



# **ONTAP** 데이터를 백업 및 복원합니다

## Cloud Backup

NetApp  
May 13, 2022

# 목차

ONTAP 데이터를 백업 및 복원합니다 .....	1
클라우드 백업을 사용하여 ONTAP 클러스터 데이터를 보호합니다 .....	1
Cloud Volumes ONTAP 데이터를 Amazon S3에 백업 .....	8
Azure Blob 저장소에 Cloud Volumes ONTAP 데이터 백업 .....	16
Cloud Volumes ONTAP 데이터를 Google 클라우드 스토리지에 백업 .....	22
사내 ONTAP 데이터를 Amazon S3에 백업 .....	28
온프레미스 ONTAP 데이터를 Azure Blob 저장소에 백업 .....	41
사내 ONTAP 데이터를 Google 클라우드 스토리지로 백업 .....	50
사내 ONTAP 데이터를 StorageGRID에 백업 .....	58
ONTAP 시스템의 백업 관리 .....	64
백업 파일에서 ONTAP 데이터를 복원하는 중입니다 .....	79

# ONTAP 데이터를 백업 및 복원합니다

## 클라우드 백업을 사용하여 ONTAP 클러스터 데이터를 보호합니다

Cloud Backup은 ONTAP 클러스터 데이터의 보호 및 장기 아카이브를 위한 백업 및 복원 기능을 제공합니다. 백업은 거의 복구 또는 클론 복제에 사용되는 볼륨 Snapshot 복사본과 관계없이 퍼블릭 또는 프라이빗 클라우드 계정의 오브젝트 저장소에 자동으로 생성되고 저장됩니다.

필요한 경우 백업에서 전체 *volume* 또는 하나 이상의 *\_files\_*를 동일하거나 다른 작업 환경으로 복원할 수 있습니다.

### 피처

#### 백업 기능:

- 데이터 볼륨의 독립적인 복사본을 저비용 오브젝트 스토리지로 백업합니다.
- 클러스터의 모든 볼륨에 단일 백업 정책을 적용하거나 고유한 복구 지점 목표가 있는 볼륨에 다른 백업 정책을 할당합니다.
- 비용 절감을 위해 오래된 백업 파일을 아카이브 스토리지에 계층화(ONTAP 9.10.1 이상을 사용하는 경우 AWS 및 Azure에서 지원)
- 클라우드에서 클라우드로, 사내 시스템에서 퍼블릭 또는 프라이빗 클라우드로 백업
- Cloud Volumes ONTAP 시스템의 경우 백업이 다른 구독/계정 또는 다른 지역에 있을 수 있습니다.
- 사용 중인 AES-256비트 암호화 유틸리티 및 TLS 1.2 HTTPS 연결로 백업 데이터를 보호합니다.
- 클라우드 공급자의 기본 암호화 키를 사용하는 대신, 고객이 관리하는 데이터 암호화 키를 사용하십시오.
- 단일 볼륨에 대해 최대 4,000개의 백업을 지원합니다.

#### 복원 기능:

- 특정 시점에서 데이터 복원
- 볼륨 또는 개별 파일을 소스 시스템 또는 다른 시스템으로 복원합니다.
- 다른 구독/계정을 사용하거나 다른 지역에 있는 작업 환경으로 데이터를 복원합니다.
- 블록 수준에서 데이터를 복원하여 원래 ACL을 보존하면서 데이터를 사용자가 지정한 위치에 직접 배치합니다.
- 단일 파일 복원을 위한 개별 파일을 선택할 수 있는 탐색 가능한 검색 가능한 파일 카탈로그

### 지원되는 ONTAP 작업 환경 및 오브젝트 스토리지 공급자

Cloud Backup을 사용하면 다음과 같은 작업 환경에서 ONTAP 볼륨을 다음 퍼블릭 및 프라이빗 클라우드 공급자의 오브젝트 스토리지로 백업할 수 있습니다.

소스 작업 환경	백업 파일 대상
AWS의 Cloud Volumes ONTAP	Amazon S3
Azure의 Cloud Volumes ONTAP	Azure Blob
Google의 Cloud Volumes ONTAP	Google 클라우드 스토리지

소스 작업 환경	백업 파일 대상
사내 ONTAP 시스템	Amazon S3 Azure Blob Google 클라우드 스토리지 NetApp StorageGRID

ONTAP 백업 파일에서 다음 작업 환경으로 볼륨 또는 개별 파일을 복원할 수 있습니다.

백업 파일	대상 작업 환경	
* 위치 *	* 볼륨 복원 *	* 파일 복원 *
Amazon S3	Cloud Volumes ONTAP를 사내의 AWS ONTAP 시스템에 설치하고	Cloud Volumes ONTAP를 사내의 AWS ONTAP 시스템에 설치하고
Azure Blob	Azure 사내 ONTAP 시스템의 Cloud Volumes ONTAP	Azure 사내 ONTAP 시스템의 Cloud Volumes ONTAP
Google 클라우드 스토리지	Google 사내 ONTAP 시스템의 Cloud Volumes ONTAP	Google 사내 ONTAP 시스템의 Cloud Volumes ONTAP
NetApp StorageGRID를 참조하십시오	사내 ONTAP 시스템	

"사내 ONTAP 시스템"을 지칭할 때 FAS, AFF 및 ONTAP Select 시스템이 포함됩니다.

## 비용

ONTAP 시스템에서 Cloud Backup을 사용할 경우 리소스 비용과 서비스 요금의 두 가지 유형이 있습니다.

- 리소스 비용 \*

클라우드 공급자에게 오브젝트 스토리지 용량과 클라우드 내 가상 머신/인스턴스 실행에 대한 리소스 비용이 지급됩니다.

- 백업의 경우 클라우드 공급자에게 오브젝트 스토리지 비용을 지불하십시오.

Cloud Backup은 소스 볼륨의 스토리지 효율성을 유지하므로 데이터\_after\_ONTAP 효율성(중복제거 및 압축이 적용된 후 더 적은 양의 데이터)에 대한 클라우드 공급자 개체 스토리지 비용을 지불하게 됩니다.

- Browse & Restore를 사용한 파일 복원의 경우 Restore 인스턴스가 실행 중일 때만 클라우드 공급자에 컴퓨팅 비용을 지불합니다.

인스턴스는 복원할 개별 파일을 찾기 위해 백업 파일을 검색할 때만 실행됩니다. 비용 절감을 위해 사용하지 않을 때는 인스턴스가 해제됩니다.

- AWS에서 복구 인스턴스는 에서 실행됩니다 **"m5n.xlarge 인스턴스"** CPU 4개, 16GB 메모리 및 EBS 전용 인스턴스 스토리지 포함. 운영 체제 이미지는 Amazon Linux 2입니다.

m5n.xlarge 인스턴스를 사용할 수 없는 지역에서는 대신 M5.xlarge 인스턴스에서 Restore가 실행됩니다.

- Azure에서 Restore virtual machine은 에서 실행됩니다 **"Standard\_D4s\_v3 VM"** CPU 4개, 16GB 메모리 및 32GiB 디스크 운영 체제 이미지는 CentOS 7.5)입니다.

인스턴스의 이름은 \_Cloud-Restore-instance\_이며 연결된 계정 ID가 있습니다. 예: \_클라우드 - 복원 -

- Browse & Restore를 사용한 볼륨 복원의 경우 별도의 인스턴스 또는 가상 머신이 필요하지 않으므로 비용이 들지 않습니다.
- 검색 및 복원을 사용한 볼륨 또는 파일 복원의 경우, 클라우드 공급자가 특정 리소스를 프로비저닝하며 검색 요청에 의해 스캔된 데이터 양과 관련된 TiB 비용이 있습니다.
  - AWS에서는 "[아마존 애써나](#)" 및 "[AWS 글루](#)" 리소스가 새로운 S3 버킷에 구축됩니다.
  - Google에서는 새로운 버킷이 배포되고 "[Google Cloud BigQuery 서비스](#)" 계정/프로젝트 수준에서 프로비저닝됩니다.
- 아카이브 스토리지로 이동한 백업 파일(ONTAP 9.10.1 이상을 사용하는 경우 AWS에서 지원)에서 볼륨 데이터를 복구해야 하는 경우 클라우드 공급자로부터 추가 Per-GiB 검색 비용 및 요청당 요금이 부과됩니다.
- 서비스 요금 \*

서비스 비용은 NetApp에 지불되며 이러한 백업에서 \_create\_backups와 to\_restore\_volumes 또는 파일에 대한 비용을 모두 부담합니다. 오브젝트 스토리지에 백업된 ONTAP 볼륨의 소스 논리적 사용 용량(\_Before\_ONTAP 효율성)을 사용하여 계산한, 자신이 보호하는 데이터에 대해서만 비용을 지불합니다. 이 용량을 FETB(Front-End Terabytes)라고도 합니다.

백업 서비스에 대한 비용을 지불하는 방법에는 세 가지가 있습니다. 첫 번째 옵션은 클라우드 공급자를 구독하는 것입니다. 구독하면 매월 요금을 지불할 수 있습니다. 두 번째 옵션은 연간 계약을 얻는 것입니다. 이 계약은 AWS를 통해서만 가능합니다. 세 번째 옵션은 NetApp에서 직접 라이선스를 구매하는 것입니다. 를 읽습니다 [라이선싱](#) 섹션을 참조하십시오.

## 라이선싱

Cloud Backup은 세 가지 라이선스 옵션, 즉 PAYGO(Pay As You Go) 구독, AWS Marketplace의 연간 계약, BYOL(Bring Your Own License) 옵션으로 제공됩니다. PAYGO에 가입하면 30일 무료 평가판을 사용할 수 있습니다.

### 용량제 구독

Cloud Backup은 용량제 모델로 소비 기반 라이선스를 제공합니다. 클라우드 공급자의 마켓플레이스를 구독한 후, 백업된 데이터의 경우 GiB당 비용을 지불하면 됩니다. 이러한 데이터를 미리 지불할 필요가 없습니다. 클라우드 공급자가 월별 요금을 청구합니다.

["선불 종량제 구독을 설정하는 방법을 알아보십시오"](#).

### 연간 계약(AWS만 해당)

AWS Marketplace에서 12개월, 24개월 또는 36개월 조건에 두 가지 연간 계약을 사용할 수 있습니다.

- Cloud Volumes ONTAP 데이터와 사내 ONTAP 데이터를 백업할 수 있는 '클라우드 백업' 계획
- Cloud Volumes ONTAP와 클라우드 백업을 번들로 제공할 수 있는 "CVO Professional" 계획. 여기에는 이 라이선스에 대해 청구된 Cloud Volumes ONTAP 볼륨에 대한 무제한 백업이 포함됩니다(백업 용량은 라이선스에 포함되지 않음).

["연간 AWS 계약을 설정하는 방법에 대해 알아보십시오"](#).

각자 보유한 라이선스를 가지고 오시기 바랍니다

BYOL은 1TiB 단위로 기간 기반(12, 24 또는 36개월) \_ 및 \_ 용량 기반 예를 들어, 1년, 최대 용량(10TiB)에 대해 서비스 사용을 위해 NetApp에 비용을 지불합니다.

Cloud Manager Digital Wallet 페이지에 입력한 일련 번호를 통해 서비스를 활성화할 수 있습니다. 두 제한 중 하나에 도달하면 라이선스를 갱신해야 합니다. Backup BYOL 라이선스는 와 관련된 모든 소스 시스템에 적용됩니다 ["Cloud Manager 계정"](#).

["BYOL 라이선스 관리 방법에 대해 알아보십시오"](#).

## Cloud Backup의 작동 방식

Cloud Volumes ONTAP 또는 사내 ONTAP 시스템에서 클라우드 백업을 활성화하면 서비스가 데이터의 전체 백업을 수행합니다. 볼륨 스냅샷은 백업 이미지에 포함되지 않습니다. 초기 백업 후에는 모든 추가 백업이 증분 백업되므로 변경된 블록과 새 블록만 백업됩니다. 이렇게 하면 네트워크 트래픽이 최소로 유지됩니다.

대부분의 경우 모든 백업 작업에 Cloud Manager UI를 사용합니다. 그러나 ONTAP 9.9.1부터 ONTAP 시스템 관리자를 사용하여 사내 ONTAP 클러스터의 볼륨 백업 작업을 시작할 수 있습니다. ["System Manager를 사용하여 Cloud Backup을 사용하여 볼륨을 클라우드에 백업하는 방법을 알아보십시오."](#)



백업 파일을 관리하거나 변경하기 위해 클라우드 제공업체 환경에서 직접 수행한 작업은 파일을 손상시킬 수 있으며 지원되지 않는 구성을 초래할 수 있습니다.

다음 이미지는 각 구성 요소 간의 관계를 보여줍니다.



백업이 상주하는 위치입니다

백업 복사본은 Cloud Manager에서 클라우드 계정에 만드는 오브젝트 저장소에 저장됩니다. 클러스터/작업 환경당 하나의 오브젝트 저장소가 있으며 Cloud Manager에서는 오브젝트 저장소의 이름을 "NetApp-backup-clusteruuid"로 지정합니다. 이 오브젝트 저장소를 삭제하지 마십시오.

- AWS에서 Cloud Manager는 를 지원합니다 **"Amazon S3 블록 공용 액세스 기능입니다"** S3 버킷에서.
- Azure에서 Cloud Manager는 Blob 컨테이너용 스토리지 계정이 있는 새 리소스 그룹 또는 기존 리소스 그룹을 사용합니다. 클라우드 관리자 **"BLOB 데이터에 대한 공개 액세스를 차단합니다"** 기본적으로 사용됩니다.
- GCP에서 Cloud Manager는 Google Cloud Storage 버킷을 위한 스토리지 계정이 있는 신규 또는 기존 프로젝트를 사용합니다.
- StorageGRID에서 Cloud Manager는 오브젝트 저장소 버킷에 기존 스토리지 계정을 사용합니다.

향후 클러스터의 대상 오브젝트 저장소를 변경하려면 가 필요합니다 **"작업 환경에 대한 클라우드 백업 등록을 취소합니다"**를 선택한 다음 새로운 클라우드 공급자 정보를 사용하여 Cloud Backup을 설정합니다.

지원되는 스토리지 클래스 또는 액세스 계층

- AWS에서는 백업이 **\_Standard\_storage** 클래스에서 시작되고 30일 후에 **\_Standard - Infrequent Access\_storage** 클래스로 전환됩니다.

클러스터에서 ONTAP 9.10.1 이상을 사용하는 경우 추가 비용 최적화를 위해 일정 일 후에 이전 백업을 **\_S3**

Glacier\_또는 \_S3 Glacier Deep Archive\_storage에 계층화하도록 선택할 수 있습니다. "[AWS 아카이브 스토리지에 대해 자세히 알아보십시오](#)".

- Azure에서 백업은 \_Cool\_access 계층과 연결됩니다.

클러스터에서 ONTAP 9.10.1 이상을 사용하는 경우 추가 비용 최적화를 위해 일정 일 후에 이전 백업을 \_Azure Archive\_storage에 계층화하도록 선택할 수 있습니다. "[Azure 아카이브 스토리지에 대해 자세히 알아보십시오](#)".

- GCP에서 백업은 기본적으로 \_Standard\_storage 클래스와 연결됩니다.

또한 더 낮은 cost\_Nearline\_storage 클래스 또는 \_Coldline\_or\_Archive\_storage 클래스를 사용할 수 있습니다. Google 항목을 참조하십시오 "[스토리지 클래스](#)" 스토리지 클래스 변경에 대한 자세한 내용은 를 참조하십시오.

- StorageGRID에서 백업은 \_Standard\_storage 클래스와 연결됩니다.

## 클러스터당 사용자 지정 가능한 백업 스케줄 및 보존 설정

작업 환경에 Cloud Backup을 활성화하면 처음에 선택한 모든 볼륨이 사용자가 정의한 기본 백업 정책을 사용하여 백업됩니다. RPO(복구 지점 목표)가 다른 특정 볼륨에 서로 다른 백업 정책을 할당하려면 해당 클러스터에 대한 추가 정책을 생성한 다음 해당 정책을 다른 볼륨에 할당할 수 있습니다.

모든 볼륨의 시간별, 일별, 주별 및 월별 백업을 조합하여 선택할 수 있습니다. 또한 3개월, 1년 및 7년 동안 백업 및 보존을 제공하는 시스템 정의 정책 중 하나를 선택할 수도 있습니다. 이러한 정책은 다음과 같습니다.

백업 정책 이름입니다	간격당 백업...			최대 백업
	* 매일 *	* 매주 *	* 매월 *	
Netapp3개월 보존	30	13	3	46
Netapp1YearRetention	30	13	12	55
Netapp7YearsRetention	30	53	84	167

ONTAP System Manager 또는 ONTAP CLI를 사용하여 클러스터에서 생성한 백업 보호 정책도 선택 사항으로 표시됩니다.

범주 또는 간격에 대한 최대 백업 수에 도달하면 오래된 백업이 제거되므로 항상 최신 백업이 유지됩니다.

참고: 이 작업은 수행할 수 있습니다 "[볼륨의 필요 시 백업을 생성합니다](#)" 예약된 백업에서 생성된 백업 파일 외에 언제든지 Backup Dashboard에서 백업 파일을 생성할 수 있습니다.



데이터 보호 볼륨의 백업 보존 기간은 소스 SnapMirror 관계에 정의된 보존 기간과 동일합니다. 원하는 경우 API를 사용하여 변경할 수 있습니다.

## FabricPool 계층화 정책 고려 사항

백업하는 볼륨이 FabricPool 애그리게이트에 있고 '없음' 이외의 할당된 정책이 있을 때 알아야 할 몇 가지 사항이 있습니다.

- FabricPool 계층 볼륨의 첫 번째 백업을 수행하려면 오브젝트 저장소에서 모든 로컬 및 모든 계층화된 데이터를 읽어야 합니다. 백업 작업에서는 오브젝트 스토리지의 콜드 데이터를 "재가열"하지 않습니다.

이 경우 클라우드 공급자로부터 데이터를 읽는 데 드는 비용이 1회 증가할 수 있습니다.



- 후속 백업은 증분 백업이므로 이 효과가 없습니다.
- 처음 생성될 때 볼륨에 계층화 정책이 할당되면 이 문제가 표시되지 않습니다.
- 모든 계층화 정책을 볼륨에 할당하기 전에 백업의 영향을 고려하십시오. 데이터는 즉시 계층화되므로 Cloud Backup은 로컬 계층이 아닌 클라우드 계층에서 데이터를 읽습니다. 동시 백업 작업은 네트워크 링크를 클라우드 오브젝트 저장소로 공유하기 때문에 네트워크 리소스가 포화 상태가 되면 성능이 저하될 수 있습니다. 이 경우 이러한 유형의 네트워크 포화를 줄이기 위해 여러 개의 네트워크 인터페이스(LIF)를 사전에 구성할 수 있습니다.

## 지원되는 볼륨

Cloud Backup은 FlexVol 읽기-쓰기 볼륨 및 SnapMirror 데이터 보호(DP) 대상 볼륨을 지원합니다.

FlexGroup 볼륨 및 SnapLock 볼륨은 현재 지원되지 않습니다.

## 제한 사항

- 이전 백업 파일을 아카이브 스토리지에 계층화하려면 클러스터에서 ONTAP 9.10.1 이상(현재 AWS 및 Azure에서 지원됨)이 실행되고 있어야 합니다. 아카이브 스토리지에 있는 백업 파일에서 볼륨을 복원하려면 대상 클러스터에서 ONTAP 9.10.1 이상이 실행되고 있어야 합니다.
- 정책에 할당된 볼륨이 없을 때 백업 정책을 생성하거나 편집할 때 유지되는 백업 수는 최대 1018개가 될 수 있습니다. 이 문제를 해결하려면 정책을 생성할 백업 수를 줄일 수 있습니다. 그런 다음 정책에 볼륨을 할당한 후 정책을 편집하여 최대 4000개의 백업을 생성할 수 있습니다.
- DP(데이터 보호) 볼륨을 백업할 때 다음 SnapMirror 레이블과의 관계는 클라우드에 백업되지 않습니다.
  - app\_consistent
  - ALL\_SOURCE\_SNAPSHOT
- SVM-DR 볼륨 백업은 다음 제한 사항으로 지원됩니다.
  - 백업은 ONTAP 보조 백업에서만 지원됩니다.
  - 볼륨에 적용된 스냅샷 정책은 매일, 매주, 매월 등 Cloud Backup에서 인식하는 정책 중 하나여야 합니다. 기본 "sm\_created" 정책(\* 미러 모든 스냅샷 \* 에 사용됨) 가 인식되지 않으며 백업할 수 있는 볼륨 목록에 DP 볼륨이 표시되지 않습니다.
- 지금 백업 \* 버튼을 사용한 임시 볼륨 백업은 데이터 보호 볼륨에서 지원되지 않습니다.
- SM-BC 구성은 지원되지 않습니다.
- MCC(MetroCluster) 백업은 ONTAP 2차 백업에서만 지원됩니다. MCC > SnapMirror > ONTAP > 클라우드 백업 > 오브젝트 스토리지.
- ONTAP는 단일 볼륨에서 여러 오브젝트 저장소로 이루어진 SnapMirror 관계를 지원하지 않습니다. 따라서 Cloud Backup에서는 이 구성을 지원하지 않습니다.
- 오브젝트 저장소의 WORM/Compliance 모드는 지원되지 않습니다.

## 단일 파일 복구 제한 사항

이러한 제한 사항은 특별히 호출되지 않는 한 검색 및 복원 및 찾아보기 및 복원 방법 모두에 적용됩니다.

- Browse & Restore는 한 번에 최대 100개의 개별 파일을 복원할 수 있습니다.
- Search & Restore는 한 번에 하나의 파일을 복원할 수 있습니다.
- 현재 폴더/디렉토리 복원을 지원하지 않습니다.

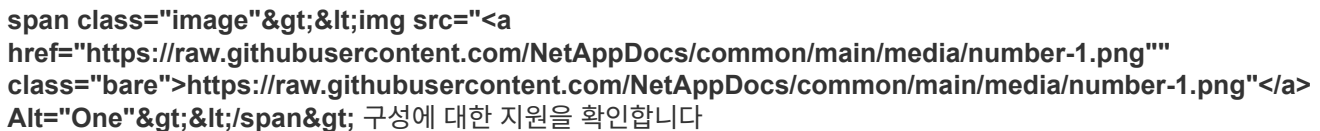
- 복원 중인 파일은 대상 볼륨의 언어와 동일한 언어를 사용해야 합니다. 언어가 동일하지 않으면 오류 메시지가 나타납니다.
- 서로 다른 서버넷에서 서로 다른 클라우드 관리자와 동일한 계정을 사용하는 경우 파일 레벨 복원이 지원되지 않습니다.
- 백업 파일이 아카이브 스토리지에 있는 경우 개별 파일을 복원할 수 없습니다.

## Cloud Volumes ONTAP 데이터를 Amazon S3에 백업

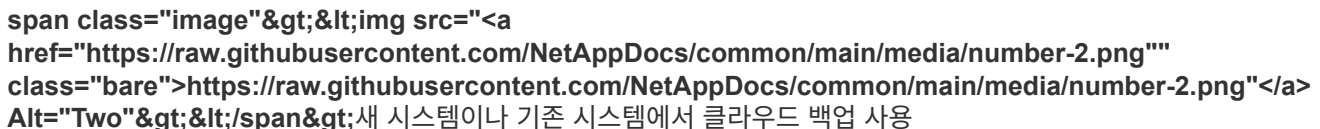
몇 가지 단계를 완료하여 Cloud Volumes ONTAP에서 Amazon S3로 데이터 백업을 시작하십시오.

