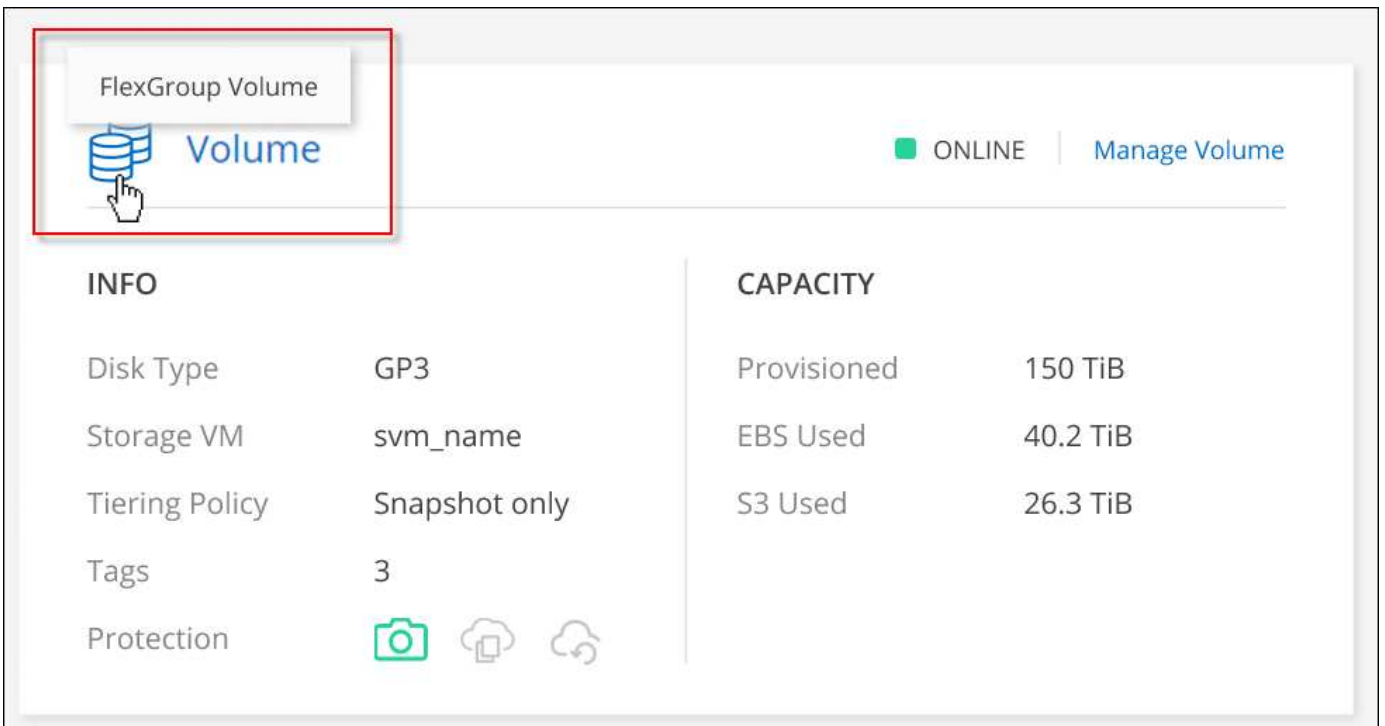


**FlexGroup 볼륨은 Cloud Volumes ONTAP를 통해 볼 수 있습니다**

CLI 또는 System Manager를 통해 직접 생성된 FlexGroup 볼륨은 이제 BlueXP의 재설계된 볼륨 타일을 통해 볼 수 있습니다. FlexVol 볼륨에 대해 제공된 정보와 동일한 BlueXP는 전용 볼륨 타일을 통해 생성된 FlexGroup 볼륨에 대한 자세한 정보를 제공합니다.



현재 BlueXP에서만 기존 FlexGroup 볼륨을 볼 수 있습니다. BlueXP에서 FlexGroup 볼륨을 생성하는 기능은 사용할 수 없지만 향후 릴리스에서 제공될 예정입니다.





"생성된 FlexGroup 볼륨을 보는 방법에 대해 자세히 알아보십시오."

## 2023년 3월 13일

### 중국 지역 지원

Cloud Volumes ONTAP 9.12.1 GA부터 중국 지역 지원이 Azure에서 다음과 같이 지원됩니다.

- Cloud Volumes ONTAP는 중국 북부에서 지원됩니다. 3.
- 단일 노드 시스템이 지원됩니다.
- NetApp에서 직접 구매한 라이선스가 지원됩니다.

지역별 이용 가능 여부는 를 참조하십시오 "[Cloud Volumes ONTAP를 위한 글로벌 지역 맵](#)".

## 2023년 3월 5일

Connector 3.9.27 릴리스에서 다음과 같은 변경 사항이 적용되었습니다.

### Cloud Volumes ONTAP 9.13.0

이제 BlueXP는 AWS, Azure 및 Google Cloud에서 Cloud Volumes ONTAP 9.13.0을 배포하고 관리할 수 있습니다.

"[이 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 자세히 알아보십시오](#)".

### Azure에서 16TiB 및 32TiB 지원

이제 Cloud Volumes ONTAP는 16TiB 및 32TiB 디스크 크기를 지원하여 Azure의 관리 대상 디스크에서 실행되는 고가용성 배포를 지원합니다.

에 대해 자세히 알아보십시오 "[Azure에서 지원되는 디스크 크기입니다](#)".

### MTEKM 라이선스

이제 MTEKM(멀티 테넌트 암호화 키 관리) 라이선스가 버전 9.12.1 GA 이상을 실행하는 새로운 기존 Cloud Volumes ONTAP 시스템과 함께 포함됩니다.

멀티 테넌트 외부 키 관리를 통해 NetApp Volume Encryption을 사용할 때 개별 스토리지 VM(SVM)이 KMIP 서버를 통해 자체 키를 유지할 수 있습니다.

"[NetApp 암호화 솔루션으로 볼륨을 암호화하는 방법을 알아보십시오](#)".

### 인터넷이 없는 환경 지원

Cloud Volumes ONTAP는 이제 인터넷으로부터 완전히 분리된 모든 클라우드 환경에서 지원됩니다. BYOL(노드 기반 라이선싱)만 이 환경에서 지원됩니다. 용량 기반 라이선스는 지원되지 않습니다. 시작하려면 커넥터 소프트웨어를 수동으로 설치하고, 커넥터에서 실행되는 BlueXP 콘솔에 로그인하고, BlueXP 디지털 지갑에 BYOL 라이선스를 추가한 다음 Cloud Volumes ONTAP를 구축하십시오.

- "[인터넷에 연결되지 않은 위치에 커넥터를 설치합니다](#)"
- "[커넥터의 BlueXP 콘솔에 액세스합니다](#)"

- ["할당되지 않은 라이선스를 추가합니다"](#)

## Google Cloud의 Flash Cache 및 빠른 쓰기 속도

Cloud Volumes ONTAP 9.13.0 릴리즈의 일부 인스턴스에서 Flash Cache, 높은 쓰기 속도 및 높은 MTU(최대 전송 단위)를 8,896바이트로 지원할 수 있습니다.

에 대해 자세히 알아보십시오 ["Google Cloud 라이선스에 의해 지원되는 구성"](#).

## 2023년 2월 5일

Connector 3.9.26 릴리스에서 다음과 같은 변경 사항이 도입되었습니다.

### AWS에서 반 배정 그룹 생성

이제 AWS HAAZ(단일 가용성 영역) 구축을 통해 반 배정 그룹을 생성할 수 있는 새로운 구성 설정이 제공됩니다. 이제 장애가 발생한 반 배정 그룹 생성을 생략하고 AWS HA 단일 AZ 구축을 성공적으로 완료하도록 선택할 수 있습니다.

반 배정 그룹 생성 설정을 구성하는 방법에 대한 자세한 내용은 ["AWS HA 단일 AZ에 대한 배치 그룹 생성 구성"](#)을 참조하십시오.

### 개인 DNS 영역 구성 업데이트

Azure Private Links를 사용할 때 개인 DNS 영역과 가상 네트워크 간의 링크를 만들지 않도록 새로운 구성 설정을 사용할 수 있습니다. 생성은 기본적으로 활성화되어 있습니다.

["Azure 프라이빗 DNS에 대한 자세한 내용은 BlueXP를 참조하십시오"](#)

### WORM 스토리지 및 데이터 계층화

이제 Cloud Volumes ONTAP 9.8 시스템 이상을 생성할 때 데이터 계층화와 WORM 스토리지를 함께 사용할 수 있습니다. WORM 스토리지를 통한 데이터 계층화를 사용하면 데이터를 클라우드의 오브젝트 저장소에 계층화할 수 있습니다.

["WORM 스토리지에 대해 자세히 알아보십시오."](#)

## 2023년 1월 1일

Connector 3.9.25 릴리스에서 다음과 같은 변경 사항이 도입되었습니다.

### Google Cloud에서 사용 가능한 라이선스 패키지

최적화된 에지 캐시 용량 기반 라이선스 패키지는 Google Cloud Marketplace에서 Cloud Volumes ONTAP에 대해 용량제 오퍼링을 제공하거나 연간 계약으로 제공됩니다.

을 참조하십시오 ["Cloud Volumes ONTAP 라이선스"](#).

### Cloud Volumes ONTAP의 기본 구성입니다

MTEKM(멀티 테넌트 암호화 키 관리) 라이선스는 새 Cloud Volumes ONTAP 배포에 더 이상 포함되지 않습니다.

Cloud Volumes ONTAP와 함께 자동으로 설치되는 ONTAP 기능 라이선스에 대한 자세한 내용은 [클 참조하십시오 "Cloud Volumes ONTAP의 기본 구성"](#).

## 2022년 12월 15일

### Cloud Volumes ONTAP 9.12.0

이제 BlueXP는 AWS 및 Google Cloud에서 Cloud Volumes ONTAP 9.12.0을 배포하고 관리할 수 있습니다.

["이 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 자세히 알아보십시오"](#).

## 2022년 12월 8일

### Cloud Volumes ONTAP 9.12.1

이제 BlueXP는 새로운 기능과 추가 클라우드 공급자 지역을 지원하는 Cloud Volumes ONTAP 9.12.1을 구축 및 관리할 수 있습니다.

["이 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 자세히 알아보십시오"](#)

## 2022년 12월 4일

Connector 3.9.24 릴리스에서 다음과 같은 변경 사항이 적용되었습니다.

**Cloud Volumes ONTAP 생성 중에 WORM + 클라우드 백업을 사용할 수 있습니다**

Cloud Volumes ONTAP 생성 프로세스 중에 WORM(Write Once, Read Many) 및 클라우드 백업 기능을 모두 활성화할 수 있습니다.

현재 이스라엘 지역은 **Google Cloud**에서 지원됩니다

현재 이스라엘 지역은 Google Cloud for Cloud Volumes ONTAP 및 Connector for Cloud Volumes ONTAP 9.11.1 P3 이상에서 지원됩니다.

## 2022년 11월 15일

Connector 3.9.23 릴리스에서 다음과 같은 변경 사항이 적용되었습니다.

**Google Cloud의 ONTAP S3 라이선스**

ONTAP S3 라이선스는 이제 Google 클라우드 플랫폼에서 버전 9.12.1 이상을 실행하는 신규 및 기존 Cloud Volumes ONTAP 시스템에 포함되어 있습니다.

["ONTAP에서 S3 오브젝트 스토리지 서비스를 구성 및 관리하는 방법에 대해 알아보십시오"](#)

## 2022년 11월 6일

Connector 3.9.23 릴리스에서 다음과 같은 변경 사항이 적용되었습니다.

**Azure**에서 리소스 그룹을 이동하는 중입니다

이제 동일한 Azure 가입 내에서 하나의 리소스 그룹에서 Azure의 다른 리소스 그룹으로 작업 환경을 이동할 수 있습니다.

자세한 내용은 을 참조하십시오 ["리소스 그룹 이동 중"](#).

### **NDMP-COPY 인증**

NDMP-copy는 현재 Cloud Volume ONTAP에서 사용하도록 인증되었습니다.

NDMP를 구성하고 사용하는 방법에 대한 자세한 내용은 을 참조하십시오 ["NDMP 구성 개요"](#).

### **Azure에 대한 관리형 디스크 암호화 지원**

이제 생성 시 모든 관리되는 디스크를 암호화할 수 있는 새로운 Azure 권한이 추가되었습니다.

이 새로운 기능에 대한 자세한 내용은 을 참조하십시오 ["Azure에서 고객이 관리하는 키를 사용하도록 Cloud Volumes ONTAP를 설정합니다"](#).

## **2022년 9월 18일**

Connector 3.9.22 릴리스에서 다음과 같은 변경 사항이 적용되었습니다.

### 디지털 지갑 기능 향상

- 이제 디지털 지갑에 최적화된 I/O 라이선스 패키지 및 사용자 계정의 Cloud Volumes ONTAP 시스템에 대해 프로비저닝된 WORM 용량에 대한 요약이 표시됩니다.

이러한 세부 정보를 통해 청구 방식 및 추가 용량 구매 여부를 보다 잘 파악할 수 있습니다.

["계정에서 사용된 용량을 확인하는 방법에 대해 알아보십시오"](#).

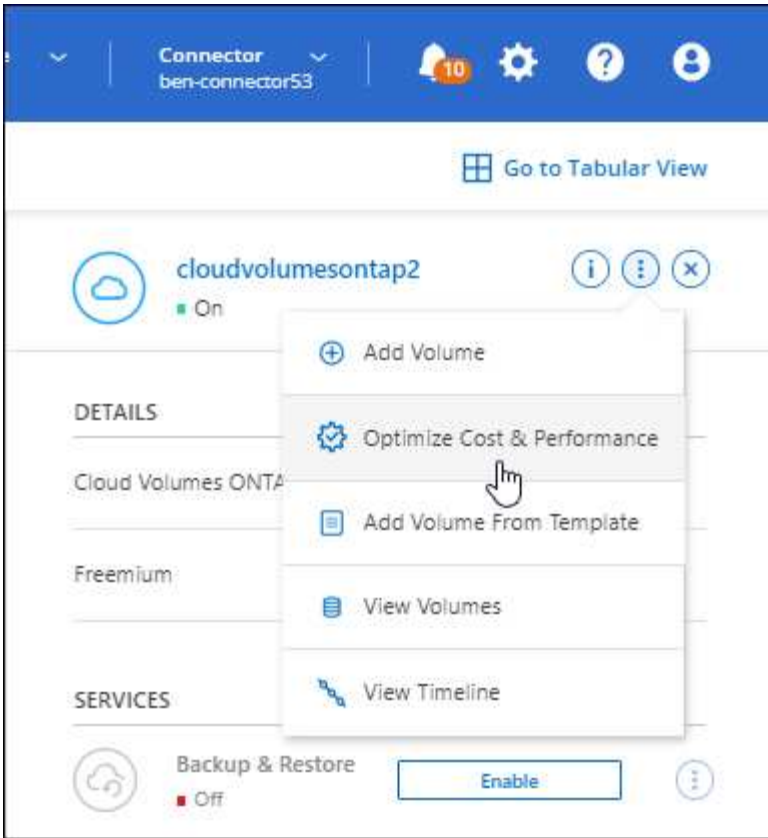
- 이제 하나의 충전 방법을 최적화된 충전 방법으로 변경할 수 있습니다.

["충전 방법을 변경하는 방법에 대해 알아보십시오"](#).

### 비용 및 성능 최적화

이제 Canvas에서 직접 Cloud Volumes ONTAP 시스템의 비용과 성능을 최적화할 수 있습니다.

작업 환경을 선택한 후 \* 비용 및 성능 최적화 \* 옵션을 선택하여 Cloud Volumes ONTAP의 인스턴스 유형을 변경할 수 있습니다. 더 작은 크기의 인스턴스를 선택하면 비용을 절감하고 더 큰 인스턴스로 변경하면 성능을 최적화할 수 있습니다.



## AutoSupport 알림

Cloud Volumes ONTAP 시스템에서 AutoSupport 메시지를 보낼 수 없는 경우 BlueXP에서 알림을 생성합니다. 이 알림에는 네트워킹 문제를 해결하는 데 사용할 수 있는 지침 링크가 포함되어 있습니다.

## 2022년 7월 31일

Connector 3.9.21 릴리스에서 다음과 같은 변경 사항이 적용되었습니다.

### MTEKM 라이선스

이제 MTEKM(멀티 테넌트 암호화 키 관리) 라이선스가 버전 9.11.1 이상을 실행하는 새로운 기존 Cloud Volumes ONTAP 시스템과 함께 포함됩니다.

멀티 테넌트 외부 키 관리를 통해 NetApp Volume Encryption을 사용할 때 개별 스토리지 VM(SVM)이 KMIP 서버를 통해 자체 키를 유지할 수 있습니다.

["NetApp 암호화 솔루션으로 볼륨을 암호화하는 방법을 알아보십시오."](#)

### 프록시 서버

이제 AutoSupport 메시지를 보낼 수 있는 아웃바운드 인터넷 연결을 사용할 수 없는 경우 BlueXP는 자동으로 커넥터를 프록시 서버로 사용하도록 Cloud Volumes ONTAP 시스템을 구성합니다.

AutoSupport은 능동적으로 시스템 상태를 모니터링하고 NetApp 기술 지원 팀에 메시지를 보냅니다.

유일한 요구 사항은 커넥터의 보안 그룹이 포트 3128을 통한 \_IN인바운드\_ 연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

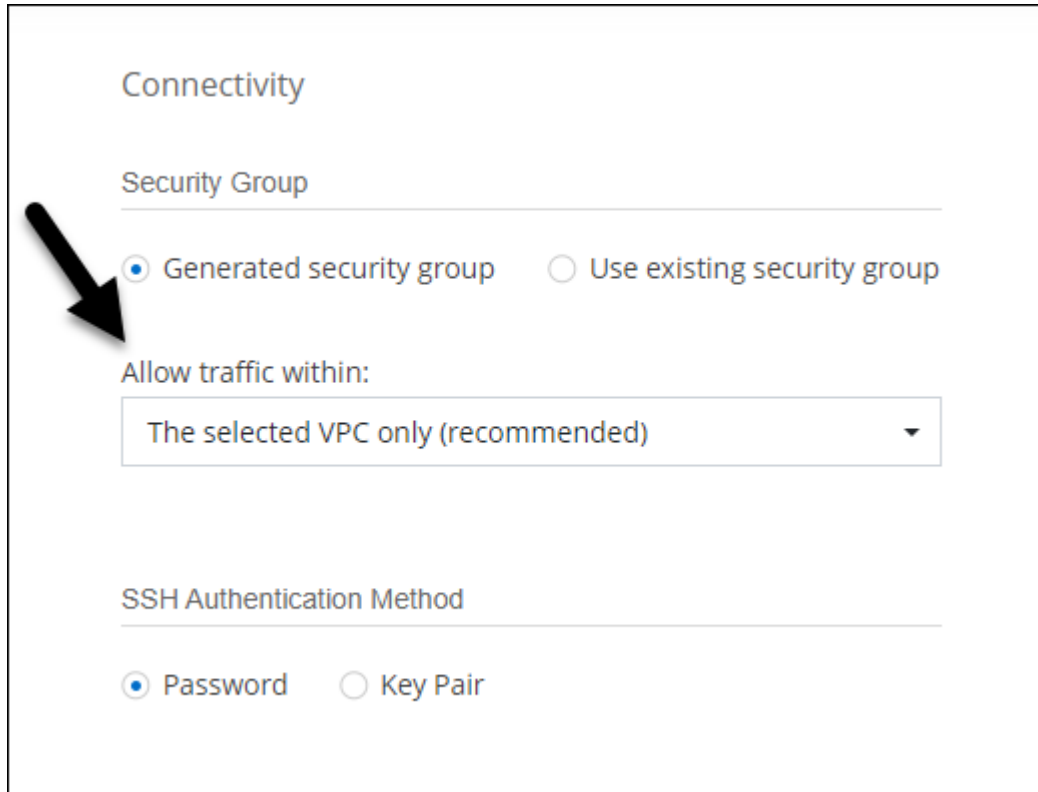
충전 방법을 변경하십시오

이제 용량 기반 라이선스를 사용하는 Cloud Volumes ONTAP 시스템의 충전 방법을 변경할 수 있습니다. 예를 들어, Essentials 패키지와 함께 Cloud Volumes ONTAP 시스템을 배포한 경우 비즈니스 요구사항이 변경되면 이를 Professional 패키지로 변경할 수 있습니다. 이 기능은 Digital Wallet에서 사용할 수 있습니다.

["충전 방법을 변경하는 방법에 대해 알아보십시오"](#).

보안 그룹 강화

Cloud Volumes ONTAP 작업 환경을 만들면 사용자 인터페이스를 통해 미리 정의된 보안 그룹이 선택한 네트워크 내에서만(권장) 또는 모든 네트워크 내의 트래픽을 허용할지 여부를 선택할 수 있습니다.



Connectivity

Security Group

Generated security group     Use existing security group

Allow traffic within:

The selected VPC only (recommended) ▼

SSH Authentication Method

Password     Key Pair

**2022년 7월 18일**

**Azure**의 새로운 라이선스 패키지

Azure Marketplace 구독을 통해 비용을 지불하는 Azure에서는 Cloud Volumes ONTAP에 대해 2가지 새로운 용량 기반 라이선스 패키지를 사용할 수 있습니다.

- \* 최적화 \*: 프로비저닝된 용량과 I/O 작업에 대해 별도로 비용을 지불합니다
- \* Edge Cache \*: 라이선스 "[Cloud Volumes Edge 캐시](#)"

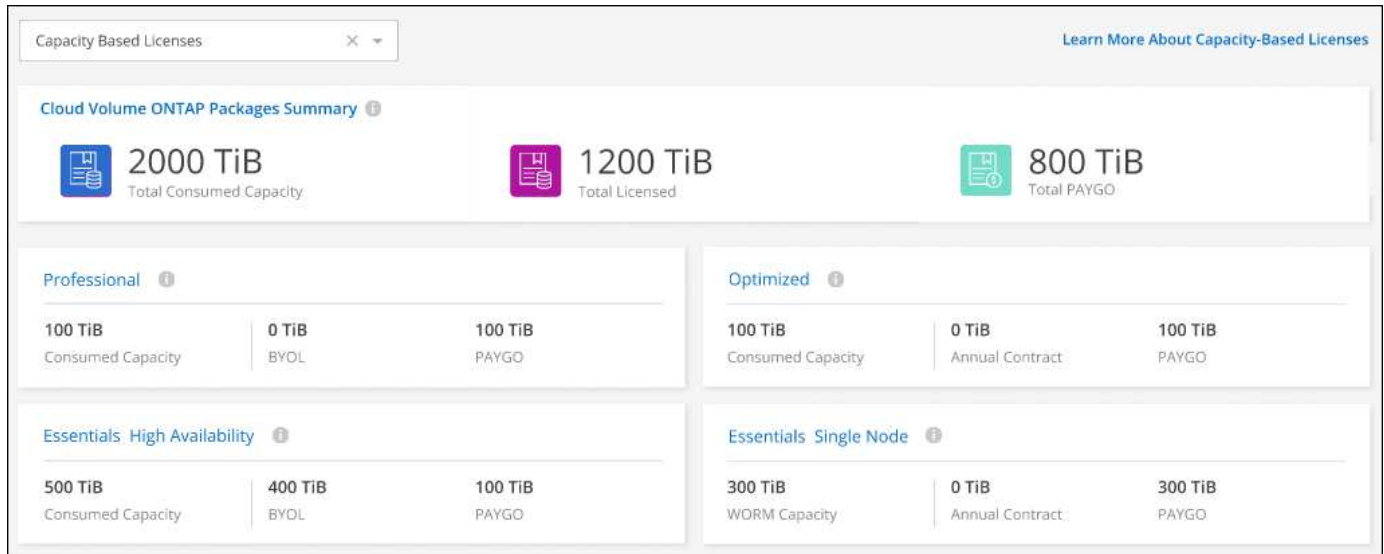
["이러한 라이선스 패키지에 대해 자세히 알아보십시오"](#).

**2022년 7월 3일**

Connector 3.9.20 릴리스에서 다음과 같은 변경 사항이 도입되었습니다.

## 디지털 지갑

이제 Digital Wallet은 사용자 계정의 총 소비된 용량과 라이선스 패키지별 소비된 용량을 표시합니다. 이를 통해 비용이 청구되는 방식 및 추가 용량을 구입해야 하는지 여부를 파악할 수 있습니다.



## 탄성 볼륨 개선

이제 BlueXP는 사용자 인터페이스에서 Cloud Volumes ONTAP 작업 환경을 생성할 때 Amazon EBS Elastic Volumes 기능을 지원합니다. GP3 또는 ios1 디스크를 사용하는 경우 Elastic Volumes 기능이 기본적으로 활성화됩니다. 스토리지 요구사항에 따라 초기 용량을 선택하고 Cloud Volumes ONTAP를 구축한 후 수정할 수 있습니다.

["AWS의 Elastic Volumes 지원에 대해 자세히 알아보십시오"](#).

## AWS의 ONTAP S3 라이선스

ONTAP S3 라이선스는 이제 AWS 버전 9.11.0 이상을 실행하는 신규 및 기존 Cloud Volumes ONTAP 시스템에 포함되어 있습니다.

["ONTAP에서 S3 오브젝트 스토리지 서비스를 구성 및 관리하는 방법에 대해 알아보십시오"](#)

## 새로운 Azure Cloud 지역 지원

9.10.1 릴리스부터는 Cloud Volumes ONTAP가 이제 Azure West US 3 지역에서 지원됩니다.

["Cloud Volumes ONTAP에 대해 지원되는 전체 영역 목록을 봅니다"](#)

## Azure의 ONTAP S3 라이선스

ONTAP S3 라이선스는 이제 Azure에서 버전 9.9.1 이상을 실행하는 신규 및 기존 Cloud Volumes ONTAP 시스템에 포함됩니다.

["ONTAP에서 S3 오브젝트 스토리지 서비스를 구성 및 관리하는 방법에 대해 알아보십시오"](#)

2022년 6월 7일

Connector 3.9.19 릴리스에서 다음과 같은 변경 사항이 적용되었습니다.

### Cloud Volumes ONTAP 9.11.1

이제 BlueXP는 새로운 기능과 추가 클라우드 공급자 지역을 지원하는 Cloud Volumes ONTAP 9.11.1을 배포 및 관리할 수 있습니다.

["이 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 자세히 알아보십시오"](#)

#### 새 고급 보기

Cloud Volumes ONTAP의 고급 관리를 수행해야 하는 경우 ONTAP 시스템과 함께 제공되는 관리 인터페이스인 ONTAP 시스템 관리자를 사용하여 이 작업을 수행할 수 있습니다. BlueXP에 System Manager 인터페이스를 직접 포함하므로 고급 관리를 위해 BlueXP를 떠날 필요가 없습니다.

이 고급 보기는 Cloud Volumes ONTAP 9.10.0 이상에서 미리 보기로 사용할 수 있습니다. NetApp은 이 경험을 개선하고 다음 릴리즈에서 향상된 기능을 추가할 계획입니다. 제품 내 채팅을 사용하여 피드백을 보내주십시오.

["고급 보기에 대해 자세히 알아보십시오"](#).

### Amazon EBS Elastic Volumes 지원

Cloud Volumes ONTAP aggregate에서 Amazon EBS Elastic Volumes 기능을 지원하여 더 나은 성능과 추가 용량을 제공하는 동시에 BlueXP에서 필요에 따라 기본 디스크 용량을 자동으로 늘릴 수 있습니다.

Elastic Volumes에 대한 지원은 `_new_` Cloud Volumes ONTAP 9.11.0 시스템과 GP3 및 ios1 EBS 디스크 유형으로 시작됩니다.

["Elastic Volumes 지원에 대해 자세히 알아보십시오"](#).

Elastic Volumes를 지원하려면 Connector에 대한 새로운 AWS 권한이 필요합니다.

```
"ec2:DescribeVolumesModifications",  
"ec2:ModifyVolume",
```

BlueXP에 추가한 각 AWS 자격 증명 세트에 이러한 권한을 제공해야 합니다. ["AWS에 대한 최신 커넥터 정책을 봅니다"](#).

### 공유 AWS 서브넷에 HA 쌍 구축 지원

Cloud Volumes ONTAP 9.11.1에는 AWS VPC 공유에 대한 지원이 포함되어 있습니다. 이번 릴리스의 Connector에서는 API를 사용할 때 AWS 공유 서브넷에 HA 쌍을 구축할 수 있습니다.

["공유 서브넷에 HA 쌍을 구축하는 방법을 알아보십시오"](#).

서비스 엔드포인트를 사용할 경우 네트워크 액세스가 제한됩니다

BlueXP는 이제 VNET 서비스 끝점을 사용하여 Cloud Volumes ONTAP와 스토리지 계정 간의 연결을 위해 네트워크 액세스를 제한합니다. BlueXP는 Azure Private Link 연결을 사용하지 않는 경우 서비스 끝점을 사용합니다.



["Cloud Volumes ONTAP를 사용한 Azure 전용 링크 연결에 대해 자세히 알아보십시오"](#).

## Google Cloud에서 스토리지 VM 생성 지원

이제 Google Cloud의 Cloud Volumes ONTAP에서 9.11.1 릴리즈부터 여러 스토리지 VM이 지원됩니다. 이번 커넥터 릴리즈부터 BlueXP를 사용하면 API를 사용하여 Google Cloud의 Cloud Volumes ONTAP HA 쌍에서 스토리지 VM을 생성할 수 있습니다.

스토리지 VM 생성을 지원하려면 Connector에 대한 새로운 Google Cloud 권한이 필요합니다.

- `compute.instanceGroups.get`
- `compute.addresses.get`

ONTAP CLI 또는 System Manager를 사용하여 단일 노드 시스템에 스토리지 VM을 생성해야 합니다.

- ["Google Cloud의 스토리지 VM 제한에 대해 자세히 알아보십시오"](#)
- ["Google Cloud에서 Cloud Volumes ONTAP용 데이터 서비스 스토리지 VM을 생성하는 방법을 알아보십시오"](#)

## 2022년 5월 2일

다음 변경 사항은 커넥터의 3.9.18 릴리스에 도입되었습니다.

### Cloud Volumes ONTAP 9.11.0

이제 BlueXP에서 Cloud Volumes ONTAP 9.11.0을 배포 및 관리할 수 있습니다.

["이 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 자세히 알아보십시오"](#).

### 중재자 업그레이드 개선

BlueXP가 HA 쌍의 중재자를 업그레이드할 때 이제 부팅 디스크를 삭제하기 전에 새 중재자 이미지를 사용할 수 있는지 확인합니다. 이 변경 사항은 업그레이드 프로세스가 실패할 경우 중재자가 계속해서 성공적으로 작동할 수 있도록 합니다.

### K8s 탭이 제거되었습니다

K8s 탭은 이전 버전에서 사용되지 않으며 이제 제거되었습니다. Kubernetes를 Cloud Volumes ONTAP와 함께 사용하려면 고급 데이터 관리를 위한 작업 환경으로 관리 Kubernetes 클러스터를 Canvas에 추가할 수 있습니다.

["BlueXP의 Kubernetes 데이터 관리에 대해 알아보십시오"](#)

### Azure에서 연간 계약

이제 Essentials 및 Professional 패키지는 Azure에서 연간 계약을 통해 제공됩니다. NetApp 세일즈 담당자에게 문의하여 연간 계약을 구매할 수 있습니다. 이 계약은 Azure 마켓플레이스에서 프라이빗 오퍼로 제공됩니다.

NetApp이 프라이빗 오퍼를 공유하면 작업 환경을 생성하는 동안 Azure 마켓플레이스에서 구독할 때 연간 계획을 선택할 수 있습니다.

["라이선스에 대해 자세히 알아보십시오"](#).

### S3 빙하 즉시 검색

이제 Amazon S3 Glacier Instant Retrieval 저장소 클래스에 계층화된 데이터를 저장할 수 있습니다.

["계층화된 데이터에 대한 스토리지 클래스를 변경하는 방법에 대해 알아보십시오"](#).

**Connector**에 새로운 **AWS** 권한이 필요합니다

이제 AZ(단일 가용성 영역)에 HA 쌍을 구축할 때 AWS 분산 배치 그룹을 생성하려면 다음 권한이 필요합니다.

```
"ec2:DescribePlacementGroups",  
"iam:GetRolePolicy",
```

이제 이러한 권한이 있어야 BlueXP에서 배치 그룹을 만드는 방법을 최적화할 수 있습니다.

BlueXP에 추가한 각 AWS 자격 증명 세트에 이러한 권한을 제공해야 합니다. ["AWS에 대한 최신 커넥터 정책을 봅니다"](#).

새로운 **Google Cloud** 지역 지원

Cloud Volumes ONTAP는 이제 9.10.1 릴리스부터 다음 Google 클라우드 영역에서 지원됩니다.

- 델리(아시아 - 남쪽 2)
- 멜번(호주 - 수테스토2)
- Milan (Europe-west8) - 단일 노드만 해당
- 산티아고(사우스메리카-west1) - 단일 노드만 해당

["Cloud Volumes ONTAP에 대해 지원되는 전체 영역 목록을 봅니다"](#)

**Google Cloud**에서 **n2-standard-16**을 지원합니다

이제 Google Cloud의 Cloud Volumes ONTAP에서 9.10.1 릴리즈부터 n2-standard-16 머신 유형이 지원됩니다.

["Google Cloud에서 Cloud Volumes ONTAP에 지원되는 구성을 봅니다"](#)

**Google Cloud** 방화벽 정책의 개선 사항

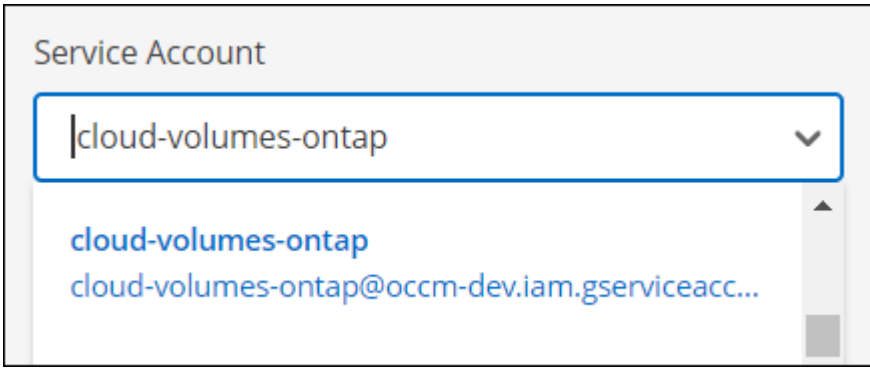
- Google Cloud에서 Cloud Volumes ONTAP HA 쌍을 생성하면 BlueXP가 VPC에 기존 방화벽 정책을 모두 표시합니다.

이전에는 BlueXP에서 대상 태그가 없는 VPC-1, VPC-2 또는 VPC-3에 정책을 표시하지 않았습니다.

- Google Cloud에서 Cloud Volumes ONTAP 단일 노드 시스템을 생성할 때, 이제 선택한 VPC 전용(권장) 또는 모든 VPC 내의 트래픽을 허용하도록 사전 정의된 방화벽 정책을 선택할 수 있습니다.

**Google Cloud** 서비스 계정 개선

Cloud Volumes ONTAP에서 사용할 Google Cloud 서비스 계정을 선택하면 BlueXP에 각 서비스 계정과 연결된 이메일 주소가 표시됩니다. 이메일 주소를 보면 동일한 이름을 공유하는 서비스 계정을 쉽게 구별할 수 있습니다.



## 2022년 4월 3일

### System Manager 링크가 제거되었습니다

이전에 Cloud Volumes ONTAP 작업 환경 내에서 사용할 수 있었던 시스템 관리자 링크가 제거되었습니다.

Cloud Volumes ONTAP 시스템에 연결된 웹 브라우저에 클러스터 관리 IP 주소를 입력하여 System Manager에 연결할 수도 있습니다. "[System Manager에 연결하는 방법에 대해 자세히 알아보십시오](#)".

### WORM 스토리지에 대한 충전 중

출시 특별 요금이 만료되었으므로 이제 WORM 스토리지 사용 요금이 부과됩니다. WORM 볼륨의 총 프로비저닝 용량에 따라 매시간 충전됩니다. 이는 신규 및 기존 Cloud Volumes ONTAP 시스템에 적용됩니다.

["WORM 스토리지 가격에 대해 자세히 알아보십시오"](#).

## 2022년 2월 27일

Connector 3.9.16 릴리스에서 다음과 같은 변경 사항이 적용되었습니다.

### 볼륨 마법사를 다시 설계했습니다

최근에 도입된 새 볼륨 생성 마법사는 \* 고급 할당 \* 옵션에서 특정 애그리게이트에 볼륨을 생성할 때 사용할 수 있습니다.

["특정 애그리게이트에서 볼륨을 생성하는 방법에 대해 알아보십시오"](#).

## 2022년 2월 9일

### 마켓플레이스 업데이트

- 이제 Essentials 패키지와 Professional 패키지를 모든 클라우드 공급자 마켓플레이스에서 사용할 수 있습니다.

이러한 용량을 기준으로 비용을 지불할 수 있으며, 연간 계약을 클라우드 공급자로부터 직접 구매할 수 있습니다. NetApp에서 직접 용량 라이선스를 구매할 수 있습니다.

클라우드 마켓플레이스에 기존 구독이 있는 경우 이러한 새로운 오퍼링을 자동으로 구독할 수 있습니다. 새로운 Cloud Volumes ONTAP 작업 환경을 구축할 때 용량 충전을 선택할 수 있습니다.

신규 고객인 경우 새 작업 환경을 만들 때 BlueXP에서 가입하라는 메시지를 표시합니다.

- 모든 클라우드 공급자 마켓플레이스의 노드별 라이선스는 더 이상 사용되지 않으며 새 가입자에게 더 이상 제공되지 않습니다. 여기에는 연간 계약 및 시간별 가입(탐색, 표준, 프리미엄)이 포함됩니다.

이 충전 방법은 활성 서브스크립션을 보유한 기존 고객에게도 계속 사용할 수 있습니다.

["Cloud Volumes ONTAP의 라이선스 옵션에 대해 자세히 알아보십시오"](#).

## 2022년 2월 6일

할당되지 않은 라이선스 교환

아직 사용하지 않은 Cloud Volumes ONTAP에 대해 할당되지 않은 노드 기반 라이선스가 있는 경우 Cloud Backup 라이선스, Cloud Data Sense 라이선스 또는 Cloud Tiering 라이선스로 변환하여 라이선스를 교환할 수 있습니다.

이 작업은 Cloud Volumes ONTAP 라이선스를 해지하고 만료 날짜가 동일한 서비스에 대해 달러 상당 라이선스를 생성합니다.

["할당되지 않은 노드 기반 라이선스를 교환하는 방법에 대해 알아보십시오"](#).

## 2022년 1월 30일

Connector 3.9.15 릴리스에서 다음과 같은 변경 사항이 도입되었습니다.

재설계된 라이선스 선택

새로운 Cloud Volumes ONTAP 작업 환경을 만들 때 라이선스 선택 화면을 다시 설계했습니다. 이 변경 사항은 2021년 7월에 소개된 용량 기준 과금 방법을 강조하며, 클라우드 공급자 마켓플레이스를 통해 예정된 오퍼링을 지원합니다.

디지털 지갑 업데이트

Cloud Volumes ONTAP 라이선스를 단일 탭에 통합하여 \* Digital Wallet \* 을 업데이트했습니다.

## 2022년 1월 2일

Connector 3.9.14 릴리스에서 다음과 같은 변경 사항이 도입되었습니다.

추가 **Azure VM** 유형 지원

Cloud Volumes ONTAP는 이제 Microsoft Azure에서 9.10.1 릴리즈부터 다음 VM 유형으로 지원됩니다.

- E4ds\_v4
- E8ds\_v4
- E32ds\_v4
- E48ds\_v4

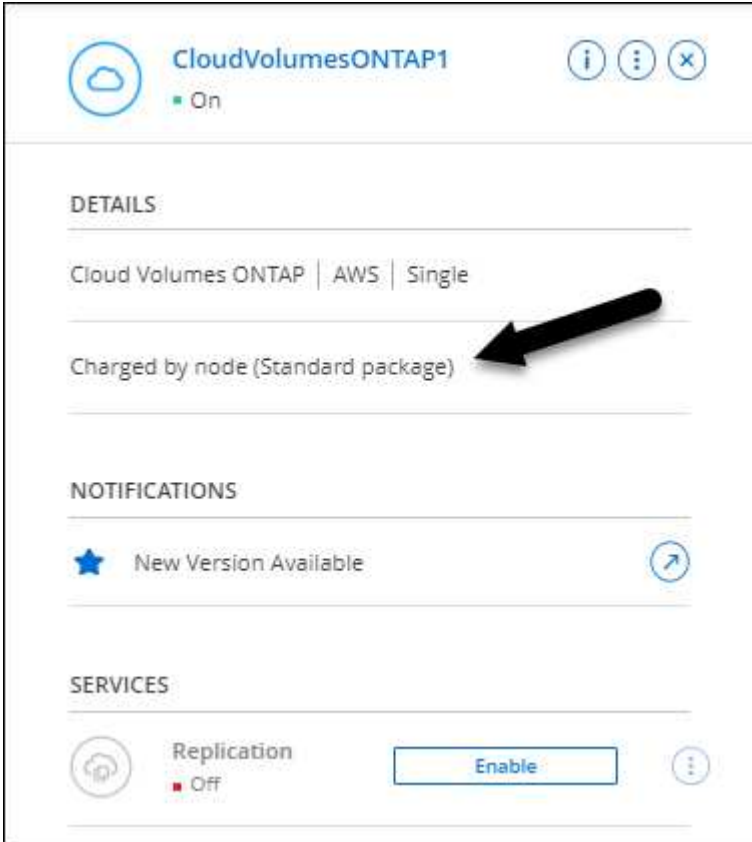
로 이동합니다 ["Cloud Volumes ONTAP 릴리즈 노트"](#) 지원되는 구성에 대한 자세한 내용은 를 참조하십시오.

## FlexClone 충전 업데이트

를 사용하는 경우 "용량 기반 라이선스" Cloud Volumes ONTAP의 경우 FlexClone 볼륨에 사용된 용량에 대해 더 이상 청구되지 않습니다.

충전 방법이 표시됩니다

BlueXP는 이제 Canvas의 오른쪽 패널에 있는 각 Cloud Volumes ONTAP 작업 환경에 대한 충전 방법을 보여 줍니다.



사용자 이름을 선택합니다

Cloud Volumes ONTAP 작업 환경을 만들면 기본 관리자 사용자 이름 대신 기본 사용자 이름을 입력할 수 있습니다.

Credentials

User Name

Password

Confirm Password

볼륨 생성 기능이 향상되었습니다

볼륨 생성을 위해 다음과 같은 몇 가지 기능이 향상되었습니다.

- 볼륨 생성 마법사를 쉽게 다시 설계했습니다.
- 볼륨에 추가한 태그는 이제 Application Templates 서비스와 연결되어 리소스 관리를 구성하고 단순화할 수 있습니다.
- 이제 NFS에 대한 사용자 지정 익스포트 정책을 선택할 수 있습니다.

Details, Protection & Tags  
  2 Protocol  
  3 Disk Type  
  4 Usage Profile & Tiering Policy  
  5 Review

**Volumes Protocol**

Select the volume's protocol:  
 NFS Protocol  
 CIFS Protocol  
 iSCSI Protocol

Access Control:

Export Policy (1 rule defined): [Manage volume's export policy](#)

## 2021년 11월 28일

Connector 3.9.13 릴리스에서 다음과 같은 변경 사항이 도입되었습니다.

### Cloud Volumes ONTAP 9.10.1

이제 BlueXP는 Cloud Volumes ONTAP 9.10.1을 구축하고 관리할 수 있습니다.

["이 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 자세히 알아보십시오"](#).

## NetApp Keystone 구독

이제 Keystone 가입을 통해 Cloud Volumes ONTAP HA 쌍에 대한 비용을 지불할 수 있습니다.

Keystone 가입은 선불 종량제 구독 기반 서비스로, OpEx 소비 모델을 선호하는 고객에게 원활한 하이브리드 클라우드 경험을 제공하여 자본 지출 또는 임대를 지원합니다.

Keystone 가입은 BlueXP에서 구축할 수 있는 모든 새로운 버전의 Cloud Volumes ONTAP에서 지원됩니다.

- ["NetApp Keystone 구독에 대해 자세히 알아보십시오"](#).
- ["BlueXP에서 Keystone 가입을 시작하는 방법을 알아보십시오"](#).

## 새로운 AWS 지역 지원

Cloud Volumes ONTAP는 현재 AWS 아시아 태평양(Osaka) 지역(AP-북동부-3)에서 지원됩니다.

## 포트 감소

포트 8023 및 4900은 단일 노드 시스템과 HA 쌍 모두에 대해 Azure의 Cloud Volumes ONTAP 시스템에서 더 이상 열리지 않습니다.

이 변경 사항은 커넥터의 3.9.13 릴리스부터 `_NEW_Cloud Volumes ONTAP` 시스템에 적용됩니다.

## 2021년 10월 4일

Connector의 3.9.11 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

### Cloud Volumes ONTAP 9.10.0

BlueXP는 이제 Cloud Volumes ONTAP 9.10.0을 구축 및 관리할 수 있습니다.

["이 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 자세히 알아보십시오"](#).

### 구축 시간 단축

일반 쓰기 속도를 사용하도록 설정한 경우 Microsoft Azure 또는 Google Cloud에서 Cloud Volumes ONTAP 작업 환경을 구축하는 데 걸리는 시간을 단축했습니다. 배포 시간은 이제 평균 3-4분 더 짧습니다.

## 2021년 9월 2일

Connector 3.9.10 릴리스에서 다음과 같은 변경 사항이 도입되었습니다.

### Azure에서 고객이 관리하는 암호화 키

Azure의 Cloud Volumes ONTAP에서 `키`를 사용하여 데이터가 자동으로 암호화됩니다. ["Azure 스토리지 서비스 암호화"](#) Microsoft 관리 키를 사용합니다. 그러나 이제 다음 단계를 완료하여 고객이 관리하는 암호화 키를 사용할 수 있습니다.

1. Azure에서 키 볼트를 작성한 다음 해당 볼트에 키를 생성합니다.
2. BlueXP에서 API를 사용하여 키를 사용하는 Cloud Volumes ONTAP 작업 환경을 만듭니다.

["이 단계에 대해 자세히 알아보십시오"](#).

## 2021년 7월 7일

커넥터 3.9.8 릴리스에는 다음과 같은 변경 사항이 도입되었습니다.

### 새로운 충전 방법

Cloud Volumes ONTAP에 새로운 충전 방법을 사용할 수 있습니다.

- \* 용량 기반 BYOL \*: 용량 기반 라이선스를 통해 Cloud Volumes ONTAP/TiB 용량 단위로 비용을 지불할 수 있습니다. 라이선스는 NetApp 계정에 연결되어 있으며 라이선스를 통해 사용할 수 있는 용량이 충분한 경우 여러 Cloud Volumes ONTAP 시스템을 생성할 수 있도록 지원합니다. 용량 기반 라이선스는 패키지 형태인 `_Essentials_`나 `_Professional_`로 제공됩니다.
- \* Freemium 제공 \*: Freemium을 통해 NetApp의 모든 Cloud Volumes ONTAP 기능을 무료로 사용할 수 있습니다(클라우드 공급자 요금은 여전히 적용됨). 시스템당 프로비저닝된 용량 500GiB로 제한되며 지원 계약이 없습니다. 최대 10개의 Freemium 시스템을 사용할 수 있습니다.


"이러한 라이선스 옵션에 대해 자세히 알아보십시오".

다음은 선택할 수 있는 충전 방법의 예입니다.


### Cloud Volumes ONTAP Charging Methods

[Learn more about our charging methods](#)

---

  Pay-As-You-Go by the hour

---

  Bring your own license


Bring your own license type

Capacity-Based ▼

Package

Professional ▼

---

  Freemium (Up to 500GB)

---

**WORM** 스토리지는 일반적인 용도로 사용할 수 있습니다

WORM(Write Once, Read Many) 스토리지는 더 이상 미리 보기에 표시되지 않으며 Cloud Volumes ONTAP에서



일반적으로 사용할 수 있습니다. "[WORM 스토리지에 대해 자세히 알아보십시오](#)".

### AWS에서 m5dn.24xlarge 지원

이제 Cloud Volumes ONTAP는 9.9.1 릴리스부터 PAYGO Premium, BYOL(Bring Your Own License) 및 Freemium과 같은 충전 방법을 사용하여 m5dn.24xLarge 인스턴스 유형을 지원합니다.

"[AWS에서 지원되는 Cloud Volumes ONTAP 구성 보기](#)".

기존 **Azure** 리소스 그룹을 선택합니다

Azure에서 Cloud Volumes ONTAP 시스템을 생성할 때 이제 VM 및 관련 리소스에 대한 기존 리소스 그룹을 선택할 수 있습니다.

The screenshot shows the 'Location & Connectivity' configuration page. Under the 'Connectivity' section, the 'Resource Group' field has two radio button options: 'Create a new group' and 'Use an existing group'. The 'Use an existing group' option is selected, and a red arrow points to it. Below this, the 'Resource Group Name' field contains the text 'RG1'.

배포 실패 또는 삭제 시 BlueXP에서 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거할 수 있는 권한은 다음과 같습니다.

```
"Microsoft.Network/privateEndpoints/delete",  
"Microsoft.Compute/availabilitySets/delete",
```

BlueXP에 추가한 각 Azure 자격 증명 세트에 이러한 권한을 제공해야 합니다. "[Azure의 최신 커넥터 정책을 봅니다](#)".

이제 **Azure**에서 **BLOB** 공용 액세스가 비활성화되었습니다

보안을 강화하기 위해 BlueXP는 Cloud Volumes ONTAP용 저장소 계정을 만들 때 \* Blob 공용 액세스 \* 를 비활성화합니다.

### Azure Private Link 기능 향상

기본적으로 BlueXP는 새 Cloud Volumes ONTAP 시스템의 부팅 진단 저장소 계정에서 Azure Private Link 연결을 활성화합니다.

즉, Cloud Volumes ONTAP의 `_ALL_STORAGE` 계정은 이제 전용 링크를 사용합니다.

["Cloud Volumes ONTAP에서 Azure 프라이빗 링크를 사용하는 방법에 대해 자세히 알아보십시오."](#)

## Google Cloud에서 균형 잡힌 영구 디스크

9.9.1 릴리스부터 Cloud Volumes ONTAP는 이제 균형 유지 디스크(PD 균형 조정)를 지원합니다.

이러한 SSD는 GiB당 더 낮은 IOPS를 제공하여 성능과 비용의 균형을 유지합니다.

### Custom-4-16384 Google Cloud에서는 더 이상 지원되지 않습니다

CUSTOM-4-16384 시스템 유형은 새로운 Cloud Volumes ONTAP 시스템에서 더 이상 지원되지 않습니다.

이 기계 유형에서 실행 중인 기존 시스템이 있는 경우 계속 사용할 수 있지만 n2-standard-4 기계 유형으로 전환하는 것이 좋습니다.

["GCP에서 Cloud Volumes ONTAP에 대해 지원되는 구성을 봅니다."](#)

## 2021년 5월 30일

Connector 3.9.7 릴리스에서 다음과 같은 변경 사항이 적용되었습니다.

### AWS의 새로운 프로페셔널 패키지

새로운 프로페셔널 패키지를 이용하면 AWS 마켓플레이스의 연간 계약을 활용하여 Cloud Volumes ONTAP와 Cloud Backup Service를 번들로 제공할 수 있습니다. 지급은 TiB당. 이 구독을 통해 온프레미스 데이터를 백업할 수 없습니다.

이 지불 옵션을 선택하면 EBS 디스크를 통해 Cloud Volumes ONTAP 시스템당 최대 2개의 PiB를 프로비저닝하고 S3 오브젝트 스토리지(단일 노드 또는 HA)로 계층화할 수 있습니다.

로 이동합니다 ["AWS 마켓플레이스 페이지를 참조하십시오"](#) 가격 세부 정보를 보려면 로 이동하십시오 ["Cloud Volumes ONTAP 릴리즈 노트"](#) 이 라이선스 옵션에 대해 자세히 알아보십시오.

### AWS의 EBS 볼륨에 있는 태그

이제 BlueXP는 새로운 Cloud Volumes ONTAP 작업 환경을 만들 때 EBS 볼륨에 태그를 추가합니다. 이 태그는 Cloud Volumes ONTAP를 배포한 후에 이미 생성되었습니다.

조직에서 SCP(서비스 제어 정책)를 사용하여 사용 권한을 관리하는 경우 이 변경 사항이 도움이 될 수 있습니다.

### 자동 계층화 정책의 최소 냉각 기간

auto\_Tiering 정책을 사용하여 볼륨에 대한 데이터 계층화를 활성화한 경우 이제 API를 사용하여 최소 냉각 기간을 조정할 수 있습니다.

["최소 냉각 기간을 조정하는 방법에 대해 알아보십시오."](#)

### 사용자 지정 익스포트 정책의 개선

새 NFS 볼륨을 생성하면 BlueXP에서 사용자 지정 내보내기 정책을 오름차순으로 표시하여 필요한 익스포트 정책을 쉽게 찾을 수 있습니다.

## 이전 클라우드 스냅샷 삭제

BlueXP는 이제 Cloud Volumes ONTAP 시스템을 배포하고 전원을 켤 때마다 생성된 루트 및 부팅 디스크의 이전 클라우드 스냅샷을 삭제합니다. 가장 최근의 두 스냅샷만 루트 볼륨과 부팅 볼륨 모두에 대해 보존됩니다.

이러한 기능 향상으로 더 이상 필요하지 않은 스냅샷을 제거하여 클라우드 공급자 비용을 절감할 수 있습니다.

Connector에는 Azure 스냅샷을 삭제할 수 있는 새로운 권한이 필요합니다. "[Azure의 최신 커넥터 정책을 봅니다](#)".

```
"Microsoft.Compute/snapshots/delete"
```

## 2021년 5월 24일

### Cloud Volumes ONTAP 9.9.1

이제 BlueXP에서 Cloud Volumes ONTAP 9.9.1을 배포하고 관리할 수 있습니다.

["이 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 자세히 알아보십시오"](#).

## 2021년 4월 11일

커넥터의 3.9.5 릴리스와 함께 다음과 같은 변경 사항이 도입되었습니다.

### 논리적 공간 보고

이제 BlueXP는 Cloud Volumes ONTAP에 대해 생성되는 초기 스토리지 VM에 대한 논리적 공간 보고를 지원합니다.

공간이 논리적으로 보고되면 ONTAP에서는 스토리지 효율성 기능으로 절약된 모든 물리적 공간이 사용된 것으로 보고하도록 볼륨 공간을 보고합니다.

### AWS에서 GP3 디스크 지원

Cloud Volumes ONTAP는 이제 9.7 릴리즈부터 \_GP3(General Purpose SSD)\_디스크를 지원합니다. GP3 디스크는 광범위한 워크로드에 대한 비용과 성능의 균형을 맞추는 가장 경제적인 SSD입니다.

["Cloud Volumes ONTAP에서 GP3 디스크를 사용하는 방법에 대해 자세히 알아보십시오"](#).

콜드 HDD 디스크는 AWS에서 더 이상 지원되지 않습니다

Cloud Volumes ONTAP는 더 이상 콜드 HDD(SC1) 디스크를 지원하지 않습니다.

### Azure 저장소 계정용 TLS 1.2

BlueXP가 Azure for Cloud Volumes ONTAP에서 저장소 계정을 만들 때 저장소 계정의 TLS 버전은 이제 1.2입니다.

## 2021년 3월 8일

Connector 3.9.4 릴리스에 다음과 같은 변경 사항이 적용되었습니다.

## Cloud Volumes ONTAP 9.9.0

BlueXP는 이제 Cloud Volumes ONTAP 9.9.0을 구축 및 관리할 수 있습니다.

["이 Cloud Volumes ONTAP 릴리스에 포함된 새로운 기능에 대해 자세히 알아보십시오."](#)

### AWS C2S 환경 지원

이제 C2S(AWS 상용 클라우드 서비스) 환경에 Cloud Volumes ONTAP 9.8을 구축할 수 있습니다.

["C2S에서 시작하는 방법에 대해 알아보십시오."](#)

### 고객 관리 CMK를 통한 AWS 암호화

BlueXP에서는 항상 AWS KMS(키 관리 서비스)를 사용하여 Cloud Volumes ONTAP 데이터를 암호화할 수 있습니다. Cloud Volumes ONTAP 9.9.0부터 EBS 디스크의 데이터와 고객이 관리하는 CMK를 선택하면 S3로 계층화된 데이터가 암호화됩니다. 이전에는 EBS 데이터만 암호화되었습니다.

CMK를 사용하려면 Cloud Volumes ONTAP IAM 역할을 제공해야 합니다.

["Cloud Volumes ONTAP를 사용하여 AWS KMS를 설정하는 방법에 대해 자세히 알아보십시오."](#)

### Azure DoD 지원

이제 Azure 국방부(DoD) Impact Level 6(IL6)에 Cloud Volumes ONTAP 9.8을 배포할 수 있습니다.

### Google Cloud의 IP 주소 감소

Cloud Volumes ONTAP 9.8 이상의 Google Cloud에 필요한 IP 주소 수를 줄였습니다. 기본적으로 IP 주소가 하나만 있으면 됩니다(인터클러스터 LIF를 노드 관리 LIF와 통합함). API를 사용할 때 SVM 관리 LIF 생성을 건너뛸 수도 있으므로 추가 IP 주소가 필요하지 않습니다.

["Google Cloud의 IP 주소 요구 사항에 대해 자세히 알아보십시오."](#)

### Google Cloud에서 공유 VPC 지원

Google Cloud에 Cloud Volumes ONTAP HA 쌍을 구축하면 VPC-1, VPC-2 및 VPC-3용 공유 VPC를 선택할 수 있습니다. 이전에는 VPC-0만 공유 VPC가 될 수 있었습니다. 이 변경 사항은 Cloud Volumes ONTAP 9.8 이상에서 지원됩니다.

["Google Cloud 네트워킹 요구 사항에 대해 자세히 알아보십시오."](#)

## 2021년 1월 4일

Connector 3.9.2 릴리스에서 다음과 같은 변경 사항이 도입되었습니다.

### AWS 아웃포스트

몇 개월 전, Cloud Volumes ONTAP은 AWS(Amazon Web Services) 아웃포스트 준비 지정을 달성했다고 발표했습니다. 오늘, AWS 아웃포스트에서 BlueXP 및 Cloud Volumes ONTAP의 검증을 마쳤습니다.

AWS 아웃포스트가 있는 경우 작업 환경 마법사에서 아웃포스트 VPC를 선택하여 해당 아웃포스트에 Cloud Volumes

ONTAP를 구축할 수 있습니다. 이러한 경험은 AWS에 상주하는 다른 VPC와 동일합니다. 먼저 AWS Outpost에 Connector를 구축해야 합니다.

몇 가지 제한 사항이 있습니다.

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

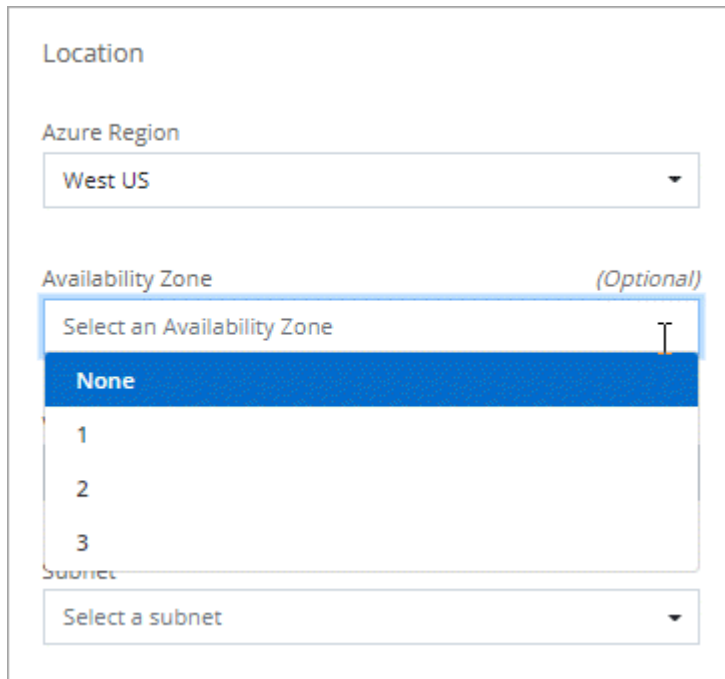
### 지원되는 Azure 지역의 Ultra SSD VNV RAM

이제 Cloud Volumes ONTAP는 단일 노드 시스템에서 E32s\_v3 VM 유형을 사용할 때 Ultra SSD를 VNV RAM으로 사용할 수 있습니다 "[지원되는 모든 Azure 지역에서 제공됩니다](#)".

VNV RAM은 향상된 쓰기 성능을 제공합니다.

### Azure에서 가용성 영역을 선택합니다

이제 단일 노드 Cloud Volumes ONTAP 시스템을 구축할 가용성 영역을 선택할 수 있습니다. AZ를 선택하지 않으면 BlueXP가 사용자를 위해 하나를 선택합니다.



The screenshot shows a configuration window for Azure. Under the 'Location' section, the 'Azure Region' is set to 'West US'. Below it, the 'Availability Zone' section is labeled '(Optional)'. A dropdown menu is open, showing 'Select an Availability Zone' at the top, followed by 'None' (highlighted in blue), '1', '2', and '3'. At the bottom of the configuration window, there is a 'Subnet' dropdown menu with 'Select a subnet' as the current selection.

### Google Cloud의 더 큰 디스크

이제 Cloud Volumes ONTAP는 GCP에서 64TB 디스크를 지원합니다.



GCP 제한으로 인해 디스크만 사용할 경우 최대 시스템 용량은 256TB로 유지됩니다.

## Google Cloud의 새로운 컴퓨터 유형

Cloud Volumes ONTAP는 이제 다음과 같은 기계 유형을 지원합니다.

- N2-standard-4(Explore 라이선스와 BYOL 포함)
- 표준 라이선스와 BYOL의 N2-Standard-8
- 프리미엄 라이선스가 있고 BYOL이 있는 N2-STANDARD-32

## 2020년 11월 3일

다음 변경 사항은 Connector의 3.9.0 릴리스에 도입되었습니다.

### Cloud Volumes ONTAP용 Azure 프라이빗 링크

기본적으로 BlueXP에서는 이제 Cloud Volumes ONTAP 및 관련 저장소 계정 간에 Azure Private Link 연결을 사용할 수 있습니다. 전용 링크는 Azure의 엔드포인트 간 연결을 보호합니다.

- ["Azure 프라이빗 링크에 대해 자세히 알아보십시오"](#)
- ["Cloud Volumes ONTAP에서 Azure 프라이빗 링크를 사용하는 방법에 대해 자세히 알아보십시오"](#)

## 알려진 제한 사항

알려진 제한 사항은 이 제품 릴리스에서 지원하지 않거나 올바르게 상호 운용되지 않는 플랫폼, 장치 또는 기능을 식별합니다. 이러한 제한 사항을 주의 깊게 검토하십시오.

이러한 제한은 BlueXP의 Cloud Volumes ONTAP 관리에만 적용됩니다. Cloud Volumes ONTAP 소프트웨어 자체의 제한 사항을 보려면 ["Cloud Volumes ONTAP 릴리즈 노트 로 이동합니다"](#)

### BlueXP는 FlexGroup 볼륨 생성을 지원하지 않습니다

Cloud Volumes ONTAP는 FlexGroup 볼륨을 지원하지만 BlueXP는 현재 FlexGroup 볼륨 생성을 지원하지 않습니다. 시스템 관리자 또는 CLI에서 FlexGroup 볼륨을 생성하는 경우 BlueXP의 용량 관리 모드를 수동으로 설정해야 합니다. FlexGroup 볼륨에서 자동 모드가 제대로 작동하지 않을 수 있습니다.



BlueXP에서 FlexGroup 볼륨을 생성할 수 있는 기능은 향후 릴리스에 제공될 예정입니다.

### BlueXP는 Cloud Volumes ONTAP에서 S3을 지원하지 않습니다

Cloud Volumes ONTAP는 S3를 스케일 아웃 스토리지 옵션으로 지원하지만 BlueXP는 이 기능에 대한 관리 기능을 제공하지 않습니다. CLI를 사용하는 것이 Cloud Volumes ONTAP에서 S3 클라이언트 액세스를 구성하는 모범 사례입니다. 자세한 내용은 ["S3 구성 전원 가이드"](#).

["S3 및 기타 클라이언트 프로토콜에 대한 Cloud Volumes ONTAP 지원에 대해 자세히 알아보십시오"](#).

### BlueXP는 스토리지 VM의 재해 복구를 지원하지 않습니다

BlueXP는 스토리지 VM(SVM) 재해 복구에 대한 설정 또는 오케스트레이션 지원을 제공하지 않습니다. System Manager 또는 CLI를 사용해야 합니다.

"SVM 재해 복구에 대해 자세히 알아보십시오".

## AsciiDoc 문자 교체 및 내장 속성 테스트

모든 언어의 현지화 및 게시를 통해 종단 간 테스트

별표

{별표}

텍스트 \*

텍스트 \*

텍스트 {별표} 텍스트

이중 콜론

::

텍스트 ::

텍스트 ::

텍스트 :: 텍스트입니다

세로 막대

|

텍스트 |

텍스트 |

텍스트 | 텍스트

또한

+

텍스트 +

텍스트 +

텍스트 + 텍스트

대괄호

[ 및 ]

텍스트 [ 및 텍스트 ]

텍스트 [ 및 텍스트 ]

텍스트 [ 및 텍스트 ] 텍스트입니다

줄 바꿈하지 않는 공간

이전

너비가 0인 공간

이전

## Cloud Volumes ONTAP 릴리즈 노트

Cloud Volumes ONTAP용 릴리스 정보 에서는 릴리스별 정보를 제공합니다. 이번 릴리즈의 새로운 기능, 지원되는 구성, 스토리지 제한, 제품 기능에 영향을 줄 수 있는 알려진 제한 사항 또는 문제

"[Cloud Volumes ONTAP 릴리즈 노트](#) 로 이동합니다"

# 시작하십시오

## Cloud Volumes ONTAP에 대해 자세히 알아보십시오

Cloud Volumes ONTAP를 사용하면 클라우드 스토리지 비용과 성능을 최적화하는 동시에 데이터 보호, 보안 및 규정 준수를 향상할 수 있습니다.

Cloud Volumes ONTAP은 클라우드에서 ONTAP 데이터 관리 소프트웨어를 실행하는 소프트웨어 전용 스토리지 어플라이언스입니다. 엔터프라이즈급 스토리지에 다음 주요 기능을 제공하며 다음 테스트 시 다음과 같습니다.

- 스토리지 효율성

내장된 데이터 중복제거, 데이터 압축, 씬 프로비저닝 및 복제를 활용하여 스토리지 비용을 최소화합니다.

- 고가용성

클라우드 환경에서 장애가 발생할 경우 엔터프라이즈급 안정성과 지속적인 운영을 보장합니다.

- 데이터 보호

Cloud Volumes ONTAP는 업계 최고 수준의 NetApp 복제 기술인 SnapMirror를 활용하여 사내 데이터를 클라우드로 복제하므로 여러 사용 사례에서 2차 복사본을 쉽게 사용할 수 있습니다.

또한 Cloud Volumes ONTAP는 BlueXP 백업 및 복구 기능과 통합되어 클라우드 데이터의 보호 및 장기 아카이브를 위한 백업 및 복원 기능을 제공합니다.

["BlueXP 백업 및 복구에 대해 자세히 알아보십시오"](#)

- 데이터 계층화

애플리케이션을 오프라인으로 전환하지 않고도 필요에 따라 고성능 및 고성능 스토리지 풀 간에 전환할 수 있습니다.

- 애플리케이션 정합성

NetApp SnapCenter를 사용하여 NetApp Snapshot 복사본의 일관성을 보장합니다.

["SnapCenter에 대해 자세히 알아보십시오"](#)

- 데이터 보안

Cloud Volumes ONTAP는 데이터 암호화를 지원하고 바이러스 및 랜섬웨어에 대한 보호를 제공합니다.

- 개인 정보 보호 규정 준수 관리

BlueXP 분류와의 통합으로 데이터 컨텍스트를 이해하고 중요한 데이터를 식별할 수 있습니다.

["BlueXP 분류에 대해 자세히 알아보십시오"](#)



ONTAP 기능에 대한 라이선스는 Cloud Volumes ONTAP에 포함되어 있습니다.



"지원되는 Cloud Volumes ONTAP 구성을 봅니다"

"Cloud Volumes ONTAP에 대해 자세히 알아보십시오"

## 새로운 배포에 지원되는 버전입니다

BlueXP를 사용하면 새로운 Cloud Volumes ONTAP 작업 환경을 만들 때 여러 ONTAP 버전 중에서 선택할 수 있습니다.

다른 모든 Cloud Volumes ONTAP 버전은 새 배포에서 지원되지 않습니다.

### 설치하고

#### 단일 노드

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

#### HA 쌍

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

### Azure를 지원합니다

#### 단일 노드

- 9.13.1 GA
- 9.12.1 GA

- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3입니다
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6
- 9.5 P6

#### **HA 쌍**

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3입니다
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6

#### **Google 클라우드**

##### 단일 노드

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

#### **HA 쌍**

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1

- 9.9.1 P6
- 9.8

## Amazon Web Services에서 시작하십시오

### AWS에서 Cloud Volumes ONTAP를 빠르게 시작합니다

몇 가지 단계를 통해 AWS에서 Cloud Volumes ONTAP를 시작하십시오.

1

커넥터를 작성합니다

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

인터넷에 액세스할 수 없는 서브넷에 Cloud Volumes ONTAP를 배포하려는 경우 수동으로 커넥터를 설치하고 해당 커넥터에서 실행 중인 BlueXP 사용자 인터페이스에 액세스해야 합니다. ["인터넷에 액세스하지 않고 커넥터에 수동으로 설치하는 방법에 대해 알아보십시오"](#)

2

구성을 계획합니다

BlueXP는 워크로드 요구 사항에 맞는 사전 구성된 패키지를 제공하거나 사용자가 직접 구성할 수 있습니다. 자신의 구성을 선택하는 경우 사용 가능한 옵션을 이해해야 합니다. ["자세한 정보"](#).

3

네트워크 설정

1. VPC와 서브넷이 커넥터와 Cloud Volumes ONTAP 간의 연결을 지원하는지 확인합니다.
2. NetApp AutoSupport용 VPC 타겟으로부터 아웃바운드 인터넷 액세스 지원

인터넷에 액세스할 수 없는 위치에 Cloud Volumes ONTAP를 배포하는 경우에는 이 단계가 필요하지 않습니다.

3. VPC 엔드포인트를 S3 서비스로 설정합니다.

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

["네트워킹 요구 사항에 대해 자세히 알아보십시오"](#).

4

AWS KMS를 설정합니다

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

5

BlueXP를 사용하여 Cloud Volumes ONTAP를 실행합니다

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

."

관련 링크

- ["BlueXP에서 커넥터 만들기"](#)
- ["AWS Marketplace에서 커넥터 실행"](#)
- ["Linux 호스트에 Connector 소프트웨어 설치"](#)
- ["BlueXP에서 AWS 권한을 사용하는 경우"](#)

## AWS에서 Cloud Volumes ONTAP 구성 계획

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

**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 AWS 지역에서 지원됩니다. ["지원되는 영역의 전체 목록을 봅니다"](#).

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

지원되는 인스턴스를 선택합니다

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

["AWS에서 Cloud Volumes ONTAP가 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.

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

**AWS에서 시스템 크기 조정**

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

## 인스턴스 유형

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

## EBS 디스크 유형입니다

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

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

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

Cloud Volumes ONTAP는 GP3 디스크를 사용하는 Amazon EBS Elastic Volumes 기능을 지원합니다. ["Elastic Volumes 지원에 대해 자세히 알아보십시오"](#).

- [\\_GP2\(General Purpose SSD\)\\_디스크](#)는 광범위한 워크로드에 대해 비용과 성능의 균형을 맞춥니다. 성능은 IOPS 측면에서 정의됩니다.
- [\\_provisioned IOPS ssd\(i1\)\\_disk](#)는 높은 비용으로 최고의 성능을 요구하는 중요한 응용 프로그램을 위한 것입니다.

Cloud Volumes ONTAP는 [iio1](#) 디스크에서 Amazon EBS Elastic Volumes 기능을 지원합니다. ["Elastic Volumes 지원에 대해 자세히 알아보십시오"](#).

- [\\_Throughput Optimized HDD\(st1\)\\_디스크](#)는 낮은 가격으로 빠르고 일관된 처리량을 필요로 하는 자주 액세스되는 워크로드에 적합합니다.



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

## EBS 디스크 크기입니다

를 지원하지 않는 구성을 선택하는 경우 ["Amazon EBS Elastic Volumes 기능"](#) 그런 다음 Cloud Volumes ONTAP 시스템을 시작할 때 초기 디스크 크기를 선택해야 합니다. 그 이후에는 가능합니다 ["BlueXP에서 시스템 용량을 관리할 수 있습니다"](#) 하지만 원하는 경우 ["스스로 애그리게이트를 생성합니다"](#) 다음 사항에 유의하십시오.

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

IOPS를 가져오지 못할 수 있습니다.

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

위에서 설명한 것처럼, Amazon EBS Elastic Volumes 기능을 지원하는 Cloud Volumes ONTAP 구성에서는 디스크 크기를 선택할 수 없습니다. ["Elastic Volumes 지원에 대해 자세히 알아보십시오"](#).

기본 시스템 디스크를 봅니다

BlueXP는 사용자 데이터를 위한 스토리지 외에도 Cloud Volumes ONTAP 시스템 데이터(부팅 데이터, 루트 데이터, 핵심 데이터 및 NVRAM)를 위한 클라우드 스토리지를 구입합니다. 계획을 위해 Cloud Volumes ONTAP를 배포하기 전에 이러한 세부 정보를 검토하는 것이 도움이 될 수 있습니다.

["AWS에서 Cloud Volumes ONTAP 시스템 데이터의 기본 디스크를 봅니다"](#).



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

### AWS 아웃포스트에 Cloud Volumes ONTAP 구축 준비

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

몇 가지 제한 사항이 있습니다.

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

네트워킹 정보를 수집합니다

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

단일 노드 또는 HA 2노드 AZ

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

여러 대의 AZs에서 HA 쌍

확인하십시오	귀사의 가치
지역	

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

#### 쓰기 속도를 선택합니다

BlueXP에서는 Cloud Volumes ONTAP에 대한 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. BlueXP에서 볼륨을 생성할 때 이러한 기능을 활성화하는 프로필이나 해당 기능을 비활성화하는 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.

#### 씬 프로비저닝

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

#### 중복 제거

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

#### 압축

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

## 네트워크 설정

### AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항

BlueXP는 IP 주소, 넷마스크 및 라우트와 같은 Cloud Volumes ONTAP용 네트워킹 구성 요소 설정을 처리합니다. 아웃바운드 인터넷 액세스를 사용할 수 있는지, 충분한 전용 IP 주소를 사용할 수 있는지, 올바른 연결이 있는지 등을 확인해야 합니다.

#### 일반 요구 사항

AWS에서 다음 요구사항을 충족해야 합니다.

#### Cloud Volumes ONTAP 노드에 대한 아웃바운드 인터넷 액세스

Cloud Volumes ONTAP 노드를 사용하려면 NetApp AutoSupport에 대한 아웃바운드 인터넷 액세스가 필요합니다. 사전 예방적으로 시스템의 상태를 모니터링하고 메시지를 NetApp 기술 지원으로 보냅니다.

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>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

NAT 인스턴스가 있는 경우 개인 서브넷에서 인터넷으로 HTTPS 트래픽을 허용하는 인바운드 보안 그룹 규칙을 정의해야 합니다.

AutoSupport 메시지를 보내는 데 아웃바운드 인터넷 연결을 사용할 수 없는 경우 BlueXP는 자동으로 Cloud Volumes ONTAP 시스템에서 커넥터를 프록시 서버로 사용하도록 구성합니다. 유일한 요구 사항은 커넥터의 보안 그룹이 포트 3128을 통한 \_IN인바운드\_ 연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

Cloud Volumes ONTAP에 대해 엄격한 아웃바운드 규칙을 정의한 경우 Cloud Volumes ONTAP 보안 그룹이 포트 3128을 통한 \_outbound\_connection을 허용하는지 확인해야 합니다.

아웃바운드 인터넷 액세스가 가능한지 확인한 후 AutoSupport를 테스트하여 메시지를 보낼 수 있는지 확인할 수 있습니다. 자세한 지침은 을 참조하십시오 ["ONTAP 문서: AutoSupport 설정"](#).

BlueXP에서 AutoSupport 메시지를 보낼 수 없다고 알리는 경우 ["AutoSupport 구성 문제를 해결합니다"](#).

#### HA 중재자를 위한 아웃바운드 인터넷 액세스

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

수동 옵션은 대상 서브넷에서 AWS EC2 서비스로 연결되는 NAT 게이트웨이 또는 인터페이스 VPC 엔드포인트일 수 있습니다. VPC 엔드포인트에 대한 자세한 내용은 을 참조하십시오 ["AWS 문서: 인터페이스 VPC 엔드포인트\(AWS PrivateLink\)"](#).

#### 전용 IP 주소

BlueXP는 필요한 수의 전용 IP 주소를 Cloud Volumes ONTAP에 자동으로 할당합니다. 네트워킹에 사용 가능한 개인 IP 주소가 충분한지 확인해야 합니다.



BlueXP에서 Cloud Volumes ONTAP에 할당하는 LIF 수는 단일 노드 시스템을 배포할지 HA 쌍을 구축하는지에 따라 달라집니다. LIF는 물리적 포트와 연결된 IP 주소입니다.

단일 노드 시스템의 **IP** 주소입니다

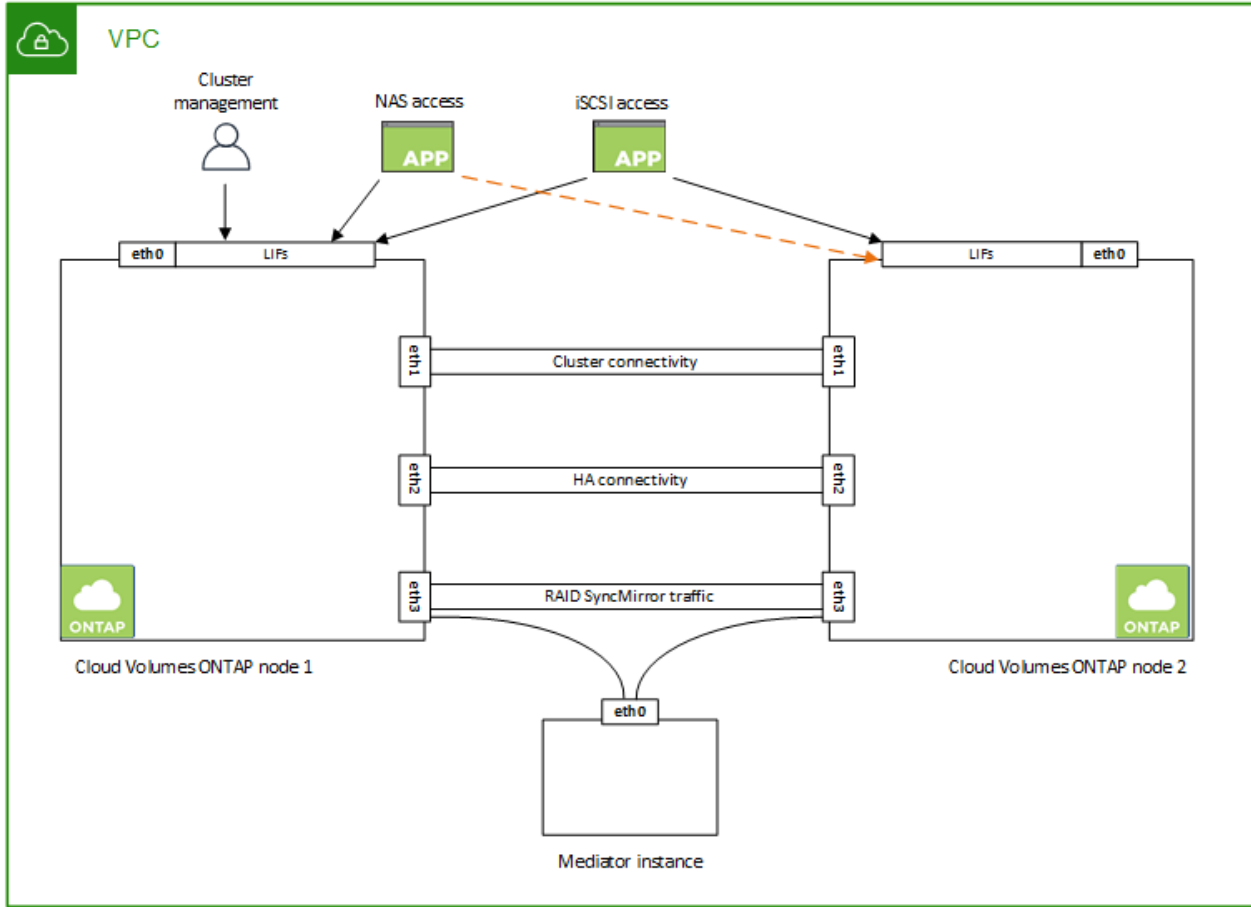
BlueXP는 단일 노드 시스템에 6개의 IP 주소를 할당합니다.

다음 표에는 각 프라이빗 IP 주소와 연결된 LIF에 대한 자세한 정보가 나와 있습니다.

LIF	목적
클러스터 관리	전체 클러스터(HA 쌍)의 관리
노드 관리	노드의 관리.
인터클러스터	클러스터 간 통신, 백업 및 복제
NAS 데이터	NAS 프로토콜을 통한 클라이언트 액세스
iSCSI 데이터	iSCSI 프로토콜을 통한 클라이언트 액세스. 또한 시스템에서 다른 중요한 네트워킹 워크플로우에 사용됩니다. 이 LIF는 필수 항목이므로 삭제할 수 없습니다.
스토리지 VM 관리	스토리지 VM 관리 LIF는 SnapCenter와 같은 관리 툴과 함께 사용됩니다.

#### HA 쌍의 IP 주소

HA Pair의 경우 단일 노드 시스템보다 더 많은 IP 주소가 필요합니다. 이러한 IP 주소는 다음 이미지와 같이 서로 다른 이더넷 인터페이스에 분산됩니다.



HA 쌍에 필요한 사설 IP 주소의 수는 선택한 구축 모델에 따라 다릅니다. AZ(Single\_AWS Availability Zone)에 구축된 HA 쌍에는 15개의 프라이빗 IP 주소가 필요하고, \_multiple\_AZs에 구축된 HA 쌍에는 13개의 프라이빗 IP 주소가 필요합니다.

다음 표에는 각 프라이빗 IP 주소와 연결된 LIF에 대한 자세한 정보가 나와 있습니다.

**단일 AZ에서 HA 쌍을 지원하는 LIF**

LIF	인터페이스	노드	목적
클러스터 관리	eth0	노드 1	전체 클러스터(HA 쌍)의 관리
노드 관리	eth0	노드 1 및 노드 2	노드의 관리.
인터클러스터	eth0	노드 1 및 노드 2	클러스터 간 통신, 백업 및 복제
NAS 데이터	eth0	노드 1	NAS 프로토콜을 통한 클라이언트 액세스
iSCSI 데이터	eth0	노드 1 및 노드 2	iSCSI 프로토콜을 통한 클라이언트 액세스. 또한 시스템에서 다른 중요한 네트워킹 워크플로우에 사용됩니다. 이러한 LIF는 필수 항목이므로 삭제할 수 없습니다.

LIF	인터페이스	노드	목적
클러스터 연결	eth1	노드 1 및 노드 2	노드가 서로 통신하고 클러스터 내에서 데이터를 이동할 수 있도록 지원합니다.
HA 연결	윤리2	노드 1 및 노드 2	페일오버 시 두 노드 간의 통신.
RSM iSCSI 트래픽입니다	eth3	노드 1 및 노드 2	RAID SyncMirror iSCSI 트래픽과 두 Cloud Volumes ONTAP 노드 및 중재자 간의 통신
중재자	eth0	중재자	스토리지 테이크오버 및 반환 프로세스를 지원하는 노드와 중재자 간의 통신 채널

### 여러 AZs의 HA 쌍에 대한 LIF

LIF	인터페이스	노드	목적
노드 관리	eth0	노드 1 및 노드 2	노드의 관리.
인터클러스터	eth0	노드 1 및 노드 2	클러스터 간 통신, 백업 및 복제
iSCSI 데이터	eth0	노드 1 및 노드 2	iSCSI 프로토콜을 통한 클라이언트 액세스. 이러한 LIF는 노드 간 부동 IP 주소의 마이그레이션도 관리합니다. 이러한 LIF는 필수 항목이므로 삭제할 수 없습니다.
클러스터 연결	eth1	노드 1 및 노드 2	노드가 서로 통신하고 클러스터 내에서 데이터를 이동할 수 있도록 지원합니다.
HA 연결	윤리2	노드 1 및 노드 2	페일오버 시 두 노드 간의 통신.
RSM iSCSI 트래픽입니다	eth3	노드 1 및 노드 2	RAID SyncMirror iSCSI 트래픽과 두 Cloud Volumes ONTAP 노드 및 중재자 간의 통신
중재자	eth0	중재자	스토리지 테이크오버 및 반환 프로세스를 지원하는 노드와 중재자 간의 통신 채널



여러 가용성 영역에 구축된 경우 여러 LIF가 에 연결됩니다 **"유동 IP 주소"** 이는 AWS 프라이빗 IP 제한에 계산되지 않습니다.

### 보안 그룹

BlueXP에서는 보안 그룹을 만들 필요가 없습니다. 직접 사용해야 하는 경우 을 참조하십시오 **"보안 그룹 규칙"**.



커넥터에 대한 정보를 찾고 계십니까? **"Connector에 대한 보안 그룹 규칙을 봅니다"**

### 데이터 계층화를 위한 연결

EBS를 성능 계층으로 사용하고 AWS S3를 용량 계층으로 사용하려면 Cloud Volumes ONTAP이 S3에 연결되어 있는지 확인해야 합니다. 이 연결을 제공하는 가장 좋은 방법은 S3 서비스에 VPC 엔드포인트를 생성하는 것입니다. 자세한 내용은 을 참조하십시오 **"AWS 설명서: 게이트웨이 엔드포인트 생성"**.

VPC 끝점을 만들 때 Cloud Volumes ONTAP 인스턴스에 해당하는 영역, VPC 및 라우팅 테이블을 선택해야 합니다. 또한 S3 엔드포인트에 대한 트래픽을 활성화하는 아웃바운드 HTTPS 규칙을 추가하려면 보안 그룹을 수정해야 합니다. 그렇지 않으면 Cloud Volumes ONTAP에서 S3 서비스에 연결할 수 없습니다.

문제가 발생하면 을 참조하십시오 ["AWS 지원 지식 센터: 게이트웨이 VPC 엔드포인트를 사용하여 S3 버킷에 연결할 수 없는 이유는 무엇입니까?"](#)

## ONTAP 시스템에 대한 연결

AWS의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 AWS VPC와 회사 네트워크 같은 다른 네트워크 간에 VPN 연결을 설정해야 합니다. 자세한 내용은 을 참조하십시오 ["AWS 설명서: AWS VPN 연결 설정"](#).

## CIFS용 DNS 및 Active Directory

CIFS 스토리지를 프로비저닝하려면 AWS에서 DNS 및 Active Directory를 설정하거나 사내 설정을 AWS로 확장해야 합니다.

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

자세한 지침은 을 참조하십시오 ["AWS 설명서: AWS 클라우드의 Active Directory 도메인 서비스: 빠른 시작 참조 배포"](#).

## VPC 공유

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

["공유 서브넷에 HA 쌍을 구축하는 방법을 알아보십시오"](#).

여러 대의 AZs에서 HA 쌍에 대한 요구 사항

추가 AWS 네트워킹 요구사항은 ZS(Multiple Availability Zones)를 사용하는 Cloud Volumes ONTAP HA 구성에 적용됩니다. 작업 환경을 생성할 때 BlueXP에 네트워킹 세부 정보를 입력해야 하므로 HA 쌍을 실행하기 전에 이러한 요구 사항을 검토해야 합니다.

HA 쌍의 작동 방식을 이해하려면 를 참조하십시오 ["고가용성 쌍"](#).

## 가용성 영역

이 HA 구축 모델은 여러 대의 AZs를 사용하여 데이터의 고가용성을 보장합니다. 각 Cloud Volumes ONTAP 인스턴스와 증재자 인스턴스에 전용 AZ를 사용해야 하며 HA 쌍 간의 통신 채널을 제공합니다.

각 가용성 영역에서 서브넷을 사용할 수 있어야 합니다.

## NAS 데이터 및 클러스터/SVM 관리를 위한 부동 IP 주소

여러 AZs의 HA 구성에서는 장애가 발생할 경우 노드 간에 이동하는 부동 IP 주소를 사용합니다. 고객이 아니라면 VPC 외부에서 기본적으로 액세스할 수 없습니다 ["AWS 전송 게이트웨이를 설정합니다"](#).

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



Windows용 SnapDrive 또는 HA 쌍을 지원하는 SnapCenter를 사용하는 경우 SVM 관리 LIF에는 부동 IP 주소가 필요합니다.

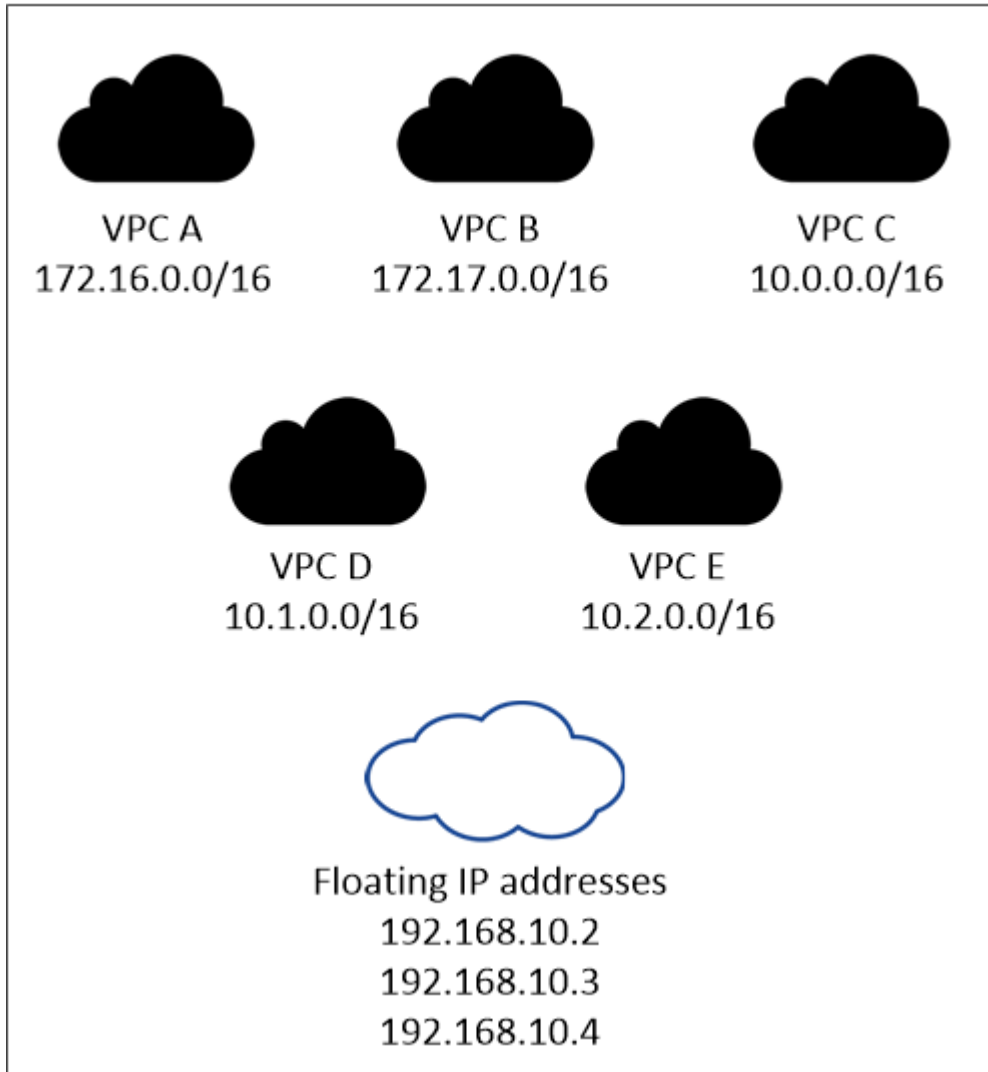
Cloud Volumes ONTAP HA 작업 환경을 생성할 때 BlueXP에서 부동 IP 주소를 입력해야 합니다. BlueXP는

시스템을 시작할 때 HA 쌍에 IP 주소를 할당합니다.

부동 IP 주소는 HA 구성을 배포하는 AWS 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 합니다. 유동 IP 주소를 해당 지역의 VPC 외부에 있는 논리적 서브넷으로 생각해 보십시오.

다음 예에서는 AWS 영역에 있는 VPC와 유동 IP 주소 간의 관계를 보여 줍니다. 부동 IP 주소는 모든 VPC에 대한 CIDR 블록 외부에 있지만 라우팅 테이블을 통해 서브넷으로 라우팅할 수 있습니다.

## AWS region



BlueXP는 VPC 외부의 클라이언트에서 iSCSI 액세스 및 NAS 액세스를 위해 정적 IP 주소를 자동으로 생성합니다. 이러한 유형의 IP 주소에 대한 요구 사항을 충족할 필요는 없습니다.

### VPC 외부에서 유동 IP 액세스를 지원하는 전송 게이트웨이

필요한 경우 ["AWS 전송 게이트웨이를 설정합니다"](#) HA 쌍이 상주하는 VPC 외부에서 HA 쌍의 부동 IP 주소에 액세스할 수 있도록 합니다.

### 배관 테이블

BlueXP에서 부동 IP 주소를 지정한 후 부동 IP 주소에 대한 경로를 포함해야 하는 라우팅 테이블을 선택하라는 메시지가 표시됩니다. 이렇게 하면 클라이언트가 HA 쌍에 액세스할 수 있습니다.

VPC(주 경로 테이블)에 있는 서브넷을 위한 경로 테이블이 하나만 있는 경우 BlueXP는 해당 라우팅 테이블에 부동 IP 주소를 자동으로 추가합니다. 둘 이상의 라우팅 테이블이 있는 경우 HA 쌍을 시작할 때 올바른 라우팅 테이블을 선택하는 것이 매우 중요합니다. 그렇지 않으면 일부 클라이언트가 Cloud Volumes ONTAP에 액세스하지 못할 수 있습니다.

예를 들어, 서로 다른 라우팅 테이블에 연결된 두 개의 서브넷이 있을 수 있습니다. 라우팅 테이블 A를 선택했지만 라우팅 테이블 B는 선택하지 않은 경우, 라우팅 테이블 A와 연결된 서브넷에 있는 클라이언트는 HA 쌍에 액세스할 수 있지만, 라우팅 테이블 B와 연결된 서브넷에 있는 클라이언트는 액세스할 수 없습니다.

라우팅 테이블에 대한 자세한 내용은 [을 참조하십시오 "AWS 설명서: 경로 테이블"](#).

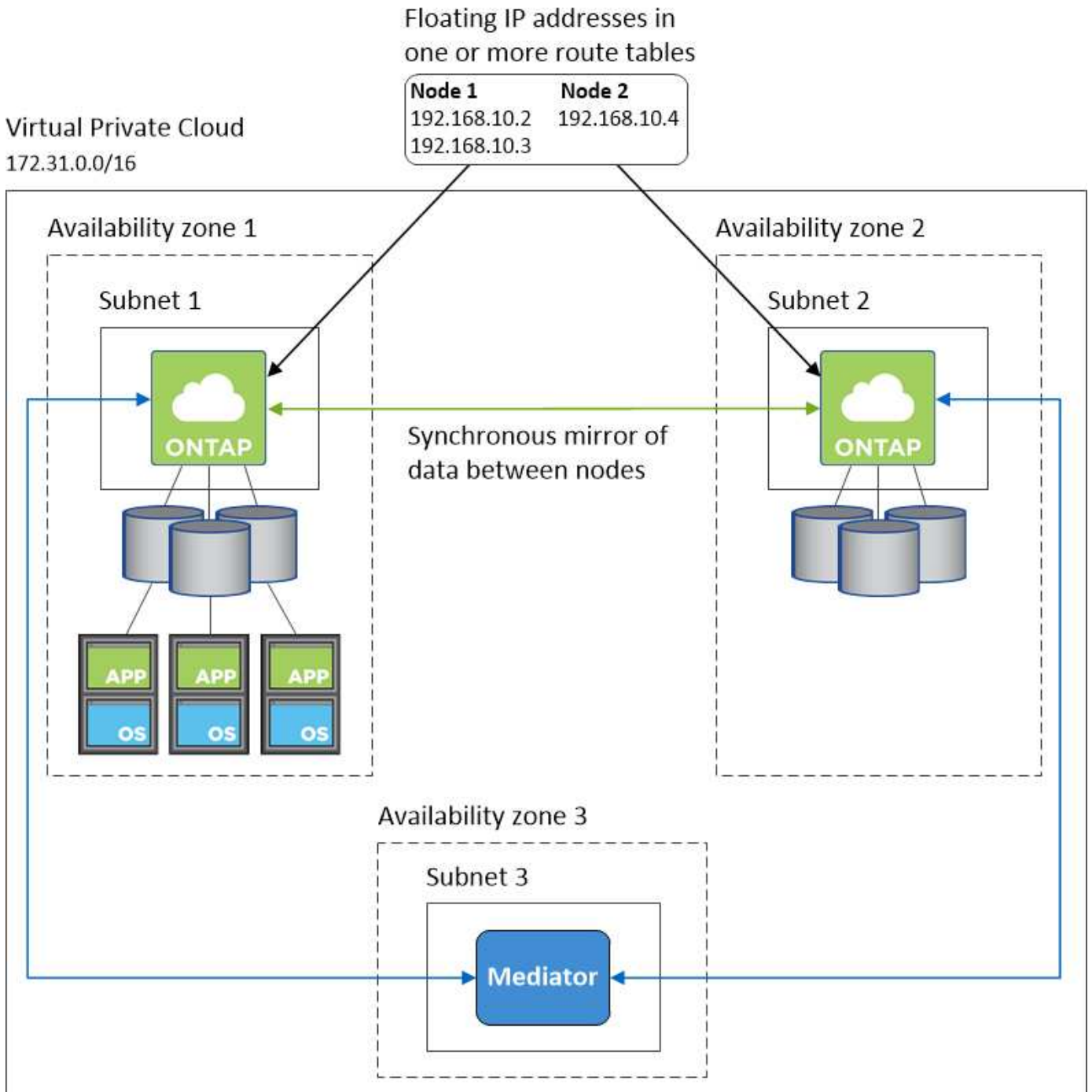
### NetApp 관리 툴에 연결

여러 AZs에 있는 HA 구성에서 NetApp 관리 툴을 사용하려면 다음 두 가지 연결 옵션을 사용할 수 있습니다.

1. NetApp 관리 툴을 다른 VPC 및 에 구축할 수 있습니다 ["AWS 전송 게이트웨이를 설정합니다"](#). 게이트웨이를 사용하면 VPC 외부에서 클러스터 관리 인터페이스의 부동 IP 주소에 액세스할 수 있습니다.
2. NAS 클라이언트와 비슷한 라우팅 구성을 사용하여 동일한 VPC에 NetApp 관리 툴을 구축합니다.

### HA 구성의 예

다음 그림에서는 여러 AZs의 HA 쌍, 즉 가용성 영역 3개, 서브넷 3개, 부동 IP 주소 및 라우팅 테이블과 같은 네트워크 구성 요소를 보여 줍니다.