### 빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션으로 스크롤하여 자세한 내용을 확인하십시오.

 구성에 대한 지원을 확인합니다

- AWS에서 Cloud Volumes ONTAP 9.6 이상을 실행하고 있습니다.
- 백업이 위치할 스토리지 공간에 대한 유효한 클라우드 공급자 가입이 있습니다.
- 에 가입했습니다 "Cloud Manager Marketplace 백업 오퍼링", 및 "AWS 연간 계약"또는 을(를) 구입한 경우 "활성화합니다" Cloud Backup BYOL 라이선스는 NetApp에서 제공
- Cloud Manager Connector에 사용 권한을 제공하는 IAM 역할에는 최신 의 S3 권한이 포함됩니다 "Cloud Manager 정책".

 새 시스템이나 기존 시스템에서 클라우드 백업 사용

- 새 시스템: 작업 환경 마법사에서 기본적으로 클라우드 백업이 설정됩니다. 옵션을 활성 상태로 유지해야 합니다.
- 기존 시스템: 작업 환경을 선택하고 오른쪽 패널의 백업 및 복원 서비스 옆에 있는 \* 활성화 \* 를 클릭한 다음 설정 마법사를 따릅니다.



AWS 계정 및 백업을 생성할 지역을 선택합니다. 기본 Amazon S3 암호화 키를 사용하는 대신 데이터 암호화에 대해 자체 고객 관리 키를 선택할 수도 있습니다.

### Provider Settings

#### Provider Information

AWS Account

AWS Access Key

AWS Secret Key

#### Location & Connectivity

Region

Encryption ?

Encryption Key Type: AWS SSE-S3 [Change Key](#)

기본 정책은 매일 볼륨을 백업하고 각 볼륨의 최근 30개 백업 복사본을 유지합니다. 시간별, 일별, 주별 또는 월별 백업으로 변경하거나 더 많은 옵션을 제공하는 시스템 정의 정책 중 하나를 선택합니다. 보존할 백업 복사본의 수를 변경할 수도 있습니다.

백업은 기본적으로 S3 Standard 스토리지에 저장됩니다. 클러스터에서 ONTAP 9.10.1 이상을 사용하는 경우 추가 비용 최적화를 위해 일정 일 후에 S3 Glacier 또는 S3 Glacier Deep Archive 스토리지에 백업을 계층화하도록 선택할 수 있습니다.

### Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule** ☒ Create a New Policy ☐ Select an Existing Policy

☐ Hourly  
☒ Daily  
☐ Weekly  
☐ Monthly

Number of backups to retain

Number of backups to retain

Number of backups to retain

Number of backups to retain

**Archival Policy**

Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.

☒ Tier Backups to Archival

Archive after (Days)

Storage Class

S3 Glacier

S3 Glacier

S3 Glacier Deep Archive

**S3 Bucket**

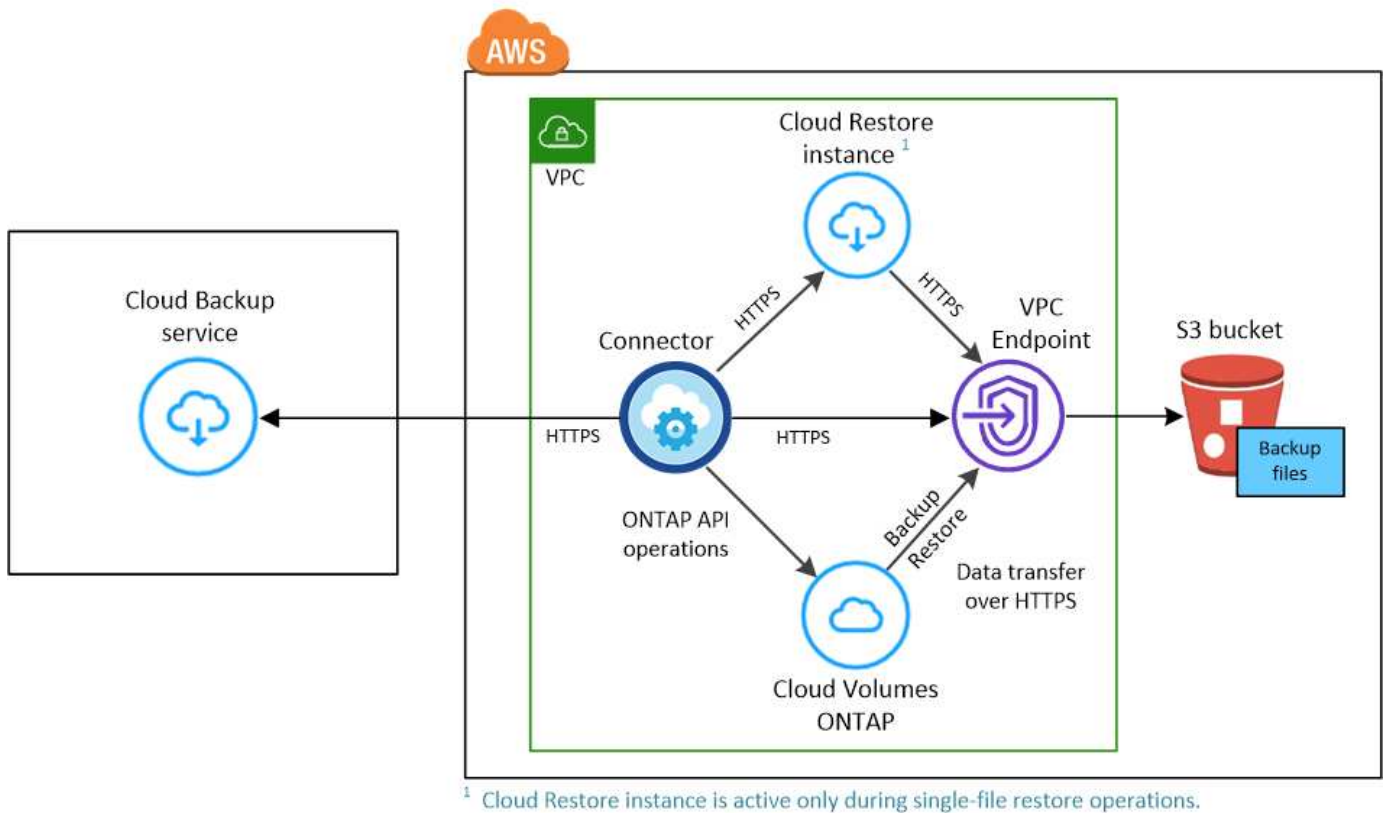
Cloud Manager will create the S3 bucket for you.

Select Volumes(볼륨 선택) 페이지의 기본 백업 정책을 사용하여 백업할 볼륨을 식별합니다. 특정 볼륨에 서로 다른 백업 정책을 할당하려면 추가 정책을 생성한 후 나중에 볼륨에 적용할 수 있습니다.

## 요구 사항

S3에 볼륨을 백업하기 전에 다음 요구 사항을 읽고 지원되는 구성이 있는지 확인합니다.

다음 이미지는 각 구성 요소와 이러한 구성 요소 간에 준비해야 하는 연결을 보여 줍니다.



Cloud Restore 인스턴스가 클라우드에 배포되면 Connector와 동일한 서브넷에 위치합니다.

#### 지원되는 **ONTAP** 버전

Cloud Volumes ONTAP 9.6 이상

#### 라이선스 요구 사항

Cloud Backup PAYGO 라이선스의 경우, Cloud Volumes ONTAP 및 클라우드 백업을 구축할 수 있는 AWS 마켓플레이스에서 Cloud Manager 구독을 지원합니다. 다음 작업을 수행해야 합니다 "[이 Cloud Manager 구독을 신청하십시오](#)" Cloud Backup을 활성화하기 전에, Cloud Backup에 대한 청구는 이 구독을 통해 이루어집니다.

Cloud Volumes ONTAP 데이터와 사내 ONTAP 데이터를 모두 백업할 수 있는 연간 계약이 체결되어 있으면 예 가입해야 합니다 "[AWS 마켓플레이스 페이지를 참조하십시오](#)" 그리고 나서 "[가입 정보를 AWS 자격 증명과 연결합니다](#)".

Cloud Volumes ONTAP 및 클라우드 백업을 번들로 제공하기 위한 연간 계약의 경우 Cloud Volumes ONTAP 작업 환경을 생성할 때 연간 계약을 설정해야 합니다. 이 옵션을 사용하면 온프레미스 데이터를 백업할 수 없습니다.

Cloud Backup BYOL 라이선스의 경우, 라이선스 기간 및 용량 동안 서비스를 사용할 수 있도록 지원하는 NetApp의 일련 번호가 필요합니다. "[BYOL 라이선스 관리 방법에 대해 알아보십시오](#)".

그리고 백업이 위치할 스토리지 공간을 위한 AWS 계정이 있어야 합니다.

#### 지원되는 **AWS** 영역

Cloud Backup은 모든 AWS 지역에서 지원됩니다 "[Cloud Volumes ONTAP가 지원되는 경우](#)" AWS GovCloud 지역 포함.

다른 **AWS** 계정에서 백업을 생성하기 위해 필요한 설정

기본적으로 백업은 Cloud Volumes ONTAP 시스템에 사용되는 계정과 동일한 계정을 사용하여 생성됩니다. 백업에 다른 AWS 계정을 사용하려면 다음을 수행해야 합니다 "[AWS 포털에 로그인하여 두 계정을 연결합니다](#)".

데이터 암호화에 대해 고객이 관리하는 키를 사용하는 데 필요한 정보입니다

기본 Amazon S3 암호화 키를 사용하는 대신 활성화 마법사에서 데이터 암호화에 대해 고객이 관리하는 키를 직접 선택할 수 있습니다. 이 경우 암호화 관리 키가 이미 설정되어 있어야 합니다. "[자신의 키를 사용하는 방법을 확인하십시오](#)".

**AWS** 백업 권한이 필요합니다

Cloud Manager에 사용 권한을 제공하는 IAM 역할에는 최신 버전의 S3 권한이 포함되어야 합니다 "[Cloud Manager 정책](#)".

다음은 정책의 특정 사용 권한입니다.

```

{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutEncryptionConfiguration",
        "athena:StartQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryExecution",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:CreateDatabase",
        "glue:GetPartitions",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition"
    ],
    "Resource": [
        "arn:aws:s3:::netapp-backup-*"
    ]
},

```

버전 3.9.15 이상을 사용하여 Connector를 배포한 경우 이러한 권한은 이미 IAM 역할의 일부여야 합니다. 그렇지 않으면 누락된 권한을 추가해야 합니다. 특히 검색 및 복원에 필요하므로 "Athena" 및 "GLUE" 권한이 필요합니다.

#### **AWS 복구 권한이 필요합니다**

Cloud Manager가 Browse & Restore 작업을 위해 Cloud Restore 인스턴스를 시작, 중지 및 종료할 수 있도록 권한을 제공하는 IAM 역할에 필요한 EC2 권한은 다음과 같습니다.

```
"Action": [
    "ec2:DescribeInstanceTypeOfferings",
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances"
]
```

## AWS 구축에 필요한 아웃바운드 인터넷 액세스

클라우드 복원 인스턴스에는 아웃바운드 인터넷 액세스가 필요합니다. 가상 또는 물리적 네트워크에서 인터넷 액세스에 프록시 서버를 사용하는 경우 인스턴스에 다음 끝점에 연결할 수 있는 아웃바운드 인터넷 액세스 권한이 있는지 확인합니다.

엔드포인트	목적
<a href="http://amazonlinux.us-east-1.amazonaws.com/2/extras/docker/stable/x86_64/4bf88ee77c395ffe1e0c3ca68530dfb3a683ec65a4a1ce9c0ff394be50e922b2/">http://amazonlinux.us-east-1.amazonaws.com/2/extras/docker/stable/x86_64/4bf88ee77c395ffe1e0c3ca68530dfb3a683ec65a4a1ce9c0ff394be50e922b2/</a>	클라우드 복원 인스턴스 AMI용 CentOS 패키지.
<a href="https://download.docker.com/linux/centos/docker-ce.repo">https://download.docker.com/linux/centos/docker-ce.repo</a> 으로 문의하십시오	Docker Engine 패키지를 제공합니다.
<a href="http://cloudmanagerinfraprod.azurecr.io">http://cloudmanagerinfraprod.azurecr.io</a> <a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a> 으로 문의하십시오	클라우드 복원 인스턴스 이미지 리포지토리.

## 새로운 시스템에서 Cloud Backup을 활성화합니다

클라우드 백업은 작업 환경 마법사에서 기본적으로 설정됩니다. 옵션을 활성 상태로 유지해야 합니다.

을 참조하십시오 ["AWS에서 Cloud Volumes ONTAP 실행"](#) Cloud Volumes ONTAP 시스템 생성에 대한 요구 사항 및 세부 정보를 확인하십시오.

단계

1. Create Cloud Volumes ONTAP \* 를 클릭합니다.
2. 클라우드 공급자로 Amazon Web Services를 선택하고 단일 노드 또는 HA 시스템을 선택합니다.
3. 세부 정보 및 자격 증명 페이지를 입력합니다.
4. 서비스 페이지에서 서비스를 활성화된 상태로 두고 \* 계속 \* 을 클릭합니다.



5. 마법사의 페이지를 완료하여 시스템을 구축합니다.

Cloud Backup은 시스템에서 활성화되어 매일 볼륨을 백업하며 최근 30개의 백업 복사본을 보존합니다.

가능합니다 "볼륨에 대한 백업을 시작 및 중지하거나 백업 일정을 변경합니다". 또한 가능합니다 "백업 파일에서 전체 볼륨 또는 개별 파일을 복원합니다" AWS의 Cloud Volumes ONTAP 시스템 또는 사내 ONTAP 시스템으로 전환

## 기존 시스템에서 **Cloud Backup** 활성화

작업 환경에서 바로 언제든지 Cloud Backup을 사용할 수 있습니다.

단계

1. 작업 환경을 선택하고 오른쪽 패널에서 백업 및 복원 서비스 옆에 있는 \* 활성화 \* 를 클릭합니다.



2. 제공업체 세부 정보를 선택하고 \* 다음 \* 을 클릭합니다.

- a. 백업을 저장하는 데 사용되는 AWS 계정입니다. 이 계정은 Cloud Volumes ONTAP 시스템이 상주하는 계정과 다를 수 있습니다.

백업에 다른 AWS 계정을 사용하려면 다음을 수행해야 합니다 "AWS 포털에 로그인하여 두 계정을 연결합니다".

- b. 백업이 저장될 영역입니다. 이 영역은 Cloud Volumes ONTAP 시스템이 있는 지역과 다를 수 있습니다.
- c. 기본 Amazon S3 암호화 키를 사용하거나 AWS 계정에서 직접 고객 관리 키를 선택하여 데이터 암호화를 관리할지 여부를 결정합니다. ("자신의 암호화 키를 사용하는 방법을 알아봅니다")를 클릭합니다.

3. 기본 백업 정책 세부 정보를 입력하고 \* 다음 \* 을 클릭합니다.

- a. 백업 스케줄을 정의하고 보존할 백업 수를 선택합니다. "선택할 수 있는 기존 정책 목록을 봅니다".
- b. ONTAP 9.10.1 이상을 사용하는 경우 추가 비용 최적화를 위해 일정 일 후에 S3 Glacier 또는 S3 Glacier Deep Archive 스토리지에 백업을 계층화하도록 선택할 수 있습니다. "아카이브 계층 사용에 대해 자세히 알아보십시오".



### Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule** ☒ Create a New Policy ☐ Select an Existing Policy

☐ Hourly

Number of backups to retain

24

☒ Daily

Number of backups to retain

30

☐ Weekly

Number of backups to retain

52

☐ Monthly

Number of backups to retain

12

---

**Archival Policy**

Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.

☒ Tier Backups to Archival

Archive after (Days)

Storage Class

30

S3 Glacier  
 S3 Glacier  
 S3 Glacier Deep Archive

---

**S3 Bucket**

Cloud Manager will create the S3 bucket for you. Wizard

4. Select Volumes(볼륨 선택) 페이지의 기본 백업 정책을 사용하여 백업할 볼륨을 선택합니다. 특정 볼륨에 서로 다른 백업 정책을 할당하려는 경우 추가 정책을 생성하여 나중에 해당 볼륨에 적용할 수 있습니다.

### Select Volumes

57 Volumes Q

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 <small>On</small>	DP	SVM_Name_2	0.25 TB	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	⊖ Not Active

☒ Automatically back up future volumes on all storage VMs with the selected backup policy ⓘ

- 모든 볼륨을 백업하려면 제목 행(☒ Volume Name)를 클릭합니다.
  - 개별 볼륨을 백업하려면 각 볼륨에 대한 확인란을 선택합니다(☒ Volume\_1)를 클릭합니다.
5. 나중에 추가된 모든 볼륨에 백업을 사용하려면 "Automatically back up future volumes..." 확인란을 선택하기만 하면 됩니다. 이 설정을 비활성화하면 이후 볼륨에 대해 백업을 수동으로 활성화해야 합니다.
6. 백업 활성화 \* 를 클릭하면 선택한 각 볼륨의 초기 백업이 시작됩니다.

Cloud Backup은 선택한 각 볼륨의 초기 백업을 시작하고, 백업 상태를 모니터링할 수 있도록 Volume Backup

Dashboard가 표시됩니다.

가능합니다 "볼륨에 대한 백업을 시작 및 중지하거나 백업 일정을 변경합니다". 또한 가능합니다 "백업 파일에서 전체 볼륨 또는 개별 파일을 복원합니다" AWS의 Cloud Volumes ONTAP 시스템 또는 사내 ONTAP 시스템으로 전환

## Azure Blob 저장소에 Cloud Volumes ONTAP 데이터 백업

Cloud Volumes ONTAP에서 Azure Blob 저장소로 데이터 백업을 시작하려면 몇 가지 단계를 완료하십시오.

### 빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션으로 스크롤하여 자세한 내용을 확인하십시오.

<https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-1.png>  
Alt="One" 구성에 대한 지원을 확인합니다

- Azure에서 Cloud Volumes ONTAP 9.7P5 이상을 실행하고 있습니다.
- 백업이 위치할 스토리지 공간에 대한 유효한 클라우드 공급자 가입이 있습니다.
- 에 가입했습니다 "Cloud Manager Marketplace 백업 오퍼링" 또는 을(를) 구입한 경우 "활성화합니다" Cloud Backup BYOL 라이선스는 NetApp에서 제공

<https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-2.png>  
Alt="Two" 새 시스템이나 기존 시스템에서 클라우드 백업 사용

- 새 시스템: 작업 환경 마법사에서 기본적으로 클라우드 백업이 설정됩니다. 옵션을 활성 상태로 유지해야 합니다.
- 기존 시스템: 작업 환경을 선택하고 오른쪽 패널의 백업 및 복원 서비스 옆에 있는 \* 활성화 \* 를 클릭한 다음 설정 마법사를 따릅니다.



공급자 구독 및 지역을 선택하고 새 리소스 그룹을 만들지 기존 리소스 그룹을 사용할지 여부를 선택합니다. 또한 기본 Microsoft 관리 암호화 키를 사용하는 대신 고객이 관리하는 데이터 암호화 키를 직접 선택할 수도 있습니다.

### Provider Settings

Azure Subscription

Azure\_Subscription\_1

Region

Default\_CM\_Region

Resource Group

☒ Create a new
 ☐ Use an existing

Resource Group Name

Encryption Managed Keys

☒ Microsoft-managed
 ☐ Customer-managed

기본 정책은 매일 볼륨을 백업하고 각 볼륨의 최근 30개 백업 복사본을 유지합니다. 시간별, 일별, 주별 또는 월별 백업으로 변경하거나 더 많은 옵션을 제공하는 시스템 정의 정책 중 하나를 선택합니다. 보존할 백업 복사본의 수를 변경할 수도 있습니다.

기본적으로 백업은 Cool 액세스 계층에 저장됩니다. 클러스터에서 ONTAP 9.10.1 이상을 사용하는 경우 추가 비용 최적화를 위해 일정 일 후에 Azure 아카이브 스토리지에 백업을 계층화하도록 선택할 수 있습니다.

### Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule** ☒ Create a New Policy ☐ Select an Existing Policy

<input type="checkbox"/> Hourly	Number of backups to retain	24
<input checked="" type="checkbox"/> Daily	Number of backups to retain	30
<input type="checkbox"/> Weekly	Number of backups to retain	52
<input type="checkbox"/> Monthly	Number of backups to retain	12

---

**Archival Policy**

Backups reside in Cool Azure Blob storage for frequently accessed data. Optionally, you can tier backups to Azure Archive storage for further cost optimization.

☒ Tier Backups to Archival

Archive after (Days)

30

Access Tier

Azure Archive

---

**Storage Account**

Cloud Manager will create the storage account after you complete the wizard

Select Volumes(볼륨 선택) 페이지의 기본 백업 정책을 사용하여 백업할 볼륨을 식별합니다. 특정 볼륨에 서로 다른 백업 정책을 할당하려면 추가 정책을 생성한 후 나중에 볼륨에 적용할 수 있습니다.

## 요구 사항

Azure Blob 저장소에 볼륨을 백업하기 전에 다음 요구 사항을 읽고 지원되는 구성이 있는지 확인합니다.

다음 이미지는 각 구성 요소와 이러한 구성 요소 간에 준비해야 하는 연결을 보여 줍니다.



클라우드 복원 가상 머신이 클라우드에 구축되면 Connector와 동일한 서브넷에 위치합니다.

#### 지원되는 **ONTAP** 버전

Cloud Volumes ONTAP 9.7P5 이상

#### 라이선스 요구 사항

Cloud Backup PAYGO 라이선스의 경우 Cloud Backup을 활성화하기 전에 Azure Marketplace를 통해 가입해야 합니다. Cloud Backup에 대한 청구는 이 구독을 통해 이루어집니다. ["작업 환경 마법사의 세부 정보 및 자격 증명 페이지에서 구독할 수 있습니다"](#).

Cloud Backup BYOL 라이선스의 경우, 라이선스 기간 및 용량 동안 서비스를 사용할 수 있도록 지원하는 NetApp의 일련 번호가 필요합니다. ["BYOL 라이선스 관리 방법에 대해 알아보십시오"](#).

그리고 백업이 위치할 스토리지 공간에 대한 Microsoft Azure 구독이 있어야 합니다.

#### 지원되는 **Azure** 지역

Cloud Backup은 모든 Azure 지역에서 지원됩니다 ["Cloud Volumes ONTAP가 지원되는 경우"](#) Azure Government 지역을 비롯한 모든 지역에서 사용할 수 있습니다.

#### 다른 **Azure** 구독에서 백업을 생성하기 위한 필수 설정

기본적으로 백업은 Cloud Volumes ONTAP 시스템에 사용되는 것과 동일한 구독을 사용하여 생성됩니다. 백업에 다른 Azure 구독을 사용하려면 을(를) 사용해야 합니다 ["Azure 포털에 로그인하고 두 구독을 연결합니다"](#).

#### 데이터 암호화에 대해 고객이 관리하는 키를 사용하는 데 필요한 정보입니다

정품 인증 마법사에서 기본 Microsoft 관리 암호화 키를 사용하는 대신 고객이 관리하는 키를 사용하여 데이터를 암호화할 수 있습니다. 이 경우 Azure 가입, 키 저장소 이름 및 키가 필요합니다. ["자신의 키를 사용하는 방법을 확인하십시오"](#).

## Azure 배포를 위한 아웃바운드 인터넷 액세스가 필요합니다

클라우드 복원 가상 컴퓨터를 사용하려면 아웃바운드 인터넷 액세스가 필요합니다. 가상 또는 물리적 네트워크에서 인터넷 액세스에 프록시 서버를 사용하는 경우 인스턴스에 다음 끝점에 연결할 수 있는 아웃바운드 인터넷 액세스 권한이 있는지 확인합니다.

엔드포인트	목적
<a href="http://olcentgbl.trafficmanager.net">http://olcentgbl.trafficmanager.net</a> <a href="https://olcentgbl.trafficmanager.net">https://olcentgbl.trafficmanager.net</a> 으로 문의하십시오	클라우드 복원 가상 머신용 CentOS 패키지를 제공합니다.
<a href="https://download.docker.com/linux/centos/docker-ce.repo">https://download.docker.com/linux/centos/docker-ce.repo</a> 으로 문의하십시오	Docker Engine 패키지를 제공합니다.
<a href="http://cloudmanagerinfraprod.azurecr.io">http://cloudmanagerinfraprod.azurecr.io</a> <a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a> 으로 문의하십시오	클라우드 복원 가상 머신 이미지 리포지토리.

## 새로운 시스템에서 Cloud Backup을 활성화합니다

클라우드 백업은 작업 환경 마법사에서 기본적으로 설정됩니다. 옵션을 활성 상태로 유지해야 합니다.

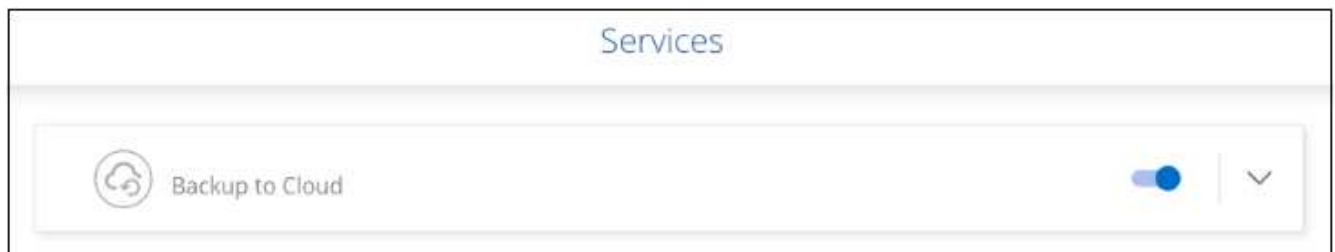
을 참조하십시오 ["Azure에서 Cloud Volumes ONTAP 실행"](#) Cloud Volumes ONTAP 시스템 생성에 대한 요구 사항 및 세부 정보를 확인하십시오.



리소스 그룹의 이름을 선택하려면 \* Cloud Volumes ONTAP 배포 시 \* 클라우드 백업을 비활성화합니다. 이 단계를 따릅니다 [기존 시스템에서 Cloud Backup 활성화](#) Cloud Backup을 활성화하고 리소스 그룹을 선택합니다.

### 단계

1. Create Cloud Volumes ONTAP \* 를 클릭합니다.
2. 클라우드 공급자로 Microsoft Azure를 선택하고 단일 노드 또는 HA 시스템을 선택합니다.
3. Azure 자격 증명 정의 페이지에서 자격 증명 이름, 클라이언트 ID, 클라이언트 암호 및 디렉터리 ID를 입력하고 \* 계속 \* 을 클릭합니다.
4. 세부 정보 및 자격 증명 페이지를 입력하고 Azure Marketplace 구독이 있는지 확인한 다음 \* 계속 \* 을 클릭합니다.
5. 서비스 페이지에서 서비스를 활성화된 상태로 두고 \* 계속 \* 을 클릭합니다.



6. 마법사의 페이지를 완료하여 시스템을 구축합니다.

Cloud Backup은 시스템에서 활성화되어 매일 볼륨을 백업하며 최근 30개의 백업 복사본을 보존합니다.

가능합니다 ["볼륨에 대한 백업을 시작 및 중지하거나 백업 일정을 변경합니다"](#). 또한 가능합니다 ["백업 파일에서 전체 볼륨 또는 개별 파일을 복원합니다"](#) Azure의 Cloud Volumes ONTAP 시스템 또는 사내 ONTAP 시스템으로 데이터를

이동합니다.

## 기존 시스템에서 **Cloud Backup** 활성화

작업 환경에서 바로 언제든지 Cloud Backup을 사용할 수 있습니다.

단계

1. 작업 환경을 선택하고 오른쪽 패널에서 백업 및 복원 서비스 옆에 있는 \* 활성화 \* 를 클릭합니다.



2. 제공업체 세부 정보를 선택하고 \* 다음 \* 을 클릭합니다.

- a. 백업을 저장하는 데 사용되는 Azure 구독입니다. 이는 Cloud Volumes ONTAP 시스템이 있는 가입과 다를 수 있습니다.

백업에 다른 Azure 구독을 사용하려면 을(를) 사용해야 합니다 ["Azure 포털에 로그인하고 두 구독을 연결합니다"](#).

- b. 백업이 저장될 영역입니다. 이 영역은 Cloud Volumes ONTAP 시스템이 있는 지역과 다를 수 있습니다.
- c. Blob 컨테이너를 관리하는 리소스 그룹 - 새 리소스 그룹을 만들거나 기존 리소스 그룹을 선택할 수 있습니다.
- d. 기본 Microsoft 관리 암호화 키를 사용하거나 고객이 직접 관리하는 키를 선택하여 데이터 암호화를 관리할지 여부를 결정합니다. (["자신의 키를 사용하는 방법을 확인하십시오"](#))를 클릭합니다.

3. 기본 백업 정책 세부 정보를 입력하고 \* 다음 \* 을 클릭합니다.

- a. 백업 스케줄을 정의하고 보존할 백업 수를 선택합니다. ["선택할 수 있는 기존 정책 목록을 봅니다"](#).
- b. ONTAP 9.10.1 이상을 사용하는 경우 추가 비용 최적화를 위해 일정 일 후에 Azure 아카이브 스토리지에 백업을 계층화하도록 선택할 수 있습니다. ["아카이브 계층 사용에 대해 자세히 알아보십시오"](#).



### Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule** ☒ Create a New Policy ☐ Select an Existing Policy

☐ Hourly  
☒ Daily  
☐ Weekly  
☐ Monthly

Number of backups to retain

24

☒ Daily  
☐ Weekly  
☐ Monthly

Number of backups to retain

30

☐ Weekly  
☐ Monthly

Number of backups to retain

52

☐ Monthly

Number of backups to retain

12

---

**Archival Policy**

Backups reside in Cool Azure Blob storage for frequently accessed data. Optionally, you can tier backups to Azure Archive storage for further cost optimization.

☒ Tier Backups to Archival

Archive after (Days)

Access Tier

30

Azure Archive

---

**Storage Account**

Cloud Manager will create the storage account after you complete the wizard

4. Select Volumes(볼륨 선택) 페이지의 기본 백업 정책을 사용하여 백업할 볼륨을 선택합니다. 특정 볼륨에 서로 다른 백업 정책을 할당하려는 경우 추가 정책을 생성하여 나중에 해당 볼륨에 적용할 수 있습니다.

### Select Volumes

57 Volumes

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 <small>On</small>	DP	SVM_Name_2	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	Not Active

☒ Automatically back up future volumes on all storage VMs with the selected backup policy

- 모든 볼륨을 백업하려면 제목 행(☒ Volume Name)를 클릭합니다.
- 개별 볼륨을 백업하려면 각 볼륨에 대한 확인란을 선택합니다(☒ Volume\_1)를 클릭합니다.

5. 나중에 추가된 모든 볼륨에 백업을 사용하려면 "Automatically back up future volumes..." 확인란을 선택하기만 하면 됩니다. 이 설정을 비활성화하면 이후 볼륨에 대해 백업을 수동으로 활성화해야 합니다.

6. 백업 활성화 \* 를 클릭하면 선택한 각 볼륨의 초기 백업이 시작됩니다.

Cloud Backup은 선택한 각 볼륨의 초기 백업을 시작하고, 백업 상태를 모니터링할 수 있도록 Volume Backup Dashboard가 표시됩니다.

가능합니다 "볼륨에 대한 백업을 시작 및 중지하거나 백업 일정을 변경합니다". 또한 가능합니다 "백업 파일에서 전체

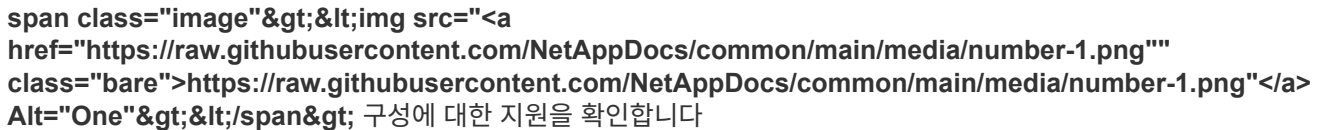
볼륨 또는 개별 파일을 복원합니다" Azure의 Cloud Volumes ONTAP 시스템 또는 사내 ONTAP 시스템으로 데이터를 이동합니다.

## Cloud Volumes ONTAP 데이터를 Google 클라우드 스토리지에 백업

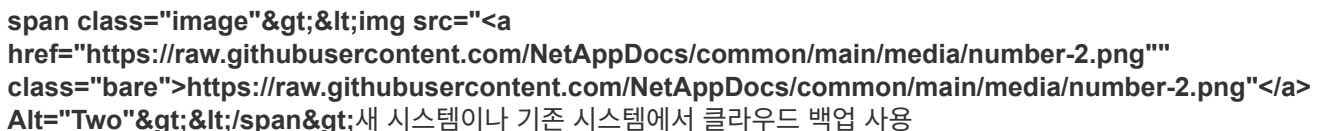
Cloud Volumes ONTAP에서 Google 클라우드 스토리지로 데이터 백업을 시작하는 몇 가지 단계를 완료하십시오.

### 빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션으로 스크롤하여 자세한 내용을 확인하십시오.

 구성에 대한 지원을 확인합니다

- GCP에서 Cloud Volumes ONTAP 9.7P5 이상을 실행하고 있습니다.
- 백업이 위치할 스토리지 공간에 대한 유효한 GCP 구독이 있습니다.
- Google Cloud Project에는 사전 정의된 스토리지 관리자 역할이 있는 서비스 계정이 있습니다.
- 에 가입했습니다 "Cloud Manager Marketplace 백업 오퍼링" 또는 을(를) 구입한 경우 "활성화합니다" Cloud Backup BYOL 라이선스는 NetApp에서 제공

 새 시스템이나 기존 시스템에서 클라우드 백업 사용

- 새로운 시스템: 새로운 작업 환경 마법사를 완료하면 클라우드 백업을 활성화할 수 있습니다.
- 기존 시스템: 작업 환경을 선택하고 오른쪽 패널의 백업 및 복원 서비스 옆에 있는 \* 활성화 \* 를 클릭한 다음 설정 마법사를 따릅니다.



Google Cloud Storage 버킷을 백업용으로 생성할 Google Cloud Project를 선택합니다.





기본 정책은 매일 볼륨을 백업하고 각 볼륨의 최근 30개 백업 복사본을 유지합니다. 시간별, 일별, 주별 또는 월별 백업으로 변경하거나 더 많은 옵션을 제공하는 시스템 정의 정책 중 하나를 선택합니다. 보존할 백업 복사본의 수를 변경할 수도 있습니다.

### Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule**
☒ Create a New Policy
 ☐ Select an Existing Policy

☐ Hourly
 Number of backups to retain

☒ Daily
 Number of backups to retain

☐ Weekly
 Number of backups to retain

☐ Monthly
 Number of backups to retain

**DP Volumes**

Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

**Google Cloud Storage Bucket**

Cloud Manager will create the Google Cloud Storage Bucket after you complete the wizard

Select Volumes(볼륨 선택) 페이지의 기본 백업 정책을 사용하여 백업할 볼륨을 식별합니다. 특정 볼륨에 서로 다른 백업 정책을 할당하려면 추가 정책을 생성한 후 나중에 볼륨에 적용할 수 있습니다.

## 요구 사항

Google Cloud 스토리지에 볼륨을 백업하기 전에 다음 요구 사항을 읽고 지원되는 구성이 있는지 확인합니다.

다음 이미지는 각 구성 요소와 이러한 구성 요소 간에 준비해야 하는 연결을 보여 줍니다.



지원되는 **ONTAP** 버전

Cloud Volumes ONTAP 9.7P5 이상

지원되는 **GCP** 지역

Cloud Backup은 모든 GCP 지역에서 지원됩니다 "[Cloud Volumes ONTAP가 지원되는 경우](#)".

라이선스 요구 사항

Cloud Backup PAYGO 라이선스의 경우, 를 통한 구독 "[GCP 마켓플레이스](#)" Cloud Backup을 활성화하기 전에 필요합니다. Cloud Backup에 대한 청구는 이 구독을 통해 이루어집니다. "[작업 환경 마법사의 세부 정보 및 자격 증명 페이지에서 구독할 수 있습니다](#)".

Cloud Backup BYOL 라이선스의 경우, 라이선스 기간 및 용량 동안 서비스를 사용할 수 있도록 지원하는 NetApp의 일련 번호가 필요합니다. "[BYOL 라이선스 관리 방법에 대해 알아보십시오](#)".

그리고 백업을 찾을 저장소 공간에 대한 Google 구독이 있어야 합니다.

**GCP** 서비스 계정

Google Cloud Project에는 사전 정의된 스토리지 관리자 역할이 있는 서비스 계정이 있어야 합니다. "[서비스 계정을 만드는 방법에 대해 알아보십시오](#)".

**Connector**에 권한을 확인하거나 추가합니다

Cloud Backup Search & Restore 기능을 사용하려면 Connector 역할에 특정 권한이 있어야 Google Cloud BigQuery 서비스에 액세스할 수 있습니다. 아래 사용 권한을 확인하고 정책을 수정해야 하는 경우 단계를 따릅니다.

단계

1. 인치 "[클라우드 콘솔](#)"에서 \* 역할 \* 페이지로 이동합니다.
2. 페이지 맨 위에 있는 드롭다운 목록을 사용하여 편집할 역할이 포함된 프로젝트나 조직을 선택합니다.

3. 사용자 지정 역할을 클릭합니다.
4. 역할 편집 \* 을 클릭하여 역할의 권한을 업데이트합니다.
5. 역할에 다음과 같은 새 권한을 추가하려면 \* 권한 추가 \* 를 클릭합니다.

```
bigquery.jobs.get  
bigquery.jobs.list  
bigquery.jobs.listAll  
bigquery.datasets.create  
bigquery.datasets.get  
bigquery.jobs.create  
bigquery.tables.get  
bigquery.tables.getData  
bigquery.tables.list  
bigquery.tables.create
```

6. Update \* 를 클릭하여 편집된 역할을 저장합니다.

## 새로운 시스템에서 **Cloud Backup**을 활성화합니다

작업 환경 마법사를 완료하여 새 Cloud Volumes ONTAP 시스템을 생성할 때 클라우드 백업을 활성화할 수 있습니다.

서비스 계정이 이미 구성되어 있어야 합니다. Cloud Volumes ONTAP 시스템을 생성할 때 서비스 계정을 선택하지 않은 경우 시스템을 끄고 GCP 콘솔에서 Cloud Volumes ONTAP에 서비스 계정을 추가해야 합니다.

을 참조하십시오 ["GCP에서 Cloud Volumes ONTAP를 시작합니다"](#) Cloud Volumes ONTAP 시스템 생성에 대한 요구 사항 및 세부 정보를 확인하십시오.

### 단계

1. 작업 환경 페이지에서 \* 작업 환경 추가 \* 를 클릭하고 화면의 지시를 따릅니다.
2. \* 위치 선택 \*: \* Google Cloud Platform \* 을 선택합니다.
3. \* 유형 선택 \*: \* Cloud Volumes ONTAP \* (단일 노드 또는 고가용성)를 선택합니다.
4. \* 상세 정보 및 자격 증명 \*: 다음 정보를 입력합니다.
  - a. 프로젝트 편집 \* 을 클릭하고 사용하려는 프로젝트가 기본 프로젝트(Cloud Manager가 있는 프로젝트)와 다른 경우 새 프로젝트를 선택합니다.
  - b. 클러스터 이름을 지정합니다.
  - c. 서비스 계정 \* 스위치를 활성화하고 사전 정의된 스토리지 관리자 역할이 있는 서비스 계정을 선택합니다. 이 작업은 백업 및 계층화를 활성화하는 데 필요합니다.
  - d. 자격 증명을 지정합니다.

GCP Marketplace 구독이 마련되어 있는지 확인합니다.

5. \* 서비스 \*: Cloud Backup Service를 활성화된 상태로 두고 \* 계속 \* 을 클릭합니다.

6. 마법사의 페이지를 완료하여 에 설명된 대로 시스템을 구축합니다 "[GCP에서 Cloud Volumes ONTAP를 시작합니다](#)".

Cloud Backup은 시스템에서 활성화되어 매일 생성한 볼륨을 백업하며 최근 30개의 백업 복사본을 보존합니다.

가능합니다 "[볼륨에 대한 백업을 시작 및 중지하거나 백업 일정을 변경합니다](#)". 또한 가능합니다 "[백업 파일에서 전체 볼륨을 복원합니다](#)" Google의 Cloud Volumes ONTAP 시스템 또는 온프레미스 ONTAP 시스템으로.

## 기존 시스템에서 **Cloud Backup** 활성화

작업 환경에서 Cloud Backup을 바로 활성화할 수 있습니다.

단계

1. 작업 환경을 선택하고 오른쪽 패널에서 백업 및 복원 서비스 옆에 있는 \* 활성화 \* 를 클릭합니다.

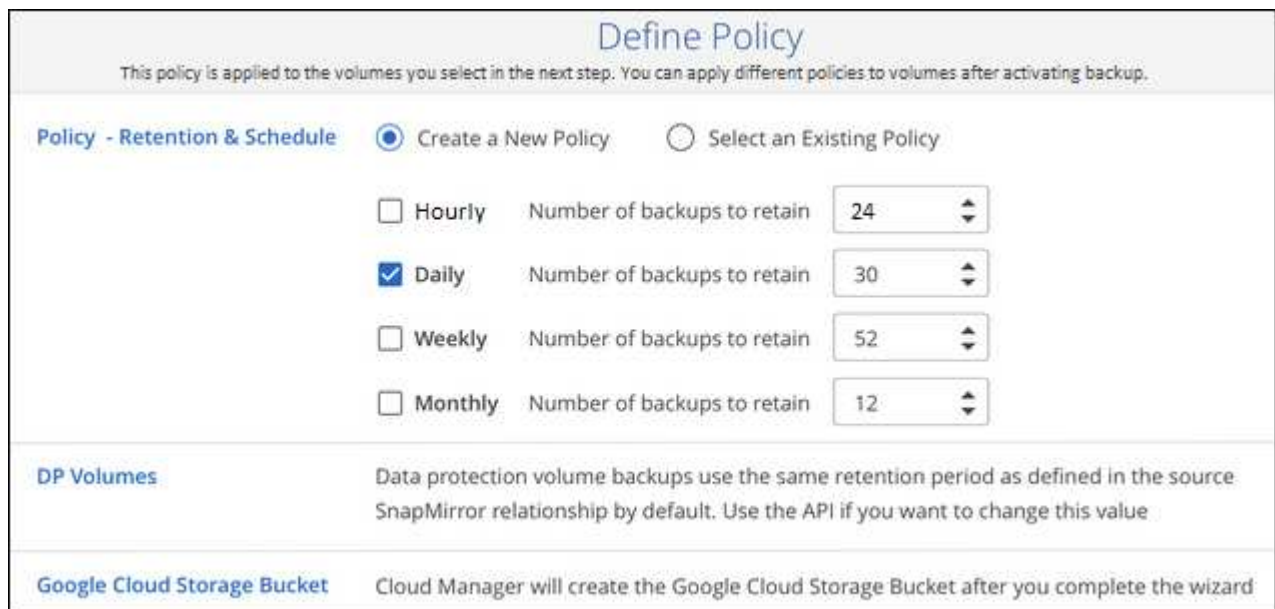
2. 백업을 위해 Google Cloud Storage 버킷을 생성할 Google Cloud Project 및 지역을 선택하고 \* Next \* 를 클릭합니다.



The image shows a 'Provider Settings' form. It has two sections: 'Google Cloud Project' with a dropdown menu showing 'Default Project', and 'Region' with a dropdown menu showing 'us-east-2'.

Project에는 미리 정의된 스토리지 관리자 역할이 있는 서비스 계정이 있어야 합니다.

3. Define Policy\_페이지에서 기본 백업 일정 및 보존 값을 선택하고 \* Next \* 를 클릭합니다.



The image shows a 'Define Policy' form. At the top, it says 'This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.' Below this, there are two radio buttons: 'Create a New Policy' (selected) and 'Select an Existing Policy'. Under 'Create a New Policy', there are four options for backup frequency: 'Hourly' (unchecked), 'Daily' (checked), 'Weekly' (unchecked), and 'Monthly' (unchecked). Each frequency has a corresponding 'Number of backups to retain' with a numeric input field: 24 for Hourly, 30 for Daily, 52 for Weekly, and 12 for Monthly. Below these, there is a section 'DP Volumes' with a note: 'Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value'. At the bottom, there is a section 'Google Cloud Storage Bucket' with a note: 'Cloud Manager will create the Google Cloud Storage Bucket after you complete the wizard'.

을 참조하십시오 "기존 정책 목록입니다".

4. Select Volumes(볼륨 선택) 페이지의 기본 백업 정책을 사용하여 백업할 볼륨을 선택합니다. 특정 볼륨에 서로 다른 백업 정책을 할당하려는 경우 추가 정책을 생성하여 나중에 해당 볼륨에 적용할 수 있습니다.

Select Volumes						
57 Volumes						
<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 On	DP	SVM_Name_2	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/> Automatically back up future volumes on all storage VMs with the selected backup policy						

- 모든 볼륨을 백업하려면 제목 행(☒ Volume Name)를 클릭합니다.
- 개별 볼륨을 백업하려면 각 볼륨에 대한 확인란을 선택합니다(☒ Volume\_1)를 클릭합니다.

- 나중에 추가된 모든 볼륨에 백업을 사용하려면 "Automatically back up future volumes..." 확인란을 선택하기만 하면 됩니다. 이 설정을 비활성화하면 이후 볼륨에 대해 백업을 수동으로 활성화해야 합니다.
- 백업 활성화 \* 를 클릭하면 선택한 각 볼륨의 초기 백업이 시작됩니다.

Cloud Backup은 선택한 각 볼륨의 초기 백업을 시작하고, 백업 상태를 모니터링할 수 있도록 Volume Backup Dashboard가 표시됩니다.

가능합니다 "볼륨에 대한 백업을 시작 및 중지하거나 백업 일정을 변경합니다". 또한 가능합니다 "백업 파일에서 볼륨 또는 파일을 복원합니다" Google의 Cloud Volumes ONTAP 시스템 또는 온프레미스 ONTAP 시스템으로.

## 사내 ONTAP 데이터를 Amazon S3에 백업

몇 가지 단계를 완료하여 사내 ONTAP 시스템에서 Amazon S3 스토리지로의 데이터 백업을 시작하십시오.

"사내 ONTAP 시스템"에는 FAS, AFF 및 ONTAP Select 시스템이 포함됩니다.

### 빠른 시작

다음 단계를 수행하여 빠르게 시작하십시오. 각 단계에 대한 자세한 내용은 이 항목의 다음 섹션을 참조하십시오.

사내 ONTAP 클러스터를 퍼블릭 인터넷을 통해 AWS S3에 직접 연결할지, VPN 또는 AWS 직접 연결을 사용할지, 프라이빗 VPC 엔드 포인트 인터페이스를 통해 트래픽을 AWS S3에 연결할지 선택합니다.

사용 가능한 연결 방법을 참조하십시오.

AWS VPC에 이미 Connector가 구축되어 있는 경우 모두 설정됩니다. 그렇지 않은 경우, ONTAP 데이터를 AWS S3 스토리지에 백업하기 위해 AWS에서 커넥터를 생성해야 합니다. 또한 AWS S3에 연결할 수 있도록 커넥터의 네트워크 설정을 사용자 지정해야 합니다.

Connector를 생성하는 방법과 필요한 네트워크 설정을 정의하는 방법을 참조하십시오.