커넥터 요구 사항

아직 Connector를 만들지 않은 경우 Connector에 대한 네트워킹 요구 사항도 검토해야 합니다.

- "커넥터에 대한 네트워킹 요구 사항을 봅니다"
- "AWS의 보안 그룹 규칙"

여러 AZs에서 HA 쌍에 대한 AWS 전송 게이트웨이 설정

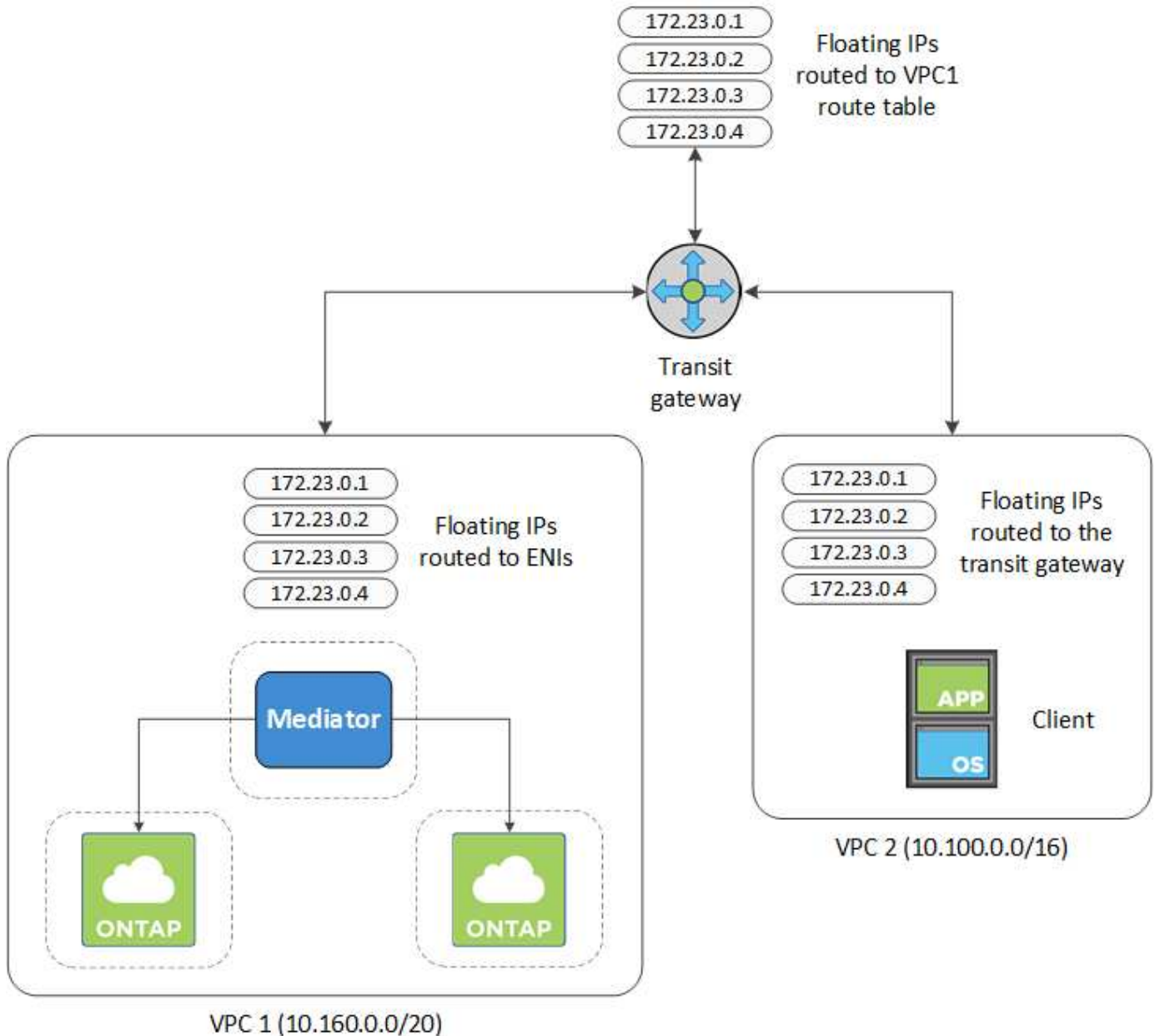
HA 쌍에 대한 액세스를 지원하는 AWS 전송 게이트웨이를 설정합니다 "유동 IP 주소" HA 쌍이 상주하는 VPC 외부에서

Cloud Volumes ONTAP HA 구성이 여러 AWS 가용성 영역에 분산되면 VPC 내에서 NAS 데이터 액세스에 유동 IP 주소가 필요합니다. 이러한 부동 IP 주소는 장애가 발생할 때 노드 간에 마이그레이션할 수 있지만 VPC 외부에서 기본적으로 액세스할 수 없습니다. 별도의 프라이빗 IP 주소를 통해 VPC 외부에서 데이터에 액세스할 수 있지만 자동 페일오버를 제공하지 않습니다.

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

AWS 전송 게이트웨이를 설정한 경우 HA 쌍이 상주하는 VPC 외부의 유동 IP 주소에 액세스할 수 있습니다. 즉, VPC 외부에 있는 NAS 클라이언트와 NetApp 관리 툴이 유동 IP에 액세스할 수 있습니다.

다음은 전송 게이트웨이에 의해 연결된 두 대의 VPC를 보여 주는 예입니다. HA 시스템은 VPC 하나에 상주하고 클라이언트는 다른 VPC에 상주합니다. 그런 다음 부동 IP 주소를 사용하여 클라이언트에 NAS 볼륨을 마운트할 수 있습니다.



다음 단계에서는 유사한 구성을 설정하는 방법을 보여 줍니다.



단계

1. "전송 게이트웨이를 만들고 VPC를 게이트웨이에 연결합니다".
2. VPC를 전송 게이트웨이 경로 테이블에 연결합니다.
  - a. VPC \* 서비스에서 \* Transit Gateway Route Tables \* 를 클릭합니다.
  - b. 라우팅 테이블을 선택합니다.
  - c. 연결 \* 을 클릭한 다음 \* 연결 생성 \* 을 선택합니다.
  - d. 연결할 첨부 파일(VPC)을 선택한 다음 \* 연결 생성 \* 을 클릭합니다.
3. HA 쌍의 부동 IP 주소를 지정하여 전송 게이트웨이의 라우팅 테이블에서 경로를 만듭니다.

BlueXP의 작업 환경 정보 페이지에서 부동 IP 주소를 찾을 수 있습니다. 예를 들면 다음과 같습니다.

## NFS & CIFS access from within the VPC using Floating IP

### Auto failover

Cluster Management : 172.23.0.1

Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

### Access

SVM Management : 172.23.0.4

다음 샘플 이미지는 전송 게이트웨이의 라우트 테이블을 보여 줍니다. 여기에는 2개의 VPC의 CIDR 블록에 대한 경로와 Cloud Volumes ONTAP에서 사용하는 4개의 부동 IP 주소가 포함됩니다.

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aedd3

Details Associations Propagations **Routes** Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route Replace route Delete route

Filter by attributes or search by keyword

<input type="checkbox"/>	CIDR	Attachment	Resource type	Route type	Route state
<input type="checkbox"/>	10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8   vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
<input type="checkbox"/>	10.160.0.0/20	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC1	propagated	active
<input type="checkbox"/>	172.23.0.1/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.2/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.3/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active
<input type="checkbox"/>	172.23.0.4/32	tgw-attach-00eba3eac3250d7db   vpc-673ae603	VPC	static	active

4. 부동 IP 주소에 액세스해야 하는 VPC의 라우팅 테이블을 수정합니다.
  - a. 부동 IP 주소에 라우트 항목을 추가합니다.

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

다음 샘플 이미지는 VPC 1에 대한 라우트 및 부동 IP 주소를 포함하는 VPC 2용 라우팅 테이블을 보여 줍니다.

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	igw-07250bd01781e67df	active	No
10.160.0.0/20	tgw-015b7c249661ac279	active	No
172.23.0.1/32	tgw-015b7c249661ac279	active	No
172.23.0.2/32	tgw-015b7c249661ac279	active	No
172.23.0.3/32	tgw-015b7c249661ac279	active	No
172.23.0.4/32	tgw-015b7c249661ac279	active	No

VPC1  
Floating IP Addresses

5. 유동 IP 주소에 액세스해야 하는 VPC에 경로를 추가하여 HA 쌍 VPC의 경로 테이블을 수정합니다.

이 단계는 VPC 간 라우팅을 완료하기 때문에 중요합니다.

다음 샘플 이미지는 VPC 1의 라우트 테이블을 보여 줍니다. 여기에는 부동 IP 주소 및 클라이언트가 있는 VPC 2로의 라우트가 포함됩니다. BlueXP는 HA 쌍을 배포할 때 라우팅 테이블에 유동 IP를 자동으로 추가했습니다.

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

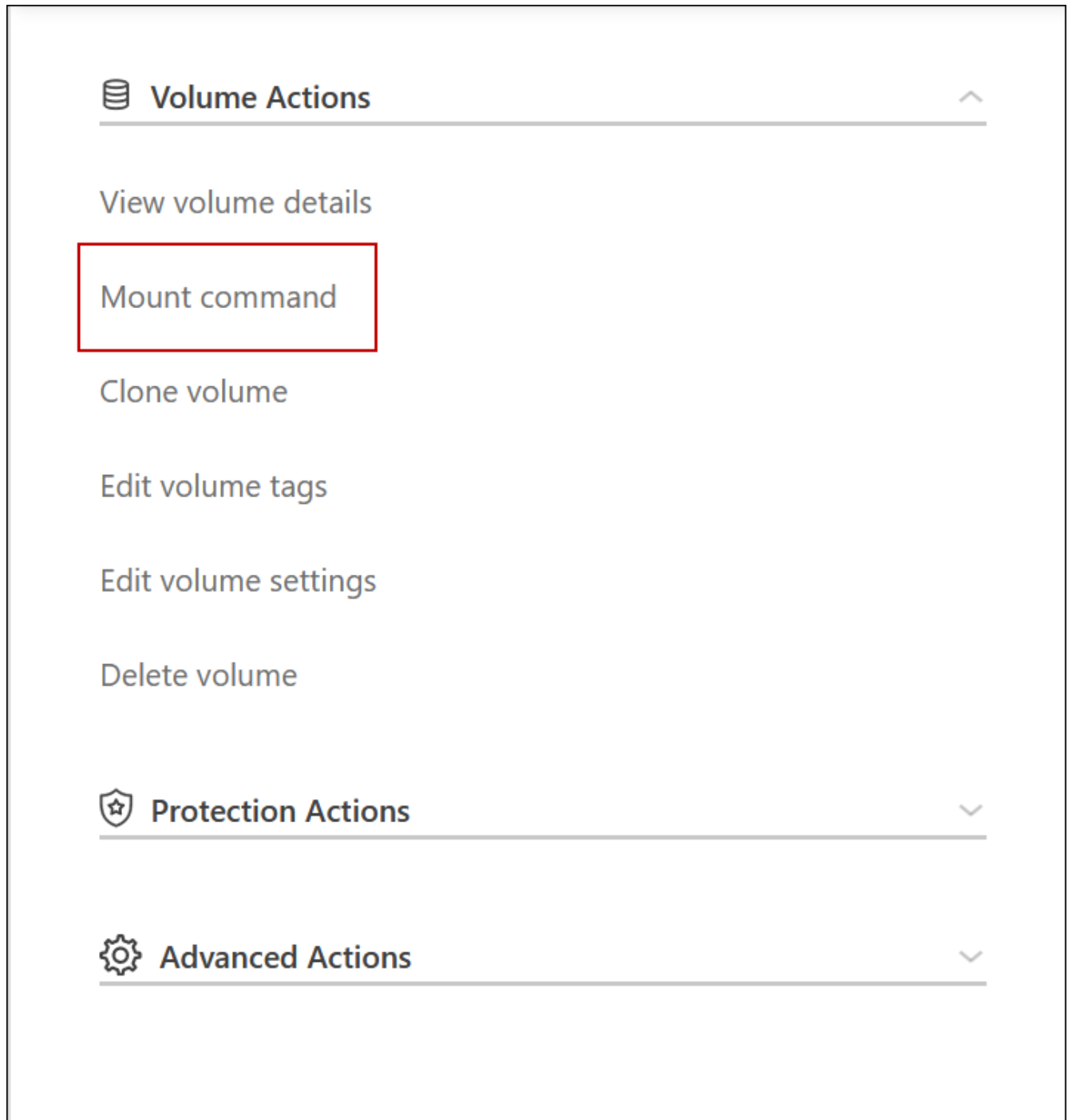
View All routes

Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	igw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-ff7e1396	active
172.23.0.1/32	eni-0854d4715559c3cdb	active
172.23.0.2/32	eni-0854d4715559c3cdb	active
172.23.0.3/32	eni-0f76681216c3108ed	active
172.23.0.4/32	eni-0854d4715559c3cdb	active

VPC2  
Floating IP Addresses

6. 부동 IP 주소를 사용하여 클라이언트에 볼륨을 마운트합니다.

BlueXP의 볼륨 관리 패널의 \* 탑재 명령 \* 옵션을 통해 BlueXP에서 올바른 IP 주소를 찾을 수 있습니다.



7. NFS 볼륨을 마운트하는 경우 클라이언트 VPC의 서브넷에 일치하도록 익스포트 정책을 구성합니다.

"볼륨을 편집하는 방법에 대해 알아봅니다".

- [관련 링크 \\*](#)
- ["AWS의 고가용성 쌍"](#)
- ["AWS의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항"](#)

공유 서브넷에 HA 쌍 구축

### 9.11.1 릴리즈부터 VPC 공유를 지원하는 AWS에서 Cloud Volumes ONTAP HA 쌍이

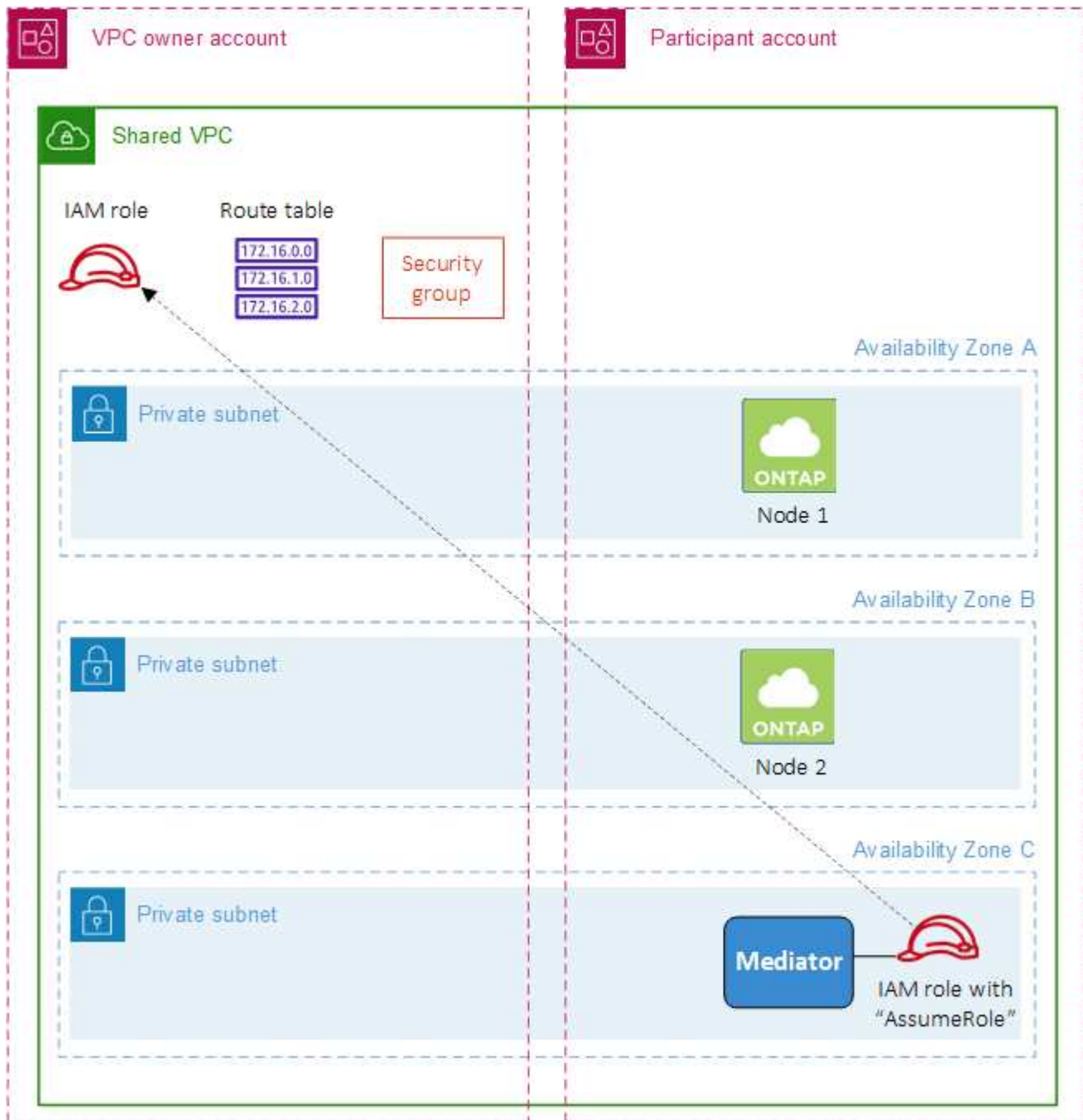
지원됩니다. VPC 공유를 사용하면 서브넷을 다른 AWS 계정과 공유할 수 있습니다. 이 구성을 사용하려면 AWS 환경을 설정한 다음 API를 사용하여 HA 쌍을 구축해야 합니다.

와 함께 "VPC 공유" Cloud Volumes ONTAP HA 구성은 다음 두 계정에 분산됩니다.

- 네트워킹을 소유하는 VPC 소유자 계정(VPC, 서브넷, 라우팅 테이블 및 Cloud Volumes ONTAP 보안 그룹)
- 참가자 계정으로, EC2 인스턴스가 공유 서브넷에 구축됩니다(여기에는 2개의 HA 노드와 중재자가 포함됨).

여러 가용성 영역에 배포된 Cloud Volumes ONTAP HA 구성의 경우 HA 중재자가 VPC 소유자 계정의 라우트 테이블에 쓸 수 있는 특정 권한이 필요합니다. 중재자가 추정할 수 있는 IAM 역할을 설정하여 이러한 권한을 제공해야 합니다.

다음 이미지는 이 구축과 관련된 구성 요소를 보여줍니다.



아래 단계에 설명된 대로 참가자 계정과 서브넷을 공유하고 VPC 소유자 계정에서 IAM 역할 및 보안 그룹을 만들어야 합니다.

Cloud Volumes ONTAP 작업 환경을 만들면 BlueXP는 자동으로 IAM 역할을 생성하여 중재자에 연결합니다. 이 역할은 HA 쌍과 연결된 경로 테이블을 변경하기 위해 VPC 소유자 계정에서 생성한 IAM 역할을 가정합니다.

#### 단계

1. VPC 소유자 계정의 서브넷을 참가자 계정과 공유합니다.

이 단계는 공유 서브넷에 HA 쌍을 구축하는 데 필요합니다.

["AWS 설명서: 서브넷을 공유합니다"](#)

2. VPC 소유자 계정에서 Cloud Volumes ONTAP용 보안 그룹을 생성합니다.

["Cloud Volumes ONTAP의 보안 그룹 규칙을 참조하십시오"](#). HA 중재자를 위한 보안 그룹을 만들 필요는 없습니다. BlueXP가 이러한 작업을 수행합니다.

3. VPC 소유자 계정에서 다음 권한이 포함된 IAM 역할을 생성합니다.

```
    "Action": [
      "ec2:AssignPrivateIpAddresses",
      "ec2:CreateRoute",
      "ec2>DeleteRoute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeVpcs",
      "ec2:ReplaceRoute",
      "ec2:UnassignPrivateIpAddresses"
```

4. BlueXP API를 사용하여 새로운 Cloud Volumes ONTAP 작업 환경을 만듭니다.

다음 필드를 지정해야 합니다.

- "보안 그룹 ID"

"securityGroupId" 필드는 VPC 소유자 계정에서 만든 보안 그룹을 지정해야 합니다(위의 2단계 참조).

- "haParams" 개체의 "assumeRoleArn"

"assumeRoleArn" 필드에는 VPC 소유자 계정에서 만든 IAM 역할의 ARN이 포함되어야 합니다(위의 3단계 참조).

예를 들면 다음과 같습니다.

```
"haParams": {
  "assumeRoleArn":
  "arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

+  
["Cloud Volumes ONTAP API에 대해 자세히 알아보십시오"](#)

## AWS의 보안 그룹 규칙

BlueXP는 Cloud Volumes ONTAP의 성공적인 운영에 필요한 인바운드 및 아웃바운드 규칙을 포함하는 AWS 보안 그룹을 생성합니다. 테스트 목적으로 또는 자체 보안 그룹을 사용하려는 경우 포트를 참조할 수 있습니다.

### Cloud Volumes ONTAP 규칙

Cloud Volumes ONTAP의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

### 인바운드 규칙

작업 환경을 만들고 미리 정의된 보안 그룹을 선택할 때 다음 중 한 가지 내에서 트래픽을 허용하도록 선택할 수 있습니다.

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

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 커넥터 및 HTTPS 액세스와의 연결
SSH를 클릭합니다	22	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다
TCP	111	NFS에 대한 원격 프로시저 호출
TCP	139	CIFS에 대한 NetBIOS 서비스 세션입니다
TCP	161-162	단순한 네트워크 관리 프로토콜
TCP	445	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
TCP	635	NFS 마운트
TCP	749	Kerberos
TCP	2049년	NFS 서버 데몬

프로토콜	포트	목적
TCP	3260입니다	iSCSI 데이터 LIF를 통한 iSCSI 액세스
TCP	4045로 문의하십시오	NFS 잠금 데몬
TCP	4046으로 문의하십시오	NFS에 대한 네트워크 상태 모니터
TCP	10000	NDMP를 사용한 백업
TCP	11104를 참조하십시오	SnapMirror에 대한 인터클러스터 통신 세션의 관리
TCP	11105를 참조하십시오	인터클러스터 LIF를 사용하여 SnapMirror 데이터 전송
UDP입니다	111	NFS에 대한 원격 프로시저 호출
UDP입니다	161-162	단순한 네트워크 관리 프로토콜
UDP입니다	635	NFS 마운트
UDP입니다	2049년	NFS 서버 데몬
UDP입니다	4045로 문의하십시오	NFS 잠금 데몬
UDP입니다	4046으로 문의하십시오	NFS에 대한 네트워크 상태 모니터
UDP입니다	4049입니다	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	88을 참조 하십시오	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니 다	137 입니 다	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	88을 참조 하십시오	데이터 LIF(NFS, CIFS, iSCSI)	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니 다	137 입니 다	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)
	TCP	3128	노드 관리 LIF	커넥터	아웃바운드 인터넷 연결을 사용할 수 없는 경우 커넥터의 프록시 서버를 통해 AutoSupport 메시지 보내기
S3로 백업	TCP	5010 입니다	인터클러스터 LIF	엔드포인트 백업 또는 복원	S3로 백업 기능의 백업 및 복원 작업
클러스터	모든 교통 정보	모든 교통 정보	모든 LIF가 하나의 노드에 있습니다	다른 노드의 모든 LIF	인터클러스터 통신(Cloud Volumes ONTAP HA에만 해당)
	TCP	3000 입니다	노드 관리 LIF	HA 중재자	ZAPI 호출(Cloud Volumes ONTAP HA 전용)
	ICMP	1	노드 관리 LIF	HA 중재자	활성 상태 유지(Cloud Volumes ONTAP HA만 해당)
구성 백업	HTTP	80	노드 관리 LIF	http://<connector-IP-address>/occm/offbo xconfig입니다	Connector로 구성 백업을 보냅니다. "구성 백업 파일에 대해 자세히 알아보십시오".
DHCP를 선택합니 다	UDP입니 다	68	노드 관리 LIF	DHCP를 선택합니다	처음으로 설정하는 DHCP 클라이언트
DHCPS	UDP입니 다	67	노드 관리 LIF	DHCP를 선택합니다	DHCP 서버
DNS	UDP입니 다	53	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
NDMP	TCP	1860 0-18 699	노드 관리 LIF	대상 서버	NDMP 복제
SMTP	TCP	25	노드 관리 LIF	메일 서버	AutoSupport에 사용할 수 있는 SMTP 경고
SNMP를 선택합니 다	TCP	161	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	UDP입니 다	161	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	TCP	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	UDP입니 다	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링

서비스	프로토콜	포트	출처	목적지	목적
SnapMirror를 참조하십시오	TCP	11104를 참조하십시오	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror에 대한 인터클러스터 통신 세션의 관리
	TCP	11105를 참조하십시오	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror 데이터 전송
Syslog를 클릭합니다	UDP입니다	514	노드 관리 LIF	Syslog 서버	Syslog 메시지를 전달합니다

외부 보안 그룹의 HA 중재자를 위한 규칙

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

인바운드 규칙

HA 중재자를 위해 미리 정의된 보안 그룹에는 다음과 같은 인바운드 규칙이 포함됩니다.

프로토콜	포트	출처	목적
TCP	3000입니다	커넥터의 CIDR	Connector에서 Restful API 액세스

아웃바운드 규칙

HA 중재자를 위한 사전 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

기본 아웃바운드 규칙

HA 중재자를 위해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

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

고급 아웃바운드 규칙

아웃바운드 트래픽에 대한 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 HA 중재자의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.

프로토콜	포트	목적지	목적
HTTP	80	AWS EC2 인스턴스에 있는 Connector의 IP 주소입니다	중재자를 위한 업그레이드 다운로드

프로토콜	포트	목적지	목적
HTTPS	443	ec2.amazonaws.com	스토리지 페일오버 지원
UDP입니다	53	ec2.amazonaws.com	스토리지 페일오버 지원



포트 443과 53을 열지 않고 타겟 서브넷에서 AWS EC2 서비스로 인터페이스 VPC 엔드포인트를 생성할 수 있습니다.

**HA 구성 내부 보안 그룹에 대한 규칙입니다**

Cloud Volumes ONTAP HA 구성에 대해 미리 정의된 내부 보안 그룹에는 다음 규칙이 포함됩니다. 이 보안 그룹은 HA 노드와 중재자 및 노드 간의 통신을 지원합니다.

BlueXP는 항상 이 보안 그룹을 만듭니다. 자신의 을(를) 사용할 수 있는 옵션이 없습니다.

**인바운드 규칙**

미리 정의된 보안 그룹에는 다음과 같은 인바운드 규칙이 포함됩니다.

프로토콜	포트	목적
모든 교통 정보	모두	HA 중재자 및 HA 노드 간 통신

**아웃바운드 규칙**

미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

프로토콜	포트	목적
모든 교통 정보	모두	HA 중재자 및 HA 노드 간 통신

**커넥터 규칙**

["Connector에 대한 보안 그룹 규칙을 봅니다"](#)

## AWS KMS 설정

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

단계

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

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

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

2. BlueXP에 대한 권한을 제공하는 IAM 역할을 `_KEY_USER`로 추가하여 각 CMK에 대한 키 정책을 수정합니다.

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

### "AWS 설명서:키 편집"

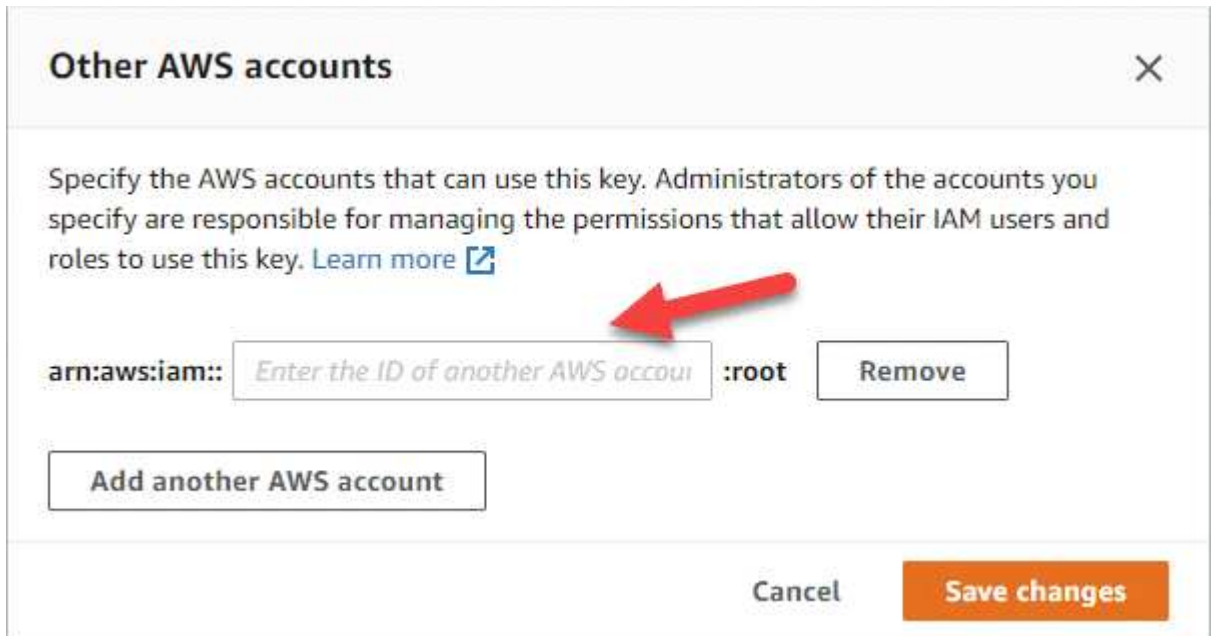
3. CMK가 다른 AWS 계정에 있는 경우 다음 단계를 수행하십시오.

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

Cloud Volumes ONTAP 시스템을 생성할 때 ARN을 BlueXP에 제공해야 합니다.

- d. 다른 AWS 계정 \* 창에서 BlueXP에 사용 권한을 제공하는 AWS 계정을 추가합니다.

대부분의 경우 이 계정은 BlueXP가 있는 계정입니다. BlueXP가 AWS에 설치되어 있지 않은 경우 BlueXP에 AWS 액세스 키를 제공한 계정이 됩니다.



- e. 이제 BlueXP에 사용 권한을 제공하고 IAM 콘솔을 여는 AWS 계정으로 전환합니다.
- f. 아래에 나열된 권한을 포함하는 IAM 정책을 생성합니다.
- g. BlueXP에 대한 권한을 제공하는 IAM 역할 또는 IAM 사용자에게 정책을 첨부합니다.

다음 정책은 BlueXP가 외부 AWS 계정에서 CMK를 사용하는 데 필요한 권한을 제공합니다. "리소스" 섹션에서

지역 및 계정 ID를 수정해야 합니다.

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

+

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

4. 고객이 관리하는 CMK를 사용하는 경우 Cloud Volumes ONTAP IAM 역할을 `_KEY_USER_`로 추가하여 CMK에

대한 주요 정책을 수정합니다.

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

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

["AWS 설명서:키 편집"](#)

## Cloud Volumes ONTAP에 대한 IAM 역할을 설정합니다

필요한 권한이 있는 IAM 역할은 각 Cloud Volumes ONTAP 노드에 연결되어야 합니다. HA 중재자의 경우도 마찬가지입니다. BlueXP에서 IAM 역할을 생성하는 것이 가장 쉽지만 자신의 역할을 사용할 수 있습니다.

이 작업은 선택 사항입니다. Cloud Volumes ONTAP 작업 환경을 생성할 때 기본 옵션은 BlueXP에서 IAM 역할을 생성할 수 있도록 하는 것입니다. 보안 정책에 따라 IAM 역할을 직접 생성해야 하는 경우 다음 단계를 따르십시오.



AWS 상용 클라우드 서비스 환경에서는 IAM의 역할을 직접 제공해야 합니다. ["C2S에 Cloud Volumes ONTAP를 배포하는 방법을 알아보십시오"](#).

단계

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

## 표준 영역

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

## GovCloud(미국) 지역



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

**C2S** 환경

```

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

```

◦ Cloud Volumes ONTAP 노드의 백업 정책

Cloud Volumes ONTAP 시스템에서 BlueXP 백업 및 복구를 사용하려는 경우 노드에 대한 IAM 역할에 아래에 나와 있는 두 번째 정책이 포함되어야 합니다.

## 표준 영역

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

## GovCloud(미국) 지역

```

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

```

**C2S** 환경

```

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

```

◦ HA 중재자

```

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

```

3. IAM 역할을 생성하고 생성한 정책을 역할에 연결합니다.

결과

이제 새로운 Cloud Volumes ONTAP 작업 환경을 생성할 때 선택할 수 있는 IAM 역할이 있습니다.

추가 정보

- ["AWS 설명서: IAM 정책 생성"](#)
- ["AWS 설명서: IAM 역할 생성"](#)

## AWS에서 Cloud Volumes ONTAP에 대한 라이선스 설정

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. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 BlueXP의 단계를 따릅니다.
  - a. Details and Credentials \* 페이지에서 \* 자격 증명 편집 > 구독 추가 \* 를 클릭한 다음 표시되는 메시지에 따라

AWS Marketplace에서 선불 종량제 오퍼링을 구독합니다.

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

### Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

**Pay-Per-TiB - Annual Contract**  
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

**Pay-as-you-go**  
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 AWS Marketplace**  
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**  
Save your subscription and associate the Marketplace subscription with your AWS credentials.

a. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 \* Freemium \* 을 선택합니다.

### Select Charging Method

**Professional** By capacity

**Essential** By capacity

**Freemium (Up to 500 GiB)** By capacity

**Per Node** By node

"AWS에서 Cloud Volumes ONTAP를 시작하는 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)
- AWS Marketplace에서 PAYGO(Pay-as-you-go) 방식으로 구독을 지원합니다
- AWS Marketplace에서 연간 계약 체결

"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. "NetApp Support 사이트 계정을 BlueXP에 추가합니다"

BlueXP는 NetApp의 라이선스 서비스에 자동으로 쿼리하여 NetApp Support 사이트 계정과 관련된 라이선스에 대한 자세한 정보를 확인합니다. 오류가 없으면 BlueXP는 자동으로 디지털 지갑에 라이선스를 추가합니다.

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

3. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 BlueXP의 단계를 따릅니다.
  - a. Details and Credentials \* 페이지에서 \* 자격 증명 편집 > 구독 추가 \* 를 클릭한 다음 표시되는 메시지에 따라 AWS Marketplace에서 선불 종량제 오퍼링을 구독합니다.

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



## Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

Pay-Per-TiB - Annual Contract

Pay for Cloud Volumes ONTAP with an annual, upfront payment.

Pay-as-you-go

Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

1 AWS Marketplace

Subscribe and then click **Set Up Your Account** to configure your account.

2 Cloud Manager

Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue

Cancel

a. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 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	∨

"AWS에서 Cloud Volumes ONTAP를 시작하는 단계별 지침을 확인하십시오".

**PAYGO** 구독

클라우드 공급자 마켓플레이스의 서비스에 가입하여 시간별 비용 지불

Cloud Volumes ONTAP 작업 환경을 생성할 때 BlueXP는 AWS 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. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 BlueXP의 단계를 따릅니다.
  - a. Details and Credentials \* 페이지에서 \* 자격 증명 편집 > 구독 추가 \* 를 클릭한 다음 표시되는 메시지에 따라 AWS Marketplace에서 선불 종량제 오퍼링을 구독합니다.

**Edit Credentials & Add Subscription**

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

**Pay-Per-TiB - Annual Contract**  
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

**Pay-as-you-go**  
Pay for Cloud Volumes ONTAP at an hourly rate.

**The next steps:**

- 1 **AWS Marketplace**  
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 **Cloud Manager**  
Save your subscription and associate the Marketplace subscription with your AWS credentials.

**Continue** **Cancel**

- b. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 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: 1em;">▾</span>
<input type="radio"/> Essential	<span style="background-color: #007bff; color: white; padding: 2px 5px;">By capacity</span> <span style="font-size: 1em;">▾</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: 1em;">▾</span>
<input type="radio"/> Per Node	<span style="background-color: #6f42c1; color: white; padding: 2px 5px;">By node</span> <span style="font-size: 1em;">▾</span>

"AWS에서 Cloud Volumes ONTAP를 시작하는 단계별 지침을 확인하십시오".



설정 > 자격 증명 페이지에서 AWS 계정과 연결된 AWS Marketplace 구독을 관리할 수 있습니다.  
["AWS 계정 및 구독을 관리하는 방법에 대해 알아보십시오"](#)

#### 연간 계약

클라우드 공급자 마켓플레이스에서 연간 계약을 구매하여 연간 지불

시간별 구독과 마찬가지로, BlueXP는 AWS 마켓플레이스에서 사용 가능한 연간 계약을 구독하라는 메시지를 표시합니다.

#### 단계

1. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 BlueXP의 단계를 따릅니다.
  - a. Details and Credentials \* 페이지에서 \* 자격 증명 편집 > 구독 추가 \* 를 클릭한 다음 표시되는 메시지에 따라 AWS Marketplace에서 연간 계약을 구독합니다.

## Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

**Pay-Per-TiB - Annual Contract**  
 Pay for Cloud Volumes ONTAP with an annual, upfront payment.

**Pay-as-you-go**  
 Pay for Cloud Volumes ONTAP at an hourly rate.

---

**The next steps:**

- 1 **AWS Marketplace**  
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 **Cloud Manager**  
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue
Cancel

b. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 용량 기반 패키지를 선택합니다.

### Select Charging Method

<input checked="" type="radio"/>	Professional	<span style="background-color: #0070c0; color: white; padding: 2px 5px;">By capacity</span> ▼
<input type="radio"/>	Essential	<span style="background-color: #0070c0; color: white; padding: 2px 5px;">By capacity</span> ▼
<input type="radio"/>	Freemium (Up to 500 GiB)	<span style="background-color: #0070c0; color: white; padding: 2px 5px;">By capacity</span> ▼
<input type="radio"/>	Per Node	<span style="background-color: #800080; color: white; padding: 2px 5px;">By node</span> ▼

"AWS에서 Cloud Volumes ONTAP를 시작하는 단계별 지침을 확인하십시오".

### Keystone 구독

Keystone 가입은 종량제 구독 기반 서비스입니다. "NetApp Keystone 구독에 대해 자세히 알아보십시오".

단계

1. 아직 구독이 없는 경우 "[NetApp에 문의하십시오](#)"
2. <mailto:ng-keystone-success@netapp.com> [NetApp에 문의]하여 하나 이상의 Keystone 구독으로 BlueXP 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 BlueXP의 단계를 따릅니다.
  - a. 충전 방법을 선택하라는 메시지가 표시되면 Keystone 가입 충전 방법을 선택합니다.

Select Charging Method

Keystone By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1

Professional By capacity v

Essential By capacity v

Freemium (Up to 500 GiB) By capacity v

Per Node By node v

"AWS에서 [Cloud Volumes ONTAP](#)를 시작하는 단계별 지침을 확인하십시오

## AWS에서 **Cloud Volumes ONTAP** 실행

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

시작하기 전에

작업 환경을 만들려면 다음이 필요합니다.

- 실행 중인 커넥터입니다.
  - 가 있어야 합니다 "[작업 영역과 연결된 커넥터입니다](#)".

◦ "항상 Connector를 실행 상태로 둘 준비가 되어 있어야 합니다".

- 사용하려는 구성에 대한 이해.

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

- Cloud Volumes ONTAP에 대한 라이선스 설정에 필요한 사항을 이해합니다.

["라이선스 설정 방법에 대해 알아보십시오"](#).

- CIFS 구성을 위한 DNS 및 Active Directory

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

### AWS에서 단일 노드 Cloud Volumes ONTAP 시스템 시작

AWS에서 Cloud Volumes ONTAP를 실행하려면 BlueXP에서 새로운 작업 환경을 만들어야 합니다

이 작업에 대해

작업 환경을 생성한 직후 BlueXP는 지정된 VPC에서 테스트 인스턴스를 시작하여 연결을 확인합니다. 성공하면 즉시 BlueXP가 인스턴스를 종료한 다음 Cloud Volumes ONTAP 시스템 배포를 시작합니다. BlueXP에서 연결을 확인할 수 없는 경우 작업 환경 생성이 실패합니다. 테스트 인스턴스는 T2.nano(기본 VPC 테넌시의 경우) 또는 m3.medium(전용 VPC 테넌시의 경우)입니다.

단계

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

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

필드에 입력합니다	설명
작업 환경 이름	BlueXP는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Amazon EC2 인스턴스 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.
태그 추가	AWS 태그는 AWS 리소스에 대한 메타데이터입니다. BlueXP는 Cloud Volumes ONTAP 인스턴스 및 인스턴스와 연관된 각 AWS 리소스에 태그를 추가합니다.  작업 환경을 만들 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 생성된 후에는 더 많은 태그를 추가할 수 있습니다. API는 작업 환경을 생성할 때 태그를 4개로 제한하지 않습니다.  태그에 대한 자세한 내용은 <a href="#">을 참조하십시오 "AWS 문서: Amazon EC2 리소스에 태그 달기"</a> .

필드에 입력합니다	설명
사용자 이름 및 암호	Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하여 System Manager 또는 CLI를 통해 Cloud Volumes ONTAP에 연결할 수 있습니다. default_admin_user 이름을 유지하거나 사용자 지정 사용자 이름으로 변경합니다.
자격 증명 편집	이 시스템을 구축할 계정과 연결된 AWS 자격 증명을 선택합니다. AWS Marketplace 구독을 연결하여 이 Cloud Volumes ONTAP 시스템에 사용할 수도 있습니다.  선택한 자격 증명을 새 AWS Marketplace 구독에 연결하려면 * Add Subscription * 을 클릭합니다. 이 구독은 연간 계약을 기준으로 하거나 시간당 요금로 Cloud Volumes ONTAP에 대한 비용을 지불할 수 있습니다.  "BlueXP에 AWS 자격 증명을 추가하는 방법에 대해 알아보십시오".

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

▶ [https://docs.netapp.com/ko-kr/test//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/ko-kr/test//media/video_subscribing_aws.mp4) (video)

여러 IAM 사용자가 동일한 AWS 계정으로 작업하는 경우 각 사용자는 가입해야 합니다. 첫 번째 사용자가 구독한 후 AWS Marketplace는 아래 이미지에 표시된 것처럼 후속 사용자에게 이미 구독했음을 알립니다. AWS\_ACCOUNT\_에 가입되어 있는 동안 각 IAM 사용자는 자신을 해당 구독과 연결해야 합니다. 아래 메시지가 표시되면 \* 여기를 클릭 \* 링크를 클릭하여 BlueXP 웹 사이트로 이동하여 프로세스를 완료합니다.



**Cloud Manager (for Cloud Volumes ONTAP)**

---

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

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

Subscribe

You are already subscribed to this product

---

**Pricing Details**

Software Fees

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

- "BlueXP 분류에 대해 자세히 알아보십시오"
- "BlueXP 백업 및 복구에 대해 자세히 알아보십시오"



WORM 및 데이터 계층화를 사용하려면 BlueXP 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 작업 환경을 구축해야 합니다.

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

다음 표에서는 지침이 필요한 필드를 설명합니다.

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

필드에 입력합니다	설명
보안 그룹을 생성했습니다	<p>BlueXP에서 보안 그룹을 생성하도록 하면 트래픽을 허용하는 방법을 선택해야 합니다.</p> <ul style="list-style-type: none"> <li>• 선택한 VPC 전용 * 을 선택한 경우 인바운드 트래픽의 소스는 선택한 VPC의 서브넷 범위와 커넥터가 상주하는 VPC의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다.</li> <li>• 모든 VPC * 를 선택한 경우 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.</li> </ul>
기존 보안 그룹을 사용합니다	<p>기존 방화벽 정책을 사용하는 경우 필수 규칙이 포함되어 있는지 확인합니다. "<a href="#">Cloud Volumes ONTAP의 방화벽 규칙에 대해 알아보십시오</a>".</p>

8. \* 데이터 암호화 \*: 데이터 암호화 또는 AWS로 관리되는 암호화를 선택하지 않습니다.

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



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

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

["지원되는 암호화 기술에 대해 자세히 알아보십시오"](#).

9. \* 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"](#).

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

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

11. \* 사전 구성된 패키지 \*: 패키지 중 하나를 선택하여 Cloud Volumes ONTAP를 빠르게 시작하거나 \* 구성 변경 \* 을 클릭하여 원하는 구성을 선택합니다.

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

12. \* IAM Role \*: BlueXP가 역할을 생성할 수 있도록 기본 옵션을 유지하는 것이 가장 좋습니다.

자체 정책을 사용하려면 이 정책이 충족해야 합니다 ["Cloud Volumes ONTAP 노드의 정책 요구사항"](#).

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



선택한 버전에 대해 최신 출시 후보, 일반 가용성 또는 패치 릴리스를 사용할 수 있는 경우 BlueXP는 작업 환경을 만들 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).



14. \* 기본 스토리지 리소스 \*: 디스크 유형을 선택하고 기본 스토리지를 구성한 다음 데이터 계층화를 사용할 것인지 선택합니다.

다음 사항에 유의하십시오.

- 디스크 유형은 초기 볼륨(및 애그리게이트)에 사용됩니다. 이후 볼륨 및 애그리게이트에 대해 다른 디스크 유형을 선택할 수 있습니다.
- GP3 또는 io1 디스크를 선택하는 경우 BlueXP는 AWS의 Elastic Volumes 기능을 사용하여 기본 스토리지 디스크 용량을 필요에 따라 자동으로 늘립니다. 스토리지 요구사항에 따라 초기 용량을 선택하고 Cloud Volumes ONTAP를 구축한 후 수정할 수 있습니다. ["AWS의 Elastic Volumes 지원에 대해 자세히 알아보십시오"](#).
- GP2 또는 st1 디스크를 선택하는 경우 초기 애그리게이트의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 BlueXP가 생성하는 추가 애그리게이트에서 디스크 크기를 선택할 수 있습니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.
- 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
- 데이터 계층화를 사용하지 않는 경우, 후속 애그리게이트에서 이 기능을 사용하도록 설정할 수 있습니다.

["데이터 계층화의 작동 방식에 대해 알아보십시오"](#).

15. \* 쓰기 속도 및 WORM \*:

a. 필요한 경우 \* Normal \* (정상 \*) 또는 \* High \* (높음 \*) 쓰기 속도를 선택합니다.

["쓰기 속도에 대해 자세히 알아보십시오"](#).

b. 필요한 경우 WORM(Write Once, Read Many) 스토리지를 활성화합니다.

Cloud Volumes ONTAP 9.7 이하 버전에서 데이터 계층화가 활성화된 경우 WORM을 사용할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로의 되돌리기 또는 다운그레이드가 차단됩니다.

["WORM 스토리지에 대해 자세히 알아보십시오"](#).

a. WORM 스토리지를 활성화한 경우 보존 기간을 선택합니다.

16. \* 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 BlueXP는 서버넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.

필드에 입력합니다	설명
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)	<p>iSCSI 스토리지 타겟을 LUN(논리 유닛)이라고 하며 호스트에 표준 블록 디바이스로 표시됩니다.</p> <p>이니시에이터 그룹은 iSCSI 호스트 노드 이름의 테이블이며 어떤 이니시에이터가 어떤 LUN을 액세스할 수 있는지 제어합니다.</p> <p>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.</p> <p>iSCSI 볼륨을 생성할 때 BlueXP에서 자동으로 LUN을 생성합니다. 볼륨 당 하나의 LUN만 생성하므로 관리가 필요 없습니다. 볼륨을 생성한 후 <b>"IQN을 사용하여 호스트에서 LUN에 연결합니다"</b>.</p>

다음 이미지는 CIFS 프로토콜에 대해 작성된 볼륨 페이지를 보여 줍니다.

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy:

Default Policy

#### Protocol

NFS   
 CIFS   
 iSCSI

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

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

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

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

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

19. \* 검토 및 승인 \*: 선택 사항을 검토 및 확인합니다.
- 구성에 대한 세부 정보를 검토합니다.
  - BlueXP가 구매할 지원 및 AWS 리소스에 대한 세부 정보를 검토하려면 \* 추가 정보 \* 를 클릭합니다.
  - 이해함... \* 확인란을 선택합니다.
  - Go \* 를 클릭합니다.

#### 결과

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

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

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

#### 작업을 마친 후

- CIFS 공유를 프로비저닝한 경우 파일 및 폴더에 대한 사용자 또는 그룹 권한을 제공하고 해당 사용자가 공유를 액세스하고 파일을 생성할 수 있는지 확인합니다.

- 볼륨에 할당량을 적용하려면 System Manager 또는 CLI를 사용하십시오.

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

## AWS에서 Cloud Volumes ONTAP HA 쌍 시작

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

### 제한

현재 HA 쌍은 AWS 아웃포스트에서 지원되지 않습니다.

### 이 작업에 대해

작업 환경을 생성한 직후 BlueXP는 지정된 VPC에서 테스트 인스턴스를 시작하여 연결을 확인합니다. 성공하면 즉시 BlueXP가 인스턴스를 종료한 다음 Cloud Volumes ONTAP 시스템 배포를 시작합니다. BlueXP에서 연결을 확인할 수 없는 경우 작업 환경 생성이 실패합니다. 테스트 인스턴스는 T2.nano(기본 VPC 테넌시의 경우) 또는 m3.medium(전용 VPC 테넌시의 경우)입니다.

### 단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 화면의 지시를 따릅니다.
3. \* 위치 선택 \*: \* 아마존 웹 서비스 \* 및 \* Cloud Volumes ONTAP HA \* 를 선택합니다.
4. \* 세부 정보 및 자격 증명 \*: AWS 자격 증명과 구독을 선택적으로 변경하고, 작업 환경 이름을 입력하고, 필요한 경우 태그를 추가한 다음 암호를 입력합니다.

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

필드에 입력합니다	설명
작업 환경 이름	BlueXP는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Amazon EC2 인스턴스 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.
태그 추가	AWS 태그는 AWS 리소스에 대한 메타데이터입니다. BlueXP는 Cloud Volumes ONTAP 인스턴스 및 인스턴스와 연관된 각 AWS 리소스에 태그를 추가합니다.  작업 환경을 만들 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 생성된 후에는 더 많은 태그를 추가할 수 있습니다. API는 작업 환경을 생성할 때 태그를 4개로 제한하지 않습니다.  태그에 대한 자세한 내용은 을 참조하십시오 " <a href="#">AWS 문서: Amazon EC2 리소스에 태그 달기</a> ".
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
자격 증명 편집	<p>이 Cloud Volumes ONTAP 시스템에서 사용할 AWS 자격 증명과 마켓플레이스 구독을 선택하십시오.</p> <p>선택한 자격 증명을 새 AWS Marketplace 구독에 연결하려면 * Add Subscription * 을 클릭합니다. 이 구독은 연간 계약을 기준으로 하거나 시간당 요금으로 Cloud Volumes ONTAP에 대한 비용을 지불할 수 있습니다.</p> <p>NetApp(BYOL)에서 직접 라이선스를 구입한 경우에는 AWS 가입이 필요하지 않습니다.</p> <p><a href="#">"BlueXP에 AWS 자격 증명을 추가하는 방법에 대해 알아보십시오"</a>.</p>

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

▶ [https://docs.netapp.com/ko-kr/test//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/ko-kr/test//media/video_subscribing_aws.mp4) (video)

여러 IAM 사용자가 동일한 AWS 계정으로 작업하는 경우 각 사용자는 가입해야 합니다. 첫 번째 사용자가 구독한 후 AWS Marketplace는 아래 이미지에 표시된 것처럼 후속 사용자에게 이미 구독했음을 알립니다. AWS\_ACCOUNT\_에 가입되어 있는 동안 각 IAM 사용자는 자신을 해당 구독과 연결해야 합니다. 아래 메시지가 표시되면 \* 여기를 클릭 \* 링크를 클릭하여 BlueXP 웹 사이트로 이동하여 프로세스를 완료합니다.



### Cloud Manager (for Cloud Volumes ONTAP)

---

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

?

**Having issues signing up for your product?**

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

Subscribe

You are already subscribed to this product

---

**Pricing Details**

Software Fees

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

- ["BlueXP 분류에 대해 자세히 알아보십시오"](#)
- ["BlueXP 백업 및 복구에 대해 자세히 알아보십시오"](#)



WORM 및 데이터 계층화를 사용하려면 BlueXP 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 작업 환경을 구축해야 합니다.

6. \* HA 배포 모델 \*: HA 구성을 선택합니다.

배포 모델에 대한 개요는 ["AWS용 Cloud Volumes ONTAP HA"](#) 을 참조하십시오.

7. \* 위치 및 연결 \* (단일 AZ) 또는 \* 지역 및 VPC \* (다중 AZs): AWS 워크시트에 기록한 네트워크 정보를 입력합니다.

다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
보안 그룹을 생성했습니다	<p>BlueXP에서 보안 그룹을 생성하도록 하면 트래픽을 허용하는 방법을 선택해야 합니다.</p> <ul style="list-style-type: none"> <li>• 선택한 VPC 전용 * 을 선택한 경우 인바운드 트래픽의 소스는 선택한 VPC의 서브넷 범위와 커넥터가 상주하는 VPC의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다.</li> <li>• 모든 VPC * 를 선택한 경우 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.</li> </ul>
기존 보안 그룹을 사용합니다	기존 방화벽 정책을 사용하는 경우 필수 규칙이 포함되어 있는지 확인합니다. " <a href="#">Cloud Volumes ONTAP의 방화벽 규칙에 대해 알아보십시오</a> ".

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

9. \* 부동 IP \*: 여러 AZs를 선택한 경우 부동 IP 주소를 지정합니다.

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

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

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

11. \* 데이터 암호화 \*: 데이터 암호화 또는 AWS로 관리되는 암호화를 선택하지 않습니다.

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



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

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

"[지원되는 암호화 기술에 대해 자세히 알아보십시오](#)".

12. \* 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](#)".

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

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

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

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

15. \* IAM Role \*: BlueXP가 역할을 생성할 수 있도록 기본 옵션을 유지하는 것이 가장 좋습니다.

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

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



선택한 버전에 대해 최신 출시 후보, 일반 가용성 또는 패치 릴리스를 사용할 수 있는 경우 BlueXP는 작업 환경을 만들 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).

17. \* 기본 스토리지 리소스 \*: 디스크 유형을 선택하고 기본 스토리지를 구성한 다음 데이터 계층화를 사용할 것인지 선택합니다.

다음 사항에 유의하십시오.

- 디스크 유형은 초기 볼륨(및 애그리게이트)에 사용됩니다. 이후 볼륨 및 애그리게이트에 대해 다른 디스크 유형을 선택할 수 있습니다.
- GP3 또는 io1 디스크를 선택하는 경우 BlueXP는 AWS의 Elastic Volumes 기능을 사용하여 기본 스토리지 디스크 용량을 필요에 따라 자동으로 늘립니다. 스토리지 요구사항에 따라 초기 용량을 선택하고 Cloud Volumes ONTAP를 구축한 후 수정할 수 있습니다. "[AWS의 Elastic Volumes 지원에 대해 자세히 알아보십시오](#)".
- GP2 또는 st1 디스크를 선택하는 경우 초기 애그리게이트의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 BlueXP가 생성하는 추가 애그리게이트에서 디스크 크기를 선택할 수 있습니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.
- 볼륨을 생성하거나 편집할 때 특정 볼륨 계층화 정책을 선택할 수 있습니다.
- 데이터 계층화를 사용하지 않는 경우, 후속 애그리게이트에서 이 기능을 사용하도록 설정할 수 있습니다.

"[데이터 계층화의 작동 방식에 대해 알아보십시오](#)".

18. \* 쓰기 속도 및 WORM \*:

- a. 필요한 경우 \* Normal \* (정상 \*) 또는 \* High \* (높음 \*) 쓰기 속도를 선택합니다.

"[쓰기 속도에 대해 자세히 알아보십시오](#)".

- b. 필요한 경우 WORM(Write Once, Read Many) 스토리지를 활성화합니다.

Cloud Volumes ONTAP 9.7 이하 버전에서 데이터 계층화가 활성화된 경우 WORM을 사용할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로의 되돌리기 또는 다운그레이드가 차단됩니다.

"[WORM 스토리지에 대해 자세히 알아보십시오](#)".

- a. WORM 스토리지를 활성화한 경우 보존 기간을 선택합니다.

19. \* 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 BlueXP는 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)	<p>iSCSI 스토리지 타겟을 LUN(논리 유닛)이라고 하며 호스트에 표준 블록 디바이스로 표시됩니다.</p> <p>이니시에이터 그룹은 iSCSI 호스트 노드 이름의 테이블이며 어떤 이니시에이터가 어떤 LUN을 액세스할 수 있는지 제어합니다.</p> <p>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.</p> <p>iSCSI 볼륨을 생성할 때 BlueXP에서 자동으로 LUN을 생성합니다. 볼륨 당 하나의 LUN만 생성하므로 관리가 필요 없습니다. 볼륨을 생성한 후 <a href="#">"IQN을 사용하여 호스트에서 LUN에 연결합니다"</a>.</p>

다음 이미지는 CIFS 프로토콜에 대해 작성된 볼륨 페이지를 보여 줍니다.



**Volume Details, Protection & Protocol**

Details & Protection	Protocol
Volume Name: <input style="width: 200px;" type="text" value="vol"/> Size (GB): <input style="width: 80px;" type="text" value="250"/>	NFS <b>CIFS</b> iSCSI
Snapshot Policy: <input style="width: 150px;" type="text" value="default"/>	Share name: <input style="width: 150px;" type="text" value="vol_share"/> Permissions: <input style="width: 150px;" type="text" value="Full Control"/>
<input type="checkbox"/> Default Policy	Users / Groups: <input style="width: 200px;" type="text" value="engineering"/> <p style="font-size: small;">Valid users and groups separated by a semicolon</p>

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

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

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

자세한 내용은 을 참조하십시오 **"볼륨 사용 프로필을 선택합니다"** 및 **"데이터 계층화 개요"**.

22. \* 검토 및 승인 \*: 선택 사항을 검토 및 확인합니다.

- 구성에 대한 세부 정보를 검토합니다.
- BlueXP가 구매할 지원 및 AWS 리소스에 대한 세부 정보를 검토하려면 \* 추가 정보 \* 를 클릭합니다.
- 이해함... \* 확인란을 선택합니다.
- Go \* 를 클릭합니다.

## 결과

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

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

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

## 작업을 마친 후

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

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

## AWS C2S 환경에서 Cloud Volumes ONTAP를 시작하십시오

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

### C2S에서 지원되는 버전입니다

- Cloud Volumes ONTAP 9.8이 지원됩니다
- 커넥터 버전 3.9.4가 지원됩니다

Connector는 AWS에서 Cloud Volumes ONTAP를 구축하고 관리하는 데 필요한 소프트웨어입니다. Connector 인스턴스에 설치되는 소프트웨어에서 Cloud Manager에 로그인합니다. Cloud Manager용 SaaS 웹 사이트는 C2S 환경에서 지원되지 않습니다.



Cloud Manager는 최근 BlueXP로 이름이 바뀌었지만 Connector 버전 3.9.4 에 포함된 사용자 인터페이스가 Cloud Manager라고 불리기 때문에 C2S에서 Cloud Manager로 계속 언급하고 있습니다.

### C2S에서 지원되는 기능

C2S 환경의 Cloud Manager에서 사용할 수 있는 기능은 다음과 같습니다.

- Cloud Volumes ONTAP
- 데이터 복제

- 감사 시간 표시 막대입니다

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

C2S의 Cloud Volumes ONTAP에서는 S3에 대한 데이터 계층화도 지원됩니다.

#### 제한 사항

- Cloud Manager에서 제공되는 NetApp 클라우드 서비스가 없습니다.
- C2S 환경에는 인터넷 액세스가 없으므로 다음 기능을 사용할 수 없습니다.
  - Cloud Manager에서 소프트웨어 업그레이드 자동화
  - NetApp AutoSupport를 참조하십시오
  - Cloud Volumes ONTAP 리소스에 대한 AWS 비용 정보입니다
- C2S 환경에서는 Freemium 라이선스가 지원되지 않습니다.

#### 구축 개요

C2S에서 Cloud Volumes ONTAP 시작하기에는 몇 가지 단계가 포함되어 있습니다.

##### 1. AWS 환경 준비

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

##### 2. Connector 설치 및 Cloud Manager 설정

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

Connector 인스턴스에 설치되는 소프트웨어에서 Cloud Manager에 로그인합니다.

##### 3. Cloud Manager에서 Cloud Volumes ONTAP 실행

이러한 각 단계는 아래에 설명되어 있습니다.

#### **AWS** 환경 준비

AWS 환경은 몇 가지 요구사항을 충족해야 합니다.

#### 네트워크 설정

Cloud Volumes ONTAP가 제대로 작동할 수 있도록 AWS 네트워킹을 설정합니다.

#### 단계

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

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

#### Cloud Volumes ONTAP에 가입하십시오

Cloud Manager에서 Cloud Volumes ONTAP를 구축하려면 Marketplace에 가입해야 합니다.

#### 단계

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

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

#### 권한 설정

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

다음 각 항목에 대해 IAM 정책 및 IAM 역할이 필요합니다.

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

#### 단계

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

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:DescribeRouteTables",
      "ec2:DescribeImages",
      "ec2:CreateTags",
      "ec2:CreateVolume",
      "ec2:DescribeVolumes",
```

```
"ec2:ModifyVolumeAttribute",
"ec2:DeleteVolume",
"ec2:CreateSecurityGroup",
"ec2:DeleteSecurityGroup",
"ec2:DescribeSecurityGroups",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateNetworkInterface",
"ec2:DescribeNetworkInterfaces",
"ec2:DeleteNetworkInterface",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:DescribeDhcpOptions",
"ec2:CreateSnapshot",
"ec2:DeleteSnapshot",
"ec2:DescribeSnapshots",
"ec2:GetConsoleOutput",
"ec2:DescribeKeyPairs",
"ec2:DescribeRegions",
"ec2:DeleteTags",
"ec2:DescribeTags",
"cloudformation:CreateStack",
"cloudformation:DeleteStack",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents",
"cloudformation:ValidateTemplate",
"iam:PassRole",
"iam:CreateRole",
"iam:DeleteRole",
"iam:PutRolePolicy",
"iam:ListInstanceProfiles",
"iam:CreateInstanceProfile",
"iam:DeleteRolePolicy",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
"iam:DeleteInstanceProfile",
"s3:GetObject",
"s3:ListBucket",
"s3:GetBucketTagging",
"s3:GetBucketLocation",
"s3:ListAllMyBuckets",
"kms:List*",
"kms:Describe*",
```

```

        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2>DeletePlacementGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
    ],
    "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
        }
    },
    "Resource": [
        "arn:aws-iso:ec2:*:*:instance/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ]
}

```

```

    ],
    "Resource": [
        "arn:aws-iso:ec2:*:*:volume/*"
    ]
}
]
}

```

3. Cloud Volumes ONTAP에 대한 정책을 생성합니다.

```

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

```

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

```

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

```

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

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

Connector 인스턴스를 실행할 때 Connector IAM 역할을 선택해야 합니다.

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

#### AWS KMS를 설정합니다

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

#### 단계

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

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

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

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

3. Connector 인스턴스의 IAM 역할을 CMK의 주요 사용자 목록에 추가합니다.

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



## Connector 설치 및 Cloud Manager 설정

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

단계

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

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

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

인스턴스를 구성할 때 다음 사항에 유의하십시오.

- T3.xLarge를 권장합니다.
- AWS 환경을 준비할 때 생성한 IAM 역할을 선택해야 합니다.
- 기본 스토리지 옵션을 유지해야 합니다.
- Connector에 필요한 연결 방법은 SSH, HTTP, HTTPS입니다.

3. Connector 인스턴스에 연결된 호스트에서 Cloud Manager를 설정합니다.
  - a. 웹 브라우저를 열고 를 입력합니다 `<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>` 여기서 `_ipaddress_`는 Connector를 설치한 Linux 호스트의 IP 주소입니다.
  - b. AWS 서비스 연결을 위한 프록시 서버를 지정합니다.
  - c. 1단계에서 얻은 인증서를 업로드합니다.
  - d. 설정 마법사의 단계를 완료하여 Cloud Manager를 설정합니다.
    - \* 시스템 세부 정보 \*: 이 Cloud Manager 인스턴스의 이름을 입력하고 회사 이름을 입력합니다.
    - \* 사용자 생성 \*: Cloud Manager 관리에 사용할 관리자 사용자를 생성합니다.
    - \* 검토 \*: 세부 정보를 검토하고 최종 사용자 사용권 계약을 승인합니다.
  - e. CA 서명 인증서의 설치를 완료하려면 EC2 콘솔에서 Connector 인스턴스를 다시 시작합니다.
4. Connector가 다시 시작된 후 설치 마법사에서 만든 관리자 사용자 계정을 사용하여 로그인합니다.

## Cloud Manager에서 Cloud Volumes ONTAP 실행

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

필요한 것

- 라이선스를 구입한 경우 NetApp에서 받은 라이선스 파일이 있어야 합니다. 라이선스 파일은 JSON 형식의 .NLF 파일입니다.

- HA 중재자가 키 기반 SSH 인증을 사용할 수 있도록 키 쌍이 필요합니다.

## 단계

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

마법사를 완료하면 다음 사항에 유의하십시오.

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

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

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

이후 볼륨에 대해 다른 디스크 유형을 선택할 수 있습니다.

- AWS 디스크의 성능은 디스크 크기와 연관되어 있습니다.

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

- 디스크 크기는 시스템의 모든 디스크에 대한 기본 크기입니다.



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

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

## 결과

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

## 보안 그룹 규칙

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

## 커넥터의 보안 그룹

Connector의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

### 인바운드 규칙

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

### 아웃바운드 규칙

Connector에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

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

## Cloud Volumes ONTAP의 보안 그룹입니다

Cloud Volumes ONTAP 노드의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

### 인바운드 규칙

작업 환경을 만들고 미리 정의된 보안 그룹을 선택할 때 다음 중 한 가지 내에서 트래픽을 허용하도록 선택할 수 있습니다.

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

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

프로토콜	포트	목적
TCP	445	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
TCP	635	NFS 마운트
TCP	749	Kerberos
TCP	2049년	NFS 서버 데몬
TCP	3260입니다	iSCSI 데이터 LIF를 통한 iSCSI 액세스
TCP	4045로 문의하십시오	NFS 잠금 데몬
TCP	4046으로 문의하십시오	NFS에 대한 네트워크 상태 모니터
TCP	10000	NDMP를 사용한 백업
TCP	11104를 참조하십시오	SnapMirror에 대한 인터클러스터 통신 세션의 관리
TCP	11105를 참조하십시오	인터클러스터 LIF를 사용하여 SnapMirror 데이터 전송
UDP입니다	111	NFS에 대한 원격 프로시저 호출
UDP입니다	161-162	단순한 네트워크 관리 프로토콜
UDP입니다	635	NFS 마운트
UDP입니다	2049년	NFS 서버 데몬
UDP입니다	4045로 문의하십시오	NFS 잠금 데몬
UDP입니다	4046으로 문의하십시오	NFS에 대한 네트워크 상태 모니터
UDP입니다	4049입니다	NFS rquotad 프로토콜

#### 아웃바운드 규칙

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

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

프로토콜	포트	목적
모든 UDP	모두	모든 아웃바운드 트래픽

#### HA 중재자를 위한 외부 보안 그룹

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

#### 인바운드 규칙

인바운드 규칙의 소스는 Connector가 상주하는 VPC의 트래픽입니다.

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

#### 아웃바운드 규칙

HA 중재자를 위해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

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

#### HA 중재자를 위한 내부 보안 그룹

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

#### 인바운드 규칙

미리 정의된 보안 그룹에는 다음과 같은 인바운드 규칙이 포함됩니다.

프로토콜	포트	목적
모든 교통 정보	모두	HA 중재자 및 HA 노드 간 통신

#### 아웃바운드 규칙

미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

프로토콜	포트	목적
모든 교통 정보	모두	HA 중재자 및 HA 노드 간 통신

# Microsoft Azure에서 시작하십시오

## Azure에서 Cloud Volumes ONTAP를 빠르게 시작합니다

몇 가지 단계를 통해 Azure용 Cloud Volumes ONTAP를 시작하십시오.

1

커넥터를 작성합니다

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

인터넷에 액세스할 수 없는 서버넷에 Cloud Volumes ONTAP를 배포하려는 경우 수동으로 커넥터를 설치하고 해당 커넥터에서 실행 중인 BlueXP 사용자 인터페이스에 액세스해야 합니다. ["인터넷에 액세스하지 않고 커넥터에 수동으로 설치하는 방법에 대해 알아보십시오"](#)

2

구성을 계획합니다

BlueXP는 워크로드 요구 사항에 맞는 사전 구성된 패키지를 제공하거나 사용자가 직접 구성할 수 있습니다. 자신의 구성을 선택하는 경우 사용 가능한 옵션을 이해해야 합니다. ["자세한 정보"](#).

3

네트워크 설정

1. VNET와 서버넷이 커넥터와 Cloud Volumes ONTAP 간의 연결을 지원하는지 확인합니다.
2. NetApp AutoSupport용 VPC 타겟으로부터 아웃바운드 인터넷 액세스 지원

인터넷에 액세스할 수 없는 위치에 Cloud Volumes ONTAP를 배포하는 경우에는 이 단계가 필요하지 않습니다.

["네트워킹 요구 사항에 대해 자세히 알아보십시오"](#).

4

BlueXP를 사용하여 Cloud Volumes ONTAP를 실행합니다

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

관련 링크

- ["BlueXP에서 커넥터 만들기"](#)
- ["Azure Marketplace에서 커넥터 만들기"](#)
- ["Linux 호스트에 Connector 소프트웨어 설치"](#)
- ["권한을 가진 BlueXP의 기능"](#)

## Azure에서 Cloud Volumes ONTAP 구성 계획

Azure에서 Cloud Volumes ONTAP를 구축할 때 워크로드 요구사항에 맞게 사전 구성된 시스템을 선택하거나 고유한 구성을 생성할 수 있습니다. 자신의 구성을 선택하는 경우 사용

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 Microsoft Azure 지역에서 지원됩니다. ["지원되는 영역의 전체 목록을 봅니다"](#).

지원되는 VM 유형을 선택합니다

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

["Azure에서 Cloud Volumes ONTAP에 대해 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.

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

## Azure에서 시스템 크기 조정

Cloud Volumes ONTAP 시스템을 사이징하면 성능 및 용량 요구사항을 충족하는 데 도움이 될 수 있습니다. VM 유형, 디스크 유형 및 디스크 크기를 선택할 때 고려해야 할 몇 가지 주요 사항은 다음과 같습니다.

가상 머신 유형입니다

에서 지원되는 가상 머신 유형을 확인합니다 ["Cloud Volumes ONTAP 릴리즈 노트"](#) 지원되는 각 VM 유형에 대한 세부 정보를 검토합니다. 각 VM 유형은 특정 수의 데이터 디스크를 지원합니다.

- ["Azure 설명서: 범용 가상 머신 크기"](#)
- ["Azure 설명서: 메모리에 최적화된 가상 머신 크기"](#)

단일 노드 시스템이 있는 Azure 디스크 유형입니다

Cloud Volumes ONTAP용 볼륨을 생성할 때 Cloud Volumes ONTAP가 디스크로 사용하는 기본 클라우드 스토리지를 선택해야 합니다.

단일 노드 시스템에서는 세 가지 유형의 Azure 관리 디스크를 사용할 수 있습니다.

- *Premium SSD* 관리 디스크 높은 비용으로 I/O 집약적인 작업 부하에 높은 성능을 제공합니다.
- *\_Standard SSD Managed Disks\_* 는 낮은 IOPS가 필요한 워크로드에 일관된 성능을 제공합니다.
- *\_표준 HDD 관리 디스크\_* 는 높은 IOPS가 필요하지 않고 비용을 절감하려는 경우에 적합합니다.

이러한 디스크의 사용 사례에 대한 자세한 내용은 ["Microsoft Azure 설명서: Azure에서 사용할 수 있는 디스크 유형은 무엇입니까?"](#).

## HA 쌍을 지원하는 Azure 디스크 유형

HA 시스템은 프리미엄 SSD 공유 관리 디스크를 사용합니다. 이 두 디스크는 모두 I/O 집약적인 워크로드를 더 높은 비용으로 처리합니다. 9.12.1 릴리즈 이전에 생성된 HA 배포에서는 프리미엄 페이지 Blob을 사용합니다.

## Azure 디스크 크기입니다

Cloud Volumes ONTAP 인스턴스를 시작할 때 Aggregate의 기본 디스크 크기를 선택해야 합니다. BlueXP에서는 이 디스크 크기를 초기 집계와 단순 프로비저닝 옵션을 사용할 때 생성되는 추가 애그리게이트에 사용합니다. 예에서는 기본적으로 와는 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다 ["고급 할당 옵션을 사용합니다"](#).



Aggregate의 모든 디스크는 동일한 크기여야 합니다.

디스크 크기를 선택할 때는 몇 가지 요소를 고려해야 합니다. 디스크 크기는 스토리지에 대한 비용 지불, 애그리게이트에서 생성할 수 있는 볼륨 크기, Cloud Volumes ONTAP에 사용할 수 있는 총 용량 및 스토리지 성능에 영향을 줍니다.

Azure 프리미엄 스토리지의 성능은 디스크 크기와 관련이 있습니다. 디스크가 클수록 IOPS와 처리량이 높아집니다. 예를 들어, 1TiB 디스크를 선택하면 더 높은 비용으로 500GiB 디스크보다 뛰어난 성능을 제공할 수 있습니다.

표준 스토리지의 디스크 크기 간에는 성능 차이가 없습니다. 필요한 용량에 따라 디스크 크기를 선택해야 합니다.

IOPS 및 디스크 크기별 처리량은 Azure를 참조하십시오.

- ["Microsoft Azure: 관리형 디스크 가격"](#)
- ["Microsoft Azure: 페이지 Blob 가격 책정"](#)

## 기본 시스템 디스크를 봅니다

BlueXP는 사용자 데이터를 위한 스토리지 외에도 Cloud Volumes ONTAP 시스템 데이터(부팅 데이터, 루트 데이터, 핵심 데이터 및 NVRAM)를 위한 클라우드 스토리지를 구입합니다. 계획을 위해 Cloud Volumes ONTAP를 배포하기 전에 이러한 세부 정보를 검토하는 것이 도움이 될 수 있습니다.

["Azure에서 Cloud Volumes ONTAP 시스템 데이터에 대한 기본 디스크를 봅니다"](#).



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

## 네트워킹 정보를 수집합니다

Azure에서 Cloud Volumes ONTAP를 구축할 때는 가상 네트워크에 대한 세부 정보를 지정해야 합니다. 워크시트를 사용하여 관리자로부터 정보를 수집할 수 있습니다.

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



쓰기 속도를 선택합니다

BlueXP에서는 Cloud Volumes ONTAP에 대한 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. BlueXP에서 볼륨을 생성할 때 이러한 기능을 활성화하는 프로필이나 해당 기능을 비활성화하는 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.

## Azure의 Cloud Volumes ONTAP에 대한 네트워킹 요구사항

Cloud Volumes ONTAP 시스템이 올바르게 작동할 수 있도록 Azure 네트워킹을 설정합니다.

**Cloud Volumes ONTAP에 대한 요구사항**

Azure에서 다음 네트워킹 요구사항을 충족해야 합니다.

아웃바운드 인터넷 액세스

Cloud Volumes ONTAP 노드를 사용하려면 NetApp AutoSupport에 대한 아웃바운드 인터넷 액세스가 필요합니다. 사전 예방적으로 시스템의 상태를 모니터링하고 메시지를 NetApp 기술 지원으로 보냅니다.

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>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

AutoSupport 메시지를 보내는 데 아웃바운드 인터넷 연결을 사용할 수 없는 경우 BlueXP는 자동으로 Cloud Volumes ONTAP 시스템에서 커넥터를 프록시 서버로 사용하도록 구성합니다. 유일한 요구 사항은 커넥터의 보안 그룹이 포트 3128을 통한 `_IN인바운드_` 연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

Cloud Volumes ONTAP에 대해 엄격한 아웃바운드 규칙을 정의한 경우 Cloud Volumes ONTAP 보안 그룹이 포트 3128을 통한 `_outbound_connection`을 허용하는지 확인해야 합니다.

아웃바운드 인터넷 액세스가 가능한지 확인한 후 AutoSupport를 테스트하여 메시지를 보낼 수 있는지 확인할 수 있습니다. 자세한 지침은 을 참조하십시오 "[ONTAP 문서: AutoSupport 설정](#)".

BlueXP에서 AutoSupport 메시지를 보낼 수 없다고 알리는 경우 "[AutoSupport 구성 문제를 해결합니다](#)".

## IP 주소

BlueXP는 Azure의 Cloud Volumes ONTAP에 필요한 수의 전용 IP 주소를 자동으로 할당합니다. 네트워킹에 사용 가능한 개인 IP 주소가 충분한지 확인해야 합니다.

BlueXP에서 Cloud Volumes ONTAP에 할당하는 LIF 수는 단일 노드 시스템을 배포할지 HA 쌍을 구축하는지에 따라 달라집니다. LIF는 물리적 포트와 연결된 IP 주소입니다. SnapCenter와 같은 관리 툴을 사용하려면 SVM 관리 LIF가 필요합니다.



iSCSI LIF는 iSCSI 프로토콜을 통해 클라이언트에 액세스할 수 있도록 지원하며 시스템에서 다른 중요한 네트워킹 워크플로우에 사용됩니다. 이러한 LIF는 필수 항목이므로 삭제할 수 없습니다.

## 단일 노드 시스템의 IP 주소입니다

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

- 클러스터 관리 IP
- 노드 관리 IP
- SnapMirror에 대한 인터클러스터 IP
- NFS/CIFS IP입니다
- iSCSI IP입니다



iSCSI IP는 iSCSI 프로토콜을 통한 클라이언트 액세스를 제공합니다. 또한 시스템에서 다른 중요한 네트워킹 워크플로우에 사용됩니다. 이 LIF는 필수 항목이므로 삭제할 수 없습니다.

- SVM 관리(선택 사항 - 기본적으로 구성되지 않음)

## HA 쌍의 IP 주소

BlueXP는 구축하는 동안 노드당 4개의 NIC에 IP 주소를 할당합니다.

BlueXP는 HA 쌍에서 SVM 관리 LIF를 생성하지만 Azure의 단일 노드 시스템에서는 생성한 것이 아닙니다.

- NIC0 \*
- 노드 관리 IP
- 인터클러스터 IP
- iSCSI IP입니다



iSCSI IP는 iSCSI 프로토콜을 통한 클라이언트 액세스를 제공합니다. 또한 시스템에서 다른 중요한 네트워킹 워크플로우에 사용됩니다. 이 LIF는 필수 항목이므로 삭제할 수 없습니다.

- NIC1 \*

- 클러스터 네트워크 IP
- NIC2 \*
- 클러스터 인터커넥트 IP(HA IC)
- NIC3 \*
- Pageblob NIC IP(디스크 액세스)



NIC3는 페이지 BLOB 스토리지를 사용하는 HA 구축에만 적용됩니다.

위의 IP 주소는 페일오버 이벤트에서 마이그레이션되지 않습니다.

또한 페일오버 이벤트에 마이그레이션하도록 4개의 프런트엔드 IP(FIPS)가 구성됩니다. 이러한 프런트엔드 IP는 로드 밸런서에 있습니다.

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

#### Azure 서비스에 대한 보안 연결

기본적으로 BlueXP는 Cloud Volumes ONTAP 및 Azure 페이지 blob 저장소 계정 간의 연결에 Azure 프라이빗 링크를 활성화합니다.

대부분의 경우 BlueXP는 Azure Private Link를 관리합니다. 그러나 Azure Private DNS를 사용하는 경우에는 구성 파일을 편집해야 합니다. Azure의 커넥터 위치에 대한 요구 사항도 알고 있어야 합니다.

비즈니스 요구 사항에 따라 필요한 경우 비공개 링크 연결을 비활성화할 수도 있습니다. 링크를 사용하지 않도록 설정하면 BlueXP는 서비스 끝점을 사용하도록 Cloud Volumes ONTAP를 구성합니다.

["Cloud Volumes ONTAP에서 Azure 프라이빗 링크 또는 서비스 엔드포인트를 사용하는 방법에 대해 자세히 알아보십시오"](#).

#### 다른 ONTAP 시스템에 대한 연결

Azure의 Cloud Volumes ONTAP 시스템과 다른 네트워크의 ONTAP 시스템 간에 데이터를 복제하려면 Azure VNET와 다른 네트워크(예: 기업 네트워크) 간에 VPN 연결이 있어야 합니다.

자세한 지침은 을 참조하십시오 ["Microsoft Azure 문서: Azure 포털에서 사이트 간 연결을 만듭니다"](#).

#### HA 인터커넥트용 포트입니다

Cloud Volumes ONTAP HA 쌍에는 HA 인터커넥트가 포함되어 있어 각 노드가 해당 파트너의 작동 여부를 지속적으로 확인하고 다른 노드의 비휘발성 메모리에 대한 로그 데이터를 미리링할 수 있습니다. HA 인터커넥트에서는 통신에 TCP 포트 10006을 사용합니다.

기본적으로 HA 인터커넥트 LIF 간 통신은 열려 있으며 이 포트에 대한 보안 그룹 규칙이 없습니다. 하지만 HA 인터커넥트 LIF 간에 방화벽을 생성하는 경우, HA 쌍이 제대로 작동할 수 있도록 TCP 트래픽이 포트 10006에 대해 열려 있는지 확인해야 합니다.

Azure 리소스 그룹에서는 하나의 HA 쌍만 제공됩니다

Azure에 구축하는 각 Cloud Volumes ONTAP HA 쌍에 대해 `_Dedicated_resource` 그룹을 사용해야 합니다. 리소스 그룹에서는 하나의 HA 쌍만 지원됩니다.

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

#### 보안 그룹 규칙

BlueXP는 Cloud Volumes ONTAP가 성공적으로 운영하는 데 필요한 인바운드 및 아웃바운드 규칙을 포함하는 Azure 보안 그룹을 만듭니다. 테스트 목적으로 또는 자체 보안 그룹을 사용하려는 경우 포트를 참조할 수 있습니다.

Cloud Volumes ONTAP의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.



커넥터에 대한 정보를 찾고 계십니까? "[Connector에 대한 보안 그룹 규칙을 봅니다](#)"

단일 노드 시스템에 대한 인바운드 규칙입니다

작업 환경을 만들고 미리 정의된 보안 그룹을 선택할 때 다음 중 한 가지 내에서 트래픽을 허용하도록 선택할 수 있습니다.

- \* 선택한 VNET만 해당 \*: 인바운드 트래픽의 소스는 Cloud Volumes ONTAP 시스템에 대한 VNET의 서브넷 범위와 커넥터가 상주하는 VNET의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다.
- \* All VNets \*: 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.

우선 순위 및 이름	포트 및 프로토콜	소스 및 대상	설명
1000입니다 inbound_ssh입니다	22 TCP	모두 해당	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다
1001 inbound_http(인바운드_http)	80 TCP	모두 해당	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTP 액세스
1002 인바운드_111_TCP	111 TCP	모두 해당	NFS에 대한 원격 프로시저 호출
1003 인바운드_111_UDP	111 UDP입니다	모두 해당	NFS에 대한 원격 프로시저 호출
1004 인바운드_139	139 TCP	모두 해당	CIFS에 대한 NetBIOS 서비스 세션입니다
1005 인바운드_161-162_TCP	161-162 TCP	모두 해당	단순한 네트워크 관리 프로토콜
1006 인바운드_161-162_UDP	161-162 UDP입니다	모두 해당	단순한 네트워크 관리 프로토콜

우선 순위 및 이름	포트 및 프로토콜	소스 및 대상	설명
1007 인바운드_443	443 TCP	모두 해당	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 커넥터 및 HTTPS 액세스와의 연결
1008년 IN인바운드_445	445 TCP	모두 해당	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
1009입니다 인바운드_635_TCP	635 TCP	모두 해당	NFS 마운트
1010 인바운드_635_UDP	635 UDP입니다	모두 해당	NFS 마운트
1011 인바운드_749	749 TCP	모두 해당	Kerberos
1012입니다 인바운드_2049_TCP	2049년 TCP	모두 해당	NFS 서버 데몬
1013 인바운드_2049_UDP	2049년 UDP입니다	모두 해당	NFS 서버 데몬
1014 인바운드_3260	3260입니다 TCP	모두 해당	iSCSI 데이터 LIF를 통한 iSCSI 액세스
1015 인바운드_4045-4046_TCP	4045-4046 을 참조하십시오 TCP	모두 해당	NFS 잠금 데몬 및 네트워크 상태 모니터
1016 인바운드_4045-4046_UDP	4045-4046 을 참조하십시오 UDP입니다	모두 해당	NFS 잠금 데몬 및 네트워크 상태 모니터
1017 인바운드 _ 10000	10000 TCP	모두 해당	NDMP를 사용한 백업
1018세 IN인바운드_11104-11105	11104-11105 를 참조하십시오 TCP	모두 해당	SnapMirror 데이터 전송
3000입니다 inbound_deny_all_tcp입 니다	모든 포트 TCP	모두 해당	다른 모든 TCP 인바운드 트래픽을 차단합니다
3001입니다 inbound_deny_all_udp입 니다	모든 포트 UDP입니다	모두 해당	다른 모든 UDP 인바운드 트래픽을 차단합니다
65000입니다 AllowVnetInBound 를 참조하십시오	모든 포트 모든 프로토콜	VirtualNetwork - VirtualNetwork	VNET 내에서 들어오는 인바운드 트래픽입니다
65001 AllowAzureLoad BalancerInBound 를 참조하십시오	모든 포트 모든 프로토콜	어느 것이든 AzureLoadBalancer를 사용합니다	Azure 표준 로드 밸런서의 데이터 트래픽

우선 순위 및 이름	포트 및 프로토콜	소스 및 대상	설명
6,5005 DenyAllInBound를 참조하십시오	모든 포트 모든 프로토콜	모두 해당	다른 모든 인바운드 트래픽을 차단합니다

## HA 시스템에 대한 인바운드 규칙

작업 환경을 만들고 미리 정의된 보안 그룹을 선택할 때 다음 중 한 가지 내에서 트래픽을 허용하도록 선택할 수 있습니다.

- \* 선택한 VNET만 해당 \*: 인바운드 트래픽의 소스는 Cloud Volumes ONTAP 시스템에 대한 VNET의 서브넷 범위와 커넥터가 상주하는 VNET의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다.
- \* All VNETs \*: 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.



인바운드 데이터 트래픽이 Azure 표준 로드 밸런서를 통과하기 때문에 HA 시스템은 단일 노드 시스템보다 인바운드 규칙이 적습니다. 따라서 "AllowAzureLoadBalancerInBound" 규칙에 나와 있는 것처럼 로드 밸런서의 트래픽이 열려 있어야 합니다.

우선 순위 및 이름	포트 및 프로토콜	소스 및 대상	설명
100 인바운드_443	443 모든 프로토콜	모두 해당	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 커넥터 및 HTTPS 액세스와의 연결
101 인바운드_111_TCP	111 모든 프로토콜	모두 해당	NFS에 대한 원격 프로시저 호출
102 인바운드_2049_TCP	2049년 모든 프로토콜	모두 해당	NFS 서버 데몬
111 inbound_ssh입니다	22 모든 프로토콜	모두 해당	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다
121 인바운드_53	53 모든 프로토콜	모두 해당	DNS 및 CIFS를 지원합니다
65000입니다 AllowVnetInBound 를 참조하십시오	모든 포트 모든 프로토콜	VirtualNetwork - VirtualNetwork	VNET 내에서 들어오는 인바운드 트래픽입니다
65001 AllowAzureLoad BalancerInBound 를 참조하십시오	모든 포트 모든 프로토콜	어느 것이든 AzureLoadBalancer를 사용합니다	Azure 표준 로드 밸런서의 데이터 트래픽
6,5005 DenyAllInBound를 참조하십시오	모든 포트 모든 프로토콜	모두 해당	다른 모든 인바운드 트래픽을 차단합니다

## 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.

포트	프로토콜	목적
모두	모든 TCP	모든 아웃바운드 트래픽
모두	모든 UDP	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	포트	프로 토콜	출처	목적지	목적
Active Directory 를 클릭합니 다					



	404	TCP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
서비스	464 포트	UDP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos 키 관리 목적
	749	TCP	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(RPCSEC_GSS)
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)
	TCP	3128	노드 관리 LIF	커넥터	아웃바운드 인터넷 연결을 사용할 수 없는 경우 커넥터의 프록시 서버를 통해 AutoSupport 메시지 보내기
구성 백업	HTTP	80	노드 관리 LIF	http://<connector-IP-address>/occm/offboxconfig입니다	Connector로 구성 백업을 보냅니다. "구성 백업 파일에 대해 자세히 알아보십시오".
DHCP를 선택합니다	68	UDP	노드 관리 LIF	DHCP를 선택합니다	처음으로 설정하는 DHCP 클라이언트
DHCPS	67	UDP	노드 관리 LIF	DHCP를 선택합니다	DHCP 서버
DNS	53	UDP	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
NDMP	18600-18699	TCP	노드 관리 LIF	대상 서버	NDMP 복제
SMTP	25	TCP	노드 관리 LIF	메일 서버	AutoSupport에 사용할 수 있는 SMTP 경고
SNMP를 선택합니다	161	TCP	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	161	UDP	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	162	TCP	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	162	UDP	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
SnapMirror를 참조하십시오	11104를 참조하십시오	TCP	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror에 대한 인터클러스터 통신 세션의 관리
	11105를 참조하십시오	TCP	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror 데이터 전송
Syslog를 클릭합니다	514	UDP	노드 관리 LIF	Syslog 서버	Syslog 메시지를 전달합니다

## 커넥터 요구 사항

아직 Connector를 만들지 않은 경우 Connector에 대한 네트워킹 요구 사항도 검토해야 합니다.

- ["커넥터에 대한 네트워킹 요구 사항을 봅니다"](#)
- ["Azure의 보안 그룹 규칙"](#)

## Azure에서 고객이 관리하는 키를 사용하도록 Cloud Volumes ONTAP를 설정합니다

Azure의 Cloud Volumes ONTAP에서 를 사용하여 데이터가 자동으로 암호화됩니다 ["Azure 스토리지 서비스 암호화"](#) Microsoft 관리 키를 사용합니다. 그러나 이 페이지의 단계를 따르면 사용자 고유의 암호화 키를 사용할 수 있습니다.

### 데이터 암호화 개요

Cloud Volumes ONTAP 데이터는 를 사용하여 Azure에서 자동으로 암호화됩니다 ["Azure 스토리지 서비스 암호화"](#). 기본 구현에는 Microsoft 관리 키가 사용됩니다. 설정이 필요하지 않습니다.

Cloud Volumes ONTAP에서 고객 관리 키를 사용하려면 다음 단계를 완료해야 합니다.

1. Azure에서 키 볼트를 작성한 다음 해당 볼트에 키를 생성합니다
2. BlueXP에서 API를 사용하여 키를 사용하는 Cloud Volumes ONTAP 작업 환경을 만듭니다

### 키 회전

새 버전의 키를 만들면 Cloud Volumes ONTAP에서 자동으로 최신 키 버전을 사용합니다.

### 데이터 암호화 방법

고객이 관리하는 키를 사용하도록 구성된 Cloud Volumes ONTAP 작업 환경을 생성한 후 Cloud Volumes ONTAP 데이터는 다음과 같이 암호화됩니다.

#### Azure HA 다중 가용성 영역

- Cloud Volumes ONTAP의 모든 Azure 저장소 계정은 고객이 관리하는 키를 사용하여 암호화됩니다.<sup>1</sup>
- 루트, 부팅, NVRAM, 코어 및 데이터 디스크의 경우 BlueXP는 디스크 암호화 세트를 사용하여 관리되는 디스크로 암호화 키를 관리할 수 있습니다.
- 새 데이터 디스크도 동일한 디스크 암호화 세트를 사용합니다.

#### Azure HA 단일 가용성 영역

- Cloud Volumes ONTAP의 모든 Azure 저장소 계정은 고객이 관리하는 키를 사용하여 암호화됩니다.<sup>1</sup>
- 디스크 또는 애그리게이트를 추가하는 경우와 같이 새로운 스토리지 계정에서도 동일한 키를 사용합니다.<sup>1</sup>
- ONTAP 9.10.1P3에서 NVRAM 및 코어 디스크의 경우 BlueXP는 을 사용합니다 ["디스크 암호화가 설정되었습니다"](#)관리 디스크를 사용하여 암호화 키를 관리할 수 있습니다. 하위 버전은 고객 관리 키 대신 Microsoft 관리 키를 사용합니다.

### 단일 노드

- Cloud Volumes ONTAP의 모든 Azure 저장소 계정은 고객이 관리하는 키를 사용하여 암호화됩니다. <sup>1</sup>

- 루트, 부팅 및 데이터 디스크의 경우 BlueXP는 을 사용합니다 **"디스크 암호화가 설정되었습니다"**관리 디스크를 사용하여 암호화 키를 관리할 수 있습니다.
- 새 데이터 디스크도 동일한 디스크 암호화 세트를 사용합니다.
- ONTAP 9.9.1P7에서 NVRAM 및 코어 디스크의 경우 BlueXP는 디스크 암호화 세트를 사용하여 관리되는 디스크로 암호화 키를 관리할 수 있습니다. 하위 버전은 고객 관리 키 대신 Microsoft 관리 키를 사용합니다.

## 각주

1. 생성 중에 스토리지 계정을 암호화하려면 CVO 생성 요청에서 리소스 ID를 생성하고 제공해야 합니다. 이는 모든 유형의 배포에 적용됩니다. 제공하지 않으면 저장소 계정은 여전히 암호화되지만 BlueXP는 먼저 Microsoft 관리 키 암호화를 사용하여 저장소 계정을 만든 다음 고객이 관리하는 키를 사용하도록 저장소 계정을 업데이트합니다.

## 사용자가 할당한 관리 ID를 만듭니다

사용자가 할당한 관리 ID라는 리소스를 만들 수 있습니다. 이렇게 하면 Cloud Volumes ONTAP 작업 환경을 생성할 때 스토리지 계정을 암호화할 수 있습니다. 키 볼트를 작성하고 키를 생성하기 전에 이 리소스를 생성하는 것이 좋습니다.

리소스의 ID는 다음과 같습니다. `userassignedidentity`.

## 단계

1. Azure에서 Azure 서비스로 이동하여 **\* Managed Identities \*** 를 선택합니다.
2. **Create \*** 를 클릭합니다.
3. 다음 세부 정보를 제공합니다.
  - **\* 구독 \***: 구독을 선택합니다. Connector 가입과 동일한 구독을 선택하는 것이 좋습니다.
  - **\* 리소스 그룹 \***: 기존 리소스 그룹을 사용하거나 새 리소스 그룹을 생성합니다.
  - **\* Region \* (영역 \*)**: 선택적으로 Connector (커넥터)와 동일한 영역을 선택합니다.
  - **\* 이름 \***: 리소스 이름을 입력합니다.
4. 필요에 따라 태그를 추가합니다.
5. **Create \*** 를 클릭합니다.

## 키 볼트를 작성하고 키를 생성합니다

키 볼트는 Cloud Volumes ONTAP 시스템을 생성하려는 Azure 가입 및 지역에 있어야 합니다.

있다면 **사용자가 할당한 관리 ID를 만들었습니다**키 볼트를 작성하는 동안 키 볼트에 대한 액세스 정책도 작성해야 합니다.

## 단계

1. **"Azure 구독에서 키 볼트를 작성합니다"**.

키 볼트에 대한 다음 요구 사항을 확인합니다.

- 키 볼트는 Cloud Volumes ONTAP 시스템과 동일한 영역에 있어야 합니다.
- 다음 옵션을 활성화해야 합니다.
  - **\* soft-delete \*** (이 옵션은 기본적으로 활성화되어 있지만 반드시 `_not_` 사용하지 않아야 함)

- \* 퍼지 보호 \*
  - \* 볼륨 암호화를 위한 Azure 디스크 암호화 \* (단일 노드 시스템 또는 여러 종의 HA 쌍)
  - 사용자 지정 관리 ID를 만든 경우 다음 옵션을 활성화해야 합니다.
    - \* 볼트 액세스 정책 \*
2. 볼트 액세스 정책을 선택한 경우, 작성 을 클릭하여 키 볼트에 대한 액세스 정책을 작성합니다. 그렇지 않은 경우 3단계로 건너뛴니다.
- a. 다음 권한을 선택합니다.
- 가져오기
  - 목록
  - 암호를 해독합니다
  - 암호화
  - 줄 바꿈 해제 키
  - 랩 키
  - 확인합니다
  - 서명
- b. 사용자가 할당한 관리 ID(리소스)를 보안 주체에 선택합니다.
- c. 액세스 정책을 검토하고 생성합니다.
3. "키 볼트에 키를 생성합니다".

키에 대한 다음 요구 사항을 확인합니다.

- 키 유형은 \* rsa \* 여야 합니다.
- 권장되는 RSA 키 크기는 \* 2048 \* 이지만 다른 크기가 지원됩니다.

암호화 키를 사용하는 작업 환경을 만듭니다

키 볼트를 작성하고 암호화 키를 생성한 후 키를 사용하도록 구성된 새 Cloud Volumes ONTAP 시스템을 작성할 수 있습니다. 이러한 단계는 BlueXP API를 사용하여 지원됩니다.

필수 권한

단일 노드 Cloud Volumes ONTAP 시스템에서 고객 관리 키를 사용하려면 BlueXP 커넥터에 다음과 같은 권한이 있는지 확인하십시오.

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

## "최신 사용 권한 목록을 봅니다"

### 단계

1. 다음 BlueXP API 호출을 사용하여 Azure 구독의 키 볼트 목록을 가져옵니다.

HA 쌍: `GET /azure/ha/metadata/vaults`

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

이름 \* 과 \* resourceGroup \* 을 기록해 둡니다. 다음 단계에서 이러한 값을 지정해야 합니다.

["이 API 호출에 대해 자세히 알아보십시오"](#).

2. 다음 BlueXP API 호출을 사용하여 볼트 내의 키 목록을 가져옵니다.

HA 쌍: `GET /azure/ha/metadata/keys-vault`

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

keyName \* 을 기록해 두십시오. 다음 단계에서 해당 값을 볼트 이름과 함께 지정해야 합니다.

["이 API 호출에 대해 자세히 알아보십시오"](#).

3. 다음 BlueXP API 호출을 사용하여 Cloud Volumes ONTAP 시스템을 생성합니다.

#### a. HA 쌍:

`POST /azure/ha/working-environments`

요청 본문에는 다음 필드가 포함되어야 합니다.

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



을 포함합니다 "userAssignedIdentity": " userAssignedIdentityId" 스토리지 계정 암호화에 사용할 이 리소스를 생성한 경우 필드입니다.

["이 API 호출에 대해 자세히 알아보십시오"](#).

#### b. 단일 노드 시스템의 경우:

`POST /azure/vsa/working-environments`

요청 본문에는 다음 필드가 포함되어야 합니다.

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



을 포함합니다 "userAssignedIdentity": " userAssignedIdentityId" 스토리지 계정 암호화에 사용할 이 리소스를 생성한 경우 필드입니다.

"이 API 호출에 대해 자세히 알아보십시오".

## 결과

데이터 암호화에 고객 관리 키를 사용하도록 구성된 새 Cloud Volumes ONTAP 시스템이 있습니다.

## Azure에서 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. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 BlueXP의 단계를 따릅니다.
  - a. 세부 정보 및 자격 증명 \* 페이지에서 \* 자격 증명 편집 > 구독 추가 \* 를 클릭한 다음 화면의 지시에 따라 Azure 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](#)".

### Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials  
 Managed Service Identity

Azure Subscription  
 OCCM Dev (Default)

Marketplace Subscription  
 ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

a. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 \* Freemium \* 을 선택합니다.

### Select Charging Method

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

"Azure에서 Cloud Volumes ONTAP를 시작하는 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)
- Azure Marketplace에서 PAYGO(Pay-as-you-Go) 구독을 통해 시간 단위로 비용을 지불하는 것이 좋습니다
- 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. "NetApp Support 사이트 계정을 BlueXP에 추가합니다"

BlueXP는 NetApp의 라이선스 서비스에 자동으로 쿼리하여 NetApp Support 사이트 계정과 관련된 라이선스에 대한 자세한 정보를 확인합니다. 오류가 없으면 BlueXP는 자동으로 디지털 지갑에 라이선스를 추가합니다.

Cloud Volumes ONTAP와 함께 사용하기 전에 BlueXP 디지털 지갑에서 라이선스를 사용할 수 있어야 합니다. 필요한 경우, 할 수 있습니다 "[BlueXP 디지털 지갑에 라이선스를 수동으로 추가합니다](#)".

3. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 BlueXP의 단계를 따릅니다.
  - a. 세부 정보 및 자격 증명 \* 페이지에서 \* 자격 증명 편집 > 구독 추가 \* 를 클릭한 다음 화면의 지시에 따라 Azure Marketplace에서 선불 종량제 서비스를 구독합니다.

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



### Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials  
 Managed Service Identity

Azure Subscription  
 OCCM Dev (Default)

Marketplace Subscription  
 ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

a. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 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	∨

"Azure에서 Cloud Volumes ONTAP를 시작하는 단계별 지침을 확인하십시오".

#### PAYGO 구독

클라우드 공급자 마켓플레이스의 서비스에 가입하여 시간별 비용 지불

Cloud Volumes ONTAP 작업 환경을 만들 때 BlueXP는 Azure 마켓플레이스에서 사용 가능한 계약을 구독하라는 메시지를 표시합니다. 그러면 해당 구독이 충전을 위한 작업 환경과 연결됩니다. 추가 작업 환경에 동일한

서브스크립션을 사용할 수 있습니다.

단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 BlueXP의 단계를 따릅니다.
  - a. 세부 정보 및 자격 증명 \* 페이지에서 \* 자격 증명 편집 > 구독 추가 \* 를 클릭한 다음 화면의 지시에 따라 Azure Marketplace에서 선불 종량제 서비스를 구독합니다.

**Edit Credentials & Add Subscription**

Associate Subscription to Credentials ⓘ

Credentials  
Managed Service Identity

Azure Subscription  
OCCM Dev (Default)

Marketplace Subscription  
ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

- b. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 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	▼

"Azure에서 Cloud Volumes ONTAP를 시작하는 단계별 지침을 확인하십시오".



설정 > 자격 증명 페이지에서 Azure 계정과 연결된 Azure 마켓플레이스 구독을 관리할 수 있습니다.  
"Azure 계정 및 구독을 관리하는 방법에 대해 알아보십시오"

연간 계약

연간 계약을 구매하여 매년 Cloud Volumes ONTAP에 대한 비용을 지불합니다.

단계

1. 연간 계약을 구입하려면 NetApp 세일즈 담당자에게 문의하십시오.

이 계약은 Azure 마켓플레이스에서 `_private_Offer`로 제공됩니다.

NetApp이 프라이빗 오퍼를 공유하면 작업 환경을 생성하는 동안 Azure 마켓플레이스에서 구독할 때 연간 계획을 선택할 수 있습니다.

2. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 BlueXP의 단계를 따릅니다.
  - a. 세부 정보 및 자격 증명 \* 페이지에서 \* 자격 증명 편집 > 구독 추가 > 계속 \* 을 클릭합니다.
  - b. Azure 포털에서 Azure 계정과 공유된 연간 계획을 선택한 다음 \* 구독 \* 을 클릭합니다.
  - c. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 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

"Azure에서 Cloud Volumes ONTAP를 시작하는 단계별 지침을 확인하십시오".

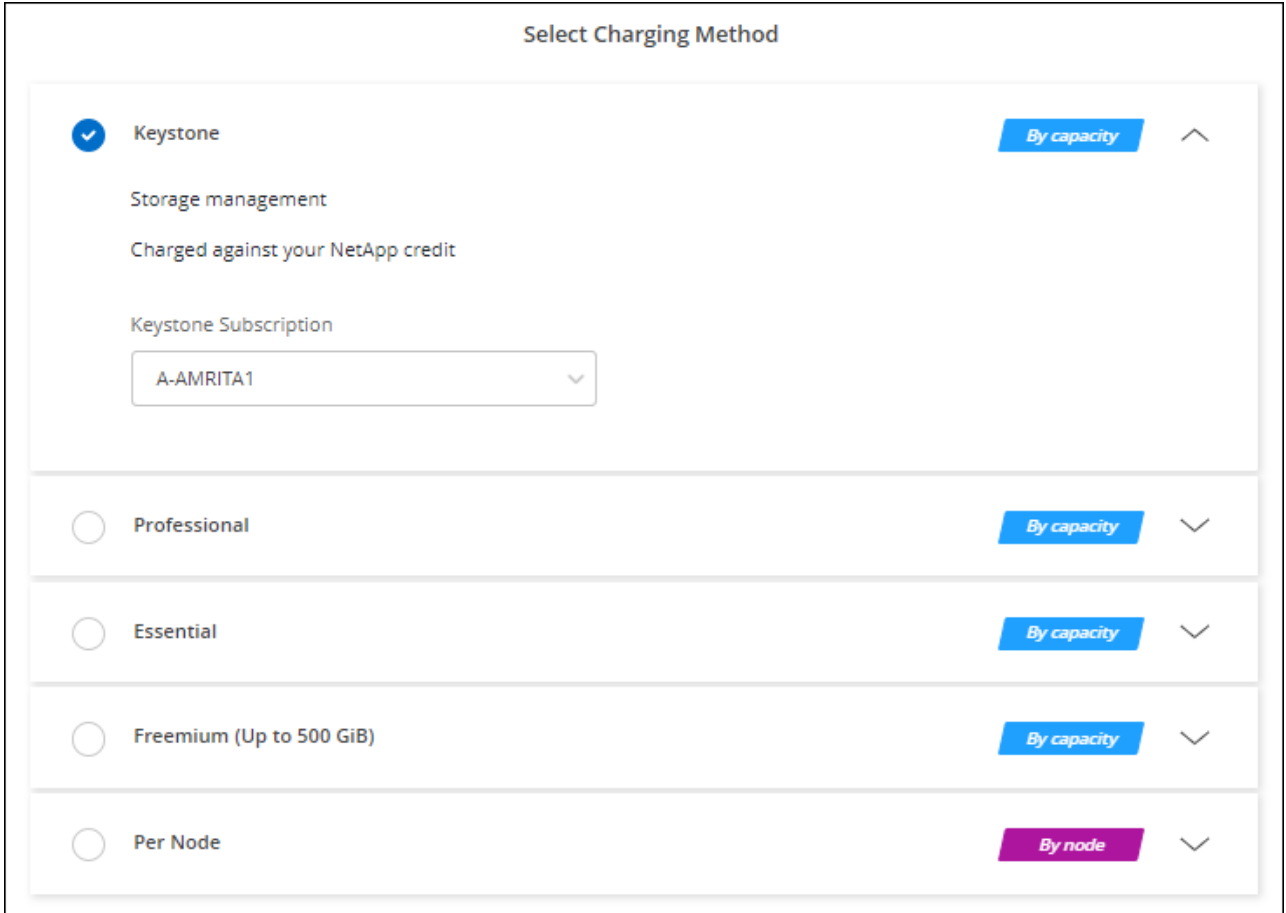
## Keystone 구독

Keystone 가입은 종량제 구독 기반 서비스입니다. "NetApp Keystone 구독에 대해 자세히 알아보십시오".

단계

1. 아직 구독이 없는 경우 "NetApp에 문의하십시오"
2. <mailto:ng-keystone-success@netapp.com> [NetApp에 문의]하여 하나 이상의 Keystone 구독으로 BlueXP 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 BlueXP의 단계를 따릅니다.
  - a. 충전 방법을 선택하라는 메시지가 표시되면 Keystone 가입 충전 방법을 선택합니다.



"Azure에서 [Cloud Volumes ONTAP](#)를 시작하는 단계별 지침을 확인하십시오".

## Azure에서 고가용성 모드를 활성화합니다

계획되지 않은 페일오버 시간을 줄이고 Cloud Volumes ONTAP에 대한 NFSv4 지원을 활성화하려면 Microsoft Azure의 고가용성 모드를 활성화해야 합니다.

Cloud Volumes ONTAP 9.10.1 릴리즈부터 Microsoft Azure에서 실행되는 Cloud Volumes ONTAP HA 쌍의 계획되지 않은 페일오버 시간을 줄이고 NFSv4에 대한 지원을 추가했습니다. Cloud Volumes ONTAP에서 이러한 향상된 기능을 사용하려면 Azure 구독에서 고가용성 기능을 활성화해야 합니다.

Azure 구독에서 이 기능을 활성화해야 하는 경우 BlueXP에서 작업 필요 메시지에 이러한 세부 정보를 표시합니다.

다음 사항에 유의하십시오.

- Cloud Volumes ONTAP HA 쌍의 고가용성에는 문제가 없습니다. 이 Azure 기능은 ONTAP와 함께 작동하여 계획되지 않은 페일오버 이벤트로 인해 NFS 프로토콜에 대해 클라이언트에서 관측된 애플리케이션 중단 시간을 줄입니다.
- 이 기능을 사용하도록 설정하는 것은 Cloud Volumes ONTAP HA 쌍의 무중단 기능입니다.

- Azure 구독에서 이 기능을 활성화해도 다른 VM에 문제가 발생하지 않습니다.

"소유자" 권한이 있는 Azure 사용자는 Azure CLI에서 이 기능을 활성화할 수 있습니다.

단계

1. ["Azure Portal에서 Azure Cloud Shell에 액세스합니다"](#)
2. 고가용성 모드 기능 등록:

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

3. 필요한 경우 기능이 지금 등록되었는지 확인합니다.

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

Azure CLI는 다음과 유사한 결과를 반환해야 합니다.

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

## Azure에서 Cloud Volumes ONTAP 실행

BlueXP에서 Cloud Volumes ONTAP 작업 환경을 생성하여 Azure에서 단일 노드 시스템 또는 HA 쌍을 시작할 수 있습니다.

필요한 것

작업 환경을 만들려면 다음이 필요합니다.

- 실행 중인 커넥터입니다.
  - 가 있어야 합니다 "작업 영역과 연결된 커넥터입니다".
  - "항상 Connector를 실행 상태로 둘 준비가 되어 있어야 합니다".

- 사용하려는 구성에 대한 이해.

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

- Cloud Volumes ONTAP에 대한 라이선스 설정에 필요한 사항을 이해합니다.

["라이선스 설정 방법에 대해 알아보십시오"](#).

#### 이 작업에 대해

BlueXP는 Azure에서 Cloud Volumes ONTAP 시스템을 생성할 때 리소스 그룹, 네트워크 인터페이스 및 스토리지 계정과 같은 여러 Azure 개체를 생성합니다. 마법사 마지막에서 리소스 요약을 검토할 수 있습니다.

#### 데이터 손실 가능성

모범 사례는 각 Cloud Volumes ONTAP 시스템에 새로운 전용 리소스 그룹을 사용하는 것입니다.



기존 공유 리소스 그룹에 Cloud Volumes ONTAP를 배포하는 것은 데이터 손실 위험이 있기 때문에 권장되지 않습니다. BlueXP는 배포 실패 또는 삭제 시 공유 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거할 수 있지만 Azure 사용자는 실수로 공유 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 삭제할 수 있습니다.

### Azure에서 단일 노드 Cloud Volumes ONTAP 시스템 시작

Azure에서 단일 노드 Cloud Volumes ONTAP 시스템을 실행하려면 BlueXP에서 단일 노드 작업 환경을 만들어야 합니다.

#### 단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 화면의 지시를 따릅니다.
3. \* 위치 선택 \*: \* Microsoft Azure \* 및 \* Cloud Volumes ONTAP 단일 노드 \* 를 선택합니다.
4. 메시지가 표시되면 ["커넥터를 작성합니다"](#).
5. \* 세부 정보 및 자격 증명 \*: 필요에 따라 Azure 자격 증명 및 구독을 변경하고, 클러스터 이름을 지정하고, 필요한 경우 태그를 추가한 다음 자격 증명을 지정합니다.

다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
작업 환경 이름	BlueXP는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Azure 가상 시스템 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.

필드에 입력합니다	설명
리소스 그룹 태그	<p>태그는 Azure 리소스에 대한 메타데이터입니다. 이 필드에 태그를 입력하면 BlueXP가 Cloud Volumes ONTAP 시스템과 연결된 리소스 그룹에 태그를 추가합니다.</p> <p>작업 환경을 만들 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 생성된 후에는 더 많은 태그를 추가할 수 있습니다. API는 작업 환경을 생성할 때 태그를 4개로 제한하지 않습니다.</p> <p>태그에 대한 자세한 내용은 을 참조하십시오 "<a href="#">Microsoft Azure 문서: 태그를 사용하여 Azure 리소스를 구성합니다</a>".</p>
사용자 이름 및 암호	<p>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.</p>
자격 증명 편집	<p>이 Cloud Volumes ONTAP 시스템에서 사용할 다른 Azure 자격 증명과 다른 Azure 구독을 선택할 수 있습니다. 선불 종량제 Cloud Volumes ONTAP 시스템을 배포하려면 Azure 마켓플레이스 구독을 선택한 Azure 구독과 연결해야 합니다. "<a href="#">자격 증명을 추가하는 방법에 대해 알아보십시오</a>".</p>

다음 비디오에서는 마켓플레이스 구독을 Azure 구독에 연결하는 방법을 보여 줍니다.

▶ [https://docs.netapp.com/ko-kr/test//media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/ko-kr/test//media/video_subscribing_azure.mp4) (video)

- \* 서비스 \*: Cloud Volumes ONTAP에서 사용하지 않을 개별 서비스를 활성화 또는 비활성화합니다.
  - "BlueXP 분류에 대해 자세히 알아보십시오"
  - "BlueXP 백업 및 복구에 대해 자세히 알아보십시오"




WORM 및 데이터 계층화를 사용하려면 BlueXP 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 작업 환경을 구축해야 합니다.

- \* Location \*: 지역, 가용성 영역, VNET 및 서브넷을 선택한 다음 확인란을 선택하여 Connector와 대상 위치 간의 네트워크 연결을 확인합니다.

단일 노드 시스템의 경우 Cloud Volumes ONTAP를 구축할 가용성 영역을 선택할 수 있습니다. AZ를 선택하지 않으면 BlueXP가 사용자를 위해 하나를 선택합니다.

- \* 연결 \*: 새 리소스 그룹 또는 기존 리소스 그룹을 선택한 다음 미리 정의된 보안 그룹을 사용할지 아니면 직접 사용할 것인지 선택합니다.

다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
리소스 그룹	<p>Cloud Volumes ONTAP에 대한 새 리소스 그룹을 만들거나 기존 리소스 그룹을 사용합니다. 모범 사례는 Cloud Volumes ONTAP에 대한 새로운 전용 리소스 그룹을 사용하는 것입니다. 기존 공유 리소스 그룹에 Cloud Volumes ONTAP를 배포할 수는 있지만 데이터 손실 위험 때문에 권장되지 않습니다. 자세한 내용은 위의 경고를 참조하십시오.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>사용 중인 Azure 계정에 가 있는 경우 "필수 권한", BlueXP는 배포 실패 또는 삭제 시 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거합니다.</p> </div>
보안 그룹을 생성했습니다	<p>BlueXP에서 보안 그룹을 생성하도록 하면 트래픽을 허용하는 방법을 선택해야 합니다.</p> <ul style="list-style-type: none"> <li>• 선택한 VNET만 * 을 선택한 경우 인바운드 트래픽의 소스는 선택한 VNET의 서브넷 범위와 커넥터가 상주하는 VNET의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다.</li> <li>• All VNets * 를 선택한 경우 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.</li> </ul>
기존 항목 사용	<p>기존 보안 그룹을 선택하는 경우 Cloud Volumes ONTAP 요구 사항을 충족해야 합니다. "기본 보안 그룹을 봅니다".</p>

9. \* 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"](#).

10. \* 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.

11. \* 라이선스 \*: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 가상 머신 유형을 선택합니다.



선택한 버전에 대해 최신 출시 후보, 일반 가용성 또는 패치 릴리스를 사용할 수 있는 경우 BlueXP는 작업 환경을 만들 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).

12. \* Azure Marketplace \* 구독: BlueXP가 Cloud Volumes ONTAP의 프로그래밍 방식 배포를 활성화할 수 없는 경우 다음 단계를 따르십시오.

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

다음 사항에 유의하십시오.

- 디스크 유형은 초기 볼륨입니다. 이후 볼륨에 대해 다른 디스크 유형을 선택할 수 있습니다.
- 디스크 크기는 초기 애그리게이트의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 BlueXP가 생성하는



추가 애그리게이트에서 사용됩니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.

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

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

["데이터 계층화에 대해 자세히 알아보십시오"](#).

14. \* 쓰기 속도 및 WORM \*:

- a. 필요한 경우 \* Normal \* (정상 \*) 또는 \* High \* (높음 \*) 쓰기 속도를 선택합니다.

["쓰기 속도에 대해 자세히 알아보십시오"](#).

- b. 필요한 경우 WORM(Write Once, Read Many) 스토리지를 활성화합니다.

이 옵션은 특정 VM 유형에만 사용할 수 있습니다. 지원되는 VM 유형에 대한 자세한 내용은 을 참조하십시오 ["HA Pair에 대한 라이선스에서 지원되는 구성"](#).

Cloud Volumes ONTAP 9.7 이하 버전에서 데이터 계층화가 활성화된 경우 WORM을 사용할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로의 되돌리기 또는 다운그레이드가 차단됩니다.

["WORM 스토리지에 대해 자세히 알아보십시오"](#).

- a. WORM 스토리지를 활성화한 경우 보존 기간을 선택합니다.

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

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

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

필드에 입력합니다	설명
크기	입력할 수 있는 최대 크기는 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 BlueXP는 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.

필드에 입력합니다	설명
고급 옵션(NFS에만 해당)	볼륨의 NFS 버전 선택: NFSv3 또는 NFSv4
이니시에이터 그룹 및 IQN(iSCSI 전용)	<p>iSCSI 스토리지 타겟을 LUN(논리 유닛)이라고 하며 호스트에 표준 블록 디바이스로 표시됩니다.</p> <p>이니시에이터 그룹은 iSCSI 호스트 노드 이름의 테이블이며 어떤 이니시에이터가 어떤 LUN을 액세스할 수 있는지 제어합니다.</p> <p>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.</p> <p>iSCSI 볼륨을 생성할 때 BlueXP에서 자동으로 LUN을 생성합니다. 볼륨 당 하나의 LUN만 생성하므로 관리가 필요 없습니다. 볼륨을 생성한 후 <b>"IQN을 사용하여 호스트에서 LUN에 연결합니다"</b>.</p>

다음 이미지는 CIFS 프로토콜에 대해 작성된 볼륨 페이지를 보여 줍니다.

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy:

Default Policy

#### Protocol

NFS     CIFS     iSCSI

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

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

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

필드에 입력합니다	설명
조직 구성 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다.  Azure AD 도메인 서비스를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 * OU=ADDC 컴퓨터 * 또는 * OU=ADDC 사용자 * 를 입력해야 합니다. <a href="#">"Azure 설명서: Azure AD 도메인 서비스 관리 도메인에 OU(조직 구성 단위)를 만듭니다"</a>
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="#">"BlueXP 자동화 문서"</a> 를 참조하십시오.  CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 생성한 후에는 구성할 수 없습니다.

17. \* 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"](#).

18. \* 검토 및 승인 \*: 선택 사항을 검토 및 확인합니다.
- 구성에 대한 세부 정보를 검토합니다.
  - BlueXP가 구매할 지원 및 Azure 리소스에 대한 세부 정보를 검토하려면 \* 추가 정보 \* 를 클릭합니다.
  - 이해함... \* 확인란을 선택합니다.
  - Go \* 를 클릭합니다.

## 결과

BlueXP는 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.

## Azure에서 Cloud Volumes ONTAP HA 쌍 시작

Azure에서 Cloud Volumes ONTAP HA 쌍을 실행하려면 BlueXP에서 HA 작업 환경을 만들어야 합니다.

단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 화면의 지시를 따릅니다.
3. 메시지가 표시되면 "커넥터를 작성합니다".
4. \* 세부 정보 및 자격 증명 \*: 필요에 따라 Azure 자격 증명 및 구독을 변경하고, 클러스터 이름을 지정하고, 필요한 경우 태그를 추가한 다음 자격 증명을 지정합니다.

다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
작업 환경 이름	BlueXP는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Azure 가상 시스템 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.
리소스 그룹 태그	태그는 Azure 리소스에 대한 메타데이터입니다. 이 필드에 태그를 입력하면 BlueXP가 Cloud Volumes ONTAP 시스템과 연결된 리소스 그룹에 태그를 추가합니다.  작업 환경을 만들 때 사용자 인터페이스에서 최대 4개의 태그를 추가할 수 있으며, 생성된 후에는 더 많은 태그를 추가할 수 있습니다. API는 작업 환경을 생성할 때 태그를 4개로 제한하지 않습니다.  태그에 대한 자세한 내용은 을 참조하십시오 " <a href="#">Microsoft Azure 문서: 태그를 사용하여 Azure 리소스를 구성합니다</a> ".
사용자 이름 및 암호	Cloud Volumes ONTAP 클러스터 관리자 계정의 자격 증명입니다. 이러한 자격 증명을 사용하여 System Manager 또는 CLI를 통해 Cloud Volumes ONTAP에 연결할 수 있습니다. default_admin_user 이름을 유지하거나 사용자 지정 사용자 이름으로 변경합니다.
자격 증명 편집	이 Cloud Volumes ONTAP 시스템에서 사용할 다른 Azure 자격 증명과 다른 Azure 구독을 선택할 수 있습니다. 선불 종량제 Cloud Volumes ONTAP 시스템을 배포하려면 Azure 마켓플레이스 구독을 선택한 Azure 구독과 연결해야 합니다. " <a href="#">자격 증명을 추가하는 방법에 대해 알아보십시오</a> ".

다음 비디오에서는 마켓플레이스 구독을 Azure 구독에 연결하는 방법을 보여 줍니다.

▶ [https://docs.netapp.com/ko-kr/test//media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/ko-kr/test//media/video_subscribing_azure.mp4) (video)

5. \* 서비스 \*: Cloud Volumes ONTAP에서 사용하지 않을 개별 서비스를 활성화 또는 비활성화합니다.
  - "[BlueXP 분류에 대해 자세히 알아보십시오](#)"
  - "[BlueXP 백업 및 복구에 대해 자세히 알아보십시오](#)"



WORM 및 데이터 계층화를 사용하려면 BlueXP 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 작업 환경을 구축해야 합니다.


6. \* HA 구축 모델 \*:
  - a. 단일 가용성 영역 \* 또는 \* 다중 가용성 영역 \* 을 선택합니다.
  - b. \* 위치 및 연결 \* (단일 AZ) 및 \* 지역 및 연결 \* (다중 AZs)

- 단일 AZ의 경우 지역, VNET 및 서브넷을 선택합니다.
- 여러 AZs의 경우 노드 1의 영역, VNET, 서브넷, 영역 및 노드 2의 영역을 선택합니다.

c. 네트워크 연결을 확인했습니다. \* 확인란을 선택합니다.

7. \* 연결 \*: 새 리소스 그룹 또는 기존 리소스 그룹을 선택한 다음 미리 정의된 보안 그룹을 사용할지 아니면 직접 사용할 것인지 선택합니다.

다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
리소스 그룹	<p>Cloud Volumes ONTAP에 대한 새 리소스 그룹을 만들거나 기존 리소스 그룹을 사용합니다. 모범 사례는 Cloud Volumes ONTAP에 대한 새로운 전용 리소스 그룹을 사용하는 것입니다. 기존 공유 리소스 그룹에 Cloud Volumes ONTAP를 배포할 수는 있지만 데이터 손실 위험 때문에 권장되지 않습니다. 자세한 내용은 위의 경고를 참조하십시오.</p> <p>Azure에 구축하는 각 Cloud Volumes ONTAP HA 쌍에 대해 전용 리소스 그룹을 사용해야 합니다. 리소스 그룹에서는 하나의 HA 쌍만 지원됩니다. Azure 리소스 그룹에 두 번째 Cloud Volumes ONTAP HA 쌍을 배포하려고 하면 BlueXP에서 연결 문제가 발생합니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>사용 중인 Azure 계정에 가 있는 경우 "필수 권한", BlueXP는 배포 실패 또는 삭제 시 리소스 그룹에서 Cloud Volumes ONTAP 리소스를 제거합니다.</p> </div>
보안 그룹을 생성했습니다	<p>BlueXP에서 보안 그룹을 생성하도록 하면 트래픽을 허용하는 방법을 선택해야 합니다.</p> <ul style="list-style-type: none"> <li>• 선택한 VNET만 * 을 선택한 경우 인바운드 트래픽의 소스는 선택한 VNET의 서브넷 범위와 커넥터가 상주하는 VNET의 서브넷 범위입니다. 이 옵션을 선택하는 것이 좋습니다.</li> <li>• All VNets * 를 선택한 경우 인바운드 트래픽의 소스는 0.0.0.0/0 IP 범위입니다.</li> </ul>
기존 항목 사용	<p>기존 보안 그룹을 선택하는 경우 Cloud Volumes ONTAP 요구 사항을 충족해야 합니다. "기본 보안 그룹을 봅니다".</p>

8. \* 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".

9. 사전 구성된 패키지 \*: Cloud Volumes ONTAP 시스템을 신속하게 배포하려면 패키지 중 하나를 선택하거나 \* 구성 변경 \* 을 클릭합니다.

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

10. \* 라이선스 \*: 필요에 따라 Cloud Volumes ONTAP 버전을 변경하고 가상 머신 유형을 선택합니다.



선택한 버전에 대해 최신 출시 후보, 일반 가용성 또는 패치 릴리스를 사용할 수 있는 경우 BlueXP는 작업 환경을 만들 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).

11. \* Azure Marketplace \* 구독: BlueXP가 Cloud Volumes ONTAP의 프로그래밍 방식 배포를 활성화할 수 없는 경우 다음 단계를 따르십시오.
12. \* 기본 스토리지 리소스 \*: 초기 애그리게이트의 설정(디스크 유형, 각 디스크의 크기, Blob 스토리지까지 데이터 계층화 활성화 여부)을 선택합니다.

다음 사항에 유의하십시오.

- 디스크 크기는 초기 애그리게이트의 모든 디스크와 간단한 프로비저닝 옵션을 사용할 때 BlueXP가 생성하는 추가 애그리게이트에서 사용됩니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.

디스크 크기 선택에 대한 도움말은 를 참조하십시오 "[Azure에서 시스템 크기 조정](#)".

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

["데이터 계층화에 대해 자세히 알아보십시오"](#).

13. \* 쓰기 속도 및 WORM \*:

- a. 필요한 경우 \* Normal \* (정상 \*) 또는 \* High \* (높음 \*) 쓰기 속도를 선택합니다.

["쓰기 속도에 대해 자세히 알아보십시오"](#).

- b. 필요한 경우 WORM(Write Once, Read Many) 스토리지를 활성화합니다.

이 옵션은 특정 VM 유형에만 사용할 수 있습니다. 지원되는 VM 유형에 대한 자세한 내용은 을 참조하십시오 "[HA Pair에 대한 라이선스에서 지원되는 구성](#)".

Cloud Volumes ONTAP 9.7 이하 버전에서 데이터 계층화가 활성화된 경우 WORM을 사용할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로의 되돌리기 또는 다운그레이드가 차단됩니다.

["WORM 스토리지에 대해 자세히 알아보십시오"](#).

- a. WORM 스토리지를 활성화한 경우 보존 기간을 선택합니다.

14. \* 스토리지와 WORM \* 에 대한 보안 통신: Azure 스토리지 계정에 대한 HTTPS 연결을 사용하도록 설정하고 필요한 경우 WORM(Write Once, Read Many) 스토리지를 활성화할지 여부를 선택합니다.

HTTPS 연결은 Cloud Volumes ONTAP 9.7 HA 쌍에서 Azure 페이지 blob 저장소 계정에 연결됩니다. 이 옵션을 설정하면 쓰기 성능에 영향을 줄 수 있습니다. 작업 환경을 만든 후에는 설정을 변경할 수 없습니다.

["WORM 스토리지에 대해 자세히 알아보십시오"](#).

데이터 계층화가 설정된 경우 WORM을 설정할 수 없습니다.

"WORM 스토리지에 대해 자세히 알아보십시오".

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

"지원되는 클라이언트 프로토콜 및 버전에 대해 알아보십시오".

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

필드에 입력합니다	설명
크기	입력할 수 있는 최대 크기는 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 BlueXP는 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 BlueXP에서 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
<p>Volume Name: <input style="width: 200px;" type="text" value="vol"/>      Size (GB): <input style="width: 80px;" type="text" value="250"/></p> <p>Snapshot Policy: <input style="width: 300px;" type="text" value="default"/></p> <p><small>Default Policy</small></p>	<p style="text-align: center;"> <input type="radio"/> NFS      <input checked="" type="radio"/> CIFS      <input type="radio"/> iSCSI         </p> <hr/> <p>Share name: <input style="width: 150px;" type="text" value="vol_share"/>      Permissions: <input style="width: 150px;" type="text" value="Full Control"/></p> <p>Users / Groups: <input style="width: 300px;" type="text" value="engineering"/></p> <p><small>Valid users and groups separated by a semicolon</small></p>

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

필드에 입력합니다	설명
DNS 기본 및 보조 IP 주소	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
연결할 Active Directory 도메인입니다	CIFS 서버를 연결할 AD(Active Directory) 도메인의 FQDN입니다.
도메인에 가입하도록 승인된 자격 증명입니다	AD 도메인 내의 지정된 OU(조직 구성 단위)에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름 및 암호입니다.
CIFS 서버 NetBIOS 이름입니다	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 구성 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다.  Azure AD 도메인 서비스를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 * OU=ADDC 컴퓨터 * 또는 * OU=ADDC 사용자 * 를 입력해야 합니다. <a href="#">"Azure 설명서: Azure AD 도메인 서비스 관리 도메인에 OU(조직 구성 단위)를 만듭니다"</a>
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="#">"BlueXP 자동화 문서"</a> 를 참조하십시오.  CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 생성한 후에는 구성할 수 없습니다.

17. \* 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 프로필을 선택합니다"](#) 및 ["데이터 계층화 개요"](#).



18. \* 검토 및 승인 \*: 선택 사항을 검토 및 확인합니다.

- a. 구성에 대한 세부 정보를 검토합니다.
- b. BlueXP가 구매할 지원 및 Azure 리소스에 대한 세부 정보를 검토하려면 \* 추가 정보 \* 를 클릭합니다.
- c. 이해함... \* 확인란을 선택합니다.
- d. Go \* 를 클릭합니다.

결과

BlueXP는 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.

## Google Cloud에서 시작하십시오

Google Cloud에서 **Cloud Volumes ONTAP**를 빠르게 시작합니다

몇 가지 단계로 Cloud Volumes ONTAP for Google Cloud를 시작하십시오.

1

커넥터를 작성합니다

가 없는 경우 ["커넥터"](#) 그러나 계정 관리자는 계정을 만들어야 합니다. ["Google Cloud에서 Connector를 만드는 방법을 알아보십시오"](#)

인터넷에 액세스할 수 없는 서버넷에 Cloud Volumes ONTAP를 배포하려는 경우 수동으로 커넥터를 설치하고 해당 커넥터에서 실행 중인 BlueXP 사용자 인터페이스에 액세스해야 합니다. ["인터넷에 액세스하지 않고 커넥터에 수동으로 설치하는 방법에 대해 알아보십시오"](#)

2

구성을 계획합니다

BlueXP는 워크로드 요구 사항에 맞는 사전 구성된 패키지를 제공하거나 사용자가 직접 구성할 수 있습니다. 자신의 구성을 선택하는 경우 사용 가능한 옵션을 이해해야 합니다.

["구성 계획에 대해 자세히 알아보십시오"](#).

3

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. NetApp AutoSupport용 VPC 타겟으로부터 아웃바운드 인터넷 액세스 지원

인터넷에 액세스할 수 없는 위치에 Cloud Volumes ONTAP를 배포하는 경우에는 이 단계가 필요하지 않습니다.

"네트워킹 요구 사항에 대해 자세히 알아보십시오".

## 4

서비스 계정을 설정합니다

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 "[BlueXP 백업 및 복구](#)" 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](#)".

## 5

Google Cloud API를 활성화합니다

"[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

## 6

BlueXP를 사용하여 Cloud Volumes ONTAP를 실행합니다

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

관련 링크

- "[BlueXP에서 커넥터 만들기](#)"
- "[Linux 호스트에 Connector 소프트웨어 설치](#)"
- "[BlueXP가 Google Cloud 사용 권한으로 수행하는 기능](#)"

## 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 사용 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 BlueXP에서 시스템 용량을 관리할 수 있지만 자체적으로 집계를 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

BlueXP는 사용자 데이터를 위한 스토리지 외에도 Cloud Volumes ONTAP 시스템 데이터(부팅 데이터, 루트 데이터, 핵심 데이터 및 NVRAM)를 위한 클라우드 스토리지를 구입합니다. 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	

GCP 정보	귀사의 가치
서브넷	
방화벽 정책(자체 사용 시)	

• 여러 존의 HA 쌍에 대한 네트워크 정보 \*

GCP 정보	귀사의 가치
지역	
노드 1의 영역	
노드 2의 영역입니다	
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

BlueXP에서는 Google Cloud의 고가용성(HA) 쌍을 제외하고 Cloud Volumes ONTAP에 대한 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. BlueXP에서 볼륨을 생성할 때 이러한 기능을 활성화하는 프로필이나 해당 기능을 비활성화하는 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.

## 씬 프로비저닝

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

## 중복 제거

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

## 압축

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

## Google Cloud의 Cloud Volumes ONTAP에 대한 네트워킹 요구 사항

Cloud Volumes ONTAP 시스템이 올바르게 작동할 수 있도록 Google Cloud 네트워킹을 설정합니다.

HA 쌍을 구축하려는 경우 "[HA 쌍이 Google Cloud에서 어떻게 작동하는지를 알아보십시오](#)".

### Cloud Volumes ONTAP에 대한 요구사항

Google Cloud에서 다음 요구사항을 충족해야 합니다.

요구사항을 충족해야 합니다

단일 노드 시스템을 배포하려는 경우 네트워킹이 다음 요구 사항을 충족하는지 확인합니다.

### VPC 1개

단일 노드 시스템을 위해 VPC(가상 프라이빗 클라우드) 1개가 필요합니다.

### 전용 IP 주소

BlueXP는 Google Cloud의 단일 노드 시스템에 3개 또는 4개의 사설 IP 주소를 할당합니다.

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

```
skipSvmManagementLif: true
```



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

### HA 쌍 관련 요구사항

HA 쌍을 구축하려는 경우 네트워킹이 다음 요구사항을 충족하는지 확인합니다.

하나 또는 여러 개의 영역

여러 영역 또는 단일 영역에 HA 구성을 배포하여 데이터의 고가용성을 보장할 수 있습니다. HA 쌍을 생성할 때

BlueXP에서 여러 존 또는 단일 존을 선택하라는 메시지가 표시됩니다.

- 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.

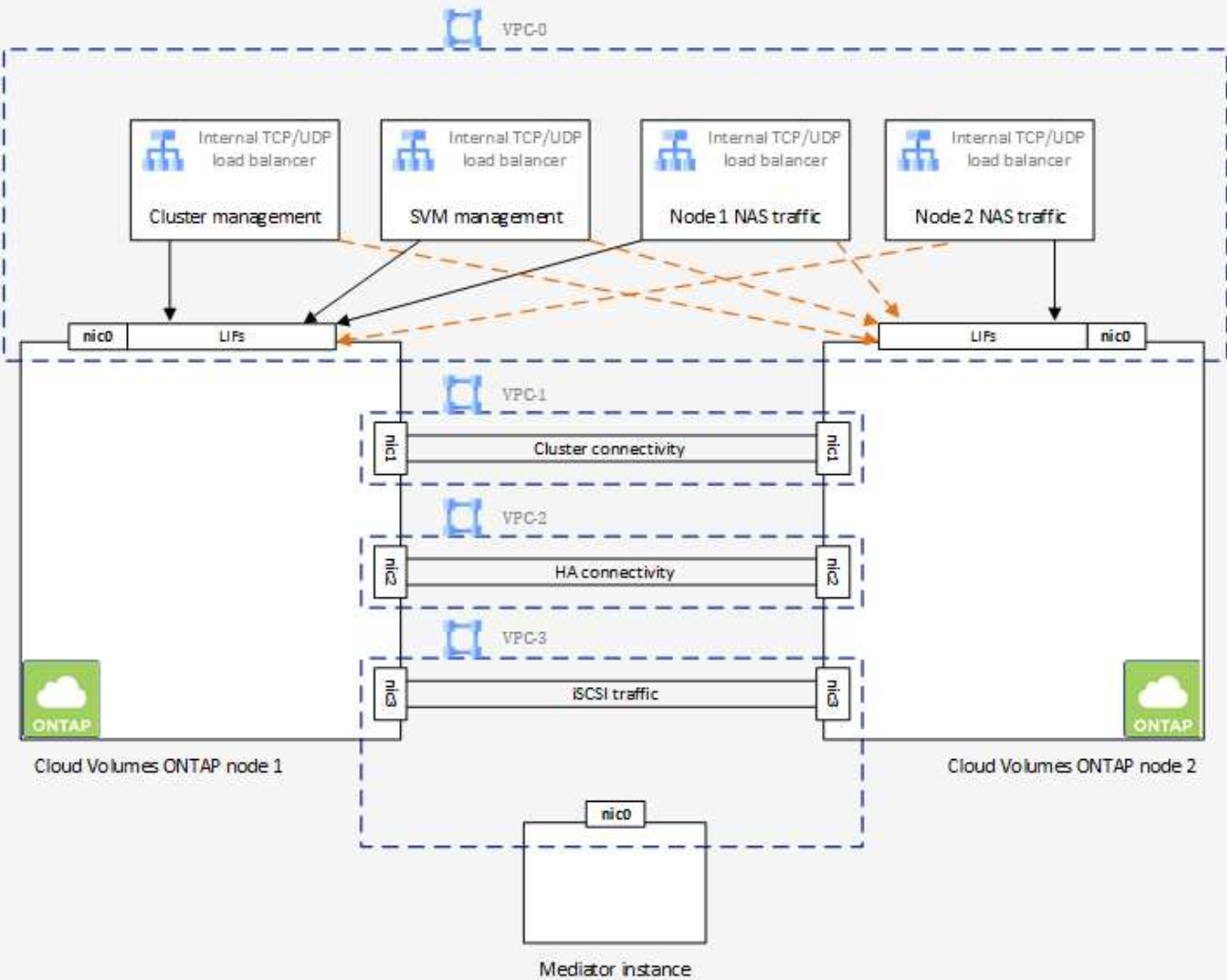
이 구축 모델은 구역 간 데이터 유출 비용이 없으므로 비용이 절감됩니다.

#### 4개의 가상 프라이빗 클라우드

HA 구성을 위해서는 4개의 가상 프라이빗 클라우드(VPC)가 필요합니다. Google Cloud에서는 각 네트워크 인터페이스가 별도의 VPC 네트워크에 상주해야 하므로 4대의 VPC가 필요합니다.

HA 쌍을 생성할 때 BlueXP에서 네 개의 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



## 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.

## 전용 IP 주소

BlueXP는 필요한 수의 사설 IP 주소를 Google Cloud의 Cloud Volumes ONTAP에 자동으로 할당합니다. 네트워킹에 사용 가능한 개인 주소가 충분한지 확인해야 합니다.

BlueXP에서 Cloud Volumes ONTAP에 할당하는 LIF 수는 단일 노드 시스템을 배포할지 HA 쌍을 구축하는지에 따라 달라집니다. LIF는 물리적 포트와 연결된 IP 주소입니다. SnapCenter와 같은 관리 툴을 사용하려면 SVM 관리 LIF가 필요합니다.

- \* 단일 노드 \*  
BlueXP는 단일 노드 시스템에 4개의 IP 주소를 할당합니다.



- 노드 관리 LIF
- 클러스터 관리 LIF
- iSCSI 데이터 LIF



iSCSI LIF는 iSCSI 프로토콜을 통해 클라이언트에 액세스할 수 있도록 지원하며 시스템에서 다른 중요한 네트워킹 워크플로우에 사용됩니다. 이러한 LIF는 필수 항목이므로 삭제할 수 없습니다.

- NAS LIF

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

```
skipSvmManagementLif: true
```

• \* HA 쌍 \*

BlueXP는 HA 쌍에 12~13개의 IP 주소를 할당:

- 노드 관리 LIF 2개(e0a)
- 클러스터 관리 LIF 1개(e0a)
- iSCSI LIF 2개(e0a)



iSCSI LIF는 iSCSI 프로토콜을 통해 클라이언트에 액세스할 수 있도록 지원하며 시스템에서 다른 중요한 네트워킹 워크플로우에 사용됩니다. 이러한 LIF는 필수 항목이므로 삭제할 수 없습니다.

- 1~2개의 NAS LIF(e0a)
- 클러스터 LIF 2개(e0b)
- HA 인터커넥트 IP 주소 2개(e0c)
- RSM iSCSI IP 주소(e0d) 2개

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

```
skipSvmManagementLif: true
```

### 내부 로드 밸런서

BlueXP는 들어오는 트래픽을 Cloud Volumes ONTAP HA 쌍으로 관리하는 4개의 Google 클라우드 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
- 하나의 지역 UDP 백엔드 서비스입니다
- 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.

## 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.

## 아웃바운드 인터넷 액세스

Cloud Volumes ONTAP를 사용하려면 NetApp AutoSupport에 대한 아웃바운드 인터넷 액세스가 필요합니다. 사전 예방적으로 시스템의 상태를 모니터링하고 메시지를 NetApp 기술 지원으로 보냅니다.

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>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

AutoSupport 메시지를 보내는 데 아웃바운드 인터넷 연결을 사용할 수 없는 경우 BlueXP는 자동으로 Cloud Volumes ONTAP 시스템에서 커넥터를 프록시 서버로 사용하도록 구성합니다. 유일한 요구 사항은 커넥터의 방화벽이 포트 3128을 통한 `_INbound_connection`을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

Cloud Volumes ONTAP에 대해 엄격한 아웃바운드 규칙을 정의한 경우 Cloud Volumes ONTAP 방화벽에서 포트 3128을 통한 `_outbound_connection`을 허용하는지 확인해야 합니다.

아웃바운드 인터넷 액세스가 가능한지 확인한 후 AutoSupport를 테스트하여 메시지를 보낼 수 있는지 확인할 수 있습니다. 자세한 지침은 을 참조하십시오 "[ONTAP 문서: AutoSupport 설정](#)".



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

BlueXP에서 AutoSupport 메시지를 보낼 수 없다고 알리는 경우 "[AutoSupport 구성 문제를 해결합니다](#)".

#### 방화벽 규칙

BlueXP는 방화벽 규칙을 만들 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](#).

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](#)".

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

#### 다른 네트워크의 ONTAP 시스템에 대한 연결

Google Cloud의 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](#)".

#### 방화벽 규칙

BlueXP는 Cloud Volumes ONTAP가 성공적으로 운영하는 데 필요한 인바운드 및 아웃바운드 규칙을 포함하는 Google Cloud 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.

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.
- 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](#).



커넥터에 대한 정보를 찾고 계십니까? "[Connector의 방화벽 규칙을 봅니다](#)"

## 인바운드 규칙

작업 환경을 만들 때 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 [을 참조하십시오 "Google Cloud 설명서: 부하 분산 방화벽 규칙"](#).

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 커넥터 및 HTTPS 액세스와의 연결
SSH를 클릭합니다	22	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다
TCP	111	NFS에 대한 원격 프로시저 호출
TCP	139	CIFS에 대한 NetBIOS 서비스 세션입니다
TCP	161-162	단순한 네트워크 관리 프로토콜
TCP	445	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
TCP	635	NFS 마운트
TCP	749	Kerberos
TCP	2049년	NFS 서버 데몬
TCP	3260입니다	iSCSI 데이터 LIF를 통한 iSCSI 액세스
TCP	4045로 문의하십시오	NFS 잠금 데몬
TCP	4046으로 문의하십시오	NFS에 대한 네트워크 상태 모니터
TCP	10000	NDMP를 사용한 백업
TCP	11104를 참조하십시오	SnapMirror에 대한 인터클러스터 통신 세션의 관리

프로토콜	포트	목적
TCP	11105를 참조하십시오	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	2049년	NFS 서버 데몬
UDP입니다	4045로 문의하십시오	NFS 잠금 데몬
UDP입니다	4046으로 문의하십시오	NFS에 대한 네트워크 상태 모니터
UDP입니다	4049입니다	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	88을 참조 하십시오	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니 다	137 입니 다	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	88을 참조 하십시오	데이터 LIF(NFS, CIFS, iSCSI)	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니 다	137 입니 다	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)
	TCP	3128	노드 관리 LIF	커넥터	아웃바운드 인터넷 연결을 사용할 수 없는 경우 커넥터의 프록시 서버를 통해 AutoSupport 메시지 보내기
클러스터	모든 교통 정보	모든 교통 정보	모든 LIF가 하나의 노드에 있습니다	다른 노드의 모든 LIF	인터클러스터 통신(Cloud Volumes ONTAP HA에만 해당)
구성 백업	HTTP	80	노드 관리 LIF	http://<connector-IP-address>/occm/offboxconfig입니다	Connector로 구성 백업을 보냅니다. "구성 백업 파일에 대해 자세히 알아보십시오".
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	11104를 참조하십시오	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror에 대한 인터클러스터 통신 세션의 관리
	TCP	11105를 참조하십시오	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-3에 대한 규칙

Google Cloud에서는 4개의 VPC에 HA 구성이 배포됩니다. VPC-0의 HA 구성에 필요한 방화벽 규칙은 [입니디 Cloud Volumes ONTAP에 대해 위에 나열되어 있습니다.](#)

한편, BlueXP가 VPC-1, VPC-2 및 VPC-3의 인스턴스에 대해 생성하는 사전 정의된 방화벽 규칙은 `_ALL_PROTOCOLS` 및 포트를 통한 수신 통신을 가능하게 합니다. 이 규칙은 HA 노드 간 통신을 지원합니다.

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



새로운 Google Cloud HA 쌍 구축에 빠른 쓰기 속도를 사용하려면 VPC-1, VPC-2 및 VPC-3에 최소 8,896바이트의 최대 전송 단위(MTU)가 필요합니다. 기존 VPC-1, VPC-2 및 VPC-3을 MTU가 8,896바이트인 경우 구성 프로세스 중에 이러한 VPC를 사용하여 모든 기존 HA 시스템을 종료해야 합니다.

## 커넥터 요구 사항

아직 Connector를 만들지 않은 경우 Connector에 대한 네트워킹 요구 사항도 검토해야 합니다.

- "[커넥터에 대한 네트워킹 요구 사항을 봅니다](#)"
- "[Google Cloud의 방화벽 규칙](#)"

## GCP에서 VPC 서비스 제어 계획

VPC 서비스 제어를 통해 Google 클라우드 환경을 잠그도록 선택할 때는 BlueXP 및 Cloud Volumes ONTAP이 Google 클라우드 API와 상호 작용하는 방식과 BlueXP 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

BlueXP는 Google Cloud API와 직접 통신합니다. 이 문제는 Google Cloud 외부의 외부 IP 주소(예: `api.services.cloud.netapp.com`) 또는 BlueXP Connector에 할당된 내부 주소에서 Google Cloud 내부에서 발생합니다.

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

## 이미지

Cloud Volumes ONTAP와 BlueXP는 모두 NetApp에서 관리하는 GCP 내 프로젝트의 이미지를 사용합니다. 조직 내에서 호스팅되지 않은 이미지의 사용을 차단하는 정책이 조직에 있는 경우 BlueXP Connector 및 Cloud Volumes ONTAP의 배포에 영향을 줄 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

- BlueXP 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.

BlueXP에 필요한 정책을 설정하려면 조직 내의 VPC 서비스 제어 경계 로 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
```

송신 규칙

```
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

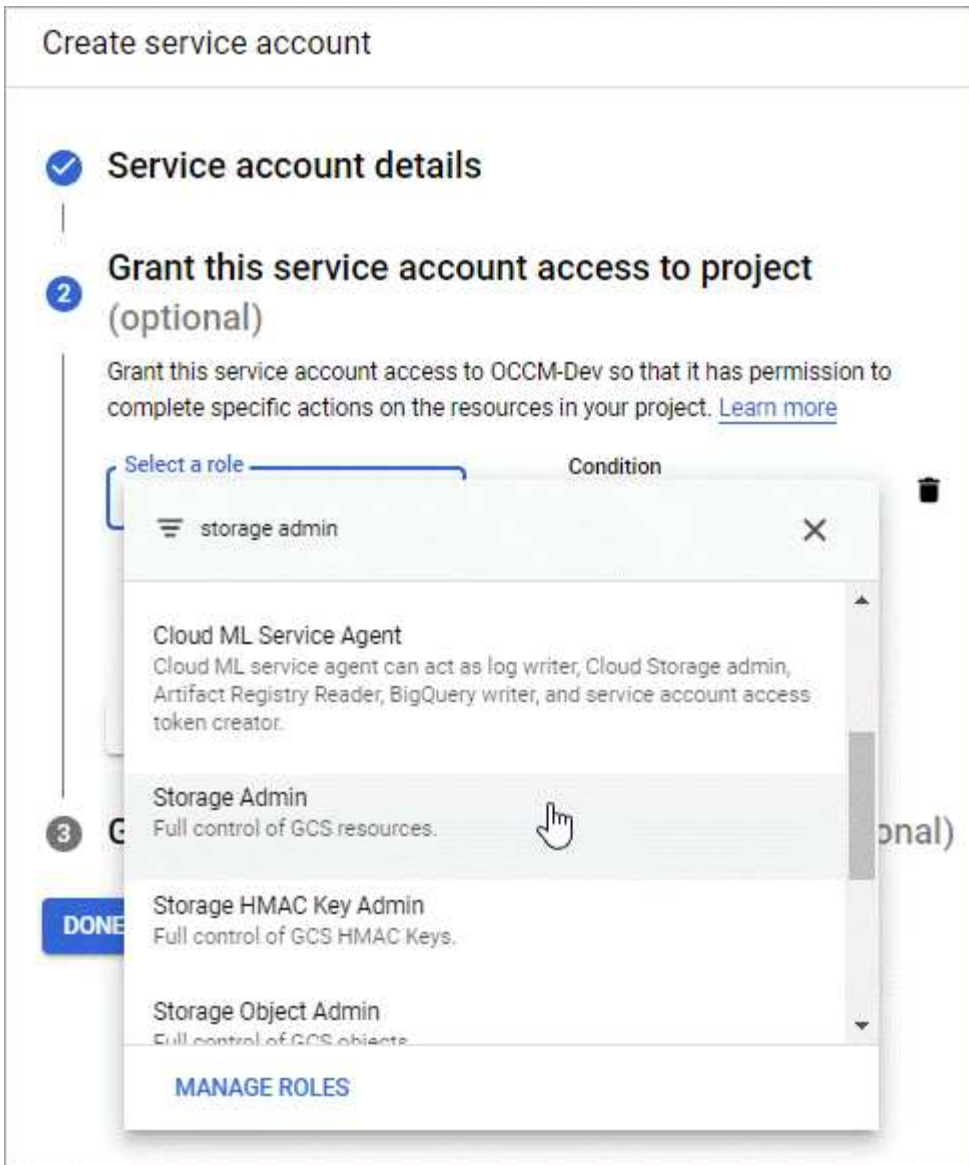
Cloud Volumes ONTAP를 사용하려면 Google Cloud 서비스 계정이 두 가지 용도로 필요합니다. 첫 번째는 를 활성화하는 것입니다 **"데이터 계층화"** Google Cloud에서 콜드 데이터를 저비용 오브젝트 스토리지로 계층화합니다. 두 번째는 를 활성화하는 것입니다 **"BlueXP 백업 및 복구"** 볼륨을 저렴한 오브젝트 스토리지에 백업

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. BlueXP 백업 및 복구에는 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

다음 단계

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

## Details and Credentials

<b>default-project</b> Google Cloud Project	<b>gcp-sub2</b> Marketplace Subscription	<a href="#">Edit Project</a>
--	---	------------------------------

### 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 BlueXP API를 사용하여 고객이 관리하는 암호화 키를 사용하는 Cloud Volumes ONTAP 시스템을 만들 수 있습니다. 클라우드 키 관리 서비스를 사용하여 GCP에서 생성하고 관리하는 키입니다.

단계

1. BlueXP Connector 서비스 계정의 프로젝트 수준에서 키가 저장된 프로젝트에 대한 올바른 권한이 있는지 확인합니다.

사용 권한은 에 제공됩니다 **"기본적으로 커넥터 서비스 계정 권한이 있습니다"**, 그러나 클라우드 키 관리 서비스에 대체 프로젝트를 사용하는 경우에는 적용되지 않을 수 있습니다.

사용 권한은 다음과 같습니다.

- `cloudkms.cryptoKeyVersions.useToEncrypt`
- `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"

- 에 대한 get 명령을 호출하여 키의 "id"를 가져옵니다 /gcp/vsa/metadata/gcp-encryption-keys API를 호출하거나 GCP 콘솔의 키에서 "Copy Resource Name"을 선택합니다.
- 고객이 관리하는 암호화 키를 사용하고 데이터를 오브젝트 스토리지에 계층화하는 경우 BlueXP는 영구 디스크를 암호화하는 데 사용되는 동일한 키를 사용하려고 합니다. 하지만 먼저 Google Cloud Storage 버킷을 활성화하여 키를 사용해야 합니다.
  - 에 따라 Google Cloud Storage 서비스 에이전트를 찾습니다 "[Google Cloud 설명서: 클라우드 스토리지 서비스 에이전트 얻기](#)".
  - 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](#)"

- 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 "[BlueXP 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

- 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
- Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 BlueXP의 단계를 따릅니다.
  - 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. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 \* Freemium \* 을 선택합니다.

Select Charging Method		
<input type="radio"/>	Professional	By capacity
<input type="radio"/>	Essential	By capacity
<input checked="" 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".

#### 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. "NetApp Support 사이트 계정을 BlueXP에 추가합니다"

BlueXP는 NetApp의 라이선스 서비스에 자동으로 쿼리하여 NetApp Support 사이트 계정과 관련된 라이선스에 대한 자세한 정보를 확인합니다. 오류가 없으면 BlueXP는 자동으로 디지털 지갑에 라이선스를 추가합니다.

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

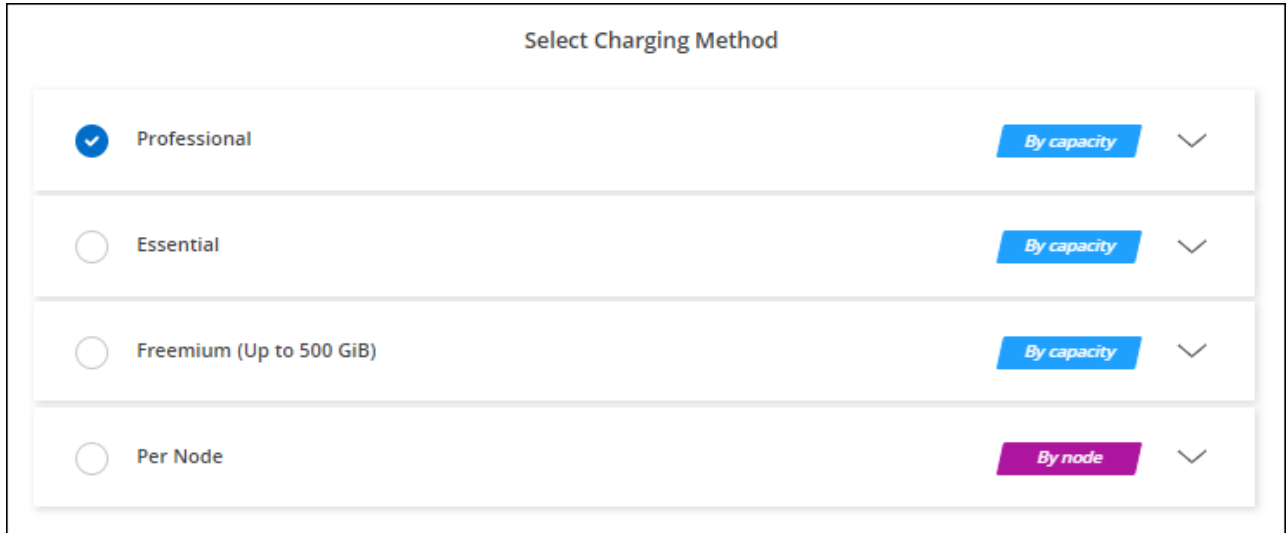
3. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 BlueXP의 단계를 따릅니다.



- 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. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 용량 기반 패키지를 선택합니다.



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

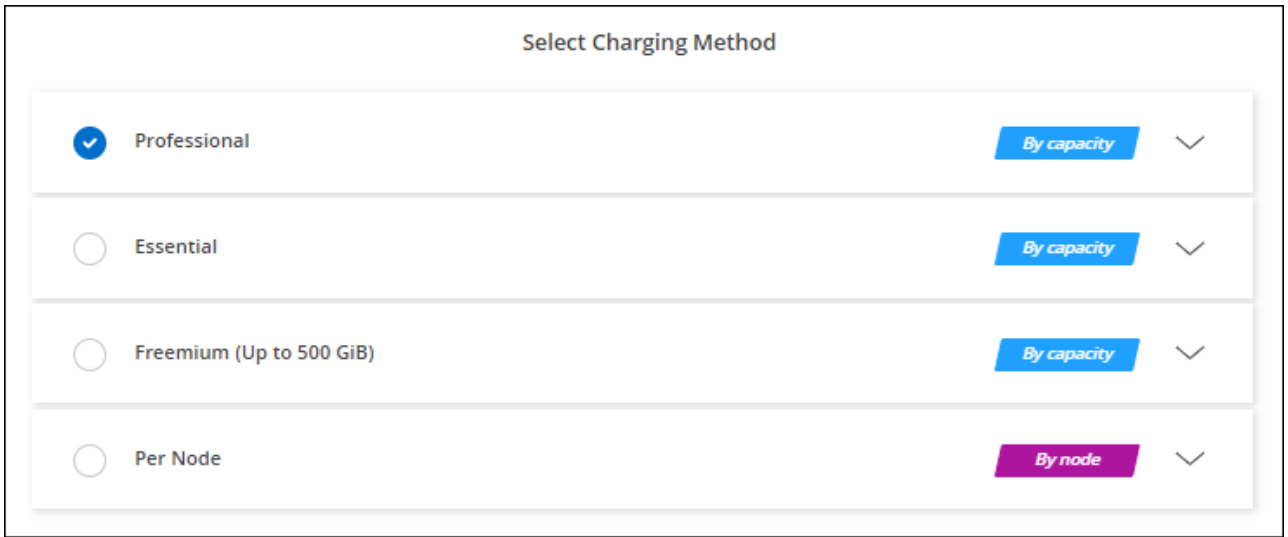
#### PAYGO 구독

클라우드 공급자 마켓플레이스의 서비스에 가입하여 시간별 비용 지불

Cloud Volumes ONTAP 작업 환경을 만들 때 BlueXP는 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. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 BlueXP의 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. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 용량 기반 패키지를 선택합니다.



"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 BlueXP의 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. BlueXP로 돌아온 후 충전 방법 페이지에 도달하면 용량 기반 패키지를 선택합니다.

Select Charging Method

<input checked="" type="radio"/>	Professional	By capacity <span style="font-size: 0.8em;">▼</span>
<input type="radio"/>	Essential	By capacity <span style="font-size: 0.8em;">▼</span>
<input type="radio"/>	Freemium (Up to 500 GiB)	By capacity <span style="font-size: 0.8em;">▼</span>
<input type="radio"/>	Per Node	By node <span style="font-size: 0.8em;">▼</span>

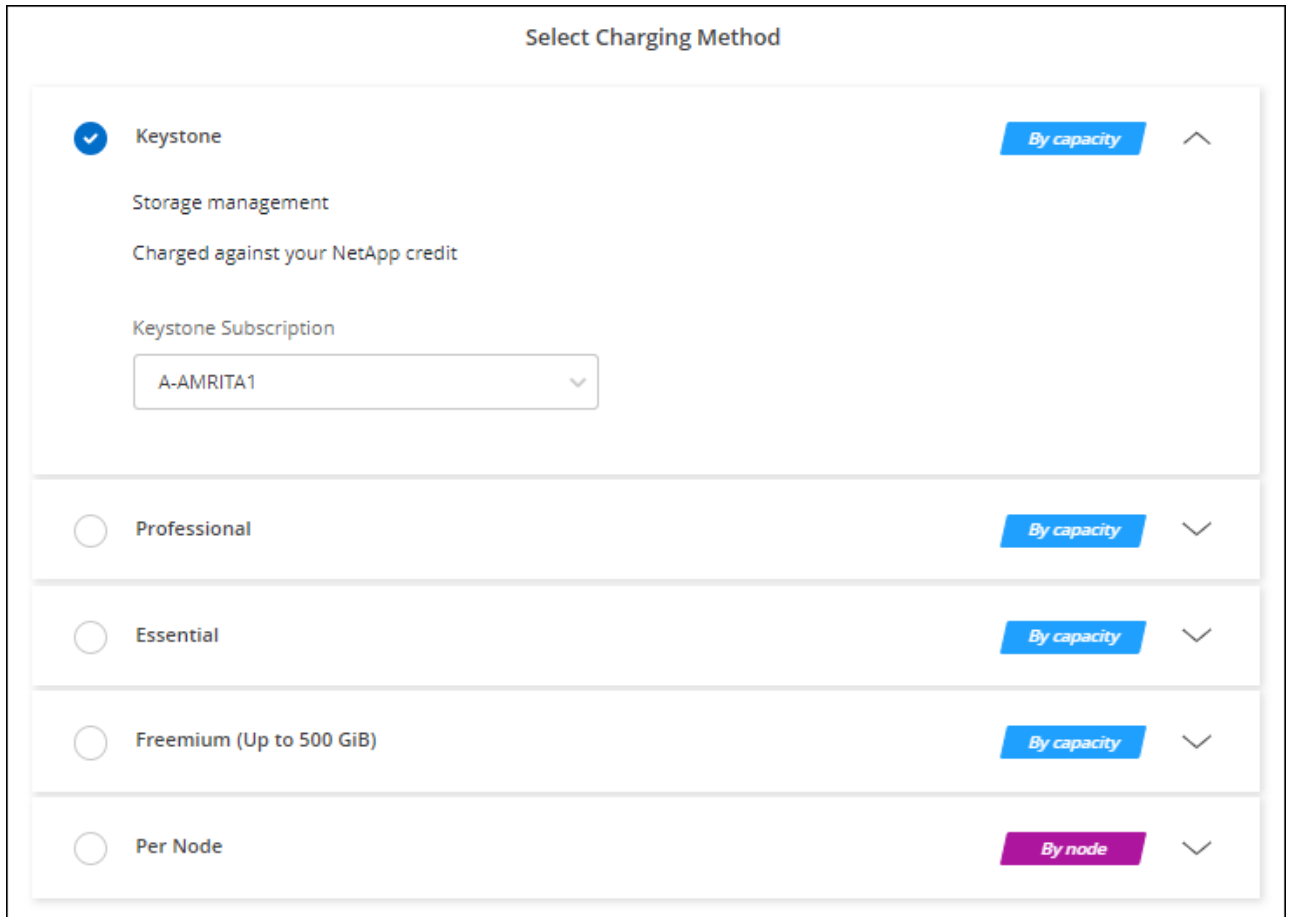
"Google Cloud에서 Cloud Volumes ONTAP를 실행하기 위한 단계별 지침을 확인하십시오".

### Keystone 구독

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

#### 단계

1. 아직 구독이 없는 경우 "[NetApp에 문의하십시오](#)"
2. <mailto:ng-keystone-success@netapp.com> [NetApp에 문의]하여 하나 이상의 Keystone 구독으로 BlueXP 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 BlueXP의 단계를 따릅니다.
  - a. 충전 방법을 선택하라는 메시지가 표시되면 Keystone 가입 충전 방법을 선택합니다.



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

## Google Cloud에서 Cloud Volumes ONTAP 실행

단일 노드 구성에서 Cloud Volumes ONTAP를 실행하거나 Google Cloud에서 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 "필요한 권한이 있어야 합니다"
- 사용하려는 구성에 대한 이해.

구성을 선택하고 관리자로부터 Google Cloud 네트워크 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 API는 입니다 "프로젝트에서 활성화됩니다":
  - Cloud Deployment Manager V2 API
  - 클라우드 로깅 API
  - Cloud Resource Manager API를 참조하십시오
  - 컴퓨팅 엔진 API
  - IAM(Identity and Access Management) API

## Google Cloud에서 단일 노드 시스템 실행


BlueXP에서 작업 환경을 만들어 Google Cloud에서 Cloud Volumes ONTAP를 실행합니다.

단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 화면의 지시를 따릅니다.
3. \* 위치 선택 \*: \* Google Cloud \* 및 \* Cloud Volumes ONTAP \* 를 선택합니다.
4. 메시지가 표시되면 "커넥터를 작성합니다".
5. \* 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	BlueXP는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Google Cloud VM 인스턴스 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.
서비스 계정 이름입니다	를 사용할 계획인 경우 "데이터 계층화" 또는 "BlueXP 백업 및 복구" Cloud Volumes ONTAP를 사용하는 경우 * 서비스 계정 * 을 활성화하고 사전 정의된 스토리지 관리 역할이 있는 서비스 계정을 선택해야 합니다. "서비스 계정을 만드는 방법에 대해 알아보십시오".
레이블 추가	레이블은 Google Cloud 리소스의 메타데이터입니다. BlueXP는 시스템에 연결된 Cloud Volumes ONTAP 시스템 및 Google Cloud 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.

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

다음 비디오에서는 선불 종량제 마켓플레이스 구독을 Google Cloud 프로젝트에 연결하는 방법을 보여 줍니다. 또는 에 있는 구독 단계를 따릅니다 "[Google Cloud 자격 증명과 마켓플레이스 가입 연결](#)" 섹션을 참조하십시오.

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

6. \* 서비스 \*: 이 시스템에서 사용할 서비스를 선택합니다. BlueXP 백업 및 복구를 선택하거나 BlueXP 계층화를 사용하려면 3단계에서 서비스 계정을 지정해야 합니다.



WORM 및 데이터 계층화를 사용하려면 BlueXP 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 작업 환경을 구축해야 합니다.

7. \* 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	<p>콜드 데이터를 Google 클라우드 스토리지 버킷에 계층화하려면 Cloud Volumes ONTAP가 상주하는 서브넷을 프라이빗 Google 액세스용으로 구성해야 합니다. 자세한 지침은 을 참조하십시오 "<a href="#">Google Cloud 설명서: 개인 Google Access 구성</a>".</p>
방화벽 정책을 생성했습니다	<p>BlueXP에서 방화벽 정책을 생성하도록 허용할 경우 트래픽을 허용하는 방법을 선택해야 합니다.</p> <ul style="list-style-type: none"> <li>• 선택한 VPC 전용 * 을 선택한 경우 인바운드 트래픽에 대한 소스 필터는 선택한 VPC의 서브넷 범위와 커넥터가 있는 VPC의 서브넷 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>

필드에 입력합니다	설명
기존 방화벽 정책을 사용합니다	기존 방화벽 정책을 사용하는 경우 필수 규칙이 포함되어 있는지 확인합니다. 링크: <a href="#">Learn Cloud Volumes ONTAP의 방화벽 규칙 정보</a> .

8. \* 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](#)".

9. \* 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.

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



선택한 버전에 대해 최신 출시 후보, 일반 가용성 또는 패치 릴리스를 사용할 수 있는 경우 BlueXP는 작업 환경을 만들 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).

11. \* 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 간단한 프로비저닝 옵션을 사용할 때 BlueXP가 생성하는 추가 애그리게이트에서 사용됩니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.

디스크 유형과 크기를 선택하는 방법은 을 참조하십시오 "[Google Cloud에서 시스템 크기를 조정합니다](#)".

12. \* Flash Cache, 쓰기 속도 및 WORM \*:

a. 필요한 경우 \* Flash Cache \* 를 활성화합니다.



Cloud Volumes ONTAP 9.13.1 부터, `_Flash Cache_` 는 n2-standard-16, n2-standard-32, n2-standard-48, n2-standard-64 인스턴스 유형에서 지원됩니다. 구축 후에는 Flash Cache를 사용하지 않도록 설정할 수 없습니다.

b. 필요한 경우 \* Normal \* (정상 \*) 또는 \* High \* (높음 \*) 쓰기 속도를 선택합니다.

"[쓰기 속도에 대해 자세히 알아보십시오](#)".



고속 \* 쓰기 속도 옵션을 통해 896바이트의 고속 쓰기 속도와 높은 최대 전송 단위(MTU)를 사용할 수 있습니다. 또한, 8,896의 MTU가 높을수록 구축을 위해 VPC-1, VPC-2 및 VPC-3을 선택해야 합니다. VPC-1, VPC-2 및 VPC-3에 대한 자세한 내용은 을 참조하십시오 "[VPC-1, VPC-2 및 VPC-3에 대한 규칙](#)".

c. 필요한 경우 WORM(Write Once, Read Many) 스토리지를 활성화합니다.

Cloud Volumes ONTAP 9.7 이하 버전에서 데이터 계층화가 활성화된 경우 WORM을 사용할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로의 되돌리기 또는 다운그레이드가 차단됩니다.

"WORM 스토리지에 대해 자세히 알아보십시오".

a. WORM 스토리지를 활성화한 경우 보존 기간을 선택합니다.

13. \* 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 Google 클라우드 계정을 선택합니다(Cloud Volumes ONTAP 9.6의 경우 필수).

다음 사항에 유의하십시오.

- BlueXP는 Cloud Volumes ONTAP 인스턴스에 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 BlueXP에서 선택할 수 없습니다
- Google Cloud 계정 추가에 대한 도움말은 을 참조하십시오 "[9.6의 데이터 계층화를 위한 Google Cloud 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 Google Cloud 콘솔에서 서비스 계정을 추가해야 합니다.

"데이터 계층화에 대해 자세히 알아보십시오".

14. \* 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 BlueXP는 서버넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.
권한 및 사용자/그룹(CIFS 전용)	이러한 필드를 사용하면 사용자 및 그룹의 공유에 대한 액세스 수준(액세스 제어 목록 또는 ACL라고도 함)을 제어할 수 있습니다. 로컬 또는 도메인 Windows 사용자 또는 그룹, UNIX 사용자 또는 그룹을 지정할 수 있습니다. 도메인 Windows 사용자 이름을 지정하는 경우 domain\username 형식을 사용하여 사용자의 도메인을 포함해야 합니다.
스냅샷 정책	스냅샷 복사본 정책은 자동으로 생성되는 NetApp 스냅샷 복사본의 수와 빈도를 지정합니다. NetApp 스냅샷 복사본은 성능 영향이 없고 최소한의 스토리지가 필요한 시점 파일 시스템 이미지입니다. 기본 정책을 선택하거나 선택하지 않을 수 있습니다. Microsoft SQL Server의 tempdb와 같이 임시 데이터에 대해 없음을 선택할 수 있습니다.
고급 옵션(NFS에만 해당)	볼륨의 NFS 버전 선택: NFSv3 또는 NFSv4



필드에 입력합니다	설명
이니시에이터 그룹 및 IQN(iSCSI 전용)	<p>iSCSI 스토리지 타겟을 LUN(논리 유닛)이라고 하며 호스트에 표준 블록 디바이스로 표시됩니다.</p> <p>이니시에이터 그룹은 iSCSI 호스트 노드 이름의 테이블이며 어떤 이니시에이터가 어떤 LUN을 액세스할 수 있는지 제어합니다.</p> <p>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.</p> <p>iSCSI 볼륨을 생성할 때 BlueXP에서 자동으로 LUN을 생성합니다. 볼륨 당 하나의 LUN만 생성하므로 관리가 필요 없습니다. 볼륨을 생성한 후 <b>"IQN을 사용하여 호스트에서 LUN에 연결합니다"</b>.</p>

다음 이미지는 CIFS 프로토콜에 대해 작성된 볼륨 페이지를 보여 줍니다.

### Volume Details, Protection & Protocol

#### Details & Protection

Volume Name:  Size (GB):

Snapshot Policy:

Default Policy

#### Protocol

NFS     CIFS     iSCSI

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

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

필드에 입력합니다	설명
DNS 기본 및 보조 IP 주소	<p>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.</p> <p>Google Managed Active Directory를 구성하는 경우 기본적으로 169.254.169.254 IP 주소를 사용하여 AD에 액세스할 수 있습니다.</p>
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.

필드에 입력합니다	설명
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="#">Google 클라우드 문서: Google Managed Microsoft AD의 조직 단위</a> "
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="#">BlueXP 자동화 문서</a> " 를 참조하십시오.  CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 생성한 후에는 구성할 수 없습니다.

16. \* 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 프로필을 선택합니다](#)" 및 "[데이터 계층화 개요](#)".

17. \* 검토 및 승인 \*: 선택 사항을 검토 및 확인합니다.

- 구성에 대한 세부 정보를 검토합니다.
- BlueXP가 구매할 지원 및 Google Cloud 리소스에 대한 세부 정보를 검토하려면 \* 추가 정보 \* 를 클릭합니다.
- 이해함... \* 확인란을 선택합니다.
- Go \* 를 클릭합니다.

## 결과

BlueXP는 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.

## Google Cloud에서 HA 쌍 시작

BlueXP에서 작업 환경을 만들어 Google Cloud에서 Cloud Volumes ONTAP를 실행합니다.

## 단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 화면의 지시를 따릅니다.
3. \* 위치 선택 \*: \* Google Cloud \* 및 \* Cloud Volumes ONTAP HA \* 를 선택합니다.
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	BlueXP는 작업 환경 이름을 사용하여 Cloud Volumes ONTAP 시스템과 Google Cloud VM 인스턴스 이름을 모두 지정합니다. 또한 이 옵션을 선택하면 미리 정의된 보안 그룹의 접두사로 이름이 사용됩니다.
서비스 계정 이름입니다	를 사용할 계획인 경우 "BlueXP 계층화" 또는 "BlueXP 백업 및 복구" 서비스를 사용하려면 * 서비스 계정 * 스위치를 활성화한 다음 미리 정의된 스토리지 관리자 역할이 있는 서비스 계정을 선택해야 합니다.
레이블 추가	레이블은 Google Cloud 리소스의 메타데이터입니다. BlueXP는 시스템에 연결된 Cloud Volumes ONTAP 시스템 및 Google Cloud 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 <a href="#">"Google Cloud 설명서: 라벨 리소스"</a> .
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	Cloud Volumes ONTAP가 상주할 프로젝트를 선택합니다. 기본 프로젝트는 BlueXP가 있는 프로젝트입니다.  드롭다운 목록에 추가 프로젝트가 표시되지 않으면 BlueXP 서비스 계정을 다른 프로젝트와 연결하지 않은 것입니다. Google Cloud 콘솔로 이동하여 IAM 서비스를 열고 프로젝트를 선택합니다. BlueXP 역할이 있는 서비스 계정을 해당 프로젝트에 추가합니다. 각 프로젝트에 대해 이 단계를 반복해야 합니다.   BlueXP에 대해 설정한 서비스 계정입니다. <a href="#">"이 페이지에 설명되어 있습니다"</a> .  선택한 자격 증명을 구독과 연결하려면 * 구독 추가 * 를 클릭합니다.  선불 종량제 Cloud Volumes ONTAP 시스템을 생성하려면 Google 클라우드 마켓플레이스에서 Cloud Volumes ONTAP 구독과 연결된 Google Cloud 프로젝트를 선택해야 합니다.

다음 비디오에서는 선불 종량제 마켓플레이스 구독을 Google Cloud 프로젝트에 연결하는 방법을 보여 줍니다. 또는 에 있는 구독 단계를 따릅니다 ["Google Cloud 자격 증명과 마켓플레이스 가입 연결"](#) 섹션을 참조하십시오.

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

5. \* 서비스 \*: 이 시스템에서 사용할 서비스를 선택합니다. BlueXP 백업 및 복구를 선택하거나 BlueXP 계층화를 사용하려면 3단계에서 서비스 계정을 지정해야 합니다.



WORM 및 데이터 계층화를 사용하려면 BlueXP 백업 및 복구를 비활성화하고 버전 9.8 이상의 Cloud Volumes ONTAP 작업 환경을 구축해야 합니다.

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

["HA 구축 모델 에 대해 자세히 알아보십시오"](#).

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

["네트워킹 요구 사항에 대해 자세히 알아보십시오"](#).

다음 표에서는 지침이 필요한 필드를 설명합니다.

필드에 입력합니다	설명
생성된 정책	BlueXP에서 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 서브넷 범위와 커넥터가 있는 VPC의 서브넷 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 항목 사용	기존 방화벽 정책을 사용하는 경우 필수 규칙이 포함되어 있는지 확인합니다. <a href="#">"Cloud Volumes ONTAP의 방화벽 규칙에 대해 알아보십시오"</a> .

8. \* 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"](#).

9. \* 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.

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



선택한 버전에 대해 최신 출시 후보, 일반 가용성 또는 패치 릴리스를 사용할 수 있는 경우 BlueXP는 작업 환경을 만들 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).

11. \* 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 간단한 프로비저닝 옵션을 사용할 때 BlueXP가 생성하는 추가 애그리게이트에서 사용됩니다. 고급 할당 옵션을 사용하여 다른 디스크 크기를 사용하는 애그리게이트를 생성할 수 있습니다.

디스크 유형과 크기를 선택하는 방법은 을 참조하십시오 ["Google Cloud에서 시스템 크기를 조정합니다"](#).

12. \* Flash Cache, 쓰기 속도 및 WORM \*:

- a. 필요한 경우 \* Flash Cache \* 를 활성화합니다.



Cloud Volumes ONTAP 9.13.1 부터, `_Flash Cache_` 는 n2-standard-16, n2-standard-32, n2-standard-48, n2-standard-64 인스턴스 유형에서 지원됩니다. 구축 후에는 Flash Cache를 사용하지 않도록 설정할 수 없습니다.

- b. 필요한 경우 \* Normal \* (정상 \*) 또는 \* High \* (높음 \*) 쓰기 속도를 선택합니다.

["쓰기 속도에 대해 자세히 알아보십시오"](#).



고속 쓰기 속도와 896바이트의 최대 전송 단위(MTU)는 n2-standard-16, n2-standard-32, n2-standard-48 및 n2-standard-64 인스턴스 유형의 \* 고속 \* 쓰기 속도 옵션을 통해 사용할 수 있습니다. 또한, 8,896의 MTU가 높을수록 구축을 위해 VPC-1, VPC-2 및 VPC-3을 선택해야 합니다. 높은 쓰기 속도 및 8,896의 MTU는 기능에 따라 다르며 구성된 인스턴스 내에서 개별적으로 비활성화할 수 없습니다. VPC-1, VPC-2 및 VPC-3에 대한 자세한 내용은 을 참조하십시오 ["VPC-1, VPC-2 및 VPC-3에 대한 규칙"](#).

- c. 필요한 경우 WORM(Write Once, Read Many) 스토리지를 활성화합니다.

Cloud Volumes ONTAP 9.7 이하 버전에서 데이터 계층화가 활성화된 경우 WORM을 사용할 수 없습니다. WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로의 되돌리기 또는 다운그레이드가 차단됩니다.

["WORM 스토리지에 대해 자세히 알아보십시오"](#).

- a. WORM 스토리지를 활성화한 경우 보존 기간을 선택합니다.

13. \* Google Cloud의 데이터 계층화 \*: 초기 애그리게이트에서 데이터 계층화를 사용할지 여부를 선택하고, 계층화 데이터에 대한 스토리지 클래스를 선택한 다음 사전 정의된 스토리지 관리 역할이 있는 서비스 계정을 선택합니다.

다음 사항에 유의하십시오.

- BlueXP는 Cloud Volumes ONTAP 인스턴스에 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 BlueXP에서 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 Google Cloud 콘솔에서 서비스 계정을 추가해야 합니다.

"데이터 계층화에 대해 자세히 알아보십시오".

14. \* 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 BlueXP는 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 BlueXP에서 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
<p>Volume Name: <input style="width: 200px;" type="text" value="vol"/>      Size (GB): <input style="width: 80px;" type="text" value="250"/></p> <p>Snapshot Policy: <input style="width: 300px;" type="text" value="default"/></p> <p><small>Default Policy</small></p>	<p style="text-align: center;"> <input type="radio"/> NFS      <input checked="" type="radio"/> CIFS      <input type="radio"/> iSCSI         </p> <hr/> <p>Share name: <input style="width: 150px;" type="text" value="vol_share"/>      Permissions: <input style="width: 150px;" type="text" value="Full Control"/></p> <p>Users / Groups: <input style="width: 300px;" type="text" value="engineering"/></p> <p style="font-size: small;">Valid users and groups separated by a semicolon</p>

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

필드에 입력합니다	설명
DNS 기본 및 보조 IP 주소	<p>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.</p> <p>Google Managed Active Directory를 구성하는 경우 기본적으로 169.254.169.254 IP 주소를 사용하여 AD에 액세스할 수 있습니다.</p>
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	<p>CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다.</p> <p>Google 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 * OU=Computers, OU=Cloud * 를 입력합니다.</p> <p><a href="#">"Google 클라우드 문서: Google Managed Microsoft AD의 조직 단위"</a></p>
DNS 도메인	SVM(Cloud Volumes ONTAP 스토리지 가상 머신)용 DNS 도메인 대부분의 경우 도메인은 AD 도메인과 동일합니다.
NTP 서버	<p>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="#">"BlueXP 자동화 문서"</a> 를 참조하십시오.</p> <p>CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 생성한 후에는 구성할 수 없습니다.</p>

16. \* 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 프로필을 선택합니다](#)" 및 "[데이터 계층화 개요](#)".

17. \* 검토 및 승인 \*: 선택 사항을 검토 및 확인합니다.

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

결과

BlueXP는 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.

## Google Cloud Platform 이미지 검증

### Google Cloud 이미지 검증 개요

Google Cloud 이미지 검증은 향상된 NetApp 보안 요구사항을 준수합니다. 이 작업을 위해 특별히 생성된 개인 키를 사용하여 이미지를 생성하는 스크립트가 변경되었습니다. 를 통해 다운로드할 수 있는 Google Cloud용 서명된 다이제스트 및 공용 인증서를 사용하여 GCP 이미지의 무결성을 확인할 수 있습니다 "[NSS](#)" 특정 릴리스에 대해.



Google 클라우드 이미지 확인은 Cloud Volumes ONTAP 소프트웨어 버전 9.13.0 이상에서 지원됩니다.

### Google Cloud에서 이미지를 RAW 형식으로 변환합니다

새 인스턴스 배포, 업그레이드 또는 기존 이미지에 사용 중인 이미지는 를 통해 클라이언트와 공유됩니다 "[NetApp Support 사이트\(NSS\)](#)". 서명된 다이제스트 및 인증서는 NSS 포털을 통해 다운로드할 수 있습니다. NetApp Support에서 공유하는 이미지에 해당하는 오른쪽 릴리스에 대한 다이제스트 및 인증서를 다운로드했는지 확인합니다. 예를 들어 9.13.0 이미지는 9.13.0 서명된 다이제스트와 NSS에서 사용할 수 있는 인증서를 갖습니다.



이 단계가 필요한 이유는 무엇입니까?

Google Cloud의 이미지는 직접 다운로드할 수 없습니다. 서명된 다이제스트 및 인증서와 이미지를 비교하려면 두 파일을 비교하여 이미지를 다운로드하는 메커니즘이 있어야 합니다. 이렇게 하려면 이미지를 disk.raw 형식으로 내보내기/변환하고 결과를 Google Cloud의 저장 버킷에 저장해야 합니다. disk.raw 파일이 tarred로 압축되어 있습니다.

사용자/서비스 계정에는 다음 작업을 수행할 수 있는 권한이 필요합니다.

- Google 스토리지 버킷에 액세스
- Google Storage 버킷에 쓰십시오
- 클라우드 구축 작업 생성(내보내기 프로세스 중 사용)
- 원하는 이미지에 액세스합니다
- 이미지 내보내기 작업을 만듭니다

이미지를 확인하려면 disk.raw 형식으로 변환한 다음 다운로드해야 합니다.

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

이미지를 클라우드 스토리지로 내보내는 기본 방법은 을 사용하는 것입니다 "[gcloud 계산 이미지 내보내기 명령](#)". 이 명령은 제공된 이미지를 가져와 tarred와 gzip이 되는 disk.raw 파일로 변환합니다. 생성된 파일은 대상 URL에 저장되며 확인을 위해 다운로드할 수 있습니다.

이 작업을 실행하려면 사용자/계정에 원하는 버킷에 액세스하고 쓰거나 이미지를 내보내고 Google에서 이미지를 내보낼 때 사용하는 클라우드 빌드에 액세스할 수 있는 권한이 있어야 합니다.

- gcloud \* 를 사용하여 Google Cloud 이미지를 내보냅니다

```
$ 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/xxxxxxxxxxxxx].  
Logs are available at [https://console.cloud.google.com/cloud-  
build/builds;region=us-central1/xxxxxxxxxxxxx?project=xxxxxxxxxxxxx].  
[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 압축 풀기 \*

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



을 참조하십시오 ["이미지 내보내기에 대한 Google Cloud 문서"](#) Google Cloud를 통해 이미지를 내보내는 방법에 대한 자세한 내용은

### 이미지 서명 확인

**Google Cloud** 서명 이미지를 확인합니다

내보낸 Google Cloud 서명 이미지를 확인하려면 NSS에서 이미지 다이제스트 파일을 다운로드하여 disk.raw 파일의 유효성을 검사하고 파일 내용을 다이제해야 합니다.

### 서명된 이미지 검증 워크플로 요약

다음은 Google Cloud 서명 이미지 검증 워크플로 프로세스에 대한 개요입니다.

- 에서 ["NSS"](#)에서 다음 파일이 포함된 Google Cloud 아카이브를 다운로드합니다.
  - 서명된 다이제스트(.SIG)
  - 공개 키(.pem)가 포함된 인증서
  - 인증서 체인(.pem)

**Cloud Volumes ONTAP** 9.13.0

Date Posted:

### Restrictions on Encryption Technology

NetApp Volume Encryption (available with ONTAP 9.1 and later releases) provides for data-at-rest encryption that requires authorizations, permits, or licenses to import, export, re-export or use this software.

A state license for importing encryption equipment is required to import ONTAP 9.1 (or later) with NetApp Volume Encryption into Member States of the Eurasian Economic Union: Russia, Belarus, Kazakhstan, Armenia and Kyrgyzstan. Moreover, in certain cases, an end-user customer must have a valid state encryption license to this software.

Consult your legal advisor on this matter.

**Cloud Volumes ONTAP**  
Non-Restricted Countries

If you are upgrading to ONTAP 9.13.0, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

[DOWNLOAD 9130\\_V\\_IMAGE.TGZ \[2.58 GB\]](#)

[View and download checksums](#)

[DOWNLOAD 9130\\_V\\_IMAGE.TGZ.PEM \[451 B\]](#)

[View and download checksums](#)

[DOWNLOAD 9130\\_V\\_IMAGE.TGZ.SIG \[256 B\]](#)

[View and download checksums](#)

**Cloud Volumes ONTAP**  
Restricted Countries

If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.

[DOWNLOAD 9130\\_V\\_NODAR\\_IMAGE.TGZ \[2.58 GB\]](#)

[View and download checksums](#)

[DOWNLOAD 9130\\_V\\_NODAR\\_IMAGE.TGZ.PEM \[451 B\]](#)

[View and download checksums](#)

[DOWNLOAD 9130\\_V\\_NODAR\\_IMAGE.TGZ.SIG \[256 B\]](#)

[View and download checksums](#)

**Cloud Volumes ONTAP**  
Google Image Digest Files

[DOWNLOAD GCP-X-9-13-0\\_PKG.TAR.GZ \[7.52 KB\]](#)

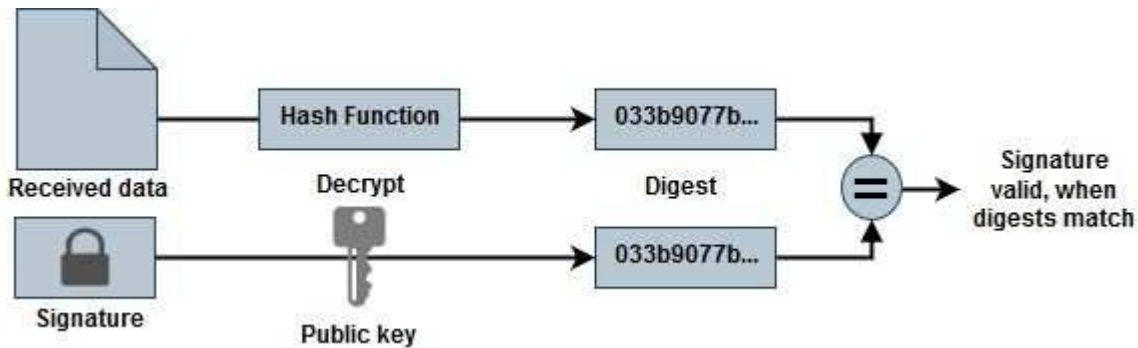
[View and download checksums](#)

Azure Image Digest File

[DOWNLOAD AZURE-9.13.0\\_PKG.TAR.GZ \[7.55 KB\]](#)

[View and download checksums](#)

- 변환된 disk.raw 파일을 다운로드합니다
- 인증서 체인을 사용하여 인증서의 유효성을 검사합니다
- 인증서에 공개 키가 포함되어 있는 서명된 다이제스트를 확인합니다
  - 공개 키를 사용하여 서명된 다이제스트를 해독하여 이미지 파일의 다이제스트를 추출합니다
  - 다운로드한 disk.raw 파일의 다이제스트를 만듭니다
  - 검증을 위해 두 개의 다이제스트 파일을 비교합니다



OpenSSL을 사용하여 disk.raw 파일 및 다이제스트 파일 내용을 확인합니다

Google Cloud에서 다운로드한 disk.raw 파일을 통해 사용 가능한 다이제스트 파일 내용과 비교하여 확인할 수 있습니다 "NSS" OpenSSL 사용.



이미지의 유효성을 검사하는 OpenSSL 명령은 Linux, Mac OS 및 Windows 시스템과 호환됩니다.

단계

1. OpenSSL을 사용하여 인증서를 확인합니다.

스크립트를 표시하려면 클릭합니다

```
# 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 OSCP request for the certificate
$ openssl ocsf -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsf -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 OSCP Manager using openssl to send the
OCSP request
$ openssl ocsf -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${oscp_url} -resp_text
-respout <response.der>
```



```
$ openssl ocspl -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: CE894F8251AA15A28462CA312361D261F8F8FE78

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 및 인증서를 디렉터리에 넣습니다.
3. OpenSSL을 사용하여 인증서에서 공개 키를 추출합니다.
4. 추출된 공개 키를 사용하여 서명을 해독하고 다운로드한 disk.raw 파일의 내용을 확인합니다.

스크립트를 표시하려면 클릭합니다

```
# 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
```

# Cloud Volumes ONTAP를 사용합니다

## 라이선스 관리

### 용량 기반 라이선스 관리

BlueXP 디지털 지갑에서 용량 기반 라이선스를 관리하여 NetApp 계정의 Cloud Volumes ONTAP 시스템 용량이 충분한지 확인합니다.

[\\_용량 기반 라이선스\\_](#) Cloud Volumes ONTAP/TiB 용량 비용을 지불할 수 있습니다.

BlueXP 디지털 지갑 [\\_을\(를\)](#) 사용하면 한 곳에서 Cloud Volumes ONTAP에 대한 라이선스를 관리할 수 있습니다. 새 라이선스를 추가하고 기존 라이선스를 업데이트할 수 있습니다.

["Cloud Volumes ONTAP 라이선스에 대해 자세히 알아보십시오"](#).

### BlueXP 디지털 지갑에 라이선스를 추가하는 방법

NetApp 세일즈 담당자로부터 라이선스를 구입하면 일련 번호와 추가 라이선스 세부 정보가 포함된 이메일이 전송됩니다.

그 동안 BlueXP는 NetApp의 라이선스 서비스에 대해 자동으로 쿼리하여 NetApp Support 사이트 계정과 연결된 라이선스에 대한 자세한 정보를 확인합니다. 오류가 없으면 BlueXP는 자동으로 디지털 지갑에 라이선스를 추가합니다.

BlueXP에서 라이선스를 추가할 수 없는 경우 디지털 지갑에 직접 추가해야 합니다. 예를 들어, 인터넷에 액세스할 수 없는 위치에 Connector가 설치되어 있는 경우 라이선스를 직접 추가해야 합니다. [구입한 라이선스를 계정에 추가하는 방법에 대해 알아봅니다](#).

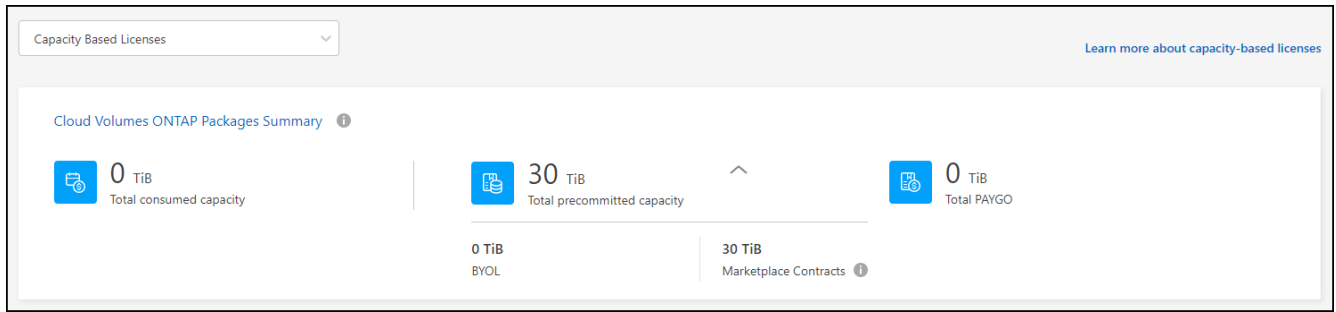
### 계정에서 사용된 용량을 확인합니다

BlueXP 디지털 지갑에는 계정의 총 소비된 용량과 라이선스 패키지를 통한 소비된 용량이 표시됩니다. 이를 통해 비용이 청구되는 방식 및 추가 용량을 구입해야 하는지 여부를 파악할 수 있습니다.

### 단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭에서 \* 용량 기반 라이선스 \* 를 선택한 상태로 유지합니다.
3. 사용된 용량, 사전 커밋된 총 용량 및 총 PAYGO 용량을 보여 주는 패키지 요약을 봅니다.
  - [\\_Total Consumed Capacity\\_](#) 는 NetApp 계정의 모든 Cloud Volumes ONTAP 시스템에 프로비저닝된 총 용량입니다. 충전은 볼륨 내의 로컬, 사용, 저장 또는 유효 공간에 관계없이 각 볼륨의 프로비저닝된 크기를 기준으로 합니다.
  - [\\_Total Prep커밋된 용량\\_](#) 은(는) NetApp에서 구매한 총 라이선스 용량(BYOL 또는 Marketplace 계약)입니다.
  - [\\_Total PAYGO\\_](#) 는 클라우드 마켓플레이스 서비스스크립션을 사용하여 프로비저닝된 총 용량입니다. PAYGO를 통한 충전은 사용된 용량이 BYOL 라이선스 용량보다 높거나 BlueXP 디지털 지갑에 사용 가능한 라이선스가 없는 경우에만 사용됩니다.

다음은 BlueXP 디지털 지갑의 Cloud Volumes ONTAP 패키지 요약의 예입니다.



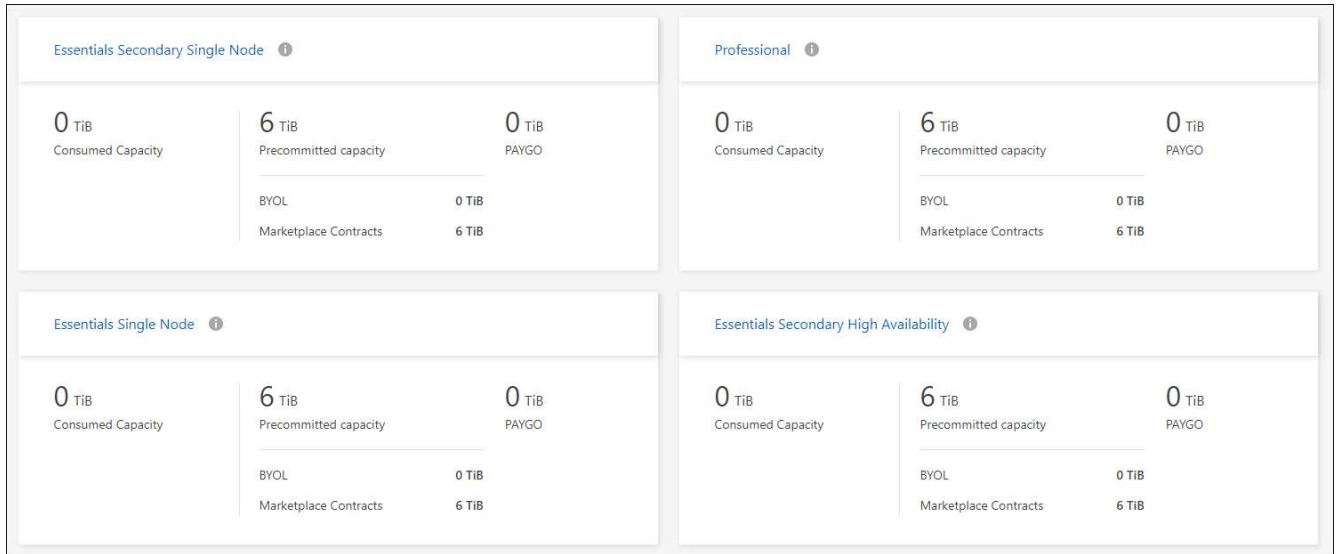
4. 요약에서 각 라이선스 패키지의 사용된 용량을 확인합니다.

- **\_Consumed capacity\_**는 해당 패키지의 볼륨 용량을 표시합니다. 특정 패키지에 대한 자세한 내용을 보려면 도구 설명 위로 마우스를 가져갑니다.

Essentials 패키지에 표시되는 용량을 더 잘 이해하려면 충전 작동 방식에 익숙해야 합니다. "[Essentials 패키지 충전 방법에 대해 알아봅니다](#)".

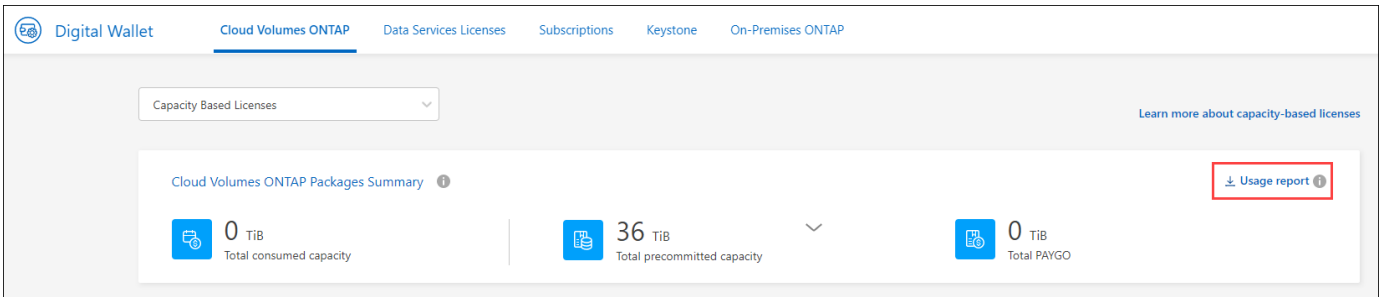
- **\_PreCommitted Capacity\_**는 NetApp에서 구매한 라이선스 용량(BYOL 또는 마켓플레이스 계약)입니다.
  - **\_BYOL\_**은 이 패키지 유형에 대해 NetApp에서 구입한 라이선스 용량을 보여 줍니다.
  - **Marketplace** 계약 은 이 패키지 유형에 대한 마켓플레이스 계약과 함께 구입한 라이선스 용량을 표시합니다.
- **\_PAYGO\_**는 라이선스 소비 모델에 따라 사용된 용량을 보여줍니다.