Cloud Manager에서 ONTAP 클러스터를 검색하고, 클러스터가 최소 요구사항을 충족하는지 확인하고, 클러스터가 AWS S3에 연결할 수 있도록 네트워크 설정을 사용자 지정합니다.

사내 ONTAP 클러스터를 준비하는 방법을 알아보십시오.

Connector에 대한 권한을 설정하여 S3 버킷을 생성 및 관리하고 Restore 인스턴스를 사용하여 데이터를 복원합니다. 또한 S3 버킷에서 데이터를 읽고 쓸 수 있도록 사내 ONTAP 클러스터에 대한 권한을 설정합니다.

선택적으로 기본 Amazon S3 암호화 키를 사용하는 대신 데이터 암호화에 대해 자체적인 사용자 정의 관리 키를 설정할 수 있습니다. [AWS S3 환경을 ONTAP 백업 수신 준비 상태로 만드는 방법을 알아보십시오.](#)

작업 환경을 선택하고 오른쪽 패널에서 백업 및 복원 서비스 옆에 있는 \* 활성화 > 볼륨 백업 \* 을 클릭합니다. 그런 다음 설정 마법사를 따라 기본 백업 정책 및 유지할 백업 수를 정의하고 백업할 볼륨을 선택합니다.

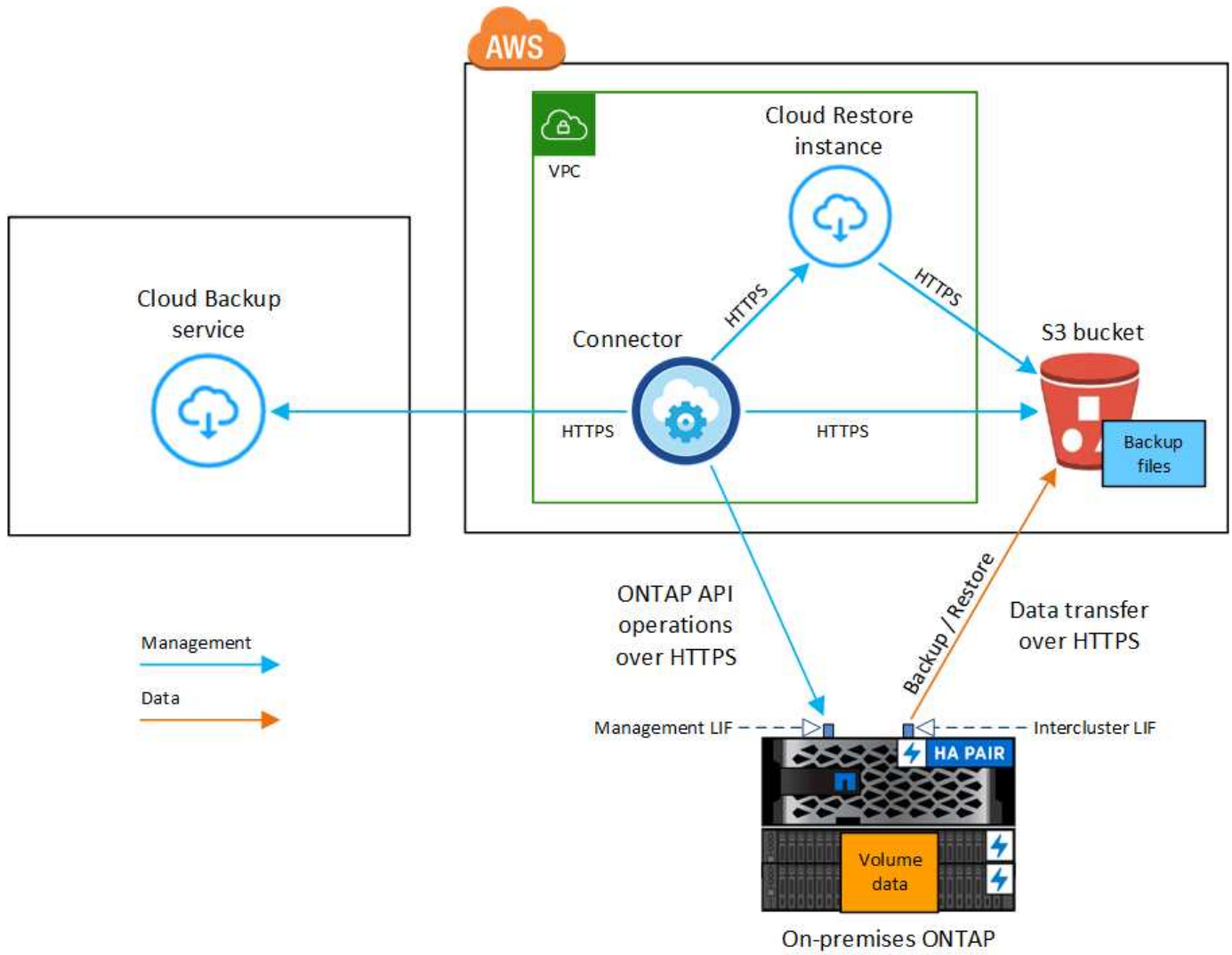
볼륨에서 [Cloud Backup](#)을 활성화하는 방법을 확인하십시오.

## 연결 옵션에 대한 네트워크 다이어그램

사내 ONTAP 시스템에서 AWS S3로 백업을 구성할 때 두 가지 연결 방법을 사용할 수 있습니다.

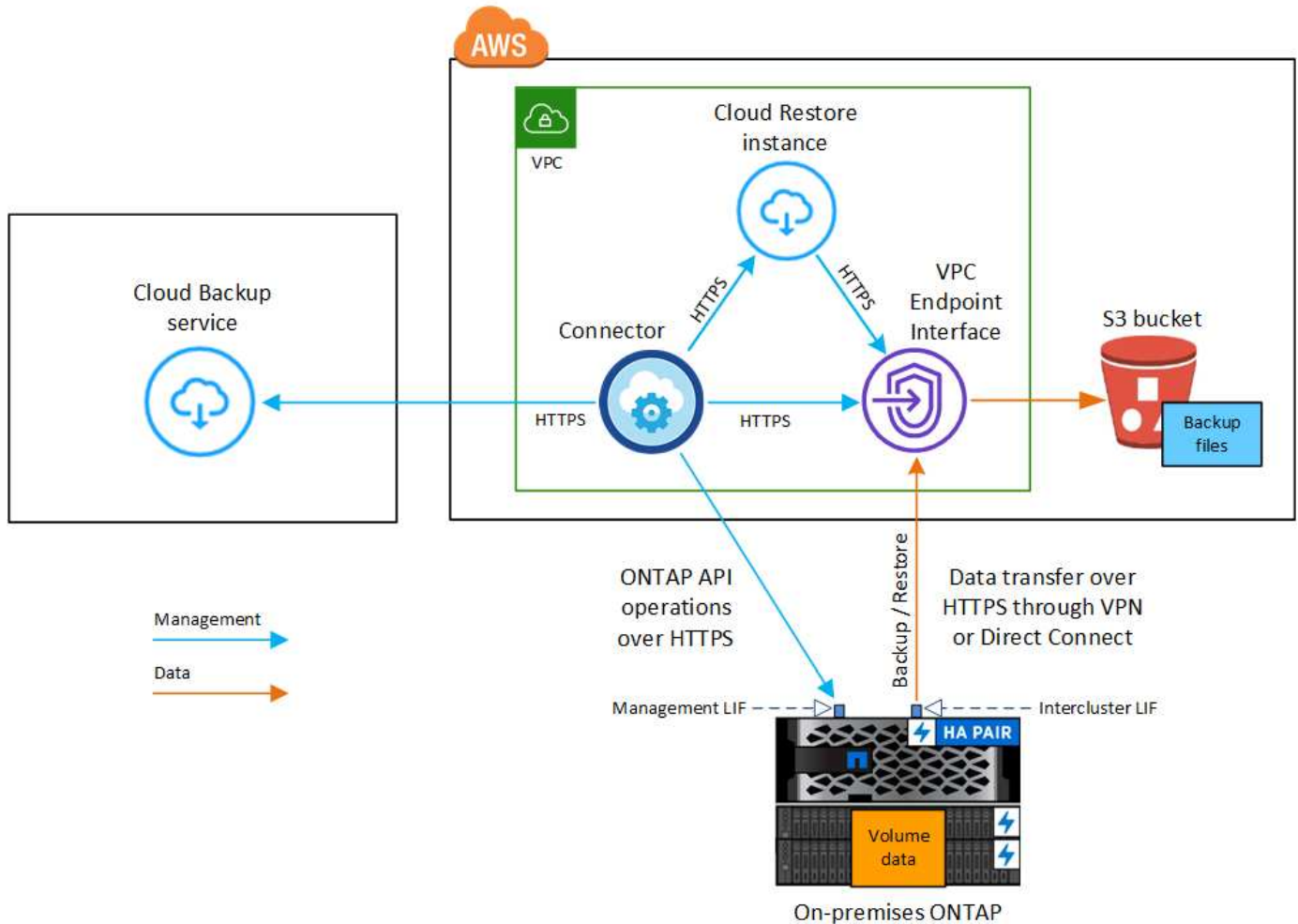
- 공용 연결 - 공용 S3 끝점을 사용하여 ONTAP 시스템을 AWS S3에 직접 연결합니다.
- 비공개 연결 - VPN 또는 AWS Direct Connect를 사용하여 전용 IP 주소를 사용하는 VPC 엔드포인트 인터페이스를 통해 트래픽을 라우팅합니다.

다음 다이어그램에서는 \* public connection \* 메서드와 구성 요소 간에 준비해야 하는 연결을 보여 줍니다.



다음 다이어그램에서는 \* private connection \* 메서드와 구성 요소 간에 준비해야 하는 연결을 보여 줍니다.





Cloud Restore 인스턴스가 클라우드에 배포되면 Connector와 동일한 서브넷에 위치합니다.

## 커넥터를 준비합니다

Cloud Manager Connector는 Cloud Manager 기능을 위한 기본 소프트웨어입니다. ONTAP 데이터를 백업하고 복원하려면 커넥터가 필요합니다.

### 커넥터 작성 또는 전환

AWS VPC에 이미 Connector를 구축한 경우 모든 준비가 된 것입니다. 그렇지 않은 경우, ONTAP 데이터를 AWS S3 스토리지에 백업하기 위해 AWS에서 새 커넥터를 생성해야 합니다. 온-프레미스에 배포되었거나 다른 클라우드 공급자에 배포된 Connector는 사용할 수 없습니다.

- ["커넥터에 대해 자세히 알아보십시오"](#)
- ["커넥터 시작하기"](#)
- ["AWS에서 커넥터를 생성합니다"](#)

### 커넥터 네트워킹 요구 사항

- 커넥터가 설치된 네트워크에서 다음 연결을 사용할 수 있는지 확인합니다.
  - 포트 443을 통해 Cloud Backup Service 및 S3 오브젝트 스토리지에 HTTPS 연결(엔드포인트 목록 참조)

"여기")

◦ 포트 443을 통해 ONTAP 클러스터 관리 LIF에 HTTPS로 연결합니다

- "커넥터에 S3 버킷을 관리할 수 있는 권한이 있는지 확인합니다".
- ONTAP 클러스터에서 VPC로의 직접 연결 또는 VPN 연결이 있고 커넥터와 S3 간의 통신을 AWS 내부 네트워크에 계속 사용하려면 S3에 VPC 엔드포인트 인터페이스를 활성화해야 합니다. [VPC 엔드포인트 인터페이스를 설정하는 방법을 확인하십시오](#).

## ONTAP 클러스터를 준비합니다

Cloud Manager에서 ONTAP 클러스터를 검색합니다

볼륨 데이터 백업을 시작하려면 Cloud Manager에서 사내 ONTAP 클러스터를 검색해야 합니다. 클러스터를 추가하려면 클러스터 관리 IP 주소와 admin 사용자 계정의 암호를 알아야 합니다.

["클러스터를 검색하는 방법에 대해 알아보십시오"](#).

### ONTAP 요구 사항

- 최소 ONTAP 9.7P5, ONTAP 9.8P11 이상을 사용하는 것이 좋습니다.
- SnapMirror 라이선스(프리미엄 번들 또는 데이터 보호 번들의 일부로 포함)
- 참고: \* Cloud Backup을 사용할 때는 "하이브리드 클라우드 번들"이 필요하지 않습니다.

자세한 내용은 를 참조하십시오 ["클러스터 라이선스를 관리합니다"](#).

- 시간 및 시간대가 올바르게 설정되었습니다.

자세한 내용은 를 참조하십시오 ["클러스터 시간을 구성합니다"](#).

### 클러스터 네트워킹 요구 사항

- 클러스터는 Connector에서 클러스터 관리 LIF로 인바운드 HTTPS 연결을 필요로 합니다.
- 인터클러스터 LIF는 백업할 볼륨을 호스팅하는 각 ONTAP 노드에 필요합니다. 이러한 인터클러스터 LIF는 오브젝트 저장소에 액세스할 수 있어야 합니다.

클러스터는 백업 및 복원 작업을 위해 클러스터 간 LIF에서 Amazon S3 스토리지로 포트 443을 통한 아웃바운드 HTTPS 연결을 시작합니다. ONTAP는 오브젝트 스토리지 간에 데이터를 읽고 씁니다. 오브젝트 스토리지는 결코 시작할 수 없으며 단지 반응합니다.

- 인터클러스터 LIF는 ONTAP가 오브젝트 스토리지에 연결하는 데 사용해야 하는 \_IPspace\_와 연결되어야 합니다. ["IPspace에 대해 자세히 알아보십시오"](#).

클라우드 백업을 설정하면 사용할 IPspace를 묻는 메시지가 표시됩니다. 이러한 LIF와 연결되는 IPspace를 선택해야 합니다. 이는 여러분이 생성한 "기본" IPspace 또는 사용자 지정 IPspace가 될 수 있습니다.

사용 중인 IPspace가 "기본값"과 다른 경우 오브젝트 스토리지에 액세스하려면 정적 라우트를 생성해야 할 수 있습니다.

IPspace 내의 모든 인터클러스터 LIF는 오브젝트 저장소에 대한 액세스 권한이 있어야 합니다. 현재 IPspace에 대해 이 기능을 구성할 수 없는 경우 모든 인터클러스터 LIF가 오브젝트 저장소에 액세스할 수 있는 전용 IPspace를

만들어야 합니다.

- 불륨이 있는 스토리지 VM에 대해 DNS 서버가 구성되어 있어야 합니다. 자세한 내용은 ["SVM을 위한 DNS 서비스 구성"](#).
- 필요한 경우, 포트 443을 통해 ONTAP에서 오브젝트 스토리지로 클라우드 백업 연결을 허용하고 포트 53(TCP/UDP)을 통해 스토리지 VM에서 DNS 서버로 이름 확인 트래픽을 허용하도록 방화벽 규칙을 업데이트합니다.
- AWS에서 S3 연결을 위해 전용 VPC 인터페이스 엔드포인트를 사용하는 경우 HTTPS/443을 사용하려면 S3 엔드포인트 인증서를 ONTAP 클러스터로 로드해야 합니다. [VPC 엔드포인트 인터페이스를 설정하고 S3 인증서를 로드하는 방법을 알아보십시오](#).
- ["ONTAP 클러스터에 S3 버킷을 액세스할 수 있는 권한이 있는지 확인합니다"](#).

## 라이선스 요구 사항을 확인합니다

- 클러스터에 Cloud Backup을 활성화하려면 먼저 AWS에서 PAYGO(Pay-as-you-Go) Cloud Manager Marketplace 오퍼링을 구독하거나 NetApp에서 Cloud Backup BYOL 라이선스를 구입하여 활성화해야 합니다. 이러한 라이선스는 사용자 계정용이며 여러 시스템에서 사용할 수 있습니다.
  - Cloud Backup PAYGO 라이선스의 경우 에 대한 구독이 필요합니다 ["AWS Cloud Manager Marketplace 오퍼링"](#) 를 사용하여 Cloud Backup을 선택합니다. Cloud Backup에 대한 청구는 이 구독을 통해 이루어집니다.
  - Cloud Backup BYOL 라이선스의 경우, 라이선스 기간 및 용량 동안 서비스를 사용할 수 있도록 지원하는 NetApp의 일련 번호가 필요합니다. ["BYOL 라이선스 관리 방법에 대해 알아보십시오"](#).
- 백업이 위치할 오브젝트 스토리지 공간에 대한 AWS 서브스크립션을 보유하고 있어야 합니다.

모든 지역의 사내 시스템에서 Amazon S3로 백업을 생성할 수 있습니다 ["Cloud Volumes ONTAP가 지원되는 경우"](#) AWS GovCloud 지역 포함. 서비스를 설정할 때 백업을 저장할 지역을 지정합니다.

## AWS 환경을 준비하십시오

### S3 권한 설정

두 가지 권한 집합을 구성해야 합니다.

- Connector에서 S3 버킷을 생성 및 관리하고 Restore 인스턴스를 사용하여 데이터를 복원할 수 있는 권한
- S3 버킷에서 데이터를 읽고 쓸 수 있도록 사내 ONTAP 클러스터에 대한 권한.

단계

1. 다음 S3 권한(최신 버전)이 있는지 확인합니다 ["Cloud Manager 정책"](#))는 Connector에 권한을 제공하는 IAM 역할의 일부입니다.

```

{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutEncryptionConfiguration",
        "athena:StartQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryExecution",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:CreateDatabase",
        "glue:GetPartitions",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition"
    ],
    "Resource": [
        "arn:aws:s3:::netapp-backup-*"
    ]
}

```

버전 3.9.15 이상을 사용하여 Connector를 배포한 경우 이러한 권한은 이미 IAM 역할의 일부여야 합니다. 그렇지 않으면 누락된 권한을 추가해야 합니다. 특히 검색 및 복원에 필요한 "Athena" 및 "GLUE" 사용 권한이 있습니다. 를 참조하십시오 ["AWS 설명서: IAM 정책 편집"](#).

2. 찾아보기 및 복원 작업을 위해 Cloud Restore 인스턴스를 시작, 중지 및 종료할 수 있도록 Connector에 권한을 제공하는 IAM 역할에 다음 EC2 권한을 추가합니다.

```

    "Action": [
        "ec2:DescribeInstanceTypeOfferings",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
    ],

```

3. 서비스를 활성화하면 백업 마법사에서 액세스 키와 암호 키를 입력하라는 메시지가 표시됩니다. 이러한 자격 증명은 ONTAP 클러스터에 전달되므로 ONTAP는 S3 버킷으로 데이터를 백업 및 복원할 수 있습니다. 이를 위해서는 다음과 같은 권한을 가진 IAM 사용자를 생성해야 합니다.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": "arn:aws:s3:::netapp-backup-*",
            "Effect": "Allow",
            "Sid": "backupPolicy"
        }
    ]
}

```

를 참조하십시오 ["AWS 설명서: IAM 사용자에게 권한을 위임하기 위한 역할 생성"](#) 를 참조하십시오.

클라우드 복원 인터넷 액세스를 확인합니다

가상 또는 물리적 네트워크에서 인터넷 액세스에 프록시 서버를 사용하는 경우 클라우드 복원 인스턴스에 다음 끝점에 연결할 수 있는 아웃바운드 인터넷 액세스 권한이 있는지 확인합니다.

엔드포인트	목적
<a href="http://amazonlinux.us-east-1.amazonaws.com/2/extras/docker/stable/x86_64/4bf88ee77c395ffe1e0c3ca68530dfb3a683ec65a4a1ce9c0ff394be50e922b2/">http://amazonlinux.us-east-1.amazonaws.com/2/extras/docker/stable/x86_64/4bf88ee77c395ffe1e0c3ca68530dfb3a683ec65a4a1ce9c0ff394be50e922b2/</a>	클라우드 복원 인스턴스 AMI용 CentOS 패키지.

엔드포인트	목적
<a href="https://download.docker.com/linux/centos/docker-ce.repo">https://download.docker.com/linux/centos/docker-ce.repo</a> 으로 문의하십시오	Docker Engine 패키지를 제공합니다.
<a href="http://cloudmanagerinfraprod.azurecr.io">http://cloudmanagerinfraprod.azurecr.io</a> <a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a> 으로 문의하십시오	클라우드 복원 인스턴스 이미지 리포지토리.

데이터 암호화를 위해 고객이 관리하는 **AWS** 키 설정

기본 Amazon S3 암호화 키를 사용하여 온프레미스 클러스터와 S3 버킷 사이에 전달된 데이터를 암호화하려는 경우 기본 설치에 해당 암호화 유형이 사용되기 때문에 모두 설정됩니다.

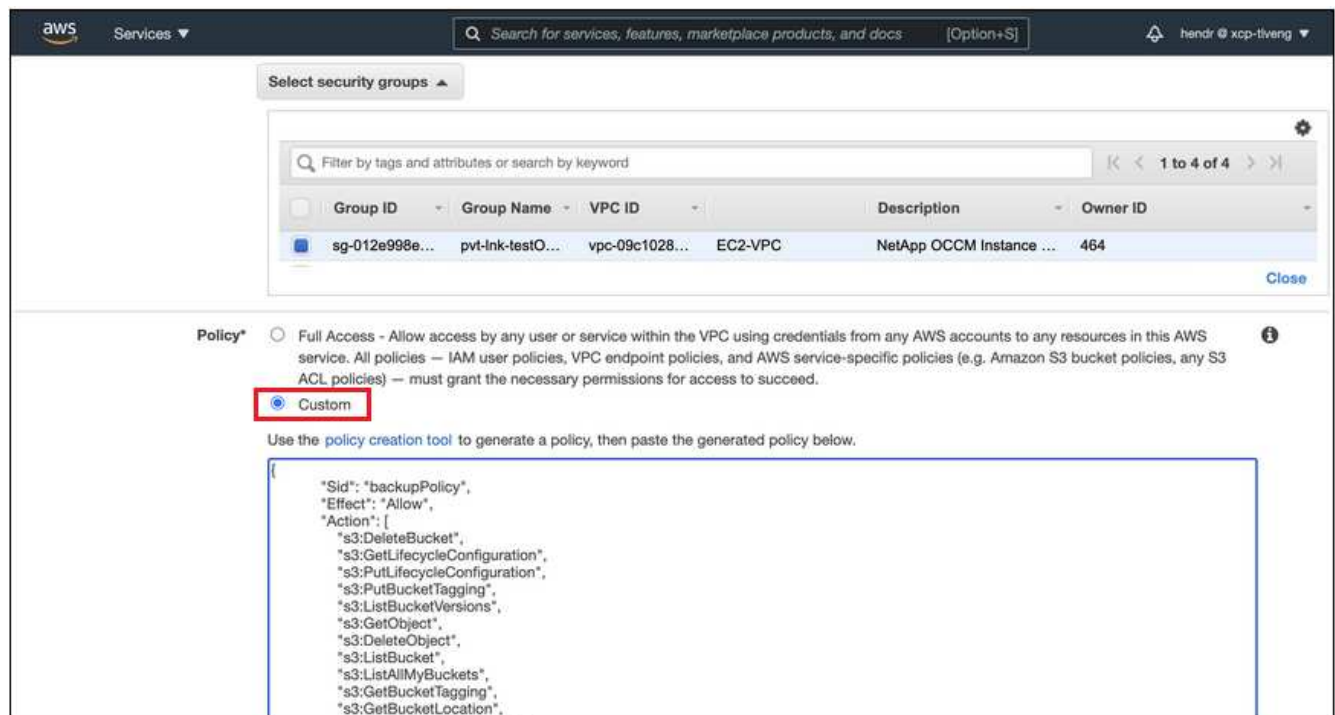
기본 키를 사용하는 대신 고객이 관리하는 키를 데이터 암호화에 사용하려면 Cloud Backup 마법사를 시작하기 전에 암호화 관리 키를 이미 설정해야 합니다. "[자신의 키를 사용하는 방법을 확인하십시오](#)".

**VPC** 엔드포인트 인터페이스를 사용하여 전용 연결을 위해 시스템을 구성합니다

표준 공용 인터넷 연결을 사용하려는 경우 모든 권한은 Connector에 의해 설정되며 다른 작업은 필요하지 않습니다. 이 연결 유형은 에 나와 있습니다 "[첫 번째 다이어그램](#)".

사내 데이터 센터에서 VPC로 인터넷을 통해 보다 안전하게 연결하려면 백업 활성화 마법사에서 AWS PrivateLink 연결을 선택하는 옵션이 있습니다. VPN 또는 AWS Direct Connect를 사용하여 프라이빗 IP 주소를 사용하는 VPC 엔드포인트 인터페이스를 통해 사내 시스템을 연결하려는 경우 필요합니다. 이 연결 유형은 에 나와 있습니다 "[두 번째 다이어그램](#)".

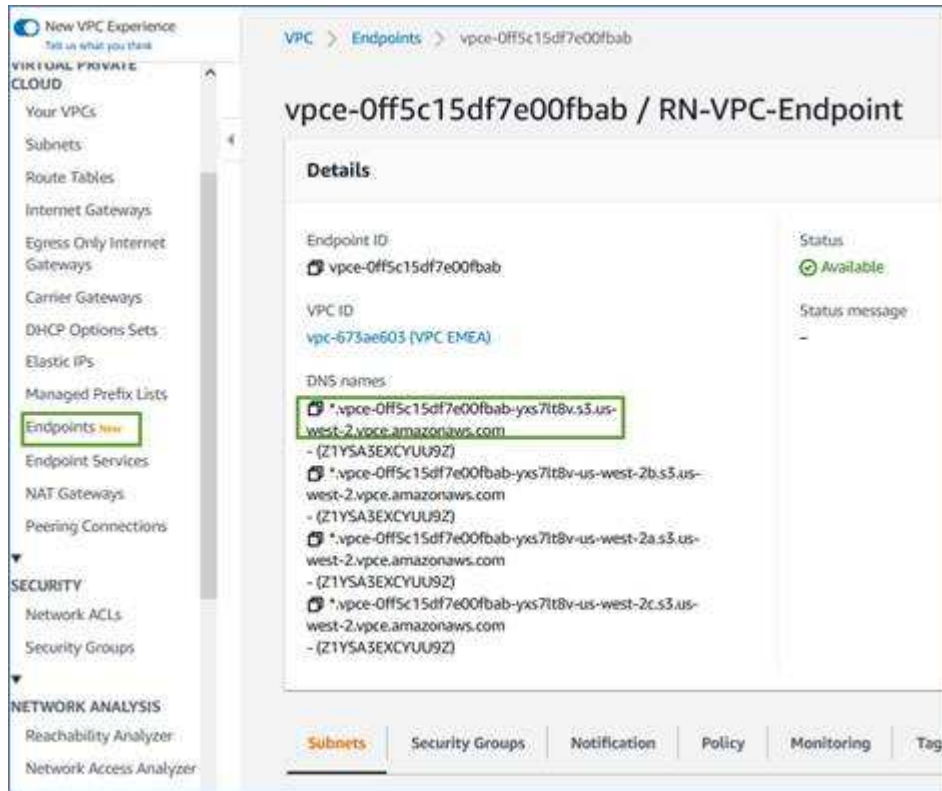
1. Amazon VPC 콘솔 또는 명령줄을 사용하여 인터페이스 엔드포인트 구성을 생성합니다. "[Amazon S3에 AWS PrivateLink를 사용하는 방법에 대한 자세한 정보를 확인하십시오](#)".
2. Cloud Manager Connector와 연결된 보안 그룹 구성을 수정합니다. 정책을 "사용자 지정"("전체 액세스"에서)으로 변경해야 하며 반드시 다음을 수행해야 합니다 [백업 정책에서 S3 권한을 추가합니다](#) 앞서 설명한 것처럼.



개인 엔드포인트와 통신하는 데 포트 80(HTTP)을 사용하는 경우 모두 설정됩니다. 지금 클러스터에서 Cloud Backup을 활성화할 수 있습니다.

개인 엔드포인트와 통신하는 데 포트 443(HTTPS)을 사용하는 경우 다음 4단계에 나와 있는 것처럼 VPC S3 엔드포인트에서 인증서를 복사하여 ONTAP 클러스터에 추가해야 합니다.

3. AWS 콘솔에서 엔드포인트의 DNS 이름을 가져옵니다.



4. VPC S3 엔드포인트에서 인증서를 가져옵니다. 당신은 이렇게 합니다 "Cloud Manager Connector를 호스팅하는 VM에 로그인합니다" 다음 명령을 실행합니다. 엔드포인트의 DNS 이름을 입력할 때 "\*"를 대체하여 "bucket"을 앞에 추가합니다.