다음은 여러 라이선스 패키지가 있는 계정의 예입니다.



사용 보고서를 다운로드합니다

계정 관리자는 BlueXP의 디지털 지갑에서 네 가지 사용 보고서를 다운로드할 수 있습니다. 이러한 사용 보고서는 구독의 용량 세부 정보를 제공하고 Cloud Volumes ONTAP 구독에 포함된 리소스에 대한 비용 청구 방식을 알려줍니다. 다운로드할 수 있는 보고서는 특정 시점에 데이터를 캡처하여 다른 사람과 쉽게 공유할 수 있습니다.



다음 보고서를 다운로드할 수 있습니다. 표시된 용량 값은 TiB입니다.

- \* 고급 사용량\*: 이 보고서는 디지털 지갑의 “Cloud Volumes ONTAP 패키지 요약” 카드에 있는 내용을 정확하게 보여줍니다. 여기에는 다음 정보가 포함됩니다.
  - 사용된 총 용량입니다
  - 사전 커밋된 총 용량입니다
  - 총 BYOL 용량
  - 총 마켓플레이스 계약 용량입니다
  - 총 PAYGO 용량
- \* Cloud Volumes ONTAP 패키지 사용 \*: 이 보고서는 디지털 지갑의 패키지 카드에 있는 내용을 정확하게 보여줍니다. 최적화된 I/O 패키지를 제외한 각 패키지에 대한 다음 정보가 포함되어 있습니다.
  - 사용된 총 용량입니다
  - 사전 커밋된 총 용량입니다
  - 총 BYOL 용량
  - 총 마켓플레이스 계약 용량입니다
  - 총 PAYGO 용량
- \* 스토리지 VM 사용량 \*: 이 보고서는 Cloud Volumes ONTAP 시스템과 스토리지 가상 시스템(SVM)에서 청구 용량이 얼마나 분석되는지를 보여줍니다. 이 정보는 디지털 지갑의 화면에서는 사용할 수 없습니다. 여기에는 다음 정보가 포함됩니다.
  - 작업 환경 ID 및 이름(UUID로 표시됨)
  - 클라우드
  - NetApp 계정 ID입니다
  - 작업 환경 구성
  - SVM 이름
  - 용량을 프로비저닝합니다
  - 데이터 중복 제거 용량
  - 마켓플레이스 청구 기간
  - Cloud Volumes ONTAP 패키지 또는 기능
  - SaaS Marketplace 구독 이름 충전 중
  - SaaS Marketplace 구독 ID를 충전하는 중입니다

- 워크로드 유형
- \* Volumes usage \*: 이 보고서는 작업 환경의 볼륨에 의해 청구된 용량이 어떻게 분할되는지 보여줍니다. 이 정보는 디지털 지갑의 화면에서는 사용할 수 없습니다. 여기에는 다음 정보가 포함됩니다.
  - 작업 환경 ID 및 이름(UUID로 표시됨)
  - SVN 이름
  - 볼륨 ID입니다
  - 볼륨 유형입니다
  - 볼륨 프로비저닝 용량입니다



FlexClone 볼륨은 이러한 유형의 볼륨에 비용이 발생하지 않으므로 이 보고서에 포함되지 않습니다.

#### 단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭에서 \* Capacity Based Licenses \* 를 선택한 상태로 두고 \* Usage report \* 를 클릭합니다.

사용량 보고서가 다운로드됩니다.

3. 다운로드한 파일을 열어 보고서에 액세스합니다.

#### 구입한 라이선스를 계정에 추가합니다

BlueXP 디지털 지갑에 구입한 라이선스가 없으면 Cloud Volumes ONTAP에 사용할 수 있도록 BlueXP에 라이선스를 추가해야 합니다.

#### 필요한 것

- 라이선스 또는 라이선스 파일의 일련 번호를 BlueXP에 제공해야 합니다.
- 일련 번호를 입력하려면 먼저 해야 합니다 ["NetApp Support 사이트 계정을 BlueXP에 추가합니다"](#). 일련 번호에 액세스할 수 있는 권한이 있는 NetApp Support 사이트 계정입니다.

#### 단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭에서 \* 용량 기반 라이선스 \* 를 선택한 상태로 두고 \* 라이선스 추가 \* 를 클릭합니다.
3. 용량 기반 라이선스의 일련 번호를 입력하거나 라이선스 파일을 업로드하십시오.

일련 번호를 입력한 경우 일련 번호에 액세스할 수 있는 권한이 있는 NetApp Support 사이트 계정도 선택해야 합니다.

4. 라이선스 추가 \* 를 클릭합니다.

#### 용량 기반 라이선스를 업데이트합니다

추가 용량을 구매하거나 라이선스 기간을 연장한 경우 BlueXP는 디지털 지갑에서 라이선스를 자동으로 업데이트합니다. 당신이 해야 할 일은 아무것도 없습니다.

하지만 인터넷에 액세스할 수 없는 위치에 BlueXP를 배포한 경우에는 BlueXP에서 라이선스를 수동으로 업데이트해야 합니다.

필요한 것

라이선스 파일(또는 HA 쌍이 있는 경우 \_ 파일 \_).

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP\* 탭에서 사용권 옆에 있는 작업 메뉴를 클릭하고 \* 사용권 업데이트 \* 를 선택합니다.
3. 라이선스 파일을 업로드합니다.
4. 라이선스 업로드 \* 를 클릭합니다.

충전 방법을 변경합니다

용량 기반 라이선스를 사용하는 Cloud Volumes ONTAP 시스템의 충전 방법을 변경할 수 있습니다. 예를 들어, Essentials 패키지와 함께 Cloud Volumes ONTAP 시스템을 배포한 경우 비즈니스 요구사항이 변경되면 이를 Professional 패키지로 변경할 수 있습니다.

제한

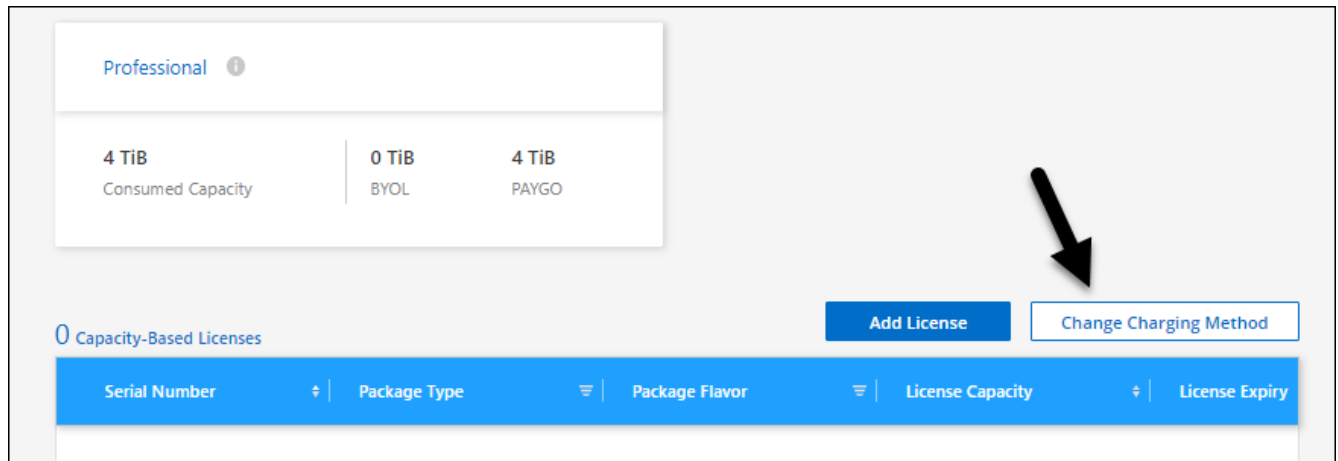
Edge Cache 라이선스로 변경하거나 변경하는 것은 지원되지 않습니다.

중요 참고 사항

클라우드 공급자 마켓플레이스에서 프라이빗 오퍼 또는 계약을 체결한 경우, 계약에 포함되지 않은 충전 방법으로 변경하면 BYOL(NetApp에서 라이선스를 구매한 경우) 또는 PAYGO에 대해 충전이 생성됩니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭에서 \* 충전 방법 변경 \* 을 클릭합니다.



3. 작업 환경을 선택하고 새 충전 방법을 선택한 다음 패키지 유형을 변경하면 서비스 요금이 달라지게 된다는 것을 이해했는지 확인합니다.



4. 충전 방법 변경 \* 을 클릭합니다.

결과

BlueXP는 Cloud Volumes ONTAP 시스템의 충전 방법을 변경합니다.

BlueXP 디지털 지갑은 각 패키지 유형의 소비된 용량을 새로 고쳐 방금 변경한 내용을 고려할 수도 있습니다.

용량 기반 라이선스를 제거합니다

용량 기반 라이선스가 만료되어 더 이상 사용되지 않는 경우 언제든지 라이선스를 제거할 수 있습니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP\* 탭에서 사용권 옆에 있는 작업 메뉴를 클릭하고 \* 사용권 제거 \* 를 선택합니다.
3. 확인하려면 \* 제거 \* 를 클릭합니다.

## Keystone 구독 관리

Cloud Volumes ONTAP에서 사용할 수 있도록 구독을 활성화하여 BlueXP 디지털 지갑에서 Keystone 가입을 관리하십시오. 또한 커밋된 용량에 대한 변경 내용을 요청하고 구독 연결을 해제할 수 있습니다.

Keystone 가입 \_ 은 NetApp이 제공하는 종량제 스토리지 서비스입니다.

BlueXP 디지털 지갑 \_을(를) 사용하면 한 곳에서 Cloud Volumes ONTAP에 대한 라이선스를 관리할 수 있습니다. 새 라이선스를 추가하고 기존 라이선스를 업데이트할 수 있습니다.

"Cloud Volumes ONTAP 라이선스에 대해 자세히 알아보십시오".

계정을 인증합니다

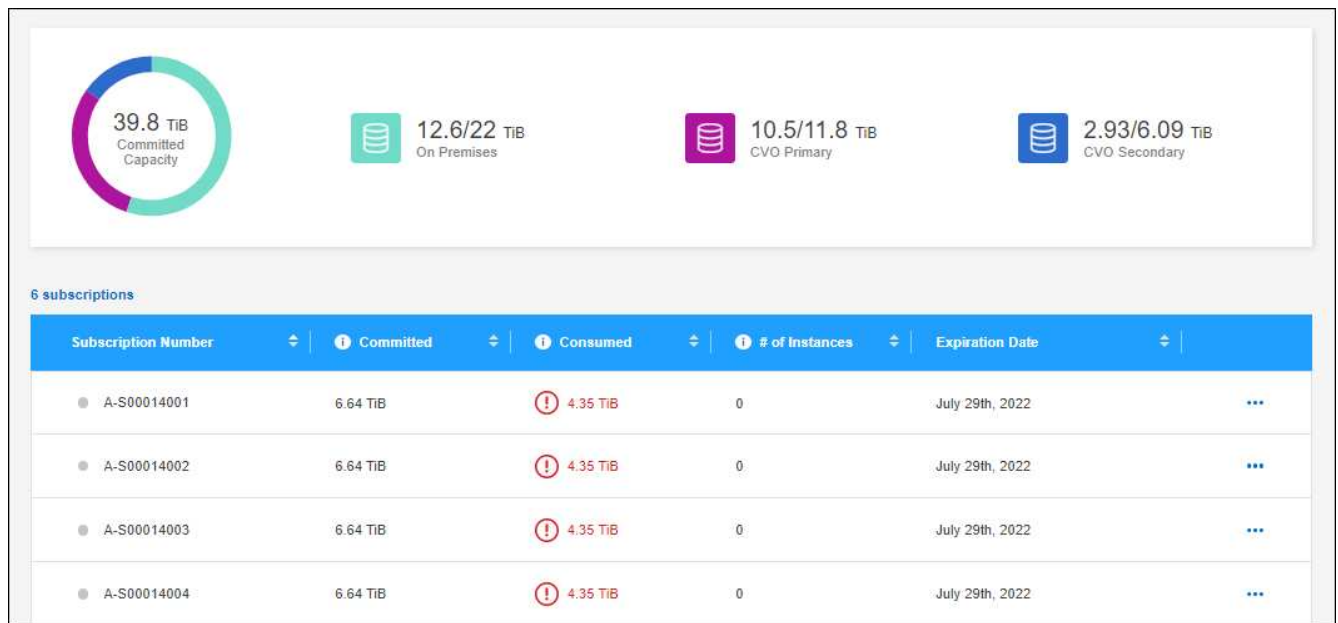
BlueXP에서 Keystone 등록을 사용하고 관리하려면 NetApp에 문의하여 Keystone 구독으로 BlueXP 사용자 계정을 인증해야 합니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Keystone \* 을 선택합니다.
3. NetApp Keystone\* 시작 페이지가 나타나면 페이지에 나열된 주소로 이메일을 보냅니다.

NetApp 담당자가 사용자 계정에 구독 액세스를 승인하여 요청을 처리합니다.

4. 가입을 보려면 \* Keystone 가입 \* 으로 돌아갑니다.



다음 단계

Cloud Volumes ONTAP에 사용할 구독을 연결합니다.

구독 링크

NetApp에서 사용자 계정을 승인한 후 Cloud Volumes ONTAP에 사용할 수 있도록 Keystone 구독을 연결해야 합니다. 이 작업을 통해 사용자는 새 Cloud Volumes ONTAP 시스템의 충전 방법으로 구독을 선택할 수 있습니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Keystone \* 을 선택합니다.

3. 연결할 구독의 경우 을 클릭합니다 ... 링크 \* 를 선택합니다.

Subscription Number	Committed	Consumed	# of Instances	Expiration Date	
A-S00014001	6.64 TiB	4.35 TiB	0	July 29th, 2022	...
A-S00014002	6.64 TiB	4.35 TiB	0	July 29th, 2022	View detail and edit
A-S00014003	6.64 TiB	4.35 TiB	0	July 29th, 2022	Link

#### 결과

이제 가입이 BlueXP 계정에 연결되어 있으며 Cloud Volumes ONTAP 작업 환경을 생성할 때 선택할 수 있습니다.

커밋된 용량을 더 많이 또는 적게 요청합니다

구독에 대해 커밋된 용량을 조정해야 하는 경우 BlueXP 인터페이스에서 바로 요청을 보낼 수 있습니다.

#### 단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Keystone \* 을 선택합니다.
3. 용량을 조정하려는 구독의 경우 을 클릭합니다 ... 를 선택하고 \* 상세 정보 보기 및 편집 \* 을 선택합니다.
4. 하나 이상의 구독에 대해 요청된 커밋 용량을 입력합니다.

### Subscription Modification for A-S00014001

Service Level	Current Committed Capacity	Current Consumed Capacity	Requested Committed Capacity
Extreme	0.977 TiB	0.293 TiB	<input type="text" value="Enter amount"/> TiB
Premium	0.977 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB
Performance	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
Standard	0.732 TiB	0.439 TiB	<input type="text" value="Enter amount"/> TiB
Value	0.977 TiB	<span style="color: orange;">!</span> 0.879 TiB	<input type="text" value="Enter amount"/> TiB
Data Tiering	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
CVO Primary	1.96 TiB	<span style="color: orange;">!</span> 1.76 TiB	<input type="text" value="3"/> TiB
CVO Secondary	1.02 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB

#### Additional Information

Is there anything else we should know about your request?  
Please be as descriptive as possible.

Enter your notes here

5. 아래로 스크롤하여 요청에 대한 추가 세부 정보를 입력한 다음 \* 제출 \* 을 클릭합니다.

결과

요청이 NetApp의 시스템에서 처리를 위한 티켓을 생성합니다.

구독 연결을 해제합니다

새 Cloud Volumes ONTAP 시스템에 Keystone 가입을 더 이상 사용하지 않으려면 가입을 연결 해제할 수 있습니다. 기존 Cloud Volumes ONTAP 구독에 연결되지 않은 구독만 연결 해제할 수 있습니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Keystone \* 을 선택합니다.
3. 연결을 해제할 구독의 경우 을 클릭합니다 ... 를 클릭하고 \* 연결 해제 \* 를 선택합니다.

결과

가입이 BlueXP 계정과 연결되어 있지 않으며 Cloud Volumes ONTAP 작업 환경을 생성할 때 더 이상 선택할 수 없습니다.

## 노드 기반 라이선스 관리

BlueXP 디지털 지갑에서 노드 기반 라이선스를 관리하여 각 Cloud Volumes ONTAP 시스템에 필요한 용량의 유효한 라이선스가 있는지 확인합니다.

\_노드 기반 라이선스\_ 은(는) 이전 세대 라이선스 모델입니다(신규 고객은 사용할 수 없습니다).

- NetApp에서 BYOL 라이선스를 구입함
- 클라우드 공급자 마켓플레이스에서 시간별 PAYGO(Pay-as-you-go) 구독을 지원합니다

BlueXP 디지털 지갑 \_을(를) 사용하면 한 곳에서 Cloud Volumes ONTAP에 대한 라이선스를 관리할 수 있습니다. 새 라이선스를 추가하고 기존 라이선스를 업데이트할 수 있습니다.

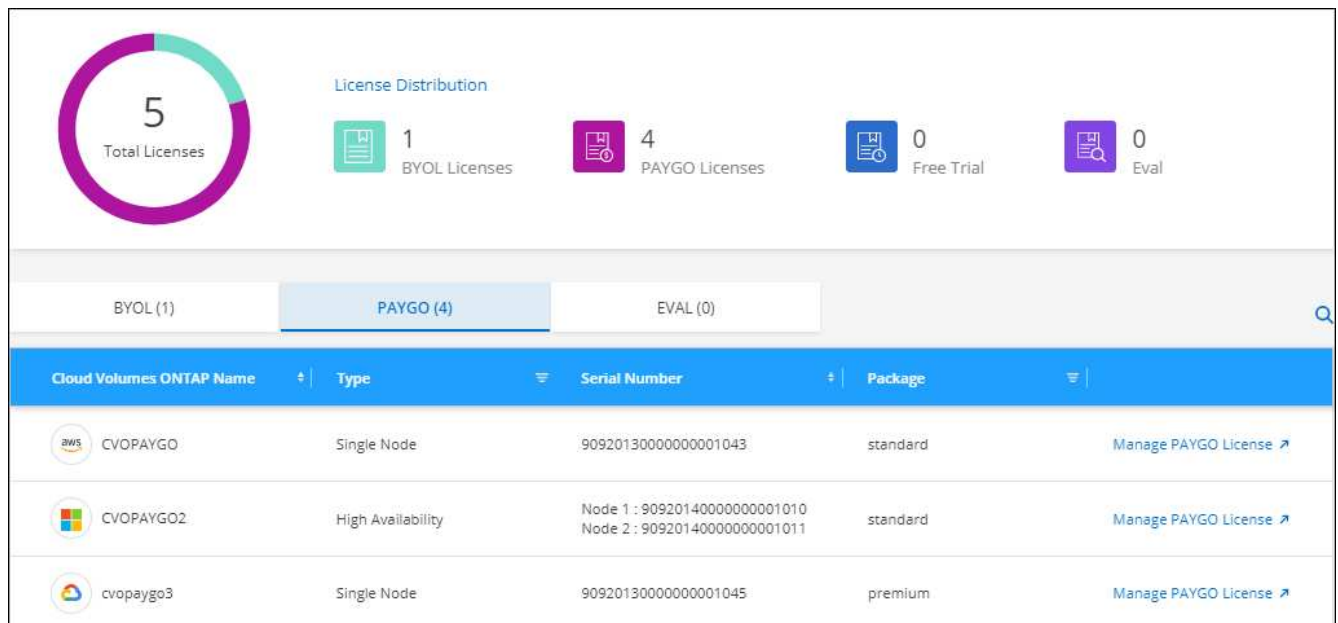
"Cloud Volumes ONTAP 라이선스에 대해 자세히 알아보십시오".

### PAYGO 라이선스를 관리합니다

BlueXP 디지털 지갑 페이지에서 일련 번호 및 PAYGO 라이선스 유형을 비롯한 각 PAYGO Cloud Volumes ONTAP 시스템에 대한 세부 정보를 볼 수 있습니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭의 드롭다운에서 \* 노드 기반 라이선스 \* 를 선택합니다.
3. PAYGO \* 를 클릭합니다.
4. 각 PAYGO 라이선스에 대한 자세한 내용은 표에서 확인하십시오.



The screenshot displays the 'License Distribution' section of the BlueXP Digital Wallet. It features a donut chart showing 5 Total Licenses, broken down into 1 BYOL License, 4 PAYGO Licenses, 0 Free Trial, and 0 Eval. Below this, there are tabs for BYOL (1), PAYGO (4), and EVAL (0). The PAYGO tab is selected, showing a table of licenses.

Cloud Volumes ONTAP Name	Type	Serial Number	Package	Actions
CVOPAYGO	Single Node	90920130000000001043	standard	<a href="#">Manage PAYGO License</a>
CVOPAYGO2	High Availability	Node 1 : 90920140000000001010 Node 2 : 90920140000000001011	standard	<a href="#">Manage PAYGO License</a>
cvopayo3	Single Node	90920130000000001045	premium	<a href="#">Manage PAYGO License</a>

5. 필요한 경우 \* PAYGO 라이선스 관리 \* 를 클릭하여 PAYGO 라이선스를 변경하거나 인스턴스 유형을 변경합니다.

## BYOL 라이선스 관리

시스템 라이선스 및 추가 용량 라이선스를 추가 및 제거하여 NetApp에서 직접 구매한 라이선스를 관리합니다.

할당되지 않은 라이선스를 추가합니다

BlueXP 디지털 지갑에 노드 기반 라이선스를 추가하여 새 Cloud Volumes ONTAP 시스템을 생성할 때 라이선스를 선택할 수 있습니다. 디지털 지갑에서 이러한 라이선스를 할당되지 않음으로 식별합니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭의 드롭다운에서 \* 노드 기반 라이선스 \* 를 선택합니다.
3. 할당되지 않음 \* 을 클릭합니다.
4. 할당되지 않은 라이선스 추가 \* 를 클릭합니다.
5. 라이선스의 일련 번호를 입력하거나 라이선스 파일을 업로드하십시오.

라이선스 파일이 아직 없는 경우 아래 섹션을 참조하십시오.

6. 라이선스 추가 \* 를 클릭합니다.

결과

BlueXP는 디지털 지갑에 라이선스를 추가합니다. 라이선스는 새 Cloud Volumes ONTAP 시스템에 연결할 때까지 할당되지 않은 것으로 식별됩니다. 그런 다음 디지털 지갑에서 \* BYOL \* 탭으로 라이선스가 이동됩니다.

할당되지 않은 **Exchange** 노드 기반 라이선스

아직 사용하지 않은 Cloud Volumes ONTAP에 대해 할당되지 않은 노드 기반 라이선스가 있는 경우 라이선스를 BlueXP 백업 및 복구 라이선스, BlueXP 분류 라이선스 또는 BlueXP 계층화 라이선스로 변환하여 교환할 수 있습니다.

라이선스 교환은 Cloud Volumes ONTAP 라이선스를 해지하고 서비스에 대해 달러 상당 라이선스를 생성합니다.

- Cloud Volumes ONTAP HA 쌍의 라이선스는 51TiB 데이터 서비스 라이선스로 변환됩니다
- Cloud Volumes ONTAP 단일 노드의 라이선스는 32TiB 데이터 서비스 라이선스로 변환됩니다

변환된 라이선스의 만료일은 Cloud Volumes ONTAP 라이선스와 동일합니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭의 드롭다운에서 \* 노드 기반 라이선스 \* 를 선택합니다.
3. 할당되지 않음 \* 을 클릭합니다.
4. Exchange 라이선스 \* 를 클릭합니다.

BYOL (14)		Eval (2)		Unassigned (3)		PAYGO (6)		Add Unassigned Licenses	
Serial Number	Type	Cloud Provider	License Expiry	Status					
012345678901234567890	Single Node	All Providers	April 20, 2022	Unassigned	Exchange License		...		
012345678901234567891	Single Node	Azure	April 20, 2022	Unassigned	Exchange License		...		
012345678901234567892	Single Node	AWS	January 1, 2022	Exchanged to Cloud Tiering on August 1, 2021					

- 라이센스를 교환할 서비스를 선택합니다.
- 메시지가 표시되면 HA 쌍에 대한 추가 라이선스를 선택합니다.
- 법적 동의를 읽고 \* 동의 \* 를 클릭합니다.

#### 결과

BlueXP는 할당되지 않은 라이선스를 선택한 서비스로 변환합니다. 데이터 서비스 라이선스 \* 탭에서 새 라이선스를 볼 수 있습니다.

시스템 라이선스 파일을 얻습니다

대부분의 경우 BlueXP는 NetApp Support 사이트 계정을 사용하여 라이선스 파일을 자동으로 가져올 수 있습니다. 그러나 그렇지 않으면 라이선스 파일을 수동으로 업로드해야 합니다. 라이선스 파일이 없는 경우 netapp.com 에서 얻을 수 있습니다.

#### 단계

- 로 이동합니다 "NetApp 라이선스 파일 생성기" 를 입력하고 NetApp Support 사이트 자격 증명을 사용하여 로그인합니다.
- 비밀번호를 입력하고 제품을 선택한 다음 일련 번호를 입력하고 개인정보 보호정책을 읽고 동의했는지 확인한 다음 \* 제출 \* 을 클릭합니다.
  - 예 \*

## License Generator

The following fields are pre-populated based on the NetApp SSO login provided.  
To download the corresponding NetApp license file, re-enter your SSO password along with the correct Product Line and Product Serial number.

First Name	<input type="text" value="Ben"/>
Last Name	<input type="text"/>
Company	<input type="text" value="Network Appliance, Inc"/>
Email Address	<input type="text"/>
Username	<input type="text"/>

Product Line*	<input type="text" value=""/>
---------------	-------------------------------

- ONTAP Select - Standard
- ONTAP Select - Premium
- ONTAP Select - Premium XL
- Cloud Volumes ONTAP for AWS (single node)
- Cloud Volumes ONTAP for AWS (HA)
- Cloud Volumes ONTAP for GCP (single node or HA)
- Cloud Volumes ONTAP for Microsoft Azure (single node)
- Cloud Volumes ONTAP for Microsoft Azure (HA)
- Service Level Manager - SLO Advanced
- StorageGRID Webscale
- StorageGRID WhiteBox
- SnapCenter Standard (capacity-based)

Not only is protecting your data required by law, it's also the right thing to do.  I have read NetApp's new **Global Data Privacy Policy** and agree that NetApp may use my personal data.

3. 이메일 또는 직접 다운로드를 통해 serialnumber.nlf JSON 파일을 수신할지 여부를 선택합니다.

시스템 라이선스를 업데이트합니다

NetApp 담당자에게 연락하여 BYOL 구독을 갱신하면, BlueXP는 NetApp에서 새로운 라이선스를 자동으로 얻어 Cloud Volumes ONTAP 시스템에 설치합니다.

보안 인터넷 연결을 통해 BlueXP에서 라이선스 파일에 액세스할 수 없는 경우 직접 파일을 얻은 다음 파일을 BlueXP에 수동으로 업로드할 수 있습니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭의 드롭다운에서 \* 노드 기반 라이선스 \* 를 선택합니다.
3. BYOL \* 탭에서 Cloud Volumes ONTAP 시스템의 세부 정보를 확장합니다.
4. 시스템 라이선스 옆에 있는 작업 메뉴를 클릭하고 \* 라이선스 업데이트 \* 를 선택합니다.
5. 라이선스 파일(또는 HA 쌍이 있는 경우 파일)을 업로드합니다.
6. Update License \* 를 클릭합니다.

결과

BlueXP는 Cloud Volumes ONTAP 시스템의 라이선스를 업데이트합니다.

추가 용량 라이선스 관리

Cloud Volumes ONTAP BYOL 시스템용 추가 용량 라이선스를 구입하여 368TiB 이상의 용량을 BYOL 시스템



라이선스와 함께 할당할 수 있습니다. 예를 들어, 라이선스 용량을 하나 더 구매하여 Cloud Volumes ONTAP에 최대 736TiB의 용량을 할당할 수 있습니다. 또는 최대 1.4PiB까지 추가 용량 라이선스를 3개 구매할 수 있습니다.

단일 노드 시스템 또는 HA 쌍에 대해 구매할 수 있는 라이선스 수는 무제한입니다.

#### 용량 라이선스 추가

BlueXP의 오른쪽 하단에 있는 채팅 아이콘을 통해 문의하여 추가 용량 라이선스를 구입하십시오. 라이선스를 구입한 후 Cloud Volumes ONTAP 시스템에 적용할 수 있습니다.

#### 단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭의 드롭다운에서 \* 노드 기반 라이선스 \* 를 선택합니다.
3. BYOL \* 탭에서 Cloud Volumes ONTAP 시스템의 세부 정보를 확장합니다.
4. 용량 라이선스 추가 \* 를 클릭합니다.
5. 일련 번호를 입력하거나 라이선스 파일(또는 HA 쌍이 있는 경우 파일)을 업로드합니다.
6. 용량 라이선스 추가 \* 를 클릭합니다.

#### 용량 라이선스를 업데이트합니다

추가 용량 라이선스 기간을 연장한 경우 BlueXP에서 라이선스를 업데이트해야 합니다.

#### 단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭의 드롭다운에서 \* 노드 기반 라이선스 \* 를 선택합니다.
3. BYOL \* 탭에서 Cloud Volumes ONTAP 시스템의 세부 정보를 확장합니다.
4. 용량 라이선스 옆에 있는 작업 메뉴를 클릭하고 \* 라이선스 업데이트 \* 를 선택합니다.
5. 라이선스 파일(또는 HA 쌍이 있는 경우 파일)을 업로드합니다.
6. Update License \* 를 클릭합니다.

#### 용량 라이선스를 제거합니다

추가 용량 라이선스가 만료되어 더 이상 사용되지 않는 경우 언제든지 라이선스를 제거할 수 있습니다.

#### 단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭의 드롭다운에서 \* 노드 기반 라이선스 \* 를 선택합니다.
3. BYOL \* 탭에서 Cloud Volumes ONTAP 시스템의 세부 정보를 확장합니다.
4. 용량 라이선스 옆에 있는 작업 메뉴를 클릭하고 \* 라이선스 제거 \* 를 선택합니다.
5. 제거 \* 를 클릭합니다.

#### Eval 라이선스를 BYOL로 변환합니다

평가판 라이선스는 30일간 사용할 수 있습니다. 현재 위치 업그레이드에 대한 평가 라이선스 위에 새로운 BYOL

라이센스를 적용할 수 있습니다.

평가판 라이선스를 BYOL로 변환하면 BlueXP가 Cloud Volumes ONTAP 시스템을 다시 시작합니다.

- 단일 노드 시스템의 경우 재시작 시 재부팅 프로세스 중에 I/O가 중단됩니다.
- HA 쌍의 경우, 재시작은 테이크오버 및 반환을 시작하여 클라이언트에 계속 I/O를 제공합니다.

단계

1. BlueXP 탐색 메뉴에서 \* Governance > Digital Wallet \* 을 선택합니다.
2. Cloud Volumes ONTAP \* 탭의 드롭다운에서 \* 노드 기반 라이선스 \* 를 선택합니다.
3. Eval \* 을 클릭합니다.
4. 표에서 Cloud Volumes ONTAP 시스템용 BYOL 라이선스 \* 로 변환 을 클릭합니다.
5. 일련 번호를 입력하거나 라이선스 파일을 업로드하십시오.
6. 사용권 변환 \* 을 클릭합니다.

결과

BlueXP가 변환 프로세스를 시작합니다. 이 프로세스의 일부로 Cloud Volumes ONTAP가 자동으로 다시 시작됩니다. 백업하는 경우 라이선스 정보에 새 라이선스가 반영됩니다.

## PAYGO와 BYOL 간 변경

시스템을 PAYGO by-node 라이선싱에서 BYOL by-node 라이선싱으로 변환하는 것은 지원되지 않으며 그 반대의 경우도 마찬가지입니다. 사용한 만큼만 지불하는 가입과 BYOL 가입형 간에 전환하려면 새 시스템을 구축하고 기존 시스템에서 새 시스템으로 데이터를 복제해야 합니다.

단계

1. 새 Cloud Volumes ONTAP 작업 환경을 만듭니다.
2. 복제해야 하는 각 볼륨에 대해 시스템 간에 일회성 데이터 복제를 설정합니다.

"시스템 간에 데이터를 복제하는 방법에 대해 알아보십시오"

3. 원래 작업 환경을 삭제하여 더 이상 필요하지 않은 Cloud Volumes ONTAP 시스템을 종료합니다.

"Cloud Volumes ONTAP 작업 환경을 삭제하는 방법에 대해 알아보십시오".

## 볼륨 및 LUN 관리

### FlexVol 볼륨을 생성합니다

초기 Cloud Volumes ONTAP 시스템을 시작한 후 더 많은 스토리지가 필요한 경우 BlueXP에서 NFS, CIFS 또는 iSCSI용 새 FlexVol 볼륨을 생성할 수 있습니다.

BlueXP에서는 여러 가지 방법으로 새 볼륨을 만들 수 있습니다.

- 새 볼륨에 대한 세부 정보를 지정하고 BlueXP에서 기본 데이터 집계를 처리하도록 합니다. [자세한 정보](#)

- 선택한 데이터 애그리게이트에 볼륨을 생성합니다. [자세한 정보](#)
- 템플릿에서 볼륨을 생성하여 데이터베이스 또는 스트리밍 서비스와 같은 특정 애플리케이션의 워크로드 요구사항에 맞게 볼륨을 최적화합니다. [자세한 정보](#)
- HA 구성의 두 번째 노드에 볼륨을 생성합니다. [자세한 정보](#)

시작하기 전에

볼륨 프로비저닝에 대한 몇 가지 참고 사항:

- iSCSI 볼륨을 생성할 때 BlueXP에서 자동으로 LUN을 생성합니다. 볼륨 당 하나의 LUN만 생성하므로 관리가 필요 없습니다. 볼륨을 생성한 후 ["iQN을 사용하여 호스트에서 LUN에 연결합니다"](#).
- System Manager 또는 CLI에서 추가 LUN을 생성할 수 있습니다.
- AWS에서 CIFS를 사용하려면 DNS와 Active Directory를 설정해야 합니다. 자세한 내용은 ["Cloud Volumes ONTAP for AWS의 네트워킹 요구사항"](#)을 참조하십시오.
- Cloud Volumes ONTAP 구성에서 Amazon EBS Elastic Volumes 기능을 지원하는 경우 원하는 대로 구성할 수 있습니다 ["볼륨을 생성할 때 발생하는 상황에 대해 자세히 알아보십시오"](#).

볼륨을 생성합니다

볼륨을 생성하는 가장 일반적인 방법은 필요한 볼륨 유형을 지정한 다음 BlueXP에서 디스크 할당을 처리하는 것입니다. 그러나 볼륨을 생성할 특정 Aggregate를 선택할 수도 있습니다.

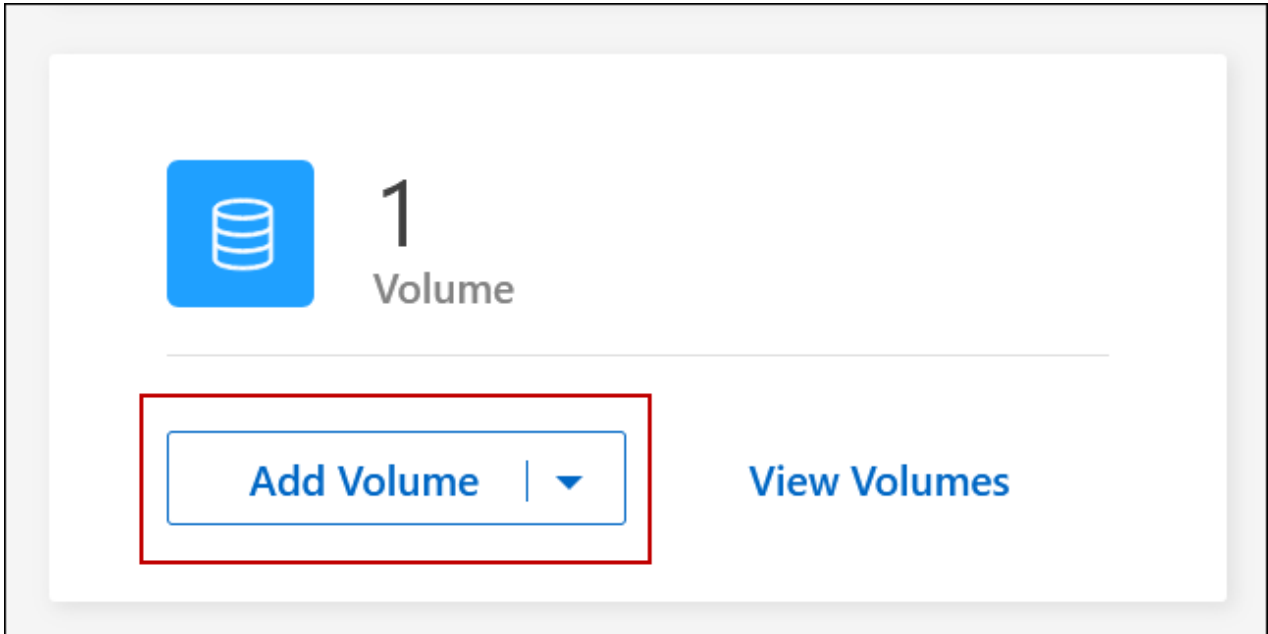
단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 FlexVol 볼륨을 프로비저닝할 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.
3. BlueXP에서 디스크 할당을 처리하도록 하거나 볼륨에 대한 특정 집계를 선택하여 새 볼륨을 생성합니다.

Cloud Volumes ONTAP 시스템의 데이터 애그리게이트를 잘 알고 있는 경우에만 특정 애그리게이트를 선택하는 것이 좋습니다.

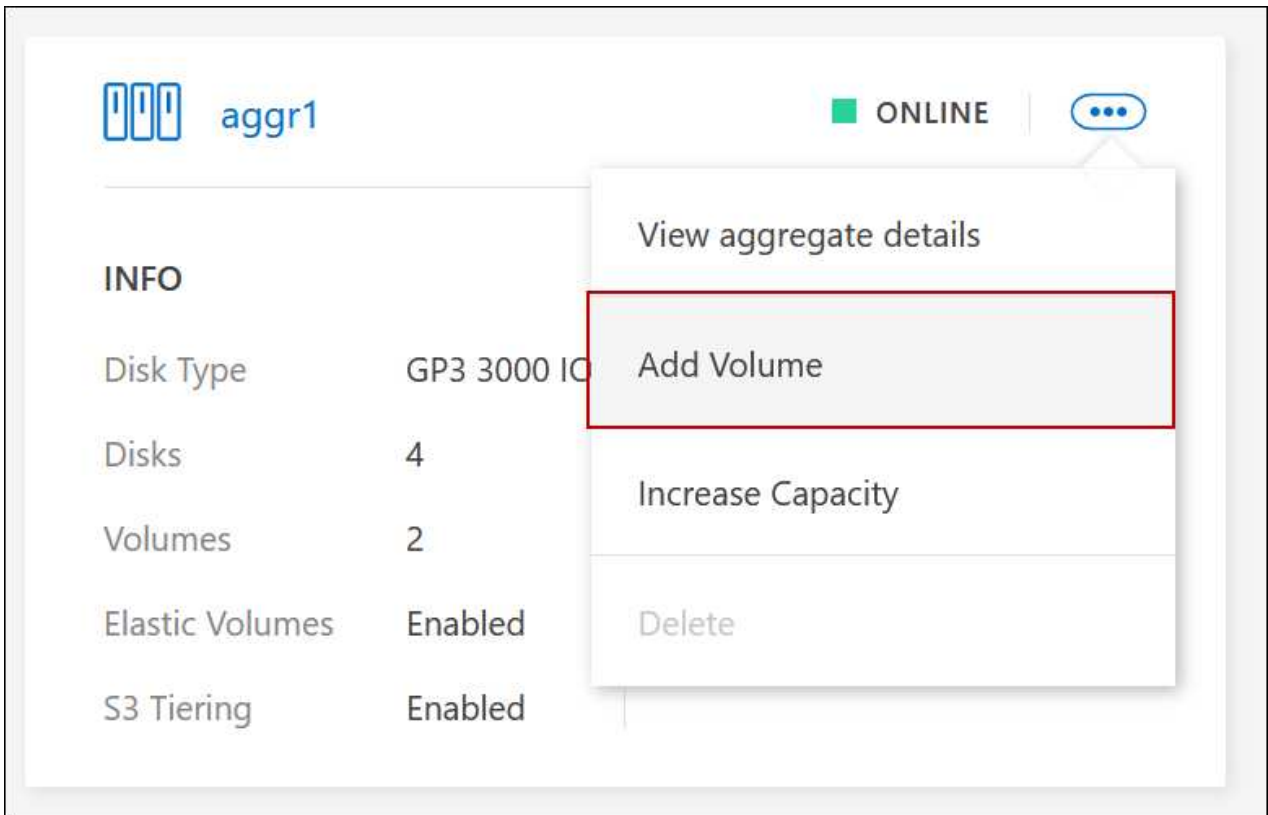
모든 애그리게이트

개요 탭에서 볼륨 타일로 이동한 다음 \* 볼륨 추가 \* 를 클릭합니다.



특정 애그리게이트

애그리게이트 탭에서 원하는 애그리게이트 타일로 이동합니다. 메뉴 아이콘을 클릭한 다음 \* 볼륨 추가 \* 를 클릭합니다.



4. 마법사의 단계에 따라 볼륨을 생성합니다.

a. \* 볼륨, 세부 정보, 보호 및 태그 \*: 볼륨에 대한 기본 세부 정보를 입력하고 스냅샷 정책을 선택합니다.

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

필드에 입력합니다	설명
볼륨 이름	새 볼륨에 입력할 수 있는 식별 가능한 이름입니다.
볼륨 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.
태그	볼륨에 추가하는 태그는 과 연결됩니다 "응용 프로그램 템플릿 서비스"을 사용하면 리소스 관리를 구성하고 단순화할 수 있습니다.
스토리지 VM(SVM)	스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에 스토리지 및 데이터 서비스를 제공합니다. SVM 또는 가상 서버로서 이를 알 수 있습니다. Cloud Volumes ONTAP는 기본적으로 하나의 스토리지 VM으로 구성되지만 일부 구성에서는 추가 스토리지 VM을 지원합니다. 새 볼륨에 대해 스토리지 VM을 지정할 수 있습니다.
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.

b. \* 프로토콜 \*: 볼륨의 프로토콜(NFS, CIFS 또는 iSCSI)을 선택한 다음 필요한 정보를 제공합니다.

CIFS를 선택하고 서버가 설정되지 않은 경우 \* 다음 \* 을 클릭하면 BlueXP에서 CIFS 연결을 설정하라는 메시지가 표시됩니다.

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

다음 섹션에서는 지침이 필요한 필드에 대해 설명합니다. 설명은 프로토콜별로 구성되어 있습니다.

## NFS 를 참조하십시오

### 액세스 제어

클라이언트에서 볼륨을 사용할 수 있도록 사용자 지정 익스포트 정책을 선택합니다.

### 익스포트 정책

볼륨을 액세스할 수 있는 서버넷의 클라이언트를 정의합니다. 기본적으로 BlueXP는 서버넷의 모든 인스턴스에 대한 액세스를 제공하는 값을 입력합니다.

## CIFS를 선택합니다

### 권한 및 사용자/그룹

사용자 및 그룹(액세스 제어 목록 또는 ACL라고도 함)에서 SMB 공유에 대한 액세스 수준을 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.

## 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.

- AWS 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 \* OU=Computers, OU=Corp \* 를 입력합니다.
- Azure AD 도메인 서비스를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 \* OU=ADDC 컴퓨터 \* 또는 \* OU=ADDC 사용자 \* 를 입력합니다.  
"Azure 설명서: Azure AD 도메인 서비스 관리 도메인에 OU(조직 구성 단위)를 만듭니다"
- Google 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 \* OU=Computers, OU=Cloud \* 를 입력합니다.  
"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 ["BlueXP 자동화 문서"](#) 를 참조하십시오.

CIFS 서버를 생성할 때만 NTP 서버를 구성할 수 있습니다. CIFS 서버를 생성한 후에는 구성할 수 없습니다.

## iSCSI

### LUN을 클릭합니다

iSCSI 스토리지 타겟을 LUN(논리 유닛)이라고 하며 호스트에 표준 블록 디바이스로 표시됩니다. iSCSI 볼륨을 생성할 때 BlueXP에서 자동으로 LUN을 생성합니다. 우리는 볼륨당 하나의 LUN만 생성하므로 관리가 필요하지 않습니다. 볼륨을 생성한 후 ["IQN을 사용하여 호스트에서 LUN에 연결합니다"](#).

### 이니시에이터 그룹

이니시에이터 그룹(igroup)은 스토리지 시스템에서 지정된 LUN에 액세스할 수 있는 호스트를 지정합니다

### 호스트 이니시에이터(IQN)

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.

a. \* 디스크 유형 \*: 성능 요구 사항 및 비용 요구 사항에 따라 볼륨의 기본 디스크 유형을 선택합니다.

- ["AWS에서 시스템 사이징"](#)
- ["Azure에서 시스템 사이징"](#)
- ["Google Cloud에서 시스템 크기 조정"](#)

5. \* Usage Profile & Tiering Policy \*: 볼륨에서 스토리지 효율성 기능을 활성화 또는 비활성화할지 여부를 선택한 다음 를 선택합니다 ["볼륨 계층화 정책"](#).

ONTAP에는 필요한 총 스토리지 양을 줄일 수 있는 몇 가지 스토리지 효율성 기능이 포함되어 있습니다. NetApp 스토리지 효율성 기능은 다음과 같은 이점을 제공합니다.

### 씬 프로비저닝

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

### 중복 제거

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

### 압축

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

6. \* Review \* (검토 \*): 볼륨에 대한 세부 정보를 검토한 다음 \* Add \* (추가 \*)를 클릭합니다.

## 결과

BlueXP는 Cloud Volumes ONTAP 시스템에 볼륨을 생성합니다.

템플릿에서 볼륨을 생성합니다

조직에서 Cloud Volumes ONTAP 볼륨 템플릿을 만들어 특정 애플리케이션의 워크로드 요구사항에 최적화된 볼륨을 구축한 경우 이 섹션의 단계를 수행하십시오.

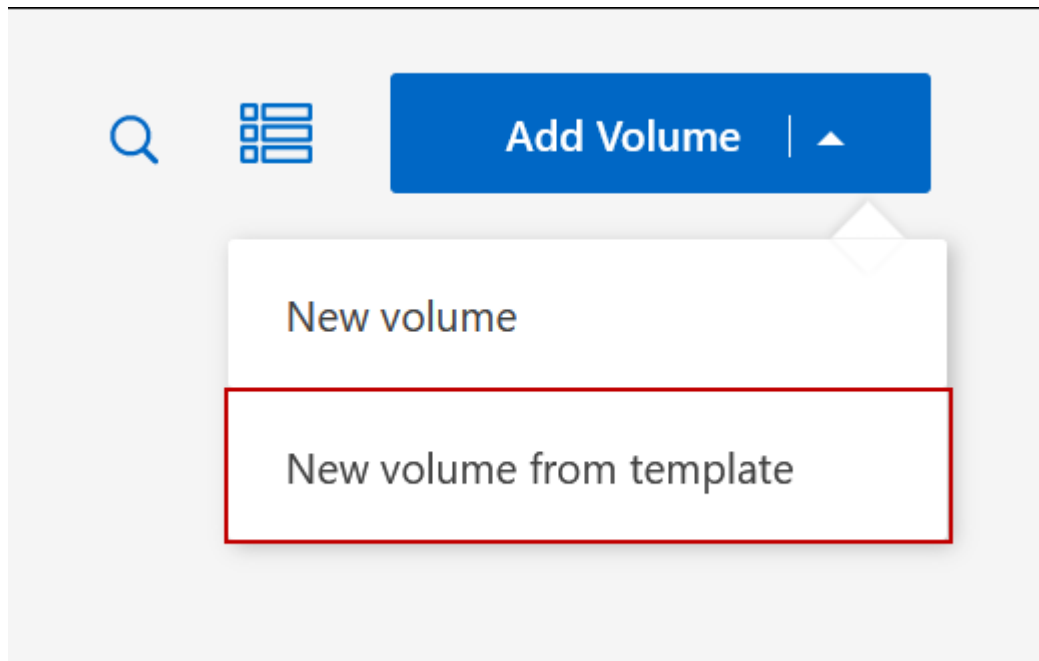
템플릿에 디스크 유형, 크기, 프로토콜, 스냅샷 정책, 클라우드 공급자 등 특정 볼륨 매개 변수가 이미 정의되어 있기 때문에 템플릿을 사용하면 작업을 보다 쉽게 수행할 수 있습니다. 있습니다. 매개 변수가 이미 미리 정의된 경우 다음 볼륨 매개 변수로 건너뛸 수 있습니다.



템플릿을 사용하는 경우에만 NFS 또는 CIFS 볼륨을 생성할 수 있습니다.

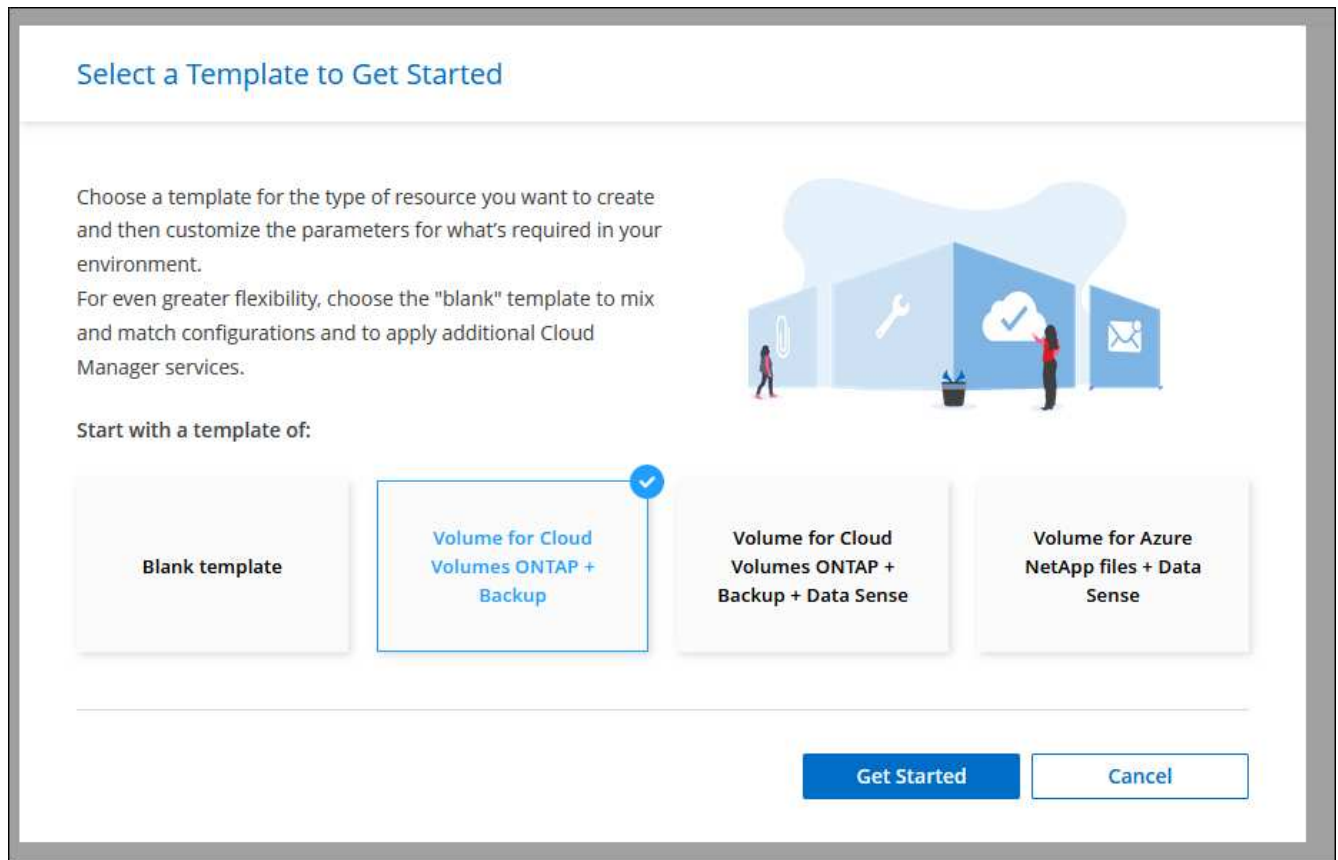
단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 볼륨을 프로비저닝할 Cloud Volumes ONTAP 시스템의 이름을 클릭합니다.
3. 볼륨 탭으로 이동하고 \* 볼륨 추가 \* > \* 템플릿에서 새 볼륨 \* 을 클릭합니다.

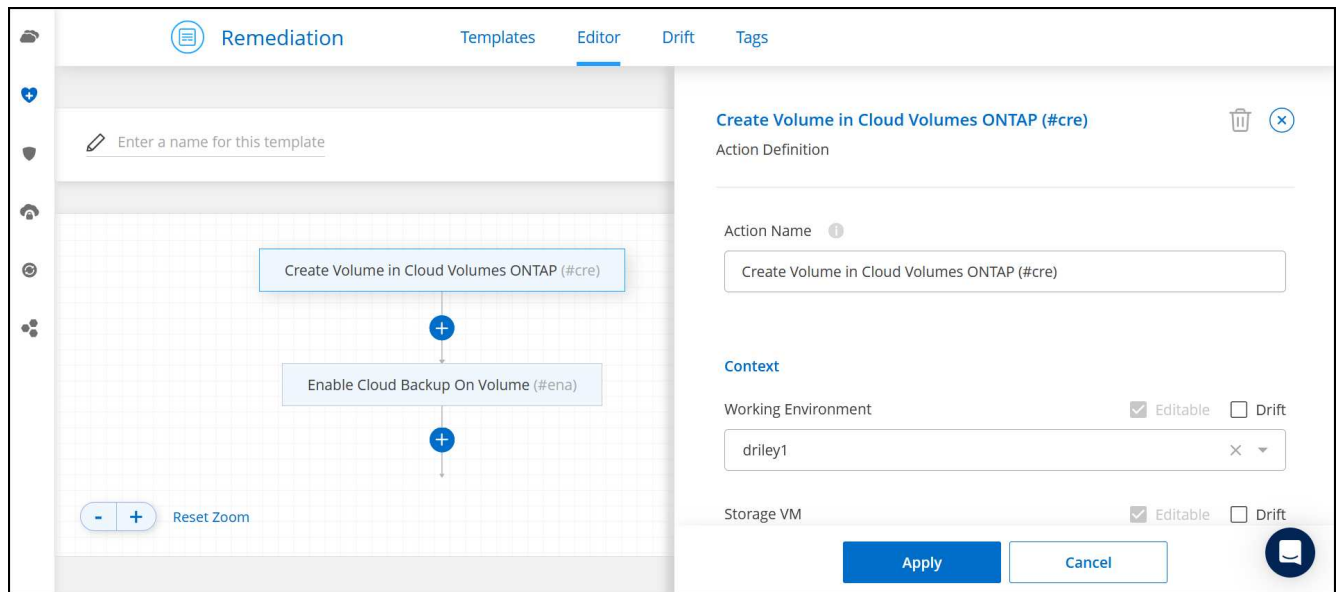


4. Select Template\_page에서 볼륨을 생성하는 데 사용할 템플릿을 선택하고 \* Next \* 를 클릭합니다.





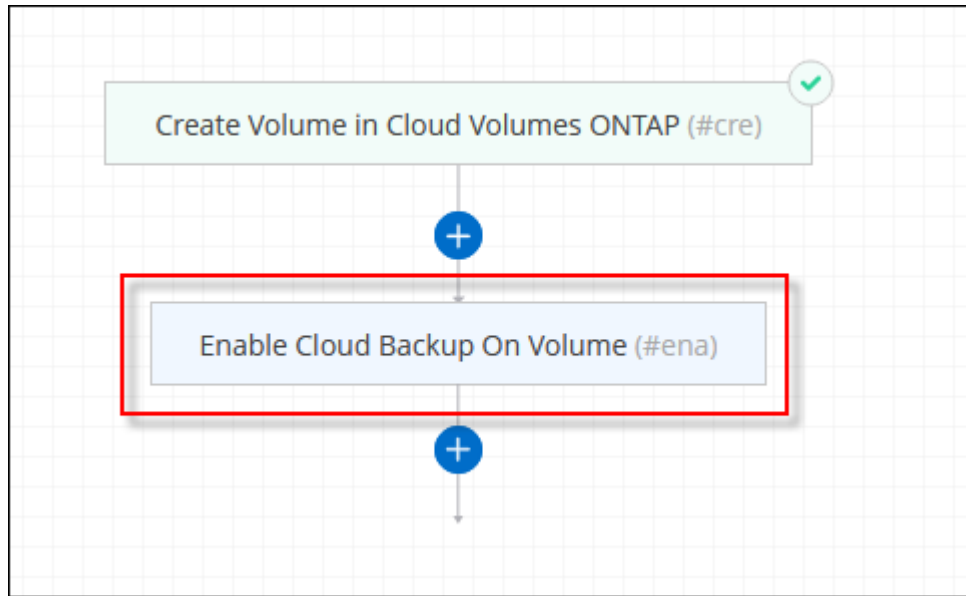
Editor\_page가 표시됩니다.



5. Action\_panel 위에 템플릿 이름을 입력합니다.
6. context\_에서 작업 환경은 시작한 작업 환경의 이름으로 채워집니다. 볼륨을 생성할 \* 스토리지 VM \* 을 선택합니다.
7. 템플릿에서 하드 코딩되지 않은 모든 매개변수에 대한 값을 추가합니다. 을 참조하십시오 **볼륨을 생성합니다** Cloud Volumes ONTAP 볼륨 구축을 완료하는 데 필요한 모든 매개 변수에 대한 자세한 내용은 를 참조하십시오.
8. Apply \* (적용 \*)를 클릭하여 구성된 매개변수를 선택한 작업에 저장합니다.

9. 정의해야 할 다른 작업이 없는 경우(예: BlueXP 백업 및 복구 구성) \* 템플릿 저장 \* 을 클릭합니다.

다른 작업이 있는 경우 왼쪽 창에서 작업을 클릭하여 완료해야 하는 매개 변수를 표시합니다.



예를 들어 Enable Cloud Backup on Volume 작업이 백업 정책을 선택해야 하는 경우 지금 선택할 수 있습니다.

10. 템플릿 작업에 대한 구성이 완료되면 \* 템플릿 저장 \* 을 클릭합니다.

결과

Cloud Volumes ONTAP에서는 진행 상황을 볼 수 있도록 볼륨을 프로비저닝하고 페이지를 표시합니다.

**Creating your resources**

This process can take a few minutes.  
Keep this page open to monitor progress, or you can close this page and check the [Timeline](#) later for details.

**Actions status**

Create Volume in Cloud Volumes ONTAP	Success
Enable Cloud Backup	Pending

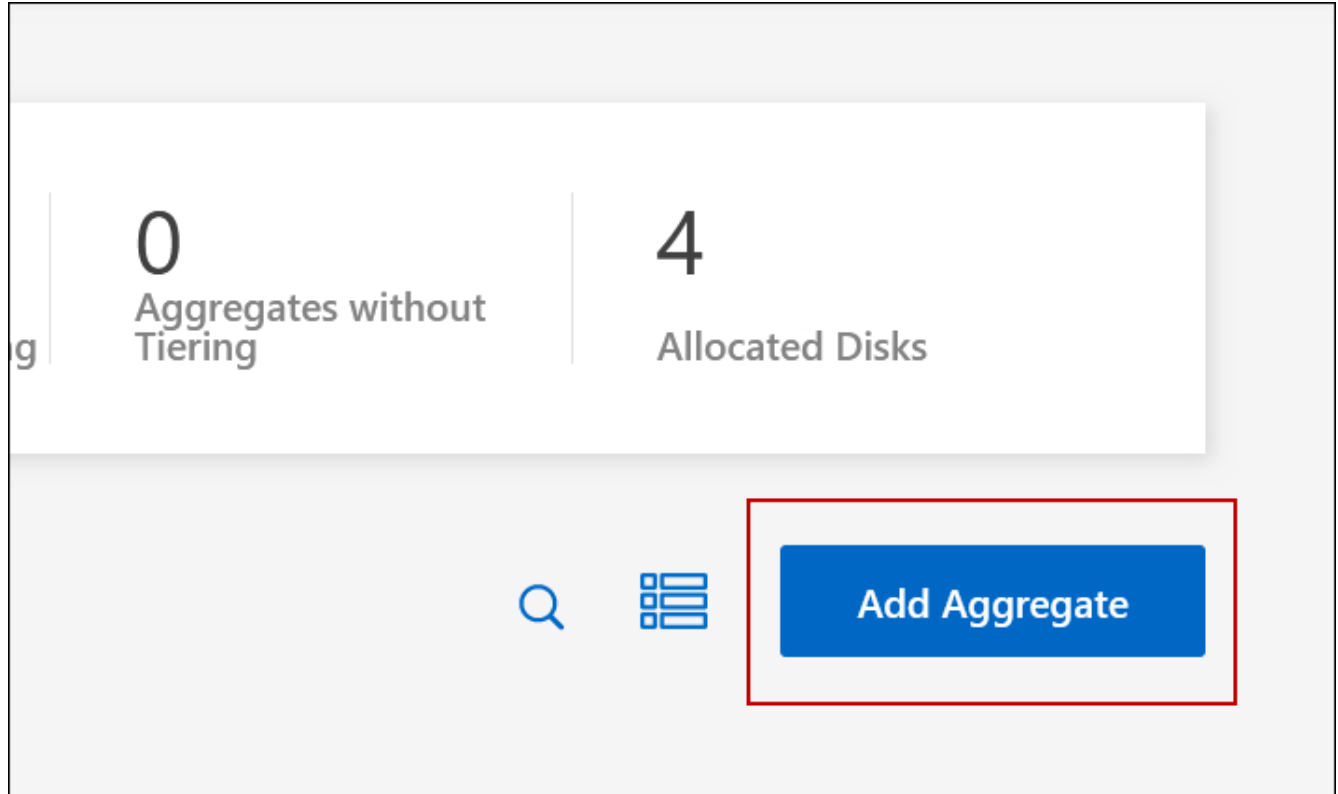
또한 볼륨에 대해 BlueXP 백업 및 복구를 활성화하는 등 템플릿에 보조 작업이 구현된 경우 해당 작업도 수행됩니다.

**HA 구성의 두 번째 노드에 볼륨을 생성합니다**

기본적으로 BlueXP는 HA 구성의 첫 번째 노드에 볼륨을 생성합니다. 두 노드에서 모두 클라이언트에 데이터를 제공하는 액티브-액티브 구성이 필요한 경우 두 번째 노드에서 애그리게이트와 볼륨을 생성해야 합니다.

## 단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 집계를 관리할 Cloud Volumes ONTAP 작업 환경의 이름을 두 번 클릭합니다.
3. 집계 탭에서 \* 집계 추가 \* 를 클릭합니다.
4. Add Aggregate\_screen에서 Aggregate를 생성합니다.



5. 홈 노드의 경우 HA 쌍의 두 번째 노드를 선택합니다.
6. BlueXP에서 애그리게이트를 생성한 후 해당 애그리게이트를 선택한 다음 \* 볼륨 생성 \* 을 클릭합니다.
7. 새 볼륨에 대한 세부 정보를 입력한 다음 \* Create \* 를 클릭합니다.

## 결과

BlueXP는 HA 쌍의 두 번째 노드에 볼륨을 생성합니다.



여러 AWS Availability Zone에 구축된 HA 쌍의 경우 볼륨이 상주하는 노드의 부동 IP 주소를 사용하여 볼륨을 클라이언트에 마운트해야 합니다.

## 볼륨을 생성한 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 사용해야 합니다. 할당량을 사용하면 사용자, 그룹 또는 qtree가 사용하는 파일 수와 디스크 공간을 제한하거나 추적할 수 있습니다.

## 기존 볼륨 관리

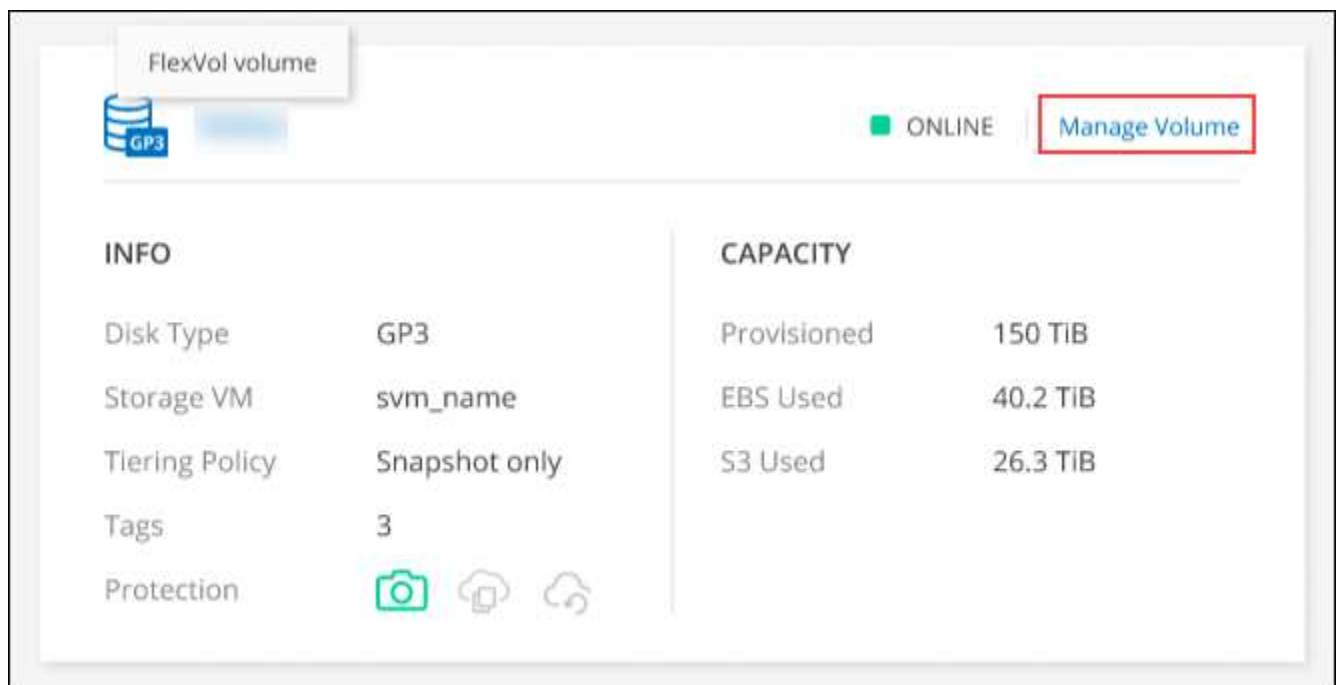
BlueXP를 사용하면 볼륨 및 CIFS 서버를 관리할 수 있습니다. 또한 용량 문제를 방지하기 위해 볼륨을 이동하라는 메시지가 표시됩니다.

### 볼륨 관리

스토리지 요구사항의 변화에 따라 볼륨을 관리할 수 있습니다. 볼륨을 보고, 편집하고, 클론, 복원 및 삭제할 수 있습니다.

#### 단계


1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 볼륨을 관리할 Cloud Volumes ONTAP 작업 환경을 두 번 클릭합니다.
3. 작업 환경에서 \* Volumes \* 탭을 클릭합니다.



4. Volumes(볼륨) 탭에서 원하는 볼륨 제목으로 이동한 다음 \* Manage volume(볼륨 관리) \* 을 클릭하여 Manage Volumes(볼륨 관리) 오른쪽 패널에 액세스합니다.

작업	조치
볼륨에 대한 정보를 봅니다	Manage volumes(볼륨 관리) 패널의 Volume Actions(볼륨 작업) 에서 * View volume details(볼륨 세부 정보 보기) * 를 클릭합니다.
NFS mount 명령을 가져옵니다	<ol style="list-style-type: none"> <li>a. 볼륨 관리 패널의 볼륨 작업 에서 * 탑재 명령 * 을 클릭합니다.</li> <li>b. 복사 * 를 클릭합니다.</li> </ol>

작업	조치
볼륨의 클론을 생성합니다	<p>a. Manage volumes(볼륨 관리) 패널의 Volume Actions(볼륨 작업) 에서 * Clone the volume(볼륨 복제) * 을 클릭합니다.</p> <p>b. 필요에 따라 클론 이름을 수정한 다음 * Clone * 을 클릭합니다.</p> <p>이 프로세스에서는 FlexClone 볼륨을 생성합니다. FlexClone 볼륨은 메타데이터에 작은 양의 공간을 사용하고 데이터가 변경 또는 추가됨에 따라 추가 공간만 사용하므로 공간 효율적인 쓰기 가능한 특정 시점 복사본입니다.</p> <p>FlexClone 볼륨에 대한 자세한 내용은 를 참조하십시오 "<a href="#">ONTAP 9 논리적 스토리지 관리 가이드</a>".</p>
볼륨 태그 편집(읽기-쓰기 볼륨만 해당)	<p>a. 볼륨 관리 패널의 볼륨 작업 에서 * 볼륨 태그 편집 * 을 클릭하여 선택한 볼륨에 할당된 볼륨 태그를 수정합니다.</p> <p>b. 제공된 필드에 볼륨 태그 키 및 값을 입력합니다.</p> <p>c. 추가 태그를 포함하려면 * 새 태그 추가 * 를 클릭합니다.</p> <p>d. 저장 * 을 클릭합니다.</p>
볼륨 편집(읽기-쓰기 볼륨만)	<p>a. 볼륨 관리 패널의 볼륨 작업 에서 * 볼륨 설정 편집 * 을 클릭합니다</p> <p>b. 볼륨의 스냅샷 정책, NFS 프로토콜 버전, NFS 액세스 제어 목록(엑스포트 정책) 또는 공유 권한을 수정한 다음 * 적용 * 을 클릭합니다.</p> <div data-bbox="609 1031 667 1094" style="border: 1px solid gray; border-radius: 50%; width: 36px; height: 36px; display: flex; align-items: center; justify-content: center; margin: 10px 0;"> <span style="font-size: 24px; font-weight: bold; color: #0070C0;">i</span> </div> <p style="margin-left: 40px;">사용자 지정 스냅샷 정책이 필요한 경우 System Manager를 사용하여 생성할 수 있습니다.</p>
볼륨을 삭제합니다	<p>a. Manage volumes(볼륨 관리) 패널의 Volume Actions(볼륨 작업) 에서 * Delete the volume(볼륨 삭제) * 을 클릭합니다.</p> <p>b. Delete Volume(볼륨 삭제) 창에서 삭제할 볼륨의 이름을 입력합니다.</p> <p>c. 확인하려면 * 삭제 * 를 다시 클릭합니다.</p>
필요 시 스냅샷 복사본을 생성합니다	<p>a. 볼륨 관리 패널의 보호 작업 에서 * 스냅샷 복사본 생성 * 을 클릭합니다.</p> <p>b. 필요한 경우 이름을 변경한 다음 * 만들기 * 를 클릭합니다.</p>
스냅샷 복사본에서 새 볼륨으로 데이터를 복원합니다	<p>a. Manage Volumes(볼륨 관리) 패널의 Protection Actions(보호 작업) 에서 * Restore from Snapshot copy(스냅샷 복사본에서 복원) * 를 클릭합니다.</p> <p>b. 스냅샷 복사본을 선택하고 새 볼륨의 이름을 입력한 다음 * 복원 * 을 클릭합니다.</p>

작업	조치
기본 디스크 유형을 변경합니다	<p>a. 볼륨 관리 패널의 고급 작업 아래에서 * 디스크 유형 변경 * 을 클릭합니다.</p> <p>b. 디스크 유형을 선택한 다음 * 변경 * 을 클릭합니다.</p> <p> BlueXP는 볼륨을 선택한 디스크 유형을 사용하는 기존 Aggregate로 이동하거나 볼륨에 대한 새 Aggregate를 생성합니다.</p>
계층화 정책을 변경합니다	<p>a. 볼륨 관리 패널의 고급 작업 에서 * 계층화 정책 변경 * 을 클릭합니다.</p> <p>b. 다른 정책을 선택하고 * 변경 * 을 클릭합니다.</p> <p> BlueXP는 계층화를 통해 선택한 디스크 유형을 사용하는 기존 Aggregate로 볼륨을 이동하거나 볼륨에 대한 새 Aggregate를 생성합니다.</p>
볼륨을 삭제합니다	<p>a. 볼륨을 선택한 다음 * 삭제 * 를 클릭합니다.</p> <p>b. 대화 상자에 볼륨의 이름을 입력합니다.</p> <p>c. 확인하려면 * 삭제 * 를 다시 클릭합니다.</p>

### 볼륨 크기를 조정합니다

기본적으로, 공간이 부족할 때 볼륨이 자동으로 최대 크기로 커집니다. 기본값은 1,000이며 이는 볼륨이 크기가 11배로 커질 수 있음을 의미합니다. 이 값은 커넥터 설정에서 구성할 수 있습니다.

볼륨 크기를 조정해야 하는 경우 에서 조정할 수 있습니다 ["ONTAP 시스템 관리자"](#). 볼륨 크기를 조정할 때 시스템의 용량 제한을 고려해야 합니다. 로 이동합니다 ["Cloud Volumes ONTAP 릴리즈 노트"](#) 를 참조하십시오.

### CIFS 서버를 수정합니다

DNS 서버 또는 Active Directory 도메인을 변경하는 경우 Cloud Volumes ONTAP에서 CIFS 서버를 수정하여 스토리지에서 클라이언트로 계속 서비스를 제공할 수 있도록 해야 합니다.

#### 단계

1. 작업 환경의 개요 탭에서 오른쪽 패널 아래의 기능 탭을 클릭합니다.
2. CIFS Setup(CIFS 설정) 필드에서 \* 연필 아이콘 \* 을 클릭하여 CIFS Setup(CIFS 설정) 창을 표시합니다.
3. CIFS 서버에 대한 설정을 지정합니다.

작업	조치
스토리지 VM(SVM) 선택	Cloud Volume ONTAP SVM(스토리지 가상 시스템)을 선택하면 구성된 CIFS 정보가 표시됩니다.
연결할 Active Directory 도메인입니다	CIFS 서버를 연결할 AD(Active Directory) 도메인의 FQDN입니다.

작업	조치
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.
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.  엔디프::GCP[]
DNS 도메인	SVM(Cloud Volumes ONTAP 스토리지 가상 머신)용 DNS 도메인 대부분의 경우 도메인은 AD 도메인과 동일합니다.
CIFS 서버 NetBIOS 이름입니다	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 구성 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다.  <ul style="list-style-type: none"> <li>• AWS 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 * OU=Computers, OU=Corp * 를 입력합니다.</li> <li>• Azure AD 도메인 서비스를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 * OU=ADDC 컴퓨터 * 또는 * OU=ADDC 사용자 * 를 입력합니다. "Azure 설명서: Azure AD 도메인 서비스 관리 도메인에 OU(조직 구성 단위)를 만듭니다"</li> <li>• Google 관리 Microsoft AD를 Cloud Volumes ONTAP용 AD 서버로 구성하려면 이 필드에 * OU=Computers, OU=Cloud * 를 입력합니다. "Google 클라우드 문서: Google Managed Microsoft AD의 조직 단위"</li> </ul>

4. Set \* 를 클릭합니다.

결과

Cloud Volumes ONTAP는 CIFS 서버를 변경 사항으로 업데이트합니다.

볼륨을 이동합니다

용량 활용률, 성능 향상, 서비스 수준 계약 충족을 위해 볼륨을 이동합니다.

볼륨 및 대상 애그리게이트를 선택하고, 볼륨 이동 작업을 시작하고, 선택적으로 볼륨 이동 작업을 모니터링하여 System Manager에서 볼륨을 이동할 수 있습니다. System Manager를 사용하면 볼륨 이동 작업이 자동으로 완료됩니다.

단계

1. System Manager 또는 CLI를 사용하여 볼륨을 애그리게이트로 이동합니다.

대부분의 경우 System Manager를 사용하여 볼륨을 이동할 수 있습니다.

자세한 내용은 를 참조하십시오 ["ONTAP 9 볼륨 이동 익스프레스 가이드"](#).

**BlueXP에 작업 필요 메시지가 표시되면 볼륨을 이동합니다**

용량 문제를 방지하려면 볼륨을 이동해야 하지만 직접 문제를 해결해야 한다는 작업 필요 메시지가 BlueXP에 표시될 수 있습니다. 이 경우 문제를 해결하는 방법을 식별한 다음 하나 이상의 볼륨을 이동해야 합니다.



BlueXP는 총 사용 용량이 90%에 도달하면 이러한 작업 필요 메시지를 표시합니다. 데이터 계층화를 사용할 경우 aggregate가 80% 사용 용량에 도달하면 메시지가 표시됩니다. 기본적으로 10%의 여유 공간은 데이터 계층화로 예약되어 있습니다. ["데이터 계층화를 위한 여유 공간 비율에 대해 자세히 알아보십시오"](#).

단계

1. 용량 문제를 해결하는 방법 파악.
2. 분석을 기초로 용량 문제를 방지하려면 볼륨을 이동하십시오.
  - 용량 문제를 방지하려면 볼륨을 다른 시스템으로 이동합니다.
  - 용량 문제를 방지하려면 볼륨을 다른 애그리게이트로 이동하십시오.

용량 문제를 해결하는 방법 파악

용량 문제를 방지하기 위해 BlueXP에서 볼륨 이동을 위한 권장 사항을 제공할 수 없는 경우 이동해야 할 볼륨과 동일한 시스템의 다른 aggregate 또는 다른 시스템으로 볼륨을 이동해야 하는지 여부를 확인해야 합니다.

단계

1. Action Required 메시지의 고급 정보를 확인하여 용량 제한에 도달한 애그리게이트를 식별합니다.

예를 들어, 고급 정보에는 Aggregate aggr1이 용량 제한에 도달했음을 나타냅니다.
2. 애그리게이트에서 이동할 하나 이상의 볼륨을 식별합니다.
  - a. 작업 환경에서 \* 집계 탭 \* 을 클릭합니다.
  - b. 원하는 집계 타일로 이동한 다음 \*... (타원 아이콘) > 애그리게이트 세부 정보 보기 \*.
  - c. Aggregate Details(집계 세부 정보) 화면의 Overview(개요) 탭에서 각 볼륨의 크기를 검토하고 aggregate에서 이동할 볼륨을 하나 이상 선택합니다.

나중에 추가 용량 문제를 방지할 수 있도록 aggregate에서 여유 공간을 확보하기 위해 충분히 큰 볼륨을 선택해야 합니다.



Aggregate Details	
aggr1	
Overview	Capacity Allocation
State	online
Home Node	iblog1-01
Encryption Type	cloudEncrypted
Volumes	2 ^
	www_iblog1_root (1 GiB)
	DATA01 (500 GiB)

3. 시스템이 디스크 제한에 도달하지 않은 경우 볼륨을 동일한 시스템의 기존 애그리게이트 또는 새 aggregate로 이동해야 합니다.

자세한 내용은 [을 참조하십시오 용량 문제를 방지하려면 볼륨을 다른 애그리게이트로 이동하십시오.](#)

4. 시스템이 디스크 제한에 도달한 경우 다음 중 하나를 수행합니다.

- 사용하지 않는 볼륨을 모두 삭제합니다.
- 볼륨을 재정렬하여 Aggregate의 여유 공간을 확보하십시오.

자세한 내용은 [을 참조하십시오 용량 문제를 방지하려면 볼륨을 다른 애그리게이트로 이동하십시오.](#)

- 둘 이상의 볼륨을 공간이 있는 다른 시스템으로 이동합니다.

자세한 내용은 [을 참조하십시오 용량 문제를 방지하려면 볼륨을 다른 애그리게이트로 이동하십시오.](#)

용량 문제를 방지하려면 볼륨을 다른 시스템으로 이동합니다

용량 문제를 방지하기 위해 하나 이상의 볼륨을 다른 Cloud Volumes ONTAP 시스템으로 이동할 수 있습니다. 시스템이 디스크 제한에 도달한 경우 이 작업을 수행해야 할 수 있습니다.

이 작업에 대해

이 작업의 단계를 따라 다음 작업 필요 메시지를 수정할 수 있습니다.

용량 문제를 방지하려면 볼륨을 이동해야 하지만 시스템이 디스크 제한에 도달했으므로 BlueXP에서 이 작업을 수행할 수 없습니다.

단계

1. 사용 가능한 용량이 있는 Cloud Volumes ONTAP 시스템을 식별하거나 새 시스템을 구축합니다.

2. 타겟 작업 환경에서 소스 작업 환경을 끌어다 놓아 볼륨의 일회성 데이터 복제를 수행합니다.

자세한 내용은 을 참조하십시오 ["시스템 간 데이터 복제"](#).

3. 복제 상태 페이지로 이동한 다음 SnapMirror 관계를 끊어서 복제된 볼륨을 데이터 보호 볼륨에서 읽기/쓰기 볼륨으로 변환합니다.

자세한 내용은 을 참조하십시오 ["데이터 복제 일정 및 관계 관리"](#).

4. 데이터 액세스를 위한 볼륨을 구성합니다.

데이터 액세스를 위한 대상 볼륨을 구성하는 방법에 대한 자세한 내용은 를 참조하십시오 ["ONTAP 9 볼륨 재해 복구 익스프레스 가이드"](#).

5. 원래 볼륨을 삭제합니다.

자세한 내용은 을 참조하십시오 ["볼륨 관리"](#).

용량 문제를 방지하려면 볼륨을 다른 애그리게이트로 이동하십시오

용량 문제를 방지하기 위해 하나 이상의 볼륨을 다른 aggregate로 이동할 수 있습니다.

이 작업에 대해

이 작업의 단계를 따라 다음 작업 필요 메시지를 수정할 수 있습니다.

용량 문제를 방지하려면 두 개 이상의 볼륨을 이동해야 하지만 BlueXP에서는 이 작업을 수행할 수 없습니다.

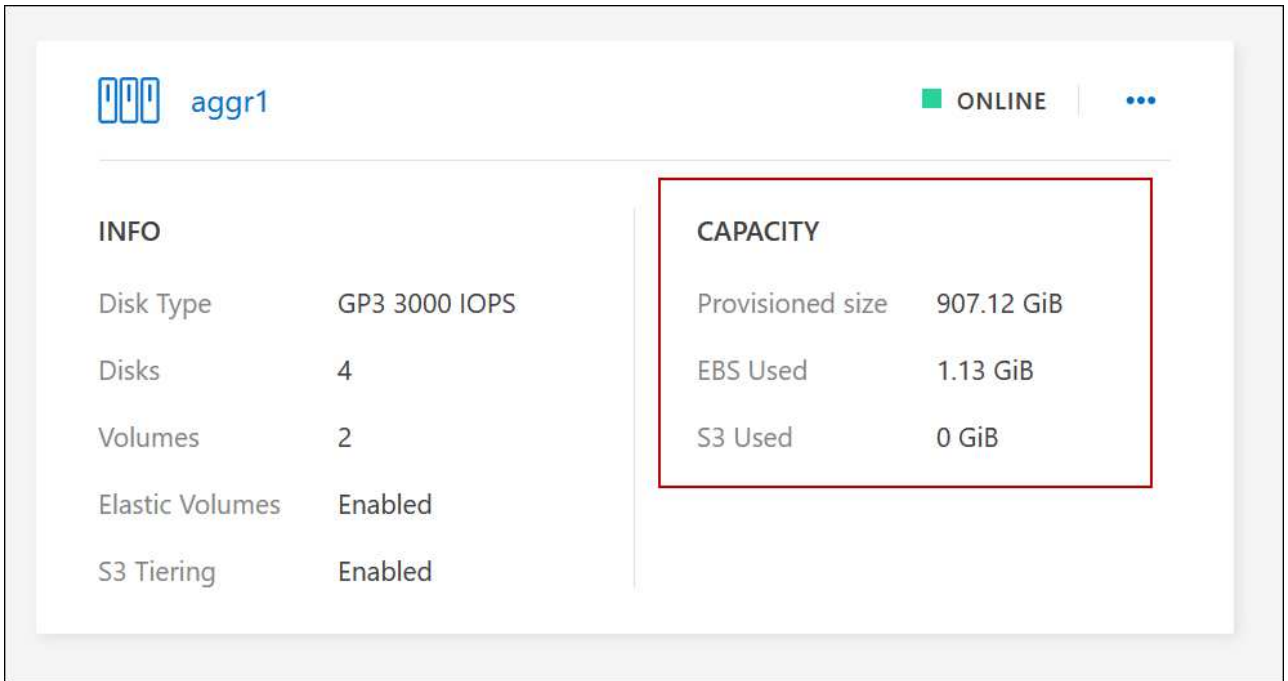
단계

1. 기존 Aggregate에 이동해야 하는 볼륨에 대해 사용 가능한 용량이 있는지 확인합니다.

a. 작업 환경에서 \* 집계 탭 \* 을 클릭합니다.

b. 원하는 집계 타일로 이동한 다음 \*... (타원 아이콘) > 애그리게이트 세부 정보 보기 \*.

c. 애그리게이트 타일에서 사용 가능한 용량(프로비저닝된 크기 - 사용된 애그리게이트 용량)을 확인합니다.



2. 필요한 경우 기존 애그리게이트에 디스크를 추가합니다.
  - a. 애그리게이트를 선택한 다음 \*... (타원 아이콘) > 디스크 추가 \*.
  - b. 추가할 디스크 수를 선택한 다음 \* 추가 \* 를 클릭합니다.
3. 가용 용량이 있는 애그리게이트가 없는 경우 새 애그리게이트를 생성합니다.  
자세한 내용은 [을 참조하십시오 "애그리게이트 생성"](#).
4. System Manager 또는 CLI를 사용하여 볼륨을 애그리게이트로 이동합니다.
5. 대부분의 경우 System Manager를 사용하여 볼륨을 이동할 수 있습니다.  
자세한 내용은 [를 참조하십시오 "ONTAP 9 볼륨 이동 익스프레스 가이드"](#).

#### 볼륨 이동이 느리게 수행될 수 있는 이유

Cloud Volumes ONTAP에 대해 다음 조건 중 하나가 참인 경우 볼륨을 이동하는 데 예상보다 시간이 오래 걸릴 수 있습니다.

- 볼륨이 클론입니다.
  - 볼륨이 클론의 부모입니다.
  - 소스 또는 대상 Aggregate에는 단일 Throughput Optimized HDD(st1) 디스크가 있습니다.
  - 애그리게이트 중 하나에서 객체에 대해 이전 명명 체계를 사용합니다. 두 애그리게이트 모두에서 같은 이름 형식을 사용해야 합니다.
- 9.4 릴리즈 이전 버전에서 데이터 계층화가 애그리게이트에서 활성화된 경우 이전 명명 체계가 사용됩니다.
- 소스 및 대상 애그리게이트에서 암호화 설정이 일치하지 않거나 키를 다시 입력하다
  - 계층화 정책을 변경하기 위해 볼륨 이동에 `_-Tiering-policy_option`이 지정되었습니다.

- 볼륨 이동 시 `_generate-destination-key_option`이 지정되었습니다.

## FlexGroup 볼륨을 봅니다

CLI 또는 System Manager를 통해 생성된 FlexGroup 볼륨은 BlueXP의 볼륨 탭을 통해 직접 볼 수 있습니다. FlexVol 볼륨에 대해 제공된 정보와 동일한 BlueXP는 전용 볼륨 타일을 통해 생성된 FlexGroup 볼륨에 대한 자세한 정보를 제공합니다. 볼륨 타일에서 아이콘의 호버 텍스트를 통해 각 FlexGroup 볼륨 그룹을 식별할 수 있습니다. 또한 볼륨 스타일 열을 통해 볼륨 목록 보기에서 FlexGroup 볼륨을 식별하고 정렬할 수 있습니다.

INFO		CAPACITY	
Disk Type	GP3	Provisioned	150 TiB
Storage VM	svm_name	EBS Used	40.2 TiB
Tiering Policy	Snapshot only	S3 Used	26.3 TiB
Tags	3		
Protection			



현재 BlueXP에서만 기존 FlexGroup 볼륨을 볼 수 있습니다. BlueXP에서 FlexGroup 볼륨을 생성하는 기능은 사용할 수 없지만 향후 릴리스에서 제공될 예정입니다.

## 비활성 데이터를 저비용 오브젝트 스토리지로 계층화

사용 빈도가 높은 데이터를 위한 SSD 또는 HDD 성능 계층과 비활성 데이터를 위한 오브젝트 스토리지 용량 계층을 결합하여 Cloud Volumes ONTAP의 스토리지 비용을 절감할 수 있습니다. 데이터 계층화는 FabricPool 기술을 기반으로 합니다. 개괄적인 개요는 을 참조하십시오 ["데이터 계층화 개요"](#).

데이터 계층화를 설정하려면 다음을 수행해야 합니다.

1

지원되는 구성을 선택합니다

대부분의 구성은 지원됩니다. 최신 버전을 실행하는 Cloud Volumes ONTAP 시스템이 있는 경우 실행하는 것이 좋습니다. ["자세한 정보"](#).

2

Cloud Volumes ONTAP와 오브젝트 스토리지 간의 연결을 보장합니다

- AWS의 경우 S3에 VPC 엔드 포인트가 필요합니다. [자세한 정보](#).
- Azure의 경우 BlueXP에 필요한 권한이 있으면 아무 작업도 수행할 필요가 없습니다. [자세한 정보](#).
- Google Cloud의 경우, 전용 Google Access에 대한 서브넷을 구성하고 서비스 계정을 설정해야 합니다. [자세한 정보](#).

3

계층화가 설정된 **Aggregate**가 있는지 확인합니다

볼륨에서 데이터 계층화를 사용하려면 애그리게이트에서 데이터 계층화를 활성화해야 합니다. 새 볼륨 및 기존 볼륨에 대한 요구사항을 알고 있어야 합니다. [자세한 정보](#).

4

볼륨을 생성, 수정 또는 복제할 때 계층화 정책을 선택합니다

볼륨을 생성, 수정 또는 복제할 때 BlueXP에서 계층화 정책을 선택하라는 메시지가 표시됩니다.

- "읽기-쓰기 볼륨의 데이터 계층화"
- "데이터 보호 볼륨의 데이터 계층화"

데이터 계층화에 필요하지 않은'은 무엇입니까?

- 데이터 계층화를 사용하기 위해 기능 라이선스를 설치할 필요가 없습니다.
- 용량 계층에 대해 오브젝트 저장소를 생성할 필요가 없습니다. BlueXP가 이러한 작업을 수행합니다.
- 시스템 레벨에서 데이터 계층화를 설정할 필요가 없습니다.

i

BlueXP는 시스템이 생성될 때 콜드 데이터에 대한 오브젝트 저장소를 생성합니다. [연결 또는 사용 권한 문제가 없는 경우](#). 그런 다음 볼륨에 대해 데이터 계층화를 활성화해야 합니다. 경우에 따라 [애그리게이트](#))를 클릭합니다.

데이터 계층화를 지원하는 구성

특정 구성 및 기능을 사용할 때 데이터 계층화를 설정할 수 있습니다.

**AWS** 지원

- Cloud Volumes ONTAP 9.2부터 AWS에서 데이터 계층화가 지원됩니다.
- 성능 계층은 범용 SSD(GP3 또는 GP2) 또는 프로비저닝된 IOPS SSD(io1)일 수 있습니다.

i

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

**Azure**에서 지원

- 데이터 계층화는 다음과 같이 Azure에서 지원됩니다.
  - 단일 노드 시스템의 경우 버전 9.4인치
  - HA 쌍이 포함된 버전 9.6인치

- 성능 계층은 프리미엄 SSD 관리 디스크, 표준 SSD 관리 디스크 또는 표준 HDD 관리 디스크일 수 있습니다.

#### Google Cloud 지원

- 데이터 계층화는 Cloud Volumes ONTAP 9.6부터 Google Cloud에서 지원됩니다.
- 성능 계층은 SSD 영구 디스크, 균형 잡힌 영구 디스크 또는 표준 영구 디스크일 수 있습니다.

#### 기능 상호 운용성

- 데이터 계층화는 암호화 기술을 통해 지원됩니다.
- 볼륨에 씬 프로비저닝이 설정되어 있어야 합니다.

#### 요구 사항

클라우드 공급자에 따라 Cloud Volumes ONTAP에서 콜드 데이터를 오브젝트 스토리지에 계층화할 수 있도록 특정 연결과 사용 권한을 설정해야 합니다.

#### 콜드 데이터를 **AWS S3**에 계층화해야 하는 요구 사항

Cloud Volumes ONTAP가 S3에 연결되어 있는지 확인합니다. 이 연결을 제공하는 가장 좋은 방법은 S3 서비스에 VPC 엔드포인트를 생성하는 것입니다. 자세한 내용은 [을 참조하십시오 "AWS 설명서: 게이트웨이 엔드포인트 생성"](#).

VPC 끝점을 만들 때 Cloud Volumes ONTAP 인스턴스에 해당하는 영역, VPC 및 라우팅 테이블을 선택해야 합니다. 또한 S3 엔드포인트에 대한 트래픽을 활성화하는 아웃바운드 HTTPS 규칙을 추가하려면 보안 그룹을 수정해야 합니다. 그렇지 않으면 Cloud Volumes ONTAP에서 S3 서비스에 연결할 수 없습니다.

문제가 발생하면 [을 참조하십시오 "AWS 지원 지식 센터: 게이트웨이 VPC 엔드포인트를 사용하여 S3 버킷에 연결할 수 없는 이유는 무엇입니까?"](#).

#### 콜드 데이터를 **Azure Blob** 저장소에 계층화하기 위한 요구사항

BlueXP에 필요한 권한이 있는 경우 성능 계층과 용량 계층 간에 연결을 설정할 필요가 없습니다. BlueXP는 Connector의 사용자 지정 역할에 다음과 같은 권한이 있는 경우 VNET 서비스 끝점을 활성화합니다.

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

사용 권한은 기본적으로 사용자 지정 역할에 포함됩니다. ["Connector에 대한 Azure 권한을 봅니다"](#)

#### 콜드 데이터를 **Google Cloud Storage** 버킷에 계층화해야 하는 요구 사항

- Cloud Volumes ONTAP가 상주하는 서브넷은 개인 Google 액세스용으로 구성해야 합니다. 자세한 지침은 [을 참조하십시오 "Google Cloud 설명서: 개인 Google Access 구성"](#).
- 서비스 계정을 Cloud Volumes ONTAP에 연결해야 합니다.

["이 서비스 계정을 설정하는 방법에 대해 알아보십시오"](#).

Cloud Volumes ONTAP 작업 환경을 생성할 때 이 서비스 계정을 선택하라는 메시지가 표시됩니다.

배포 중에 서비스 계정을 선택하지 않으면 Cloud Volumes ONTAP을 종료하고 Google Cloud 콘솔로 이동한 다음 Cloud Volumes ONTAP 인스턴스에 서비스 계정을 연결해야 합니다. 그런 다음 다음 다음 다음 섹션에 설명된 대로 데이터 계층화를 설정할 수 있습니다.

- 고객이 관리하는 암호화 키로 버킷을 암호화하려면 Google Cloud 스토리지 버킷에서 키를 사용할 수 있습니다.

["Cloud Volumes ONTAP에서 고객이 관리하는 암호화 키를 사용하는 방법에 대해 알아보십시오"](#).

요구사항을 구현한 후 데이터 계층화를 사용하도록 설정

BlueXP는 연결 또는 사용 권한 문제가 없는 한 시스템이 생성될 때 콜드 데이터에 대한 개체 저장소를 생성합니다. 시스템을 생성하기 전까지는 위에 나열된 요구 사항을 구현하지 않았다면 개체 저장소를 생성하는 API 또는 System Manager를 통해 계층화를 수동으로 활성화해야 합니다.



BlueXP 사용자 인터페이스를 통해 계층화를 활성화하는 기능은 향후 Cloud Volumes ONTAP 릴리스에서 제공될 예정입니다.

애그리게이트에서 계층화가 설정되었는지 확인합니다

볼륨에서 데이터 계층화를 사용하려면 애그리게이트에서 데이터 계층화를 활성화해야 합니다. 새 볼륨 및 기존 볼륨에 대한 요구사항을 알고 있어야 합니다.

- \* 새 볼륨 \*

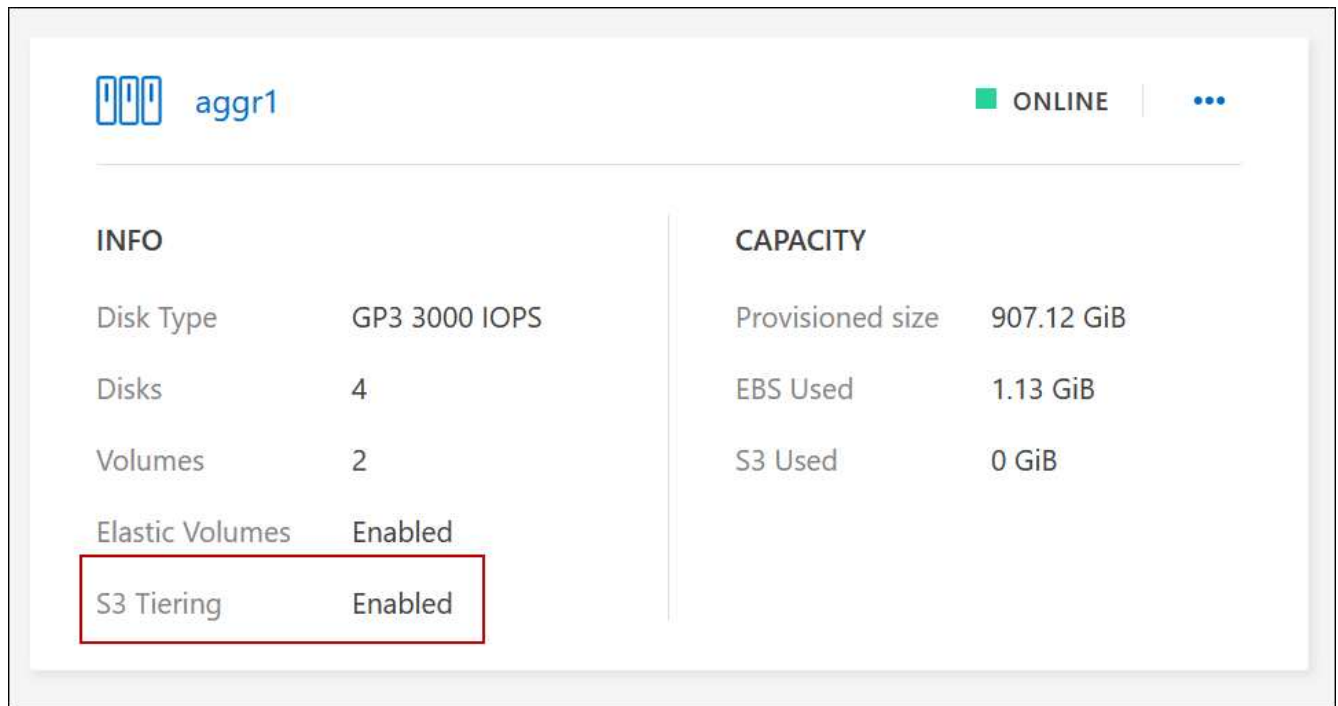
새 볼륨에서 데이터 계층화를 사용하는 경우에는 애그리게이트에서 데이터 계층화를 사용할 필요가 없습니다. BlueXP는 계층화가 활성화된 기존 애그리게이트에 볼륨을 생성하거나, 데이터 계층화가 활성화된 애그리게이트가 아직 존재하지 않는 경우 볼륨에 대한 새 애그리게이트를 생성합니다.

- \* 기존 볼륨 \*

기존 볼륨에서 데이터 계층화를 사용하려면 기본 애그리게이트에 데이터 계층화가 설정되어 있는지 확인해야 합니다. 기존 애그리게이트에서 데이터 계층화를 사용하지 않는 경우 System Manager를 사용하여 기존 애그리게이트를 오브젝트 저장소에 연결해야 합니다.

**Aggregate**에서 계층화가 설정되었는지 확인하는 단계입니다

1. BlueXP에서 작업 환경을 엽니다.
2. 애그리게이트 탭을 클릭합니다.
3. 원하는 타일로 이동하여 애그리게이트에서 계층화가 설정되었는지 여부를 확인합니다.



**Aggregate**에서 계층화를 활성화하는 단계입니다

1. System Manager에서 \* Storage > Tiers \* 를 클릭합니다.
2. Aggregate에 대한 작업 메뉴를 클릭하고 \* Attach Cloud Tiers \* 를 선택합니다.
3. 연결할 클라우드 계층을 선택하고 \* 저장 \* 을 클릭합니다.

다음 단계

이제 다음 섹션에 설명된 대로 새 볼륨과 기존 볼륨에 대해 데이터 계층화를 설정할 수 있습니다.

읽기-쓰기 볼륨의 데이터 계층화

Cloud Volumes ONTAP는 읽기-쓰기 볼륨의 비활성 데이터를 비용 효율적인 오브젝트 스토리지에 계층화하여 핫 데이터에 대한 성능 계층을 확보할 수 있습니다.

단계

1. 작업 환경의 볼륨 탭에서 새 볼륨을 생성하거나 기존 볼륨의 계층을 변경합니다.

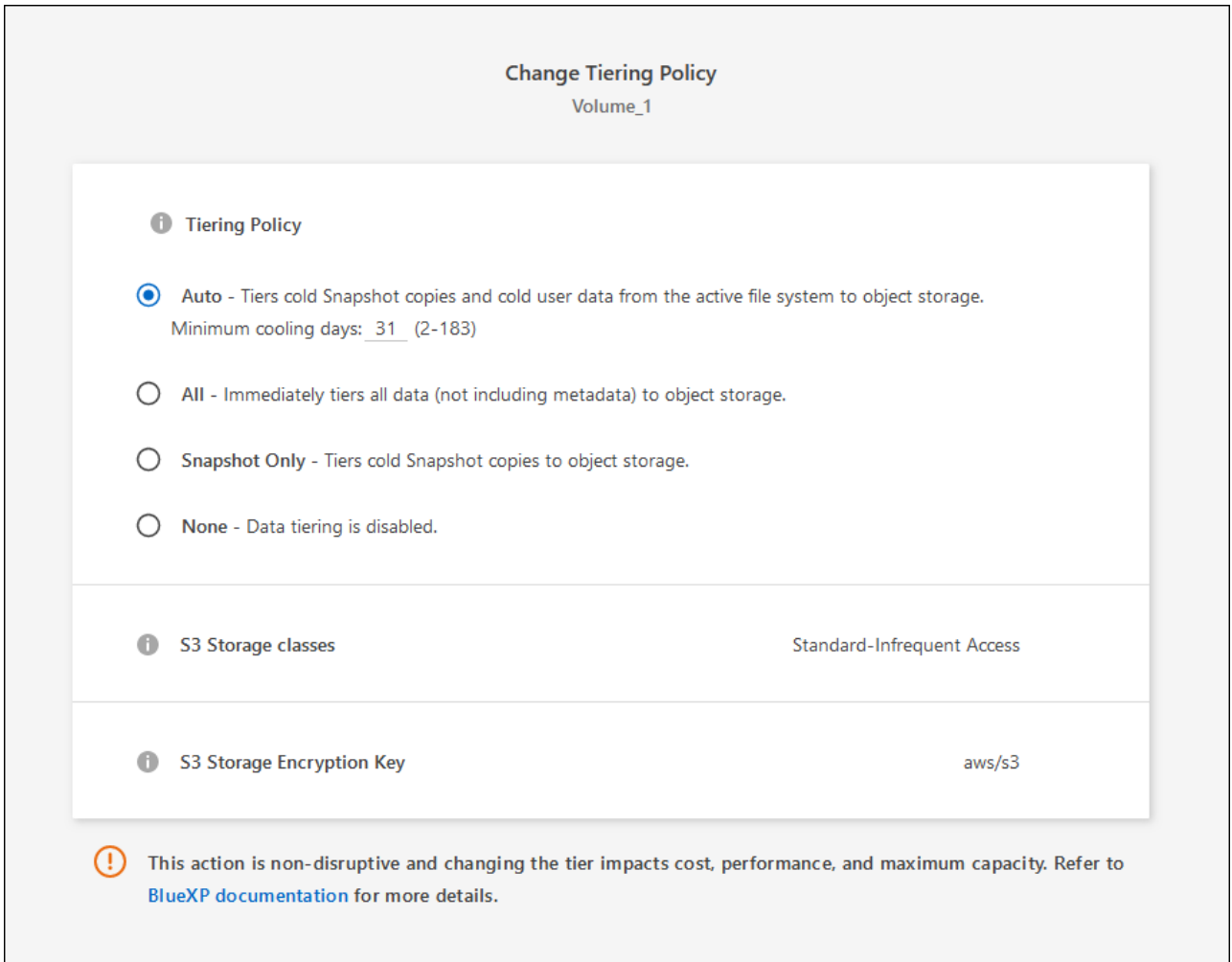
작업	조치
새 볼륨을 생성합니다	새 볼륨 추가 * 를 클릭합니다.
기존 볼륨을 수정합니다	원하는 볼륨 타일을 선택하고 * 볼륨 관리 * 를 클릭하여 볼륨 관리 오른쪽 패널에 액세스한 다음 오른쪽 패널에서 * 고급 작업 * 및 * 계층화 정책 변경 * 을 클릭합니다.

2. 계층화 정책을 선택합니다.

이러한 정책에 대한 설명은 를 참조하십시오 ["데이터 계층화 개요"](#).

- 예 \*





데이터 계층화가 활성화된 애그리게이트가 아직 존재하지 않는 경우 BlueXP는 볼륨에 대한 새로운 애그리게이트를 생성합니다.

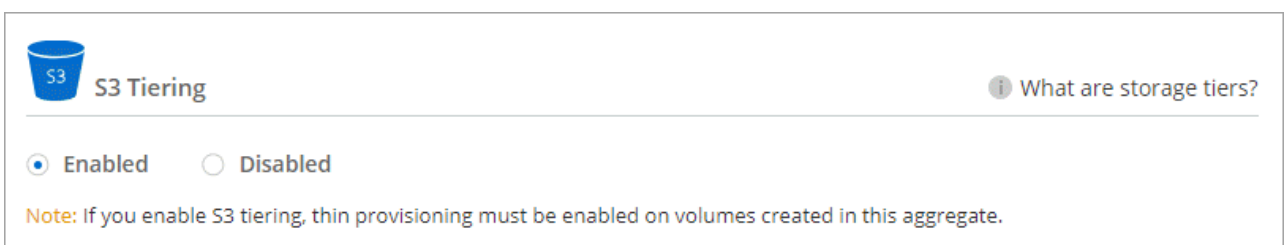
### 데이터 보호 볼륨에서 데이터 계층화

Cloud Volumes ONTAP는 데이터 보호 볼륨의 데이터를 용량 계층으로 계층화할 수 있습니다. 대상 볼륨을 활성화하면 데이터가 읽혀지면서 성능 계층으로 서서히 이동합니다.

### 단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 소스 볼륨이 포함된 작업 환경을 선택한 다음 볼륨을 복제할 작업 환경으로 끌어다 놓습니다.
3. 표시되는 메시지에 따라 계층화 페이지로 이동한 다음 오브젝트 스토리지에 데이터 계층화를 설정합니다.

◦ 예 \*



데이터 복제에 대한 도움말은 을 참조하십시오 "[클라우드 간 데이터 복제](#)".

## 계층화된 데이터에 대한 스토리지 클래스 변경

Cloud Volumes ONTAP를 구축한 후 30일 동안 액세스하지 않은 비활성 데이터의 스토리지 클래스를 변경하여 스토리지 비용을 절감할 수 있습니다. 데이터에 액세스하는 경우 액세스 비용이 더 높아지므로 스토리지 클래스를 변경하기 전에 액세스 비용을 고려해야 합니다.

계층형 데이터를 위한 스토리지 클래스는 시스템 전체에 적용됩니다. 즉, 볼륨을 기준으로 하지 않습니다.

지원되는 스토리지 클래스에 대한 자세한 내용은 를 참조하십시오 "[데이터 계층화 개요](#)".

### 단계

1. 작업 환경에서 메뉴 아이콘을 클릭한 다음 \* 스토리지 클래스 \* 또는 \* Blob 스토리지 계층화 \* 를 클릭합니다.
2. 스토리지 클래스를 선택한 다음 \* 저장 \* 을 클릭합니다.

## 데이터 계층화의 사용 가능한 공간 비율을 변경합니다

데이터 계층화를 위한 여유 공간 비율은 데이터를 오브젝트 스토리지로 계층화할 때 Cloud Volumes ONTAP SSD/HDD에 필요한 여유 공간을 정의합니다. 기본 설정은 10%의 여유 공간이지만 요구 사항에 따라 설정을 조정할 수 있습니다.

예를 들어, 구입한 용량을 사용하기 위해 10% 미만의 여유 공간을 선택할 수 있습니다. 그런 다음 BlueXP는 추가 용량이 필요할 때 추가 디스크를 구입할 수 있습니다(최대 Aggregate의 디스크 한도에 도달할 때까지).

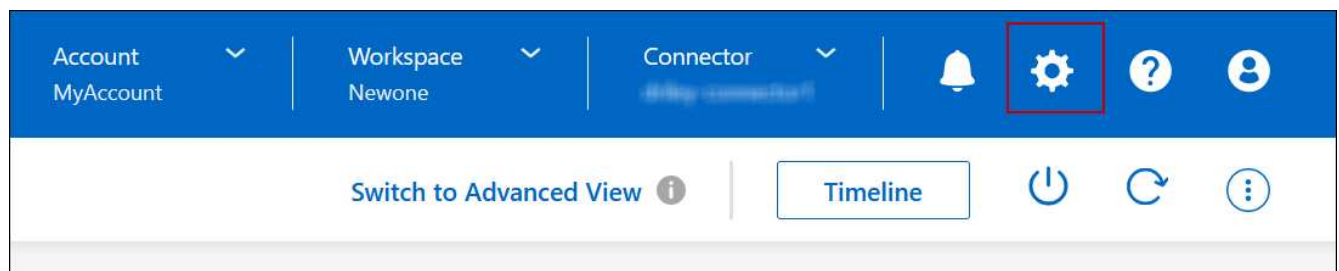


공간이 부족하면 Cloud Volumes ONTAP에서 데이터를 이동할 수 없어 성능이 저하될 수 있습니다. 모든 변경은 신중하게 수행해야 합니다. 확실하지 않은 경우 NetApp 지원 팀에 연락하여 안내를 받으십시오.

이 비율은 오브젝트 저장소에서 데이터를 읽을 때 Cloud Volumes ONTAP 더 나은 성능을 제공하기 위해 데이터를 SSD/HDD로 이동하기 때문에 재해 복구 시나리오에 중요합니다. 공간이 부족하면 Cloud Volumes ONTAP에서 데이터를 이동할 수 없습니다. 이 점을 고려하여 비율을 변경하면 비즈니스 요구 사항을 충족할 수 있습니다.

### 단계

1. BlueXP 콘솔의 오른쪽 상단에서 \* 설정 \* 아이콘을 클릭하고 \* 커넥터 설정 \* 을 선택합니다.



2. Capacity \* 에서 \* Aggregate Capacity Thresholds - Free Space Ratio for Data Tiering \* 을 클릭합니다.
3. 요구 사항에 따라 여유 공간 비율을 변경하고 \* Save \* 를 클릭합니다.

## 자동 계층화 정책의 냉각 기간 변경

Cloud Volumes ONTAP 볼륨에서 `_auto_Tiering` 정책을 사용하여 데이터 계층화를 활성화한 경우 비즈니스 요구에 따라 기본 냉각 기간을 조정할 수 있습니다. 이 작업은 API 및 CLI에서만 지원됩니다.

냉각 기간은 볼륨의 사용자 데이터가 "콜드" 상태로 간주되어 오브젝트 스토리지로 이동되기 전에 비활성 상태로 유지해야 하는 일 수입니다.

자동 계층화 정책의 기본 냉각 기간은 31일입니다. 냉각 기간을 다음과 같이 변경할 수 있습니다.

- 9.8 이상: 2일에서 183일
- 9.7 이하: 2일~63일

### 단계

1. 볼륨을 생성하거나 기존 볼륨을 수정할 때 API 요청과 함께 `_minimumCoolingDays_` 매개 변수를 사용하십시오.

## LUN을 호스트에 연결합니다

iSCSI 볼륨을 생성할 때 BlueXP에서 자동으로 LUN을 생성합니다. NetApp은 볼륨당 하나의 LUN만 생성하므로 관리가 필요하지 않습니다. 볼륨을 생성한 후 IQN을 사용하여 호스트에서 LUN에 연결합니다.

다음 사항에 유의하십시오.

- BlueXP의 자동 용량 관리는 LUN에 적용되지 않습니다. BlueXP에서 LUN을 생성하면 자동 확장 기능이 비활성화됩니다.
- System Manager 또는 CLI에서 추가 LUN을 생성할 수 있습니다.

### 단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 볼륨을 관리할 Cloud Volumes ONTAP 작업 환경을 두 번 클릭합니다.
3. 작업 환경에서 \* Volumes \* 탭을 클릭합니다.
4. Volumes(볼륨) 탭에서 원하는 볼륨 제목으로 이동한 다음 \* Manage volume(볼륨 관리) \* 을 클릭하여 Manage Volumes(볼륨 관리) 오른쪽 패널에 액세스합니다.
5. 대상 IQN \* 을 클릭합니다.
6. IQN 이름을 복사하려면 \* Copy \* 를 클릭합니다.
7. 호스트에서 LUN으로의 iSCSI 접속을 설정합니다.
  - ["Red Hat Enterprise Linux용 ONTAP 9 iSCSI Express 구성: 대상으로 iSCSI 세션 시작"](#)
  - ["Windows용 ONTAP 9 iSCSI Express 구성: 타겟으로 iSCSI 세션 시작"](#)
  - ["ONTAP SAN 호스트 구성"](#)

## FlexCache 볼륨을 사용하여 데이터 액세스 가속화

FlexCache 볼륨은 원본(또는 소스) 볼륨에서 SMB 및 NFS 읽기 데이터를 캐싱하는 스토리지 볼륨입니다. 이후에 캐싱된 데이터를 읽으면 해당 데이터에 더 빠르게 액세스할 수 있습니다.

FlexCache 볼륨을 사용하면 데이터 액세스 속도를 높이거나 자주 액세스하는 볼륨에서 트래픽을 오프로드할 수 있습니다. FlexCache 볼륨은 원본 볼륨에 액세스하지 않고도 직접 데이터를 제공할 수 있으므로 클라이언트가 동일한 데이터에 반복적으로 액세스해야 할 때 성능을 개선할 수 있습니다. FlexCache 볼륨은 읽기 집약적인 시스템 워크로드에 적합합니다.

BlueXP는 를 사용하여 FlexCache 볼륨을 관리할 수 있는 기능을 제공합니다 "BlueXP 볼륨 캐싱" 서비스.

ONTAP CLI 또는 ONTAP System Manager를 사용하여 FlexCache 볼륨을 생성하고 관리할 수도 있습니다.

- "빠른 데이터 액세스를 위한 FlexCache 볼륨 전원 가이드"
- "System Manager에서 FlexCache 볼륨 생성"

BlueXP는 모든 새로운 Cloud Volumes ONTAP 시스템에 대한 FlexCache 라이선스를 생성합니다. 이 라이선스에는 500GiB 사용 제한이 포함됩니다.



## 통합 관리

### 애그리게이트 생성

볼륨을 생성할 때 직접 애그리게이트를 생성하거나 BlueXP에서 자동으로 집계하도록 할 수 있습니다. 애그리게이트를 직접 생성할 때의 이점은 기본 디스크 크기를 선택할 수 있다는 것입니다. 이를 통해 필요한 용량 또는 성능에 맞게 애그리게이트 크기를 조정할 수 있습니다.



모든 디스크와 애그리게이트는 BlueXP에서 직접 생성 및 삭제해야 합니다. 다른 관리 도구에서 이러한 작업을 수행해서는 안 됩니다. 이렇게 하면 시스템 안정성에 영향을 주고 향후 디스크를 추가할 수 없도록 하며 중복 클라우드 공급자 비용을 생성할 수 있습니다.

## 단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 집계를 관리할 Cloud Volumes ONTAP 인스턴스의 이름을 두 번 클릭합니다.
3. 애그리게이트 탭에서 \* 애그리게이트 추가 \* 를 클릭한 다음 애그리게이트의 세부 정보를 지정합니다.

## 설치하고

- 디스크 유형과 디스크 크기를 선택하라는 메시지가 표시되면 을 참조하십시오 "[AWS에서 Cloud Volumes ONTAP 구성 계획](#)".
- 애그리게이트의 용량 크기를 입력하라는 메시지가 표시되면 Amazon EBS Elastic Volumes 기능을 지원하는 구성에 애그리게이트를 생성합니다. 다음 스크린샷은 GP3 디스크로 구성된 새로운 Aggregate의 예를 보여줍니다.

The screenshot displays the 'Select Disk Type' interface in the AWS console. At the top, there are four numbered steps: 1. Disk Type, 2. Aggregate details, 3. Tiering Data, and 4. Review. The main heading is 'Select Disk Type'. Below it, a 'Disk Type' dropdown menu is set to 'GP3 - General Purpose SSD Dynamic Performance'. A detailed view for 'General Purpose SSD (gp3) Disk Properties' is shown, including a description: 'General purpose SSD volume that balances price and performance (performance level is independent of storage capacity)'. Two input fields are visible: 'IOPS Value' set to 12000 and 'Throughput MB/s' set to 250.

"[Elastic Volumes 지원에 대해 자세히 알아보십시오](#)".

## Azure를 지원합니다

디스크 유형 및 디스크 크기에 대한 도움말은 을 참조하십시오 "[Azure에서 Cloud Volumes ONTAP 구성 계획](#)".

## Google 클라우드

디스크 유형 및 디스크 크기에 대한 도움말은 을 참조하십시오 "[Google Cloud에서 Cloud Volumes ONTAP 구성을 계획하십시오](#)".

4. Go \* 를 클릭한 다음 \* Approve and Purchase \* 를 클릭합니다.

## 애그리게이트 관리

디스크를 추가하고, 애그리게이트에 대한 정보를 확인하고, 삭제하여 애그리게이트를 직접 관리하십시오.



모든 디스크와 애그리게이트는 BlueXP에서 직접 생성 및 삭제해야 합니다. 다른 관리 도구에서 이러한 작업을 수행해서는 안 됩니다. 이렇게 하면 시스템 안정성에 영향을 주고 향후 디스크를 추가할 수 없도록 하며 중복 클라우드 공급자 비용을 생성할 수 있습니다.

시작하기 전에

Aggregate를 삭제하려면 먼저 Aggregate의 볼륨을 삭제해야 합니다.

이 작업에 대해


Aggregate에 공간이 부족할 경우 System Manager를 사용하여 볼륨을 다른 애그리게이트로 이동할 수 있습니다.

단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 집계를 관리할 Cloud Volumes ONTAP 작업 환경을 두 번 클릭합니다.
3. 작업 환경에서 \* 집계 \* 탭을 클릭합니다.
4. 애그리게이트 탭에서 원하는 제목으로 이동한 다음 \*... (타원 아이콘) \*.

INFO		CAPACITY	
Disk Type	GP3 3000 IOPS	Provisioned size	907.12 GiB
Disks	4	EBS Used	1.13 GiB
Volumes	2	S3 Used	0 GiB
Elastic Volumes	Enabled		
S3 Tiering	Enabled		

5. 애그리게이트 관리:

작업	조치
Aggregate에 대한 정보를 봅니다	아래에서... (타원 아이콘) 메뉴에서 * 애그리게이트 세부 정보 보기 * 를 클릭합니다.
특정 Aggregate에 볼륨을 생성합니다	아래에서... (타원 아이콘) 메뉴에서 * 볼륨 추가 * 를 클릭합니다.
Aggregate에 디스크를 추가합니다	<p>a. 아래에서... (타원 아이콘) 메뉴에서 * 디스크 추가 * 를 클릭합니다.</p> <p>b. 추가할 디스크 수를 선택하고 * 추가 * 를 클릭합니다.</p> <p> Aggregate의 모든 디스크는 동일한 크기여야 합니다.</p>
Amazon EBS Elastic Volumes를 지원하는 애그리게이트의 용량을 늘립니다	<p>a. 아래에서... (타원 아이콘) 메뉴에서 * 용량 증가 * 를 클릭합니다.</p> <p>b. 추가할 추가 용량을 입력한 다음 * 증가 * 를 클릭합니다.</p> <p>Aggregate의 용량을 최소 256GiB 또는 애그리게이트 크기의 10% 이상으로 늘려야 합니다.</p> <p>예를 들어 1.77TiB Aggregate가 있는 경우 10%는 181GiB입니다. 이 값이 256GiB보다 낮으므로 애그리게이트의 크기를 최소 256GiB까지 늘려야 합니다.</p>
애그리게이트 삭제	<p>a. 볼륨을 포함하지 않는 집계 타일을 선택합니다. *...를 클릭합니다. (타원 아이콘) &gt; 삭제 *.</p> <p>b. 확인하려면 * 삭제 * 를 다시 클릭합니다.</p>

## 커넥터의 용량 설정을 관리합니다

각 커넥터에는 Cloud Volumes ONTAP의 총 용량을 관리하는 방법을 결정하는 설정이 있습니다.

이러한 설정은 커넥터에 의해 관리되는 모든 Cloud Volumes ONTAP 시스템에 영향을 줍니다. 다른 커넥터가 있는 경우 다르게 구성할 수 있습니다.

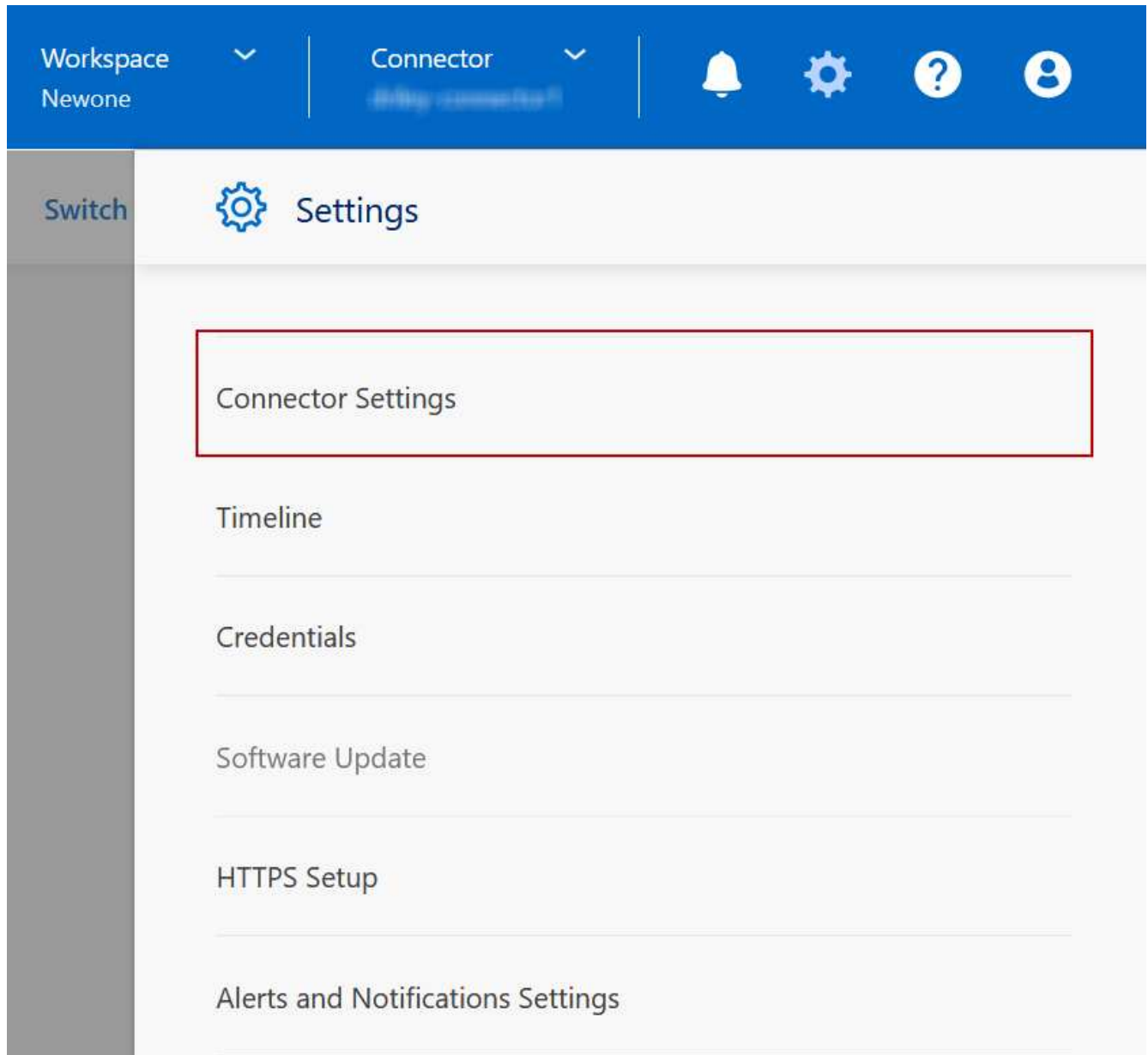
### 필수 권한

커넥터 설정을 수정하려면 계정 관리자 권한이 필요합니다.

### 단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 클릭하고 \* 커넥터 설정 \* 을 선택합니다.





2. Capacity \* 에서 다음 설정을 수정합니다.

#### 용량 관리 모드

BlueXP에서 스토리지 용량 결정을 통지할지 아니면 BlueXP에서 자동으로 용량 요구 사항을 관리할지 여부를 선택합니다.

["용량 관리 모드의 작동 방식에 대해 알아보십시오"](#).

#### 애그리게이트 용량 임계값 - 사용 가능한 공간 비율

Aggregate의 여유 공간 비율이 지정된 임계값 아래로 떨어지면 알림을 트리거합니다.

여유 공간 비율은 다음과 같이 계산됩니다.

(Aggregate capacity - 애그리게이트에서 사용하는 총 용량입니다.) / 애그리게이트 용량입니다

### Aggregate Capacity Thresholds - Data Tiering의 여유 공간 비율입니다

데이터를 용량 계층(오브젝트 스토리지)으로 계층화할 때 성능 계층(디스크)에 필요한 여유 공간을 정의합니다.

이 비율은 재해 복구 시나리오에 중요합니다. 용량 계층에서 데이터를 읽으면 Cloud Volumes ONTAP는 더 나은 성능을 제공하기 위해 데이터를 성능 계층으로 이동합니다. 공간이 부족하면 Cloud Volumes ONTAP에서 데이터를 이동할 수 없습니다.

3. 저장 \* 을 클릭합니다.

## 스토리지 VM 관리

### BlueXP에서 스토리지 VM 관리

스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에 스토리지 및 데이터 서비스를 제공합니다. 이를 SVM 또는 `_vserver_`로 알고 있을 수 있습니다. Cloud Volumes ONTAP는 기본적으로 하나의 스토리지 VM으로 구성되지만 일부 구성에서는 추가 스토리지 VM을 지원합니다.

지원되는 스토리지 VM 수입니다

특정 구성에서는 여러 스토리지 VM이 지원됩니다. 로 이동합니다 "[Cloud Volumes ONTAP 릴리즈 노트](#)" 사용 중인 Cloud Volumes ONTAP 버전에 대해 지원되는 스토리지 VM 수를 확인하려면 다음을 수행합니다.

여러 스토리지 VM과 함께 작업

BlueXP는 System Manager 또는 CLI에서 생성한 추가 스토리지 VM을 지원합니다.

예를 들어, 다음 이미지는 볼륨을 생성할 때 스토리지 VM을 선택하는 방법을 보여줍니다.

### Details & Protection

Storage VM Name ?

svm\_name1 ▼

Volume Name Size (GiB) ?

Snapshot Policy

default ▼

? Default Policy

다음 이미지는 다른 시스템으로 볼륨을 복제할 때 스토리지 VM을 선택하는 방법을 보여 줍니다.

Destination Volume Name

volume\_copy

Destination Storage VM Name

svm\_name1 ▼

Destination Aggregate

Automatically select the best aggregate ▼

기본 스토리지 **VM**의 이름을 수정합니다

BlueXP는 Cloud Volumes ONTAP용으로 생성한 단일 스토리지 VM의 이름을 자동으로 지정합니다. 엄격한 명명 규칙이 있는 경우 System Manager, CLI 또는 API에서 스토리지 VM 이름을 수정할 수 있습니다. 예를 들어, 이름이 ONTAP 클러스터에 대한 스토리지 VM의 이름을 지정하는 방법과 일치할 수 있습니다.

## AWS에서 Cloud Volumes ONTAP를 위한 데이터 서비스 스토리지 VM을 생성합니다

스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에 스토리지 및 데이터 서비스를 제공합니다. 이를 SVM 또는 `_vserver_`로 알고 있을 수 있습니다. Cloud Volumes ONTAP는 기본적으로 하나의 스토리지 VM으로 구성되지만 일부 구성에서는 추가 스토리지 VM을 지원합니다.

추가 데이터 서비스 스토리지 VM을 생성하려면 AWS에서 IP 주소를 할당한 다음 Cloud Volumes ONTAP 구성에 따라 ONTAP 명령을 실행해야 합니다.

지원되는 스토리지 VM 수입니다

9.7 릴리즈부터 특정 Cloud Volumes ONTAP 구성에서 여러 스토리지 VM이 지원됩니다. 로 이동합니다 "[Cloud Volumes ONTAP 릴리즈 노트](#)" 사용 중인 Cloud Volumes ONTAP 버전에 대해 지원되는 스토리지 VM 수를 확인하려면 다음을 수행합니다.

다른 모든 Cloud Volumes ONTAP 구성에서는 재해 복구에 사용되는 1개의 데이터 서비스 스토리지 VM과 1개의 대상 스토리지 VM을 지원합니다. 소스 스토리지 VM에 중단이 발생할 경우 데이터 액세스를 위해 대상 스토리지 VM을 활성화할 수 있습니다.

구성에 대한 제한을 확인합니다

각 EC2 인스턴스는 네트워크 인터페이스당 최대 수의 전용 IPv4 주소를 지원합니다. 새 스토리지 VM에 대해 AWS에서 IP 주소를 할당하기 전에 한도를 확인해야 합니다.

단계

1. 로 이동합니다 "[Cloud Volumes ONTAP 릴리즈 노트의 스토리지 제한 사항 섹션을 참조하십시오](#)".
2. 인스턴스 유형에 대한 인터페이스당 최대 IP 주소 수를 식별합니다.
3. AWS에서 IP 주소를 할당할 때 다음 섹션에서 필요하므로 이 번호를 기록해 두십시오.

AWS에서 IP 주소를 할당합니다

새 스토리지 VM에 대한 LIF를 생성하기 전에 AWS의 포트 e0a에 프라이빗 IPv4 주소를 할당해야 합니다.

스토리지 VM을 위한 선택적 관리 LIF는 단일 노드 시스템과 단일 AZ의 HA 쌍에서 프라이빗 IP 주소를 필요로 합니다. 이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

단계

1. AWS에 로그인하고 EC2 서비스를 엽니다.
2. Cloud Volumes ONTAP 인스턴스를 선택하고 \* 네트워크 \* 을 클릭합니다.  
  
HA 쌍에서 스토리지 VM을 생성하는 경우 노드 1을 선택합니다.
3. 아래로 \* 네트워크 인터페이스 \* 로 스크롤하고 포트 e0a의 \* 인터페이스 ID \* 를 클릭합니다.

Name	Insta...	Instance state	Instance type	Status check
<input type="checkbox"/> danielleAws	i-070...	Running	m5.2xlarge	2/2 check
<input type="checkbox"/> occmTiering0702	i-0a7...	Stopped	m5.2xlarge	-
<input checked="" type="checkbox"/> cvoTiering1	i-02a...	Stopped	m5.2xlarge	-

Interface ID	Description
<input checked="" type="checkbox"/> <a href="#">eni-07c301...</a>	Interface for Node & Cluster Management, Inter-Cluster Communication, and Data - e0a

4. 네트워크 인터페이스를 선택하고 \* 작업 > IP 주소 관리 \* 를 클릭합니다.
5. e0a의 IP 주소 목록을 확장합니다.
6. IP 주소 확인:
  - a. 할당된 IP 주소의 수를 세어하여 포트에 추가 IP를 위한 공간이 있는지 확인합니다.  
이 페이지의 이전 섹션에서 인터페이스당 지원되는 최대 IP 주소 수를 확인해야 합니다.
  - b. 선택 사항: Cloud Volumes ONTAP용 CLI로 이동하여 \* network interface show \* 를 실행하여 각 IP 주소가 사용 중인지 확인합니다.  
IP 주소를 사용하지 않는 경우 새 스토리지 VM에서 사용할 수 있습니다.
7. AWS 콘솔로 돌아가서 \* Assign new IP address \* 를 클릭하여 새 스토리지 VM에 필요한 양에 따라 추가 IP 주소를 할당합니다.
  - 단일 노드 시스템: 사용되지 않는 1개의 보조 전용 IP가 필요합니다.  
스토리지 VM에 관리 LIF를 생성하려면 선택적인 보조 프라이빗 IP가 필요합니다.
  - 단일 AZ의 HA 쌍: 노드 1에 사용되지 않는 2차 프라이빗 IP가 1개 필요합니다.  
스토리지 VM에 관리 LIF를 생성하려면 선택적인 보조 프라이빗 IP가 필요합니다.
  - 여러 AZs의 HA 쌍: 각 노드에 사용하지 않는 2차 프라이빗 IP가 1개 필요합니다.
8. 단일 AZ의 HA 쌍에서 IP 주소를 할당하는 경우 \* Allow secondary private IPv4 address to be reassigned되도록 \* 를 활성화합니다.
9. 저장 \* 을 클릭합니다.
10. 여러 AZs에 HA 쌍이 있는 경우 노드 2에 대해 이 단계를 반복해야 합니다.

단일 노드 시스템에 스토리지 VM을 생성합니다

다음 단계에서는 단일 노드 시스템에 새 스토리지 VM을 생성합니다. NAS LIF를 생성하려면 하나의 프라이빗 IP 주소가 필요하며, 관리 LIF를 생성하려면 또 다른 선택적 프라이빗 IP 주소가 필요합니다.

## 단계

1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. NAS LIF를 생성합니다.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address private_ip_x -netmask  
node1Mask -lif ip_nas_2 -home-node cvo-node
```

여기서 `_private_ip_x`는 e0a에서 사용되지 않는 보조 전용 IP입니다.

3. 선택 사항: 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address private_ip_y -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

여기서 `_private_ip_y`는 e0a에서 사용되지 않는 또 다른 보조 전용 IP입니다.

4. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

## 단일 AZ에서 HA 쌍에 스토리지 VM을 생성합니다

다음 단계에서는 단일 AZ의 HA 쌍에서 새 스토리지 VM을 생성합니다. NAS LIF를 생성하려면 하나의 프라이빗 IP 주소가 필요하며, 관리 LIF를 생성하려면 또 다른 선택적 프라이빗 IP 주소가 필요합니다.

이 두 LIF는 모두 노드 1에 할당됩니다. 장애가 발생할 경우 전용 IP 주소를 노드 간에 이동할 수 있습니다.

## 단계

1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

## 2. 노드 1에 NAS LIF를 생성합니다.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

여기서 `_private_ip_x`는 `cvo-node1`의 `e0a`에서 사용되지 않는 보조 전용 IP입니다. 서비스 정책 `default-data-files`는 IP가 파트너 노드로 마이그레이션할 수 있음을 나타내므로 테이크오버의 경우 이 IP 주소를 `cvo-node2`의 `e0a`로 재배치할 수 있습니다.

## 3. 선택 사항: 노드 1에 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

여기서 `_private_ip_y`는 `e0a`에서 사용되지 않는 또 다른 보조 전용 IP입니다.

## 4. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

## 5. Cloud Volumes ONTAP 9.11.1 이상을 실행 중인 경우 스토리지 VM에 대한 네트워크 서비스 정책을 수정합니다.

Cloud Volumes ONTAP가 아웃바운드 관리 연결에 iSCSI LIF를 사용할 수 있도록 하기 때문에 서비스를 수정해야 합니다.

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client

```

여러 AZs의 HA 쌍에서 스토리지 VM을 생성합니다

다음 단계에서는 여러 AZs의 HA 쌍에서 새 스토리지 VM을 생성합니다.

NAS LIF에는 `_floating_IP` 주소가 필요하며 관리 LIF에는 선택 사항입니다. 이러한 부동 IP 주소는 AWS에서 전용 IP를 할당할 필요가 없습니다. 대신, 동일한 VPC에서 특정 노드의 ENI를 가리키도록 AWS 라우트 테이블에 유동 IP가 자동으로 구성됩니다.

유동 IP가 ONTAP와 연동하려면 각 노드의 모든 스토리지 VM에 전용 IP 주소를 구성해야 합니다. 이 내용은 아래 단계에서 iSCSI LIF가 노드 1과 노드 2에 생성되는 것으로 반영됩니다.

단계

1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.



```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

## 2. 노드 1에 NAS LIF를 생성합니다.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

- 유동 IP 주소는 HA 구성을 배포하는 AWS 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 합니다. 192.168.209.27은 부동 IP 주소의 예입니다. "[부동 IP 주소 선택에 대해 자세히 알아보십시오](#)".
- -service-policy default-data-files IP가 파트너 노드로 마이그레이션할 수 있음을 나타냅니다.

## 3. 선택 사항: 노드 1에 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

## 4. 노드 1에 iSCSI LIF를 생성합니다.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmask node1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

- 이 iSCSI LIF는 스토리지 VM에 있는 유동 IP의 LIF 마이그레이션을 지원하는 데 필요합니다. iSCSI LIF가 될 필요는 없지만 노드 간에 마이그레이션하도록 구성할 수는 없습니다.
- -service-policy default-data-block IP 주소가 노드 간에 마이그레이션되지 않음을 나타냅니다.
- `_private_ip_`은 `cvo_node1`의 `eth0(e0a)`에서 사용되지 않는 보조 전용 IP 주소입니다.

## 5. 노드 2에 iSCSI LIF를 생성합니다.

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif
ip_node2_iscsi_2 -home-node cvo-node2
```

- 이 iSCSI LIF는 스토리지 VM에 있는 유동 IP의 LIF 마이그레이션을 지원하는 데 필요합니다. iSCSI LIF가 될

필요는 없지만 노드 간에 마이그레이션하도록 구성할 수는 없습니다.

- `-service-policy default-data-block` IP 주소가 노드 간에 마이그레이션되지 않음을 나타냅니다.
- `_private_ip_`는 `cvo_node2`의 `eth0(e0a)`에서 사용되지 않는 보조 전용 IP 주소입니다.

6. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

7. Cloud Volumes ONTAP 9.11.1 이상을 실행 중인 경우 스토리지 VM에 대한 네트워크 서비스 정책을 수정합니다.

Cloud Volumes ONTAP가 아웃바운드 관리 연결에 iSCSI LIF를 사용할 수 있도록 하기 때문에 서비스를 수정해야 합니다.

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client

```

## Azure에서 Cloud Volumes ONTAP를 위한 데이터 서비스 스토리지 VM을 생성합니다

스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에 스토리지 및 데이터 서비스를 제공합니다. 이를 SVM 또는 `_vserver_`로 알고 있을 수 있습니다. Cloud Volumes ONTAP는 기본적으로 하나의 스토리지 VM으로 구성되지만 Azure에서 Cloud Volumes ONTAP를 실행할 때 추가 스토리지 VM이 지원됩니다.

데이터를 지원하는 스토리지 VM을 추가로 생성하려면 Azure에서 IP 주소를 할당한 다음 ONTAP 명령을 실행하여 스토리지 VM 및 데이터 LIF를 생성해야 합니다.

지원되는 스토리지 VM 수입니다

9.9.0 릴리즈부터 특정 Cloud Volumes ONTAP 구성에서 여러 스토리지 VM이 지원됩니다. 로 이동합니다 ["Cloud Volumes ONTAP 릴리즈 노트"](#) 사용 중인 Cloud Volumes ONTAP 버전에 대해 지원되는 스토리지 VM 수를

확인하려면 다음을 수행합니다.

다른 모든 Cloud Volumes ONTAP 구성에서는 재해 복구에 사용되는 1개의 데이터 서비스 스토리지 VM과 1개의 대상 스토리지 VM을 지원합니다. 소스 스토리지 VM에 중단이 발생할 경우 데이터 액세스를 위해 대상 스토리지 VM을 활성화할 수 있습니다.

### Azure에서 IP 주소를 할당합니다

스토리지 VM을 생성하고 LIF를 할당하기 전에 Azure에서 IP 주소를 할당해야 합니다.

단일 노드 시스템

스토리지 VM을 생성하고 LIF를 할당하기 전에 Azure에서 nic0에 IP 주소를 할당해야 합니다.

데이터 LIF 액세스를 위한 IP 주소와 스토리지 VM(SVM) 관리 LIF를 위한 선택적 IP 주소를 생성해야 합니다. 이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

단계

1. Azure 포털에 로그인하고 \* Virtual Machine \* 서비스를 엽니다.
2. Cloud Volumes ONTAP VM의 이름을 클릭합니다.
3. 네트워킹 \* 을 클릭합니다.
4. nic0의 네트워크 인터페이스 이름을 클릭합니다.
5. 설정 \* 에서 \* IP 구성 \* 을 클릭합니다.
6. 추가 \* 를 클릭합니다.
7. IP 구성의 이름을 입력하고 \* Dynamic \* 을 선택한 다음 \* OK \* 를 클릭합니다.
8. 방금 만든 IP 구성의 이름을 클릭하고 \* Assignment \* 를 \* Static \* 으로 변경한 다음 \* Save \* 를 클릭합니다.

정적 IP 주소를 사용하면 IP 주소가 변경되지 않으므로 정적 IP 주소를 사용하는 것이 가장 좋습니다. 이렇게 하면 응용 프로그램이 불필요하게 중단되는 것을 방지할 수 있습니다.

SVM 관리 LIF를 생성하려면 이 단계를 반복하여 추가 IP 주소를 생성합니다.

작업을 마친 후

방금 만든 개인 IP 주소를 복사합니다. 새 스토리지 VM에 대한 LIF를 생성할 때 이러한 IP 주소를 지정해야 합니다.

### HA 쌍

HA 쌍에 대한 IP 주소를 할당하는 방법은 사용 중인 스토리지 프로토콜에 따라 다릅니다.

## iSCSI

스토리지 VM을 생성하고 LIF를 할당하기 전에 Azure의 nic0에 iSCSI IP 주소를 할당해야 합니다. iSCSI는 페일오버에 ALUA를 사용하므로 iSCSI용 IPS는 로드 밸런서가 아니라 nic0에 할당됩니다.

다음 IP 주소를 만들어야 합니다.

- 노드 1에서 iSCSI 데이터 LIF 액세스를 위한 단일 IP 주소
- 노드 2의 iSCSI 데이터 LIF 액세스를 위한 하나의 IP 주소
- 스토리지 VM(SVM) 관리 LIF의 선택적 IP 주소입니다

이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

### 단계

1. Azure 포털에 로그인하고 \* Virtual Machine \* 서비스를 엽니다.
2. 노드 1의 Cloud Volumes ONTAP VM 이름을 클릭합니다.
3. 네트워킹 \* 을 클릭합니다.
4. nic0의 네트워크 인터페이스 이름을 클릭합니다.
5. 설정 \* 에서 \* IP 구성 \* 을 클릭합니다.
6. 추가 \* 를 클릭합니다.
7. IP 구성의 이름을 입력하고 \* Dynamic \* 을 선택한 다음 \* OK \* 를 클릭합니다.
8. 방금 만든 IP 구성의 이름을 클릭하고 \* Assignment \* 를 \* Static \* 으로 변경한 다음 \* Save \* 를 클릭합니다.

정적 IP 주소를 사용하면 IP 주소가 변경되지 않으므로 정적 IP 주소를 사용하는 것이 가장 좋습니다. 이렇게 하면 응용 프로그램이 불필요하게 중단되는 것을 방지할 수 있습니다.

9. 노드 2에서 이 단계를 반복합니다.
10. SVM 관리 LIF를 생성하려면 노드 1에서 이 단계를 반복합니다.

### NFS 를 참조하십시오

NFS에 사용하는 IP 주소는 로드 밸런싱 장치에 할당되어 페일오버 이벤트가 발생할 경우 IP 주소가 다른 노드로 마이그레이션될 수 있습니다.

다음 IP 주소를 만들어야 합니다.

- 노드 1에서 NAS 데이터 LIF 액세스를 위한 단일 IP 주소
- 노드 2의 NAS 데이터 LIF 액세스를 위한 하나의 IP 주소
- 스토리지 VM(SVM) 관리 LIF의 선택적 IP 주소입니다

DNS 통신을 위해 iSCSI LIF가 필요합니다. iSCSI LIF는 페일오버 시 마이그레이션되지 않으므로 이 용도로 사용됩니다.

이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

### 단계

1. Azure 포털에서 \* 로드 밸런서 \* 서비스를 엽니다.
2. HA 쌍에 대한 로드 밸런싱 장치의 이름을 클릭합니다.
3. 노드 1에서 데이터 LIF 액세스를 위한 프론트엔드 IP 구성을 하나 생성하고, 노드 2에서 데이터 LIF 액세스를 위한 또 다른 프론트엔드 IP를 생성하고, 스토리지 VM(SVM) 관리 LIF를 위한 또 다른 선택적 프론트엔드 IP를 생성합니다.
  - a. Settings \* 에서 \* Frontend IP configuration \* 을 클릭합니다.
  - b. 추가 \* 를 클릭합니다.
  - c. 프론트엔드 IP의 이름을 입력하고, Cloud Volumes ONTAP HA 쌍의 서브넷을 선택하고, \* Dynamic \* 을 선택한 상태로 두고, 가용성 영역이 있는 지역에서는 \* Zone-Redundant \* 를 선택된 상태로 두어 존이 실패하는 경우 IP 주소를 계속 사용할 수 있도록 합니다.

The screenshot shows the Azure portal interface for configuring a frontend IP. The breadcrumb path is 'Home > Load balancing > azureha1011s3-rg-lb >'. The main heading is 'Add frontend IP configuration'. Below this, the resource name 'azureha1011s3-rg-lb' is shown. The configuration form includes the following fields:

- Name \***: A text input field containing 'ip-for-svm2'.
- Virtual network**: A dropdown menu showing 'Default-Networking-vnet'.
- Subnet \***: A dropdown menu showing 'default (172.19.2.0/24)'.
- Assignment**: Radio buttons for 'Dynamic' (which is selected) and 'Static'.
- Availability zone \***: A dropdown menu showing 'Zone-redundant'.

- d. 방금 만든 프론트엔드 IP 구성의 이름을 클릭하고 \* Assignment \* 를 \* Static \* 으로 변경하고 \* Save \* 를 클릭합니다.

정적 IP 주소를 사용하면 IP 주소가 변경되지 않으므로 정적 IP 주소를 사용하는 것이 가장 좋습니다. 이렇게 하면 응용 프로그램이 불필요하게 중단되는 것을 방지할 수 있습니다.

4. 방금 생성한 각 프론트엔드 IP에 대해 상태 탐침을 추가합니다.
  - a. 부하 분산 장치의 \* 설정 \* 에서 \* 상태 프로브 \* 를 클릭합니다.
  - b. 추가 \* 를 클릭합니다.
  - c. 상태 프로브의 이름을 입력하고 63005에서 65000 사이의 포트 번호를 입력합니다. 다른 필드의 기본값을 유지합니다.

포트 번호는 63005에서 65000 사이여야 합니다. 예를 들어 상태 프로브를 3개 생성하는 경우 포트 번호 63005, 63006 및 63007을 사용하는 프로브를 입력할 수 있습니다.



Home > Load balancers > azureha1011s3-rg-lb >

## Add health probe ...

azureha1011s3-rg-lb

Name *	<input type="text" value="svm2-health-probe1"/>	✓
Protocol *	<input type="text" value="TCP"/>	▼
Port * ⓘ	<input type="text" value="63005"/>	✓
Interval * ⓘ	<input type="text" value="5"/>	seconds
Unhealthy threshold * ⓘ	<input type="text" value="2"/>	consecutive failures
Used by ⓘ	Not used	

5. 각 프런트엔드 IP에 대한 새 로드 밸런싱 규칙을 생성합니다.

a. 부하 분산 장치의 \* 설정 \* 아래에서 \* 로드 밸런싱 규칙 \* 을 클릭합니다.

b. 추가 \* 를 클릭하고 필요한 정보를 입력합니다.

- \* 이름 \*: 규칙의 이름을 입력합니다.
- \* IP 버전 \*: \* IPv4 \* 를 선택합니다.
- \* 프런트엔드 IP 주소 \*: 방금 생성한 프런트엔드 IP 주소 중 하나를 선택합니다.
- \* HA 포트 \*: 이 옵션을 활성화합니다.
- \* 백엔드 풀 \*: 이미 선택된 기본 백엔드 풀을 유지합니다.
- \* 상태 프로브 \*: 선택한 프런트엔드 IP에 대해 생성한 상태 프로브를 선택합니다.
- \* 세션 지속성 \*: \* 없음 \* 을 선택합니다.
- \* Floating IP \*: \* Enabled \* 를 선택합니다.

## Add load balancing rule

chandanaTcpRst3-rg-lb

**i** A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name \*  
jimmy\_new\_rule ✓

IP Version \*  
 IPv4  IPv6

Frontend IP address \* ⓘ  
10.1.0.156 (dataAFIP) ▾

HA Ports ⓘ

Backend pool ⓘ  
backendPool (2 virtual machines) ▾

Health probe ⓘ  
dataProbe (TCP:63002) ▾

Session persistence ⓘ  
None ▾

Floating IP ⓘ  
 Disabled  Enabled

6. Cloud Volumes ONTAP에 대한 네트워크 보안 그룹 규칙을 통해 로드 밸런서가 위의 4단계에서 만든 상태 탐침에 대한 TCP 탐침을 보낼 수 있는지 확인합니다. 이 작업은 기본적으로 허용됩니다.

### 중소기업

SMB 데이터에 사용하는 IP 주소는 로드 밸런서에 할당되어 파일오버 이벤트가 발생할 경우 IP 주소가 다른 노드로 마이그레이션될 수 있습니다.

로드 밸런서에 다음 IP 주소를 만들어야 합니다.

- 노드 1에서 NAS 데이터 LIF 액세스를 위한 단일 IP 주소
- 노드 2의 NAS 데이터 LIF 액세스를 위한 하나의 IP 주소
- 각 VM의 해당 NIC0에 있는 노드 1의 iSCSI LIF에 대한 IP 주소 1개
- 노드 2의 iSCSI LIF에 대한 IP 주소 1개

iSCSI LIF는 DNS 및 SMB 통신에 필요합니다. iSCSI LIF는 파일오버 시 마이그레이션되지 않으므로 이 용도로 사용됩니다.

- 스토리지 VM(SVM) 관리 LIF의 선택적 IP 주소입니다

이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.



## 단계

1. Azure 포털에서 \* 로드 밸런서 \* 서비스를 엽니다.
2. HA 쌍에 대한 로드 밸런싱 장치의 이름을 클릭합니다.
3. 데이터 및 SVM LIF에 필요한 수의 프론트엔드 IP 구성을 생성합니다.



프론트엔드 IP는 각 해당 SVM에 대해 NIC0 아래에 생성되어야 합니다. SVM NIC0에 IP 주소를 추가하는 방법에 대한 자세한 내용은 "7단계[하이퍼링크]" 를 참조하십시오.

- a. Settings \* 에서 \* Frontend IP configuration \* 을 클릭합니다.
- b. 추가 \* 를 클릭합니다.
- c. 프론트엔드 IP의 이름을 입력하고, Cloud Volumes ONTAP HA 쌍의 서브넷을 선택하고, \* Dynamic \* 을 선택한 상태로 두고, 가용성 영역이 있는 지역에서는 \* Zone-Redundant \* 를 선택된 상태로 두어 존이 실패하는 경우 IP 주소를 계속 사용할 수 있도록 합니다.

The screenshot shows the 'Add frontend IP configuration' page in the Microsoft Azure portal. The breadcrumb navigation is 'Home > Load balancing > azureha1011s3-rg-lb >'. The page title is 'Add frontend IP configuration' with a sub-header 'azureha1011s3-rg-lb'. The form contains the following fields:

- Name \***: ip-for-svm2
- Virtual network**: Default-Networking-vnet
- Subnet \***: default (172.19.2.0/24)
- Assignment**:  Dynamic  Static
- Availability zone \***: Zone-redundant

- d. 방금 만든 프론트엔드 IP 구성의 이름을 클릭하고 \* Assignment \* 를 \* Static \* 으로 변경하고 \* Save \* 를 클릭합니다.

정적 IP 주소를 사용하면 IP 주소가 변경되지 않으므로 정적 IP 주소를 사용하는 것이 가장 좋습니다. 이렇게 하면 응용 프로그램이 불필요하게 중단되는 것을 방지할 수 있습니다.

4. 방금 생성한 각 프론트엔드 IP에 대해 상태 탐침을 추가합니다.
  - a. 부하 분산 장치의 \* 설정 \* 에서 \* 상태 프로브 \* 를 클릭합니다.
  - b. 추가 \* 를 클릭합니다.
  - c. 상태 프로브의 이름을 입력하고 63005에서 65000 사이의 포트 번호를 입력합니다. 다른 필드의 기본값을 유지합니다.

포트 번호는 63005에서 65000 사이여야 합니다. 예를 들어 상태 프로브를 3개 생성하는 경우 포트 번호 63005, 63006 및 63007을 사용하는 프로브를 입력할 수 있습니다.



Home > Load balancers > azureha1011s3-rg-lb >

## Add health probe ...

azureha1011s3-rg-lb

Name *	<input type="text" value="svm2-health-probe1"/>	✓
Protocol *	<input type="text" value="TCP"/>	▼
Port * ⓘ	<input type="text" value="63005"/>	✓
Interval * ⓘ	<input type="text" value="5"/>	seconds
Unhealthy threshold * ⓘ	<input type="text" value="2"/>	consecutive failures
Used by ⓘ	Not used	

5. 각 프런트엔드 IP에 대한 새 로드 밸런싱 규칙을 생성합니다.

a. 부하 분산 장치의 \* 설정 \* 아래에서 \* 로드 밸런싱 규칙 \* 을 클릭합니다.

b. 추가 \* 를 클릭하고 필요한 정보를 입력합니다.

- \* 이름 \*: 규칙의 이름을 입력합니다.
- \* IP 버전 \*: \* IPv4 \* 를 선택합니다.
- \* 프런트엔드 IP 주소 \*: 방금 생성한 프런트엔드 IP 주소 중 하나를 선택합니다.
- \* HA 포트 \*: 이 옵션을 활성화합니다.
- \* 백엔드 풀 \*: 이미 선택된 기본 백엔드 풀을 유지합니다.
- \* 상태 프로브 \*: 선택한 프런트엔드 IP에 대해 생성한 상태 프로브를 선택합니다.
- \* 세션 지속성 \*: \* 없음 \* 을 선택합니다.
- \* Floating IP \*: \* Enabled \* 를 선택합니다.

## Add load balancing rule ...

chandanaTcpRst3-rg-lb

**i** A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name \*

IP Version \*  
 IPv4  IPv6

Frontend IP address \* ⓘ

HA Ports ⓘ

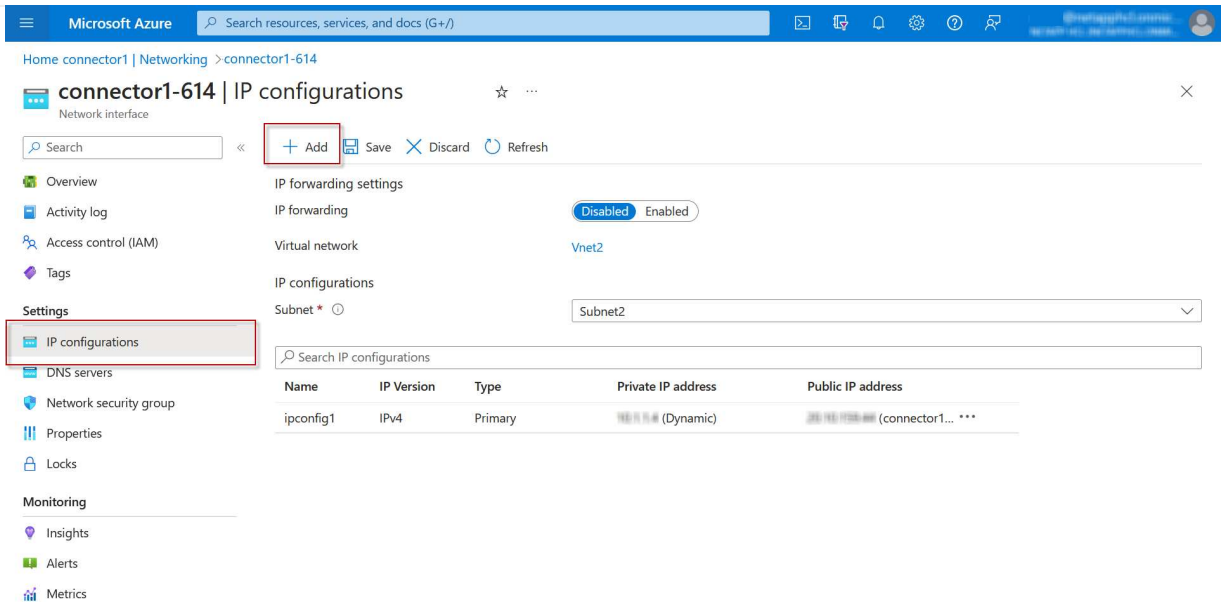
Backend pool ⓘ

Health probe ⓘ

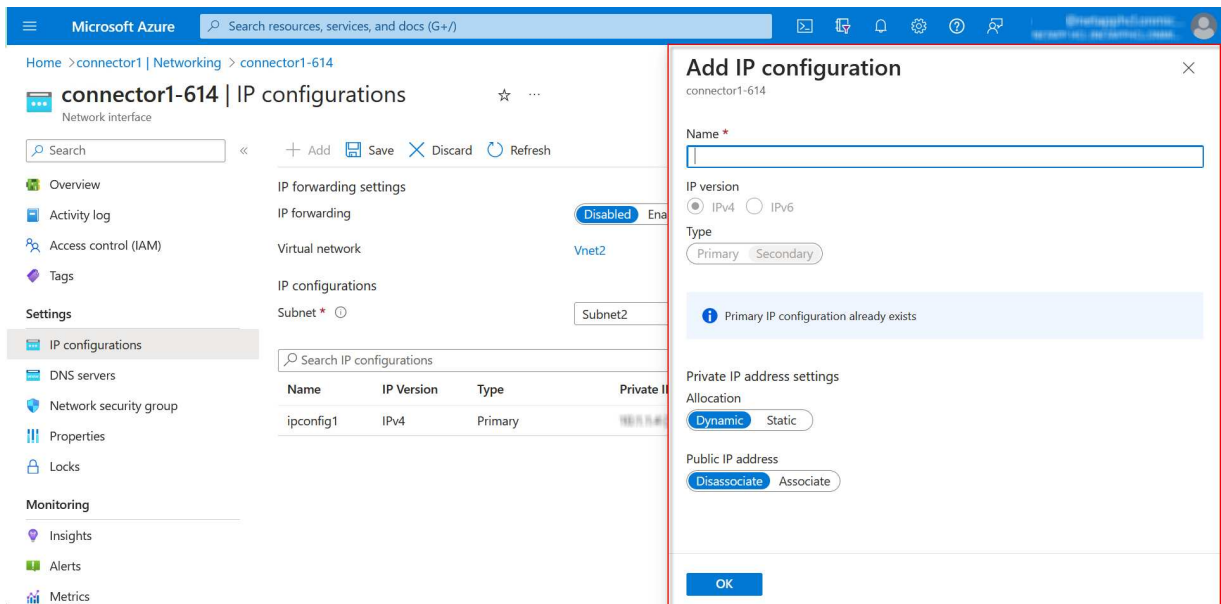
Session persistence ⓘ

Floating IP ⓘ

6. Cloud Volumes ONTAP에 대한 네트워크 보안 그룹 규칙을 통해 로드 밸런서가 위의 4단계에서 만든 상태 탐침에 대한 TCP 탐침을 보낼 수 있는지 확인합니다. 이 작업은 기본적으로 허용됩니다.
7. iSCSI LIF의 경우 NIC0의 IP 주소를 추가합니다.
  - a. Cloud Volumes ONTAP VM의 이름을 클릭합니다.
  - b. 네트워킹 \* 을 클릭합니다.
  - c. nic0의 네트워크 인터페이스 이름을 클릭합니다.
  - d. 설정에서 \* IP 설정 \* 을 클릭합니다.
  - e. 추가 \* 를 클릭합니다.



f. IP 구성의 이름을 입력하고 Dynamic 을 선택한 다음 \* OK \* 를 클릭합니다.



g. 방금 만든 IP 구성의 이름을 클릭하고 Assignment 를 Static 으로 변경한 다음 \* Save \* 를 클릭합니다.



정적 IP 주소를 사용하면 IP 주소가 변경되지 않으므로 정적 IP 주소를 사용하는 것이 가장 좋습니다. 이렇게 하면 응용 프로그램이 불필요하게 중단되는 것을 방지할 수 있습니다.

작업을 마친 후

방금 만든 개인 IP 주소를 복사합니다. 새 스토리지 VM에 대한 LIF를 생성할 때 이러한 IP 주소를 지정해야 합니다.

스토리지 VM 및 LIF 생성

Azure에서 IP 주소를 할당한 후에는 단일 노드 시스템 또는 HA 쌍 에 새 스토리지 VM을 생성할 수 있습니다.

단일 노드 시스템

단일 노드 시스템에서 스토리지 VM 및 LIF를 생성하는 방법은 사용 중인 스토리지 프로토콜에 따라 다릅니다.

## iSCSI

필요한 LIF와 함께 새 스토리지 VM을 생성하려면 다음 단계를 따르십시오.

### 단계

1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. 데이터 LIF 생성:

```
network interface create -vserver <svm-name> -home-port e0a -address  
<iscsi-ip-address> -netmask-length <# of mask bits> -lif <lif-name>  
-home-node <name-of-nodel> -data-protocol iscsi
```

3. 선택 사항: 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-nodel> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default
```

4. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

## NFS 를 참조하십시오

필요한 LIF와 함께 새 스토리지 VM을 생성하려면 다음 단계를 따르십시오.

### 단계

1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name> -gateway <ip-of-gateway-server>
```

## 2. 데이터 LIF 생성:

```
network interface create -vserver <svm-name> -lif <lif-name> -role data -data-protocol cifs,nfs -address <nas-ip-address> -netmask -length <length> -home-node <name-of-node1> -status-admin up -failover-policy disabled -firewall-policy data -home-port e0a -auto-revert true -failover-group Default
```

## 3. 선택 사항: 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name> -role data -data-protocol none -address <svm-mgmt-ip-address> -netmask -length <length> -home-node <name-of-node1> -status-admin up -failover-policy system-defined -firewall-policy mgmt -home-port e0a -auto-revert false -failover-group Default
```

## 4. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

### 중소기업

필요한 LIF와 함께 새 스토리지 VM을 생성하려면 다음 단계를 따르십시오.

#### 단계

##### 1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

## 2. 데이터 LIF 생성:

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nas-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

## 3. 선택 사항: 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

## 4. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

## HA 쌍

HA 쌍에서 스토리지 VM 및 LIF를 생성하는 방법은 사용 중인 스토리지 프로토콜에 따라 다릅니다.



## iSCSI

필요한 LIF와 함께 새 스토리지 VM을 생성하려면 다음 단계를 따르십시오.

### 단계

1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. 데이터 LIF 생성:

- a. 다음 명령을 사용하여 노드 1에 iSCSI LIF를 생성합니다.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif  
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

- b. 다음 명령을 사용하여 노드 2에 iSCSI LIF를 생성합니다.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif  
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

3. 선택 사항: 노드 1에 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy system-defined -firewall-policy mgmt -home-port e0a  
-auto-revert false -failover-group Default
```

이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

4. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

5. Cloud Volumes ONTAP 9.11.1 이상을 실행 중인 경우 스토리지 VM에 대한 네트워크 서비스 정책을 수정합니다.

- a. 다음 명령을 입력하여 고급 모드에 액세스합니다.

```
::> set adv -con off
```

Cloud Volumes ONTAP가 아웃바운드 관리 연결에 iSCSI LIF를 사용할 수 있도록 하기 때문에 서비스를 수정해야 합니다.

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

**NFS** 를 참조하십시오

필요한 LIF와 함께 새 스토리지 VM을 생성하려면 다음 단계를 따르십시오.

단계

1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
vserver create -vserver <svm-name> -subtype default -rootvolume  
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>  
-gateway <ip-of-gateway-server>
```

2. 데이터 LIF 생성:

- a. 다음 명령을 사용하여 노드 1에 NAS LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-node1> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe1>
```

- b. 다음 명령을 사용하여 노드 2에 NAS LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-node2> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe2>
```

3. DNS 통신을 제공하기 위해 iSCSI LIF 생성:

- a. 다음 명령을 사용하여 노드 1에 iSCSI LIF를 생성합니다.

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif  
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

- b. 다음 명령을 사용하여 노드 2에 iSCSI LIF를 생성합니다.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

4. 선택 사항: 노드 1에 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

5. 선택 사항: 노드 1에 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

6. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

7. Cloud Volumes ONTAP 9.11.1 이상을 실행 중인 경우 스토리지 VM에 대한 네트워크 서비스 정책을 수정합니다.

- a. 다음 명령을 입력하여 고급 모드에 액세스합니다.

```
::> set adv -con off
```

Cloud Volumes ONTAP가 아웃바운드 관리 연결에 iSCSI LIF를 사용할 수 있도록 하기 때문에 서비스를 수정해야 합니다.

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client

```

## 중소기업

필요한 LIF와 함께 새 스토리지 VM을 생성하려면 다음 단계를 따르십시오.

### 단계

1. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```

vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix

```

```

network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>

```

## 2. NAS 데이터 LIF 생성:

- a. 다음 명령을 사용하여 노드 1에 NAS LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node1> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe1>
```

- b. 다음 명령을 사용하여 노드 2에 NAS LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node2> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe2>
```

## 3. DNS 통신을 제공하기 위해 iSCSI LIF 생성:

- a. 다음 명령을 사용하여 노드 1에 iSCSI LIF를 생성합니다.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

- b. 다음 명령을 사용하여 노드 2에 iSCSI LIF를 생성합니다.

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

## 4. 선택 사항: 노드 1에 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

이 관리 LIF는 SnapCenter과 같은 관리 툴에 연결할 수 있습니다.

5. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

6. Cloud Volumes ONTAP 9.11.1 이상을 실행 중인 경우 스토리지 VM에 대한 네트워크 서비스 정책을 수정합니다.

- a. 다음 명령을 입력하여 고급 모드에 액세스합니다.

```
::> set adv -con off
```

Cloud Volumes ONTAP가 아웃바운드 관리 연결에 iSCSI LIF를 사용할 수 있도록 하기 때문에 서비스를 수정해야 합니다.

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client

```

#### 다음 단계

HA 쌍에서 스토리지 VM을 생성하면 해당 SVM에서 스토리지를 프로비저닝하기 전에 12시간을 기다리는 것이 좋습니다. Cloud Volumes ONTAP 9.10.1 릴리즈부터 BlueXP는 12시간 간격으로 HA 쌍의 로드 밸런서에 대한 설정을 검색합니다. 새로운 SVM이 있는 경우 BlueXP에서 계획되지 않은 페일오버 시간을 단축해 주는 설정을 사용할 수 있습니다.

### Google Cloud에서 Cloud Volumes ONTAP용 데이터 서비스 스토리지 VM을 생성합니다

스토리지 VM은 ONTAP 내에서 실행되는 가상 머신으로, 클라이언트에 스토리지 및 데이터 서비스를 제공합니다. 이를 SVM 또는 `_vserver_`로 알고 있을 수 있습니다. Cloud Volumes ONTAP는 기본적으로 하나의 스토리지 VM으로 구성되지만 일부 구성에서는 추가 스토리지 VM을 지원합니다.



지원되는 스토리지 **VM** 수입니다

9.11.1 릴리즈부터 Google Cloud의 특정 Cloud Volumes ONTAP 구성에서 여러 스토리지 VM이 지원됩니다. 로 이동합니다 "[Cloud Volumes ONTAP 릴리즈 노트](#)" 사용 중인 Cloud Volumes ONTAP 버전에 대해 지원되는 스토리지 VM 수를 확인하려면 다음을 수행합니다.

다른 모든 Cloud Volumes ONTAP 구성에서는 재해 복구에 사용되는 1개의 데이터 서비스 스토리지 VM과 1개의 대상 스토리지 VM을 지원합니다. 소스 스토리지 VM에 중단이 발생할 경우 데이터 액세스를 위해 대상 스토리지 VM을 활성화할 수 있습니다.

스토리지 **VM**을 생성합니다

라이선스로 지원되는 경우 단일 노드 시스템 또는 HA 쌍에서 여러 스토리지 VM을 생성할 수 있습니다. BlueXP API를 사용하여 HA 쌍에서 스토리지 VM을 생성해야 하지만, CLI 또는 System Manager를 사용하여 단일 노드 시스템에 스토리지 VM을 생성할 수 있습니다.

단일 노드 시스템

다음 단계에서는 CLI를 사용하여 단일 노드 시스템에 새 스토리지 VM을 생성합니다. 데이터 LIF를 생성하려면 하나의 프라이빗 IP 주소가 필요하며, 관리 LIF를 생성하려면 또 다른 선택적 프라이빗 IP 주소가 필요합니다.

단계

1. Google Cloud에서 Cloud Volumes ONTAP 인스턴스로 이동하고 각 LIF에 대한 IP 주소를 nic0에 추가합니다.

**Edit network interface**

Network \*  
default

Subnetwork \*  
default IPv4 (10.138.0.0/20)

**i** To use IPv6, you need an IPv6 subnet range. [LEARN MORE](#)

**IP stack type**

IPv4 (single-stack)

IPv4 and IPv6 (dual-stack)

Primary internal IP  
gpcvo-vm-ip-nic0-nodemgmt (10.138.0.46)

**Alias IP ranges**

Subnet range 1 Primary (10.138.0.0/20)	Alias IP range 1 * 10.138.0.25/32
Subnet range 2 Primary (10.138.0.0/20)	Alias IP range 2 * 10.138.0.23/32
Subnet range 3 Primary (10.138.0.0/20)	Alias IP range 3 * 10.138.0.21/32
Subnet range 4 Primary (10.138.0.0/20)	Alias IP range 4 * 10.138.0.31/32

**+ ADD IP RANGE**

External IPv4 address  
None

스토리지 VM에서 관리 LIF를 생성하려면 데이터 LIF에 하나의 IP 주소와 다른 선택적 IP 주소가 필요합니다.

"[Google Cloud 설명서: 기존 인스턴스에 별칭 IP 범위 추가](#)"

2. 스토리지 VM을 생성하고 스토리지 VM으로 가는 경로를 생성합니다.

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name> -gateway <ip-of-gateway-server>
```

3. Google Cloud에 추가한 IP 주소를 지정하여 데이터 LIF를 생성합니다.

## iSCSI

```
network interface create -vserver <svm-name> -home-port e0a -address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-nodel> -data -protocol iscsi
```

## NFS 또는 SMB

```
network interface create -vserver <svm-name> -lif <lif-name> -role data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask -length <length> -home-node <name-of-nodel> -status-admin up -failover-policy disabled -firewall-policy data -home-port e0a -auto -revert true -failover-group Default
```

4. 선택 사항: Google Cloud에 추가한 IP 주소를 지정하여 스토리지 VM 관리 LIF를 생성합니다.

```
network interface create -vserver <svm-name> -lif <lif-name> -role data -data-protocol none -address <svm-mgmt-ip-address> -netmask-length <length> -home-node <name-of-nodel> -status-admin up -failover-policy system-defined -firewall-policy mgmt -home-port e0a -auto-revert false -failover-group Default
```

5. 스토리지 VM에 하나 이상의 애그리게이트를 할당합니다.

```
vserver add-aggregates -vserver <svm-name> -aggregates <aggr1,aggr2>
```

스토리지 VM에서 볼륨을 생성하기 전에 새 스토리지 VM이 적어도 하나의 애그리게이트에 액세스해야 하기 때문에 이 단계가 필요합니다.

## HA 쌍

BlueXP API를 사용하여 Google Cloud의 Cloud Volumes ONTAP 시스템에서 스토리지 VM을 생성해야 합니다. BlueXP는 필요한 LIF 서비스와 아웃바운드 SMB/CIFS 통신에 필요한 iSCSI LIF를 사용하여 스토리지 VM을 구성하기 때문에 System Manager 또는 CLI가 아닌 API를 사용해야 합니다.

BlueXP는 Google Cloud에 필요한 IP 주소를 할당하고 SMB/NFS 액세스를 위한 데이터 LIF와 아웃바운드 SMB 통신을 위한 iSCSI LIF를 사용하여 스토리지 VM을 생성합니다.

## Google Cloud 권한이 필요합니다

Connector에는 Cloud Volumes ONTAP HA 쌍에 대한 스토리지 VM을 생성하고 관리할 수 있는 특정 권한이 필요합니다. 필요한 권한은 에 포함되어 있습니다 "[NetApp에서 제공하는 정책](#)".

단계

1. 다음 API 호출을 사용하여 스토리지 VM을 생성합니다.

```
POST /occm/api/gcp/ha/working-environments/{WE_ID}/svm/
```

요청 본문에는 다음이 포함되어야 합니다.

```
{ "svmName": "myNewSvm1" }
```

## HA 쌍에서 스토리지 VM 관리

또한 BlueXP API는 HA 쌍에서 스토리지 VM의 이름 변경 및 삭제를 지원합니다.

스토리지 VM의 이름을 바꿉니다

필요한 경우 언제든지 스토리지 VM의 이름을 변경할 수 있습니다.

단계

1. 다음 API 호출을 사용하여 스토리지 VM의 이름을 바꿉니다.

```
PUT /occm/api/gcp/ha/working-environments/{WE_ID}/svm
```

요청 본문에는 다음이 포함되어야 합니다.

```
{  
  "svmNewName": "newSvmName",  
  "svmName": "oldSvmName"  
}
```

스토리지 VM을 삭제합니다

스토리지 VM이 더 이상 필요하지 않은 경우 Cloud Volumes ONTAP에서 삭제할 수 있습니다.

단계

1. 다음 API 호출을 사용하여 스토리지 VM을 삭제합니다.

```
DELETE /occm/api/gcp/ha/working-environments/{WE_ID}/svm/{SVM_NAME}
```

## SVM 재해 복구 설정

BlueXP는 스토리지 VM(SVM) 재해 복구에 대한 설정 또는 오케스트레이션 지원을 제공하지 않습니다. System Manager 또는 CLI를 사용해야 합니다.

두 Cloud Volumes ONTAP 시스템 간에 SnapMirror SVM 복제를 설정할 경우 두 개의 HA 쌍 시스템 또는 두 개의 단일 노드 시스템 간에 복제를 수행해야 합니다. HA 쌍과 단일 노드 시스템 간에 SnapMirror SVM 복제를 설정할 수 없습니다.

CLI 지침은 다음 문서를 참조하십시오.

- ["SVM 재해 복구 준비 Express 가이드"](#)
- ["SVM 재해 복구 익스프레스 가이드 를 참조하십시오"](#)

## 보안 및 데이터 암호화

### NetApp 암호화 솔루션으로 볼륨 암호화

Cloud Volumes ONTAP는 NVE(NetApp Volume Encryption) 및 NAE(NetApp Aggregate Encryption)를 지원합니다. NVE와 NAE는 FIPS 140-2를 준수하는 볼륨 유희 데이터 암호화를 지원하는 소프트웨어 기반 솔루션입니다. ["이러한 암호화 솔루션에 대해 자세히 알아보십시오"](#).

NVE와 NAE는 모두 외부 키 관리자로 지원됩니다.

### AWS 키 관리 서비스로 키를 관리합니다

을 사용할 수 있습니다 ["AWS KMS\(Key Management Service\)"](#) Google Cloud Platform에서 구축한 응용 프로그램에서 ONTAP 암호화 키를 보호합니다.

AWS KMS를 사용한 키 관리는 CLI 또는 ONTAP REST API를 통해 활성화할 수 있습니다.

KMS를 사용할 때는 기본적으로 데이터 SVM의 LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용됩니다. 노드 관리 네트워크는 AWS의 인증 서비스와 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않은 경우 클러스터는 키 관리 서비스를 제대로 사용하지 않습니다.

시작하기 전에

- Cloud Volumes ONTAP는 버전 9.12.0 이상을 실행해야 합니다
- 볼륨 암호화(VE) 라이선스 및 을(를) 설치해야 합니다
- MTEKM(멀티 테넌트 암호화 키 관리) 라이선스가 설치되어 있어야 합니다.
- 클러스터 또는 SVM 관리자여야 합니다
- 활성 AWS 구독이 있어야 합니다



데이터 SVM에 대한 키만 구성할 수 있습니다.

구성

설치하고

1. 을(를) 만들어야 합니다 ["허가"](#) 암호화를 관리하는 IAM 역할에 사용되는 AWS KMS 키의 경우 IAM 역할에는 다음 작업을 허용하는 정책이 포함되어야 합니다.
  - DescribeKey
  - Encrypt
  - Decrypt보조금을 생성하려면 을 참조하십시오 ["AWS 문서"](#).

2. "적절한 IAM 역할에 정책을 추가합니다." 이 정책은 을 지원해야 합니다 DescribeKey, Encrypt, 및 Decrypt 운영:

### Cloud Volumes ONTAP

1. Cloud Volumes ONTAP 환경으로 전환하십시오.
2. 고급 권한 레벨로 전환합니다.  
`set -privilege advanced`
3. AWS 키 관리자를 활성화합니다.  
`security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. 메시지가 표시되면 비밀 키를 입력합니다.
5. AWS KMS가 올바르게 구성되었는지 확인합니다.  
`security key-manager external aws show -vserver svm_name`

### Azure Key Vault를 사용하여 키를 관리합니다

을 사용할 수 있습니다 "Azure 키 저장소(AKV)" Azure로 배포된 응용 프로그램에서 ONTAP 암호화 키를 보호합니다.

AKV를 사용하여 보호할 수 있습니다 "NVE(NetApp Volume Encryption) 키" 데이터 SVM에만 해당.

AKV를 사용한 키 관리는 CLI 또는 ONTAP REST API를 사용하여 활성화할 수 있습니다.

AKV를 사용할 때는 기본적으로 데이터 SVM LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용됩니다. 노드 관리 네트워크는 클라우드 공급자의 인증 서비스(login.microsoftonline.com 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않은 경우 클러스터는 키 관리 서비스를 제대로 사용하지 않습니다.

#### 시작하기 전에

- Cloud Volumes ONTAP에서 버전 9.10.1 이상을 실행해야 합니다
- 설치된 볼륨 암호화(VE) 라이선스(NetApp 볼륨 암호화 라이선스는 NetApp Support에 등록된 각 Cloud Volumes ONTAP 시스템에 자동으로 설치됨)
- 멀티 테넌트 암호화 키 관리(MT\_EK\_MGMT) 라이선스가 있어야 합니다
- 클러스터 또는 SVM 관리자여야 합니다
- Active Azure 구독

#### 제한 사항

- AKV는 데이터 SVM에서만 구성할 수 있습니다

#### 구성 프로세스

이 단계에서는 Azure에 Cloud Volumes ONTAP 구성을 등록하는 방법과 Azure 키 저장소 및 키를 생성하는 방법을 설명합니다. 이 단계를 이미 완료한 경우, 특히 에서 올바른 구성 설정이 있는지 확인하십시오 [Azure Key Vault를 작성합니다](#)을 클릭한 다음 로 진행합니다 [Cloud Volumes ONTAP 구성](#).

- [Azure 애플리케이션 등록](#)
- [Azure 클라이언트 암호를 생성합니다](#)

- Azure Key Vault를 작성합니다
- 암호화 키를 생성합니다
- Azure Active Directory 끝점 생성(HA만 해당)
- Cloud Volumes ONTAP 구성

#### Azure 애플리케이션 등록

1. 먼저 Cloud Volumes ONTAP가 Azure 키 저장소에 액세스하기 위해 사용할 Azure 구독에 응용 프로그램을 등록해야 합니다. Azure 포털에서 앱 등록 을 선택합니다.
2. 새 등록\*\* 을 선택합니다.
3. 응용 프로그램의 이름을 제공하고 지원되는 응용 프로그램 유형을 선택합니다. Azure Key Vault 사용에 대한 기본 단일 테넌트 접미사 **Register** (등록\*\*)을 선택합니다.
4. Azure 개요 창에서 등록한 애플리케이션을 선택합니다. 애플리케이션(클라이언트) ID 및 디렉토리(테넌트) ID 를 안전한 위치에 복사합니다. 등록 프로세스 후반부에 필요합니다.

#### Azure 클라이언트 암호를 생성합니다

1. Azure 키 저장소 앱 등록을 위한 Azure 포털에서 인증서 및 비밀 창을 선택합니다.
2. 새 클라이언트 암호\*\* 를 선택합니다. 클라이언트 비밀에 의미 있는 이름을 입력합니다. NetApp에서는 24개월의 만료 기간을 권장합니다. 단, 특정 클라우드 거버넌스 정책에는 다른 설정이 필요할 수 있습니다.
3. 클라이언트 암호를 만들려면 추가 를 클릭합니다. 값\*\* 열에 나열된 암호 문자열을 복사하여 에서 나중에 사용할 수 있도록 안전한 위치에 저장합니다 [Cloud Volumes ONTAP 구성](#). 페이지를 벗어나 이동하면 암호 값이 다시 표시되지 않습니다.

#### Azure Key Vault를 작성합니다

1. 기존 Azure 키 저장소가 있는 경우 Cloud Volumes ONTAP 구성에 연결할 수 있지만 이 프로세스의 설정에 액세스 정책을 적용해야 합니다.
2. Azure 포털에서 **Key Vaults** 섹션으로 이동합니다.
3. **+Create**를 클릭하고 리소스 그룹, 지역 및 가격 책정 계층을 포함한 필수 정보를 입력합니다. 또한, 삭제된 볼트를 보관할 일 수를 입력하고 키 볼트에서 삭제 보호 활성화를 선택합니다.
4. 액세스 정책을 선택하려면 다음 을 선택합니다.
5. 다음 옵션을 선택합니다.
  - a. **Access configuration** 아래에서 **Vault access policy**를 선택합니다.
  - b. 리소스 액세스 아래에서 볼륨 암호화를 위한 **Azure** 디스크 암호화 를 선택합니다.
6. 액세스 정책을 추가하려면 **+ Create** 를 선택합니다.
7. 템플릿에서 구성 아래에서 드롭다운 메뉴를 클릭한 다음 키, 암호 및 인증서 관리\*\* 템플릿을 선택합니다.
8. 각 드롭다운 권한 메뉴(키, 암호, 인증서)를 선택한 다음 메뉴 목록 상단의 모두 선택 을 선택하여 사용 가능한 모든 권한을 선택합니다. 다음과 같은 항목이 있어야 합니다.
  - 키 권한:20이 선택되었습니다
  - 비밀 권한:8 선택됨
  - 인증서 권한:16 선택됨

# Create an access policy



- 1 **Permissions**   2 Principal   3 Application (optional)   4 Review + create

Configure from a template

Key, Secret, & Certificate Management

## Key permissions

### Key Management Operations

- Select all
- Get
- List
- Update
- Create
- Import
- Delete
- Recover
- Backup
- Restore

### Cryptographic Operations

- Select all
- Decrypt
- Encrypt
- Unwrap Key
- Wrap Key
- Verify
- Sign

### Privileged Key Operations

- Select all
- Purge
- Release

### Rotation Policy Operations

- Select all
- Rotate
- Get Rotation Policy
- Set Rotation Policy

## Secret permissions

### Secret Management Operations

- Select all
- Get
- List
- Set
- Delete
- Recover
- Backup
- Restore

### Privileged Secret Operations

- Select all
- Purge

## Certificate permissions

### Certificate Management Operations

- Select all
- Get
- List
- Update
- Create
- Import
- Delete
- Recover
- Backup
- Restore
- Manage Contacts
- Manage Certificate Authorities
- Get Certificate Authorities
- List Certificate Authorities
- Set Certificate Authorities
- Delete Certificate Authorities

### Privileged Certificate Operations

- Select all
- Purge

Previous

Next



9. 에서 만든 기본 Azure 등록 응용 프로그램을 선택하려면 다음 을 클릭합니다 [Azure 애플리케이션 등록](#). 다음\*\* 을 선택합니다.



정책당 하나의 보안 주기만 할당할 수 있습니다.

## Create an access policy ✕

✓ Permissions
2 Principal
③ Application (optional)
④ Review + create

Only 1 principal can be assigned per access policy.  
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

**Selected item**

No item selected

---

Previous
Next

10. 검토 후 작성 이 나타날 때까지 다음 을 두 번 클릭합니다. 그런 다음 만들기 를 클릭합니다.
11. 다음 을 선택하여 네트워킹 옵션으로 진행합니다.
12. 적절한 네트워크 액세스 방법을 선택하거나 모든 네트워크 및 검토 + 작성을 선택하여 키 볼트를 작성합니다.  
(네트워크 액세스 방법은 거버넌스 정책 또는 회사 클라우드 보안 팀에서 규정할 수 있습니다.)
13. 키 볼트 URI 기록: 작성한 키 볼트에서 개요 메뉴로 이동하여 오른쪽 컬럼에서 볼트 **URI**를 복사합니다. 이 작업은 나중에 수행해야 합니다.

암호화 키를 생성합니다

1. Cloud Volumes ONTAP에 대해 만든 키 저장소 메뉴에서 키 옵션으로 이동합니다.
2. 새 키를 만들려면 **Generate/import** 를 선택합니다.
3. 기본 옵션을 **Generate** 로 설정된 상태로 둡니다.
4. 다음 정보를 제공합니다.
  - 암호화 키 이름입니다

- 키 유형: RSA
- RSA 키 크기: 2048
- 사용: 예

5. 암호화 키를 만들려면 만들기 를 선택합니다.
6. 키 메뉴로 돌아가서 방금 만든 키를 선택합니다.
7. 키 속성을 보려면 현재 버전 아래에서 키 ID를 선택합니다.
8. 키 식별자 필드를 찾습니다. 16진수 문자열을 포함하지만 포함되지 않는 최대 URI를 복사합니다.

#### Azure Active Directory 끝점 생성(HA만 해당)

1. 이 프로세스는 HA Cloud Volumes ONTAP 작업 환경을 위해 Azure 키 저장소를 구성하는 경우에만 필요합니다.
2. Azure 포털에서 가상 네트워크로 이동합니다.
3. Cloud Volumes ONTAP 작업 환경을 배포한 가상 네트워크를 선택하고 페이지 왼쪽의 **Subnets** 메뉴를 선택합니다.
4. 목록에서 Cloud Volumes ONTAP 구축의 서브넷 이름을 선택합니다.
5. 서비스 엔드포인트 제목으로 이동합니다. 드롭다운 메뉴에서 다음을 선택합니다.
  - NET Framework 클래스 라이브러리 Control.OnEventArgs 클래스 참고: 이 속성은 .NET Framework 버전 2.0
  - **Microsoft.KeyVault**
  - **Microsoft.Storage**(선택 사항)

**SERVICE ENDPOINTS**

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

3 selected

Service	Status	
Microsoft.Storage	Succeeded	
Microsoft.AzureActiveDirectory	Succeeded	
Microsoft.KeyVault	Succeeded	

Service endpoint policies

0 selected

**SUBNET DELEGATION**

Delegate subnet to a service ⓘ

None

**NETWORK POLICY FOR PRIVATE ENDPOINTS**

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. [Learn more](#)

Private endpoint network policy

Disabled

**Save** **Cancel**

6. 설정을 캡처하려면 저장을 선택합니다.

#### Cloud Volumes ONTAP 구성

1. 기본 SSH 클라이언트를 사용하여 클러스터 관리 LIF에 연결합니다.
2. ONTAP에서 고급 권한 모드로 들어갑니다.

```
set advanced -con off
```

3. 원하는 Data SVM을 식별하고 DNS 구성을 확인합니다.

```
vserver services name-service dns show
```

- a. 원하는 데이터 SVM에 대한 DNS 항목이 있고 Azure DNS에 대한 항목이 포함된 경우 별도의 조치가 필요하지 않습니다. 그렇지 않으면 Azure DNS, 프라이빗 DNS 또는 사내 서버를 가리키는 데이터 SVM용 DNS 서버 항목을 추가합니다. 이 값은 클러스터 관리자 SVM의 항목과 일치해야 합니다.

```
vserver services name-service dns create -vserver SVM_name -domains domain  
-name-servers IP_address
```

- b. 데이터 SVM에 대한 DNS 서비스가 생성되었는지 확인합니다.

```
vserver services name-service dns show
```

4. 응용 프로그램 등록 후 저장된 클라이언트 ID 및 테넌트 ID를 사용하여 Azure Key Vault를 활성화합니다.

```
security key-manager external azure enable -vserver SVM_name -client-id  
Azure_client_ID -tenant-id Azure_tenant_ID -name Azure_key_vault_name -key-id  
Azure_key_ID
```

5. 키 관리자의 상태를 확인합니다.

```
security key-manager external azure check  
출력은 다음과 같이 표시됩니다.
```

```
::*> security key-manager external azure check
```

```
Vserver: data_svm_name
```

```
Node: akvlab01-01
```

```
Category: service_reachability
```

```
Status: OK
```

```
Category: ekmip_server
```

```
Status: OK
```

```
Category: kms_wrapped_key_status
```

```
Status: UNKNOWN
```

```
Details: No volumes created yet for the vserver. Wrapped KEK status  
will be available after creating encrypted volumes.
```

```
3 entries were displayed.
```

를 누릅니다 `service_reachability` 상태가 아닙니다 `OK` SVM은 필요한 모든 연결 및 사용 권한으로 Azure Key Vault 서비스에 연결할 수 없습니다. Azure 네트워크 정책 및 라우팅으로 인해 프라이빗 VNET가 Azure KeyVault Public 엔드포인트에 도달하지 못하도록 차단하지 않는지 확인합니다. 이러한 경우, VNET 내에서 키 볼트에 액세스하기 위해 Azure 프라이빗 끝점을 사용하는 것이 좋습니다. 또한 종점의 전용 IP 주소를 확인하기 위해 SVM에 정적 호스트 항목을 추가해야 할 수도 있습니다.

를 클릭합니다 `kms_wrapped_key_status` 보고합니다 UNKNOWN 초기 구성 시 상태가 로 변경됩니다 OK 첫 번째 볼륨이 암호화된 후

6. 선택 사항: NVE의 기능을 확인하기 위한 테스트 볼륨을 생성합니다.

```
vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
-state online -policy default
```

올바르게 구성된 경우 Cloud Volumes ONTAP는 자동으로 볼륨을 생성하고 볼륨 암호화를 활성화합니다.

7. 볼륨이 올바르게 생성되고 암호화되었는지 확인합니다. 있다면, 입니다 `-is-encrypted` 매개 변수는 로 표시됩니다 `true`.

```
vol show -vserver SVM_name -fields is-encrypted
```

## Google의 클라우드 키 관리 서비스로 키를 관리합니다

을 사용할 수 있습니다 "[Google Cloud Platform의 키 관리 서비스\(Cloud KMS\)](#)" Google Cloud Platform에서 구축한 응용 프로그램에서 ONTAP 암호화 키를 보호합니다.

Cloud KMS를 사용한 키 관리는 CLI 또는 ONTAP REST API를 통해 활성화할 수 있습니다.

Cloud KMS를 사용할 때는 기본적으로 데이터 SVM의 LIF가 클라우드 키 관리 엔드포인트와 통신하는 데 사용됩니다. 노드 관리 네트워크는 클라우드 공급자의 인증 서비스(`oauth2.googleapis.com` 통신하는 데 사용됩니다. 클러스터 네트워크가 올바르게 구성되지 않은 경우 클러스터는 키 관리 서비스를 제대로 사용하지 않습니다.

시작하기 전에

- Cloud Volumes ONTAP에서 버전 9.10.1 이상을 실행해야 합니다
- VE(Volume Encryption) 라이선스가 설치되었습니다
- 멀티 테넌트 암호화 키 관리(MTEKM) 라이선스가 설치되어 있으며 Cloud Volumes ONTAP 9.12.1 GA부터 시작합니다.
- 클러스터 또는 SVM 관리자여야 합니다
- Google Cloud Platform의 활성 서브스크립션입니다

제한 사항

- 클라우드 KMS는 데이터 SVM에서만 구성할 수 있습니다

구성

### Google 클라우드

1. Google Cloud 환경에서는 "[대칭 GCP 키 링 및 키를 생성합니다](#)".
2. Cloud Volumes ONTAP 서비스 계정에 대한 사용자 지정 역할을 만듭니다.

```

gcloud iam roles create kmsCustomRole
  --project=<project_id>
  --title=<kms_custom_role_name>
  --description=<custom_role_description>

  --permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA

```

- 클라우드 KMS 키 및 Cloud Volumes ONTAP 서비스 계정에 사용자 지정 역할을 할당합니다.

```

gcloud kms keys add-iam-policy-binding key_name --keyring key_ring_name
--location key_location --member serviceAccount:_service_account_Name_ --role
projects/customer_project_id/roles/kmsCustomRole

```

- 서비스 계정 JSON 키 다운로드:

```

gcloud iam service-accounts keys create key-file --iam-account=sa-name
@project-id.iam.gserviceaccount.com

```

## Cloud Volumes ONTAP

- 기본 SSH 클라이언트를 사용하여 클러스터 관리 LIF에 연결합니다.

- 고급 권한 레벨로 전환합니다.

```
set -privilege advanced
```

- 데이터 SVM을 위한 DNS를 생성합니다.

```
dns create -domains c.<project>.internal -name-servers server_address -vserver
SVM_name
```

- CMEK 항목 작성:

```
security key-manager external gcp enable -vserver SVM_name -project-id project
-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name
key_name
```

- 메시지가 표시되면 GCP 계정의 서비스 계정 JSON 키를 입력합니다.

- 활성화된 프로세스가 성공했는지 확인합니다.

```
security key-manager external gcp check -vserver svm_name
```

- 선택 사항: 암호화를 테스트할 볼륨을 생성합니다
- ```
vol create volume_name -aggregate aggregate
-vserver vserver_name -size 10G
```

## 문제 해결

문제를 해결해야 하는 경우 위의 마지막 두 단계에서 원시 REST API 로그를 지정할 수 있습니다.

- set d

- systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2\_client.log

## 랜섬웨어에 대한 보호 개선









랜섬웨어 공격은 비즈니스 시간, 리소스 및 평판에 악영향을 줄 수 있습니다. BlueXP를 사용하면 일반적인 랜섬웨어 파일 확장으로부터 보호하는 것과 자율적 랜섬웨어 방어(ARP)라는 두 가지 NetApp 솔루션을 랜섬웨어용 구현할 수 있습니다. 이러한 솔루션은 가시성, 감지, 문제 해결을 위한 효과적인 툴을 제공합니다.

### 일반적인 랜섬웨어 파일 확장명으로부터 보호

BlueXP를 통해 제공되는 랜섬웨어 방어 설정에서 ONTAP FPolicy 기능을 활용하여 일반적인 랜섬웨어 파일 확장 유형을 방지할 수 있습니다.

### 단계

1. Canvas 페이지에서 랜섬웨어 보호를 구성하는 시스템의 이름을 두 번 클릭합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 \* 랜섬웨어 보호 \* 옆에 있는 연필 아이콘을 클릭합니다.

| Information              |                            | Features                                                                                     |
|--------------------------|----------------------------|----------------------------------------------------------------------------------------------|
| Working Environment Tags |                            | Tags      |
| Scheduled Downtime       |                            | Off       |
| S3 Storage Classes       | Standard-Infrequent Access |           |
| Instance Type            | m5.xlarge                  |           |
| Write Speed              |                            | Normal  |
| Ransomware Protection    |                            | Off     |
| Support Registration     | Not Registered             |         |
| CIFs Setup               |                            |         |

3. 랜섬웨어에 대한 NetApp 솔루션 구현:

- a. 스냅샷 정책이 활성화되지 않은 볼륨이 있는 경우 \* 스냅샷 정책 활성화 \* 를 클릭합니다.



NetApp Snapshot 기술은 랜섬웨어 해결을 위한 업계 최고의 솔루션을 제공합니다. 성공적인 복구의 핵심은 감염되지 않은 백업에서 복원하는 것입니다. Snapshot 복사본은 읽기 전용이므로 랜섬웨어 손상을 방지합니다. 또한 세분화하여 단일 파일 복사본 또는 전체 재해 복구 솔루션의 이미지를 생성할 수도 있습니다.

- b. FPolicy \* 활성화 를 클릭하여 ONTAP의 FPolicy 솔루션을 활성화합니다. FPolicy 솔루션은 파일의 확장명에 따라 파일 작업을 차단할 수 있습니다.

이 예방적 솔루션은 일반적인 랜섬웨어 파일 유형을 차단하여 랜섬웨어 공격으로부터 보호를 개선합니다.

기본 FPolicy 범위는 다음 확장명의 파일을 차단합니다.

마이크로, 암호화, 잠김, 암호화, 암호화, crinf, r5a, XRNT, XTBL, R16M01D05, pzdc, 양호, LOL!, OMG!, RDM, RK, encryptedRS, crjoker, enciped, LeChiffre



Cloud Volumes ONTAP에서 FPolicy를 활성화하면 BlueXP에서 이 범위가 생성됩니다. 이 목록은 일반적인 랜섬웨어 파일 유형을 기반으로 합니다. Cloud Volumes ONTAP CLI에서 `vserver FPolicy scope` 명령을 사용하여 차단된 파일 확장명을 사용자 지정할 수 있습니다.

**Ransomware Protection**

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

**1 Enable Snapshot Copy Protection**

50 % Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

[Activate Snapshot Policy](#)

**2 Block Ransomware File Extensions**

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

[View Denied File Names](#)

[Activate FPolicy](#)

## 자율 랜섬웨어 보호

Cloud Volumes ONTAP는 워크로드 분석을 수행하여 랜섬웨어 공격을 나타낼 수 있는 비정상적인 활동을 사전에 감지하고 경고하는 ARP(Autonomous 랜섬웨어 Protection) 기능을 지원합니다.

를 통해 제공되는 파일 확장자 보호와 분리됩니다 "랜섬웨어 차단 설정"ARP 기능은 워크로드 분석을 사용하여 감지된 "비정상적인 활동"을 기반으로 잠재적인 공격에 대해 사용자에게 경고합니다. 랜섬웨어 차단 설정과 ARP 기능을 모두 포괄적인 랜섬웨어 방어에 함께 사용할 수 있습니다.

ARP 기능은 노드 기반 및 용량 기반 라이선스 모델 모두에서 BYOL 라이선스(1년, 2년, 3년 조건)에만 사용할 수 있습니다. Cloud Volumes ONTAP의 ARP 기능과 함께 사용하기 위해 별도의 새 애드온 라이선스를 구입하려면 NetApp 영업 담당자에게 문의해야 합니다.

추가 라이선스를 구입하여 디지털 지갑에 추가하면 Cloud Volumes ONTAP를 사용하여 볼륨별로 ARP를 활성화할 수 있습니다. 볼륨에 대한 ARP 구성은 ONTAP 시스템 관리자 및 ONTAP CLI를 통해 수행됩니다.