```
[ec2-user@ip-10-160-4-68 ~]$ openssl s_client -connect bucket.vpce-0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443 -showcerts
```

5. 이 명령의 출력에서 S3 인증서(BEGIN /end certificate 태그 사이에 있는 모든 데이터)를 복사합니다.

```
Certificate chain
0 s:/CN=s3.us-west-2.amazonaws.com`
  i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
-----BEGIN CERTIFICATE-----
MIIM6zCCC9OgAwIBAgIQA7MGJ4FaDBR8uL0KR3oltTANBgkqhkiG9w0BAQsFADBG
...
...
GqvbOz/oo2NWLLFCqI+xmKLCmiPrZy+/6Af+HH2mLCM4EsI2b+IpBmPkriWnnxo=
-----END CERTIFICATE-----
```

6. ONTAP 클러스터 CLI에 로그인하여 다음 명령을 사용하여 복사한 인증서를 적용합니다(자체 스토리지 VM 이름 대체).

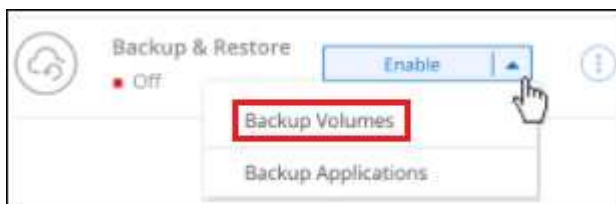
```
cluster1::> security certificate install -vserver cluster1 -type server-
ca
Please enter Certificate: Press <Enter> when done
```

## 클라우드 백업 활성화

사내 작업 환경에서 언제든지 직접 Cloud Backup을 사용할 수 있습니다.

단계

1. Canvas에서 작업 환경을 선택하고 오른쪽 패널의 백업 및 복원 서비스 옆에 있는 \* 활성화 > 볼륨 백업 \* 을 클릭합니다.



2. 공급자로서 Amazon Web Services를 선택하고 \* 다음 \* 을 클릭합니다.
3. 제공업체 세부사항을 입력하고 \* 다음 \* 을 클릭합니다.
  - a. 백업을 저장하는 데 사용되는 AWS 계정, AWS 액세스 키 및 비밀 키  
  
 액세스 키 및 비밀 키는 ONTAP 클러스터에 S3 버킷을 액세스할 수 있도록 생성한 IAM 사용자를 위한 것입니다.
  - b. 백업이 저장될 AWS 영역입니다.
  - c. 기본 Amazon S3 암호화 키를 사용할지, AWS 계정에서 고객이 직접 관리하는 키를 선택할지 상관없이 데이터 암호화를 관리하게 됩니다. ("[자신의 키를 사용하는 방법을 확인하십시오](#)")를 클릭합니다.



### Provider Settings

#### Provider Information

AWS Account:

AWS Access Key:

AWS Secret Key:

#### Location & Connectivity

Region:

Encryption ?

Encryption Key Type: AWS SSE-S3 [Change Key](#)

4. 계정에 대한 기존 Cloud Backup 라이선스가 없는 경우 이 시점에서 사용할 충전 방법 유형을 선택하라는 메시지가 표시됩니다. AWS에서 PAYGO(Pay-as-you-Go) Cloud Manager Marketplace 오퍼링을 구독하거나(또는 구독을 여러 개 선택한 경우) NetApp에서 Cloud Backup BYOL 라이선스를 구입하여 활성화할 수 있습니다. ["Cloud Backup 라이선스를 설정하는 방법에 대해 알아보십시오."](#)
5. 네트워킹 세부 정보를 입력하고 \* 다음 \* 을 클릭합니다.
  - a. 백업할 볼륨이 상주하는 ONTAP 클러스터의 IPspace 이 IPspace용 인터클러스터 LIF는 아웃바운드 인터넷 액세스를 가져야 합니다.
  - b. 필요에 따라 이전에 구성한 AWS PrivateLink를 사용할지 여부를 선택합니다. ["Amazon S3에 AWS PrivateLink를 사용하는 방법에 대한 자세한 정보를 확인하십시오."](#)

### Networking

IPspace

☒ Private Link Configuration

Select Private Link

	Name	VPC	Endpoint ID
<input type="radio"/>	Private_Link_Name_001	vpce0-012345678901234567890 (Default)	vpce0-012345678901234567890
<input type="radio"/>	Private_Link_Name_002	vpce0-012345678901234567890 (k8s)	vpce0-012345678901234567890

6. 기본 백업 정책 세부 정보를 입력하고 \* 다음 \* 을 클릭합니다.
  - a. 백업 스케줄을 정의하고 보존할 백업 수를 선택합니다. ["선택할 수 있는 기존 정책 목록을 봅니다."](#)
  - b. ONTAP 9.10.1 이상을 사용하는 경우 추가 비용 최적화를 위해 일정 일 후에 S3 Glacier 또는 S3 Glacier Deep Archive 스토리지에 백업을 계층화하도록 선택할 수 있습니다. ["아카이브 계층 사용에 대해 자세히 알아보십시오."](#)

### Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule** ☒ Create a New Policy ☐ Select an Existing Policy

☐ Hourly

Number of backups to retain

24

☒ Daily

Number of backups to retain

30

☐ Weekly

Number of backups to retain

52

☐ Monthly

Number of backups to retain

12

---

**Archival Policy**

Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.

☒ Tier Backups to Archival

Archive after (Days)

Storage Class

30

S3 Glacier  
 S3 Glacier  
 S3 Glacier Deep Archive

**S3 Bucket** Cloud Manager will create the S3 bucket for you. Wizard

7. Select Volumes(볼륨 선택) 페이지의 기본 백업 정책을 사용하여 백업할 볼륨을 선택합니다. 특정 볼륨에 서로 다른 백업 정책을 할당하려는 경우 추가 정책을 생성하여 나중에 해당 볼륨에 적용할 수 있습니다.

- 모든 볼륨을 백업하려면 제목 행(☒ Volume Name)를 클릭합니다.
- 개별 볼륨을 백업하려면 각 볼륨에 대한 확인란을 선택합니다(☒ Volume\_1)를 클릭합니다.

### Select Volumes

57 Volumes

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 On	DP	SVM_Name_2	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active

☒ Automatically back up future volumes on all storage VMs with the selected backup policy

나중에 추가된 모든 볼륨에 백업을 사용하려면 "Automatically back up future volumes..." 확인란을 선택하기만 하면 됩니다. 이 설정을 비활성화하면 이후 볼륨에 대해 백업을 수동으로 활성화해야 합니다.

8. 백업 활성화 \* 를 클릭하면 Cloud Backup이 볼륨의 초기 백업을 시작합니다.

Cloud Backup은 선택한 각 볼륨의 초기 백업을 시작하고, 백업 상태를 모니터링할 수 있도록 Volume Backup

Dashboard가 표시됩니다.

가능합니다 "볼륨에 대한 백업을 시작 및 중지하거나 백업 일정을 변경합니다". 또한 가능합니다 "백업 파일에서 전체 볼륨 또는 개별 파일을 복원합니다" AWS의 Cloud Volumes ONTAP 시스템 또는 사내 ONTAP 시스템으로 전환

## 온프레미스 ONTAP 데이터를 Azure Blob 저장소에 백업

몇 가지 단계를 완료하여 사내 ONTAP 시스템에서 Azure Blob 저장소로 데이터 백업을 시작하십시오.

"사내 ONTAP 시스템"에는 FAS, AFF 및 ONTAP Select 시스템이 포함됩니다.

### 빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션을 아래로 스크롤하여 자세한 내용을 확인하십시오.

<https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-1.png>  
Alt="One" 구성에 대한 지원을 확인합니다

- 온프레미스 클러스터를 검색한 후 Cloud Manager의 작업 환경에 추가했습니다. 을 참조하십시오 "ONTAP 클러스터 검색" 를 참조하십시오.
  - 클러스터에서 ONTAP 9.7P5 이상이 실행 중입니다.
  - 클러스터에는 SnapMirror 라이선스가 있으며, 이 라이선스는 프리미엄 번들 또는 데이터 보호 번들의 일부로 포함됩니다.
  - 클러스터에는 Blob 저장소 및 커넥터에 대한 필수 네트워크 연결이 있어야 합니다.
- Connector는 Blob 저장소 및 클러스터에 대한 필수 네트워크 연결과 필요한 권한이 있어야 합니다.
- 백업이 위치할 오브젝트 스토리지 공간에 대한 유효한 Azure 구독이 있습니다.

작업 환경을 선택하고 오른쪽 패널에서 백업 및 복원 서비스 옆에 있는 \* 활성화 > 볼륨 백업 \* 을 클릭한 다음 설정 마법사를 따릅니다.



공급자로서 Microsoft Azure를 선택한 다음 공급자 세부 정보를 입력합니다. 백업을 생성할 Azure 가입 및 지역을 선택해야 합니다. 기본 Microsoft 관리 암호화 키를 사용하는 대신 데이터 암호화에 대해 고객이 관리하는 키를 직접 선택할 수도 있습니다.

**Provider Settings**

Azure Subscription: Azure\_Subscription\_1

Region: Default\_CM\_Region

Resource Group: ☐ Create a new ☒ Use an existing  
Select an Existing Resource Group: Resource\_Group\_1

Encryption: ☒ Microsoft-managed ☐ Customer-managed

볼륨이 상주하는 ONTAP 클러스터에서 IPspace를 선택합니다. 온프레미스 데이터 센터에서 VNET에 보다 안전하게 연결할 수 있도록 기존 Azure 프라이빗 끝점을 사용하도록 선택할 수도 있습니다.

**Networking**

IPspace: IP\_Space\_1

☒ Private Endpoint Configuration

VNet: Select VNet

Subnet: Select Subnet

기본 정책은 매일 볼륨을 백업하고 각 볼륨의 최근 30개 백업 복사본을 유지합니다. 시간별, 일별, 주별 또는 월별 백업으로 변경하거나 더 많은 옵션을 제공하는 시스템 정의 정책 중 하나를 선택합니다. 보존할 백업 복사본의 수를 변경할 수도 있습니다.

기본적으로 백업은 Cool 액세스 계층에 저장됩니다. 클러스터에서 ONTAP 9.10.1 이상을 사용하는 경우 추가 비용 최적화를 위해 일정 일 후에 Azure 아카이브 스토리지에 백업을 계층화하도록 선택할 수 있습니다.

## Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule**

☒ Create a New Policy
☐ Select an Existing Policy

☐ Hourly
 Number of backups to retain:

☒ Daily
 Number of backups to retain:

☐ Weekly
 Number of backups to retain:

☐ Monthly
 Number of backups to retain:

**Archival Policy**

Backups reside in Cool Azure Blob storage for frequently accessed data.  
Optionally, you can tier backups to Azure Archive storage for further cost optimization.

☒ Tier Backups to Archival

Archive after (Days)
Access Tier

Azure Archive

**Storage Account**

Cloud Manager will create the storage account after you complete the wizard

Select Volumes(볼륨 선택) 페이지의 기본 백업 정책을 사용하여 백업할 볼륨을 식별합니다. 특정 볼륨에 서로 다른 백업 정책을 할당하려면 추가 정책을 생성한 후 나중에 볼륨에 적용할 수 있습니다.

## 요구 사항

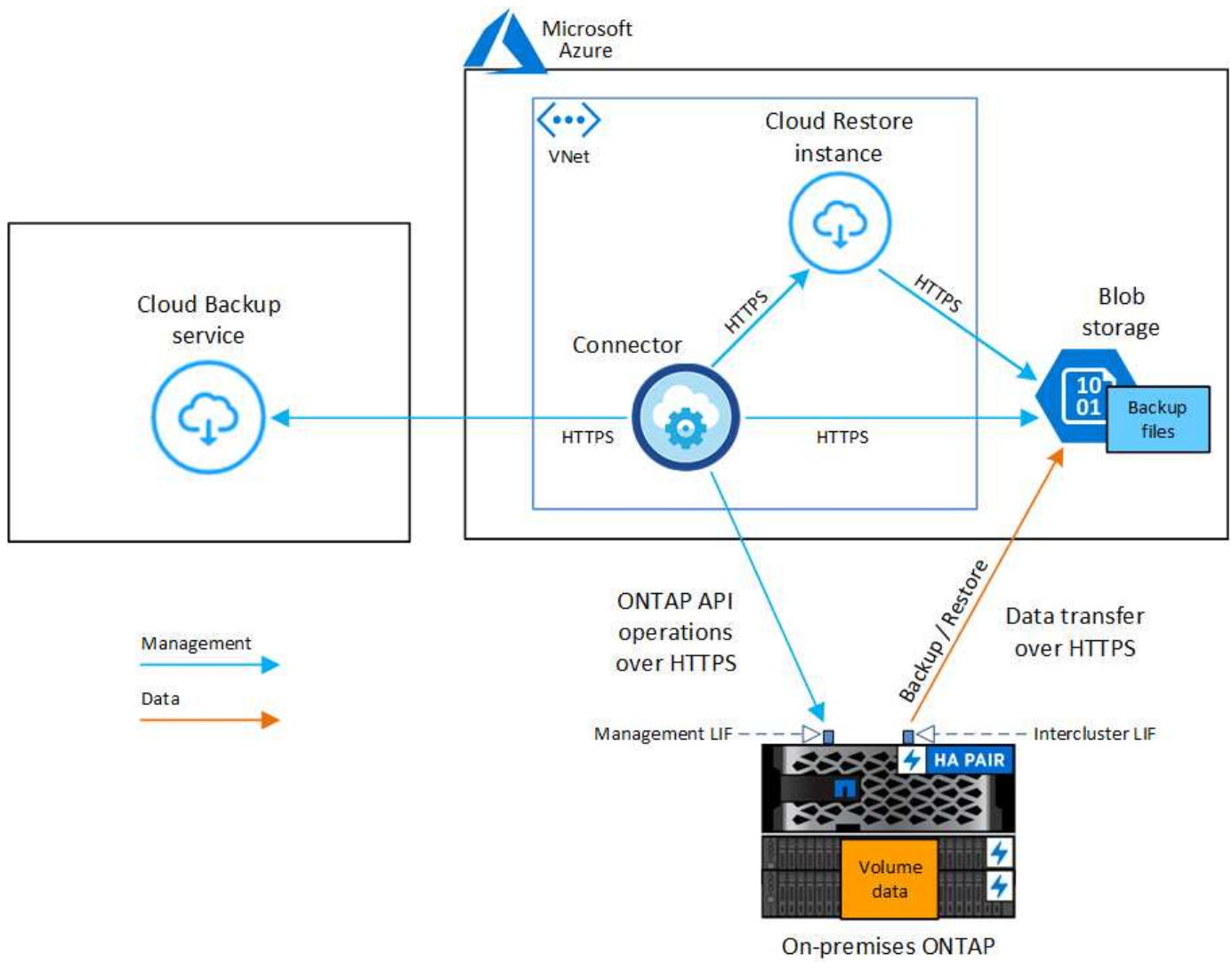
온프레미스 볼륨을 Azure Blob 저장소에 백업하기 전에 다음 요구 사항을 읽고 지원되는 구성이 있는지 확인합니다.

사내 ONTAP 시스템에서 Azure Blob으로 백업을 구성할 때 사용할 수 있는 두 가지 연결 방법이 있습니다.

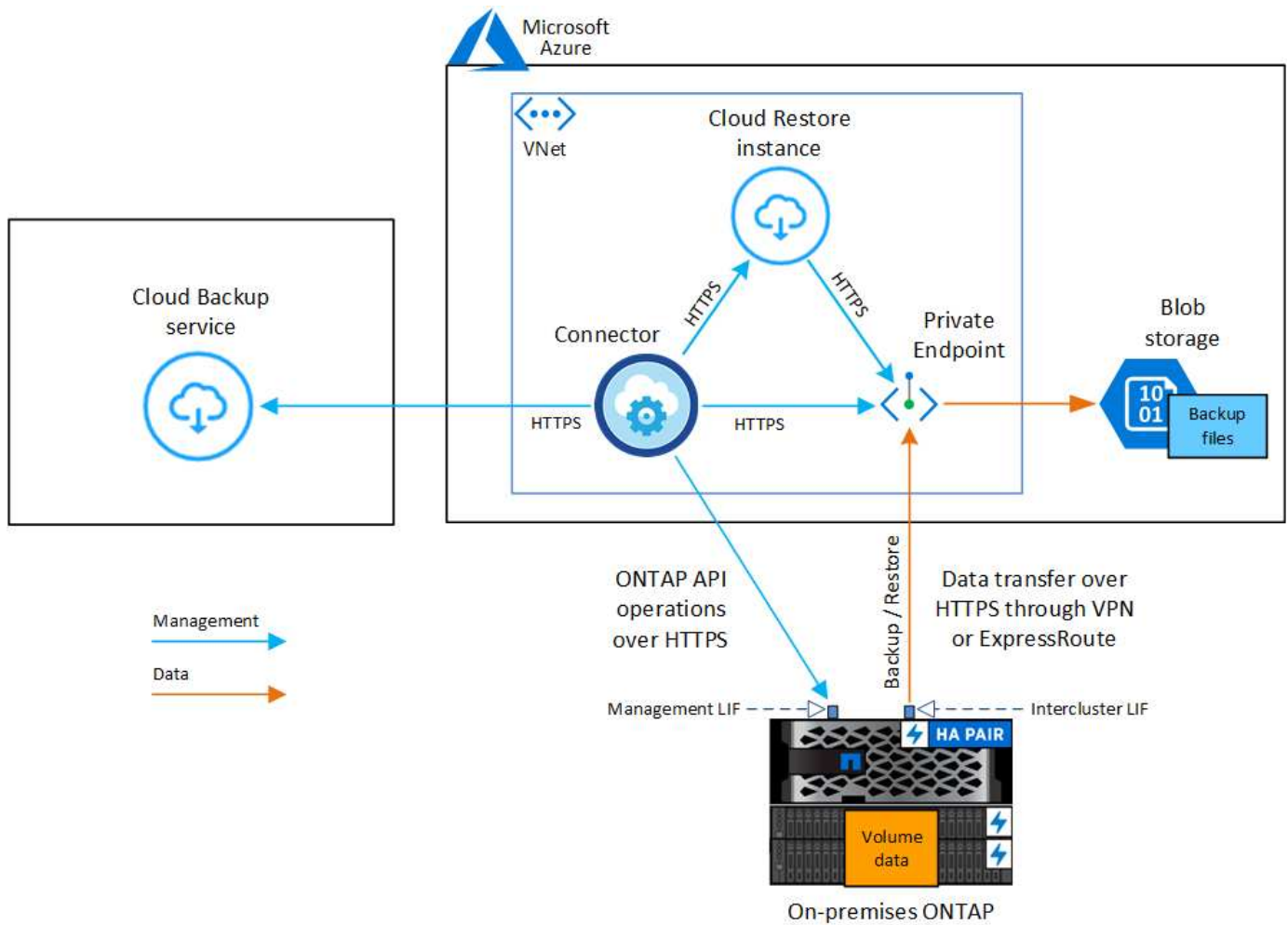
- 공용 연결 - 공용 Azure 끝점을 사용하여 ONTAP 시스템을 Azure Blob 저장소에 직접 연결합니다.
- 비공개 연결 - VPN 또는 ExpressRoute를 사용하여 전용 IP 주소를 사용하는 VNET 전용 엔드포인트를 통해 트래픽을 라우팅합니다.

다음 그림에서는 공용 연결 방법과 구성 요소 간에 준비해야 하는 연결을 보여 줍니다.

43



다음 그림에서는 전용 연결 방법과 구성 요소 간에 준비해야 하는 연결을 보여 줍니다.



Cloud Restore 인스턴스가 클라우드에 배포되면 Connector와 동일한 서브넷에 위치합니다.

## ONTAP 클러스터 준비

볼륨 데이터 백업을 시작하려면 Cloud Manager에서 사내 ONTAP 클러스터를 검색해야 합니다.

"클러스터를 검색하는 방법에 대해 알아보십시오".

## ONTAP 요구 사항

- ONTAP 9.7P5 이상
- SnapMirror 라이선스(프리미엄 번들 또는 데이터 보호 번들의 일부로 포함)
- 참고: \* Cloud Backup을 사용할 때는 "하이브리드 클라우드 번들"이 필요하지 않습니다.

자세한 내용은 를 참조하십시오 "클러스터 라이선스를 관리합니다".

- 시간 및 시간대가 올바르게 설정되었습니다.

자세한 내용은 를 참조하십시오 "클러스터 시간을 구성합니다".

## 클러스터 네트워킹 요구 사항

- ONTAP 클러스터는 백업 및 복원 작업을 위해 인터클러스터 LIF에서 Azure Blob 스토리지의 포트 443을



통한 HTTPS 연결을 시작합니다.

ONTAP은 오브젝트 스토리지 간에 데이터를 읽고 씁니다. 오브젝트 스토리지는 한 번도 시작되고, 응답 하기만 합니다.

- ONTAP를 사용하려면 Connector에서 클러스터 관리 LIF로 인바운드 연결이 필요합니다. 커넥터는 Azure VNET에 상주할 수 있습니다.
- 인터클러스터 LIF는 백업할 볼륨을 호스팅하는 각 ONTAP 노드에 필요합니다. LIF는 ONTAP가 오브젝트 스토리지에 연결하는 데 사용해야 하는 \_IPspace\_와 연결되어 있어야 합니다. "[IPspace에 대해 자세히 알아보십시오](#)".

클라우드 백업을 설정하면 사용할 IPspace를 묻는 메시지가 표시됩니다. 각 LIF가 연결되는 IPspace를 선택해야 합니다. 이는 여러분이 생성한 "기본" IPspace 또는 사용자 지정 IPspace가 될 수 있습니다.

- 노드의 및 인터클러스터 LIF는 오브젝트 저장소에 액세스할 수 있습니다.
- 볼륨이 있는 스토리지 VM에 대해 DNS 서버가 구성되었습니다. 자세한 내용은 를 참조하십시오 "[SVM을 위한 DNS 서비스 구성](#)".
- 을 사용하는 경우 기본값 이외의 IPspace를 사용하는 경우 오브젝트 스토리지에 액세스하려면 정적 라우트를 생성해야 할 수 있습니다.
- 필요한 경우 포트 443을 통해 ONTAP에서 오브젝트 스토리지로 Cloud Backup Service 연결을 허용하고 포트 53(TCP/UDP)을 통해 스토리지 VM에서 DNS 서버로 이름 확인 트래픽을 허용하도록 방화벽 규칙을 업데이트합니다.

## 커넥터 작성 또는 전환

Azure Blob 저장소에 데이터를 백업할 때는 Connector가 Azure VNET에 있고, Connector는 클라우드에 데이터를 백업하는 데 필요합니다. 온-프레미스에 배포된 Connector는 사용할 수 없습니다. 새 커넥터를 만들거나 현재 선택한 커넥터가 올바른 공급자에 있는지 확인해야 합니다.

- "[커넥터에 대해 자세히 알아보십시오](#)"
- "[Azure에서 커넥터 만들기](#)"
- "[커넥터 간 전환](#)"

## 커넥터를 위한 네트워킹 준비

커넥터에 필요한 네트워크 연결이 있는지 확인합니다.

### 단계

1. 커넥터가 설치된 네트워크에서 다음 연결을 사용할 수 있는지 확인합니다.
  - 포트 443(HTTPS)을 통해 Cloud Backup Service에 아웃바운드 인터넷 연결
  - Blob 개체 저장소에 대한 포트 443을 통한 HTTPS 연결
  - 포트 443을 통해 ONTAP 클러스터 관리 LIF에 HTTPS로 연결합니다
2. Azure 스토리지에 VNET 프라이빗 엔드포인트를 설정합니다. 이 기능은 ONTAP 클러스터에서 VNET로 ExpressRoute 또는 VPN 연결을 사용하는 경우, Connector와 Blob 스토리지 간의 통신을 가상 프라이빗 네트워크에 유지하는 데 필요합니다.



## 지원 지역

모든 지역의 온프레미스 시스템에서 Azure Blob으로 백업을 생성할 수 있습니다 "[Cloud Volumes ONTAP가 지원되는 경우](#)" Azure Government 지역을 비롯한 모든 지역에서 사용할 수 있습니다. 서비스를 설정할 때 백업을 저장할 지역을 지정합니다.

## 라이선스 요구 사항을 확인합니다

- 클러스터에 대한 Cloud Backup을 활성화하려면 먼저 Azure에서 PAYGO(Pay-as-you-Go) Cloud Manager Marketplace 오퍼링을 구독하거나 NetApp에서 Cloud Backup BYOL 라이선스를 구입하여 활성화해야 합니다. 이러한 라이선스는 사용자 계정용이며 여러 시스템에서 사용할 수 있습니다.