ONTAP 시스템 관리자 및 CLI에서 ARP를 활성화하는 방법에 대한 자세한 내용은 를 참조하십시오 "자율주행 랜섬웨어 보호 활성화".



라이센스가 없는 경우 라이선스가 부여된 기능을 사용할 수 없습니다.

**Autonomous Ransomware Protection** ⓘ

|                                    |                                         |                       |
|------------------------------------|-----------------------------------------|-----------------------|
| <b>0</b> TiB<br>Protected Capacity | <b>100</b> TiB<br>Precommitted capacity | <b>0</b> TiB<br>PAYGO |
|                                    | BYOL <b>100 TiB</b>                     |                       |
|                                    | Marketplace Contracts <b>0 TiB</b>      |                       |

## 시스템 관리

### Cloud Volumes ONTAP 소프트웨어를 업그레이드합니다

BlueXP에서 Cloud Volumes ONTAP를 업그레이드하여 최신 새 기능 및 향상된 기능을 이용할 수 있습니다. 소프트웨어를 업그레이드하기 전에 Cloud Volumes ONTAP 시스템을 준비해야 합니다.

#### 업그레이드 개요

Cloud Volumes ONTAP 업그레이드 프로세스를 시작하기 전에 다음 사항을 숙지해야 합니다.

#### BlueXP에서만 업그레이드합니다

Cloud Volumes ONTAP 업그레이드는 BlueXP에서 완료해야 합니다. System Manager 또는 CLI를 사용하여 Cloud Volumes ONTAP를 업그레이드해서는 안 됩니다. 이렇게 하면 시스템 안정성에 영향을 줄 수 있습니다.

#### 업그레이드 방법

BlueXP는 Cloud Volumes ONTAP를 업그레이드할 수 있는 두 가지 방법을 제공합니다.

- 작업 환경에 나타나는 업그레이드 알림을 따릅니다
- 업그레이드 이미지를 HTTPS 위치에 배치한 다음 BlueXP에 URL을 제공합니다

#### 지원되는 업그레이드 경로

업그레이드할 수 있는 Cloud Volumes ONTAP 버전은 현재 실행 중인 Cloud Volumes ONTAP 버전에 따라 다릅니다.

|              |                        |
|--------------|------------------------|
| 현재 버전        | 로 직접 업그레이드할 수 있는 버전입니다 |
| 9.13.0       | 9.13.1                 |
| 9.12.1       | 9.13.1                 |
|              | 9.13.0                 |
| 9.12.0       | 9.12.1                 |
| 9.11.1       | 9.12.1                 |
|              | 9.12.0                 |
| 9.11.0       | 9.11.1                 |
| 9.10.1       | 9.11.1                 |
|              | 9.11.0                 |
| 9.10.0       | 9.10.1                 |
| 9.9.1        | 9.10.1                 |
|              | 9.10.0                 |
| 9.9.0        | 9.9.1                  |
| 9.8          | 9.9.1                  |
| 9.7          | 9.8                    |
| 9.6          | 9.7                    |
| 9.5          | 9.6                    |
| 9.4 를 참조하십시오 | 9.5                    |
| 9.3          | 9.4 를 참조하십시오           |
| 9.2          | 9.3                    |
| 9.1          | 9.2                    |
| 9.0          | 9.1                    |
| 8.3          | 9.0                    |

다음 사항에 유의하십시오.

- Cloud Volumes ONTAP에 대해 지원되는 업그레이드 경로는 사내 ONTAP 클러스터에 대한 업그레이드 경로와 다릅니다.
- 작업 환경에 나타나는 업그레이드 알림에 따라 업그레이드하는 경우 BlueXP에서 지원되는 업그레이드 경로 다음에 나오는 릴리스로 업그레이드하라는 메시지가 표시됩니다.
- HTTPS 위치에 업그레이드 이미지를 배치하여 업그레이드하는 경우 지원되는 업그레이드 경로를 따르십시오.
- 경우에 따라 타겟 릴리스로 업그레이드하기 위해 몇 차례 업그레이드해야 할 수도 있습니다.

예를 들어 9.8 버전을 실행 중이고 9.10.1로 업그레이드하려면 먼저 9.9.1 버전으로 업그레이드한 다음 9.10.1로 업그레이드해야 합니다.

- 패치(P) 릴리스의 경우 한 버전 릴리스에서 다음 버전의 모든 P 릴리스로 업그레이드할 수 있습니다.

다음은 몇 가지 예입니다.

- 9.13.0 > 9.13.1P15
- 9.12.1 > 9.13.1P2

되돌리기 또는 다운그레이드

Cloud Volumes ONTAP를 이전 릴리즈로 되돌리거나 다운그레이드하는 것은 지원되지 않습니다.

지원 등록

이 페이지에 설명된 방법을 사용하여 소프트웨어를 업그레이드하려면 Cloud Volumes ONTAP를 NetApp 지원 팀에 등록해야 합니다. 이 내용은 PAYGO 및 BYOL 모두에 적용됩니다. 필요한 것이 있습니다 ["PAYGO 시스템을 수동으로 등록합니다"](#) BYOL 시스템은 기본적으로 등록되지만



지원이 등록되지 않은 시스템은 새 버전이 출시되어도 BlueXP에 나타나는 소프트웨어 업데이트 알림을 계속 받게 됩니다. 그러나 소프트웨어를 업그레이드하기 전에 시스템을 등록해야 합니다.

HA 중재자의 업그레이드

또한 BlueXP는 Cloud Volumes ONTAP 업그레이드 프로세스 중에 필요에 따라 중재자 인스턴스를 업데이트합니다.

업그레이드 준비

업그레이드를 수행하기 전에 시스템이 준비되어 있는지 확인하고 필요한 구성을 변경해야 합니다.

- [다운타임을 계획합니다](#)
- [자동 반환이 여전히 활성화되어 있는지 확인합니다](#)
- [SnapMirror 전송을 일시 중단합니다](#)
- [애그리게이트가 온라인 상태인지 확인합니다](#)

다운타임을 계획합니다

단일 노드 시스템을 업그레이드할 경우 업그레이드 프로세스에서는 I/O가 중단되는 동안 시스템을 최대 25분 동안 오프라인 상태로 전환합니다.

대부분의 경우 HA 쌍의 업그레이드는 무중단으로 가능하며 I/O는 중단되지 않습니다. 이 무중단 업그레이드 프로세스 중에 각 노드가 동시 업그레이드되어 클라이언트에 I/O를 계속 제공합니다.

세션 지향 프로토콜은 업그레이드 중 특정 영역의 클라이언트 및 애플리케이션에 부정적인 영향을 미칠 수 있습니다. 자세한 내용은 ["ONTAP 설명서를 참조하십시오"](#)

자동 반환이 여전히 활성화되어 있는지 확인합니다

Cloud Volumes ONTAP HA 쌍(기본 설정)에서 자동 반환이 활성화되어 있어야 합니다. 그렇지 않으면 작업이 실패합니다.

["ONTAP 9 설명서: 자동 반환 구성을 위한 명령입니다"](#)

## SnapMirror 전송을 일시 중단합니다

Cloud Volumes ONTAP 시스템에 활성 SnapMirror 관계가 있는 경우 Cloud Volumes ONTAP 소프트웨어를 업데이트하기 전에 전송을 일시 중지하는 것이 좋습니다. 전송을 일시 중단하면 SnapMirror 장애가 방지됩니다. 대상 시스템에서 전송을 일시 중지해야 합니다.



BlueXP 백업 및 복구는 SnapMirror 구현을 사용하여 백업 파일(SnapMirror Cloud라고 함)을 생성하지만 시스템을 업그레이드할 때 백업을 일시 중단할 필요가 없습니다.

이 작업에 대해

다음 단계에서는 버전 9.3 이상에서 System Manager를 사용하는 방법을 설명합니다.

단계

1. 대상 시스템에서 System Manager에 로그인합니다.

웹 브라우저에서 클러스터 관리 LIF의 IP 주소를 지정하면 System Manager에 로그인할 수 있습니다. Cloud Volumes ONTAP 작업 환경에서 IP 주소를 찾을 수 있습니다.



BlueXP에 액세스하는 컴퓨터에는 Cloud Volumes ONTAP에 대한 네트워크 연결이 있어야 합니다. 예를 들어, 클라우드 제공업체 네트워크에 있는 점프 호스트에서 BlueXP에 로그인해야 할 수 있습니다.

2. 보호 > 관계 \* 를 클릭합니다.
3. 관계를 선택하고 \* 작업 > 정지 \* 를 클릭합니다.

애그리게이트가 온라인 상태인지 확인합니다

소프트웨어를 업데이트하기 전에 Cloud Volumes ONTAP용 애그리게이트가 온라인 상태여야 합니다. 애그리게이트는 대부분의 구성에서 온라인 상태여야 하지만, 그렇지 않을 경우 온라인 상태로 전환할 수 있습니다.

이 작업에 대해

다음 단계에서는 버전 9.3 이상에서 System Manager를 사용하는 방법을 설명합니다.

단계

1. 작업 환경에서 \* 집계 \* 탭을 클릭합니다.
2. 집계 제목 아래에서 타원 버튼을 클릭한 다음 \* 집계 세부 정보 보기 \* 를 선택합니다.

| Aggregate Details |                     |
|-------------------|---------------------|
| aggr1             |                     |
| Overview          | Capacity Allocation |
| State             | online              |
| Home Node         | *****               |
| Encryption Type   | cloudEncrypted      |
| Volumes           | 2 ▾                 |

3. 애그리게이트는 오프라인 상태인 경우 System Manager를 사용하여 애그리게이트를 온라인 상태로 전환합니다.
  - a. 스토리지 > 애그리게이트 및 디스크 > 애그리게이트 \* 를 클릭합니다.
  - b. 애그리게이트를 선택한 다음 \* 추가 작업 > 상태 > 온라인 \* 을 클릭합니다.

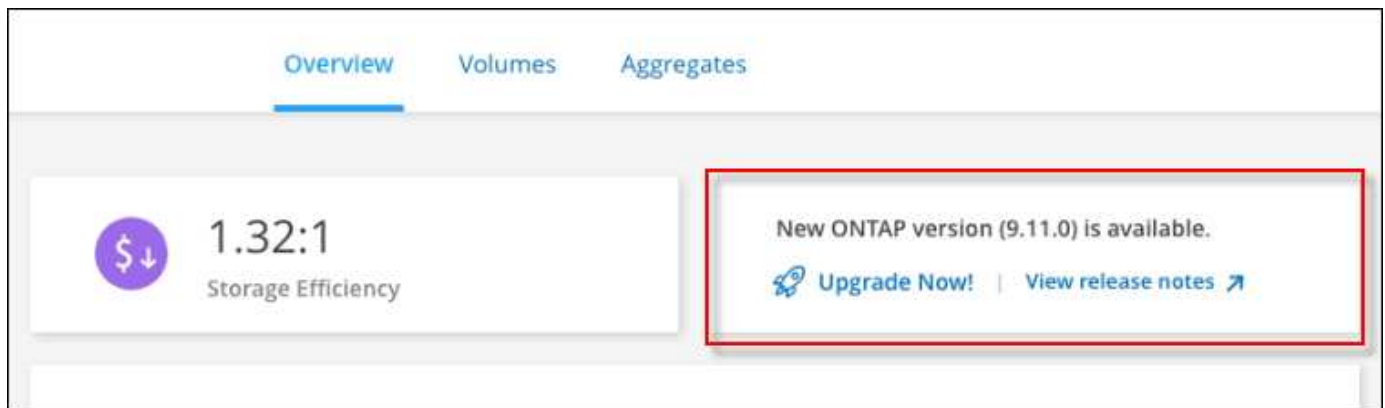
### Cloud Volumes ONTAP를 업그레이드합니다

BlueXP는 새 버전을 업그레이드할 수 있을 때 사용자에게 알립니다. 이 알림에서 업그레이드 프로세스를 시작할 수 있습니다. 자세한 내용은 [을 참조하십시오](#) [BlueXP 알림에서 업그레이드합니다](#).

외부 URL의 이미지를 사용하여 소프트웨어 업그레이드를 수행하는 또 다른 방법입니다. 이 옵션은 BlueXP가 S3 버킷을 액세스하여 소프트웨어를 업그레이드할 수 없거나 패치가 제공된 경우에 유용합니다. 자세한 내용은 [을 참조하십시오](#) [URL에서 사용할 수 있는 이미지에서 업그레이드합니다](#).

### BlueXP 알림에서 업그레이드합니다

BlueXP는 새 버전의 Cloud Volumes ONTAP를 사용할 수 있을 때 Cloud Volumes ONTAP 작업 환경에 알림을 표시합니다.



이 알림에서 업그레이드 프로세스를 시작하여 S3 버킷에서 소프트웨어 이미지를 가져온 다음 이미지를 설치한 다음 시스템을 다시 시작하여 프로세스를 자동화할 수 있습니다.

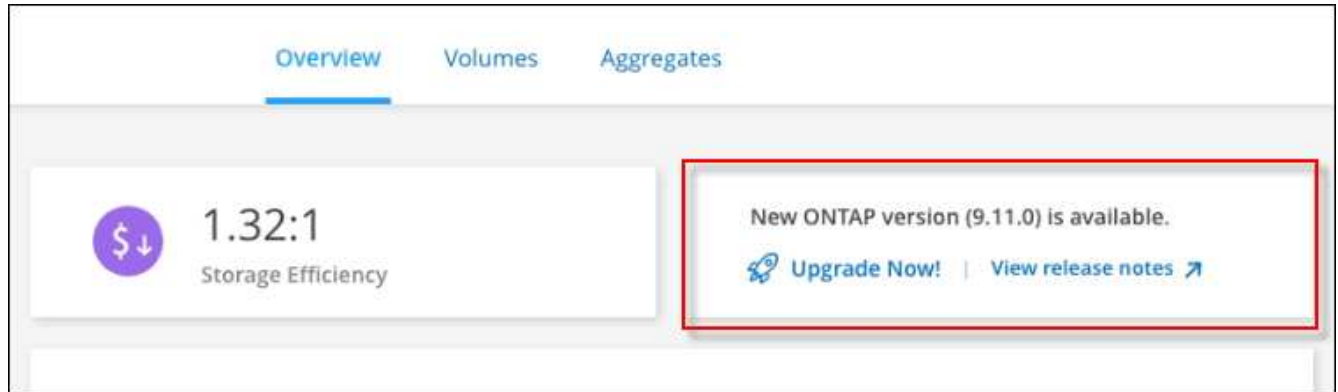
시작하기 전에

볼륨 또는 애그리게이트 생성과 같은 BlueXP 작업은 Cloud Volumes ONTAP 시스템에서 진행 중이지 않아야 합니다.

단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. 작업 환경을 선택합니다.

새 버전을 사용할 수 있는 경우 개요 탭에 알림이 나타납니다.



3. 새 버전을 사용할 수 있는 경우 \* 지금 업그레이드! \* 를 클릭합니다

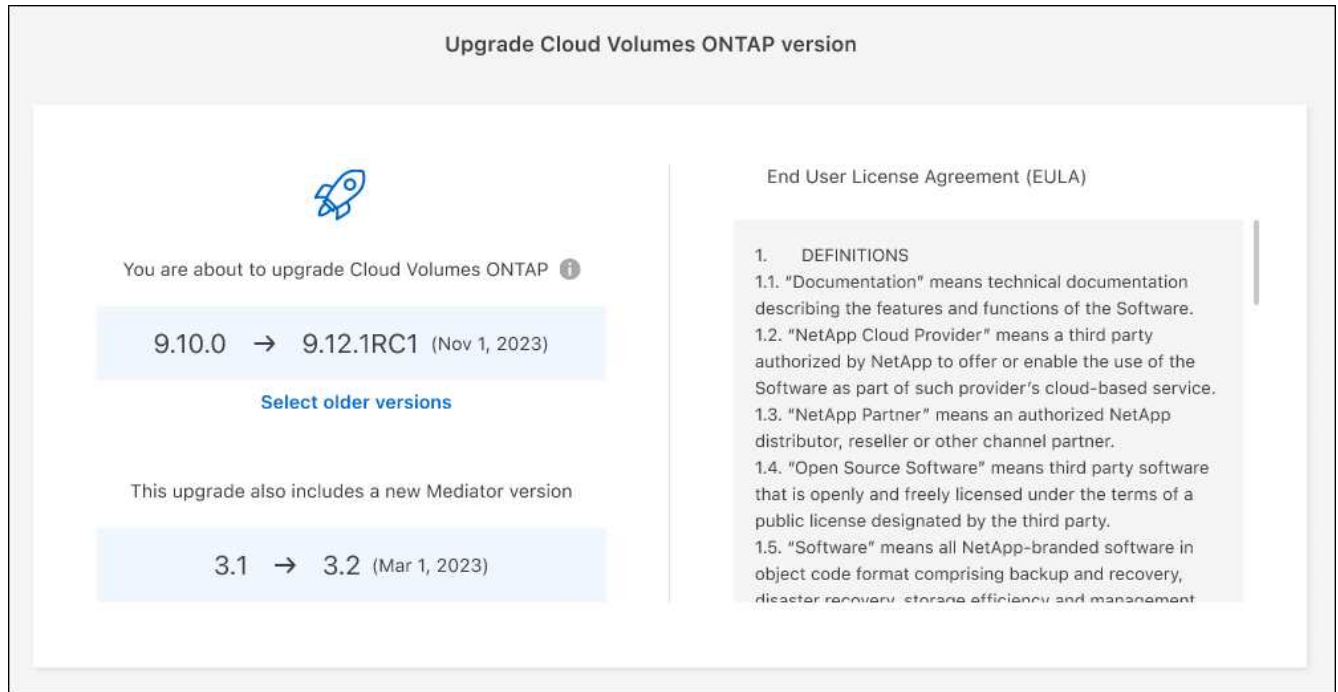


BlueXP 알림을 통해 Cloud Volumes ONTAP를 업그레이드하려면 먼저 NetApp Support 사이트 계정이 있어야 합니다.

4. Upgrade Cloud Volumes ONTAP 페이지에서 EULA를 읽은 다음 \* EULA \* 를 읽고 승인합니다 \* 를 선택합니다.
5. 업그레이드 \* 를 클릭합니다.



Upgrade Cloud Volumes ONTAP 페이지에서는 기본적으로 업그레이드할 최신 Cloud Volumes ONTAP 버전을 선택합니다. 사용 가능한 경우 \* 이전 버전 선택 \* 을 클릭하여 업그레이드를 위해 이전 버전의 Cloud Volumes ONTAP를 선택할 수 있습니다. 을 참조하십시오 "지원되는 업그레이드 경로 목록입니다" 현재 Cloud Volumes ONTAP 버전을 기반으로 적절한 업그레이드 경로를 선택합니다.



6. 업그레이드 상태를 확인하려면 설정 아이콘을 클릭하고 \* 타임라인 \* 을 선택합니다.

#### 결과

BlueXP가 소프트웨어 업그레이드를 시작합니다. 소프트웨어 업데이트가 완료되면 작업 환경에서 작업을 수행할 수 있습니다.

#### 작업을 마친 후

SnapMirror 전송을 일시 중지한 경우 System Manager를 사용하여 전송을 다시 시작합니다.

URL에서 사용할 수 있는 이미지에서 업그레이드합니다

Cloud Volumes ONTAP 소프트웨어 이미지를 커넥터 또는 HTTP 서버에 배치한 다음 BlueXP에서 소프트웨어 업그레이드를 시작할 수 있습니다. BlueXP에서 S3 버킷을 액세스하여 소프트웨어를 업그레이드할 수 없는 경우 이 옵션을 사용할 수 있습니다.

#### 시작하기 전에

- 볼륨 또는 애그리게이트 생성과 같은 BlueXP 작업은 Cloud Volumes ONTAP 시스템에서 진행 중이지 않아야 합니다.
- HTTPS를 사용하여 ONTAP 이미지를 호스팅하는 경우 인증서 누락으로 인한 SSL 인증 문제로 인해 업그레이드가 실패할 수 있습니다. 해결 방법은 ONTAP와 BlueXP 간의 인증에 사용할 CA 서명 인증서를 생성하고 설치하는 것입니다.

NetApp 기술 문서로 이동하여 단계별 지침을 확인하십시오.

["NetApp KB: 업그레이드 이미지를 호스팅하기 위해 BlueXP를 HTTPS 서버로 구성하는 방법"](#)

#### 단계

1. 선택 사항: Cloud Volumes ONTAP 소프트웨어 이미지를 호스팅할 수 있는 HTTP 서버를 설정합니다.

가상 네트워크에 VPN이 연결되어 있는 경우 Cloud Volumes ONTAP 소프트웨어 이미지를 자체 네트워크의



HTTP 서버에 배치할 수 있습니다. 그렇지 않으면 클라우드에 있는 HTTP 서버에 파일을 배치해야 합니다.

2. Cloud Volumes ONTAP에 대해 고유한 보안 그룹을 사용하는 경우 Cloud Volumes ONTAP가 소프트웨어 이미지에 액세스할 수 있도록 아웃바운드 규칙이 HTTP 연결을 허용하는지 확인합니다.



미리 정의된 Cloud Volumes ONTAP 보안 그룹은 기본적으로 아웃바운드 HTTP 연결을 허용합니다.

3. 에서 소프트웨어 이미지를 가져옵니다 "[NetApp Support 사이트](#)".
4. 파일을 제공할 Connector 또는 HTTP 서버의 디렉토리에 소프트웨어 이미지를 복사합니다.

두 개의 경로를 사용할 수 있습니다. 올바른 경로는 커넥터 버전에 따라 다릅니다.

- /opt/application/netapp/cloudmanager/docker\_occm/data/ontap/images/
- /opt/application/netapp/cloudmanager/ontap/images/

5. BlueXP의 작업 환경에서 \*... (타원 아이콘) \* 을 클릭한 다음 \* Cloud Volumes ONTAP 업데이트 \* 를 클릭합니다.
6. Cloud Volumes ONTAP 버전 업데이트 페이지에서 URL을 입력한 다음 \* 이미지 변경 \* 을 클릭합니다.

위에 표시된 경로의 커넥터에 소프트웨어 이미지를 복사한 경우 다음 URL을 입력합니다.

http://<Connector-private-IP-address>/ontap/images/<image-file-name> 를 참조하십시오



URL에서 \* image-file-name \* 은 "cot.image.9.13.1P2.tgz" 형식을 따라야 합니다.

7. 계속하려면 \* Proceed \* (진행 \*)를 클릭합니다.

#### 결과

BlueXP가 소프트웨어 업데이트를 시작합니다. 소프트웨어 업데이트가 완료되면 작업 환경에서 작업을 수행할 수 있습니다.

#### 작업을 마친 후

SnapMirror 전송을 일시 중지한 경우 System Manager를 사용하여 전송을 다시 시작합니다.

#### Google Cloud NAT 게이트웨이를 사용할 때 다운로드 오류를 수정합니다

커넥터는 Cloud Volumes ONTAP용 소프트웨어 업데이트를 자동으로 다운로드합니다. 구성에서 Google Cloud NAT 게이트웨이를 사용하는 경우 다운로드가 실패할 수 있습니다. 소프트웨어 이미지를 분할하는 부품 수를 제한하여 이 문제를 해결할 수 있습니다. 이 단계는 BlueXP API를 사용하여 완료해야 합니다.

#### 단계

1. 다음과 같은 JSON을 본문으로 /occm/config에 PUT 요청을 제출합니다.

```
{
  "maxDownloadSessions": 32
}
```

maxDownloadSessions\_ 값은 1이거나 1보다 큰 정수일 수 있습니다. 값이 1이면 다운로드한 이미지는 분할되지 않습니다.

32는 예제 값입니다. 사용할 값은 NAT 구성과 동시에 사용할 수 있는 세션 수에 따라 다릅니다.

["/occm/config API 호출에 대해 자세히 알아보십시오](#)".

## 선불 종량제 시스템을 등록하는 중입니다

NetApp의 지원은 Cloud Volumes ONTAP PAYGO 시스템에 포함되어 있지만 먼저 NetApp에 시스템을 등록하여 지원을 활성화해야 합니다.

모든 방법을 사용하여 ONTAP 소프트웨어를 업그레이드하려면 PAYGO 시스템을 NetApp에 등록해야 합니다 ["이 페이지에 설명되어 있습니다"](#).











지원이 등록되지 않은 시스템은 새 버전이 출시되어도 BlueXP에 나타나는 소프트웨어 업데이트 알림을 계속 받게 됩니다. 그러나 소프트웨어를 업그레이드하기 전에 시스템을 등록해야 합니다.

### 단계

1. NetApp Support 사이트 계정을 BlueXP에 아직 추가하지 않은 경우 \* 계정 설정 \* 으로 이동하여 지금 추가하십시오.

["NetApp Support 사이트 계정을 추가하는 방법을 알아보십시오"](#).

2. Canvas 페이지에서 등록할 시스템의 이름을 두 번 클릭합니다.
3. 개요 탭에서 기능 패널을 클릭한 다음 \* 지원 등록 \* 옆에 있는 연필 아이콘을 클릭합니다.

| Information              |                            | Features                                                                                      |
|--------------------------|----------------------------|-----------------------------------------------------------------------------------------------|
| Working Environment Tags |                            | Tags       |
| Scheduled Downtime       |                            | Off        |
| S3 Storage Classes       | Standard-Infrequent Access |            |
| Instance Type            |                            | m5.xlarge  |
| Write Speed              |                            | Normal   |
| Ransomware Protection    |                            | Off      |
| Support Registration     | Not Registered             |          |
| CIFs Setup               |                            |          |

4. NetApp Support 사이트 계정을 선택하고 \* Register \* 를 클릭합니다.

결과

BlueXP는 시스템을 NetApp에 등록합니다.

## Cloud Volumes ONTAP의 상태 관리

BlueXP에서 Cloud Volumes ONTAP를 중지하고 시작하여 클라우드 컴퓨팅 비용을 관리할 수 있습니다.

### Cloud Volumes ONTAP의 자동 종료 예약

특정 시간 간격 동안 Cloud Volumes ONTAP를 종료하여 컴퓨팅 비용을 낮출 수 있습니다. 이 작업을 수동으로 수행하는 대신 특정 시간에 시스템이 자동으로 종료된 후 다시 시작하도록 BlueXP를 구성할 수 있습니다.

이 작업에 대해

- Cloud Volumes ONTAP 시스템의 자동 종료를 예약하면 활성 데이터 전송이 진행 중인 경우 BlueXP가 종료를 연기합니다.









전송이 완료된 후 BlueXP가 시스템을 종료합니다.

- 이 작업은 HA 2노드에서 두 노드의 자동 종료를 예약합니다.
- 예약된 종료를 통해 Cloud Volumes ONTAP를 끌 때 부팅 및 루트 디스크의 스냅샷이 생성되지 않습니다.

스냅샷은 다음 섹션에 설명된 대로 수동 종료를 수행할 때만 자동으로 생성됩니다.

단계

1. Canvas 페이지에서 원하는 작업 환경을 두 번 클릭합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 \* 예정된 가동 중지 시간 \* 옆에 있는 연필 아이콘을 클릭합니다.

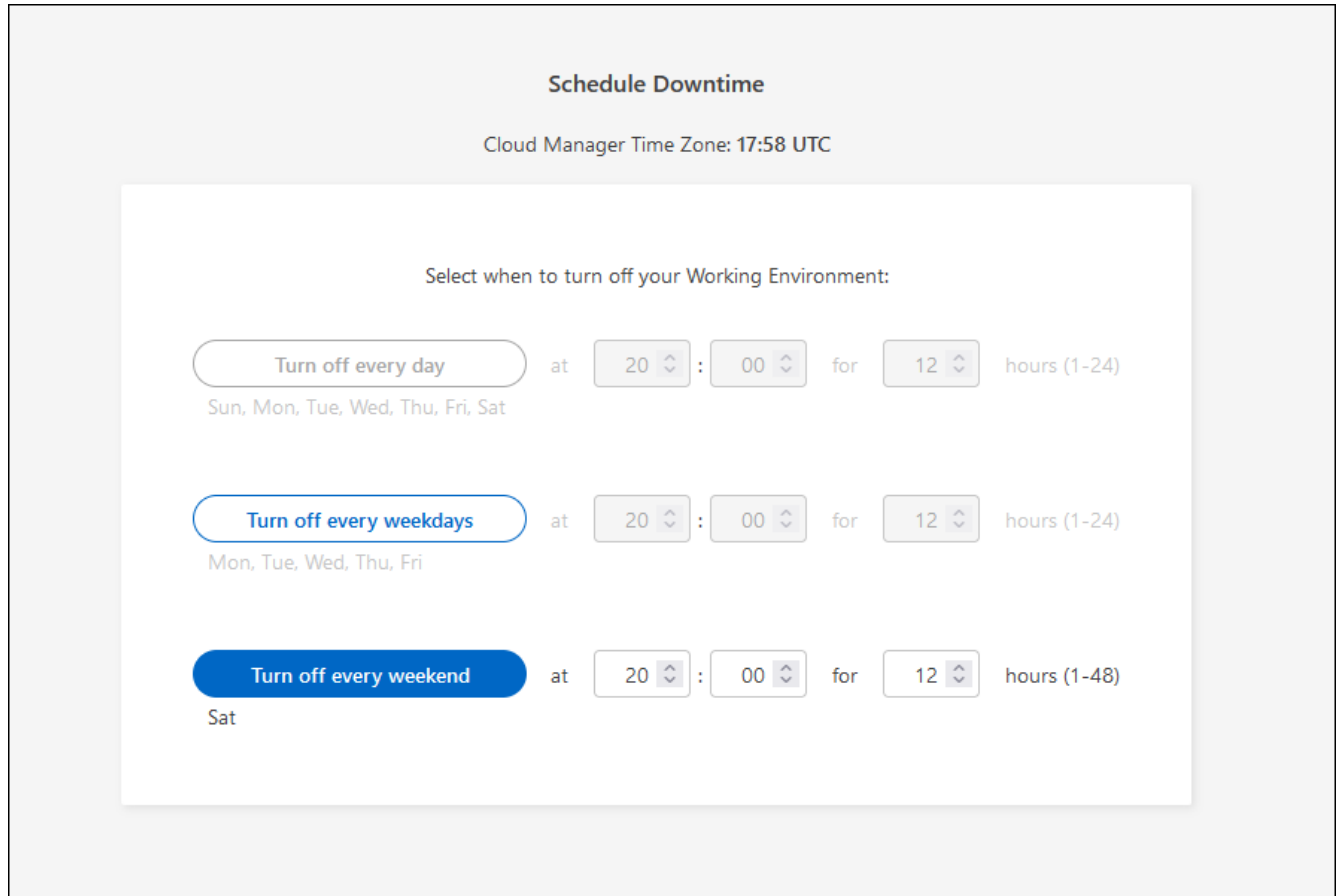
| Information              | Features                                                                                                       |
|--------------------------|----------------------------------------------------------------------------------------------------------------|
| Working Environment Tags | Tags                        |
| Scheduled Downtime       | Off                         |
| S3 Storage Classes       | Standard-Infrequent Access  |
| Instance Type            | m5.xlarge                   |
| Write Speed              | Normal                    |
| Ransomware Protection    | Off                       |
| Support Registration     | Not Registered            |
| CIFs Setup               |                           |

3. 종료 일정을 지정합니다.

- 매일, 매주 평일, 매주 또는 세 가지 옵션의 조합을 종료할지 여부를 선택합니다.
- 시스템 전원을 끌 시기 및 시스템 전원을 끌 시간을 지정합니다.

▪ 예 \*

다음 이미지는 매주 토요일 오후 20시에 BlueXP가 시스템을 종료하도록 지시하는 스케줄을 보여줍니다 (오후 8:00) 12시간 동안 BlueXP는 매주 월요일 오전 12시에 시스템을 다시 시작합니다



4. 저장 \* 을 클릭합니다.

결과

BlueXP는 일정을 저장합니다. Features(기능) 패널 아래의 해당 Scheduled Downtime line(예정된 가동 중지 라인) 항목에 'On(켜짐)'이 표시됩니다.

**Cloud Volumes ONTAP**를 중지하는 중입니다

Cloud Volumes ONTAP를 중지하면 계산 비용이 절약되고 루트 및 부팅 디스크의 스냅샷이 생성되므로 문제 해결에 도움이 됩니다.



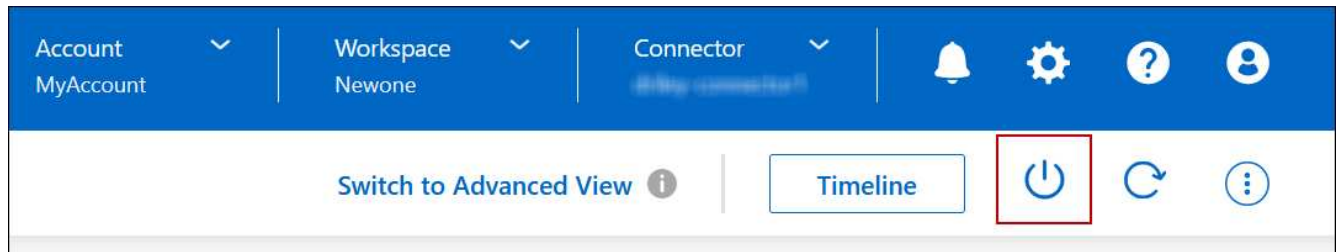
비용을 줄이기 위해 BlueXP는 루트 및 부팅 디스크의 이전 스냅샷을 주기적으로 삭제합니다. 루트와 부팅 디스크 모두에 대해 가장 최근의 두 스냅샷만 보존됩니다.

이 작업에 대해

HA 쌍을 중지하면 BlueXP가 두 노드를 모두 종료합니다.

단계

1. 작업 환경에서 \* 끄기 \* 아이콘을 클릭합니다.



2. 스냅샷이 시스템 복구를 활성화할 수 있으므로 스냅샷을 생성하는 옵션을 활성 상태로 유지합니다.
3. 끄기 \* 를 클릭합니다.

시스템을 중지하는 데 몇 분 정도 걸릴 수 있습니다. 나중에 작업 환경 페이지에서 시스템을 다시 시작할 수 있습니다.



스냅샷은 재부팅 시 자동으로 생성됩니다.

## NTP를 사용하여 시스템 시간을 동기화합니다

NTP 서버를 지정하면 네트워크 시스템 간의 시간이 동기화되어 시간 차이로 인한 문제를 방지할 수 있습니다.

를 사용하여 NTP 서버를 지정합니다 **"BlueXP API"** 또는 사용자 인터페이스에서 **"CIFS 서버를 생성합니다"**.

## 시스템 쓰기 속도를 수정합니다

BlueXP를 사용하면 Cloud Volumes ONTAP에 대한 일반 또는 고속 쓰기 속도를 선택할 수 있습니다. 기본 쓰기 속도는 정상입니다. 워크로드에 빠른 쓰기 성능이 필요한 경우 빠른 쓰기 속도로 변경할 수 있습니다.

모든 유형의 단일 노드 시스템 및 일부 HA 쌍 구성에서 고속 쓰기 속도가 지원됩니다. 에서 지원되는 구성을 봅니다 **"Cloud Volumes ONTAP 릴리즈 노트"**









쓰기 속도를 변경하려면 먼저 해야 합니다 **"정상 설정과 높음 설정의 차이를 이해합니다"**.

이 작업에 대해

- 볼륨 또는 애그리게이트 생성과 같은 작업이 진행 중이 아닌지 확인합니다.
- 이 변경 사항은 Cloud Volumes ONTAP 시스템을 다시 시작합니다. 이는 전체 시스템의 다운타임이 필요한 업무 중단입니다.

단계

1. Canvas 페이지에서 쓰기 속도로 구성하는 시스템의 이름을 두 번 클릭합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 \* 쓰기 속도 \* 옆에 있는 연필 아이콘을 클릭합니다.

| Information              | Features                                                                                                       |
|--------------------------|----------------------------------------------------------------------------------------------------------------|
| Working Environment Tags | Tags                        |
| Scheduled Downtime       | Off                         |
| S3 Storage Classes       | Standard-Infrequent Access  |
| Instance Type            | m5.xlarge                   |
| Write Speed              | Normal                    |
| Ransomware Protection    | Off                       |
| Support Registration     | Not Registered            |
| CIFs Setup               |                           |

3. Normal \* (정상 \*) 또는 \* High \* (높음 \*)를 선택합니다.

높음 을 선택한 경우 "이해했습니다..." 문장을 읽고 확인란을 선택하여 확인해야 합니다.





고속 \* 쓰기 속도 옵션은 버전 9.13.0부터 Google Cloud의 Cloud Volumes ONTAP HA 쌍에서 지원됩니다.

4. 저장 \* 을 클릭하고 확인 메시지를 검토한 다음 \* 승인 \* 을 클릭합니다.

## Cloud Volumes ONTAP의 암호를 변경합니다

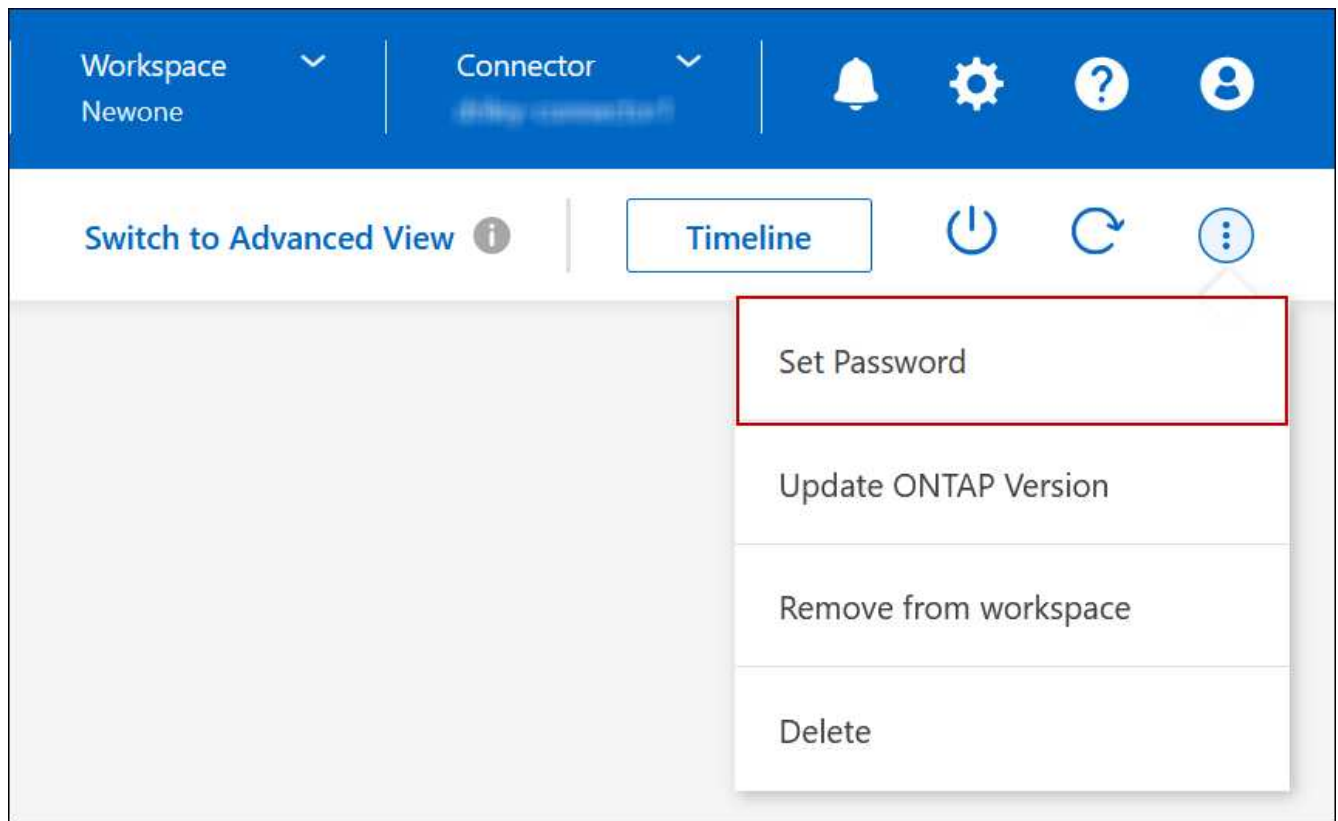
Cloud Volumes ONTAP에는 클러스터 관리자 계정이 포함되어 있습니다. 필요한 경우 BlueXP에서 이 계정의 암호를 변경할 수 있습니다.



System Manager 또는 CLI를 통해 admin 계정의 암호를 변경하지 마십시오. 암호는 BlueXP에 반영되지 않습니다. 따라서 BlueXP는 인스턴스를 제대로 모니터링할 수 없습니다.

단계

1. Canvas 페이지에서 Cloud Volumes ONTAP 작업 환경의 이름을 두 번 클릭합니다.
2. BlueXP 콘솔의 오른쪽 상단에서 타원 아이콘을 클릭하고 \* 암호 설정 \* 을 선택합니다.



새 암호는 마지막으로 사용한 6개의 암호 중 하나와 달라야 합니다.

## 시스템을 추가, 제거 또는 삭제합니다

기존 **Cloud Volumes ONTAP** 시스템을 **BlueXP**에 추가

기존 Cloud Volumes ONTAP 시스템을 검색하고 BlueXP에 추가할 수 있습니다. 새 BlueXP

시스템을 배포한 경우 이 작업을 수행할 수 있습니다.

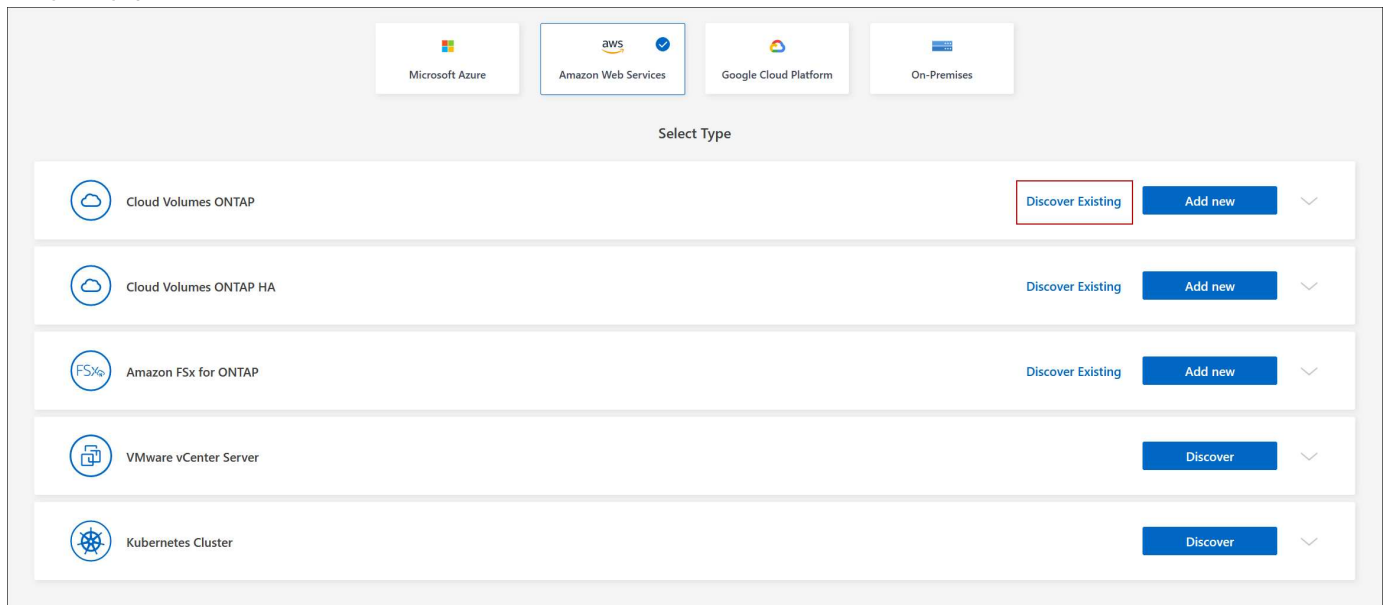
시작하기 전에

Cloud Volumes ONTAP admin 사용자 계정의 암호를 알아야 합니다.

단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 \* 작업 환경 추가 \* 를 클릭합니다.
3. 시스템이 상주하는 클라우드 공급자를 선택합니다.
4. Cloud Volumes ONTAP 시스템의 유형을 선택합니다.
5. 기존 시스템을 검색하려면 링크를 클릭하십시오.

를 누릅니다



1. 영역 페이지에서 인스턴스가 실행 중인 영역을 선택한 다음 인스턴스를 선택합니다.
2. 자격 증명 페이지에서 Cloud Volumes ONTAP 관리자 사용자의 암호를 입력한 다음 \* GO \* 를 클릭합니다.

결과

BlueXP는 Cloud Volumes ONTAP 인스턴스를 작업 영역에 추가합니다.

### Cloud Volumes ONTAP 작업 환경 제거

계정 관리자는 Cloud Volumes ONTAP 작업 환경을 제거하여 다른 시스템으로 이동하거나 검색 문제를 해결할 수 있습니다.

이 작업에 대해

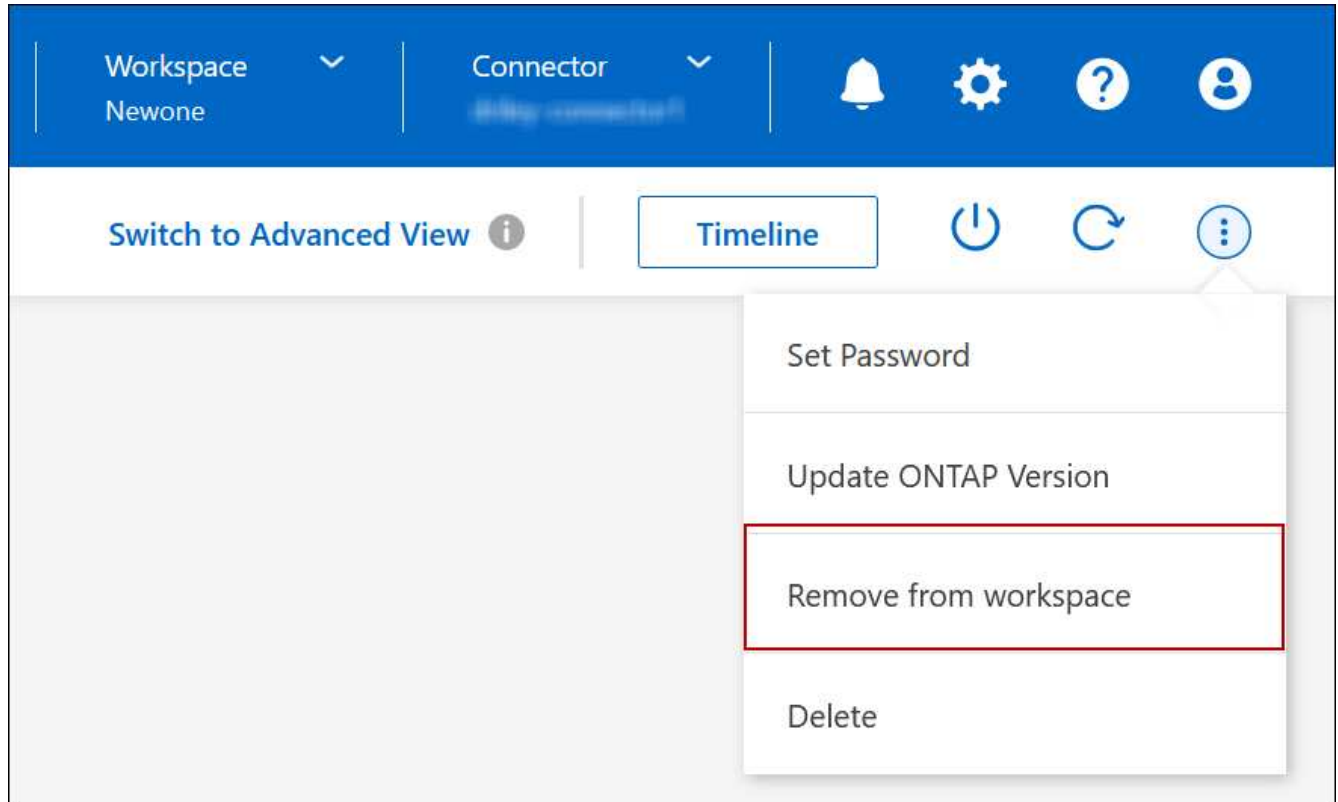
Cloud Volumes ONTAP 작업 환경을 제거하면 BlueXP에서 제거됩니다. Cloud Volumes ONTAP 시스템은 삭제되지 않습니다. 나중에 작업 환경을 다시 검색할 수 있습니다.

BlueXP에서 작업 환경을 제거하면 다음과 같은 작업을 수행할 수 있습니다.

- 다른 작업 공간에서 다시 검색합니다
- 다른 BlueXP 시스템에서 재검색합니다
- 초기 검색 중에 문제가 발생한 경우 다시 검색합니다

단계

1. Canvas 페이지에서 제거할 작업 환경을 두 번 클릭합니다.
2. BlueXP 콘솔의 오른쪽 상단에서 타원 아이콘을 클릭하고 \* 작업 영역에서 제거 \* 를 선택합니다.



3. 작업 공간에서 검토 창에서 \* 제거 \* 를 클릭합니다.

결과

BlueXP는 작업 환경을 제거합니다. 사용자는 언제든지 Canvas 페이지에서 이 작업 환경을 다시 검색할 수 있습니다.

### Cloud Volumes ONTAP 시스템 삭제

클라우드 공급자의 콘솔이 아닌 BlueXP에서 Cloud Volumes ONTAP 시스템을 항상 삭제해야 합니다. 예를 들어, 클라우드 공급자로부터 라이선스가 부여된 Cloud Volumes ONTAP 인스턴스를 종료하는 경우 다른 인스턴스에 대해 라이선스 키를 사용할 수 없습니다. 라이선스를 해제하려면 BlueXP에서 작업 환경을 삭제해야 합니다.

작업 환경을 삭제하면 BlueXP에서 Cloud Volumes ONTAP 인스턴스를 종료하고 디스크 및 스냅샷을 삭제합니다.

BlueXP 백업 및 복구, BlueXP 분류 인스턴스 등과 같은 다른 서비스에서 관리하는 리소스는 작업 환경을 삭제할 때 삭제되지 않습니다. 수동으로 삭제해야 합니다. 그렇지 않으면 이러한 리소스에 대한 비용을 계속 받게 됩니다.



BlueXP가 클라우드 공급업체에 Cloud Volumes ONTAP를 배포할 때 인스턴스에 대한 종료 보호를 활성화합니다. 이 옵션은 우발적인 종료를 방지하는 데 도움이 됩니다.

## 단계

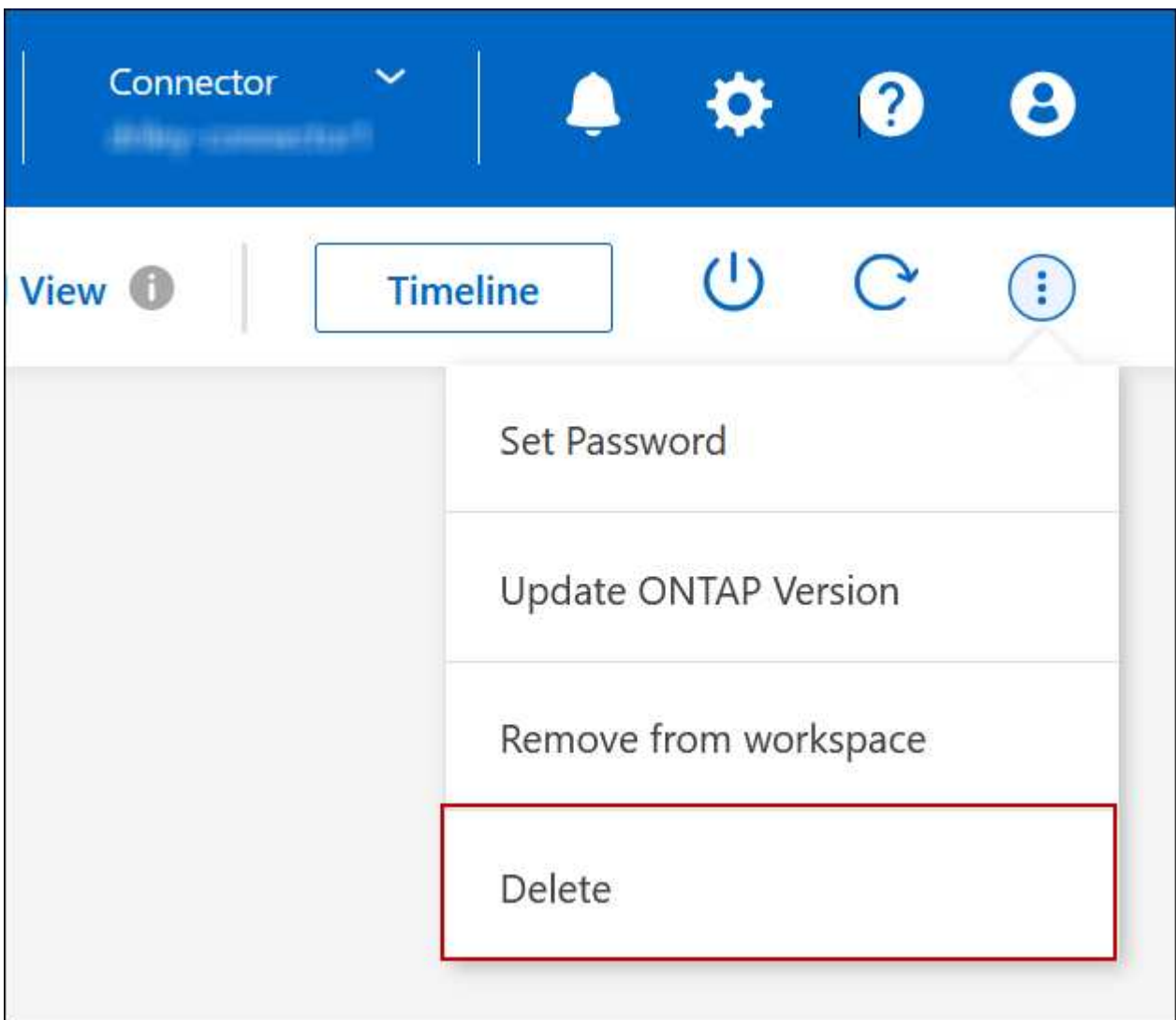
1. 작업 환경에서 BlueXP 백업 및 복구를 활성화한 경우 백업된 데이터가 여전히 필요한지 확인한 다음 **"필요한 경우 백업을 삭제합니다"**.

BlueXP 백업 및 복구는 설계상 Cloud Volumes ONTAP와 독립적입니다. Cloud Volumes ONTAP 시스템을 삭제할 때 BlueXP 백업 및 복구는 자동으로 백업을 삭제하지 않으며, 시스템이 삭제된 후 백업을 삭제할 수 있도록 UI에 현재 지원이 없습니다.

2. 이 작업 환경에서 BlueXP 분류를 사용하도록 설정했고 다른 작업 환경에서 이 서비스를 사용하지 않는 경우 서비스 인스턴스를 삭제해야 합니다.

**"BlueXP 분류 인스턴스에 대해 자세히 알아보십시오"**.

3. Cloud Volumes ONTAP 작업 환경을 삭제합니다.
  - a. Canvas 페이지에서 삭제할 Cloud Volumes ONTAP 작업 환경의 이름을 두 번 클릭합니다.
  - b. BlueXP 콘솔의 오른쪽 상단에서 타원 아이콘을 클릭하고 \* 삭제 \* 를 선택합니다.



c. 작업 환경 삭제 창에서 작업 환경의 이름을 입력한 다음 \* 삭제 \* 를 클릭합니다.

작업 환경을 삭제하는 데 최대 5분이 걸릴 수 있습니다.

## 설치하고

### Cloud Volumes ONTAP의 EC2 인스턴스 유형을 변경합니다

AWS에서 Cloud Volumes ONTAP를 시작할 때 여러 인스턴스 또는 유형 중에서 선택할 수 있습니다. 필요에 따라 크기가 작거나 크기 초과로 결정되면 언제든지 인스턴스 유형을 변경할 수 있습니다.

이 작업에 대해

- Cloud Volumes ONTAP HA 쌍(기본 설정)에서 자동 반환이 활성화되어 있어야 합니다. 그렇지 않으면 작업이 실패합니다.

"ONTAP 9 설명서: 자동 반환 구성을 위한 명령입니다"

- 인스턴스 유형을 변경하면 AWS 서비스 요금에 영향을 줄 수 있습니다.
- Cloud Volumes ONTAP가 다시 시작됩니다.

단일 노드 시스템의 경우 입출력이 중단됩니다.

HA 쌍의 경우 변경은 무중단 것입니다. HA 쌍이 계속해서 데이터를 제공합니다.











BlueXP는 테이크오버를 시작하고 Giveback을 기다리면서 한 번에 하나의 노드를 정상적으로 변경합니다. NetApp의 QA 팀은 이 프로세스 중에 파일 쓰기와 읽기를 모두 테스트했지만 클라이언트 측에서는 문제가 발생하지 않았습니다. 접속이 변경됨에 따라 입출력 레벨에서 재시도 횟수가 확인되었지만 애플리케이션 계층은 NFS/CIFS 연결의 이러한 짧은 "재연결"을 극복했습니다.

참조하십시오

AWS에서 지원되는 인스턴스 유형 목록은 를 참조하십시오 "[지원되는 EC2 인스턴스](#)".

단계

1. Canvas 페이지에서 작업 환경을 선택합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 \* 인스턴스 유형 \* 옆에 있는 연필 아이콘을 클릭합니다.

| Information              |                            | Features                                                                                     |
|--------------------------|----------------------------|----------------------------------------------------------------------------------------------|
| Working Environment Tags |                            | Tags      |
| Scheduled Downtime       |                            | Off       |
| S3 Storage Classes       | Standard-Infrequent Access |           |
| Instance Type            | m5.xlarge                  |           |
| Write Speed              |                            | Normal  |
| Ransomware Protection    |                            | Off     |
| Support Registration     | Not Registered             |         |
| CIFs Setup               |                            |         |

a. 노드 기반 PAYGO 라이선스를 사용하는 경우 \* 라이선스 유형 \* 옆에 있는 연필 아이콘을 클릭하여 다른 라이선스 및 인스턴스 유형을 선택할 수도 있습니다.

3. 인스턴스 유형을 선택하고 확인란을 선택하여 변경의 영향을 이해했는지 확인한 다음 \* 변경 \* 을 클릭합니다.

결과

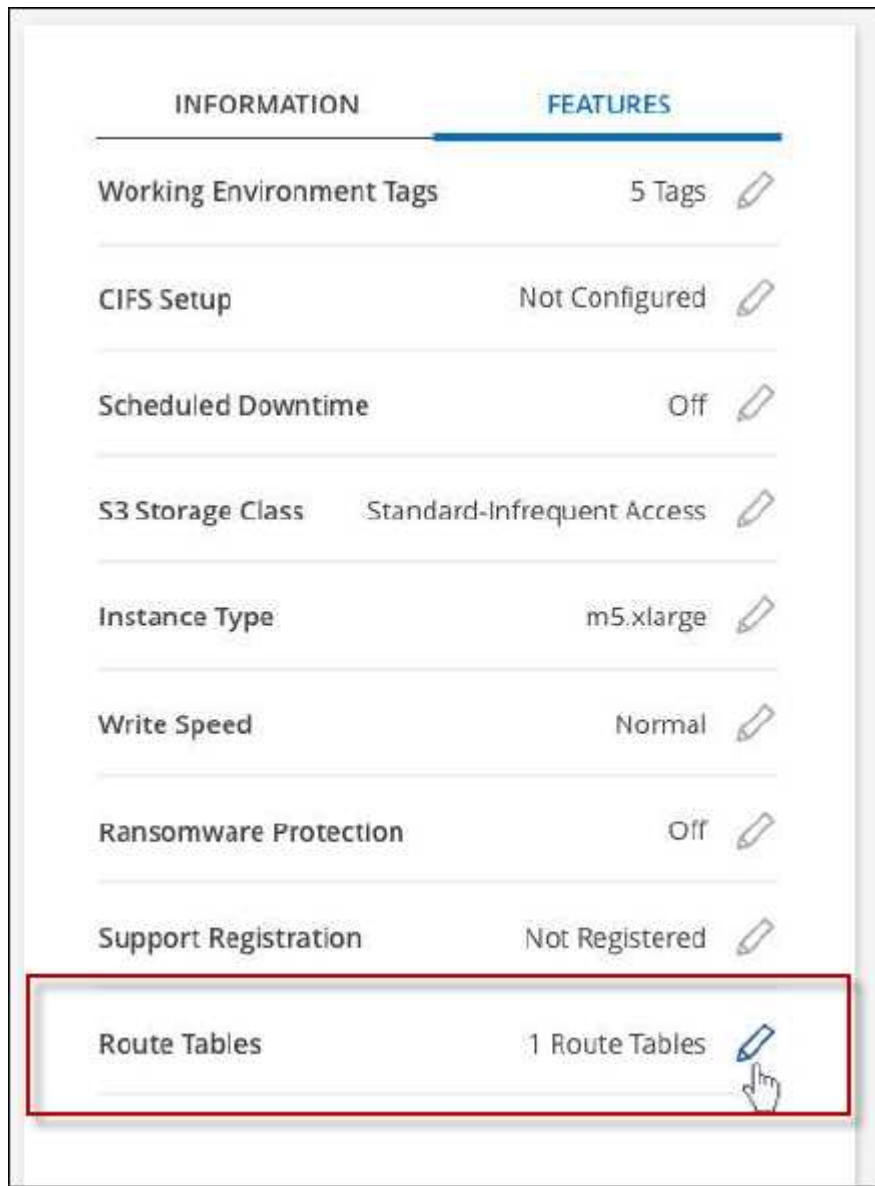
Cloud Volumes ONTAP가 새 구성으로 재부팅됩니다.

여러 AZs에서 HA 쌍의 경로 테이블을 변경합니다

여러 AZs(AWS Availability Zone)에 구축된 HA 쌍의 부동 IP 주소에 대한 라우트가 포함된 AWS 경로 테이블을 수정할 수 있습니다. 새로운 NFS 또는 CIFS 클라이언트가 AWS의 HA 쌍에 액세스해야 하는 경우 이 작업을 수행할 수 있습니다.

단계

1. Canvas 페이지에서 작업 환경을 선택합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 \* 경로 표 \* 옆에 있는 연필 아이콘을 클릭합니다.



3. 선택한 라우팅 테이블 목록을 수정하고 \* 저장 \* 을 클릭합니다.

결과

BlueXP는 AWS 요청을 전송하여 경로 테이블을 수정합니다.

## Azure 관리

### Cloud Volumes ONTAP의 Azure VM 유형을 변경합니다

Microsoft Azure에서 Cloud Volumes ONTAP를 시작할 때 여러 VM 유형 중에서 선택할 수 있습니다. 필요에 따라 크기가 작거나 특대형 것으로 판단될 경우 언제든지 VM 유형을 변경할 수 있습니다.

이 작업에 대해

- Cloud Volumes ONTAP HA 쌍(기본 설정)에서 자동 반환이 활성화되어 있어야 합니다. 그렇지 않으면 작업이 실패합니다.

"ONTAP 9 설명서: 자동 반환 구성을 위한 명령입니다"

- VM 유형을 변경하면 Microsoft Azure 서비스 요금에 영향을 줄 수 있습니다.
- Cloud Volumes ONTAP가 다시 시작됩니다.

단일 노드 시스템의 경우 입출력이 중단됩니다.

HA 쌍의 경우 변경은 무중단 것입니다. HA 쌍이 계속해서 데이터를 제공합니다.

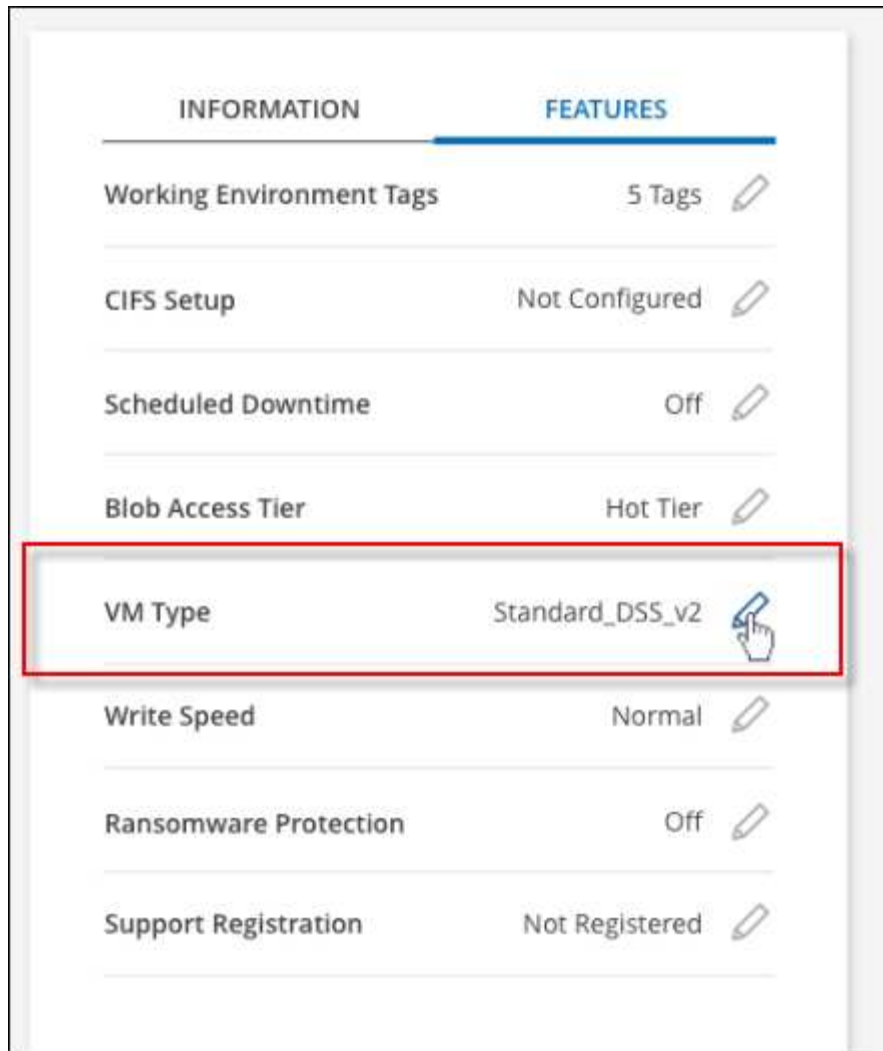


BlueXP는 테이크오버를 시작하고 Giveback을 기다리면서 한 번에 하나의 노드를 정상적으로 변경합니다. NetApp의 QA 팀은 이 프로세스 중에 파일 쓰기와 읽기를 모두 테스트했지만 클라이언트 측에서는 문제가 발생하지 않았습니다. 접속이 변경됨에 따라 입출력 레벨에서 재시도 횟수가 확인되었지만 애플리케이션 계층은 NFS/CIFS 연결의 이러한 짧은 "재연결"을 극복했습니다.

단계

1. Canvas 페이지에서 작업 환경을 선택합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 \* VM 유형 \* 옆에 있는 연필 아이콘을 클릭합니다.





a. 노드 기반 PAYGO 라이선스를 사용하는 경우 \* 라이선스 유형 \* 옆에 있는 연필 아이콘을 클릭하여 다른 라이선스 및 VM 유형을 선택할 수 있습니다.

3. VM 유형을 선택하고 확인란을 선택하여 변경의 영향을 이해했는지 확인한 다음 \* 변경 \* 을 클릭합니다.

결과

Cloud Volumes ONTAP가 새 구성으로 재부팅됩니다.

### Azure의 Cloud Volumes ONTAP HA 쌍에 대한 CIFS 잠금 재정의

계정 관리자는 BlueXP에서 Azure 유지 관리 이벤트 중에 Cloud Volumes ONTAP 스토리지 반환과 관련된 문제를 방지하는 설정을 활성화할 수 있습니다. 이 설정을 활성화하면 Cloud Volumes ONTAP가 CIFS 잠금을 확인하고 활성 CIFS 세션을 재설정합니다.

이 작업에 대해

Microsoft Azure는 가상 시스템에서 정기적인 유지 관리 이벤트를 예약합니다. Cloud Volumes ONTAP HA 쌍에서 유지보수 이벤트가 발생하면 HA 쌍이 스토리지 테이크오버 시작됩니다. 이 유지 관리 이벤트 중에 활성 CIFS 세션이 있는 경우 CIFS 파일의 잠금이 스토리지 반환을 방지할 수 있습니다.

이 설정을 활성화하면 Cloud Volumes ONTAP가 잠금을 거부하여 활성 CIFS 세션을 재설정합니다. 따라서 HA 쌍이 이러한 유지보수 이벤트 중에 스토리지 반환을 완료할 수 있습니다.



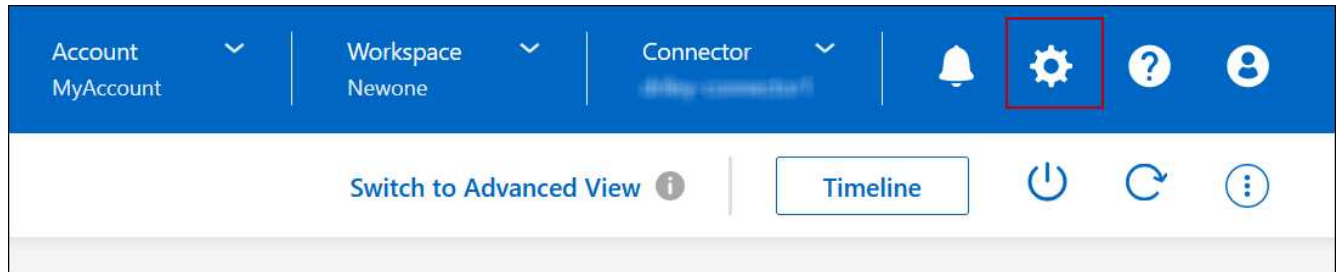
이 프로세스는 CIFS 클라이언트에 영향을 줄 수 있습니다. CIFS 클라이언트에서 커밋되지 않은 데이터는 손실될 수 있습니다.

#### 필요한 것

BlueXP 설정을 변경하려면 먼저 커넥터를 만들어야 합니다. "[자세히 알아보기](#)".

#### 단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 클릭하고 \* 커넥터 설정 \* 을 선택합니다.



2. Azure \* 에서 \* Azure HA 작업 환경에 대한 \* Azure CIFS 잠금을 클릭합니다.
3. 확인란을 클릭하여 기능을 활성화한 다음 \* 저장 \* 을 클릭합니다.

#### Azure Private Link 또는 서비스 끝점을 사용합니다

Cloud Volumes ONTAP는 Azure 프라이빗 링크를 사용하여 연결된 저장소 계정에 연결합니다. 필요한 경우 Azure Private Links를 비활성화하고 서비스 끝점을 대신 사용할 수 있습니다.

#### 개요

기본적으로 BlueXP는 Cloud Volumes ONTAP과 관련 저장소 계정 간의 연결을 위해 Azure 개인 링크를 활성화합니다. Azure Private Link는 Azure의 엔드포인트 간 연결을 보호하고 성능상의 이점을 제공합니다.

필요한 경우 Azure 프라이빗 링크 대신 서비스 끝점을 사용하도록 Cloud Volumes ONTAP를 구성할 수 있습니다.

BlueXP는 두 가지 구성 모두 Cloud Volumes ONTAP 및 스토리지 계정 간의 연결을 위해 항상 네트워크 액세스를 제한합니다. 네트워크 액세스는 Cloud Volumes ONTAP가 배포된 VNET와 커넥터가 배포된 VNET로 제한됩니다.

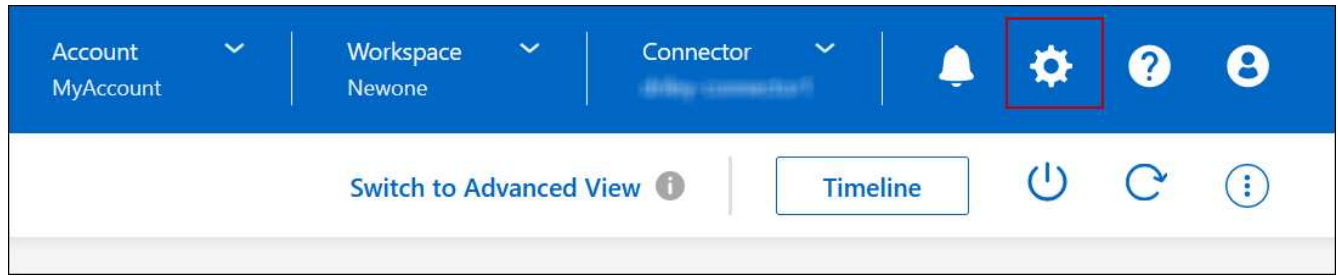
대신 **Azure** 전용 링크를 비활성화하고 서비스 끝점을 사용합니다

회사에서 요구하는 경우, BlueXP에서 Azure Private Link 대신 서비스 끝점을 사용하도록 Cloud Volumes ONTAP를 구성하도록 설정을 변경할 수 있습니다. 이 설정을 변경하면 새로 만든 Cloud Volumes ONTAP 시스템에 적용됩니다. 서비스 끝점은 에서만 지원됩니다 "[Azure 지역 쌍](#)" 커넥터와 Cloud Volumes ONTAP VNETs 사이.

커넥터는 해당 커넥터가 관리하는 Cloud Volumes ONTAP 시스템과 동일한 Azure 영역에 배포하거나 에 배포되어야 합니다 "[Azure 지역 쌍](#)" Cloud Volumes ONTAP 시스템의 경우

#### 단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 클릭하고 \* 커넥터 설정 \* 을 선택합니다.



2. Azure \* 에서 \* Azure Private Link \* 를 클릭합니다.
3. Cloud Volumes ONTAP 및 스토리지 계정 간 \* 프라이빗 링크 연결을 선택 취소합니다.
4. 저장 \* 을 클릭합니다.

작업을 마친 후

Azure Private Links를 사용하지 않도록 설정하고 Connector가 프록시 서버를 사용하는 경우 직접 API 트래픽을 활성화해야 합니다.

["Connector에서 직접 API 트래픽을 활성화하는 방법에 대해 알아봅니다"](#)

#### Azure 개인 링크 사용

대부분의 경우 Cloud Volumes ONTAP로 Azure Private 링크를 설정할 필요가 없습니다. BlueXP는 Azure 프라이빗 링크를 관리합니다. 그러나 기존 Azure Private DNS 영역을 사용하는 경우에는 구성 파일을 편집해야 합니다.

#### 사용자 지정 DNS 요구 사항

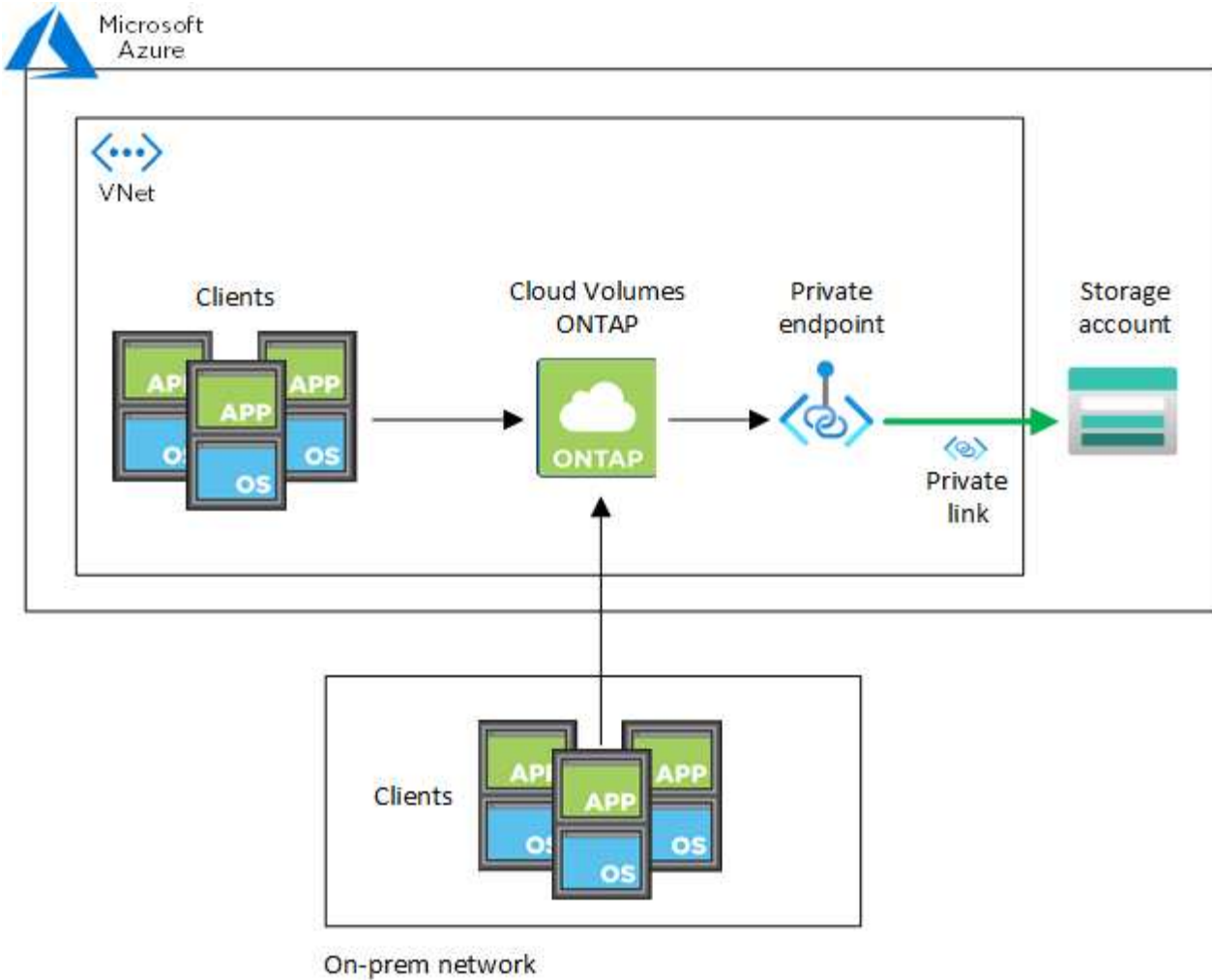
필요에 따라 사용자 지정 DNS로 작업하는 경우 사용자 지정 DNS 서버에서 Azure 개인 DNS 영역에 조건부 전달자를 만들어야 합니다. 자세한 내용은 [을 참조하십시오 "DNS 전달자 사용에 대한 Azure의 설명서"](#).

#### 개별 링크 연결의 작동 방식

BlueXP는 Azure에 Cloud Volumes ONTAP를 배포할 때 리소스 그룹에 개인 끝점을 만듭니다. 프라이빗 엔드포인트는 Cloud Volumes ONTAP의 스토리지 계정과 연결되어 있습니다. 따라서 Cloud Volumes ONTAP 스토리지에 대한 액세스는 Microsoft 백본 네트워크를 통해 이루어집니다.

클라이언트가 Cloud Volumes ONTAP와 동일한 VNET 내에 있거나, 피어링된 VNETs 내에 있거나, VNET에 대한 전용 VPN 또는 ExpressRoute 연결을 사용할 때 사내 네트워크에 있는 경우 클라이언트 액세스는 개인 링크를 통해 이루어집니다.

이 예에서는 동일한 VNET 내의 전용 링크와 전용 VPN 또는 ExpressRoute 연결이 있는 온프레미스 네트워크에서 클라이언트 액세스를 보여 줍니다.



커넥터 및 Cloud Volumes ONTAP 시스템이 다른 VNets에 구축된 경우 커넥터가 배포된 VNET와 Cloud Volumes ONTAP 시스템이 배포된 VNET 간에 VNET 피어링을 설정해야 합니다.

**Azure** 프라이빗 DNS에 대한 자세한 내용은 **BlueXP**를 참조하십시오

를 사용하는 경우 "**Azure 프라이빗 DNS**" 그런 다음 각 Connector에서 설정 파일을 수정해야 합니다. 그렇지 않으면 BlueXP에서 Cloud Volumes ONTAP 및 관련 저장소 계정 간에 Azure Private Link 연결을 활성화할 수 없습니다.

DNS 이름은 Azure DNS 명명 요구 사항과 일치해야 합니다 "**Azure 설명서에 나와 있는 대로 적용됩니다**".

단계

1. 커넥터 호스트에 SSH로 접속하고 로그인합니다.
2. /opt/application/netapp/cloudmanager/docker\_occm/data 디렉토리로 이동합니다
3. "user-private-dns-zone-settings" 매개 변수를 다음 키워드 값 쌍으로 추가하여 app.conf를 편집합니다.

```
"user-private-dns-zone-settings" : {
  "resource-group" : "<resource group name of the DNS zone>",
  "subscription" : "<subscription ID>",
  "use-existing" : true,
  "create-private-dns-zone-link" : true
}
```

아래와 같이 "system-id"와 동일한 수준으로 매개 변수를 입력해야 합니다.

```
"system-id" : "<system ID>",
"user-private-dns-zone-settings" : {
```

전용 DNS 영역이 Connector와 다른 구독에 있는 경우에만 subscription 키워드가 필요합니다.

#### 4. 파일을 저장하고 Connector를 로그오프합니다.

재부팅할 필요는 없습니다.

#### 장애 시 롤백 사용

BlueXP가 특정 작업의 일부로 Azure Private Link를 생성하지 못할 경우 Azure Private Link 연결이 없어도 작업이 완료됩니다. 이는 새 작업 환경(단일 노드 또는 HA 쌍)을 생성하거나 HA 쌍에서 다음 작업이 발생하는 경우, 즉 새 애그리게이트 생성, 기존 애그리게이트에 디스크 추가, 32TiB 이상으로 진행할 때 발생할 수 있습니다.

BlueXP에서 Azure Private Link를 생성하지 못할 경우 롤백을 활성화하여 이 기본 동작을 변경할 수 있습니다. 이를 통해 회사의 보안 규정을 완벽하게 준수할 수 있습니다.

롤백을 활성화하면 BlueXP는 작업을 중지하고 작업의 일부로 생성된 모든 리소스를 롤백합니다.

API를 통해 또는 app.conf 파일을 업데이트하여 롤백을 활성화할 수 있습니다.

- API를 통한 롤백 활성화 \*

#### 단계

1. 를 사용합니다 PUT /occm/config 다음 요청 본문이 있는 API 호출:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

- app.conf \* 를 업데이트하여 롤백 기능을 활성화합니다

#### 단계

1. 커넥터 호스트에 SSH로 접속하고 로그인합니다.
2. /opt/application/netapp/cloudmanager/docker\_occm/data 디렉토리로 이동합니다
3. 다음 매개 변수와 값을 추가하여 app.conf를 편집합니다.

```
"rollback-on-private-link-failure": true
```

. 파일을 저장하고 Connector를 로그오프합니다.

재부팅할 필요는 없습니다.

리소스 그룹 이동 중

Cloud Volumes ONTAP는 Azure 리소스 그룹 이동을 지원하지만 워크플로는 Azure 콘솔에서만 실행됩니다.

동일한 Azure 가입 내에서 하나의 리소스 그룹에서 Azure의 다른 리소스 그룹으로 작업 환경을 이동할 수 있습니다. 서로 다른 Azure 구독 간에 리소스 그룹을 이동하는 것은 지원되지 않습니다.

단계

1. Canvas \* 에서 작업 환경을 제거합니다.

작업 환경을 제거하는 방법에 대한 자세한 내용은 을 참조하십시오 "[Cloud Volumes ONTAP 작업 환경 제거](#)".

2. Azure 콘솔에서 리소스 그룹 이동을 실행합니다.

이동을 완료하려면 을 참조하십시오 "[리소스를 새 리소스 그룹 또는 Microsoft Azure 설명서에 있는 구독으로 이동합니다](#)".

3. Canvas \* 에서 작업 환경을 검색합니다.
4. 작업 환경에 대한 정보에서 새 리소스 그룹을 찾습니다.

결과

작업 환경 및 해당 리소스(VM, 디스크, 스토리지 계정, 네트워크 인터페이스, 스냅샷)가 새 리소스 그룹에 있습니다.

## Google Cloud 관리

Cloud Volumes ONTAP의 Google Cloud 컴퓨터 유형을 변경합니다

Google Cloud에서 Cloud Volumes ONTAP를 시작할 때 여러 컴퓨터 유형 중에서 선택할 수 있습니다. 필요에 따라 크기가 작거나 너무 큰 것으로 판단될 경우 언제든지 인스턴스 또는 컴퓨터 유형을 변경할 수 있습니다.

이 작업에 대해

- Cloud Volumes ONTAP HA 쌍(기본 설정)에서 자동 반환이 활성화되어 있어야 합니다. 그렇지 않으면 작업이 실패합니다.

["ONTAP 9 설명서: 자동 반환 구성을 위한 명령입니다"](#)

- 컴퓨터 유형을 변경하면 Google Cloud 서비스 요금에 영향을 줄 수 있습니다.
- Cloud Volumes ONTAP가 다시 시작됩니다.

단일 노드 시스템의 경우 입출력이 중단됩니다.

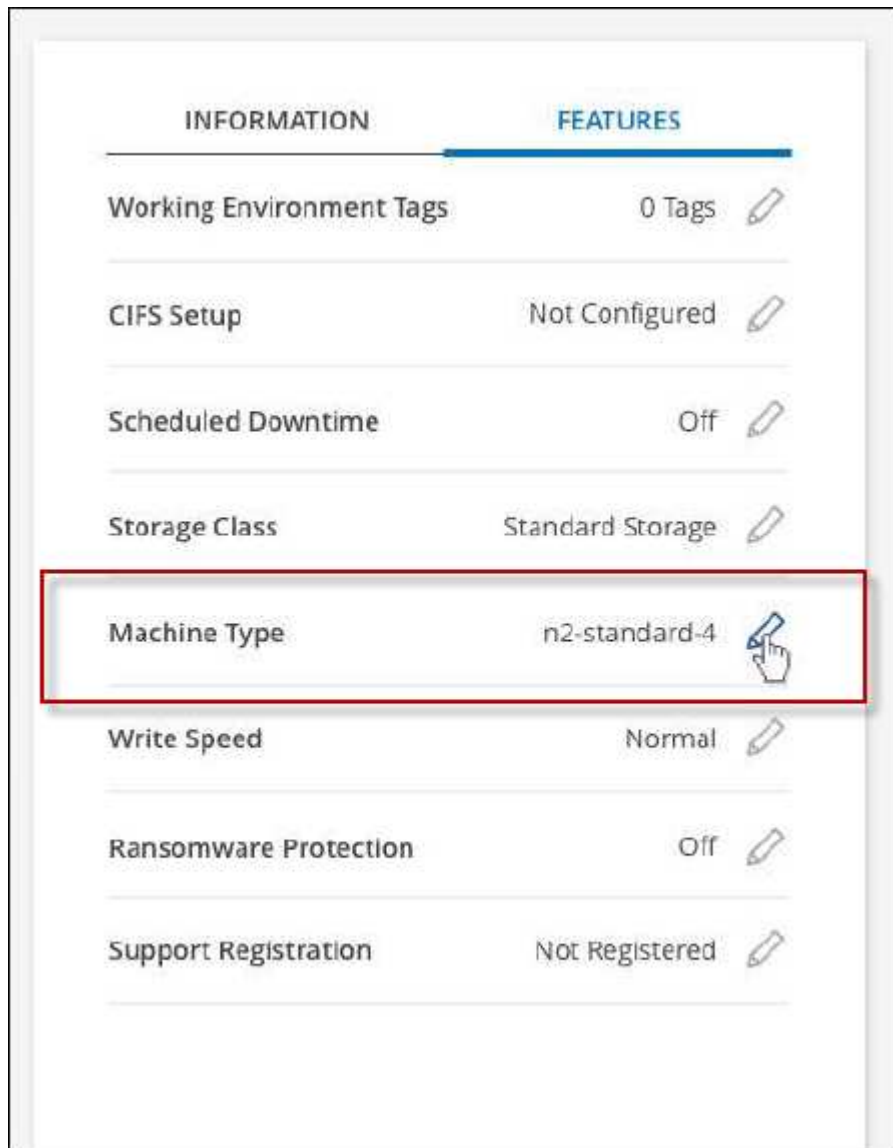
HA 쌍의 경우 변경은 무중단 것입니다. HA 쌍이 계속해서 데이터를 제공합니다.



BlueXP는 테이크오버를 시작하고 Giveback을 기다리면서 한 번에 하나의 노드를 정상적으로 변경합니다. NetApp의 QA 팀은 이 프로세스 중에 파일 쓰기와 읽기를 모두 테스트했지만 클라이언트 측에서는 문제가 발생하지 않았습니다. 접속이 변경됨에 따라 입출력 레벨에서 재시도 횟수가 확인되었지만 애플리케이션 계층은 NFS/CIFS 연결의 이러한 짧은 "재연결"을 극복했습니다.

단계

1. Canvas 페이지에서 작업 환경을 선택합니다.
2. 개요 탭에서 기능 패널을 클릭한 다음 \* 기계 유형 \* 옆에 있는 연필 아이콘을 클릭합니다.



- a. 노드 기반 PAYGO 라이선스를 사용하는 경우 \* 라이선스 유형 \* 옆에 있는 연필 아이콘을 클릭하여 다른 라이선스 및 컴퓨터 유형을 선택할 수 있습니다.
3. 시스템 유형을 선택하고 확인란을 선택하여 변경의 영향을 이해했는지 확인한 다음 \* 변경 \* 을 클릭합니다.

결과

Cloud Volumes ONTAP가 새 구성으로 재부팅됩니다.

## 고급 보기를 사용하여 **Cloud Volumes ONTAP**를 관리합니다

Cloud Volumes ONTAP의 고급 관리를 수행해야 하는 경우, ONTAP 시스템과 함께 제공되는 관리 인터페이스인 ONTAP System Manager를 사용하면 됩니다. BlueXP에 System Manager 인터페이스를 직접 포함하므로 고급 관리를 위해 BlueXP를 떠날 필요가 없습니다.

이 고급 보기는 미리 보기로 사용할 수 있습니다. NetApp은 이 경험을 개선하고 다음 릴리즈에서 향상된 기능을 추가할 계획입니다. 제품 내 채팅을 사용하여 피드백을 보내주십시오.

### 피처

BlueXP의 고급 보기를 통해 다음과 같은 추가 관리 기능을 사용할 수 있습니다.

- 고급 스토리지 관리  
일관성 그룹, 공유, Qtree, 할당량 및 스토리지 VM을 관리합니다.
- 네트워킹 관리  
IPspace, 네트워크 인터페이스, 포트 세트 및 이더넷 포트 관리
- 이벤트 및 작업  
이벤트 로그, 시스템 경고, 작업 및 감사 로그를 봅니다.
- 고급 데이터 보호  
스토리지 VM, LUN 및 일관성 그룹을 보호합니다.
- 호스트 관리  
SAN 이니시에이터 그룹 및 NFS 클라이언트를 설정합니다.

### 지원되는 구성

System Manager를 통한 고급 관리는 표준 클라우드 지역에서 Cloud Volumes ONTAP 9.10.0 이상에서 지원됩니다.

GovCloud 지역 또는 아웃바운드 인터넷 액세스가 없는 지역에서는 System Manager 통합이 지원되지 않습니다.

### 제한 사항

Cloud Volumes ONTAP에서는 System Manager 인터페이스에 표시되는 몇 가지 기능을 지원하지 않습니다.

- BlueXP 계층화  
Cloud Volumes ONTAP에서는 BlueXP 계층화 서비스가 지원되지 않습니다. 볼륨 생성 시 BlueXP의 표준 보기에서 데이터를 오브젝트 스토리지로 계층화하도록 직접 설정해야 합니다.
- 계층



System Manager에서는 애그리게이트 관리(로컬 계층 및 클라우드 계층 포함)가 지원되지 않습니다. BlueXP의 표준 보기에서 직접 애그리게이트를 관리해야 합니다.

- 펌웨어 업그레이드

Cloud Volumes ONTAP에서는 \* 클러스터 > 설정 \* 페이지의 자동 펌웨어 업데이트가 지원되지 않습니다.

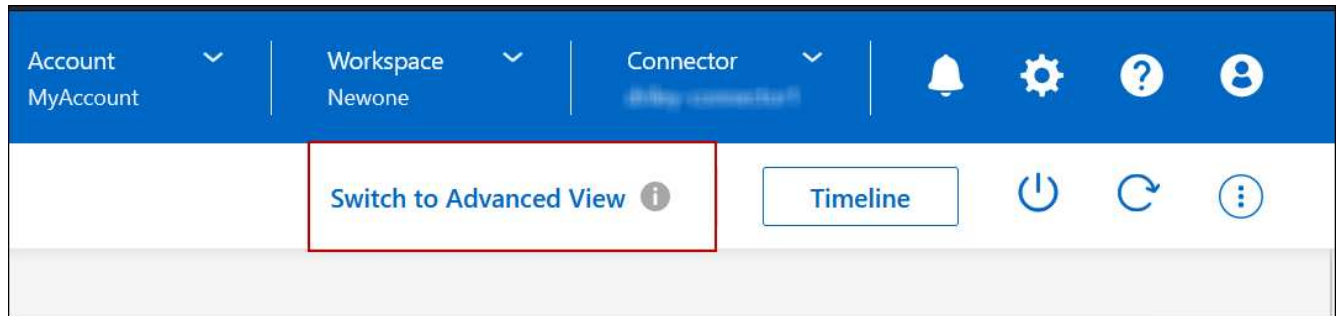
또한 System Manager의 역할 기반 액세스 제어가 지원되지 않습니다.

### 시작하는 방법

Cloud Volumes ONTAP 작업 환경을 열고 고급 보기 옵션을 클릭합니다.

### 단계

1. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
2. Canvas 페이지에서 Cloud Volumes ONTAP 시스템의 이름을 두 번 클릭합니다.
3. 오른쪽 상단에서 \* 고급 보기로 전환 \* 을 클릭합니다.



4. 확인 메시지가 나타나면 메시지를 읽고 \* 닫기 \* 를 클릭합니다.
5. 시스템 관리자를 사용하여 Cloud Volumes ONTAP를 관리합니다.
6. 필요한 경우 \* 표준 보기로 전환 \* 을 클릭하여 BlueXP를 통한 표준 관리로 돌아갑니다.

### System Manager 사용에 대한 도움말

Cloud Volumes ONTAP에서 System Manager를 사용하는 데 도움이 필요한 경우 을 참조하십시오 ["ONTAP 설명서"](#) 을 참조하십시오. 다음은 도움이 될 수 있는 몇 가지 링크입니다.

- ["볼륨 및 LUN 관리"](#)
- ["네트워크 관리"](#)
- ["데이터 보호"](#)

### CLI에서 Cloud Volumes ONTAP를 관리합니다

Cloud Volumes ONTAP CLI를 사용하면 모든 관리 명령을 실행할 수 있으며 고급 작업에 이상적이고 CLI를 사용하는 것이 더 편할 경우 적합합니다. SSH(Secure Shell)를 사용하여 CLI에 연결할 수 있습니다.

## 시작하기 전에

Cloud Volumes ONTAP에 연결하기 위해 SSH를 사용하는 호스트에는 Cloud Volumes ONTAP에 대한 네트워크 연결이 있어야 합니다. 예를 들어, 클라우드 공급자 네트워크에 있는 점프 호스트에서 SSH를 사용해야 할 수 있습니다.



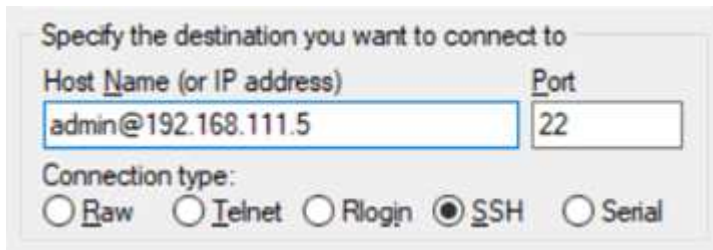
여러 AZs에 구축된 Cloud Volumes ONTAP HA 구성에서는 클러스터 관리 인터페이스에 부동 IP 주소를 사용합니다. 즉, 외부 라우팅을 사용할 수 없습니다. 동일한 라우팅 도메인의 일부인 호스트에서 접속해야 합니다.

## 단계

1. BlueXP에서 클러스터 관리 인터페이스의 IP 주소를 확인합니다.
  - a. 왼쪽 탐색 메뉴에서 \* Storage > Canvas \* 를 선택합니다.
  - b. Canvas 페이지에서 Cloud Volumes ONTAP 시스템을 선택합니다.
  - c. 오른쪽 창에 표시되는 클러스터 관리 IP 주소를 복사합니다.
2. SSH를 사용하여 admin 계정을 사용하여 클러스터 관리 인터페이스 IP 주소에 연결합니다.

◦ 예 \*

다음 이미지는 PuTTY를 사용하는 예를 보여 줍니다.



3. 로그인 프롬프트에서 admin 계정의 암호를 입력합니다.

◦ 예 \*

```
Password: *****  
COT2::>
```

## 시스템 상태 및 이벤트입니다

### AutoSupport 설정을 확인합니다

AutoSupport은 능동적으로 시스템 상태를 모니터링하고 NetApp 기술 지원 팀에 메시지를 보냅니다. 기본적으로 AutoSupport은 각 노드에서 HTTPS 전송 프로토콜을 사용하여 기술 지원 부서에 메시지를 보내도록 설정됩니다. AutoSupport에서 이러한 메시지를 보낼 수 있는지 확인하는 것이 가장 좋습니다.

필요한 유일한 구성 단계는 Cloud Volumes ONTAP가 아웃바운드 인터넷 연결을 사용할 수 있도록 하는 것입니다. 자세한 내용은 해당 클라우드 공급자의 네트워킹 요구 사항을 참조하십시오.

## AutoSupport 요구 사항

Cloud Volumes ONTAP 노드를 사용하려면 NetApp AutoSupport에 대한 아웃바운드 인터넷 액세스가 필요합니다. 사전 예방적으로 시스템의 상태를 모니터링하고 메시지를 NetApp 기술 지원으로 보냅니다.

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>
- <https://support.netapp.com/asupprod/post/1.0/postAsup>

AutoSupport 메시지를 보내는 데 아웃바운드 인터넷 연결을 사용할 수 없는 경우 BlueXP는 자동으로 Cloud Volumes ONTAP 시스템에서 커넥터를 프록시 서버로 사용하도록 구성합니다. 유일한 요구 사항은 커넥터의 보안 그룹이 포트 3128을 통한 `_IN`인바운드\_연결을 허용하는지 확인하는 것입니다. Connector를 배포한 후 이 포트를 열어야 합니다.

Cloud Volumes ONTAP에 대해 엄격한 아웃바운드 규칙을 정의한 경우 Cloud Volumes ONTAP 보안 그룹이 포트 3128을 통한 `_outbound_connection`을 허용하는지 확인해야 합니다.

아웃바운드 인터넷 액세스가 가능한지 확인한 후 AutoSupport를 테스트하여 메시지를 보낼 수 있는지 확인할 수 있습니다. 자세한 지침은 을 참조하십시오 ["ONTAP 문서: AutoSupport 설정"](#).

## AutoSupport 구성 문제를 해결합니다

아웃바운드 연결을 사용할 수 없고 BlueXP에서 커넥터를 프록시 서버로 사용하도록 Cloud Volumes ONTAP 시스템을 구성할 수 없는 경우 "<작업 환경 이름>이(가) AutoSupport 메시지를 보낼 수 없습니다."라는 제목의 BlueXP에서 알림을 받게 됩니다.

네트워킹 문제로 인해 이 메시지가 표시될 가능성이 높습니다.

이 문제를 해결하려면 다음 단계를 수행하십시오.

단계

1. Cloud Volumes ONTAP 시스템에 SSH를 사용하여 CLI에서 시스템을 관리할 수 있습니다.

["Cloud Volumes ONTAP에 SSH를 사용하는 방법에 대해 알아보십시오"](#).