  - Cloud Backup PAYGO 라이선스의 경우 에 대한 구독이 필요합니다 "[Azure를 지원합니다](#)" Cloud Backup을 사용하는 Cloud Manager Marketplace 오퍼링 Cloud Backup에 대한 청구는 이 구독을 통해 이루어집니다.
  - Cloud Backup BYOL 라이선스의 경우, 라이선스 기간 및 용량 동안 서비스를 사용할 수 있도록 지원하는 NetApp의 일련 번호가 필요합니다. "[BYOL 라이선스 관리 방법에 대해 알아보십시오](#)".
- 백업이 위치할 오브젝트 스토리지 공간에 Azure를 구독해야 합니다.

모든 지역의 온프레미스 시스템에서 Azure Blob으로 백업을 생성할 수 있습니다 "[Cloud Volumes ONTAP가 지원되는 경우](#)" Azure Government 지역을 비롯한 모든 지역에서 사용할 수 있습니다. 서비스를 설정할 때 백업을 저장할 지역을 지정합니다.

## 백업을 위한 **Azure Blob** 저장소 준비

- 가상 또는 물리적 네트워크에서 인터넷 액세스에 프록시 서버를 사용하는 경우 클라우드 복원 가상 시스템이 다음 끝점에 연결할 수 있는 아웃바운드 인터넷 액세스를 가지고 있는지 확인합니다.

엔드포인트	목적
<a href="http://olcentgbl.trafficmanager.net">http://olcentgbl.trafficmanager.net</a> <a href="https://olcentgbl.trafficmanager.net">https://olcentgbl.trafficmanager.net</a> 으로 문의하십시오	클라우드 복원 가상 머신용 CentOS 패키지를 제공합니다.
<a href="https://download.docker.com/linux/centos/docker-ce.repo">https://download.docker.com/linux/centos/docker-ce.repo</a> 으로 문의하십시오	Docker Engine 패키지를 제공합니다.
<a href="http://cloudmanagerinfraprod.azurecr.io">http://cloudmanagerinfraprod.azurecr.io</a> <a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a> 으로 문의하십시오	클라우드 복원 가상 머신 이미지 리포지토리.

- 기본 Microsoft 관리 암호화 키를 사용하는 대신 활성화 마법사에서 데이터 암호화에 대해 사용자 지정 관리 키를 선택합니다. 이 경우 Azure 가입, 키 저장소 이름 및 키가 필요합니다. "[자신의 키를 사용하는 방법을 확인하십시오](#)".
- 온프레미스 데이터 센터에서 VNET로 공용 인터넷을 통해 보다 안전하게 연결하려면 활성화 마법사에서 Azure 프라이빗 끝점을 구성하는 옵션이 있습니다. 이 경우 이 연결에 대한 VNET 및 서브넷을 알아야 합니다. "[개인 엔드포인트 사용에 대한 자세한 내용을 참조하십시오](#)".

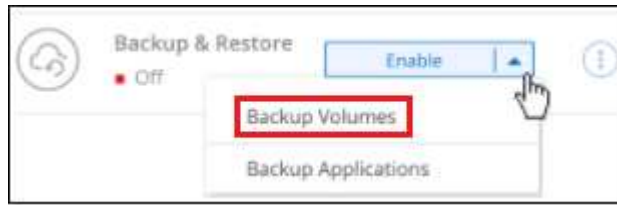
## 클라우드 백업 활성화

사내 작업 환경에서 언제든지 직접 Cloud Backup을 사용할 수 있습니다.

### 단계

- Canvas에서 작업 환경을 선택하고 오른쪽 패널의 백업 및 복원 서비스 옆에 있는 \* 활성화 > 볼륨 백업 \* 을

클릭합니다.



2. 공급자로서 Microsoft Azure를 선택하고 \* 다음 \* 을 클릭합니다.
3. 제공업체 세부사항을 입력하고 \* 다음 \* 을 클릭합니다.
  - a. 백업에 사용되는 Azure 가입 및 백업을 저장할 Azure 지역
  - b. Blob 컨테이너를 관리하는 리소스 그룹 - 새 리소스 그룹을 만들거나 기존 리소스 그룹을 선택할 수 있습니다.
  - c. 기본 Microsoft 관리 암호화 키를 사용할지 또는 고객이 관리하는 키를 직접 선택하여 데이터 암호화를 관리할지 여부를 결정합니다. ("[자신의 키를 사용하는 방법을 확인하십시오](#)")를 클릭합니다.

4. 계정에 대한 기존 Cloud Backup 라이선스가 없는 경우 이 시점에서 사용할 충전 방법 유형을 선택하라는 메시지가 표시됩니다. Azure에서 PAYGO(Pay-as-you-Go) Cloud Manager Marketplace 오퍼링을 구독하거나(또는 구독을 여러 개 선택한 경우) NetApp에서 Cloud Backup BYOL 라이선스를 구입하여 활성화할 수 있습니다. "[Cloud Backup 라이선스를 설정하는 방법에 대해 알아보십시오](#)."
5. 네트워킹 세부 정보를 입력하고 \* 다음 \* 을 클릭합니다.
  - a. 백업할 볼륨이 상주하는 ONTAP 클러스터의 IPspace 이 IPspace용 인터클러스터 LIF는 아웃바운드 인터넷 액세스를 가져야 합니다.
  - b. 필요에 따라 Azure 프라이빗 끝점을 구성할지 여부를 선택합니다. "[개인 엔드포인트 사용에 대한 자세한 내용을 참조하십시오](#)".

**Networking**

IPspace  
IP\_Space\_1

☐ Private Endpoint Configuration

VNet  
Select VNet

Subnet  
Select Subnet

6. 기본 백업 정책 세부 정보를 입력하고 \* 다음 \* 을 클릭합니다.

- 백업 스케줄을 정의하고 보존할 백업 수를 선택합니다. ["선택할 수 있는 기존 정책 목록을 봅니다"](#).
- ONTAP 9.10.1 이상을 사용하는 경우 추가 비용 최적화를 위해 일정 일 후에 Azure 아카이브 스토리지에 백업을 계층화하도록 선택할 수 있습니다. ["아카이브 계층 사용에 대해 자세히 알아보십시오"](#).

**Define Policy**

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule** ☒ Create a New Policy ☐ Select an Existing Policy

<input type="checkbox"/> Hourly	Number of backups to retain	24
<input checked="" type="checkbox"/> Daily	Number of backups to retain	30
<input type="checkbox"/> Weekly	Number of backups to retain	52
<input type="checkbox"/> Monthly	Number of backups to retain	12

**Archival Policy**

Backups reside in Cool Azure Blob storage for frequently accessed data.  
Optionally, you can tier backups to Azure Archive storage for further cost optimization.

☒ Tier Backups to Archival

Archive after (Days): 30 | Access Tier: Azure Archive

**Storage Account** Cloud Manager will create the storage account after you complete the wizard

7. Select Volumes(볼륨 선택) 페이지의 기본 백업 정책을 사용하여 백업할 볼륨을 선택합니다. 특정 볼륨에 서로 다른 백업 정책을 할당하려는 경우 추가 정책을 생성하여 나중에 해당 볼륨에 적용할 수 있습니다.

- 모든 볼륨을 백업하려면 제목 행(☒ Volume Name)를 클릭합니다.
- 개별 볼륨을 백업하려면 각 볼륨에 대한 확인란을 선택합니다(☒ Volume\_1)를 클릭합니다.

Select Volumes						
57 Volumes						
<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 On	DP	SVM_Name_2	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/> Automatically back up future volumes on all storage VMs with the selected backup policy						

나중에 추가된 모든 볼륨에 백업을 사용하려면 "Automatically back up future volumes..." 확인란을 선택하기만 하면 됩니다. 이 설정을 비활성화하면 이후 볼륨에 대해 백업을 수동으로 활성화해야 합니다.

8. 백업 활성화 \* 를 클릭하면 Cloud Backup이 볼륨의 초기 백업을 시작합니다.

Cloud Backup은 선택한 각 볼륨의 초기 백업을 시작하고, 백업 상태를 모니터링할 수 있도록 Volume Backup Dashboard가 표시됩니다.

가능합니다 "볼륨에 대한 백업을 시작 및 중지하거나 백업 일정을 변경합니다". 또한 가능합니다 "백업 파일에서 전체 볼륨 또는 개별 파일을 복원합니다" Azure의 Cloud Volumes ONTAP 시스템 또는 사내 ONTAP 시스템으로 데이터를 이동합니다.

## 사내 ONTAP 데이터를 Google 클라우드 스토리지로 백업

몇 가지 단계를 완료하여 사내 ONTAP 시스템에서 Google 클라우드 스토리지로 데이터 백업을 시작하십시오.

"사내 ONTAP 시스템"에는 FAS, AFF 및 ONTAP Select 시스템이 포함됩니다.

### 빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션을 아래로 스크롤하여 자세한 내용을 확인하십시오.

<https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-1.png>  
 구성에 대한 지원을 확인합니다

- 온프레미스 클러스터를 검색한 후 Cloud Manager의 작업 환경에 추가했습니다. 을 참조하십시오 **"ONTAP 클러스터 검색"** 를 참조하십시오.
  - 클러스터에서 ONTAP 9.7P5 이상이 실행 중입니다.
  - 클러스터에는 SnapMirror 라이선스가 있으며, 이 라이선스는 프리미엄 번들 또는 데이터 보호 번들의 일부로 포함됩니다.
  - 클러스터에는 Google 스토리지 및 커넥터에 대한 필수 네트워크 연결이 있어야 합니다.

- 커넥터는 Google 스토리지 및 클러스터에 필요한 네트워크 연결을 가지고 있어야 합니다.
- 백업이 위치할 객체 저장소 공간에 대한 유효한 Google 가입이 있습니다.
- ONTAP 클러스터에서 데이터를 백업 및 복원할 수 있도록 액세스 키와 비밀 키가 있는 Google 계정이 있습니다.

작업 환경을 선택하고 오른쪽 패널에서 백업 및 복원 서비스 옆에 있는 \* 활성화 > 볼륨 백업 \* 을 클릭한 다음 설정 마법사를 따릅니다.



Google Cloud를 공급자로 선택한 다음 공급자 세부 정보를 입력합니다. 또한 볼륨이 상주하는 ONTAP 클러스터에서 IPspace를 지정해야 합니다.

기본 정책은 매일 볼륨을 백업하고 각 볼륨의 최근 30개 백업 복사본을 유지합니다. 시간별, 일별, 주별 또는 월별 백업으로 변경하거나 더 많은 옵션을 제공하는 시스템 정의 정책 중 하나를 선택합니다. 보존할 백업 복사본의 수를 변경할 수도 있습니다.

### Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule**
☒ Create a New Policy
 ☐ Select an Existing Policy

☐ Hourly
 Number of backups to retain

☒ Daily
 Number of backups to retain

☐ Weekly
 Number of backups to retain

☐ Monthly
 Number of backups to retain

**DP Volumes**

Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

**Google Cloud Storage Bucket**

Cloud Manager will create the Google Cloud Storage Bucket after you complete the wizard

Select Volumes(볼륨 선택) 페이지의 기본 백업 정책을 사용하여 백업할 볼륨을 식별합니다. 특정 볼륨에 서로 다른 백업 정책을 할당하려면 추가 정책을 생성한 후 나중에 볼륨에 적용할 수 있습니다.

## 요구 사항

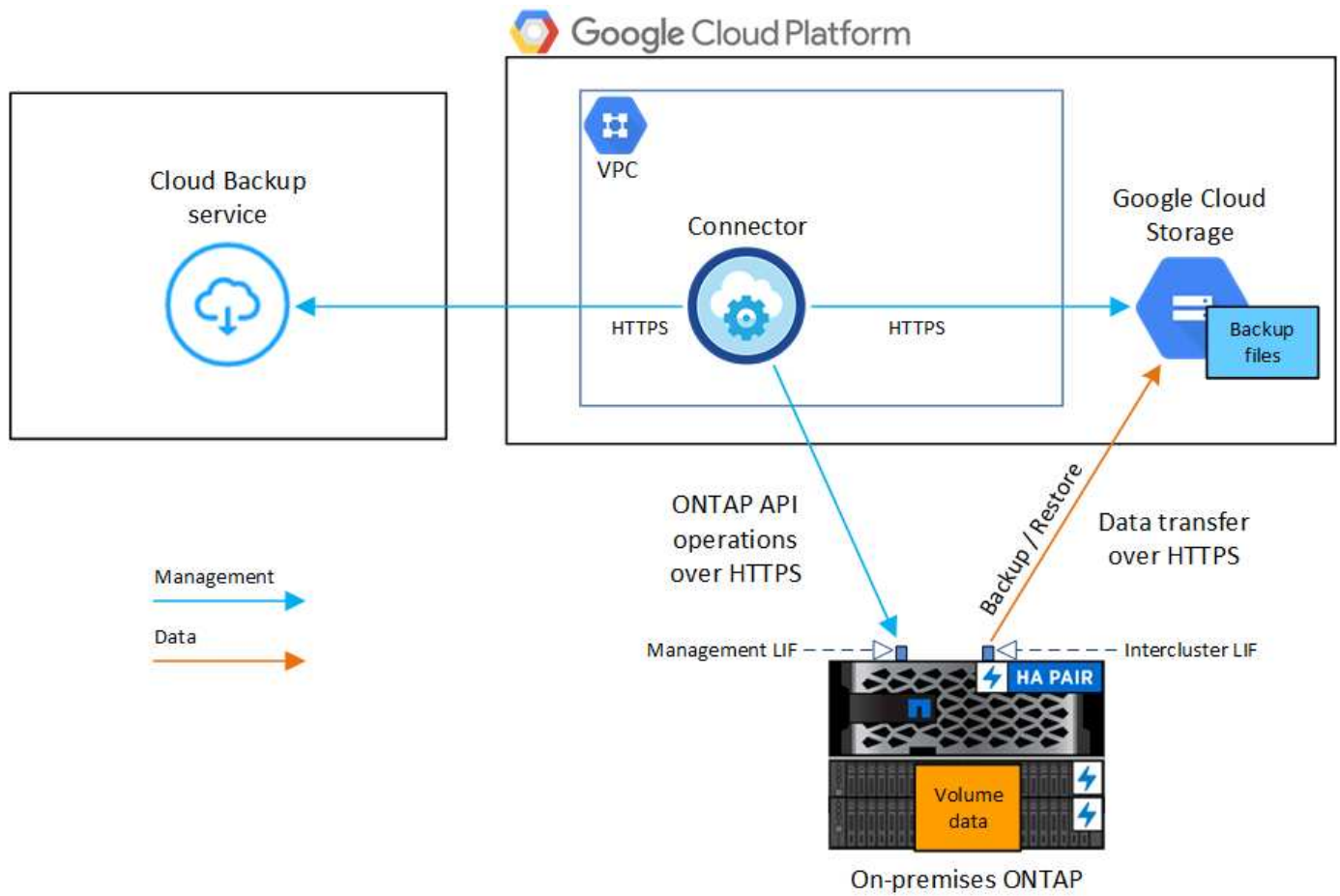
온프레미스 볼륨을 Google Cloud 스토리지에 백업하기 전에 다음 요구 사항을 읽고 지원되는 구성이 있는지 확인합니다.

사내 ONTAP 시스템에서 Google 클라우드 스토리지로 백업을 구성할 때 두 가지 연결 방법을 사용할 수 있습니다.

- 공용 연결 - 공용 Google 엔드포인트를 사용하여 ONTAP 시스템을 Google 클라우드 스토리지에 직접 연결합니다.
- 비공개 연결 - VPN 또는 개인 서비스 연결을 사용하여 개인 IP 주소를 사용하는 개인 Google 액세스 인터페이스를

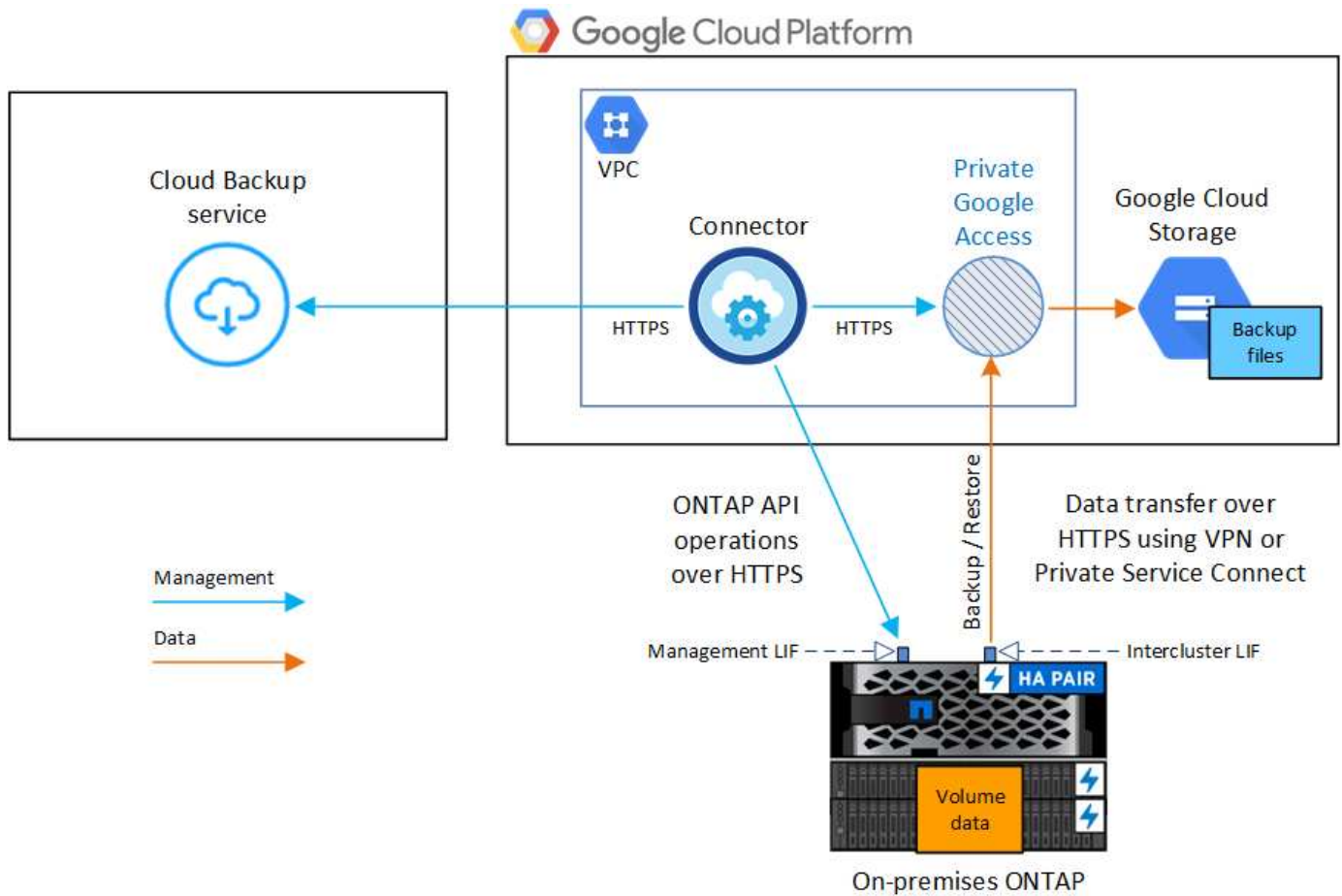
통해 트래픽을 라우팅합니다.

다음 그림에서는 공용 연결 방법과 구성 요소 간에 준비해야 하는 연결을 보여 줍니다.



다음 그림에서는 전용 연결 방법과 구성 요소 간에 준비해야 하는 연결을 보여 줍니다.





## ONTAP 클러스터 준비

볼륨 데이터 백업을 시작하려면 Cloud Manager에서 사내 ONTAP 클러스터를 검색해야 합니다.

["클러스터를 검색하는 방법에 대해 알아보십시오"](#).

## ONTAP 요구 사항

- ONTAP 9.7P5 이상
- SnapMirror 라이선스(프리미엄 번들 또는 데이터 보호 번들의 일부로 포함)
- 참고: \* Cloud Backup을 사용할 때는 "하이브리드 클라우드 번들"이 필요하지 않습니다.

자세한 내용은 를 참조하십시오 ["클러스터 라이선스를 관리합니다"](#).

- 시간 및 시간대가 올바르게 설정되었습니다.

자세한 내용은 를 참조하십시오 ["클러스터 시간을 구성합니다"](#).

## 클러스터 네트워킹 요구 사항

- ONTAP 클러스터는 백업 및 복원 작업을 위해 인터클러스터 LIF에서 Google Cloud 스토리지에 대한 포트 443을 통한 HTTPS 연결을 시작합니다.

ONTAP는 오브젝트 스토리지 간에 데이터를 읽고 씁니다. 오브젝트 스토리지는 한 번도 시작되고, 응답 하기만 합니다.

- ONTAP를 사용하려면 Connector에서 클러스터 관리 LIF로 인바운드 연결이 필요합니다. Connector는 Google Cloud Platform VPC에 상주할 수 있습니다.
- 인터클러스터 LIF는 백업할 볼륨을 호스팅하는 각 ONTAP 노드에 필요합니다. LIF는 ONTAP가 오브젝트 스토리지에 연결하는 데 사용해야 하는 `_IPspace_`와 연결되어 있어야 합니다. "[IPspace에 대해 자세히 알아보십시오](#)".

클라우드 백업을 설정하면 사용할 IPspace를 묻는 메시지가 표시됩니다. 각 LIF가 연결되는 IPspace를 선택해야 합니다. 이는 여러분이 생성한 "기본" IPspace 또는 사용자 지정 IPspace가 될 수 있습니다.

- 노드의 인터클러스터 LIF는 오브젝트 저장소에 액세스할 수 있습니다.
- 볼륨이 있는 스토리지 VM에 대해 DNS 서버가 구성되었습니다. 자세한 내용은 [참조하십시오 "SVM을 위한 DNS 서비스 구성"](#).
- 을 사용하는 경우 기본값 이외의 IPspace를 사용하는 경우 오브젝트 스토리지에 액세스하려면 정적 라우트를 생성해야 할 수 있습니다.
- 필요한 경우 포트 443을 통해 ONTAP에서 오브젝트 스토리지로 Cloud Backup Service 연결을 허용하고 포트 53(TCP/UDP)을 통해 스토리지 VM에서 DNS 서버로 이름 확인 트래픽을 허용하도록 방화벽 규칙을 업데이트합니다.

## 커넥터 작성 또는 전환

데이터를 클라우드에 백업하려면 Connector가 필요하며, Google Cloud 스토리지에 데이터를 백업할 때는 Connector가 Google Cloud Platform VPC에 있어야 합니다. 온-프레미스에 배포된 Connector는 사용할 수 없습니다. 새 커넥터를 만들거나 현재 선택한 커넥터가 올바른 공급자에 있는지 확인해야 합니다.

- "[커넥터에 대해 자세히 알아보십시오](#)"
- "[GCP에서 커넥터를 생성하는 중입니다](#)"
- "[커넥터 간 전환](#)"

## 커넥터를 위한 네트워킹 준비

커넥터에 필요한 네트워크 연결이 있는지 확인합니다.

### 단계

1. 커넥터가 설치된 네트워크에서 다음 연결을 사용할 수 있는지 확인합니다.
  - 포트 443(HTTPS)을 통해 Cloud Backup Service에 아웃바운드 인터넷 연결
  - Google Cloud 스토리지에 포트 443을 통한 HTTPS 연결
  - 포트 443을 통해 ONTAP 클러스터 관리 LIF에 HTTPS로 연결합니다
2. 커넥터를 배포할 서브넷에서 개인 Google 액세스를 활성화합니다. "[개인 Google 액세스](#)" ONTAP 클러스터에서 VPC로 직접 연결하고 커넥터 및 Google 클라우드 스토리지 간의 통신을 가상 프라이빗 네트워크에 유지하고자 하는 경우 이 필요합니다.

Private Google Access는 내부(전용) IP 주소(외부 IP 주소 없음)만 있는 VM 인스턴스와 작동합니다.

## Connector에 권한을 확인하거나 추가합니다

Cloud Backup Search & Restore 기능을 사용하려면 Connector 역할에 특정 권한이 있어야 Google Cloud



BigQuery 서비스에 액세스할 수 있습니다. 아래 사용 권한을 확인하고 정책을 수정해야 하는 경우 단계를 따릅니다.

#### 단계

1. 인치 **"클라우드 콘솔"**에서 **\* 역할 \*** 페이지로 이동합니다.
2. 페이지 맨 위에 있는 드롭다운 목록을 사용하여 편집할 역할이 포함된 프로젝트나 조직을 선택합니다.
3. 사용자 지정 역할을 클릭합니다.
4. 역할 편집 **\*** 을 클릭하여 역할의 권한을 업데이트합니다.
5. 역할에 다음과 같은 새 권한을 추가하려면 **\* 권한 추가 \*** 를 클릭합니다.

```
bigquery.jobs.get  
bigquery.jobs.list  
bigquery.jobs.listAll  
bigquery.datasets.create  
bigquery.datasets.get  
bigquery.jobs.create  
bigquery.tables.get  
bigquery.tables.getData  
bigquery.tables.list  
bigquery.tables.create
```

6. Update **\*** 를 클릭하여 편집된 역할을 저장합니다.

#### 라이선스 요구 사항을 확인합니다

- 클러스터에 Cloud Backup을 활성화하려면 먼저 Google에서 PAYGO(Pay-as-you-Go) Cloud Manager Marketplace 오퍼링을 구독하거나 NetApp에서 Cloud Backup BYOL 라이선스를 구입하여 활성화해야 합니다. 이러한 라이선스는 사용자 계정용이며 여러 시스템에서 사용할 수 있습니다.
  - Cloud Backup PAYGO 라이선스의 경우 에 대한 구독이 필요합니다 **"구글"** Cloud Backup을 사용하는 Cloud Manager Marketplace 오퍼링 Cloud Backup에 대한 청구는 이 구독을 통해 이루어집니다.
  - Cloud Backup BYOL 라이선스의 경우, 라이선스 기간 및 용량 동안 서비스를 사용할 수 있도록 지원하는 NetApp의 일련 번호가 필요합니다. **"BYOL 라이선스 관리 방법에 대해 알아보십시오"**.
- 백업을 찾을 오브젝트 스토리지 공간에 Google에 가입해야 합니다.

모든 지역의 사내 시스템에서 Google Cloud 스토리지로 백업을 생성할 수 있습니다 **"Cloud Volumes ONTAP가 지원되는 경우"**. 서비스를 설정할 때 백업을 저장할 지역을 지정합니다.

#### 백업을 위해 **Google Cloud Storage** 준비 중

백업을 설정할 때는 스토리지 관리자 권한이 있는 서비스 계정에 대한 스토리지 액세스 키를 제공해야 합니다. 서비스 계정을 사용하면 Cloud Backup에서 백업을 저장하는 데 사용되는 Cloud Storage 버킷을 인증하고 액세스할 수 있습니다. Google Cloud Storage가 누가 요청을 하는지 알 수 있도록 키가 필요합니다.

#### 단계

1. **"사전 정의된 스토리지 관리자 역할이 있는 서비스 계정을 생성합니다"**.

2. 로 이동합니다 "GCP 스토리지 설정" 서비스 계정에 대한 액세스 키를 생성합니다.

- 프로젝트를 선택하고 \* 상호 운용성 \* 을 클릭합니다. 아직 수행하지 않았다면 \* 상호 운용성 액세스 사용 \* 을 클릭하십시오.
- 서비스 계정의 액세스 키 \* 에서 \* 서비스 계정의 키 생성 \* 을 클릭하고 방금 생성한 서비스 계정을 선택한 다음 \* 키 생성 \* 을 클릭합니다.

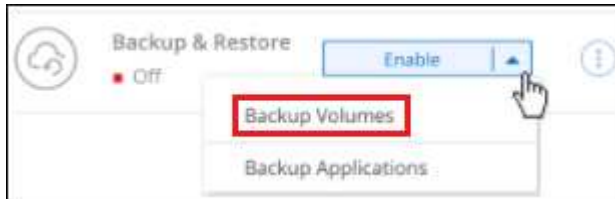
나중에 백업 서비스를 구성할 때 Cloud Backup에 키를 입력해야 합니다.

## 클라우드 백업 활성화

사내 작업 환경에서 언제든지 직접 Cloud Backup을 사용할 수 있습니다.

단계

- Canvas에서 작업 환경을 선택하고 오른쪽 패널의 백업 및 복원 서비스 옆에 있는 \* 활성화 > 볼륨 백업 \* 을 클릭합니다.



- 공급자로 Google Cloud를 선택하고 \* 다음 \* 을 클릭합니다.

- 제공업체 세부사항을 입력하고 \* 다음 \* 을 클릭합니다.

- 백업을 위해 Google Cloud Storage 버킷을 생성할 Google Cloud Project. (프로젝트에 미리 정의된 스토리지 관리 역할이 있는 서비스 계정이 있어야 합니다.)
- 백업을 저장하는 데 사용되는 Google Access Key 및 Secret Key입니다.
- 백업을 저장할 Google 지역
- 백업할 볼륨이 상주하는 ONTAP 클러스터의 IPspace 이 IPspace용 인터클러스터 LIF는 아웃바운드 인터넷 액세스를 가져야 합니다.

- 계정에 대한 기존 Cloud Backup 라이선스가 없는 경우 이 시점에서 사용할 충전 방법 유형을 선택하라는 메시지가

표시됩니다. Google에서 PAYGO(pay-as-you-go) Cloud Manager Marketplace 오퍼링을 구독하거나(또는 여러 구독을 선택한 경우) NetApp에서 Cloud Backup BYOL 라이선스를 구입하여 활성화할 수 있습니다. "[Cloud Backup 라이선스를 설정하는 방법에 대해 알아보십시오.](#)"

- Define Policy\_페이지에서 기존 백업 스케줄과 보존 값을 선택하거나 새 기본 백업 정책을 정의하고 \* Next \* 를 클릭합니다.

**Define Policy**

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule** ☒ Create a New Policy ☐ Select an Existing Policy

☐ Hourly Number of backups to retain 24

☒ Daily Number of backups to retain 30

☐ Weekly Number of backups to retain 52

☐ Monthly Number of backups to retain 12

**DP Volumes** Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

**Google Cloud Storage Bucket** Cloud Manager will create the Google Cloud Storage Bucket after you complete the wizard

을 참조하십시오 "[기존 정책 목록입니다.](#)"

- Select Volumes(볼륨 선택) 페이지의 기본 백업 정책을 사용하여 백업할 볼륨을 선택합니다. 특정 볼륨에 서로 다른 백업 정책을 할당하려는 경우 추가 정책을 생성하여 나중에 해당 볼륨에 적용할 수 있습니다.
  - 모든 볼륨을 백업하려면 제목 행(☒ Volume Name)를 클릭합니다.
  - 개별 볼륨을 백업하려면 각 볼륨에 대한 확인란을 선택합니다(☒ Volume\_1)를 클릭합니다.

**Select Volumes**

57 Volumes

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 On	DP	SVM_Name_2	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active

☒ Automatically back up future volumes on all storage VMs with the selected backup policy

나중에 추가된 모든 볼륨에 백업을 사용하려면 "Automatically back up future volumes..." 확인란을 선택하기만 하면 됩니다. 이 설정을 비활성화하면 이후 볼륨에 대해 백업을 수동으로 활성화해야 합니다.

7. 백업 활성화 \* 를 클릭하면 Cloud Backup이 볼륨의 초기 백업을 시작합니다.

Cloud Backup은 선택한 각 볼륨의 초기 백업을 시작하고, 백업 상태를 모니터링할 수 있도록 Volume Backup Dashboard가 표시됩니다.

가능합니다 "볼륨에 대한 백업을 시작 및 중지하거나 백업 일정을 변경합니다". 또한 가능합니다 "백업 파일에서 볼륨 또는 파일을 복원합니다" Google의 Cloud Volumes ONTAP 시스템 또는 온프레미스 ONTAP 시스템으로.

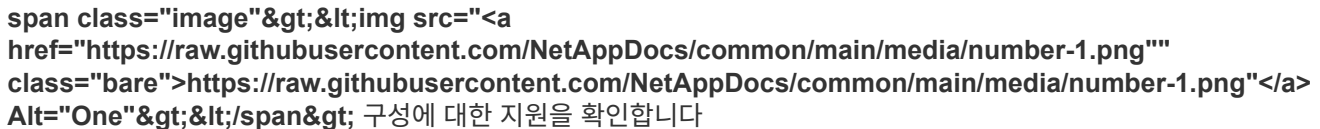
## 사내 ONTAP 데이터를 StorageGRID에 백업

몇 가지 단계를 완료하여 사내 ONTAP 시스템의 데이터를 NetApp StorageGRID 시스템의 오브젝트 스토리지로 백업을 시작하십시오.

"사내 ONTAP 시스템"에는 FAS, AFF 및 ONTAP Select 시스템이 포함됩니다.

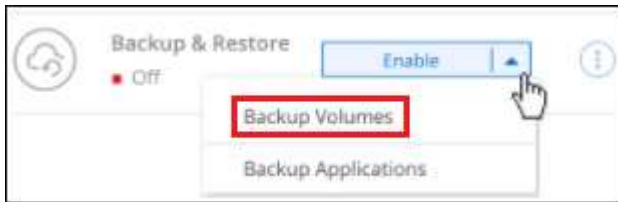
### 빠른 시작

다음 단계를 따라 빠르게 시작하거나 나머지 섹션을 아래로 스크롤하여 자세한 내용을 확인하십시오.

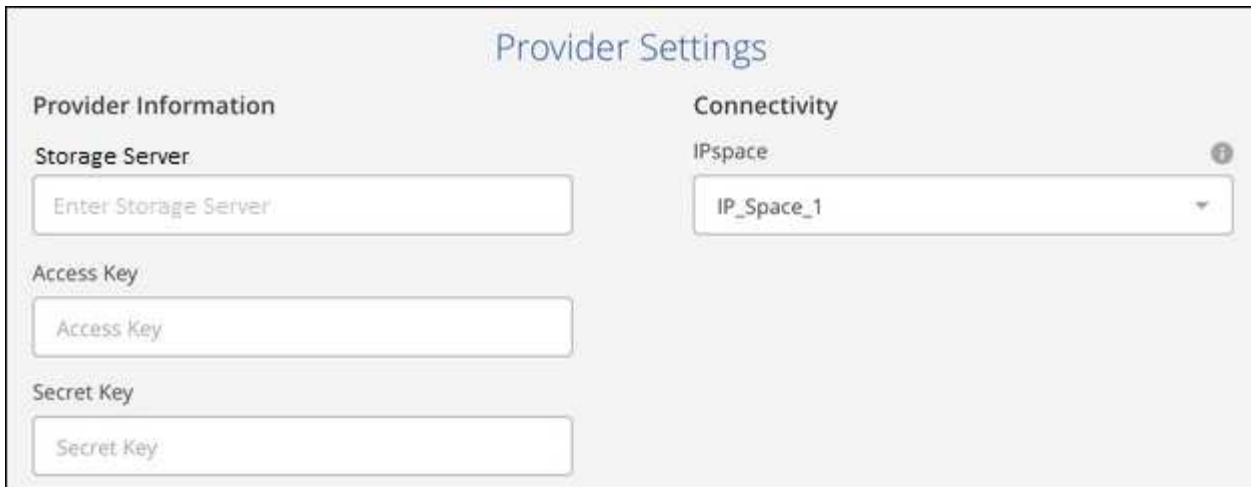
 구성에 대한 지원을 확인합니다

- 온프레미스 클러스터를 검색한 후 Cloud Manager의 작업 환경에 추가했습니다. 을 참조하십시오 "ONTAP 클러스터 검색" 를 참조하십시오.
  - 클러스터에서 ONTAP 9.7P5 이상이 실행 중입니다.
  - 클러스터에는 SnapMirror 라이선스가 있으며, 이 라이선스는 프리미엄 번들 또는 데이터 보호 번들의 일부로 포함됩니다.
  - 클러스터에는 StorageGRID 및 커넥터에 대한 필수 네트워크 연결이 있어야 합니다.
- Connector가 구내에 설치되어 있습니다.
  - 커넥터 네트워킹은 ONTAP 클러스터 및 StorageGRID에 대한 아웃바운드 HTTPS 연결을 활성화합니다.
- 을(를) 구입했습니다 "활성화합니다" Cloud Backup BYOL 라이선스는 NetApp에서 제공
- StorageGRID의 버전 10.3 이상에는 S3 권한이 있는 액세스 키가 있습니다.

작업 환경을 선택하고 오른쪽 패널에서 백업 및 복원 서비스 옆에 있는 \* 활성화 > 볼륨 백업 \* 을 클릭한 다음 설정 마법사를 따릅니다.

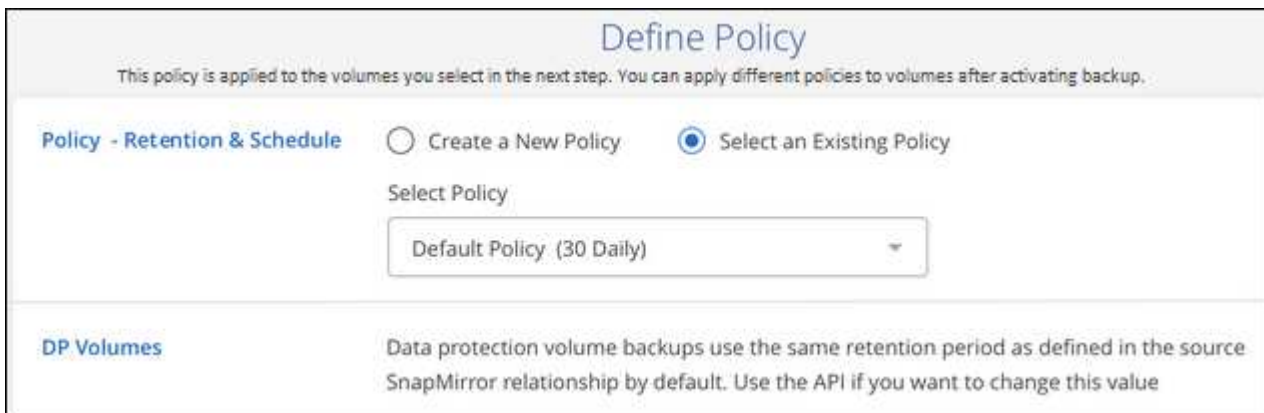


공급자로 StorageGRID를 선택하고 StorageGRID 서버 및 서비스 계정 세부 정보를 입력합니다. 또한 볼륨이 상주하는 ONTAP 클러스터에서 IPspace를 지정해야 합니다.



The 'Provider Settings' form is divided into two main sections: 'Provider Information' and 'Connectivity'. Under 'Provider Information', there are three input fields: 'Storage Server' with a placeholder 'Enter Storage Server', 'Access Key' with a placeholder 'Access Key', and 'Secret Key' with a placeholder 'Secret Key'. Under 'Connectivity', there is a dropdown menu labeled 'IPspace' with a value of 'IP\_Space\_1' and a small information icon to its right.

기본 정책은 매일 볼륨을 백업하고 각 볼륨의 최근 30개 백업 복사본을 유지합니다. 시간별, 일별, 주별 또는 월별 백업으로 변경하거나 더 많은 옵션을 제공하는 시스템 정의 정책 중 하나를 선택합니다. 보존할 백업 복사본의 수를 변경할 수도 있습니다.



The 'Define Policy' form has a header with the title 'Define Policy' and a sub-header: 'This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.' Below this, there are two radio buttons: 'Create a New Policy' (unselected) and 'Select an Existing Policy' (selected). Under 'Select an Existing Policy', there is a dropdown menu labeled 'Select Policy' with the value 'Default Policy (30 Daily)'. At the bottom, there is a section titled 'DP Volumes' with the text: 'Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value'.