2. AutoSupport 하위 시스템의 세부 상태를 표시합니다.

```
autosupport check show-details
```

응답은 다음과 비슷해야 합니다.

```

Category: smtp
  Component: mail-server
  Status: failed
  Detail: SMTP connectivity check failed for destination:
         mailhost. Error: Could not resolve host -
'mailhost'
  Corrective Action: Check the hostname of the SMTP server

Category: http-https
  Component: http-put-destination
  Status: ok
  Detail: Successfully connected to:
         <https://support.netapp.com/put/AsupPut/>.

  Component: http-post-destination
  Status: ok
  Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

Category: on-demand
  Component: ondemand-server
  Status: ok
  Detail: Successfully connected to:
         https://support.netapp.com/aods/asupmessage.

Category: configuration
  Component: configuration
  Status: ok
  Detail: No configuration issues found.
5 entries were displayed.

```

http-https 범주의 상태가 "ok"이면 AutoSupport가 올바르게 구성되어 메시지를 보낼 수 있음을 의미합니다.

3. 상태가 정상이 아닌 경우 각 Cloud Volumes ONTAP 노드의 프록시 URL을 확인합니다.

```
autosupport show -fields proxy-url
```

4. 프록시 URL 매개 변수가 비어 있는 경우 Cloud Volumes ONTAP에서 커넥터를 프록시로 사용하도록 구성합니다.

```
autosupport modify -proxy-url http://<connector private ip>:3128
```

5. AutoSupport 상태 다시 확인:

```
autosupport check show-details
```

6. 상태가 여전히 FAILED인 경우 Cloud Volumes ONTAP와 포트 3128을 통한 커넥터 사이에 연결이 있는지

확인합니다.

7. 연결이 있는지 확인한 후에도 상태 ID가 계속 실패하면 커넥터에 SSH를 연결합니다.

"Connector용 Linux VM에 연결하는 방법에 대해 자세히 알아보십시오"

8. 로 이동합니다 /opt/application/netapp/cloudmanager/docker\_occm/data/
9. 프록시 구성 파일을 엽니다 squid.conf

파일의 기본 구조는 다음과 같습니다.

```
http_port 3128
acl localnet src 172.31.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

localnet src 값은 Cloud Volumes ONTAP 시스템의 CIDR입니다.

10. Cloud Volumes ONTAP 시스템의 CIDR 블록이 파일에 지정된 범위에 있지 않으면 다음과 같이 값을 업데이트하거나 새 항목을 추가합니다.

```
acl cvonet src <cidr>
```

이 새 항목을 추가하는 경우 허용 항목도 추가해야 합니다.

```
http_access allow cvonet
```

예를 들면 다음과 같습니다.

```
http_port 3128
acl localnet src 172.31.0.0/16
acl cvonet src 172.33.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access allow cvonet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

11. 구성 파일을 편집한 후 프록시 컨테이너를 sudo로 다시 시작합니다.

```
docker restart squid
```

12. Cloud Volumes ONTAP CLI로 돌아가서 Cloud Volumes ONTAP가 AutoSupport 메시지를 보낼 수 있는지 확인합니다.

```
autosupport check show-details
```

## EMS를 설정한다

EMS(이벤트 관리 시스템)는 ONTAP 시스템에서 발생하는 이벤트에 대한 정보를 수집하여 표시합니다. 이벤트 알림을 수신하려면 이벤트 대상(이메일 주소, SNMP 트랩 호스트 또는 syslog 서버)과 이벤트 경로를 특정 이벤트 심각도에 대해 설정할 수 있습니다.

CLI를 이용하여 EMS를 구성할 수 있다. 자세한 지침은 을 참조하십시오 "[ONTAP 문서: EMS 구성 개요](#)".

# 개념

## Cloud Volumes ONTAP 라이선스

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

### 라이선스 개요

신규 고객은 다음과 같은 라이선스 옵션을 사용할 수 있습니다.

#### 용량 기반 라이선스

프로비저닝된 용량을 기준으로 NetApp 계정의 여러 Cloud Volumes ONTAP 시스템에 대한 비용 지불 애드온 클라우드 데이터 서비스를 구매할 수 있는 기능이 포함되어 있습니다.

#### Keystone 구독

HA 쌍에 대한 원활한 하이브리드 클라우드 경험을 제공하는 용량제 구독 기반 서비스입니다.

이전 by-node 라이선스 모델은 이미 라이선스를 구입했거나 현재 마켓플레이스 서브스크립션을 보유하고 있는 기존 고객에게도 계속 사용할 수 있습니다.

다음 섹션에서는 이러한 각 옵션에 대해 자세히 설명합니다.



라이선스가 없는 경우 라이선스가 부여된 기능을 사용할 수 없습니다.

### 용량 기반 라이선스

용량 기반 라이선스 패키지를 사용하여 Cloud Volumes ONTAP/TiB 용량 단위로 비용을 지불할 수 있습니다. 라이선스는 NetApp 계정에 연결되며, 라이선스를 통해 사용할 수 있는 용량이 충분한 경우 라이선스에 대해 여러 시스템을 청구할 수 있습니다.

예를 들어, 20TiB 라이선스 1개를 구입하고 Cloud Volumes ONTAP 시스템 4개를 배포한 다음 각 시스템에 5TiB 볼륨을 할당하여 총 20TiB를 할당할 수 있습니다. 용량은 해당 계정에 구축된 각 Cloud Volumes ONTAP 시스템의 볼륨에 사용할 수 있습니다.

용량 기반 라이선스는 *package* 형식으로 제공됩니다. Cloud Volumes ONTAP 시스템을 구축할 때 비즈니스 요구 사항에 따라 여러 라이선스 패키지 중에서 선택할 수 있습니다.

#### 패키지

Cloud Volumes ONTAP에 사용할 수 있는 용량 기반 패키지는 다음과 같습니다.

#### 프리모늄

NetApp에서 무료로 모든 Cloud Volumes ONTAP 기능을 제공합니다(클라우드 공급자 요금은 여전히 적용됨).

- 라이선스 또는 계약이 필요하지 않습니다.
- NetApp의 지원은 포함되지 않습니다.

- Cloud Volumes ONTAP 시스템당 프로비저닝된 용량 500GiB로 제한됩니다.
- 모든 클라우드 공급자가 NetApp 계정 하나당 Freemium 제품을 사용하면 최대 10대의 Cloud Volumes ONTAP 시스템을 사용할 수 있습니다.
- Cloud Volumes ONTAP 시스템에 대해 프로비저닝된 용량이 500GiB를 초과하면 BlueXP는 시스템을 Essentials 패키지로 변환합니다.

시스템이 Essentials 패키지로 변환되는 즉시, 가 표시됩니다 **최소 충전** 적용됩니다.

프로비저닝된 용량이 500GiB 미만인 다른 모든 시스템은 Freemium에 그대로 유지됩니다(Freemium 제품을 사용하여 구축한 경우).

#### 최적화

프로비저닝된 용량 및 I/O 작업에 대해 별도로 비용을 지불합니다.

- Cloud Volumes ONTAP 단일 노드 또는 HA
- 충전은 스토리지와 용도(I/O)의 두 가지 비용 구성 요소를 기반으로 합니다.

데이터 복제(SnapMirror) 또는 NDMP와 관련된 입출력에는 비용이 청구되지 않습니다.

- Azure Marketplace에서 용량제 오퍼링을 제공하거나 연간 계약으로 사용할 수 있습니다
- Google Cloud Marketplace에서 선불 종량제 또는 연간 계약으로 제공됩니다
- 선택한 VM 유형에서 지원됨:
  - Azure의 경우: E4s\_v3, E4ds\_v4, DS4\_v2, DS13\_v2, E8s\_v3, 및 E8ds\_v4를 참조하십시오
  - Google Cloud의 경우: n2-standard-4, n2-standard-8
- NetApp의 클라우드 데이터 서비스를 추가 비용으로 이용할 수 있습니다

#### 필수 요소

다양한 구성의 Cloud Volumes ONTAP에 대한 용량 기준 지불

- Cloud Volumes ONTAP 구성 선택:
  - 단일 노드 또는 HA 시스템
  - DR(재해 복구)을 위한 파일 및 블록 스토리지 또는 보조 데이터
- NetApp의 클라우드 데이터 서비스를 추가 비용으로 이용할 수 있습니다

#### 전문가입니다

무제한 백업을 통해 모든 유형의 Cloud Volumes ONTAP 구성에 대한 용량별 지불.

- 모든 Cloud Volumes ONTAP 구성에 대한 라이선스를 제공합니다
- 동일한 속도로 운영 및 2차 볼륨의 용량을 충전하는 단일 노드 또는 HA
- BlueXP 백업 및 복구를 사용한 볼륨 백업 무제한 포함, 프로페셔널 패키지를 사용하는 Cloud Volumes ONTAP 시스템에만 해당



- NetApp의 클라우드 데이터 서비스를 추가 비용으로 이용할 수 있습니다

#### 에지 캐시

Cloud Volumes Edge Cache에 대한 라이선스를 제공합니다.

- 분산 엔터프라이즈를 위한 비즈니스 연속성 및 데이터 보호 기능을 제공하는 Professional 패키지와 동일한 기능입니다
- 각 위치에서 설치 공간이 작은 Windows VM을 통한 지능형 에지 캐싱
- 구매한 용량이 3Tib마다 엣지 노드 1개
- Azure Marketplace에서 용량제 오퍼링을 제공하거나 연간 계약으로 사용할 수 있습니다
- Google Cloud Marketplace에서 선불 종량제 또는 연간 계약으로 제공됩니다

["Cloud Volumes Edge Cache를 통해 비즈니스를 지원하는 방법에 대해 자세히 알아보십시오"](#)

#### 소비 모델

용량 기반 라이선스 패키지는 다음 소비 모델에서 사용할 수 있습니다.

- \* BYOL \*: NetApp에서 구입한 라이선스로 클라우드 공급자에 상관없이 Cloud Volumes ONTAP를 구축할 수 있습니다.

#### 를 누릅니다

Optimized 및 Edge Cache 패키지는 BYOL에서 사용할 수 없습니다.

- \* PAYGO \*: 클라우드 공급자 마켓플레이스의 시간별 구독입니다.
- \* 연간 \*: 클라우드 공급자 마켓플레이스로부터 연간 계약을 체결합니다.

다음 사항에 유의하십시오.

- NetApp(BYOL)에서 라이선스를 구입하는 경우 클라우드 공급자 마켓플레이스의 PAYGO 오퍼링을 구독해야 합니다.

라이선스는 항상 먼저 부과되지만 다음과 같은 경우 마켓플레이스의 시간당 유희로 비용이 청구됩니다.

- 라이선스 용량을 초과하는 경우
- 라이선스 기간이 만료된 경우
- 마켓플레이스로부터 연간 계약을 체결한 경우 \_All\_Cloud Volumes ONTAP 시스템에 해당 계약이 적용됩니다. BYOL은 연간 마켓플레이스 계약을 혼합하여 사용할 수 없습니다.
- 중국 지역에서는 BYOL을 사용하는 단일 노드 시스템만 지원됩니다.

#### 패키지를 변경하는 중입니다

배포 후에는 용량 기반 라이선스를 사용하는 Cloud Volumes ONTAP 시스템의 패키지를 변경할 수 있습니다. 예를 들어, Essentials 패키지와 함께 Cloud Volumes ONTAP 시스템을 배포한 경우 비즈니스 요구사항이 변경되면 이를 Professional 패키지로 변경할 수 있습니다.

["충전 방법을 변경하는 방법에 대해 알아보십시오"](#).

## 가격

가격에 대한 자세한 내용은 [클릭](#) 참조하십시오 "NetApp BlueXP 웹 사이트".

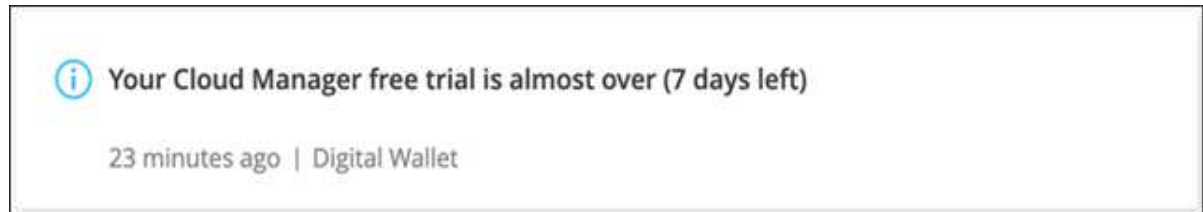
## 무료 평가판

클라우드 공급자 마켓플레이스의 용량제 구독을 통해 30일 무료 평가판을 사용할 수 있습니다. 무료 평가판에는 Cloud Volumes ONTAP 및 BlueXP 백업 및 복구가 포함됩니다. 이 평가판은 사용자가 마켓플레이스의 서비스에 가입할 때 시작됩니다.

인스턴스 또는 용량 제한은 없습니다. 원하는 만큼 Cloud Volumes ONTAP 시스템을 구축하고 30일 동안 무료로 필요한 용량을 할당할 수 있습니다. 무료 평가판은 30일 후에 자동으로 유료 시간별 구독으로 변환됩니다.

Cloud Volumes ONTAP에는 시간당 소프트웨어 라이선스 비용이 부과되지 않지만, 클라우드 공급자의 인프라 비용이 여전히 적용됩니다.

무료 평가판이 시작될 때, 7일 남았을 때, 1일 남았을 때 BlueXP에서 알림을 받게 됩니다. 예를 들면 다음과 같습니다.



## 지원되는 구성

용량 기반 라이선스 패키지는 Cloud Volumes ONTAP 9.7 이상에서 사용할 수 있습니다.

## 용량 제한

이 라이선스 모델을 통해 각 개별 Cloud Volumes ONTAP 시스템은 디스크를 통해 최대 2개의 PiB 용량을 지원하고 오브젝트 스토리지로 계층화합니다.

라이선스 자체에는 최대 용량 제한이 없습니다.

## 최대 시스템 수

용량 기반 라이선스는 Cloud Volumes ONTAP 시스템의 최대 수를 NetApp 계정당 20개로 제한합니다. system\_은 Cloud Volumes ONTAP HA 쌍, Cloud Volumes ONTAP 단일 노드 시스템 또는 사용자가 생성하는 추가 스토리지 VM입니다. 기본 스토리지 VM은 제한에 대해 계산되지 않습니다. 이 제한은 모든 라이선스 모델에 적용됩니다.

예를 들어, 다음과 같은 세 가지 작업 환경이 있다고 가정해 보겠습니다.

- 스토리지 VM이 1개인 단일 노드 Cloud Volumes ONTAP 시스템(Cloud Volumes ONTAP 구축 시 생성되는 기본 스토리지 VM)

이 작업 환경은 하나의 시스템으로 간주됩니다.

- 스토리지 VM 2개(기본 스토리지 VM과 생성한 추가 스토리지 VM 1개)가 있는 단일 노드 Cloud Volumes ONTAP 시스템

이 작업 환경은 두 시스템으로 계산됩니다. 하나는 단일 노드 시스템이고 다른 하나는 추가 스토리지 VM입니다.

- Cloud Volumes ONTAP HA 2노드: 스토리지 VM 3개(기본 스토리지 VM + 직접 생성한 추가 스토리지 VM 2개)

이 작업 환경은 HA Pair용, 그리고 추가 스토리지 VM용 시스템의 세 가지로 계산됩니다.

시스템에 대한 총 6개의 시스템이 있습니다. 그러면 계정에 14개의 추가 시스템을 추가할 수 있는 공간이 있습니다.

20대 이상의 시스템이 필요한 대규모 구축 환경의 경우 고객 담당자 또는 세일즈 팀에 문의하십시오.

["NetApp 계정 에 대해 자세히 알아보십시오"](#).

## 충전 관련 참고 사항

다음 세부 정보는 용량 기반 라이선싱에서 충전이 어떻게 작동하는지 이해하는 데 도움이 됩니다.

### 최소 충전

기본(읽기-쓰기) 볼륨이 하나 이상 있는 데이터 서비스 스토리지 VM마다 최소 4TiB가 필요합니다. 운영 볼륨의 합계가 4TiB 미만인 경우 BlueXP는 해당 스토리지 VM에 4TiB 최소 요금을 적용합니다.

아직 볼륨을 프로비저닝하지 않은 경우 최소 요금이 적용되지 않습니다.

Essentials 패키지의 경우 4TiB 최소 용량 비용은 보조(데이터 보호) 볼륨만 포함된 스토리지 VM에 적용되지 않습니다. 예를 들어, 1TiB의 보조 데이터를 사용하는 스토리지 VM의 경우 해당 1TiB 데이터에 대한 요금이 청구됩니다.

Essentials 이외의 모든 패키지 유형(Optimized(최적화), Professional(프로페셔널), Edge Cache(에지 캐시))에서 4TiB의 최소 용량 충전은 볼륨 유형에 관계없이 적용됩니다.

### 초과

BYOL 용량을 초과하거나 라이선스가 만료된 경우, 마켓플레이스 가입을 기준으로 시간당 요금이 초과됩니다.

### Essentials 패키지를 선택합니다

Essentials 패키지를 사용하면 배포 유형(HA 또는 단일 노드) 및 볼륨 유형(기본 또는 보조)으로 비용이 청구됩니다. 예를 들어, `_Essentials HA_`의 가격이 `_Essentials 보조 HA_`와 다릅니다.

NetApp에서 BYOL(Essentials) 라이선스를 구매하고 해당 배포 및 볼륨 유형에 대해 라이선스 용량을 초과하는 경우 BlueXP 디지털 지갑은 가격이 더 높은 Essentials 라이선스(있는 경우)에 대해 초과 요금을 부과합니다. 이는 시장에 대해 충전하기 전에 이미 선결제 용량으로 구매한 가용 용량을 처음 사용하기 때문입니다. 마켓플레이스에 비용을 청구하면 월별 청구서에 비용이 추가됩니다.

예를 들어, Essentials 패키지에 대해 다음 라이선스를 보유하고 있다고 가정해 보겠습니다.

- 500TiB\_Essentials 보조 HA\_license에 커밋된 용량이 500TiB입니다
- 100TiB의 커밋된 용량만 있는 500TiB\_Essentials 단일 Node\_license

보조 볼륨이 있는 HA 쌍에서 50TiB가 또 다른 프로비저닝됩니다. BlueXP 디지털 지갑은 50TiB에서 PAYGO로 충전하는 대신 `_Essentials Single Node_license`에 대해 50TiB 초과를 충전합니다. 이 라이선스는 `_Essentials Secondary HA_`보다 비싸지만 PAYGO 요금보다 저렴합니다.

BlueXP 디지털 지갑에서 50TiB가 `_Essentials Single Node_license`에 대해 청구된 것으로 표시됩니다.

## 스토리지 VM

- 추가 SVM(Data-Serving Storage VM)에 대한 추가 라이선스 비용은 없지만, 데이터 서비스 SVM당 최소 용량 비용은 4TiB입니다.
- 재해 복구 SVM은 프로비저닝된 용량에 따라 충전됩니다.

## HA 쌍

HA 쌍의 경우 노드의 프로비저닝된 용량에 대해서만 비용이 청구됩니다. 파트너 노드에 동기식으로 미러링되는 데이터에 대해서는 비용이 청구되지 않습니다.

## FlexClone 및 FlexCache 볼륨

- FlexClone 볼륨에 사용된 용량에 대해서는 비용이 청구되지 않습니다.
- 소스 및 타겟 FlexCache 볼륨은 프로비저닝된 공간에 따라 운영 데이터로 간주되고 충전됩니다.

## 시작하는 방법

용량 기반 라이선스를 시작하는 방법에 대해 알아보십시오.

- ["AWS에서 Cloud Volumes ONTAP에 대한 라이선스 설정"](#)
- ["Azure에서 Cloud Volumes ONTAP에 대한 라이선스를 설정합니다"](#)
- ["Google Cloud에서 Cloud Volumes ONTAP에 대한 라이선스를 설정합니다"](#)

## Keystone 구독

OpEx 소비 모델을 선호하는 투자자들에게 원활한 하이브리드 클라우드 경험을 제공하여 선불 CapEx 또는 임대를 지불하는 종량제 구독 기반 서비스입니다.

충전은 Keystone 가입 중 하나 이상의 Cloud Volumes ONTAP HA 쌍에서 대해 확정된 용량 크기를 기준으로 합니다.

각 볼륨에 대해 프로비저닝된 용량은 주기적으로 Keystone 가입 시 할당된 용량과 비교되며, Keystone 가입 시 초과요금이 부과됩니다.

["NetApp Keystone에 대해 자세히 알아보십시오"](#).

## 지원되는 구성

Keystone 구독은 HA 쌍으로 지원됩니다. 현재 단일 노드 시스템에서는 이 라이선스 옵션이 지원되지 않습니다.

## 용량 제한

각 개별 Cloud Volumes ONTAP 시스템은 디스크를 통해 최대 2개의 PiB 용량을 지원하고 오브젝트 스토리지로 계층화합니다.

## 시작하는 방법

Keystone 가입을 시작하는 방법 알아보기:

- ["AWS에서 Cloud Volumes ONTAP에 대한 라이선스 설정"](#)

- "Azure에서 Cloud Volumes ONTAP에 대한 라이선스를 설정합니다"
- "Google Cloud에서 Cloud Volumes ONTAP에 대한 라이선스를 설정합니다"

## 노드 기반 라이선스

노드 기반 라이선스는 이전 세대 라이선스 모델로, 노드별로 Cloud Volumes ONTAP에 대한 라이선스를 부여할 수 있도록 지원합니다. 이 라이선스 모델은 신규 고객에는 제공되지 않으며 무료 평가판을 사용할 수 없습니다. 노드별 충전은 위에서 설명한 용량 기준 충전 방법으로 대체되었습니다.

기존 고객은 노드 기반 라이선스를 계속 사용할 수 있습니다.

- 활성 라이선스가 있는 경우 BYOL은 라이선스 갱신에만 사용할 수 있습니다.
- 유효한 마켓플레이스 가입이 있는 경우에도 해당 구독을 통해 충전할 수 있습니다.

## 라이선스 변환

기존 Cloud Volumes ONTAP 시스템을 다른 라이선스 방식으로 변환하는 것은 지원되지 않습니다. 현재 세 가지 라이선스 방법은 용량 기반 라이선스, Keystone 가입 및 노드 기반 라이선싱입니다. 예를 들어, 시스템을 노드 기반 라이선싱에서 용량 기반 라이선싱으로 전환할 수 없습니다. 반대의 경우도 마찬가지입니다.

다른 라이선스 방법으로 이전하려는 경우 라이선스를 구입하고 해당 라이선스를 사용하여 새 Cloud Volumes ONTAP 시스템을 배포한 다음 데이터를 새 시스템으로 복제할 수 있습니다.

시스템을 PAYGO by-node 라이선싱에서 BYOL by-node 라이선싱으로 변환하는 기능은 지원되지 않습니다. 새 시스템을 구축한 다음 데이터를 해당 시스템으로 복제해야 합니다. ["PAYGO와 BYOL 간 전환 방법에 대해 알아보십시오"](#).

## 스토리지

### 클라이언트 프로토콜

Cloud Volumes ONTAP는 iSCSI, NFS, SMB, NVMe-TCP 및 S3 클라이언트 프로토콜을 지원합니다.

#### iSCSI

iSCSI는 표준 이더넷 네트워크에서 실행할 수 있는 블록 프로토콜입니다. 대부분의 클라이언트 운영 체제는 표준 이더넷 포트를 통해 실행되는 소프트웨어 이니시에이터를 제공합니다.

#### NFS 를 참조하십시오

NFS는 UNIX 및 Linux 시스템을 위한 기존 파일 액세스 프로토콜입니다. 클라이언트는 NFSv3, NFSv4 및 NFSv4.1 프로토콜을 사용하여 ONTAP 볼륨의 파일에 액세스할 수 있습니다. UNIX 스타일 사용 권한, NTFS 스타일 사용 권한 또는 이 두 가지를 혼합하여 파일 액세스를 제어할 수 있습니다.

클라이언트는 NFS 및 SMB 프로토콜을 모두 사용하여 동일한 파일에 액세스할 수 있습니다.

## 중소기업

SMB는 Windows 시스템을 위한 기존 파일 액세스 프로토콜입니다. 클라이언트는 SMB 2.0, SMB 2.1, SMB 3.0 및 SMB 3.1.1 프로토콜을 사용하여 ONTAP 볼륨의 파일에 액세스할 수 있습니다. NFS와 마찬가지로 사용 권한 스타일의 조합이 지원됩니다.

### S3

Cloud Volumes ONTAP은 스케일아웃 스토리지 옵션으로 S3를 지원합니다. S3 프로토콜 지원을 통해 스토리지 VM(SVM)의 버킷에 포함된 오브젝트에 대한 S3 클라이언트 액세스를 구성할 수 있습니다.

["S3 멀티 프로토콜의 작동 방식에 대해 알아보십시오"](#).

["ONTAP에서 S3 오브젝트 스토리지 서비스를 구성 및 관리하는 방법에 대해 알아보십시오"](#).

### NVMe-TCP

Cloud Volumes ONTAP 버전 9.12.1 이상을 사용하는 경우 클라우드 공급자는 NVMe-TCP를 지원합니다. BlueXP는 NVMe-TCP에 대한 관리 기능을 제공하지 않습니다.

ONTAP를 통해 NVMe를 구성하는 방법에 대한 자세한 내용은 ["NVMe용 스토리지 VM을 구성합니다"](#)를 참조하십시오.

## 디스크와 애그리게이트

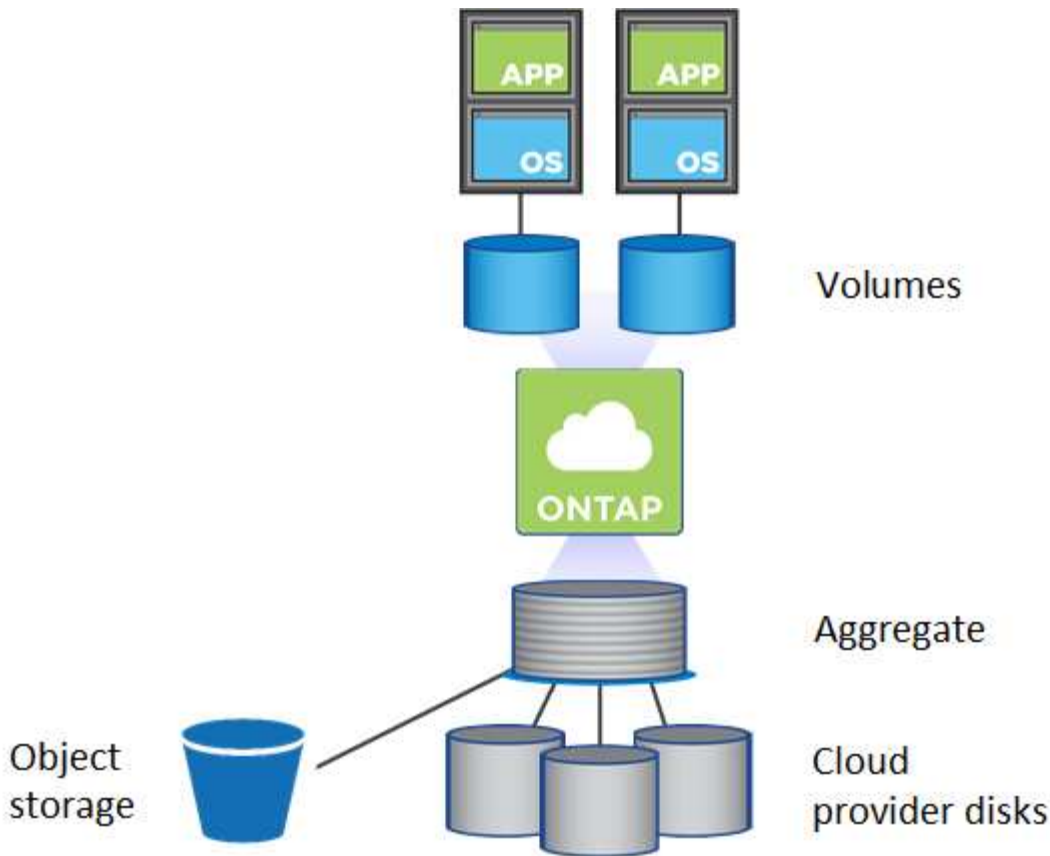
Cloud Volumes ONTAP에서 클라우드 스토리지를 사용하는 방법을 이해하면 스토리지 비용을 이해하는 데 도움이 됩니다.



모든 디스크와 애그리게이트는 BlueXP에서 직접 생성 및 삭제해야 합니다. 다른 관리 도구에서 이러한 작업을 수행해서는 안 됩니다. 이렇게 하면 시스템 안정성에 영향을 주고 향후 디스크를 추가할 수 없도록 하며 중복 클라우드 공급자 비용을 생성할 수 있습니다.

## 개요

Cloud Volumes ONTAP은 클라우드 공급자 스토리지를 디스크로 사용하고 이러한 스토리지를 하나 이상의 애그리게이트로 그룹화합니다. 애그리게이트는 하나 이상의 볼륨에 스토리지를 제공합니다.



여러 유형의 클라우드 디스크가 지원됩니다. Cloud Volumes ONTAP를 배포할 때 볼륨을 생성할 때 디스크 유형을 선택하고 기본 디스크 크기를 선택합니다.



클라우드 공급자로부터 구입한 총 스토리지 양은 `_raw capacity_`입니다. 가용 용량은 약 12~14%가 Cloud Volumes ONTAP용으로 예약된 오버헤드이므로 `_이(가)` 적습니다. 예를 들어, BlueXP가 500GiB 애그리게이트를 생성할 경우 가용 용량은 442.94GiB입니다.

## 설치하고

AWS에서 Cloud Volumes ONTAP는 사용자 데이터에 EBS 스토리지를 사용하고, 일부 EC2 인스턴스 유형에서 로컬 NVMe 스토리지를 Flash Cache로 사용합니다.

## EBS 스토리지

AWS에서는 aggregate에 동일한 크기의 디스크를 최대 6개까지 포함할 수 있습니다. 하지만 Amazon EBS Elastic Volumes 기능을 지원하는 구성이 있는 경우 aggregate에 디스크를 최대 8개까지 포함할 수 있습니다. "[Elastic Volumes 지원에 대해 자세히 알아보십시오](#)".

최대 디스크 크기는 16TiB입니다.

기본 EBS 디스크 유형은 범용 SSD(GP3 또는 GP2), 프로비저닝된 IOPS SSD(i1) 또는 처리량 최적화 HDD(st1)일 수 있습니다. EBS 디스크를 Amazon S3와 에 페어링할 수 있습니다. "[비활성 데이터를 저비용 오브젝트 스토리지로 계층화합니다](#)".



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

## 로컬 NVMe 스토리지

일부 EC2 인스턴스 유형에는 Cloud Volumes ONTAP이 사용하는 로컬 NVMe 스토리지가 있습니다 "[Flash Cache를 참조하십시오](#)".

- [관련 링크 \\*](#)
- "[AWS 설명서:EBS 볼륨 유형](#)"
- "[AWS에서 시스템의 디스크 유형 및 디스크 크기를 선택하는 방법에 대해 알아보십시오](#)"
- "[AWS의 Cloud Volumes ONTAP에 대한 스토리지 제한을 검토합니다](#)"
- "[AWS에서 지원되는 Cloud Volumes ONTAP 구성 검토](#)"

## Azure 스토리지

Azure에서는 aggregate가 동일한 크기의 디스크를 최대 12개까지 포함할 수 있습니다. 디스크 유형과 최대 디스크 크기는 단일 노드 시스템을 사용하는지 HA 쌍을 사용하는지에 따라 달라집니다.

### 단일 노드 시스템

단일 노드 시스템에서는 세 가지 유형의 Azure 관리 디스크를 사용할 수 있습니다.

- *Premium SSD* 관리 디스크 높은 비용으로 I/O 집약적인 작업 부하에 높은 성능을 제공합니다.
- *\_Standard SSD Managed Disks\_* 는 낮은 IOPS가 필요한 워크로드에 일관된 성능을 제공합니다.
- *\_표준 HDD 관리 디스크\_* 는 높은 IOPS가 필요하지 않고 비용을 절감하려는 경우에 적합합니다.

관리되는 각 디스크 유형의 최대 디스크 크기는 32TiB입니다.

Azure Blob 저장소와 관리되는 디스크를 에 페어링할 수 있습니다 "[비활성 데이터를 저비용 오브젝트 스토리지로 계층화합니다](#)".

## HA 쌍

HA Pair는 저렴한 비용으로 I/O 집약적인 워크로드에 고성능을 제공하는 두 가지 유형의 디스크를 사용합니다.

- *\_PREMIUM PAGE BLOBS\_* 로, 최대 디스크 크기는 8TiB입니다
- *\_관리되는 디스크\_* 최대 디스크 크기가 32TiB인 경우
- [관련 링크 \\*](#)
- "[Microsoft Azure 설명서: Azure 관리 디스크 유형](#)"
- "[Microsoft Azure 설명서: Azure 페이지 Blob의 개요](#)"
- "[Azure에서 시스템의 디스크 유형 및 디스크 크기를 선택하는 방법에 대해 알아보십시오](#)"
- "[Azure의 Cloud Volumes ONTAP에 대한 스토리지 제한을 검토합니다](#)"

## Google Cloud 스토리지

Google Cloud에서는 aggregate에 동일한 크기의 디스크를 최대 6개까지 포함할 수 있습니다. 최대 디스크 크기는 64TiB입니다.

디스크 유형은 *\_ Zonal SSD 영구 디스크 \_*, *\_ 균형 조정 영구 디스크 \_* 또는 *\_ Zonal 표준 영구 디스크 \_* 일 수



있습니다. 영구 디스크를 Google Storage 버킷과 에 페어링할 수 있습니다 ["비활성 데이터를 저비용 오브젝트 스토리지로 계층화합니다"](#).

- [관련 링크 \\*](#)
- ["Google Cloud 설명서: 스토리지 옵션"](#)
- ["Google Cloud의 Cloud Volumes ONTAP에 대한 스토리지 제한사항을 검토하십시오"](#)

## RAID 유형입니다

각 Cloud Volumes ONTAP 애그리게이트의 RAID 유형은 RAID0(스트라이핑)입니다. Cloud Volumes ONTAP은 클라우드 공급자에 의존하여 디스크 가용성 및 내구성을 제공합니다. 다른 RAID 유형은 지원되지 않습니다.

핫 스페어

RAID0은 중복성을 위해 핫 스페어 사용을 지원하지 않습니다.

Cloud Volumes ONTAP 인스턴스에 연결된 사용하지 않는 디스크(핫 스페어)를 생성하는 것은 불필요한 비용이며 필요에 따라 추가 공간을 프로비저닝하지 못할 수 있습니다. 따라서 권장되지 않습니다.

## AWS의 탄력적인 볼륨

Cloud Volumes ONTAP aggregate에서 Amazon EBS Elastic Volumes 기능을 지원하여 더 나은 성능과 추가 용량을 제공하는 동시에 BlueXP에서 필요에 따라 기본 디스크 용량을 자동으로 늘릴 수 있습니다.

이점

- 동적 디스크 확장

BlueXP는 Cloud Volumes ONTAP가 실행 중이고 디스크가 연결되어 있는 동안 디스크의 크기를 동적으로 늘릴 수 있습니다.

- 더 뛰어난 성능

Elastic Volumes에서 설정된 애그리게이트에는 2개의 RAID 그룹에 걸쳐 동일한 활용의 최대 8개의 디스크를 포함할 수 있습니다. 이 구성은 더 많은 처리량과 일관된 성능을 제공합니다.

- 더 커진 애그리게이트

8개의 디스크를 지원하여 최대 128TiB의 애그리게이트 용량을 제공합니다. 이러한 제한은 Elastic Volumes 기능을 사용할 수 없는 애그리게이트에 대해 6개의 디스크 한계 및 96TiB 제한보다 높습니다.

총 시스템 용량 제한은 동일하게 유지됩니다.

["AWS의 Elastic Volumes에 대해 자세히 알아보십시오"](#)

지원되는 구성

Amazon EBS Elastic Volumes 기능은 특정 Cloud Volumes ONTAP 버전 및 특정 EBS 디스크 유형에서 지원됩니다.

## Cloud Volumes ONTAP 버전입니다

탄성 볼륨 기능은 버전 9.11.0 이상에서 생성된 `_NEW_` Cloud Volumes ONTAP 시스템에서 지원됩니다. 이 기능은 9.11.0 이전에 배포된 기존 Cloud Volumes ONTAP 시스템에서 `_NOT_` 지원됨 입니다.

예를 들어, Cloud Volumes ONTAP 9.9.0 시스템을 만든 다음 나중에 이 시스템을 버전 9.11.0으로 업그레이드한 경우에는 탄성 볼륨 기능이 지원되지 않습니다. 버전 9.11.0 이상을 사용하여 배포된 새 시스템이어야 합니다.

## EBS 디스크 유형

GP3(General Purpose SSD) 또는 ios1(Provisioned IOPS SSD)을 사용하는 경우 Elastic Volumes 기능이 애그리게이트 레벨에서 자동으로 활성화됩니다. Elastic Volumes 기능은 다른 디스크 유형을 사용하는 애그리게이트에서는 지원되지 않습니다.

## 필수 AWS 권한

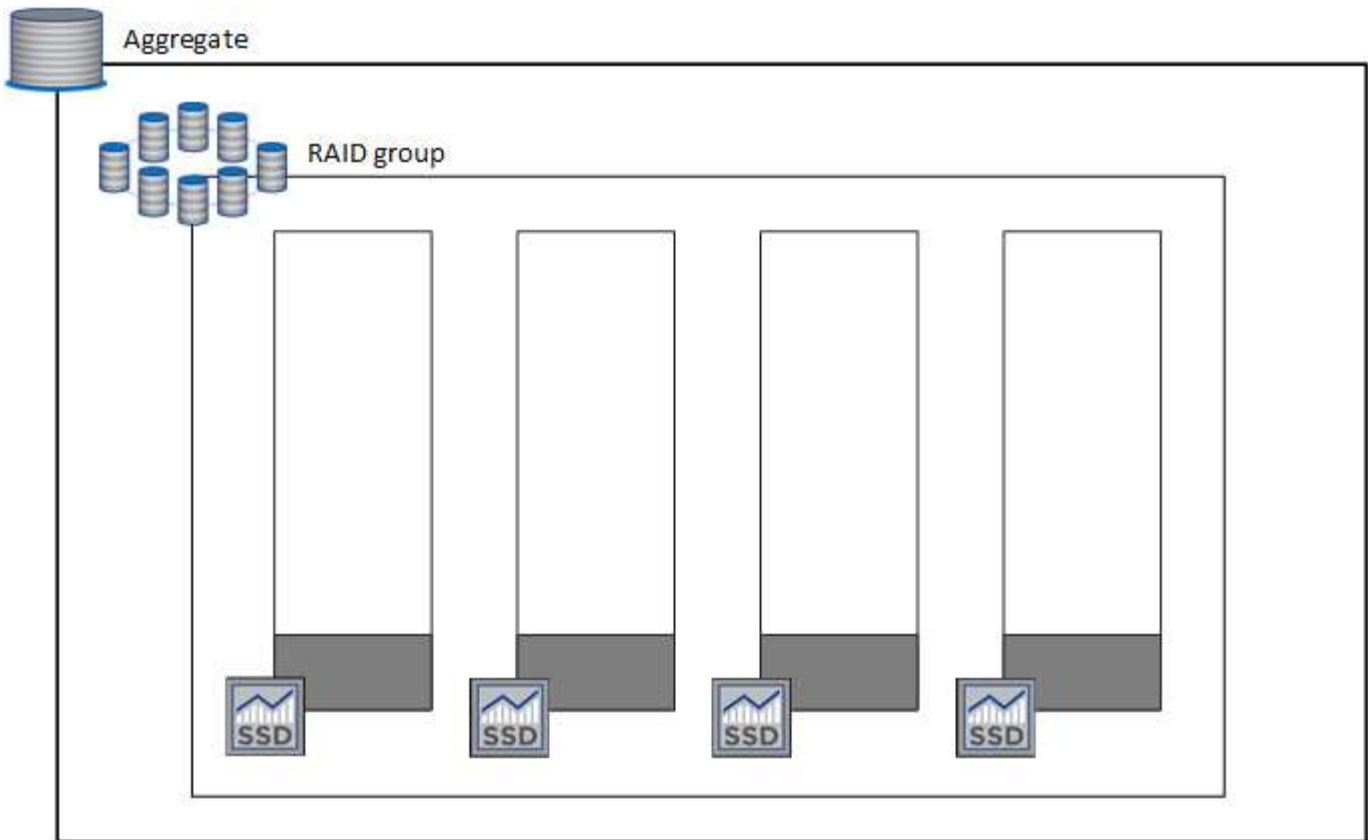
3.9.19 릴리즈부터 Cloud Volumes ONTAP 애그리게이트에서 탄성 볼륨 기능을 활성화하고 관리하려면 다음 권한이 필요합니다.

- EC2: 볼륨 수정 설명
- EC2: ModifyVolume(수정 볼륨)

이러한 권한은 에 포함되어 있습니다 ["NetApp에서 제공하는 정책"](#)

## Elastic Volumes의 지원 방식

Elastic Volumes 기능이 설정된 애그리게이트는 하나 또는 두 개의 RAID 그룹으로 구성됩니다. 각 RAID 그룹에는 동일한 용량을 가진 4개의 동일한 디스크가 있습니다. 다음은 각각 2.5TiB인 디스크 4개가 있는 10TiB 애그리게이트의 예입니다.



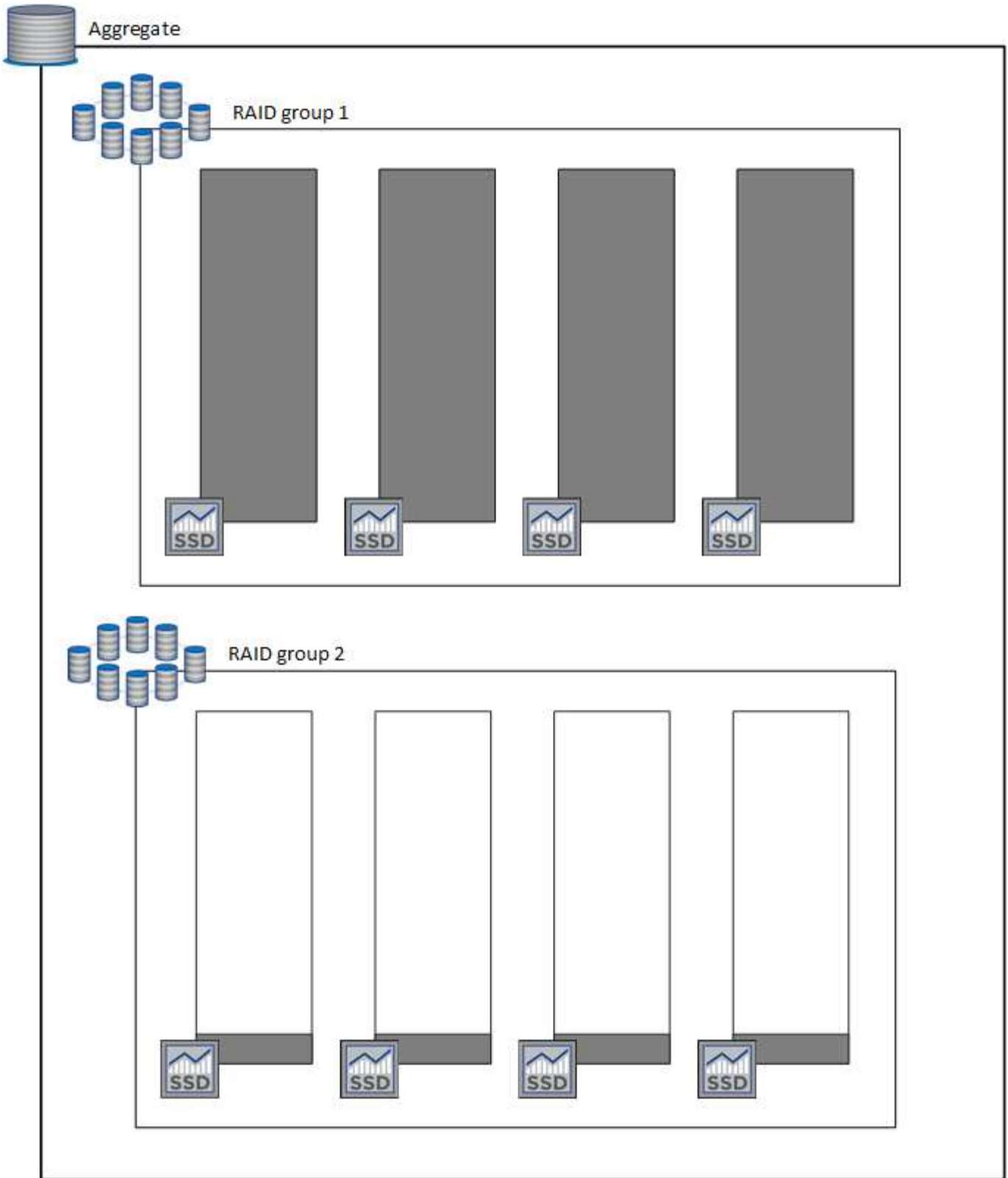
BlueXP에서 애그리게이트를 생성하면 하나의 RAID 그룹으로 시작됩니다. 추가 용량이 필요한 경우 RAID 그룹에 있는 모든 디스크의 용량을 동일한 용량으로 늘려 전체 용량을 늘릴 수 있습니다. 용량 증가는 애그리게이트 크기의 최소 256GiB 또는 10%입니다.

예를 들어, 1TiB Aggregate가 있는 경우 각 디스크는 250GiB입니다. 총 용량의 10%는 100GiB입니다. 이 값이 256GiB보다 낮으므로 애그리게이트의 크기가 최소 256GiB(각 디스크의 경우 64GiB)까지 증가합니다.

BlueXP는 Cloud Volumes ONTAP 시스템이 실행되는 동안 디스크가 연결되어 있는 동안 디스크의 크기를 늘립니다. 이러한 변경은 무중단으로 제공됩니다.

aggregate가 64TiB(또는 각 디스크의 16TiB)에 도달하면 BlueXP가 추가 용량을 위해 두 번째 RAID 그룹을 생성합니다. 두 번째 RAID 그룹은 첫 번째 RAID 그룹과 동일하게 작동합니다. 네 개의 디스크가 정확히 동일한 용량으로 최대 64TiB까지 증가할 수 있습니다. 즉, Aggregate의 최대 용량은 128TiB입니다.

다음은 두 개의 RAID 그룹이 있는 애그리게이트의 예입니다. 첫 번째 RAID 그룹의 용량 제한에 도달했으며 두 번째 RAID 그룹의 디스크에 여유 공간이 충분합니다.



볼륨을 생성할 때 수행되는 작업

GP3 또는 ios1 디스크를 사용하는 볼륨을 생성하는 경우 BlueXP는 다음과 같이 aggregate에 볼륨을 생성합니다.

- Elastic Volumes가 활성화된 기존 GP3 또는 iio1 애그리게이트는 BlueXP에서 해당 애그리게이트에 볼륨을 생성합니다.

- Elastic Volumes가 활성화된 GP3 또는 iio1 애그리게이트가 여러 개 있는 경우 BlueXP는 최소한의 리소스를 필요로 하는 볼륨을 애그리게이트에 생성합니다.
- 시스템에 Elastic Volumes에 대해 활성화되지 않은 GP3 또는 ios1 애그리게이트만 있는 경우 해당 애그리게이트에 볼륨이 생성됩니다.

이 시나리오는 가능성이 낮지만 다음 두 가지 경우에 가능합니다.



- API에서 Aggregate를 생성할 때 Elastic Volumes 기능을 명시적으로 비활성화했습니다.
- 사용자 인터페이스에서 새 Cloud Volumes ONTAP 시스템을 생성했습니다. 이 경우 초기 애그리게이트에 탄성 볼륨 기능이 비활성화됩니다. 검토 [제한 사항](#) 을 참조하십시오.

- 기존 Aggregate의 용량이 충분하지 않은 경우, BlueXP는 Elastic Volumes가 설정된 Aggregate를 생성한 다음 해당 새 Aggregate에 볼륨을 생성합니다.

Aggregate의 크기는 요청된 볼륨 크기와 추가 10% 용량을 기준으로 합니다.

#### 용량 관리 모드

Connector의 용량 관리 모드는 다른 유형의 집선과 유사한 방식으로 Elastic Volumes와 작동합니다.

- 자동 모드가 활성화되면(기본 설정) 추가 용량이 필요할 경우 BlueXP가 자동으로 집계 크기를 늘립니다.
- 용량 관리 모드를 수동으로 변경하면 BlueXP에서 추가 용량 구매 승인을 요청합니다.

["용량 관리 모드에 대해 자세히 알아보십시오"](#).

#### 제한 사항

애그리게이트 크기를 늘리는 데 최대 6시간이 걸릴 수 있습니다. 그 동안 BlueXP는 해당 집계의 추가 용량을 요청할 수 없습니다.

#### 탄성 볼륨 작업 방법

다음과 같이 BlueXP에서 탄성 볼륨으로 작업할 수 있습니다.

- GP3 또는 io1 디스크를 사용할 때 초기 애그리게이트에 Elastic Volumes가 설정된 새 시스템을 생성합니다

["Cloud Volumes ONTAP 시스템을 생성하는 방법을 알아보십시오"](#)

- Elastic Volumes가 설정된 Aggregate에 새 볼륨을 생성합니다

GP3 또는 io1 디스크를 사용하는 볼륨을 생성하는 경우 BlueXP는 Elastic Volumes가 활성화된 Aggregate에 볼륨을 자동으로 생성합니다. 자세한 내용은 [볼륨을 생성할 때 수행되는 작업](#).

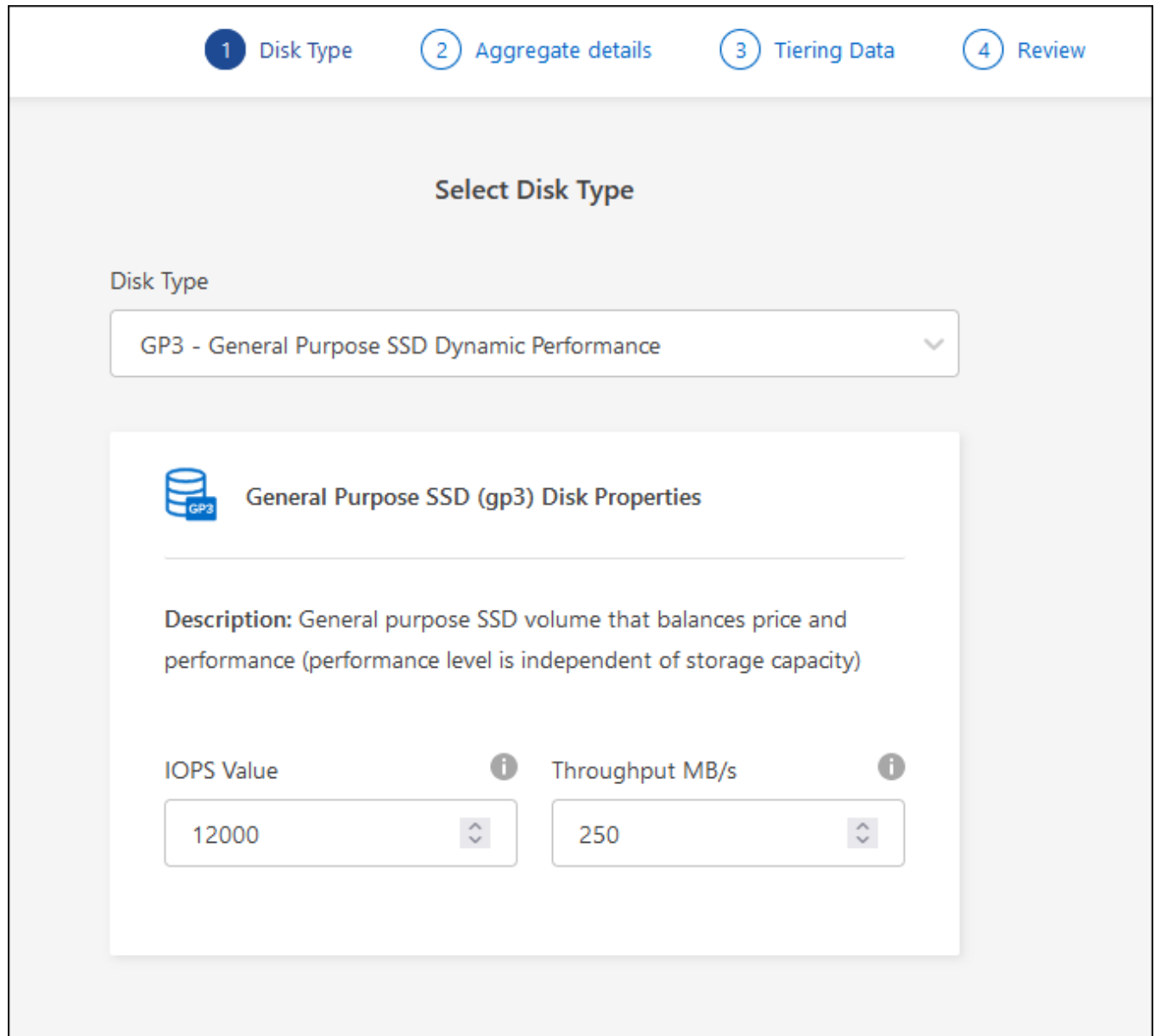
["볼륨을 생성하는 방법에 대해 알아보십시오"](#).

- Elastic Volumes가 설정된 새 Aggregate를 생성합니다

Cloud Volumes ONTAP 시스템이 버전 9.11.0 이상에서 생성된 경우 GP3 또는 ios1 디스크를 사용하는 새 애그리게이트에 탄력적인 볼륨이 자동으로 활성화됩니다.

Aggregate를 생성할 때 BlueXP에서 Aggregate의 용량 크기를 묻는 메시지를 표시합니다. 이는 디스크 크기 및 디스크 수를 선택하는 다른 구성과 다릅니다.

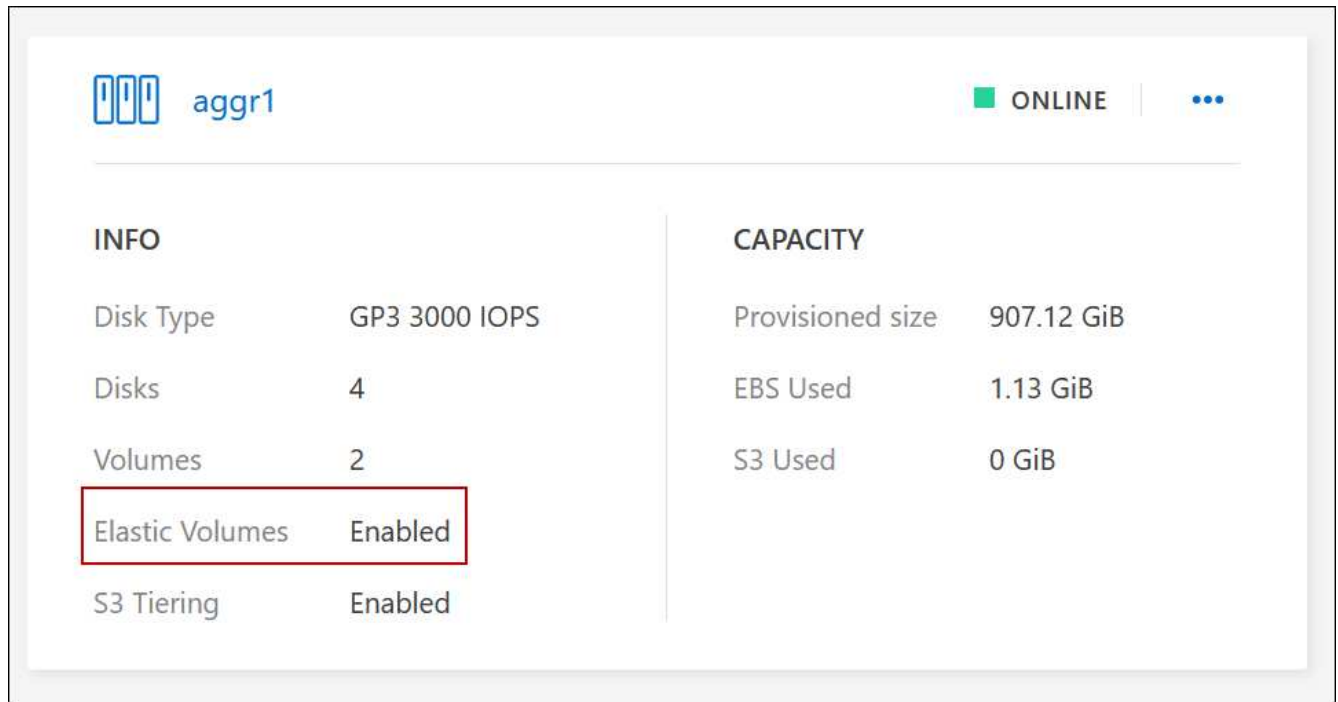
다음 스크린샷은 GP3 디스크로 구성된 새로운 Aggregate의 예를 보여줍니다.



["Aggregate를 생성하는 방법을 알아보십시오."](#)

- Elastic Volumes가 설정된 애그리게이트를 식별합니다

고급 할당 페이지로 이동하면 애그리게이트에 Elastic Volumes 기능이 설정되어 있는지 확인할 수 있습니다. 다음 예에서는 aggr1에 Elastic Volumes가 활성화되어 있습니다.



- Aggregate에 용량을 추가합니다

BlueXP는 필요에 따라 자동으로 Aggregate 용량을 추가하지만 수동으로 용량을 늘릴 수 있습니다.

["애그리게이트 용량을 늘리는 방법에 대해 알아보십시오"](#).

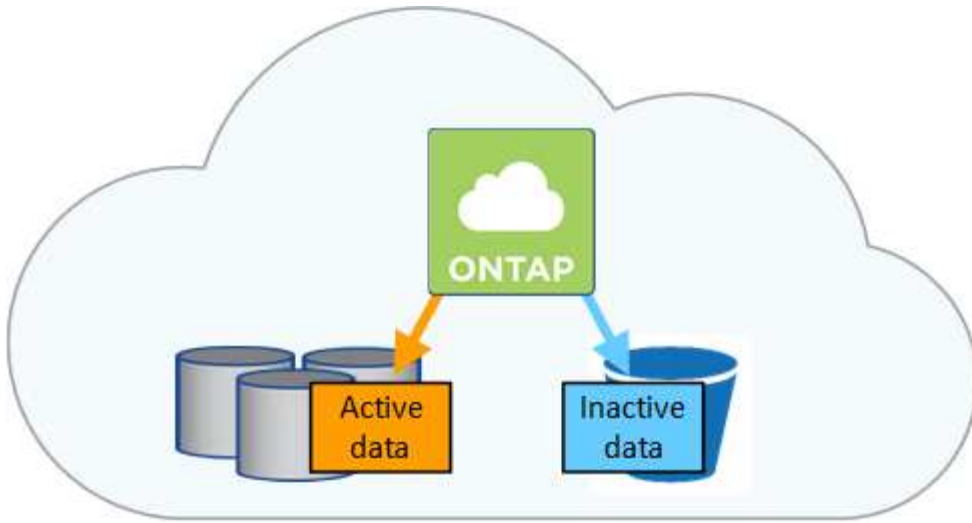
- Elastic Volumes가 설정된 Aggregate에 데이터를 복제합니다

대상 Cloud Volumes ONTAP 시스템이 Elastic Volumes를 지원하는 경우, GP3 또는 ios1 디스크를 선택하면 대상 볼륨이 활성화된 Aggregate에 배치됩니다.

["데이터 복제를 설정하는 방법에 대해 알아보십시오"](#)

## 데이터 계층화 개요

비활성 데이터를 저비용 오브젝트 스토리지로 자동 계층화하여 스토리지 비용을 절감합니다. 활성 데이터는 고성능 SSD 또는 HDD에 남아 있고 비활성 데이터는 저비용 오브젝트 스토리지로 계층화되어 있습니다. 따라서 운영 스토리지의 공간을 재확보하고 2차 스토리지를 축소할 수 있습니다.



데이터 계층화는 FabricPool 기술을 기반으로 합니다.



FabricPool(데이터 계층화)를 사용하기 위해 기능 라이선스를 설치할 필요가 없습니다.

### AWS의 데이터 계층화

AWS에서 데이터 계층화를 활성화하면 Cloud Volumes ONTAP은 EBS를 핫 데이터의 성능 계층으로, AWS S3를 비활성 데이터의 용량 계층으로 사용합니다.

#### 성능 계층

성능 계층은 범용 SSD(GP3 또는 GP2) 또는 프로비저닝된 IOPS SSD(io1)일 수 있습니다.

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

#### 용량 계층

Cloud Volumes ONTAP 시스템은 비활성 데이터를 단일 S3 버킷에 계층화합니다.

BlueXP는 각 작업 환경에 대해 단일 S3 버킷을 생성하고 Fabric-pool-\_cluster unique identifier\_라는 이름을 지정합니다. 각 볼륨에 대해 다른 S3 버킷이 생성되지 않습니다.

BlueXP에서 S3 버킷을 생성할 때 다음 기본 설정을 사용합니다.

- 스토리지 클래스: 표준
- 기본 암호화: 사용 안 함
- 공용 액세스 차단: 모든 공용 액세스를 차단합니다
- 객체 소유권: ACL이 설정되었습니다
- 버킷 버전 관리: 비활성화됨
- 개체 잠금: 사용 안 함

#### 스토리지 클래스

AWS의 계층형 데이터에 대한 기본 스토리지 클래스는 \_Standard\_입니다. 표준은 여러 가용성 영역에 걸쳐 자주 액세스하는 데이터에 적합합니다.



비활성 데이터에 액세스할 계획이 없는 경우 스토리지 클래스를 *Intelligent Tiering*, *One-Zone Infrequent Access*, *Standard - Infrequent Access* 또는 *S3 Glacier Instant Retrieval* 중 하나로 변경하여 저장소 비용을 줄일 수 있습니다. 스토리지 클래스를 변경하면 비활성 데이터가 표준 스토리지 클래스에서 시작되어 30일 후에 액세스하지 않는 경우 선택한 스토리지 클래스로 전환됩니다.

데이터에 액세스하는 경우 액세스 비용이 더 높아지므로 스토리지 클래스를 변경하기 전에 이 점을 고려해야 합니다. "[Amazon S3 스토리지 클래스에 대해 자세히 알아보십시오](#)".

작업 환경을 생성할 때 스토리지 클래스를 선택하면 이후에 언제든지 변경할 수 있습니다. 스토리지 클래스 변경에 대한 자세한 내용은 ["비활성 데이터를 저비용 오브젝트 스토리지로 계층화"](#).

데이터 계층화를 위한 스토리지 클래스는 볼륨이 아니라 시스템 전체에 적용됩니다.

## Azure의 데이터 계층화

Azure에서 데이터 계층화를 활성화하면 Cloud Volumes ONTAP는 Azure 관리 디스크를 핫 데이터의 성능 계층으로, Azure Blob 스토리지를 비활성 데이터의 용량 계층으로 사용합니다.

### 성능 계층

성능 계층은 SSD 또는 HDD가 될 수 있습니다.

### 용량 계층

Cloud Volumes ONTAP 시스템은 비활성 데이터를 단일 Blob 컨테이너에 계층화합니다.

BlueXP는 각 Cloud Volumes ONTAP 작업 환경에 대한 컨테이너로 새 저장소 계정을 만듭니다. 스토리지 계정의 이름은 임의로 지정됩니다. 각 볼륨에 대해 다른 컨테이너가 생성되지 않습니다.

BlueXP는 다음과 같은 설정으로 저장소 계정을 만듭니다.

- 액세스 계층: 핫
- 성능: 표준
- 이중화: LRS(Locally-Redundant Storage)
- 계정:StorageV2(범용 v2)
- REST API 작업을 위한 보안 전송 필요: 사용
- 스토리지 계정 키 액세스: 사용
- 최소 TLS 버전: 버전 1.2
- 인프라 암호화: 사용 안 함

### 스토리지 액세스 계층

Azure의 계층화된 데이터에 대한 기본 스토리지 액세스 계층은 `_hot_tier`입니다. 핫 계층은 용량 계층에서 자주 액세스하는 데이터에 적합합니다.

용량 계층의 비활성 데이터에 액세스할 계획이 없는 경우 `_cool_storage` 계층으로 변경하여 스토리지 비용을 절감할 수 있습니다. 스토리지 계층을 냉각으로 변경하면 비활성 용량 계층 데이터가 차가운 스토리지 계층으로 직접 이동합니다.

데이터에 액세스하는 경우 액세스 비용이 더 높아지므로 스토리지 계층을 변경하기 전에 이 점을 고려해야 합니다. "[Azure Blob 스토리지 액세스 계층에 대해 자세히 알아보십시오](#)".

작업 환경을 생성할 때 스토리지 계층을 선택할 수 있으며 그 후에는 언제든지 변경할 수 있습니다. 스토리지 계층 변경에 대한 자세한 내용은 ["비활성 데이터를 저비용 오브젝트 스토리지로 계층화"](#).

데이터 계층화를 위한 스토리지 액세스 계층은 볼륨 단위로 표시되지 않고 시스템 전체에 적용됩니다.

## Google Cloud의 데이터 계층화

Google Cloud에서 데이터 계층화를 활성화하면 Cloud Volumes ONTAP은 핫 데이터를 위한 성능 계층으로 영구 디스크를 사용하고 비활성 데이터를 위한 용량 계층으로 Google Cloud Storage 버킷을 사용합니다.

### 성능 계층

성능 계층은 SSD 영구 디스크, 균형 잡힌 영구 디스크 또는 표준 영구 디스크일 수 있습니다.

### 용량 계층

Cloud Volumes ONTAP 시스템은 단일 Google 클라우드 스토리지 버킷에 비활성 데이터를 계층화합니다.

BlueXP는 각 작업 환경에 대한 버킷을 생성하여 `Fabric-pool-_cluster unique identifier`로 명명합니다. 각 볼륨에 대해 다른 버킷이 생성되지 않습니다.

BlueXP에서 버킷을 생성할 때 다음 기본 설정을 사용합니다.

- 위치 유형: 지역
- 스토리지 클래스: 표준
- 공용 액세스: 개체 ACL의 영향을 받습니다
- 액세스 제어: 미세
- 보호: 없음
- 데이터 암호화: Google에서 관리하는 키입니다

### 스토리지 클래스

계층화된 데이터에 대한 기본 스토리지 클래스는 *Standard Storage\_class*입니다. 데이터에 자주 액세스하지 않는 경우 *\_Nearline Storage* 또는 *Coldline Storage*로 변경하여 스토리지 비용을 절감할 수 있습니다. 스토리지 클래스를 변경하면 비활성 데이터가 선택한 클래스로 직접 이동합니다.

데이터에 액세스하는 경우 액세스 비용이 더 높아지므로 스토리지 클래스를 변경하기 전에 이 점을 고려해야 합니다. ["Google Cloud Storage용 스토리지 클래스에 대해 자세히 알아보십시오"](#).

작업 환경을 생성할 때 스토리지 계층을 선택할 수 있으며 그 후에는 언제든지 변경할 수 있습니다. 스토리지 클래스 변경에 대한 자세한 내용은 ["비활성 데이터를 저비용 오브젝트 스토리지로 계층화"](#).

데이터 계층화를 위한 스토리지 클래스는 볼륨이 아니라 시스템 전체에 적용됩니다.

### 데이터 계층화 및 용량 제한

데이터 계층화를 사용하는 경우 시스템의 용량 제한은 동일하게 유지됩니다. 이 제한은 성능 계층과 용량 계층 전체에 분산됩니다.

### 볼륨 계층화 정책

데이터 계층화를 사용하려면 볼륨을 생성, 수정 또는 복제할 때 볼륨 계층화 정책을 선택해야 합니다. 각 볼륨에 대해

다른 정책을 선택할 수 있습니다.

일부 계층화 정책에는 연결된 최소 냉각 기간이 있습니다. 이 기간은 볼륨의 사용자 데이터가 "콜드"로 간주되어 용량 계층으로 이동되기 위해 비활성 상태로 유지되어야 하는 시간을 설정합니다. 냉각 기간은 데이터를 Aggregate에 쓸 때 시작됩니다.



최소 냉각 기간 및 기본 집계 임계값을 50%로 변경할 수 있습니다(아래 참조). "냉각 기간을 변경하는 방법에 대해 알아보십시오" 및 "임계값을 변경하는 방법에 대해 알아보십시오".

BlueXP에서는 볼륨을 생성하거나 수정할 때 다음 볼륨 계층화 정책 중에서 선택할 수 있습니다.

#### 스냅샷만

Aggregate가 50% 용량에 도달하면 Cloud Volumes ONTAP는 활성 파일 시스템과 연결되지 않은 스냅샷 복사본의 콜드 사용자 데이터를 용량 계층으로 이동합니다. 냉각 기간은 약 2일입니다.

읽으면 용량 계층의 콜드 데이터 블록이 핫 상태가 되고 성능 계층으로 이동합니다.

#### 모두

모든 데이터(메타데이터 제외)는 즉시 오브젝트 스토리지에 대해 콜드 및 계층화되도록 빨리 표시됩니다. 볼륨의 새 블록이 냉각될 때까지 48시간 동안 기다릴 필요가 없습니다. 모든 정책을 설정하기 전에 볼륨에 있는 블록이 콜드 상태가 되려면 48시간이 걸립니다.

읽으면 클라우드 계층의 콜드 데이터 블록이 콜드 상태를 유지하고 성능 계층에 다시 기록되지 않습니다. 이 정책은 ONTAP 9.6부터 사용할 수 있습니다.

#### 자동

Aggregate가 50% 용량에 도달하면 Cloud Volumes ONTAP는 볼륨의 콜드 데이터 블록을 용량 계층에 계층화합니다. 콜드 데이터에는 스냅샷 복사본뿐만 아니라 액티브 파일 시스템의 콜드 사용자 데이터도 포함됩니다. 냉각 기간은 약 31일입니다.

이 정책은 Cloud Volumes ONTAP 9.4부터 지원됩니다.

랜덤 읽기로 읽는 경우 용량 계층의 콜드 데이터 블록이 핫 상태가 되어 성능 계층으로 이동합니다. 인덱스 및 바이러스 백신 검사와 관련된 읽기 작업을 순차적으로 수행할 경우 콜드 데이터 블록이 콜드 상태를 유지하고 성능 계층으로 이동하지 않습니다.

#### 없음

볼륨의 데이터를 성능 계층에 유지하여 용량 계층으로 이동하지 않도록 합니다.

볼륨을 복제할 때 데이터를 오브젝트 스토리지에 계층화할지 여부를 선택할 수 있습니다. BlueXP는 데이터 보호 볼륨에 \*백업\* 정책을 적용합니다. Cloud Volumes ONTAP 9.6부터 \*All\* 계층화 정책은 백업 정책을 대체합니다.

#### Cloud Volumes ONTAP를 끄면 냉각 기간에 영향을 줍니다

데이터 블록은 냉각 스캔을 통해 냉각됩니다. 이 과정에서 사용되지 않은 블록은 블록 온도를 다음으로 낮은 값으로 이동(냉각)했습니다. 기본 냉각 시간은 볼륨 계층화 정책에 따라 달라집니다.

- 자동: 31일
- 스냅샷 전용: 2일

냉각 스캔이 작동하려면 Cloud Volumes ONTAP가 실행 중이어야 합니다. Cloud Volumes ONTAP가 꺼져 있으면

냉각도 중지됩니다. 결과적으로 냉각 시간이 길어집니다.



Cloud Volumes ONTAP를 끄면 시스템을 다시 시작할 때까지 각 블록의 온도가 유지됩니다. 예를 들어, 시스템을 끌 때 블록의 온도가 5이면 시스템을 다시 켤 때 온도가 5가 됩니다.

## 데이터 계층화 설정

지원되는 구성의 지침과 목록은 를 참조하십시오 "[비활성 데이터를 저비용 오브젝트 스토리지로 계층화](#)".

## 스토리지 관리

BlueXP는 Cloud Volumes ONTAP 스토리지의 단순하고 고급 관리 기능을 제공합니다.



모든 디스크와 애그리게이트는 BlueXP에서 직접 생성 및 삭제해야 합니다. 다른 관리 도구에서 이러한 작업을 수행해서는 안 됩니다. 이렇게 하면 시스템 안정성에 영향을 주고 향후 디스크를 추가할 수 없도록 하며 중복 클라우드 공급자 비용을 생성할 수 있습니다.

## 스토리지 프로비저닝

BlueXP는 디스크를 구매하고 애그리게이트를 관리하여 Cloud Volumes ONTAP에 대한 스토리지 프로비저닝을 쉽게 수행합니다. 볼륨을 생성하기만 하면 됩니다. 필요한 경우 고급 할당 옵션을 사용하여 애그리게이트를 직접 프로비저닝할 수 있습니다.

### 간소화된 프로비저닝

애그리게이트는 볼륨에 클라우드 스토리지를 제공합니다. BlueXP는 인스턴스를 시작할 때와 추가 볼륨을 프로비저닝할 때 사용자를 위해 애그리게이트를 생성합니다.

볼륨을 만들 때 BlueXP는 다음 세 가지 중 하나를 수행합니다.

- 여유 공간이 충분한 기존 애그리게이트에 볼륨을 배치합니다.
- 이 Aggregate에 사용할 디스크를 더 많이 구입하여 기존 Aggregate에 볼륨을 배치합니다.

### 를 누릅니다

AWS에서 Elastic Volumes를 지원하는 애그리게이트의 경우 BlueXP는 RAID 그룹의 디스크 크기도 증가합니다. "[Elastic Volumes 지원에 대해 자세히 알아보십시오](#)".

- 새로운 애그리게이트를 위해 디스크를 구매하고 애그리게이트에 볼륨을 배치했습니다.

BlueXP는 애그리게이트의 최대 크기, 씬 프로비저닝 활성화 여부, 애그리게이트의 여유 공간 임계값 등 여러 요소를 확인하여 새 볼륨을 배치할 위치를 결정합니다.



계정 관리자는 \* 설정 \* 페이지에서 여유 공간 임계값을 수정할 수 있습니다.

## AWS에서 Aggregate를 위한 디스크 크기 선택

BlueXP는 AWS에서 Cloud Volumes ONTAP에 새로운 애그리게이트를 만들 때, 시스템의 애그리게이트 수가 증가함에 따라 애그리게이트의 디스크 크기가 점차적으로 증가합니다. BlueXP는 이를 통해 AWS에서 허용하는 최대 데이터 디스크 수에 도달하기 전에 시스템의 최대 용량을 활용할 수 있습니다.

예를 들어, BlueXP는 다음과 같은 디스크 크기를 선택할 수 있습니다.

| 집계 번호 | 디스크 크기입니다 | 최대 애그리게이트 용량입니다 |
|-------|-----------|-----------------|
| 1     | 500GiB    | 3TiB            |
| 4     | 1TiB      | 6TiB            |
| 6     | 2TiB      | 12TiB           |



이 동작은 Amazon EBS Elastic Volumes 기능을 지원하는 애그리게이트에는 적용되지 않습니다. Elastic Volumes가 설정된 애그리게이트는 하나 또는 두 개의 RAID 그룹으로 구성됩니다. 각 RAID 그룹에는 동일한 용량을 가진 4개의 동일한 디스크가 있습니다. "[Elastic Volumes 지원에 대해 자세히 알아보십시오](#)".

고급 할당 옵션을 사용하여 디스크 크기를 직접 선택할 수 있습니다.

#### 고급 할당

BlueXP에서 집계를 관리하는 대신 직접 관리할 수 있습니다. "[고급 할당 \\* 페이지에서 선택합니다](#)" 특정 수의 디스크를 포함하는 새 애그리게이트를 생성하고, 기존 애그리게이트에 디스크를 추가하고, 특정 애그리게이트에서 볼륨을 생성할 수 있습니다.

#### 용량 관리

계정 관리자는 BlueXP에서 스토리지 용량 결정을 통지할지 아니면 BlueXP에서 자동으로 용량 요구 사항을 관리할지 여부를 선택할 수 있습니다.

이 동작은 커넥터의 `_용량 관리 모드`에 의해 결정됩니다. 용량 관리 모드는 해당 커넥터가 관리하는 모든 Cloud Volumes ONTAP 시스템에 영향을 줍니다. 다른 커넥터가 있는 경우 다르게 구성할 수 있습니다.

#### 자동 용량 관리

Capacity Management Mode(용량 관리 모드)는 기본적으로 Automatic(자동)으로 설정됩니다. 이 모드에서 BlueXP는 더 많은 용량이 필요할 때 Cloud Volumes ONTAP 인스턴스에 대해 새 디스크를 자동으로 구매하고, 사용되지 않는 디스크 컬렉션(애그리게이트)을 삭제하고, 필요할 때 애그리게이트 간에 볼륨을 이동하며, 디스크 장애를 제거합니다.

다음 예제에서는 이 모드가 작동하는 방식을 보여 줍니다.

- Aggregate가 용량 임계값에 도달하고 더 많은 디스크를 수용할 수 있는 공간이 있는 경우 BlueXP는 해당 aggregate에 대한 새 디스크를 자동으로 구매하여 볼륨이 계속 증가할 수 있도록 합니다.

BlueXP는 15분마다 사용 가능한 공간 비율을 확인하여 추가 디스크를 구입해야 하는지 확인합니다.

#### 를 누릅니다

AWS에서 Elastic Volumes를 지원하는 애그리게이트의 경우 BlueXP는 RAID 그룹의 디스크 크기도 증가합니다. "[Elastic Volumes 지원에 대해 자세히 알아보십시오](#)".

- aggregate가 용량 임계값에 도달하고 추가 디스크를 지원할 수 없는 경우, BlueXP는 자동으로 볼륨을 해당 aggregate에서 가용 용량을 가진 aggregate 또는 새로운 aggregate로 이동합니다.

BlueXP에서 볼륨에 대한 새 애그리게이트를 생성할 경우 해당 볼륨의 크기에 맞는 디스크 크기를 선택합니다.

이제 원래 aggregate에서 여유 공간을 사용할 수 있습니다. 기존 볼륨 또는 새 볼륨에서 해당 공간을 사용할 수 있습니다. 이 시나리오에서는 공간을 클라우드 프로저더(cloud provider)로 반환할 수 없습니다.

- Aggregate에 12시간 이상 볼륨이 없는 경우 BlueXP에서 해당 볼륨을 삭제합니다.

## 자동 용량 관리를 통한 LUN 관리

BlueXP의 자동 용량 관리는 LUN에 적용되지 않습니다. BlueXP에서 LUN을 생성하면 자동 확장 기능이 비활성화됩니다.

### 수동 용량 관리

계정 관리자가 용량 관리 모드를 수동으로 설정한 경우 용량 결정을 내려야 할 때 BlueXP에 작업 필요 메시지가 표시됩니다. 자동 모드에서 설명한 것과 동일한 예가 수동 모드에 적용되지만 사용자는 이 작업을 수락할 수 있습니다.

### 자세한 정보

["용량 관리 모드를 수정하는 방법을 알아보십시오"](#).

## 쓰기 속도

BlueXP를 사용하면 대부분의 Cloud Volumes ONTAP 구성에서 일반 또는 고속 쓰기 속도를 선택할 수 있습니다. 쓰기 속도를 선택하기 전에 고속 쓰기 속도를 사용할 때 정상 및 높음 설정의 차이점과 위험 및 권장 사항을 이해해야 합니다.

### 정상적인 쓰기 속도

일반적인 쓰기 속도를 선택하면 데이터가 디스크에 직접 기록됩니다. 데이터를 디스크에 직접 쓸 경우 계획되지 않은 시스템 중단 시 데이터 손실 가능성 또는 계획되지 않은 시스템 중단 시 계단식 오류 발생 가능성(HA 쌍만 해당)을 줄입니다.

기본 옵션은 일반 쓰기 속도입니다.

### 빠른 쓰기 속도

빠른 쓰기 속도를 선택하면 데이터가 디스크에 쓰기 전에 메모리에 버퍼링되어 쓰기 성능이 향상됩니다. 이 캐싱으로 인해 계획되지 않은 시스템 중단이 발생할 경우 데이터 손실이 발생할 수 있습니다.

계획되지 않은 시스템 중단 시 손실될 수 있는 데이터 양은 마지막 두 정합성 보장 지점의 스패입니다. 정합성 보장 지점은 버퍼링된 데이터를 디스크에 쓰는 작업을 가리킵니다. 정합성 보장 지점은 쓰기 로그가 꽉 찼거나 10초 후에(둘 중 먼저 도래하는 시점)에 발생합니다. 그러나 클라우드 공급자가 제공하는 스토리지의 성능은 정합성 보장 지점 처리 시간에 영향을 줄 수 있습니다.

### 빠른 쓰기 속도 사용 시기

빠른 쓰기 성능이 워크로드에 필요한 경우, 계획되지 않은 시스템 중단 시 데이터 손실 위험이나 계획되지 않은 시스템 중단 시 계단식 장애(HA 쌍만 해당)를 견딜 수 있는 경우, 빠른 쓰기 속도가 가장 좋습니다.

### 빠른 쓰기 속도 사용 시 권장 사항

빠른 쓰기 속도를 사용하는 경우 응용 프로그램 계층에서 쓰기 보호를 수행하거나 데이터 손실이 발생할 경우 응용 프로그램이 데이터 손실을 허용할 수 있는지 확인해야 합니다.

## AWS의 HA 쌍을 통한 빠른 쓰기 속도

AWS의 HA 쌍에서 고속 쓰기 속도를 사용하려는 경우 AZ(다중 가용성 영역) 구축과 AZ 단일 구축 간의 보호 수준 차이를 이해해야 합니다. 여러 AZs에 HA 쌍을 구축하면 더 뛰어난 복원력을 제공할 뿐만 아니라 데이터 손실 가능성을 줄일 수 있습니다.

["AWS의 HA 쌍에 대해 자세히 알아보십시오"](#).

빠른 쓰기 속도를 지원하는 구성

모든 Cloud Volumes ONTAP 구성에서 고속 쓰기 속도를 지원하는 것은 아닙니다. 이러한 구성은 기본적으로 일반 쓰기 속도를 사용합니다.

설치하고

단일 노드 시스템을 사용하는 경우 Cloud Volumes ONTAP는 모든 인스턴스 유형에서 빠른 쓰기 속도를 지원합니다.

9.8 릴리즈부터 Cloud Volumes ONTAP는 지원되는 EC2 인스턴스 유형 중 M5.xLarge 및 R5.xLarge를 제외한 거의 모든 유형을 사용할 때 HA 쌍을 포함한 고속 쓰기 속도를 지원합니다.

["Cloud Volumes ONTAP가 지원하는 Amazon EC2 인스턴스에 대해 자세히 알아보십시오"](#).

**Azure**를 지원합니다

단일 노드 시스템을 사용하는 경우 Cloud Volumes ONTAP는 모든 VM 유형에 대해 고속 쓰기 속도를 지원합니다.

HA 쌍을 사용하는 경우 Cloud Volumes ONTAP는 9.8 릴리즈부터 시작하여 여러 VM 유형에서 높은 쓰기 속도를 지원합니다. 로 이동합니다 ["Cloud Volumes ONTAP 릴리즈 노트"](#) 고속 쓰기 속도를 지원하는 VM 유형을 확인합니다.

**Google** 클라우드

단일 노드 시스템을 사용하는 경우 Cloud Volumes ONTAP는 모든 시스템 유형에 대해 고속 쓰기 속도를 지원합니다.

HA 쌍을 사용하는 경우 Cloud Volumes ONTAP는 9.13.0 릴리즈부터 시작하여 여러 VM 유형에서 높은 쓰기 속도를 지원합니다. 로 이동합니다 ["Cloud Volumes ONTAP 릴리즈 노트"](#) 고속 쓰기 속도를 지원하는 VM 유형을 확인합니다.

["Cloud Volumes ONTAP가 지원하는 Google 클라우드 머신 유형에 대해 자세히 알아보십시오"](#).

쓰기 속도를 선택하는 방법

새 작업 환경을 만들 때 쓰기 속도를 선택할 수 있으며, 이 경우 쓰기 속도를 선택할 수 있습니다 ["기존 시스템의 쓰기 속도를 변경합니다"](#).

데이터 손실이 발생할 경우 예상되는 상황

빠른 쓰기 속도로 인해 데이터가 손실되면 EMS(Event Management System)에서 다음 두 이벤트를 보고합니다.

- Cloud Volumes ONTAP 9.12.1 이상

```
NOTICE nv.data.loss.possible: An unexpected shutdown occurred while in
high write speed mode, which possibly caused a loss of data.
* Cloud Volumes ONTAP 9.11.0에서 9.11.1까지
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown with High Write Speed mode"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect..
* Cloud Volumes ONTAP 9.8 ~ 9.10.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect.
```

이 경우 Cloud Volumes ONTAP는 사용자 개입 없이 부팅하여 데이터를 계속 제공할 수 있어야 합니다.

데이터 손실이 발생할 경우 데이터 액세스를 중지하는 방법

데이터 손실이 걱정되고 데이터 손실 문제가 적절하게 해결되면 애플리케이션 실행이 중지되고 데이터 액세스가 재개되기를 원할 경우 CLI의 NVFAIL 옵션을 사용하여 해당 목표를 달성할 수 있습니다.

**NVFAIL** 옵션을 활성화합니다

```
vol modify -volume <vol-name> -nvfail on
```

**NVFAIL** 설정을 확인합니다

```
vol show -volume <vol-name> -fields nvfail
```

**NVFAIL** 옵션을 비활성화합니다

```
vol modify -volume <vol-name> -nvfail off
```

데이터 손실이 발생하면 NVFAIL을 사용하는 NFS 또는 iSCSI 볼륨에서 데이터 서비스를 중지해야 합니다(상태 비저장 프로토콜인 CIFS에는 영향을 주지 않음). 자세한 내용은 [을 참조하십시오 "NVFAIL이 NFS 볼륨 또는 LUN에 대한 액세스에 미치는 영향"](#).

**NVFAIL** 상태를 확인합니다

```
vol show -fields in-nvfailed-state
```



데이터 손실 문제가 적절하게 해결된 후에는 NVFAIL 상태를 지울 수 있으며 데이터 액세스를 위해 볼륨을 사용할 수 있습니다.

**NVFAIL** 상태를 지우려면

```
vol modify -volume <vol-name> -in-nvfailed-state false
```

## Flash Cache를 참조하십시오

일부 Cloud Volumes ONTAP 구성에는 성능을 높이기 위해 Cloud Volumes ONTAP이 `_Flash Cache_`로 사용하는 로컬 NVMe 스토리지가 포함됩니다. 토큰 업데이트 테스트를 위한 행을 추가하는 중입니다.

**Flash Cache**란 무엇입니까?

Flash Cache는 최근에 읽은 사용자 데이터와 NetApp 메타데이터의 실시간 지능형 캐싱을 통해 데이터 액세스 속도를 높입니다. 데이터베이스, 이메일, 파일 서비스를 비롯한 랜덤 읽기 집약적인 워크로드에 효과적입니다.

지원되는 구성

Flash Cache는 특정 Cloud Volumes ONTAP 구성에서 지원됩니다. 에서 지원되는 구성을 보십시오 ["Cloud Volumes ONTAP 릴리즈 노트"](#)

제한 사항

- Cloud Volumes ONTAP 9.12.0까지 Flash Cache 성능 향상을 활용하려면 모든 볼륨에서 압축을 해제해야 합니다. Cloud Volumes ONTAP 9.12.1을 배포하거나 업그레이드할 때 압축을 비활성화할 필요가 없습니다.  
  
BlueXP에서 볼륨을 생성할 때 스토리지 효율성 없음 을 선택하거나 볼륨을 생성한 후 를 선택합니다 ["CLI를 사용하여 데이터 압축을 비활성화합니다"](#).
- 재부팅 후 캐시 재가기는 Cloud Volumes ONTAP에서 지원되지 않습니다.

## WORM 스토리지

Cloud Volumes ONTAP 시스템에서 WORM(Write Once, Read Many) 스토리지를 활성화하여 지정된 보존 기간 동안 수정되지 않은 형식으로 파일을 보존할 수 있습니다. 클라우드 WORM 스토리지는 SnapLock 기술을 기반으로 하며, 이는 WORM 파일이 파일 레벨에서 보호됨을 의미합니다.

**WORM** 스토리지의 작동 방식

파일이 WORM 스토리지에 커밋되면 보존 기간이 만료된 후에도 수정할 수 없습니다. 변조 방지 시계는 WORM 파일의 보존 기간이 경과된 시점을 결정합니다.

보존 기간이 경과한 후에는 더 이상 필요하지 않은 파일을 삭제해야 합니다.

총전 중

WORM 볼륨의 총 프로비저닝 용량에 따라 WORM 스토리지에 대한 총전이 매시간 가능합니다.

PAYGO 또는 연간 약정 조건에서만 사용할 수 있으며, WORM용 라이선스는 클라우드 공급자 마켓플레이스를 통해 구입할 수 있습니다. WORM은 노드 기반 및 용량 기반 라이선스 모델을 모두 지원합니다.



Cloud Volumes ONTAP에서 WORM 스토리지에 BYOL 라이선스를 사용할 수 없음

Cloud Volumes ONTAP 9.10.1 이상에서는 다음과 같은 충전 동작을 이해해야 합니다.

- ONTAP 9.10.1.1부터 WORM 볼륨과 비 WORM 볼륨이 동일한 애그리게이트에 존재할 수 있습니다.
- Cloud Volumes ONTAP 작업 환경을 생성할 때 WORM을 활성화하면 BlueXP에서 생성한 모든 볼륨에서 WORM이 활성화됩니다. 그러나 ONTAP CLI 또는 System Manager를 사용하여 WORM이 비활성화된 볼륨을 생성할 수 있습니다. 이러한 볼륨은 WORM 속도로 충전되지 않습니다.
- 작업 환경을 생성할 때 WORM을 활성화하지 않으면 BlueXP에서 생성한 모든 볼륨에서 WORM이 비활성화됩니다. 해당 볼륨에 대해 WORM 속도로 충전되지 않습니다.

["WORM 스토리지 가격에 대해 자세히 알아보십시오"](#)

**WORM** 스토리지를 활성화하는 중입니다

WORM 스토리지의 활성화 방법은 사용 중인 Cloud Volumes ONTAP 버전에 따라 다릅니다.

버전 **9.10.1** 이상

Cloud Volumes ONTAP 9.10.1부터 볼륨 레벨에서 WORM을 활성화 또는 비활성화할 수 있습니다.

새 Cloud Volumes ONTAP 작업 환경을 생성할 때 WORM 스토리지를 설정하거나 해제하라는 메시지가 표시됩니다.

- 작업 환경을 생성할 때 WORM 스토리지를 활성화하면 BlueXP에서 생성한 모든 볼륨에서 WORM이 활성화됩니다. 그러나 System Manager 또는 CLI를 사용하여 WORM을 사용하지 않는 볼륨을 생성할 수 있습니다.
- 작업 환경을 생성할 때 WORM 스토리지를 비활성화하면 BlueXP, System Manager 또는 CLI에서 생성한 모든 볼륨에서 WORM 스토리지가 비활성화됩니다. 생성 중 활성화되지 않은 Cloud Volumes ONTAP 작업 환경에서 WORM을 활성화하려면 NetApp 지원 부서의 지원 티켓을 생성해야 합니다.

두 가지 옵션 중 하나를 사용할 경우 가능합니다 [충전 작동 방식을 이해합니다](#).

버전 **9.10.0** 이하

새로운 작업 환경을 생성할 때 Cloud Volumes ONTAP 시스템에서 WORM 스토리지를 활성화할 수 있습니다. BlueXP에서 생성한 모든 볼륨에서 WORM이 활성화되어 있습니다. 개별 볼륨에서 WORM 스토리지를 비활성화할 수 없습니다.

**WORM**에 파일 커밋 중

애플리케이션을 사용하여 NFS 또는 CIFS를 통해 WORM에 파일을 커밋하거나 ONTAP CLI를 사용하여 파일을 WORM에 자동으로 커밋할 수 있습니다. 또한 WORM 추가 가능 파일을 사용하여 로그 정보와 같이 점증적으로 기록된 데이터를 보존할 수 있습니다.

Cloud Volumes ONTAP 시스템에서 WORM 스토리지를 활성화한 후에는 모든 WORM 스토리지 관리에 ONTAP CLI를 사용해야 합니다. 자세한 지침은 [참조하십시오 "ONTAP 설명서"](#).

## WORM 파일을 삭제하는 중입니다

보존 기간 동안 권한이 있는 삭제 기능을 사용하여 WORM 파일을 삭제할 수 있습니다.

자세한 지침은 을 참조하십시오 "[ONTAP 설명서](#)"

## WORM 및 데이터 계층화

새로운 Cloud Volumes ONTAP 9.8 시스템 이상을 생성할 때 데이터 계층화와 WORM 스토리지를 함께 사용할 수 있습니다. WORM 스토리지를 통한 데이터 계층화를 사용하면 데이터를 클라우드의 오브젝트 저장소에 계층화할 수 있습니다.

데이터 계층화와 WORM 스토리지 모두에 대한 설정 방법은 다음과 같습니다.

- 오브젝트 스토리지로 계층화되어 있는 데이터에는 ONTAP WORM 기능이 포함되지 않습니다. 엔드 투 엔드 WORM 기능을 보장하려면 버킷 권한을 올바르게 설정해야 합니다.
- 오브젝트 스토리지로 계층화된 데이터에는 WORM 기능이 없습니다. 즉, 기술적으로 버킷 및 컨테이너에 대한 모든 액세스 권한이 있는 사람은 ONTAP에 의해 계층화된 오브젝트를 이동 및 삭제할 수 있습니다.
- WORM 및 계층화를 활성화한 후에는 Cloud Volumes ONTAP 9.8로의 되돌리기 또는 다운그레이드가 차단됩니다.

## 제한 사항

- Cloud Volumes ONTAP의 WORM 스토리지는 "신뢰할 수 있는 스토리지 관리자" 모델로 운영됩니다. WORM 파일은 변경 또는 수정으로부터 보호되지만, 만료되지 않은 WORM 데이터가 포함된 볼륨에도 클러스터 관리자가 볼륨을 삭제할 수 있습니다.
- 신뢰할 수 있는 스토리지 관리자 모델 외에도 Cloud Volumes ONTAP의 WORM 스토리지는 "신뢰할 수 있는 클라우드 관리자" 모델에서도 암시적으로 작동합니다. 클라우드 관리자는 클라우드 공급자에서 직접 클라우드 스토리지를 제거 또는 편집하여 만료 날짜 이전에 WORM 데이터를 삭제할 수 있습니다.

# 고가용성 쌍

## AWS의 고가용성 쌍

Cloud Volumes ONTAP HA(고가용성) 구성은 무중단 운영 및 내결함성을 제공합니다. AWS에서는 데이터가 두 노드 간에 동기식으로 미러링됩니다.

### HA 구성 요소

AWS에서 Cloud Volumes ONTAP HA 구성에는 다음과 같은 구성요소가 포함됩니다.

- 데이터가 서로 동기식으로 미러링되는 2개의 Cloud Volumes ONTAP 노드
- 스토리지 테이크오버 및 반환 프로세스를 지원하는 노드 간 통신 채널을 제공하는 중재자 인스턴스

### 중재자

다음은 AWS의 중재자 인스턴스에 대한 몇 가지 주요 정보입니다.

## 인스턴스 유형

T2-마이크로

## 디스크

약 8GiB의 EBS 마그네틱 디스크 1개

## 운영 체제

데비안 11



Cloud Volumes ONTAP 9.10.0 이전 버전에서는 데비안 10이 중재자위에 설치되었습니다.

## 업그레이드

Cloud Volumes ONTAP를 업그레이드할 때 BlueXP는 필요에 따라 중재자 인스턴스도 업데이트합니다.

## 인스턴스에 대한 액세스

BlueXP에서 Cloud Volumes ONTAP HA 쌍을 만들면 중재자 인스턴스에 대한 키 쌍을 제공하라는 메시지가 표시됩니다. 를 사용하여 SSH 액세스에 이 키 쌍을 사용할 수 있습니다 admin 사용자.

## 제3자 에이전트

타사 에이전트 또는 VM 확장은 중재자 인스턴스에서 지원되지 않습니다.

## 스토리지 테이크오버 및 반환

노드가 중단되면 다른 노드가 파트너에게 데이터를 제공하여 지속적인 데이터 서비스를 제공할 수 있습니다. 데이터는 파트너에게 동기식으로 미러링되므로 클라이언트가 파트너 노드에서 동일한 데이터에 액세스할 수 있습니다.

노드가 재부팅된 후 파트너가 스토리지를 반환하기 전에 데이터를 다시 동기화해야 합니다. 데이터를 재동기화하는 데 걸리는 시간은 노드가 다운된 동안 변경된 데이터의 양에 따라 달라집니다.

스토리지 테이크오버, 재동기화 및 반환은 기본적으로 모두 자동으로 수행됩니다. 사용자 작업이 필요하지 않습니다.

## RPO 및 RTO

HA 구성을 사용하면 다음과 같이 데이터의 고가용성을 유지할 수 있습니다.

- 복구 지점 목표(RPO)는 0초입니다.  
데이터는 데이터 손실 없이 트랜잭션 측면에서 일관적입니다.
- 복구 시간 목표(RTO)는 120초이다.  
정전이 발생할 경우 120초 이내에 데이터를 사용할 수 있어야 합니다.

## HA 구축 모델

여러 AZs(Availability Zone) 또는 단일 AZ에 HA 구성을 배포하여 데이터의 고가용성을 보장할 수 있습니다. 각 구성에 대한 자세한 내용을 검토하여 요구 사항에 가장 적합한 구성을 선택해야 합니다.

## 여러 가용성 영역

AZ(Multiple Availability Zones)에 HA 구성을 구축하면 AZ 또는 Cloud Volumes ONTAP 노드를 실행하는 인스턴스에서 장애가 발생할 경우 데이터의 고가용성을 보장할 수 있습니다. NAS IP 주소가 데이터 액세스 및 스토리지

페일오버에 미치는 영향을 이해해야 합니다.

## NFS 및 CIFS 데이터 액세스

HA 구성이 여러 가용성 영역 간에 분산되면 `_floating IP addresses_enable` NAS 클라이언트 액세스를 사용합니다. 해당 지역의 모든 VPC에 대한 CIDR 블록 외부에 있어야 하는 부동 IP 주소는 장애가 발생할 경우 노드 간에 마이그레이션할 수 있습니다. 고객이 아닌 한 VPC 외부에 있는 클라이언트에서 기본적으로 액세스할 수 없습니다. ["AWS 전송 게이트웨이를 설정합니다"](#).

전송 게이트웨이를 설정할 수 없는 경우 VPC 외부에 있는 NAS 클라이언트에서 전용 IP 주소를 사용할 수 있습니다. 그러나 이러한 IP 주소는 정적이며 노드 간에 페일오버할 수 없습니다.

여러 가용성 영역에 HA 구성을 배포하기 전에 부동 IP 주소 및 라우팅 테이블에 대한 요구 사항을 검토해야 합니다. 구성을 배포할 때 부동 IP 주소를 지정해야 합니다. BlueXP에서 개인 IP 주소를 자동으로 생성합니다.

자세한 내용은 을 참조하십시오 ["여러 AZs에서 Cloud Volumes ONTAP HA를 위한 AWS 네트워킹 요구사항"](#).

## iSCSI 데이터 액세스

iSCSI는 부동 IP 주소를 사용하지 않으므로 Cross-VPC 데이터 통신은 문제가 되지 않습니다.

### iSCSI의 테이크오버 및 반환

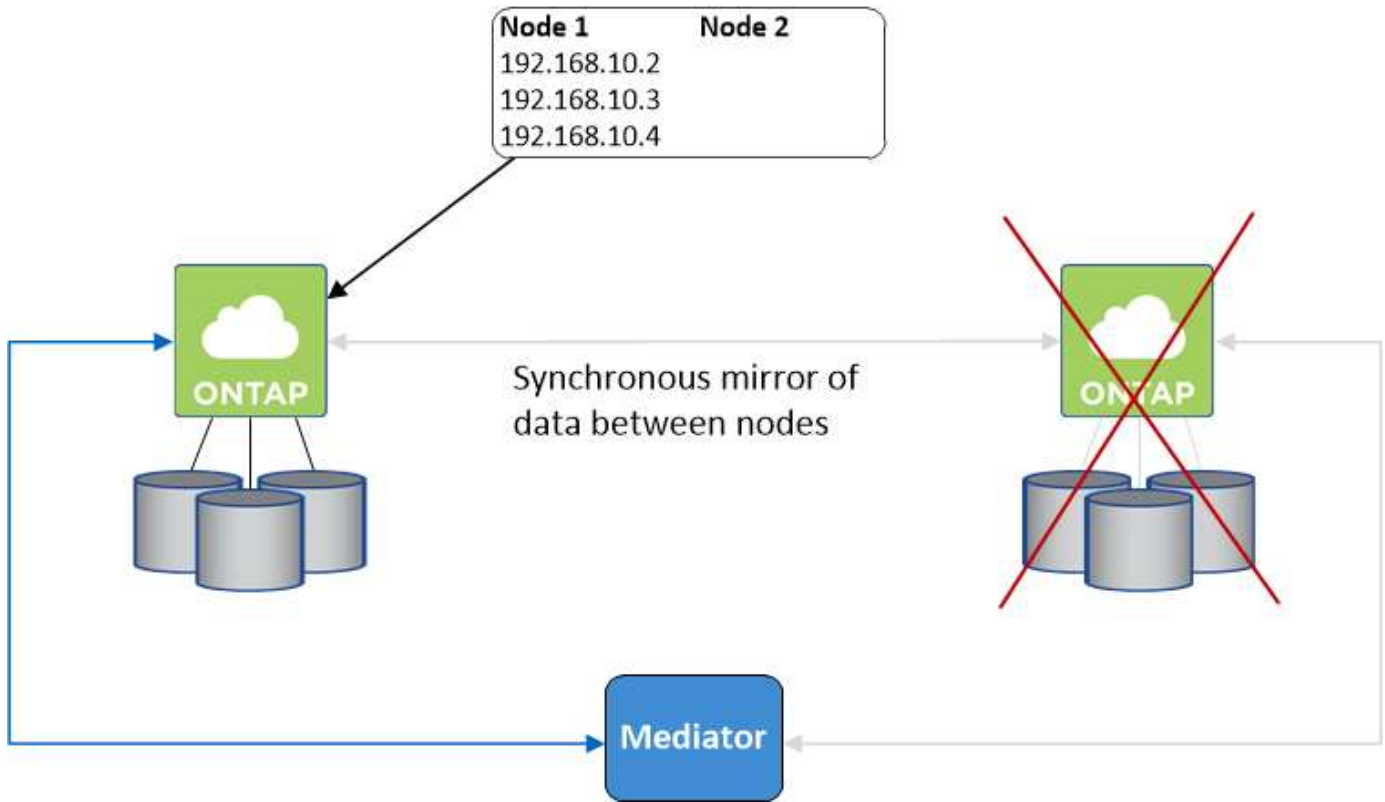
iSCSI의 경우 Cloud Volumes ONTAP는 다중 경로 I/O(MPIO) 및 ALUA(Asymmetric Logical Unit Access)를 사용하여 능동 최적화 경로와 최적화되지 않은 경로 간의 경로 페일오버를 관리합니다.



ALUA를 지원하는 특정 호스트 구성에 대한 자세한 내용은 를 참조하십시오 ["NetApp 상호 운용성 매트릭스 툴"](#) 및 호스트 운영 체제용 Host Utilities 설치 및 설정 설명서를 참조하십시오.

### NAS의 테이크오버 및 반환

유동 IP를 사용하는 NAS 구성에서 테이크오버가 발생하면 클라이언트가 데이터에 액세스하는 데 사용하는 노드의 부동 IP 주소가 다른 노드로 이동합니다. 다음 이미지는 유동 IP를 사용하는 NAS 구성의 스토리지 테이크오버를 보여 줍니다. 노드 2가 다운되면 노드 2의 부동 IP 주소가 노드 1로 이동합니다.



외부 VPC 액세스에 사용되는 NAS 데이터 IP는 장애가 발생할 경우 노드 간에 마이그레이션할 수 없습니다. 노드가 오프라인이 되면 다른 노드의 IP 주소를 사용하여 VPC 외부의 클라이언트에 볼륨을 수동으로 다시 마운트해야 합니다.

장애가 발생한 노드가 다시 온라인 상태가 되면 원래 IP 주소를 사용하여 클라이언트를 볼륨에 다시 마운트합니다. 이 단계는 두 HA 노드 간에 불필요한 데이터를 전송하지 않아야 하므로 성능에 중대한 영향을 미칠 수 있습니다.

볼륨을 선택하고 \* 탑재 명령 \* 을 클릭하여 BlueXP에서 올바른 IP 주소를 쉽게 식별할 수 있습니다.

#### 단일 가용성 영역

AZ(단일 가용성 영역)에 HA 구성을 구축하면 Cloud Volumes ONTAP 노드를 실행하는 인스턴스에 장애가 발생할 경우 데이터의 고가용성을 보장할 수 있습니다. 모든 데이터는 VPC 외부에서 기본적으로 액세스할 수 있습니다.

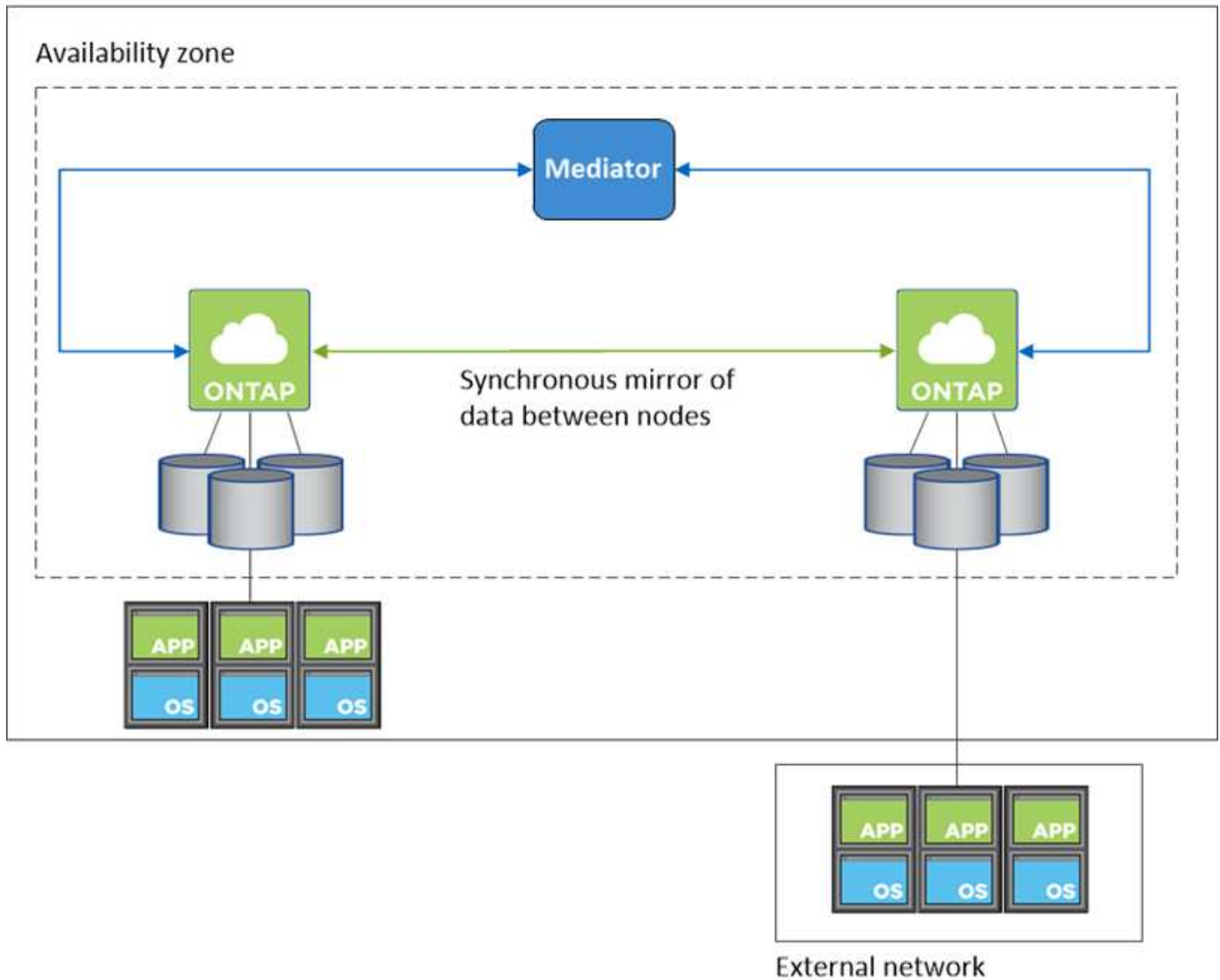


BlueXP는 을 생성합니다 **"AWS 배치 그룹 분산"** 그런 다음 해당 배치 그룹에서 2개의 HA 노드를 시작합니다. 배치 그룹은 서로 다른 기본 하드웨어에 인스턴스를 분산하여 동시 오류 위험을 줄입니다. 이 기능은 디스크 장애 관점이 아니라 컴퓨팅 측면에서 중복성을 향상시킵니다.

#### 데이터 액세스

이 구성은 단일 AZ에 있으므로 부동 IP 주소가 필요하지 않습니다. VPC 내부 및 VPC 외부에서 동일한 IP 주소를 사용하여 데이터에 액세스할 수 있습니다.

다음 이미지는 단일 AZ의 HA 구성을 보여줍니다. VPC 내부 및 VPC 외부에서 데이터에 액세스할 수 있습니다.



### 테이크오버 및 반환

iSCSI의 경우 Cloud Volumes ONTAP는 다중 경로 I/O(MPIO) 및 ALUA(Asymmetric Logical Unit Access)를 사용하여 능동 최적화 경로와 최적화되지 않은 경로 간의 경로 페일오버를 관리합니다.



ALUA를 지원하는 특정 호스트 구성에 대한 자세한 내용은 ["NetApp 상호 운용성 매트릭스 툴"](#) 및 호스트 운영 체제용 Host Utilities 설치 및 설정 설명서를 참조하십시오.

NAS 구성의 경우 장애가 발생할 경우 데이터 IP 주소를 HA 노드 간에 마이그레이션할 수 있습니다. 이렇게 하면 클라이언트가 스토리지에 액세스할 수 있습니다.

### HA Pair의 스토리지 작동 방식

ONTAP 클러스터와 달리 Cloud Volumes ONTAP HA 쌍의 스토리지는 노드 간에 공유되지 않습니다. 대신 데이터가 노드 간에 동기식으로 미러링되므로 장애 발생 시 데이터를 사용할 수 있습니다.

## 스토리지 할당

새 볼륨을 생성하고 추가 디스크가 필요한 경우 BlueXP는 두 노드에 동일한 수의 디스크를 할당하고 미러링된 애그리게이트를 생성한 다음 새 볼륨을 생성합니다. 예를 들어, 볼륨에 두 개의 디스크가 필요한 경우 BlueXP는 노드당 두 개의 디스크를 총 4개의 디스크에 할당합니다.

## 구성의 스토리지

HA 쌍을 액티브-액티브 구성으로 사용할 수 있으며, 이 구성에서는 두 노드가 클라이언트에 데이터를 제공합니다. 또는 액티브-패시브 구성으로 사용할 수 있습니다. 패시브 노드는 액티브 노드의 스토리지를 인계한 경우에만 데이터 요청에 응답합니다.



스토리지 시스템 보기에서 BlueXP를 사용하는 경우에만 활성-활성 구성을 설정할 수 있습니다.

## 성능 기대치

Cloud Volumes ONTAP HA 구성은 노드 간에 데이터를 동기식으로 복제하여 네트워크 대역폭을 사용합니다. 따라서 단일 노드 Cloud Volumes ONTAP 구성과 비교하여 다음과 같은 성능을 기대할 수 있습니다.

- 한 노드의 데이터만 제공하는 HA 구성의 경우 읽기 성능은 단일 노드 구성의 읽기 성능과 비슷하며 쓰기 성능은 낮습니다.
- 두 노드의 데이터를 제공하는 HA 구성의 경우 읽기 성능은 단일 노드 구성의 읽기 성능보다 높고 쓰기 성능은 동일하거나 더 높습니다.

Cloud Volumes ONTAP 성능에 대한 자세한 내용은 [클라우드 볼륨 성능](#)을 참조하십시오 "성능".

## 스토리지에 대한 클라이언트 액세스

클라이언트는 볼륨이 상주하는 노드의 데이터 IP 주소를 사용하여 NFS 및 CIFS 볼륨을 액세스해야 합니다. NAS 클라이언트가 파트너 노드의 IP 주소를 사용하여 볼륨에 액세스하는 경우 트래픽이 두 노드 간에 이동하므로 성능이 저하됩니다.



HA 쌍에서 노드 간에 볼륨을 이동하는 경우 다른 노드의 IP 주소를 사용하여 볼륨을 다시 마운트해야 합니다. 그렇지 않으면 성능이 저하될 수 있습니다. 클라이언트가 CIFS에 대한 NFSv4 참조 또는 폴더 리디렉션 지원을 지원하는 경우 Cloud Volumes ONTAP 시스템에서 이러한 기능을 설정하여 볼륨을 다시 마운트하지 않도록 할 수 있습니다. 자세한 내용은 ONTAP 설명서를 참조하십시오.

BlueXP의 볼륨 관리 패널에서 *Mount Command* 옵션을 통해 올바른 IP 주소를 쉽게 식별할 수 있습니다.



## Volume Actions

---

View volume details

Mount command

Clone volume

Edit volume tags

Edit volume settings

Delete volume

## Protection Actions

---

## Advanced Actions

---

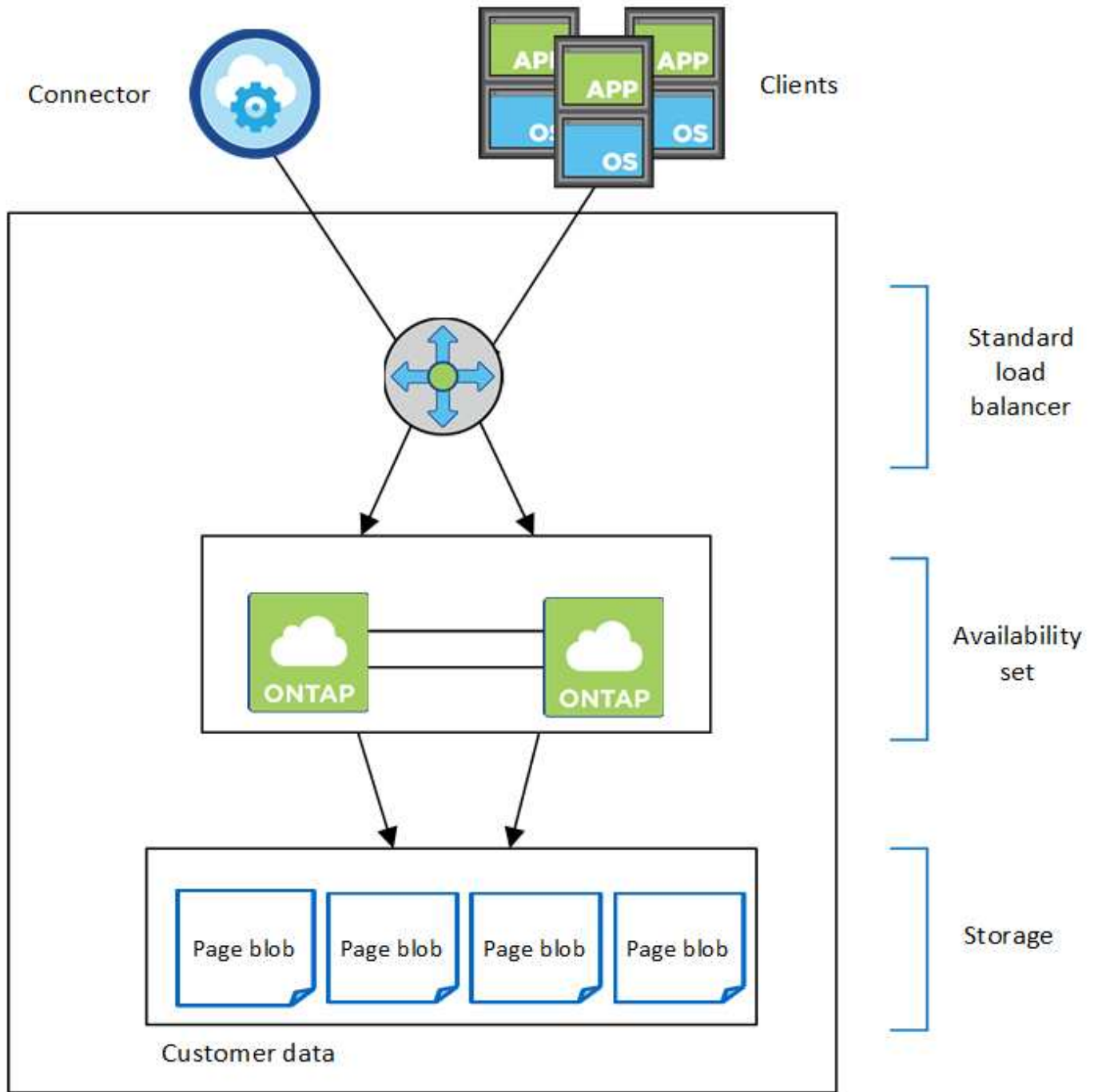
### Azure의 고가용성 쌍

Cloud Volumes ONTAP HA(고가용성) 쌍은 클라우드 환경에서 장애가 발생할 경우 엔터프라이즈급 안정성과 지속적인 운영을 제공합니다. Azure에서 스토리지는 두 노드 간에 공유됩니다.

### HA 구성 요소

페이지 Blob을 사용한 HA 단일 가용성 영역 구성

Azure의 Cloud Volumes ONTAP HA 페이지 BLOB 구성에는 다음과 같은 구성요소가 포함됩니다.



Resource group

BlueXP가 배포하는 Azure 구성 요소에 대한 다음 사항에 유의하십시오.

**Azure** 표준 로드 밸런서

로드 밸런서는 Cloud Volumes ONTAP HA 쌍에 대한 들어오는 트래픽을 관리합니다.

## 가용성 설정

Azure 가용성 집합은 Cloud Volumes ONTAP 노드의 논리적 그룹입니다. Availability Set는 노드가 서로 다른 장애 상태를 유지하도록 하고 도메인을 업데이트하여 이중화 및 가용성을 제공합니다. "[Azure 문서의 가용성 집합에 대해 자세히 알아보십시오](#)".

## 디스크

고객 데이터는 프리미엄 스토리지 페이지 Blob에 있습니다. 각 노드는 다른 노드의 스토리지에 액세스할 수 있습니다. 의 경우 추가 스토리지도 필요합니다 "[부팅, 루트 및 코어 데이터](#)".

## 스토리지 계정

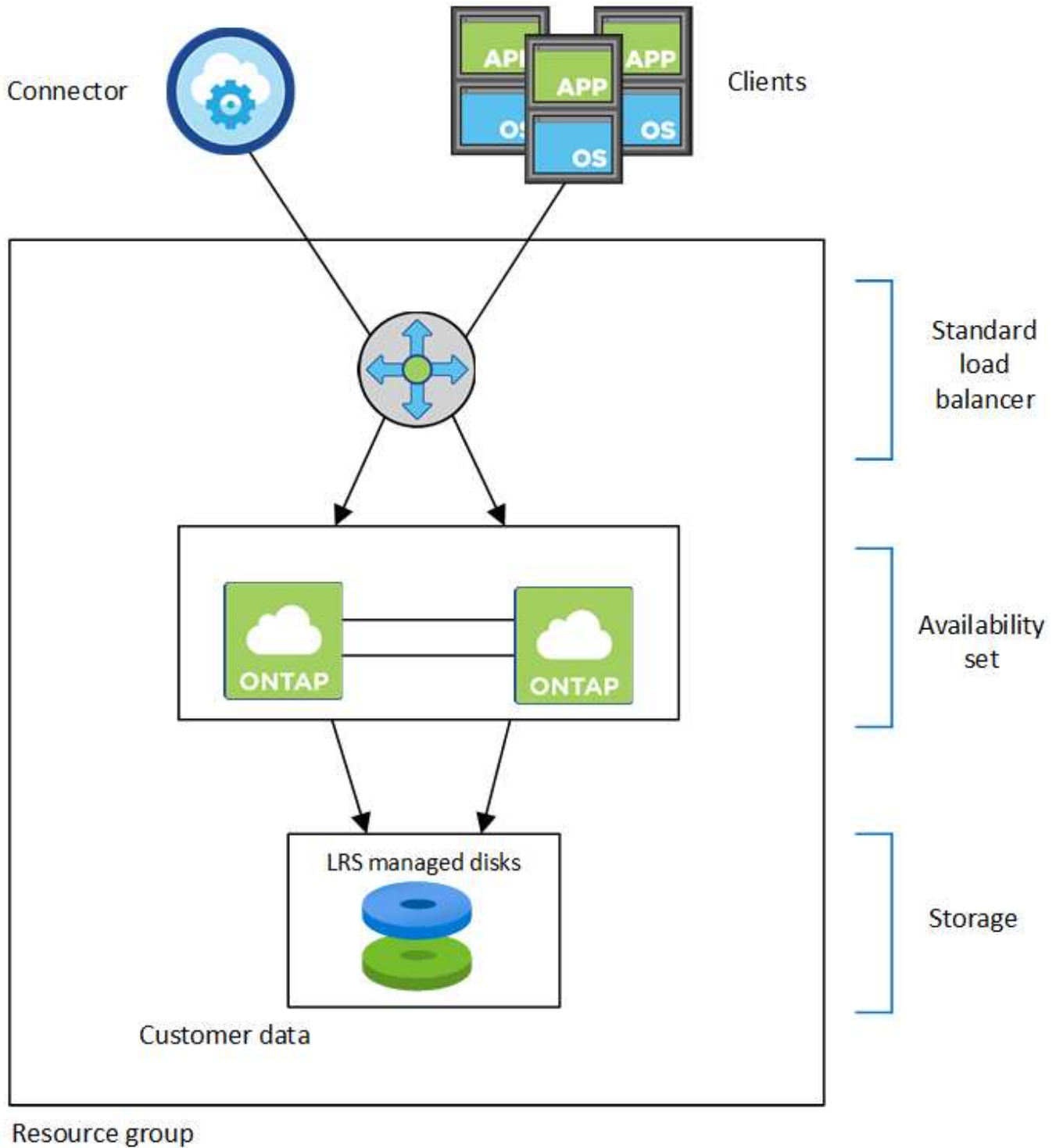
- 관리되는 디스크에는 하나의 스토리지 계정이 필요합니다.
- 스토리지 계정당 디스크 용량 제한에 도달했으므로 프리미엄 스토리지 페이지 Blob에 하나 이상의 스토리지 계정이 필요합니다.

"[Azure 문서: 스토리지 계정의 Azure 스토리지 확장성 및 성능 목표](#)".

- Azure Blob 저장소에 데이터를 계층화하려면 하나의 스토리지 계정이 필요합니다.
- Cloud Volumes ONTAP 9.7부터 BlueXP가 HA 쌍에 대해 생성하는 스토리지 계정은 범용 v2 스토리지 계정입니다.
- 작업 환경을 생성할 때 Cloud Volumes ONTAP 9.7 HA 쌍에서 Azure 스토리지 계정으로 HTTPS 연결을 설정할 수 있습니다. 이 옵션을 설정하면 쓰기 성능에 영향을 줄 수 있습니다. 작업 환경을 만든 후에는 설정을 변경할 수 없습니다.

## 공유 관리 디스크를 사용하는 HA 단일 가용성 영역 구성

공유 관리 디스크를 기반으로 실행되는 Cloud Volumes ONTAP HA 단일 가용성 영역 구성에는 다음과 같은 구성요소가 포함됩니다.



BlueXP가 배포하는 Azure 구성 요소에 대한 다음 사항에 유의하십시오.

#### Azure 표준 로드 밸런서

로드 밸런서는 Cloud Volumes ONTAP HA 쌍에 대한 들어오는 트래픽을 관리합니다.

#### 가용성 설정

Azure 가용성 집합은 Cloud Volumes ONTAP 노드의 논리적 그룹입니다. Availability Set은 노드가 서로 다른 장애 상태를 유지하도록 하고 도메인을 업데이트하여 이중화 및 가용성을 제공합니다. ["Azure 문서의 가용성 집합에 대해 자세히 알아보십시오"](#).

## 디스크

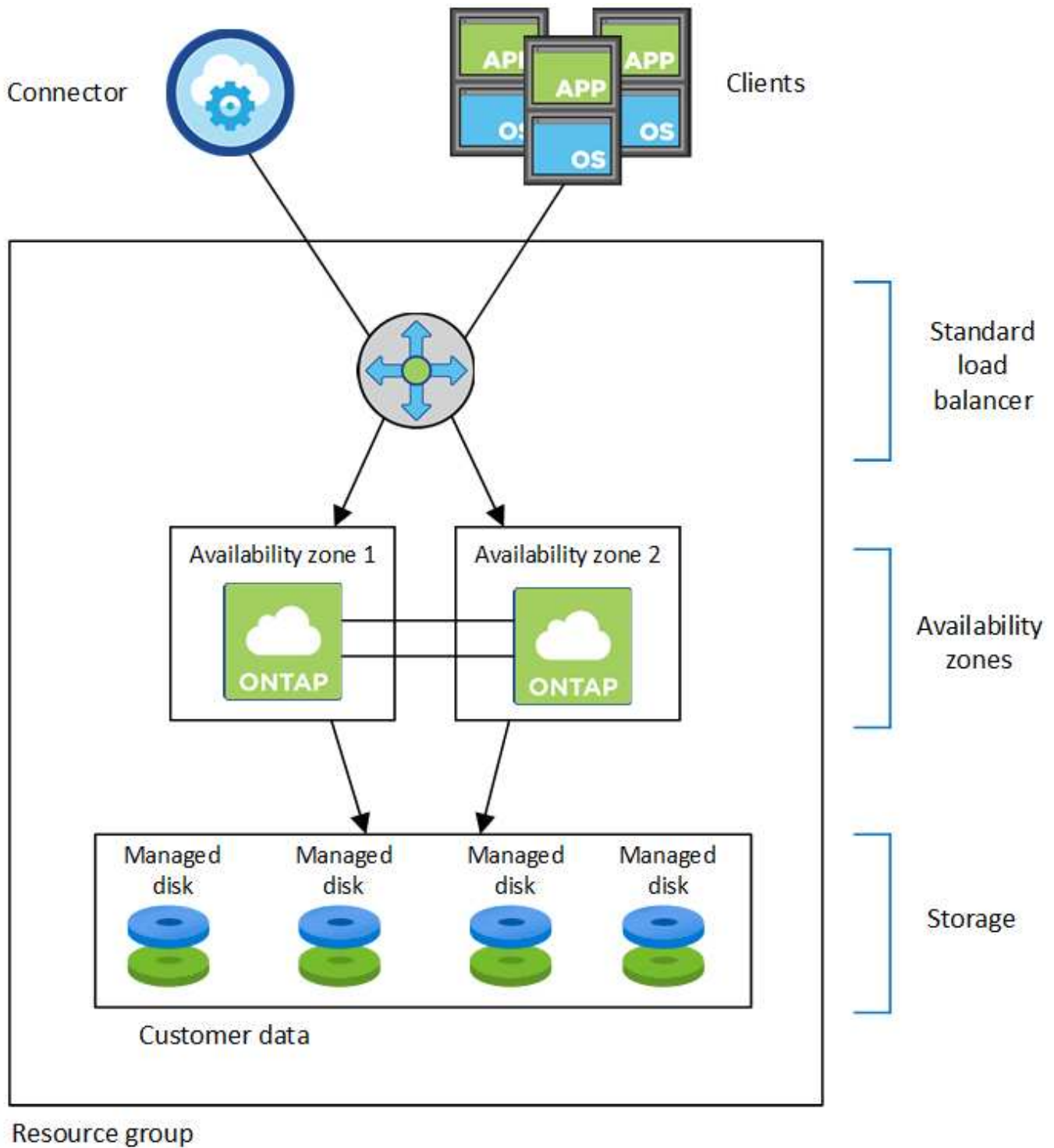
고객 데이터는 LRS(Locally Redundant Storage) 관리 디스크에 상주합니다. 각 노드는 다른 노드의 스토리지에 액세스할 수 있습니다. 의 경우 추가 스토리지도 필요합니다 "부팅, 루트, 파트너 루트, 코어 및 NVRAM 데이터".

## 스토리지 계정

스토리지 계정은 관리 디스크 기반 구축에 사용되어 진단 로그를 처리하고 BLOB 스토리지에 계층화합니다.

## HA 다중 가용성 영역 구성

Azure의 Cloud Volumes ONTAP HA 다중 가용성 영역 구성에는 다음과 같은 구성요소가 포함됩니다.



BlueXP가 배포하는 Azure 구성 요소에 대한 다음 사항에 유의하십시오.

#### Azure 표준 로드 밸런서

로드 밸런서는 Cloud Volumes ONTAP HA 쌍에 대한 들어오는 트래픽을 관리합니다.

#### 가용성 영역

두 개의 Cloud Volumes ONTAP 노드가 서로 다른 가용성 영역에 구축됩니다. 가용성 영역은 노드가 서로 다른 장애 도메인에 있는지 확인합니다. "[Azure 문서에서 관리되는 디스크를 위한 Azure 영역 중복 스토리지에 대해 자세히 알아보십시오](#)".

## 디스크

고객 데이터는 ZRS(Zone-Redundant Storage) 관리 디스크에 있습니다. 각 노드는 다른 노드의 스토리지에 액세스할 수 있습니다. 의 경우 추가 스토리지도 필요합니다 "[부팅, 루트, 파트너 루트 및 핵심 데이터](#)".

## 스토리지 계정

스토리지 계정은 관리 디스크 기반 구축에 사용되어 진단 로그를 처리하고 BLOB 스토리지에 계층화합니다.

## RPO 및 RTO

HA 구성을 사용하면 다음과 같이 데이터의 고가용성을 유지할 수 있습니다.

- 복구 지점 목표(RPO)는 0초입니다.  
데이터는 데이터 손실 없이 트랜잭션 측면에서 일관적입니다.
- 복구 시간 목표(RTO)는 120초이다.  
정전이 발생할 경우 120초 이내에 데이터를 사용할 수 있어야 합니다.

## 스토리지 테이크오버 및 반환

물리적 ONTAP 클러스터와 마찬가지로 Azure HA 쌍의 스토리지가 노드 간에 공유됩니다. 파트너의 스토리지에 연결하면 각 노드가 `_Takeover_`가 발생한 경우 다른 노드의 스토리지에 액세스할 수 있습니다. 네트워크 경로 페일오버 메커니즘을 통해 클라이언트 및 호스트가 정상 작동하는 노드와 계속 통신할 수 있습니다. 노드가 다시 온라인 상태가 되면 `PARTNER_`에서 `BACK_STORAGE`를 제공합니다.

NAS 구성의 경우 장애가 발생할 경우 데이터 IP 주소가 HA 노드 간에 자동으로 마이그레이션됩니다.

iSCSI의 경우 Cloud Volumes ONTAP는 다중 경로 I/O(MPIO) 및 ALUA(Asymmetric Logical Unit Access)를 사용하여 능동 최적화 경로와 최적화되지 않은 경로 간의 경로 페일오버를 관리합니다.



ALUA를 지원하는 특정 호스트 구성에 대한 자세한 내용은 [참조하십시오 "NetApp 상호 운용성 매트릭스 툴"](#) 및 호스트 운영 체제용 Host Utilities 설치 및 설정 설명서를 참조하십시오.

스토리지 테이크오버, 재동기화 및 반환은 기본적으로 모두 자동으로 수행됩니다. 사용자 작업이 필요하지 않습니다.

## 구성의 스토리지

HA 쌍을 액티브-액티브 구성으로 사용할 수 있으며, 두 노드에서 클라이언트에 데이터를 제공하거나 액티브-패시브 구성으로 사용할 수 있습니다. 이 구성에서는 패시브 노드가 액티브 노드의 스토리지를 인계받은 경우에만 데이터 요청에 응답합니다.

## Google Cloud의 고가용성 쌍

Cloud Volumes ONTAP HA(고가용성) 구성은 무중단 운영 및 내결함성을 제공합니다. Google Cloud에서는 두 노드 간에 데이터를 동기식으로 미러링합니다.

## HA 구성 요소

Google Cloud의 Cloud Volumes ONTAP HA 구성에는 다음과 같은 구성요소가 포함됩니다.

- 데이터가 서로 동기식으로 미러링되는 2개의 Cloud Volumes ONTAP 노드

- 스토리지 테이크오버 및 반환 프로세스를 지원하는 노드 간 통신 채널을 제공하는 중재자 인스턴스
- 구역 1개 또는 구역 3개(권장)

세 개의 영역을 선택하면 두 개의 노드와 중재자가 별도의 Google Cloud 영역에 있습니다.

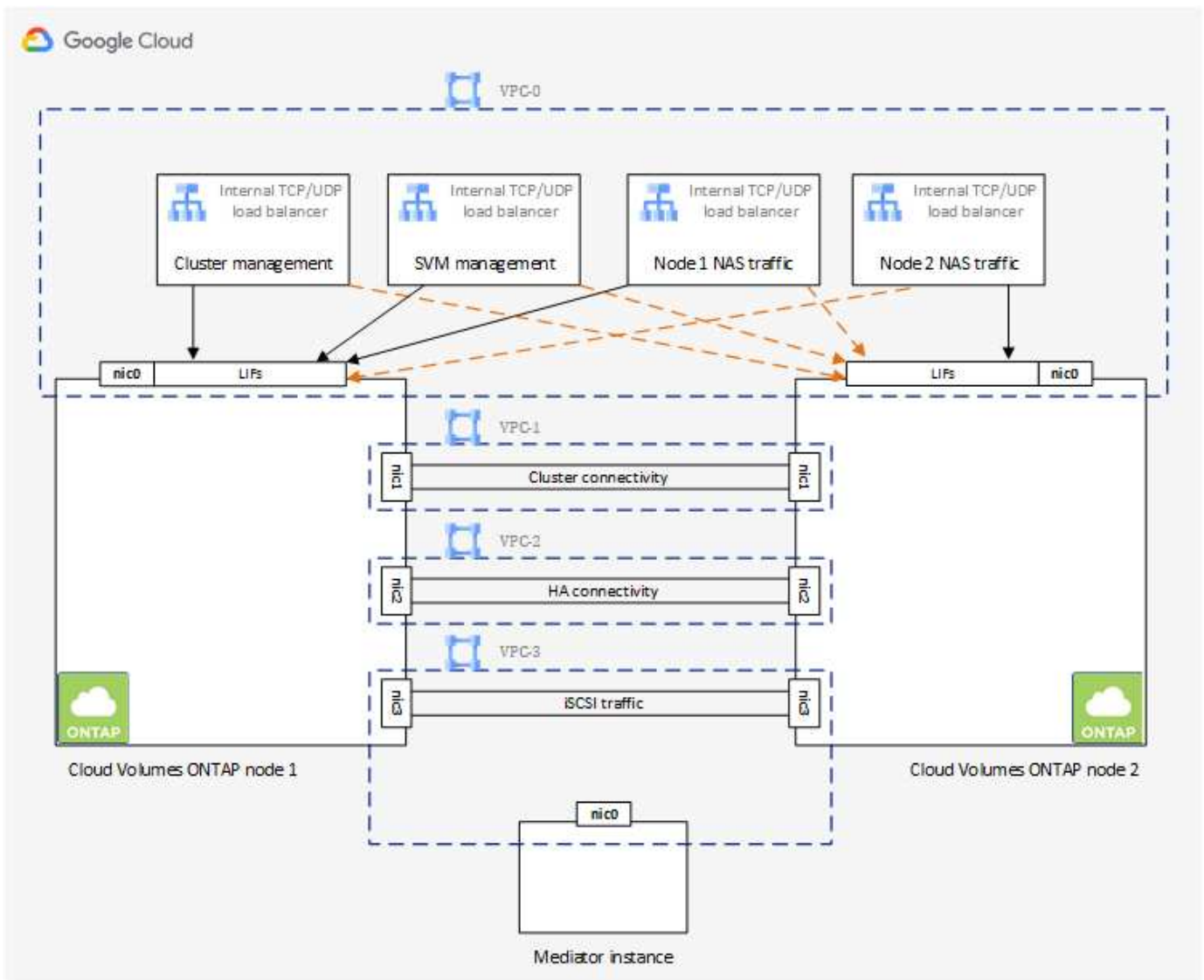
- 4개의 가상 프라이빗 클라우드(VPC).

GCP는 각 네트워크 인터페이스가 별도의 VPC 네트워크에 상주하도록 요구하기 때문에 이 구성에서는 4개의 VPC를 사용합니다.

- Cloud Volumes ONTAP HA 쌍으로 들어오는 트래픽을 관리하는 Google 클라우드 내부 로드 밸런서(TCP/UDP) 4개

"네트워킹 요구 사항에 대해 알아보십시오" 부하 분산 장치, VPC, 내부 IP 주소, 서브넷 등에 대한 자세한 정보를 제공합니다.

다음 개념적 이미지는 Cloud Volumes ONTAP HA 쌍 및 구성 요소가 나와 있습니다.





## 중재자

다음은 Google Cloud의 중재자 인스턴스에 대한 몇 가지 주요 세부 사항입니다.

## 인스턴스 유형

E2-마이크로(이전에 F1-마이크로 인스턴스가 사용됨)

## 디스크

각각 10GiB인 2개의 표준 영구 디스크

## 운영 체제

데비안 11



Cloud Volumes ONTAP 9.10.0 이전 버전에서는 데비안 10이 중재자위에 설치되었습니다.

## 업그레이드

Cloud Volumes ONTAP를 업그레이드할 때 BlueXP는 필요에 따라 중재자 인스턴스도 업데이트합니다.

## 인스턴스에 대한 액세스

데비안의 경우 기본 클라우드 사용자는 `admin`. Google Cloud에서 에 대한 인증서를 생성하고 추가합니다 `admin` Google Cloud 콘솔 또는 `gcloud` 명령줄을 통해 SSH 액세스가 요청된 경우 사용자 지정할 수 있습니다 `sudo` 루트 권한을 획득합니다.

## 제3자 에이전트

타사 에이전트 또는 VM 확장은 중재자 인스턴스에서 지원되지 않습니다.

## 스토리지 테이크오버 및 반환

노드가 중단되면 다른 노드가 파트너에게 데이터를 제공하여 지속적인 데이터 서비스를 제공할 수 있습니다. 데이터는 파트너에게 동기식으로 미러링되므로 클라이언트가 파트너 노드에서 동일한 데이터에 액세스할 수 있습니다.

노드가 재부팅된 후 파트너가 스토리지를 반환하기 전에 데이터를 다시 동기화해야 합니다. 데이터를 재동기화하는 데 걸리는 시간은 노드가 다운된 동안 변경된 데이터의 양에 따라 달라집니다.

스토리지 테이크오버, 재동기화 및 반환은 기본적으로 모두 자동으로 수행됩니다. 사용자 작업이 필요하지 않습니다.

## RPO 및 RTO

HA 구성을 사용하면 다음과 같이 데이터의 고가용성을 유지할 수 있습니다.

- 복구 지점 목표(RPO)는 0초입니다.

데이터는 데이터 손실 없이 트랜잭션 측면에서 일관적입니다.

- 복구 시간 목표(RTO)는 120초이다.

정전이 발생할 경우 120초 이내에 데이터를 사용할 수 있어야 합니다.

## HA 구축 모델

여러 존 또는 단일 존에 HA 구성을 구축하여 데이터의 고가용성을 보장할 수 있습니다.

### 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 Pair의 스토리지 작동 방식

ONTAP 클러스터와 달리 GCP의 Cloud Volumes ONTAP HA 쌍에 있는 스토리지는 노드 간에 공유되지 않습니다. 대신 데이터가 노드 간에 동기식으로 미러링되므로 장애 발생 시 데이터를 사용할 수 있습니다.

### 스토리지 할당

새 볼륨을 생성하고 추가 디스크가 필요한 경우 BlueXP는 두 노드에 동일한 수의 디스크를 할당하고 미러링된 애그리게이트를 생성한 다음 새 볼륨을 생성합니다. 예를 들어, 볼륨에 두 개의 디스크가 필요한 경우 BlueXP는 노드당 두 개의 디스크를 총 4개의 디스크에 할당합니다.

### 구성의 스토리지

HA 쌍을 액티브-액티브 구성으로 사용할 수 있으며, 두 노드에서 클라이언트에 데이터를 제공하거나 액티브-패시브 구성으로 사용할 수 있습니다. 이 구성에서는 패시브 노드가 액티브 노드의 스토리지를 인계받은 경우에만 데이터 요청에 응답합니다.

### HA 구성에 대한 성능 기대치

Cloud Volumes ONTAP HA 구성은 노드 간에 데이터를 동기식으로 복제하여 네트워크 대역폭을 사용합니다. 따라서 단일 노드 Cloud Volumes ONTAP 구성과 비교하여 다음과 같은 성능을 기대할 수 있습니다.

- 한 노드의 데이터만 제공하는 HA 구성의 경우 읽기 성능은 단일 노드 구성의 읽기 성능과 비슷하며 쓰기 성능은 낮습니다.
- 두 노드의 데이터를 제공하는 HA 구성의 경우 읽기 성능은 단일 노드 구성의 읽기 성능보다 높고 쓰기 성능은 동일하거나 더 높습니다.

Cloud Volumes ONTAP 성능에 대한 자세한 내용은 [를 참조하십시오 "성능"](#).

### 스토리지에 대한 클라이언트 액세스

클라이언트는 볼륨이 상주하는 노드의 데이터 IP 주소를 사용하여 NFS 및 CIFS 볼륨을 액세스해야 합니다. NAS 클라이언트가 파트너 노드의 IP 주소를 사용하여 볼륨에 액세스하는 경우 트래픽이 두 노드 간에 이동하므로 성능이 저하됩니다.



HA 쌍에서 노드 간에 볼륨을 이동하는 경우 다른 노드의 IP 주소를 사용하여 볼륨을 다시 마운트해야 합니다. 그렇지 않으면 성능이 저하될 수 있습니다. 클라이언트가 CIFS에 대한 NFSv4 참조 또는 폴더 리디렉션을 지원하는 경우 Cloud Volumes ONTAP 시스템에서 이러한 기능을 설정하여 볼륨을 다시 마운트하지 않도록 할 수 있습니다. 자세한 내용은 ONTAP 설명서를 참조하십시오.

BlueXP의 볼륨 관리 패널에서 *Mount Command* 옵션을 통해 올바른 IP 주소를 쉽게 식별할 수 있습니다.

The screenshot shows the 'Volume Actions' section of the BlueXP interface. It features a list of actions for a volume, including 'View volume details', 'Mount command', 'Clone volume', 'Edit volume tags', 'Edit volume settings', and 'Delete volume'. Below this list are three expandable sections: 'Protection Actions' (with a shield icon), 'Advanced Actions' (with a gear icon), and another section with a downward arrow icon. The 'Mount command' option is highlighted with a red rectangular box.

관련 링크

- ["네트워킹 요구 사항에 대해 알아보십시오"](#)

- "GCP에서 시작하는 방법을 알아보십시오"

테이크오버 중에 작업을 사용할 수 없습니다

HA 쌍의 노드를 사용할 수 없는 경우 다른 노드는 파트너에게 지속적인 데이터 서비스를 제공하는 데이터를 제공합니다. 이를 `_storage takeover_`라고 합니다. 스토리지 반환이 완료될 때까지 몇 가지 작업을 사용할 수 없습니다.



HA 쌍의 노드를 사용할 수 없는 경우 BlueXP의 작업 환경 상태는 `_ Degraded _`입니다.

BlueXP 스토리지 테이크오버에서는 다음 작업을 사용할 수 없습니다.

- 지원 등록
- 사용권 변경
- 인스턴스 또는 VM 유형 변경
- 쓰기 속도 변경
- CIFS 설정
- 구성 백업의 위치 변경
- 클러스터 암호 설정
- 디스크 및 애그리게이트 관리(고급 할당)

이러한 작업은 스토리지 반환이 완료되고 작업 환경의 상태가 정상으로 돌아온 후에 다시 사용할 수 있습니다.

## 보안

Cloud Volumes ONTAP는 데이터 암호화를 지원하고 바이러스 및 랜섬웨어에 대한 보호를 제공합니다.

### 유휴 데이터의 암호화

Cloud Volumes ONTAP는 다음과 같은 암호화 기술을 지원합니다.

- NetApp 암호화 솔루션(NVE 및 NAE)
- AWS 키 관리 서비스
- Azure 스토리지 서비스 암호화
- Google Cloud Platform 기본 암호화

클라우드 공급자의 기본 암호화와 함께 NetApp 암호화 솔루션을 사용할 수 있으며, 하이퍼바이저 레벨에서 데이터를 암호화할 수 있습니다. 이렇게 하면 매우 민감한 데이터에 필요할 수 있는 이중 암호화가 제공됩니다. 암호화된 데이터에 액세스할 때 하이퍼바이저 수준에서 한 번(클라우드 공급자의 키 사용) 암호화되지 않은 다음 다시 NetApp 암호화 솔루션(외부 키 관리자의 키 사용)을 사용합니다.

## NetApp 암호화 솔루션(NVE 및 NAE)

Cloud Volumes ONTAP 지원 ["NVE\(NetApp Volume Encryption\) 및 NetApp NAE\(Aggregate Encryption\)"](#). NVE와 NAE는 볼륨의 유휴 데이터 암호화를 FIPS(140-2를 준수하는 소프트웨어 기반 솔루션입니다. NVE와 NAE는 모두 AES 256비트 암호화를 사용합니다.

- NVE는 유휴 데이터를 한 번에 한 볼륨씩 암호화합니다. 각 데이터 볼륨에는 고유한 암호화 키가 있습니다.
- NAE는 NVE의 확장판이며 각 볼륨의 데이터를 암호화하고 애그리게이트 전체에서 볼륨을 공유합니다. NAE는 또한 애그리게이트의 모든 볼륨 전반에서 공통 블록을 중복제거할 수 있습니다.

NVE와 NAE는 모두 외부 키 관리자로 지원됩니다.

새 애그리게이트에는 외부 키 관리자를 설정한 후 기본적으로 NAE(NetApp Aggregate Encryption)가 활성화되어 있습니다. NAE 애그리게이트에 속하지 않는 새로운 볼륨은 기본적으로 NetApp Volume Encryption(NVE)이 활성화되어 있습니다(예: 외부 키 관리자를 설정하기 전에 생성된 기존 애그리게이트가 있는 경우).

지원되는 키 관리자를 설정하는 것은 필요한 유일한 단계입니다. 설치 지침은 [을 참조하십시오 "NetApp 암호화 솔루션으로 볼륨 암호화"](#).

## AWS 키 관리 서비스

AWS에서 Cloud Volumes ONTAP 시스템을 시작하면 [를 사용하여](#) 데이터 암호화를 설정할 수 있습니다 ["AWS KMS\(키 관리 서비스\)"](#). BlueXP는 CMK(Customer Master Key)를 사용하여 데이터 키를 요청합니다.



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

이 암호화 옵션을 사용하려면 AWS KMS가 적절하게 설정되어 있는지 확인해야 합니다. 자세한 내용은 [을 참조하십시오 "AWS KMS 설정"](#).

## Azure 스토리지 서비스 암호화

Azure의 Cloud Volumes ONTAP에서 [를 사용하여](#) 데이터가 자동으로 암호화됩니다 ["Azure 스토리지 서비스 암호화"](#) Microsoft 관리 키를 사용합니다.

원하는 경우 자체 암호화 키를 사용할 수 있습니다. ["Azure에서 고객이 관리하는 키를 사용하도록 Cloud Volumes ONTAP를 설정하는 방법에 대해 알아보십시오"](#).

## Google Cloud Platform 기본 암호화

["Google Cloud Platform 유휴 데이터 암호화"](#) Cloud Volumes ONTAP에 대해 기본적으로 활성화됩니다. 설정이 필요하지 않습니다.

Google 클라우드 스토리지는 디스크에 데이터를 쓰기 전에 항상 데이터를 암호화하지만 BlueXP API를 사용하여 고객이 관리하는 암호화 키를 사용하는 Cloud Volumes ONTAP 시스템을 만들 수 있습니다. 클라우드 키 관리 서비스를 사용하여 GCP에서 생성하고 관리하는 키입니다. ["자세한 정보"](#).

## ONTAP 바이러스 검사

ONTAP 시스템에서 통합 바이러스 백신 기능을 사용하여 바이러스나 기타 악성 코드에 의해 데이터가 손상되는 것을 방지할 수 있습니다.

ONTAP 바이러스 검사(Vscan)는 동급 최강의 타사 바이러스 백신 소프트웨어와 ONTAP 기능을 결합하여 언제 어떤 파일을 스캔할지 제어하는 데 필요한 유연성을 제공합니다.

Vscan에서 지원하는 공급업체, 소프트웨어 및 버전에 대한 자세한 내용은 ["NetApp 상호 운용성 매트릭스"](#).

ONTAP 시스템에서 바이러스 백신 기능을 구성 및 관리하는 방법에 대한 자세한 내용은 ["ONTAP 9 안티바이러스 구성 가이드"](#).

## 랜섬웨어 보호

랜섬웨어 공격은 비즈니스 시간, 리소스 및 평판에 악영향을 줄 수 있습니다. BlueXP를 사용하면 랜섬웨어에 대한 NetApp 솔루션을 구현할 수 있으며, 이 솔루션은 가시성, 탐지 및 문제 해결에 효과적인 툴을 제공합니다.

- BlueXP는 스냅샷 정책에 의해 보호되지 않는 볼륨을 식별하고 이러한 볼륨에 대한 기본 스냅샷 정책을 활성화할 수 있도록 합니다.


Snapshot 복사본은 읽기 전용이므로 랜섬웨어 손상을 방지합니다. 또한 세분화하여 단일 파일 복사본 또는 전체 재해 복구 솔루션의 이미지를 생성할 수도 있습니다.

- 또한 BlueXP에서는 ONTAP의 FPolicy 솔루션을 사용하여 일반적인 랜섬웨어 파일 확장을 차단할 수 있습니다.

### Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

#### 1 Enable Snapshot Copy Protection




50 % Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

Activate Snapshot Policy

#### 2 Block Ransomware File Extensions



ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

View Denied File Names

Activate FPolicy

"랜섬웨어에 대한 NetApp 솔루션을 구축하는 방법을 알아보십시오".

## 성능

성능 결과를 검토하여 Cloud Volumes ONTAP에 적합한 워크로드를 결정할 수 있습니다.

### 성능 기술 보고서

- AWS 환경을 위한 Cloud Volumes ONTAP

["NetApp 기술 보고서 4383: 애플리케이션 워크로드를 포함한 Amazon Web Services의 Cloud Volumes ONTAP 성능 특성"](#)

- Microsoft Azure용 Cloud Volumes ONTAP

["NetApp 기술 보고서 4671: 애플리케이션 워크로드를 포함한 Azure의 Cloud Volumes ONTAP 성능 특성"](#)

- Google Cloud용 Cloud Volumes ONTAP

["NetApp 기술 보고서 4816: Cloud Volumes ONTAP for Google Cloud의 성능 특성"](#)

## CPU 성능

Cloud Volumes ONTAP 노드는 클라우드 공급자의 모니터링 툴을 사용해 활용률이 90% 이상인 것으로 나타났습니다. 이는 ONTAP가 필요한 경우 사용할 수 있도록 가상 머신에 제공되는 모든 vCPU를 예약하기 때문입니다.

자세한 내용은 를 참조하십시오 ["CLI를 사용하여 ONTAP CPU 활용률을 모니터링하는 방법에 대한 NetApp 기술 자료 문서"](#)

## 노드 기반 BYOL의 라이선스 관리

노드 기반 BYOL을 사용하는 각 Cloud Volumes ONTAP 시스템에는 활성 상태의 시스템 라이선스가 설치되어 있어야 합니다. BlueXP는 라이선스를 관리하고 만료 전에 경고를 표시하여 프로세스를 간소화합니다.



노드 기반 라이선스는 이전 세대 BYOL for Cloud Volumes ONTAP입니다. 노드 기반 라이선스는 라이선스 갱신에만 사용할 수 있습니다.

["Cloud Volumes ONTAP 라이선스 옵션에 대해 자세히 알아보십시오"](#).

["노드 기반 라이선스를 관리하는 방법에 대해 자세히 알아보십시오"](#).

## BYOL 시스템 라이선스

노드 기반 라이선스는 단일 노드 또는 HA 쌍에 대해 최대 368TiB의 용량을 제공합니다.

Cloud Volumes ONTAP BYOL 시스템에 여러 개의 라이선스를 구매하여 368TiB 이상의 용량을 할당할 수 있습니다. 예를 들어, 2개의 라이선스를 구입하여 최대 736TiB의 용량을 Cloud Volumes ONTAP에 할당할 수 있습니다. 또는 4개의 라이선스를 구입하여 최대 1.4개의 PiB를 구입할 수 있습니다.

단일 노드 시스템 또는 HA 쌍에 대해 구매할 수 있는 라이선스 수는 무제한입니다.

디스크 제한만으로는 용량 제한에 도달하지 못할 수 있습니다. 를 사용하면 디스크 제한을 초과할 수 있습니다 ["비활성 데이터를 오브젝트 스토리지로 계층화"](#). 디스크 제한에 대한 자세한 내용은 를 참조하십시오 ["Cloud Volumes ONTAP 릴리즈 노트의 저장 용량 제한"](#).

## 새 시스템의 라이선스 관리

노드 기반 BYOL 시스템을 생성하는 경우 BlueXP는 라이선스 및 NetApp Support 사이트 계정의 일련 번호를 묻습니다. BlueXP에서는 계정을 사용하여 NetApp에서 라이선스 파일을 다운로드하고 Cloud Volumes ONTAP 시스템에 설치합니다.

"NetApp Support 사이트 계정을 BlueXP에 추가하는 방법에 대해 알아봅니다".

보안 인터넷 연결을 통해 BlueXP에서 라이선스 파일에 액세스할 수 없는 경우 "파일을 직접 얻은 다음 파일을 BlueXP에 수동으로 업로드합니다".

## 라이선스 만료

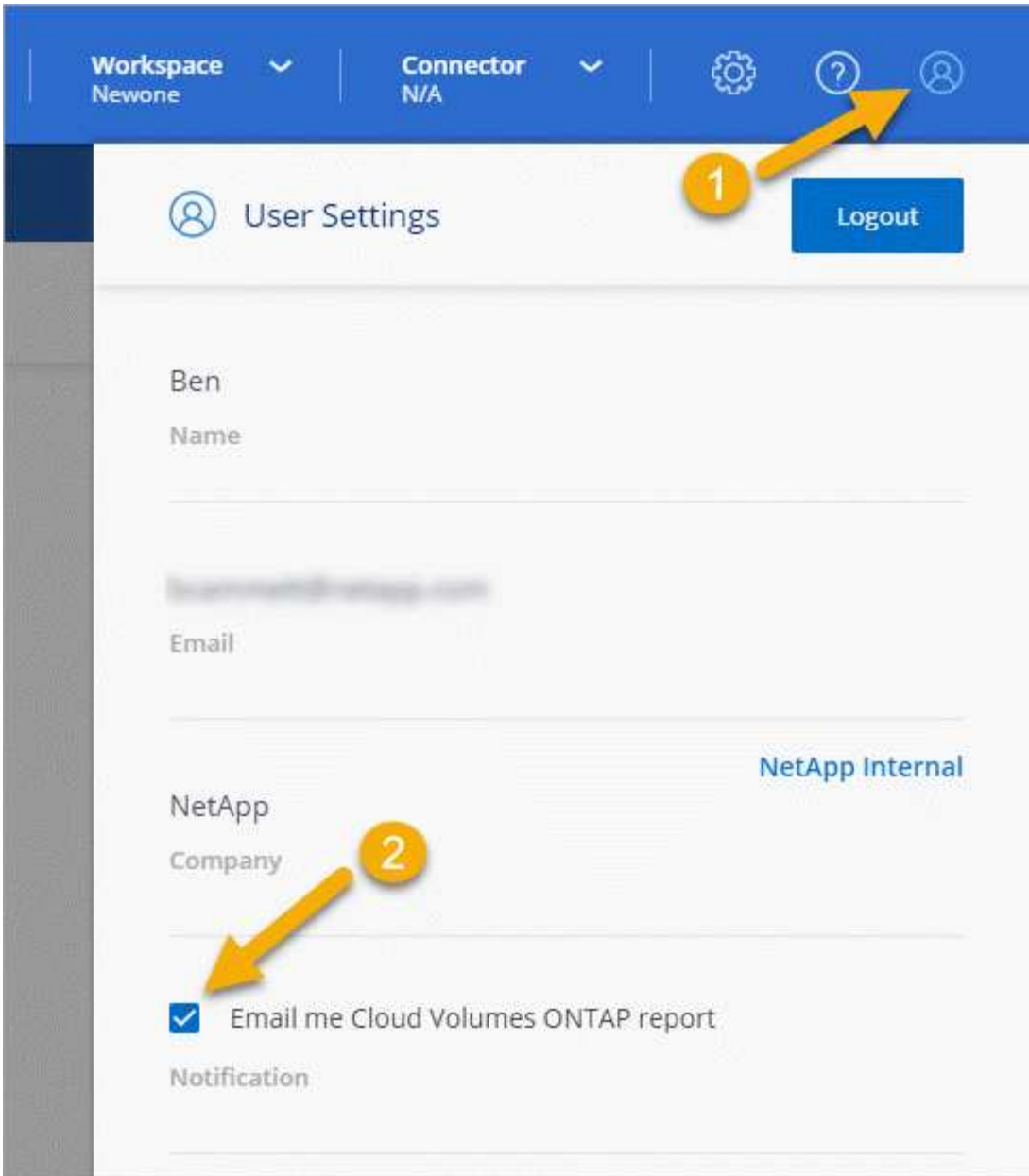
BlueXP는 노드 기반 라이선스가 만료되기 30일 전과 라이선스가 만료되면 경고를 표시합니다. 다음 이미지는 사용자 인터페이스에 표시되는 30일 만료 경고입니다.



작업 환경을 선택하여 메시지를 검토할 수 있습니다.

BlueXP에는 계정 관리자이고 옵션을 활성화한 경우 이메일로 전송되는 Cloud Volumes ONTAP 보고서에 라이선스 만료 경고가 포함됩니다.





e-메일 보고서에는 2주마다 라이선스 만료 경고가 포함됩니다.

라이선스를 제때 갱신하지 않으면 Cloud Volumes ONTAP 시스템이 자동으로 종료됩니다. 다시 시작하면 자동으로 종료됩니다.

## 라이선스 갱신

NetApp 담당자에게 연락하여 노드 기반 BYOL 가입을 갱신하면, BlueXP는 NetApp에서 새로운 라이선스를 자동으로 얻어 Cloud Volumes ONTAP 시스템에 설치합니다.

보안 인터넷 연결을 통해 BlueXP에서 라이선스 파일에 액세스할 수 없는 경우 ["파일을 직접 얻은 다음 파일을 BlueXP에 수동으로 업로드합니다"](#).

## 새 시스템으로 라이선스 이전

노드 기반 BYOL 라이선스는 기존 시스템을 삭제한 후 동일한 라이선스를 사용하여 새 시스템을 생성하는 경우 Cloud

Volumes ONTAP 시스템 간에 이전할 수 있습니다.

예를 들어, 기존의 라이선스가 있는 시스템을 삭제한 다음 다른 VPC/VNET 또는 클라우드 공급자에서 새 BYOL 시스템과 함께 라이선스를 사용할 수 있습니다. 모든 클라우드 공급자에서는 \_cloud-종류를 붙인 \_일련 번호만 작동합니다. 클라우드 독립적 일련 번호는 \_908xxxx\_ 접두사로 시작합니다.

BYOL 라이선스는 회사 및 특정 NetApp Support 사이트 자격 증명과 관련이 있습니다.

## AutoSupport 및 Active IQ 디지털 자문업체

ONTAP의 AutoSupport 구성 요소는 원격 측정을 수집하여 분석을 위해 전송합니다. Active IQ 디지털 어드바이저는 AutoSupport의 데이터를 분석하고 능동적인 관리 및 최적화를 제공합니다. Active IQ은 인공지능을 사용하여 잠재적인 문제를 파악하고 비즈니스에 영향을 미치기 전에 이를 해결하도록 지원합니다. 컷오버 테스트를 위한 변경 사항

현지화 변경 사항 Docbot 및 테스트 위치 표시를 활성화합니다. dockbot 비활성화 테스트 중입니다. 세 번째로 루비 업그레이드를 다시 테스트합니다. 루비 업그레이드 푸시 테스트

Active IQ을 사용하면 클라우드 기반 포털 및 모바일 앱을 통해 실행 가능한 예측 분석과 능동적 지원을 제공하여 글로벌 하이브리드 클라우드 전반에서 데이터 인프라를 최적화할 수 있습니다. SupportEdge의 데이터 중심 인사이트와 권장사항은 Active IQ 계약이 체결된 모든 NetApp 고객(기능은 제품 및 지원 계층에 따라 다름)에게 제공됩니다.

다음은 Active IQ에서 수행할 수 있는 몇 가지 사항입니다.

- 업그레이드 계획

Active IQ는 사용자 환경에서 최신 버전의 ONTAP로 업그레이드하여 해결할 수 있는 문제를 식별하며, 업그레이드 관리자 구성 요소는 성공적인 업그레이드를 계획하는 데 도움이 됩니다.

- 시스템 상태 보기

Active IQ 대시보드에서 웰빙과 관련된 모든 문제를 보고하고 문제를 해결할 수 있습니다. 시스템 용량을 모니터링하여 스토리지 공간이 부족하지 않도록 하십시오. 시스템에 대한 지원 케이스를 봅니다.

- 성능 관리

Active IQ는 ONTAP System Manager에서 볼 수 있는 것보다 더 오랜 기간 동안의 시스템 성능을 보여 줍니다. 성능에 영향을 주는 구성 및 시스템 문제를 식별합니다. 효율성 극대화 스토리지 효율성 메트릭을 확인하고 더 적은 공간에 더 많은 데이터를 저장하는 방법을 알아보십시오.

- 인벤토리 및 구성을 봅니다.

Active IQ는 전체 인벤토리 및 소프트웨어 및 하드웨어 구성 정보를 표시합니다. 서비스 계약이 만료되는 시기를 확인하고 서비스 계약을 갱신하여 계속 지원을 받을 수 있도록 합니다.

관련 정보

- ["NetApp 설명서: Active IQ 디지털 자문업체"](#)
- ["Active IQ를 시작합니다"](#)
- ["SupportEdge 서비스"](#)

# Cloud Volumes ONTAP의 기본 구성입니다

Cloud Volumes ONTAP가 기본적으로 어떻게 구성되어 있는지 이해하면 시스템을 설정하고 관리하는 데 도움이 됩니다. 특히 ONTAP에 익숙한 경우 Cloud Volumes ONTAP의 기본 설정은 ONTAP와 다르기 때문입니다.

## 기본 설정

- BlueXP는 Cloud Volumes ONTAP를 배포할 때 데이터 서비스 스토리지 VM을 하나만 생성합니다. 일부 구성은 추가 스토리지 VM을 지원합니다. "[스토리지 VM 관리에 대해 자세히 알아보십시오](#)".

BlueXP 3.9.5 릴리스부터는 초기 스토리지 VM에서 논리적 공간 보고가 활성화됩니다. 공간이 논리적으로 보고되면 ONTAP에서는 스토리지 효율성 기능으로 절약된 모든 물리적 공간이 사용된 것으로 보고하도록 볼륨 공간을 보고합니다.

- BlueXP는 Cloud Volumes ONTAP에 다음과 같은 ONTAP 기능 라이선스를 자동으로 설치합니다.
  - CIFS를 선택합니다
  - FlexCache
  - 플렉스클론
  - iSCSI
  - 멀티 테넌트 암호화 키 관리(MTEKM), Cloud Volumes ONTAP 9.12.1 GA로 시작
  - NetApp 볼륨 암호화(BYOL 또는 등록 PAYGO 시스템에만 해당)
  - NFS 를 참조하십시오
- SnapMirror를 참조하십시오
- SnapRestore
- SnapVault
  - 기본적으로 여러 네트워크 인터페이스가 생성됩니다.
- 클러스터 관리 LIF
- 인터클러스터 LIF
- Azure의 HA 시스템에서 SVM 관리 LIF
- Google Cloud의 HA 시스템에서 SVM 관리 LIF
- AWS의 단일 노드 시스템에서 SVM 관리 LIF를 관리합니다
- 노드 관리 LIF

를 누릅니다

Google Cloud에서 이 LIF는 인터클러스터 LIF와 결합됩니다.

- iSCSI 데이터 LIF
- CIFS 및 NFS 데이터 LIF



클라우드 공급자의 요구사항으로 인해 LIF 페일오버가 Cloud Volumes ONTAP에 대해 기본적으로 비활성화되어 있습니다. LIF를 다른 포트로 마이그레이션하면 IP 주소와 인스턴스 네트워크 인터페이스 간의 외부 매핑이 분리되므로 LIF에 액세스할 수 없습니다.

- Cloud Volumes ONTAP는 HTTP를 사용하여 구성 백업을 Connector로 전송합니다.

백업은 `http://ipaddress/occm/offboxconfig/`에서 액세스할 수 있습니다. 여기서 `_ipaddress_`는 커넥터 호스트의 IP 주소입니다.

- BlueXP는 다른 관리 도구(예: System Manager 또는 CLI)와 몇 가지 볼륨 속성을 다르게 설정합니다.

다음 표에는 BlueXP가 기본값과 다르게 설정하는 볼륨 특성이 나열되어 있습니다.

| 속성                | BlueXP에서 설정한 값입니다                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------|
| 자동 크기 조정 모드입니다    | 성장                                                                                                                            |
| 최대 자동 크기 조정       | 1,000%<br> 계정 관리자는 설정 페이지에서 이 값을 수정할 수 있습니다. |
| 보안 스타일            | CIFS 볼륨용 NTFS<br>NFS 볼륨용 UNIX입니다                                                                                              |
| 공간 보장 스타일         | 없음                                                                                                                            |
| UNIX 권한(NFS에만 해당) | 777                                                                                                                           |

+ 를 참조하십시오 ["ONTAP\\_volume create\\_man 페이지"](#) 이러한 속성에 대한 자세한 내용은 를 참조하십시오.

## 시스템 데이터용 내부 디스크

BlueXP는 사용자 데이터를 위한 스토리지 외에도 시스템 데이터를 위한 클라우드 스토리지를 구입합니다.

### 설치하고

- 부팅, 루트 및 코어 데이터를 위한 노드당 디스크 3개:
  - 부팅 데이터용 45GiB io1 디스크
  - 루트 데이터용 140GiB GP3 디스크
  - 핵심 데이터용 540GiB GP2 디스크
- 각 부팅 디스크 및 루트 디스크마다 하나의 EBS 스냅샷



스냅샷은 재부팅 시 자동으로 생성됩니다.

- HA 쌍의 경우 중재자 인스턴스를 위한 하나의 EBS 볼륨, 약 8GiB입니다
- KMS(키 관리 서비스)를 사용하여 AWS에서 데이터 암호화를 설정하면 Cloud Volumes ONTAP의 부팅 및 루트 디스크도 암호화됩니다. 여기에는 HA 쌍의 중재자 인스턴스를 위한 부팅 디스크가 포함됩니다. 디스크는 작업 환경을 생성할 때 선택한 CMK를 사용하여 암호화됩니다.



AWS에서 NVRAM은 부팅 디스크에 있습니다.

### Azure(단일 노드)

- 3개의 프리미엄 SSD 디스크:
  - 부팅 데이터용 10GiB 디스크 1개
  - 루트 데이터용 140GiB 디스크 1개
  - NVRAM에 512MB 디스크 1개

Cloud Volumes ONTAP에 대해 선택한 가상 시스템이 Ultra SSD를 지원하는 경우 시스템은 프리미엄 SSD가 아닌 NVRAM에 32GiB Ultra SSD를 사용합니다.

- 코어 절약을 위한 1024GiB 표준 HDD 디스크 1개
- 각 부팅 디스크 및 루트 디스크에 대해 Azure 스냅샷 1개
- Azure에서 기본적으로 모든 디스크는 저장된 상태로 암호화됩니다.

### Azure(HA 쌍,

#### 페이지 blob과 HA 쌍

- 부팅 볼륨용 10GiB 프리미엄 SSD 디스크 2개(노드당 1개)
- 루트 볼륨에 대해 140GiB 프리미엄 스토리지 페이지 Blob 2개(노드당 1개)
- 코어 저장용 1024GiB 표준 HDD 디스크 2개(노드당 1개)
- NVRAM을 위한 512GiB 프리미엄 SSD 디스크 2개(노드당 1개)
- 각 부팅 디스크 및 루트 디스크에 대해 Azure 스냅샷 1개



스냅샷은 재부팅 시 자동으로 생성됩니다.

- Azure에서 기본적으로 모든 디스크는 저장된 상태로 암호화됩니다.

#### 여러 가용성 영역의 HA 쌍

- 부팅 볼륨용 10GiB 프리미엄 SSD 디스크 2개(노드당 1개)
- 루트 볼륨에 대해 2개의 512GiB 프리미엄 스토리지 페이지 Blob(노드당 1개)
- 코어 저장용 1024GiB 표준 HDD 디스크 2개(노드당 1개)
- NVRAM을 위한 512GiB 프리미엄 SSD 디스크 2개(노드당 1개)
- 각 부팅 디스크 및 루트 디스크에 대해 Azure 스냅샷 1개



스냅샷은 재부팅 시 자동으로 생성됩니다.

- Azure에서 기본적으로 모든 디스크는 저장된 상태로 암호화됩니다.

### Google Cloud(단일 노드)

- 부팅 데이터용 10GiB SSD 영구 디스크 1개
- 루트 데이터용 64GiB SSD 영구 디스크 1개
- NVRAM에 대해 500GiB SSD 영구 디스크 1개
- 코어 절약을 위한 315GiB 표준 영구 디스크 1개
- 부팅 및 루트 데이터용 스냅샷입니다



스냅샷은 재부팅 시 자동으로 생성됩니다.

- 부팅 및 루트 디스크는 기본적으로 암호화됩니다.

### Google Cloud(HA 쌍,

- 부팅 데이터를 위한 10GiB SSD 영구 디스크 2개
- 루트 데이터를 위한 64GiB SSD 영구 디스크 4개
- NVRAM에 대해 500GiB SSD 영구 디스크 2개
- 코어 절약을 위한 315GiB 표준 영구 디스크 2개
- 중재자 데이터를 위한 10GiB 표준 영구 디스크 1개
- 부팅 데이터의 중재자를 위한 10GiB 표준 영구 디스크 1개
- 부팅 및 루트 데이터용 스냅샷입니다



스냅샷은 재부팅 시 자동으로 생성됩니다.

- 부팅 및 루트 디스크는 기본적으로 암호화됩니다.

디스크가 상주하는 위치입니다

BlueXP는 다음과 같이 스토리지를 배치합니다.

- 부팅 데이터는 인스턴스 또는 가상 머신에 연결된 디스크에 있습니다.

부팅 이미지가 포함된 이 디스크는 Cloud Volumes ONTAP에서 사용할 수 없습니다.

- 시스템 구성 및 로그가 포함된 루트 데이터는 aggr0에 상주합니다.
- 스토리지 가상 시스템(SVM) 루트 볼륨은 aggr1에 있습니다.
- 데이터 볼륨은 aggr1에도 상주합니다.

# 지식 및 지원

## 지원을 위해 등록하십시오

BlueXP 및 해당 스토리지 솔루션 및 서비스와 관련된 기술 지원을 받으려면 지원을 등록해야 합니다. Cloud Volumes ONTAP 시스템의 주요 워크플로우를 사용하려면 지원 등록도 필요합니다.

지원을 등록한다고 해서 클라우드 공급자 파일 서비스에 대한 NetApp 지원이 활성화되지 않습니다. 클라우드 공급자의 파일 서비스, 자체 인프라 또는 서비스를 사용하는 솔루션과 관련된 기술 지원은 해당 제품의 BlueXP 설명서에서 "도움말 열기"를 참조하십시오.

- "ONTAP용 Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud용 Cloud Volumes Service"

### 지원 등록 개요

지원 권한을 활성화하려면 두 가지 형태의 등록이 있습니다.

- BlueXP 계정 ID 지원 가입 등록(BlueXP의 지원 리소스 페이지에 있는 20자리 960xxxxxxxxx 일련 번호)

이는 BlueXP 내의 모든 서비스에 대한 단일 지원 가입 ID의 역할을 합니다. 각 BlueXP 계정 수준 지원 구독을 등록해야 합니다.

- 클라우드 공급자 마켓플레이스의 구독과 연결된 Cloud Volumes ONTAP 일련 번호 등록(20자리 909201xxxxxxxx 일련 번호)

이러한 일련 번호는 일반적으로 `_PAYGO 일련 번호_`라고 하며 Cloud Volumes ONTAP 배포 시 BlueXP에서 생성됩니다.

두 가지 유형의 일련 번호를 등록하면 지원 티켓 열기와 자동 케이스 생성 등의 기능을 사용할 수 있습니다. 아래 설명과 같이 BlueXP에 NetApp Support 사이트(NSS) 계정을 추가하여 등록을 완료합니다.

### NetApp 지원을 위해 BlueXP 계정을 등록합니다

지원을 등록하고 지원 권한을 활성화하려면 BlueXP 계정의 한 사용자가 NetApp Support 사이트 계정을 BlueXP 로그인에 연결해야 합니다. NetApp 지원에 등록하는 방법은 NetApp Support 사이트(NSS) 계정이 이미 있는지 여부에 따라 다릅니다.

#### NSS 계정이 있는 기존 고객

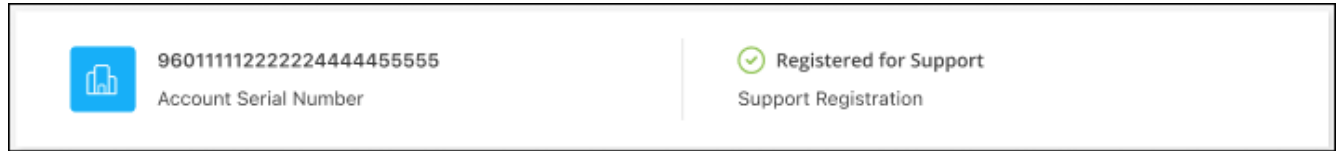
NSS 계정을 가지고 있는 NetApp 고객은 BlueXP를 통해 지원을 받기 위해 등록하기만 하면 됩니다.

#### 단계

1. BlueXP 콘솔의 오른쪽 상단에서 설정 아이콘을 선택하고 \* 자격 증명 \* 을 선택합니다.
2. 사용자 자격 증명 \* 을 선택합니다.

3. NSS 자격 증명 추가 \* 를 선택하고 NetApp Support 사이트(NSS) 인증 프롬프트를 따릅니다.
4. 등록 프로세스가 성공적으로 완료되었는지 확인하려면 도움말 아이콘을 선택하고 \* 지원 \* 을 선택합니다.

리소스 \* 페이지에 계정이 지원을 위해 등록되었다는 내용이 표시됩니다.



다른 BlueXP 사용자는 BlueXP 로그인과 NetApp Support 사이트 계정을 연결하지 않은 경우 동일한 지원 등록 상태를 볼 수 없습니다. 그러나 BlueXP 계정이 지원을 위해 등록되지 않은 것은 아닙니다. 계정에 있는 한 사용자가 이 단계를 따랐을 경우 계정이 등록되었습니다.

기존 고객이지만 **NSS** 계정은 없습니다

기존 사용권 및 제품 번호가 \_NO\_NSS인 기존 NetApp 고객인 경우 NSS 계정을 만들어 BlueXP 로그인과 연결해야 합니다.

단계

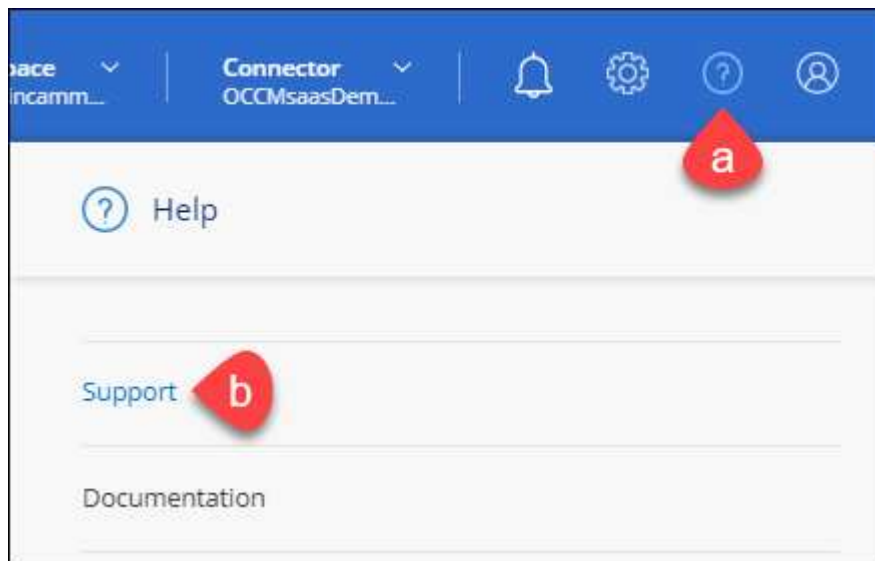
1. 를 완료하여 NetApp Support 사이트 계정을 생성합니다 **"NetApp Support 사이트 사용자 등록 양식"**
  - a. 적절한 사용자 레벨(일반적으로 \* NetApp 고객/최종 사용자 \*)을 선택해야 합니다.
  - b. 위에 사용된 BlueXP 계정 일련 번호(960xxxx)를 일련 번호 필드에 복사해야 합니다. 이렇게 하면 계정 처리 속도가 빨라집니다.
2. 의 단계를 완료하여 새 NSS 계정을 BlueXP 로그인에 연결합니다 **NSS 계정이 있는 기존 고객**.

**NetApp**이 처음이었습니다

NetApp의 새로운 브랜드이고 NSS 계정이 없는 경우 아래의 각 단계를 수행하십시오.

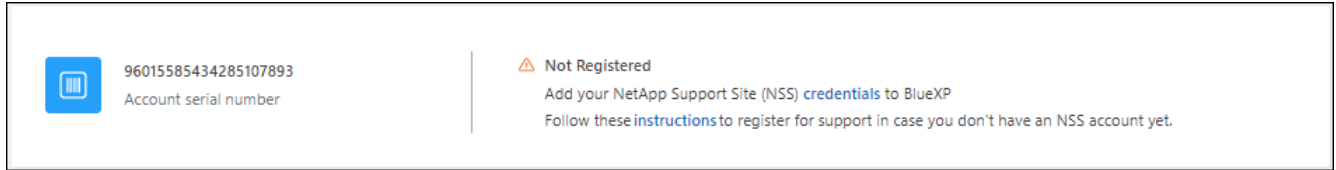
단계

1. BlueXP 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 \* 지원 \* 을 선택합니다.





2. 지원 등록 페이지에서 계정 ID 일련 번호를 찾습니다.



3. 로 이동합니다 "[NetApp의 지원 등록 사이트](#)" 를 선택하고 \* 등록된 NetApp 고객이 아닙니다 \* 를 선택합니다.

4. 필수 필드(빨간색 별표가 있는 필드)를 입력합니다.

5. [제품 라인] \* 필드에서 \* Cloud Manager \* 를 선택한 다음 해당 청구 공급자를 선택합니다.

6. 위의 2단계에서 계정의 일련 번호를 복사하고 보안 검색을 완료한 다음 NetApp의 글로벌 데이터 개인 정보 보호 정책을 읽는지 확인합니다.

이 보안 트랜잭션을 완료하기 위해 제공된 사서함으로 즉시 이메일이 전송됩니다. 몇 분 내에 확인 이메일이 도착하지 않으면 스팸 폴더를 확인해야 합니다.

7. 이메일 내에서 작업을 확인합니다.

확인 시 NetApp에 요청이 제출되고 NetApp Support 사이트 계정을 만들 것을 권장합니다.

8. 를 완료하여 NetApp Support 사이트 계정을 생성합니다 "[NetApp Support 사이트 사용자 등록 양식](#)"

a. 적절한 사용자 레벨(일반적으로 \* NetApp 고객/최종 사용자 \*)을 선택해야 합니다.

b. 일련 번호 필드에 위에서 사용된 계정 일련 번호(960xxxx)를 복사해 주십시오. 이렇게 하면 계정 처리 속도가 빨라집니다.

작업을 마친 후

이 과정에서 NetApp이 연락을 드릴 것입니다. 신규 사용자를 위한 일회성 온보딩 연습입니다.

NetApp Support 사이트 계정이 있으면 의 단계를 완료하여 계정을 BlueXP 로그인에 연결합니다 [NSS 계정이 있는 기존 고객](#).

## Cloud Volumes ONTAP 지원을 위해 NSS 자격 증명을 연결합니다

Cloud Volumes ONTAP에 대해 다음 주요 워크플로를 사용하려면 NetApp Support 사이트 자격 증명을 BlueXP 계정과 연결해야 합니다.

- 지원을 위해 선불 종량제 Cloud Volumes ONTAP 시스템을 등록합니다

NSS 계정을 제공하면 시스템에 대한 지원을 활성화하고 NetApp 기술 지원 리소스에 액세스할 수 있습니다.

- BYOL(Bring Your Own License) 방식으로 Cloud Volumes ONTAP 구축

BlueXP에서 사용권 키를 업로드하고 구입한 용어에 대한 구독을 활성화하려면 NSS 계정을 제공해야 합니다. 여기에는 기간 갱신을 위한 자동 업데이트가 포함됩니다.

- Cloud Volumes ONTAP 소프트웨어를 최신 릴리즈로 업그레이드하는 중입니다

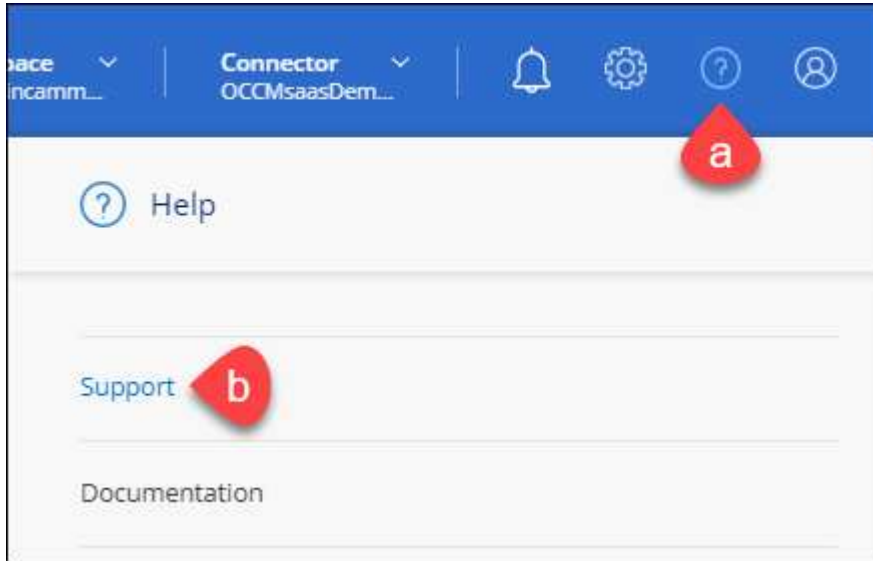
NSS 자격 증명을 BlueXP 계정과 연결하는 것은 BlueXP 사용자 로그인과 연결된 NSS 계정과 다릅니다.

이러한 NSS 자격 증명은 특정 BlueXP 계정 ID와 연결됩니다. BlueXP 계정에 속한 사용자는 \* 지원 > NSS 관리 \* 에서 이러한 자격 증명에 액세스할 수 있습니다.

- 고객 수준 계정이 있는 경우 하나 이상의 NSS 계정을 추가할 수 있습니다.
- 파트너 또는 리셀러 계정이 있는 경우 NSS 계정을 하나 이상 추가할 수 있지만 고객 수준 계정과 함께 추가할 수는 없습니다.

단계

1. BlueXP 콘솔의 오른쪽 상단에서 도움말 아이콘을 선택하고 \* 지원 \* 을 선택합니다.



2. NSS 관리 > NSS 계정 추가 \* 를 선택합니다.
3. 메시지가 표시되면 \* 계속 \* 을 선택하여 Microsoft 로그인 페이지로 리디렉션합니다.

NetApp는 지원 및 라이선스와 관련된 인증 서비스의 ID 공급자로 Microsoft Entra ID를 사용합니다.

4. 로그인 페이지에서 인증 프로세스를 수행할 수 있도록 NetApp Support 사이트의 등록 이메일 주소와 암호를 제공합니다.

이러한 작업을 통해 BlueXP는 NSS 계정을 사용하여 라이선스 다운로드, 소프트웨어 업그레이드 확인 및 향후 지원 등록과 같은 작업을 수행할 수 있습니다.

다음 사항에 유의하십시오.

- NSS 계정은 고객 수준 계정이어야 합니다(게스트 또는 임시 계정이 아님). 여러 개의 고객 수준 NSS 계정을 가질 수 있습니다.
- NSS 계정은 파트너 수준 계정인 경우 하나만 있을 수 있습니다. 고객 수준 NSS 계정을 추가하려고 하면 파트너 수준 계정이 있으면 다음 오류 메시지가 나타납니다.

"NSS 고객 유형은 이미 다른 유형의 NSS 사용자가 있으므로 이 계정에 허용되지 않습니다."

기존 고객 수준 NSS 계정이 있는 경우에도 마찬가지로 파트너 수준 계정을 추가하려고 합니다.

- 로그인에 성공하면 NetApp은 NSS 사용자 이름을 저장합니다.

이 ID는 이메일에 매핑되는 시스템 생성 ID입니다. NSS 관리 \* 페이지의 에서 이메일을 표시할 수 있습니다 ... 메뉴.

- 로그인 자격 증명 토큰을 새로 고쳐야 하는 경우 에 \* 자격 증명 업데이트 \* 옵션이 있습니다 ... 메뉴.

이 옵션을 사용하면 다시 로그인하라는 메시지가 표시됩니다. 이러한 계정의 토큰은 90일 후에 만료됩니다. 이를 알리는 알림이 게시됩니다.

## 도움을 받으십시오

NetApp은 다양한 방법으로 BlueXP 및 클라우드 서비스를 지원합니다. 기술 자료(KB) 기사 및 커뮤니티 포럼과 같은 광범위한 무료 셀프 지원 옵션이 24x7 제공됩니다. 지원 등록에는 웹 티켓팅을 통한 원격 기술 지원이 포함됩니다.

### 클라우드 공급자의 파일 서비스에 대한 지원을 받습니다

클라우드 공급자의 파일 서비스, 자체 인프라 또는 서비스를 사용하는 솔루션과 관련된 기술 지원은 해당 제품의 BlueXP 설명서에서 "도움말 얻기"를 참조하십시오.

- ["ONTAP용 Amazon FSx"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud용 Cloud Volumes Service"](#)

BlueXP 및 해당 스토리지 솔루션 및 서비스에 관한 기술 지원을 받으려면 아래에 설명된 지원 옵션을 사용하십시오.

### 자체 지원 옵션을 사용합니다

이 옵션은 하루 24시간, 주 7일 동안 무료로 사용할 수 있습니다.

- 문서화

현재 보고 있는 BlueXP 문서입니다.

- ["기술 자료"](#)

문제를 해결하는 데 도움이 되는 문서를 찾으려면 BlueXP 기술 자료를 검색하십시오.

- ["커뮤니티"](#)

BlueXP 커뮤니티에 가입하여 진행 중인 토론을 팔로우하거나 새 토론을 만드십시오.

## NetApp Support로 케이스 생성

위의 자체 지원 옵션 외에도 NetApp 지원 전문가와 협력하여 지원을 활성화한 이후의 모든 문제를 해결할 수 있습니다.


### 시작하기 전에

- 케이스 생성 \* 기능을 사용하려면 먼저 NetApp Support 사이트 자격 증명을 BlueXP 로그인에 연결해야 합니다. ["BlueXP 로그인과 관련된 자격 증명을 관리하는 방법에 대해 알아봅니다"](#).

- 일련 번호가 있는 ONTAP 시스템의 케이스를 여는 경우 NSS 계정은 해당 시스템의 일련 번호와 연결되어 있어야 합니다.

## 단계

1. BlueXP에서 \* 도움말 > 지원 \* 을 선택합니다.
2. 리소스 \* 페이지의 기술 지원 아래에서 사용 가능한 옵션 중 하나를 선택합니다.
  - a. 전화로 통화하려면 \* 전화 \* 를 선택하십시오. 전화를 걸 수 있는 전화 번호가 나열된 netapp.com 페이지로 연결됩니다.
  - b. NetApp 지원 전문가와 함께 티켓을 열려면 \* 케이스 생성 \* 을 선택하십시오.
    - \* 서비스 \*: 문제와 관련된 서비스를 선택합니다. 예를 들어, 서비스 내의 워크플로우 또는 기능과 관련된 기술 지원 문제에 해당하는 BlueXP를 예로 들 수 있습니다.
    - \* 작업 환경 \*: 스토리지에 적용 가능한 경우 \* Cloud Volumes ONTAP \* 또는 \* On-Premise \* 를 선택한 다음 관련 작업 환경을 선택합니다.  
  
작업 환경 목록은 서비스의 상단 배너에서 선택한 BlueXP 계정, 작업 영역 및 커넥터의 범위 내에 있습니다.
    - \* 케이스 우선 순위 \*: 케이스의 우선 순위를 선택합니다. 우선 순위는 낮음, 중간, 높음 또는 긴급입니다.  
  
이러한 우선 순위에 대한 자세한 내용을 보려면 필드 이름 옆에 있는 정보 아이콘 위로 마우스를 가져갑니다.
    - \* 문제 설명 \*: 해당 오류 메시지 또는 수행한 문제 해결 단계를 포함하여 문제에 대한 자세한 설명을 제공합니다.
    - \* 추가 이메일 주소 \*: 다른 사람에게 이 문제를 알고자 할 경우 추가 이메일 주소를 입력하십시오.
    - \* 첨부 파일(선택 사항) \*: 한 번에 하나씩 최대 5개의 첨부 파일을 업로드합니다.  
  
첨부 파일은 파일당 25MB로 제한됩니다. txt, log, pdf, jpg/jpeg, rtf, DOC/docx, xls/xlsx 및 CSV.


ntapitdemo 

NetApp Support Site Account

---

Service Working Environment


Select Select

Case Priority 


Low - General guidance



Issue Description

Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional) 

Type here

Attachment (Optional) Upload 

No files selected  

작업을 마친 후

지원 케이스 번호와 함께 팝업이 나타납니다. NetApp 지원 전문가가 귀하의 사례를 검토하고 곧 다시 연결해 드릴 것입니다.

지원 케이스 내역을 보려면 \* 설정 > 타임라인 \* 을 선택하고 "지원 케이스 생성"이라는 이름의 작업을 찾습니다. 오른쪽 끝에 있는 버튼을 사용하여 작업을 확장하여 세부 정보를 볼 수 있습니다.

케이스를 생성하려고 할 때 다음과 같은 오류 메시지가 나타날 수 있습니다.

"선택한 서비스에 대해 케이스를 생성할 권한이 없습니다."

이 오류는 NSS 계정과 연결된 레코드 회사가 BlueXP 계정 일련 번호( 960xxxx) 또는 작동 환경 일련 번호 다음 옵션 중 하나를 사용하여 지원을 요청할 수 있습니다.

- 제품 내 채팅을 사용합니다
- 에서 비기술 케이스를 제출하십시오 <https://mysupport.netapp.com/site/help>

## 지원 사례 관리(Preview)

BlueXP에서 직접 활성 및 해결된 지원 사례를 보고 관리할 수 있습니다. NSS 계정 및 회사와 관련된 케이스를 관리할 수 있습니다.

케이스 관리를 미리 보기로 사용할 수 있습니다. NetApp은 이 경험을 개선하고 다음 릴리즈에서 향상된 기능을 추가할 계획입니다. 제품 내 채팅을 사용하여 피드백을 보내주십시오.

다음 사항에 유의하십시오.

- 페이지 상단의 케이스 관리 대시보드에서는 두 가지 보기를 제공합니다.
  - 왼쪽 보기에는 사용자가 제공한 NSS 계정으로 지난 3개월 동안 개설된 총 케이스가 표시됩니다.
  - 오른쪽 보기에는 사용자 NSS 계정을 기준으로 회사 수준에서 지난 3개월 동안 개설된 총 사례가 표시됩니다.테이블의 결과에는 선택한 보기와 관련된 사례가 반영됩니다.
- 관심 있는 열을 추가 또는 제거할 수 있으며 우선 순위 및 상태 등의 열 내용을 필터링할 수 있습니다. 다른 열은 정렬 기능만 제공합니다.

자세한 내용은 아래 단계를 참조하십시오.

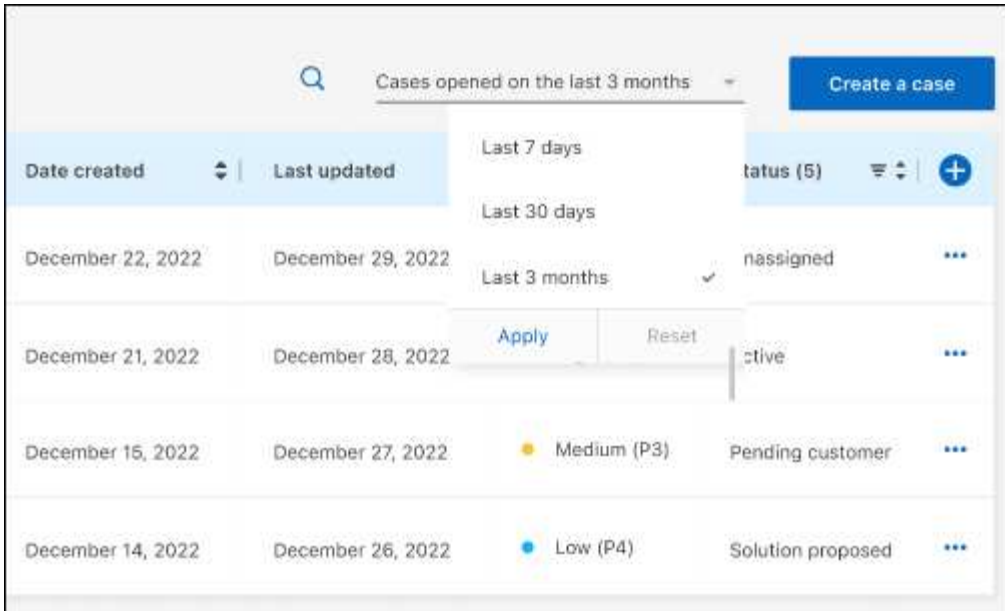
- 케이스 수준별로 케이스 메모를 업데이트하거나 아직 종결 또는 미결 종결 상태가 아닌 케이스를 종결할 수 있습니다.

### 단계

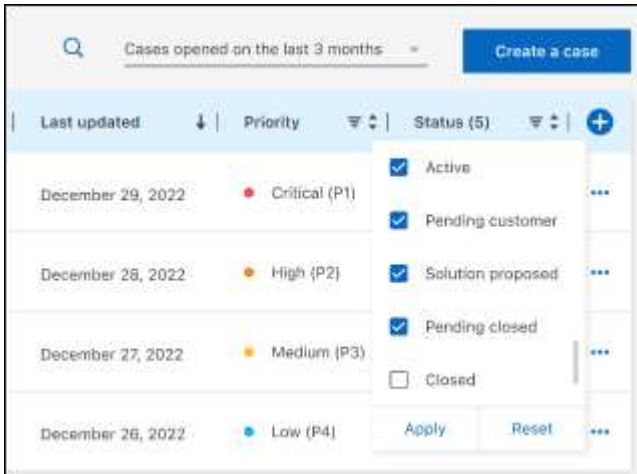
1. BlueXP에서 \* 도움말 > 지원 \* 을 선택합니다.
2. Case Management \* 를 선택하고 메시지가 표시되면 NSS 계정을 BlueXP에 추가합니다.

케이스 관리 \* 페이지에는 BlueXP 사용자 계정과 연결된 NSS 계정과 관련된 미해결 케이스가 표시됩니다. NSS 관리 \* 페이지 상단에 나타나는 것과 동일한 NSS 계정입니다.

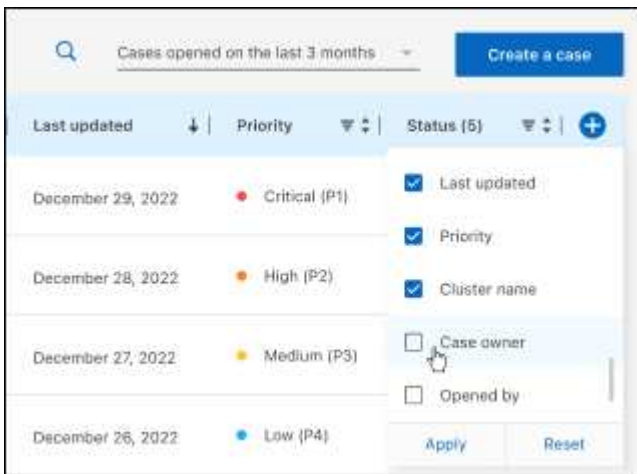
3. 필요한 경우 테이블에 표시되는 정보를 수정합니다.
  - 조직의 케이스 \* 에서 \* 보기 \* 를 선택하여 회사와 관련된 모든 케이스를 봅니다.
  - 정확한 날짜 범위를 선택하거나 다른 기간을 선택하여 날짜 범위를 수정합니다.



- 열의 내용을 필터링합니다.



- 를 선택하여 테이블에 표시되는 열을 변경합니다 + 표시할 열을 선택합니다.

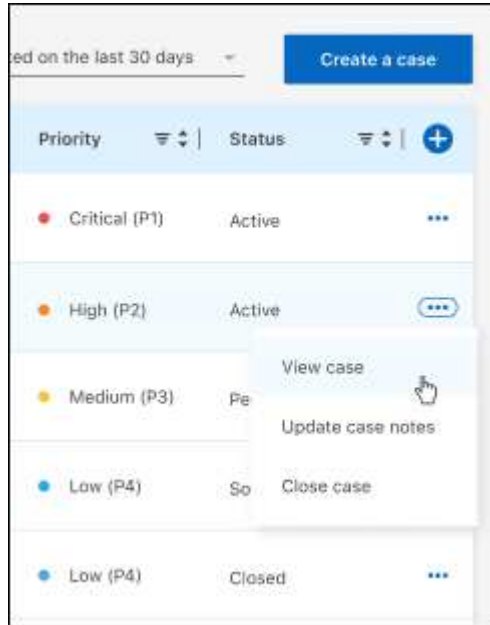


4. 를 선택하여 기존 케이스를 관리합니다 ... 사용 가능한 옵션 중 하나를 선택합니다.

- \* 사례 보기 \*: 특정 케이스에 대한 전체 세부 정보를 봅니다.
- \* 케이스 메모 업데이트 \*: 문제에 대한 추가 세부 정보를 제공하거나 \* 파일 업로드 \* 를 선택하여 최대 5개의 파일을 첨부할 수 있습니다.

첨부 파일은 파일당 25MB로 제한됩니다. txt, log, pdf, jpg/jpeg, rtf, DOC/docx, xls/xlsx 및 CSV.

- \* 케이스 종료 \*: 케이스를 종료하는 이유에 대한 세부 정보를 제공하고 \* 케이스 닫기 \* 를 선택합니다.





# 법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

## 저작권

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## 상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## 특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## 개인 정보 보호 정책

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## 오픈 소스

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이선스에 대한 정보를 제공합니다.

- "BlueXP에 대한 고지 사항"
- "Cloud Volumes ONTAP 중재자를 위한 고지 사항"
- "ONTAP에 대한 고지 사항"

## 저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 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 라이선스와 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 라이선스도 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 라이선스를 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 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

## 상표 정보

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