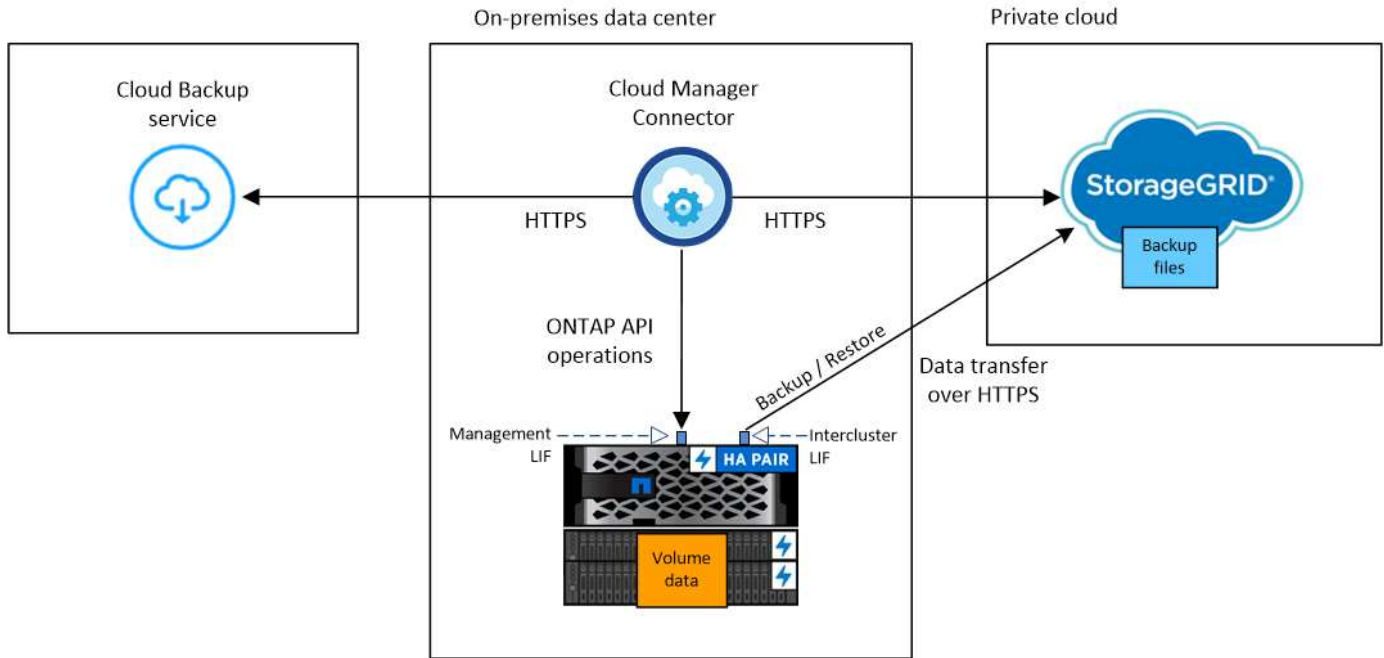
Select Volumes(볼륨 선택) 페이지의 기본 백업 정책을 사용하여 백업할 볼륨을 식별합니다. 특정 볼륨에 서로 다른 백업 정책을 할당하려면 추가 정책을 생성한 후 나중에 볼륨에 적용할 수 있습니다.

S3 버킷은 입력한 S3 액세스 키와 비밀 키로 표시된 서비스 계정에 자동으로 생성되며 백업 파일은 여기에 저장됩니다.

## 요구 사항

사내 볼륨을 StorageGRID에 백업하기 전에 다음 요구 사항을 읽고 지원되는 구성이 있는지 확인합니다.

다음 이미지는 온프레미스 ONTAP 시스템을 StorageGRID에 백업할 때의 각 구성 요소와 이러한 시스템 간에 준비해야 하는 연결을 보여 줍니다.



현재 StorageGRID를 사용할 때 단일 파일 복원이 지원되지 않으므로 클라우드 복원 인스턴스는 이 다이어그램에 표시되지 않습니다.

## ONTAP 클러스터 준비

볼륨 데이터 백업을 시작하려면 Cloud Manager에서 사내 ONTAP 클러스터를 검색해야 합니다.

["클러스터를 검색하는 방법에 대해 알아보십시오"](#).

## ONTAP 요구 사항

- ONTAP 9.7P5 이상
- SnapMirror 라이선스(프리미엄 번들 또는 데이터 보호 번들의 일부로 포함)
- 참고: \* Cloud Backup을 사용할 때는 "하이브리드 클라우드 번들"이 필요하지 않습니다.

자세한 내용은 를 참조하십시오 ["클러스터 라이선스를 관리합니다"](#).

- 시간 및 시간대가 올바르게 설정되었습니다.

자세한 내용은 를 참조하십시오 ["클러스터 시간을 구성합니다"](#).

## 클러스터 네트워킹 요구 사항

- ONTAP 클러스터는 백업 및 복원 작업을 위해 인터클러스터 LIF에서 StorageGRID로 사용자 지정 포트를 통한 HTTPS 연결을 시작합니다. 백업 설정 중에 포트를 구성할 수 있습니다.

ONTAP는 오브젝트 스토리지 간에 데이터를 읽고 씁니다. 오브젝트 스토리지는 한 번도 시작되고, 응답 하기만 합니다.

- ONTAP를 사용하려면 Connector에서 클러스터 관리 LIF로 인바운드 연결이 필요합니다. 커넥터는 해당 위치에 있어야 합니다.
- 인터클러스터 LIF는 백업할 볼륨을 호스팅하는 각 ONTAP 노드에 필요합니다. LIF는 ONTAP가 오브젝트

스토리지에 연결하는 데 사용해야 하는 `_IPspace_`와 연결되어 있어야 합니다. "[IPspace에 대해 자세히 알아보십시오](#)".

클라우드 백업을 설정하면 사용할 IPspace를 묻는 메시지가 표시됩니다. 각 LIF가 연결되는 IPspace를 선택해야 합니다. 이는 여러분이 생성한 "기본" IPspace 또는 사용자 지정 IPspace가 될 수 있습니다.

- 노드의 인터클러스터 LIF는 오브젝트 저장소에 액세스할 수 있습니다.
- 볼륨이 있는 스토리지 VM에 대해 DNS 서버가 구성되었습니다. 자세한 내용은 [참조하십시오 "SVM을 위한 DNS 서비스 구성"](#).
- 을 사용하는 경우 기본값 이외의 IPspace를 사용하는 경우 오브젝트 스토리지에 액세스하려면 정적 라우트를 생성해야 할 수 있습니다.
- 필요한 경우 Cloud Backup Service에서 지정한 포트(일반적으로 포트 443)를 통해 개체 스토리지로 ONTAP 연결을 허용하고 포트 53(TCP/UDP)을 통해 스토리지 VM에서 DNS 서버로 이름 확인 트래픽을 허용하도록 방화벽 규칙을 업데이트합니다.

## StorageGRID 준비 중

StorageGRID는 다음 요구 사항을 충족해야 합니다. [참조하십시오 "StorageGRID 설명서"](#)를 참조하십시오.

지원되는 **StorageGRID** 버전

StorageGRID 10.3 이상이 지원됩니다.

## S3 자격 증명

StorageGRID에 백업을 설정하면 백업 마법사에서 서비스 계정에 대한 S3 액세스 키와 암호 키를 입력하라는 메시지가 표시됩니다. 서비스 계정을 사용하면 클라우드 백업에서 백업을 저장하는 데 사용되는 StorageGRID 버킷을 인증하고 액세스할 수 있습니다. 키는 StorageGRID가 누가 요청하는지 알 수 있도록 필요합니다.

이러한 액세스 키는 다음 권한을 가진 사용자와 연결되어야 합니다.

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

## 오브젝트 버전 관리

오브젝트 저장소 버킷에서 StorageGRID 오브젝트 버전 관리를 사용하도록 설정하면 안 됩니다.

## 커넥터 작성 또는 전환

데이터를 StorageGRID에 백업할 때 Connector를 사내에서 사용할 수 있어야 합니다. 새 커넥터를 설치하거나 현재 선택한 커넥터가 내부에 있는지 확인해야 합니다.

- "[커넥터에 대해 자세히 알아보십시오](#)"
- "[인터넷에 액세스할 수 있는 Linux 호스트에 커넥터 설치](#)"
- "[커넥터 간 전환](#)"



커넥터를 위한 네트워킹 준비

커넥터에 필요한 네트워크 연결이 있는지 확인합니다.

단계

1. 커넥터가 설치된 네트워크에서 다음 연결을 사용할 수 있는지 확인합니다.
  - 포트 443을 통해 StorageGRID에 HTTPS로 연결합니다
  - 포트 443을 통해 ONTAP 클러스터 관리 LIF에 HTTPS로 연결합니다
  - 포트 443을 통해 클라우드 백업으로 아웃바운드 인터넷 연결

라이선스 요구 사항

클러스터에서 Cloud Backup을 활성화하려면 NetApp에서 Cloud Backup BYOL 라이선스를 구입하여 활성화해야 합니다. 이 라이선스는 계정에 사용되며 여러 시스템에서 사용할 수 있습니다.

라이선스 기간 및 용량 동안 서비스를 사용할 수 있도록 NetApp의 일련 번호가 필요합니다. "[BYOL 라이선스 관리 방법에 대해 알아보십시오](#)".



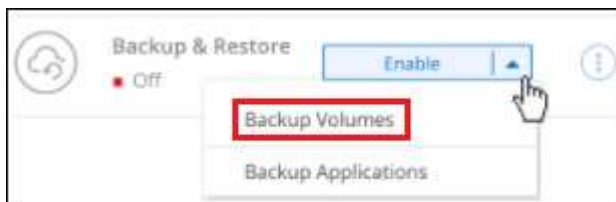
StorageGRID에 파일을 백업할 때는 PAYGO 라이선스가 지원되지 않습니다.

## StorageGRID로 클라우드 백업 지원

사내 작업 환경에서 언제든지 직접 Cloud Backup을 사용할 수 있습니다.

단계

1. Canvas에서 온-프레미스 작업 환경을 선택하고 오른쪽 패널의 백업 및 복원 서비스 옆에 있는 \* 활성화 > 볼륨 백업 \* 을 클릭합니다.



2. 공급자로 \* StorageGRID \* 를 선택하고 \* 다음 \* 을 클릭한 후 공급자 세부 정보를 입력합니다.
  - a. StorageGRID 서버의 FQDN과 ONTAP이 StorageGRID와의 HTTPS 통신에 사용해야 하는 포트(예: S3.eng.company.com:8082')
  - b. 백업을 저장하기 위해 버킷에 액세스하는 데 사용되는 액세스 키 및 비밀 키
  - c. 백업할 볼륨이 상주하는 ONTAP 클러스터의 IPspace 이 IPspace용 인터클러스터 LIF는 아웃바운드 인터넷 액세스를 가져야 합니다.

올바른 IPspace를 선택하면 클라우드 백업이 ONTAP에서 StorageGRID 오브젝트 스토리지로의 연결을 설정할 수 있습니다.



서비스가 시작된 후에는 이 정보를 변경할 수 없습니다.

3. Define Policy\_페이지에서 기본 백업 일정 및 보존 값을 선택하고 \* Next \* 를 클릭합니다.

을 참조하십시오 "기존 정책 목록입니다".

4. Select Volumes(볼륨 선택) 페이지의 기본 백업 정책을 사용하여 백업할 볼륨을 선택합니다. 특정 볼륨에 서로 다른 백업 정책을 할당하려는 경우 추가 정책을 생성하여 나중에 해당 볼륨에 적용할 수 있습니다.

- 모든 볼륨을 백업하려면 제목 행(☒ Volume Name)를 클릭합니다.
- 개별 볼륨을 백업하려면 각 볼륨에 대한 확인란을 선택합니다(☒ Volume\_1)를 클릭합니다.

Select Volumes						
57 Volumes						
<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 On	DP	SVM_Name_2	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/> Automatically back up future volumes on all storage VMs with the selected backup policy ⓘ						

나중에 이 클러스터에 추가된 모든 볼륨에 백업을 사용하도록 설정하려면 "Automatically back up future volumes..." 확인란을 선택한 상태로 둡니다. 이 설정을 비활성화하면 이후 볼륨에 대해 백업을 수동으로 활성화해야 합니다.

5. 백업 활성화 \* 를 클릭하면 선택한 각 볼륨의 초기 백업이 시작됩니다.

S3 버킷은 입력한 S3 액세스 키와 비밀 키로 표시된 서비스 계정에 자동으로 생성되며 백업 파일은 여기에 저장됩니다. 백업 상태를 모니터링할 수 있도록 볼륨 백업 대시보드가 표시됩니다.

가능합니다 "볼륨에 대한 백업을 시작 및 중지하거나 백업 일정을 변경합니다". 또한 가능합니다 "백업 파일에서 전체 볼륨을 복원합니다" 새로운 볼륨으로 ONTAP 데이터를 이동합니다.

## ONTAP 시스템의 백업 관리

백업 일정을 변경하고, 볼륨 백업을 활성화/비활성화하고, 백업을 삭제하는 등 Cloud Volumes ONTAP 및 온-프레미스 ONTAP 시스템의 백업을 관리할 수 있습니다.



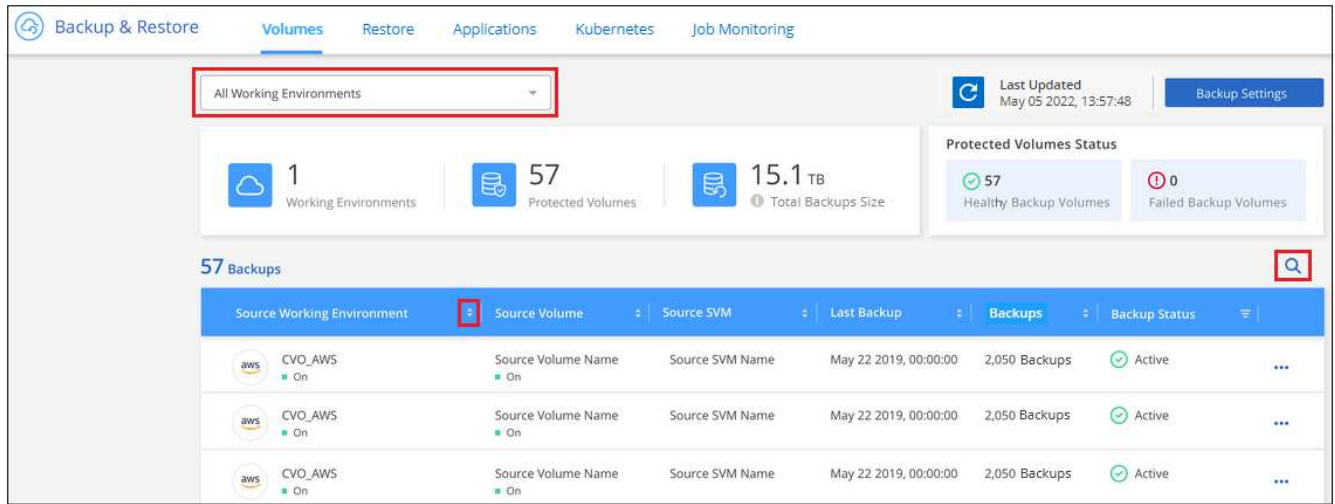
클라우드 공급자 환경에서 직접 백업 파일을 관리하거나 변경하지 마십시오. 이로 인해 파일이 손상되어 지원되지 않는 구성이 발생할 수 있습니다.

### 백업 중인 볼륨 보기

Backup Dashboard에서 현재 백업 중인 모든 볼륨의 목록을 볼 수 있습니다.

단계

1. 백업 및 복원 \* 탭을 클릭합니다.
2. 볼륨 \* 탭을 클릭하여 Cloud Volumes ONTAP 및 온-프레미스 ONTAP 시스템의 볼륨 목록을 표시합니다.



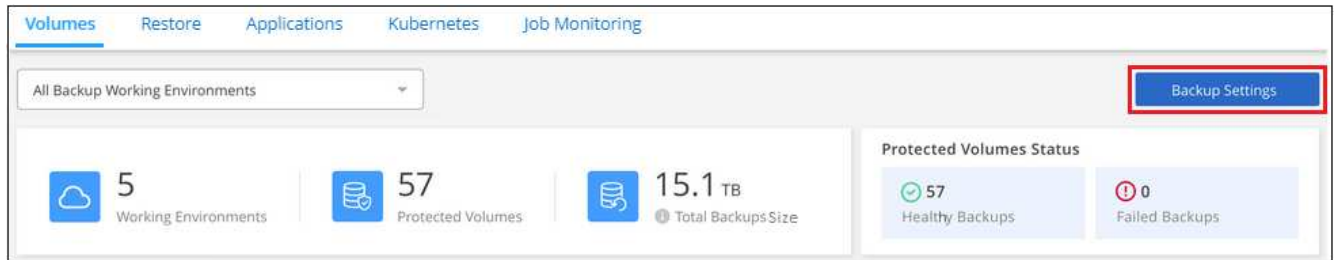
특정 작업 환경에서 특정 볼륨을 찾는 경우 작업 환경 및 볼륨으로 목록을 세분화하거나 검색 필터를 사용할 수 있습니다.

## 볼륨 백업 활성화 및 비활성화

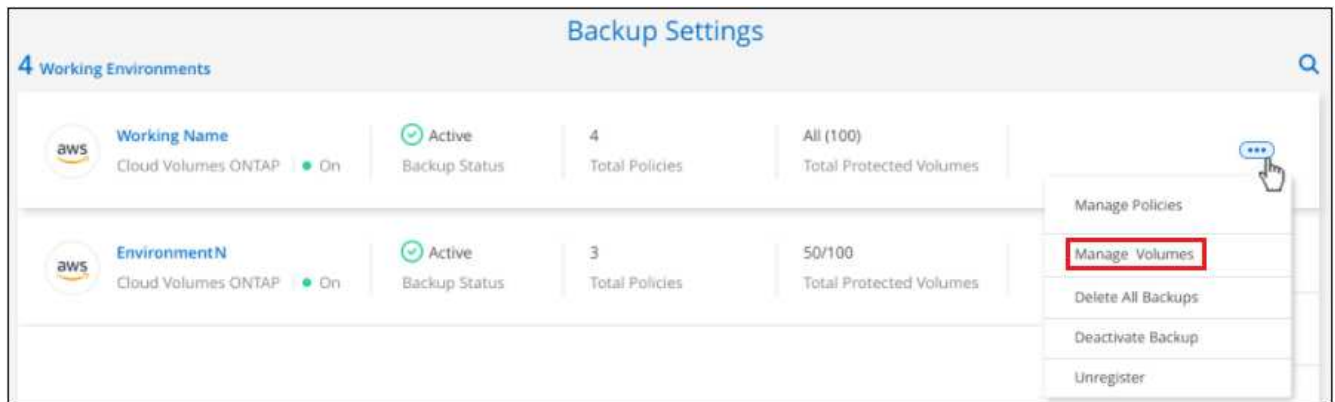
해당 볼륨의 백업 복사본이 필요하지 않고 백업 저장 비용을 지불하지 않으려는 경우 볼륨 백업을 중지할 수 있습니다. 현재 백업 중이 아닌 경우 백업 목록에 새 볼륨을 추가할 수도 있습니다.

단계

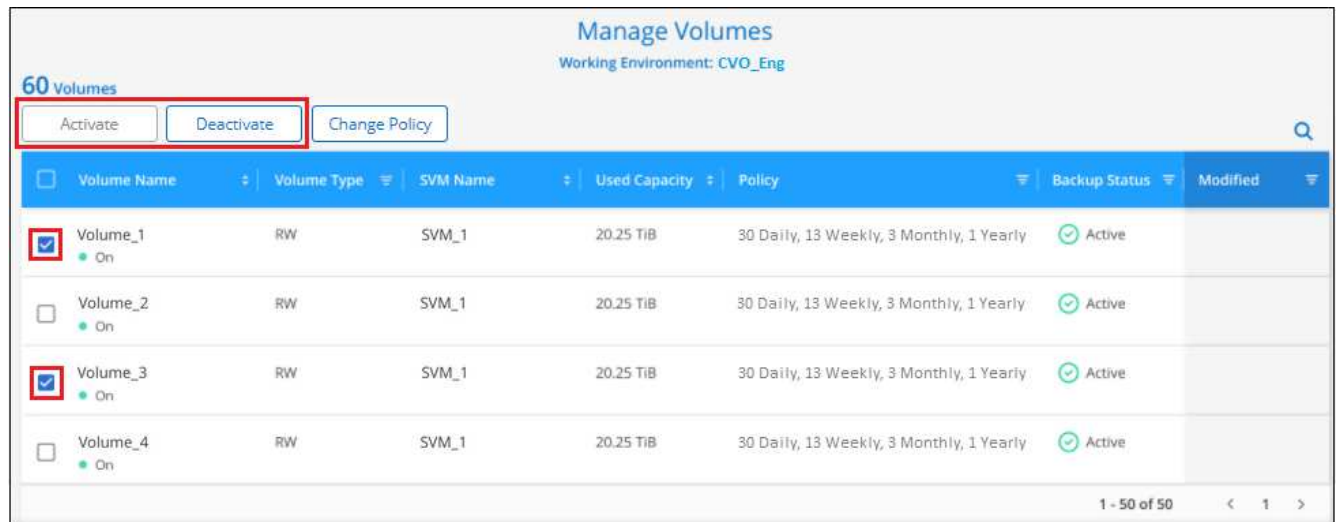
1. 볼륨 \* 탭에서 \* 백업 설정 \* 을 선택합니다.



2. 백업 설정 페이지에서 \_ 을(를) 클릭합니다 ... 작업 환경의 경우 \* 볼륨 관리 \* 를 선택합니다.



3. 변경할 볼륨 또는 볼륨의 확인란을 선택한 다음 볼륨의 백업을 시작 또는 중지할지 여부에 따라 \* 활성화 \* 또는 \* 비활성화 \* 를 클릭합니다.



4. 변경 사항을 적용하려면 \* 저장 \* 을 클릭합니다.

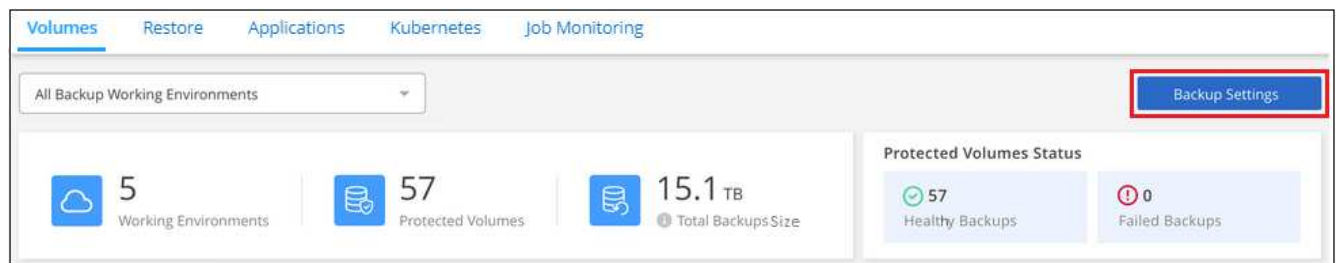
- 참고: \* 볼륨이 백업되지 않도록 하는 경우 클라우드 공급자가 백업이 사용하는 용량에 대한 객체 스토리지 비용을 계속 청구합니다 백업을 삭제합니다.

## 기존 백업 정책 편집

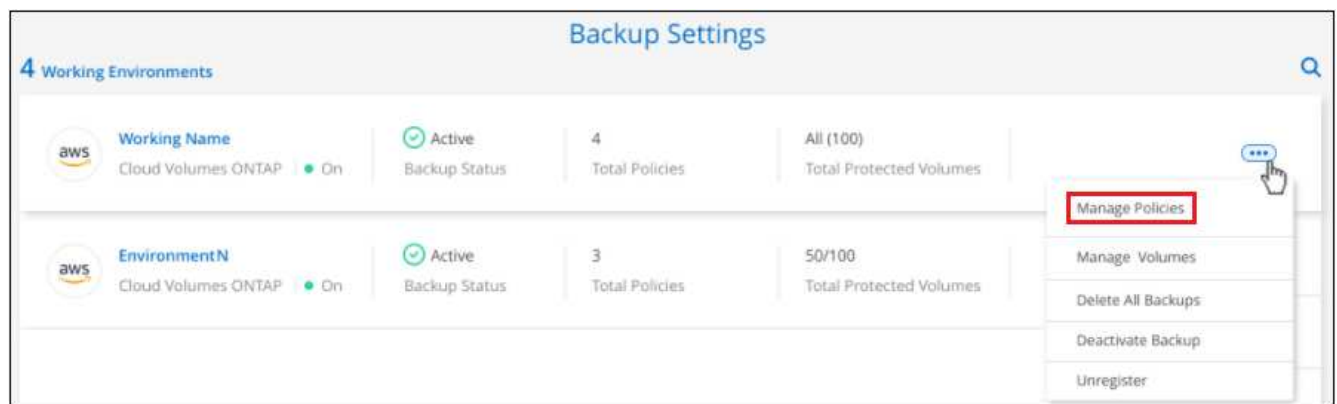
작업 환경의 볼륨에 현재 적용된 백업 정책의 속성을 변경할 수 있습니다. 백업 정책을 변경하면 정책을 사용하는 모든 기존 볼륨에 영향을 줍니다.

단계

1. 볼륨 \* 탭에서 \* 백업 설정 \* 을 선택합니다.



2. 백업 설정 페이지에서 을 클릭합니다 ... 설정을 변경하려는 작업 환경의 경우 \* 정책 관리 \* 를 선택합니다.



3. Manage Policies\_ 페이지에서 해당 작업 환경에서 변경할 백업 정책에 대해 \* Edit Policy \* 를 클릭합니다.

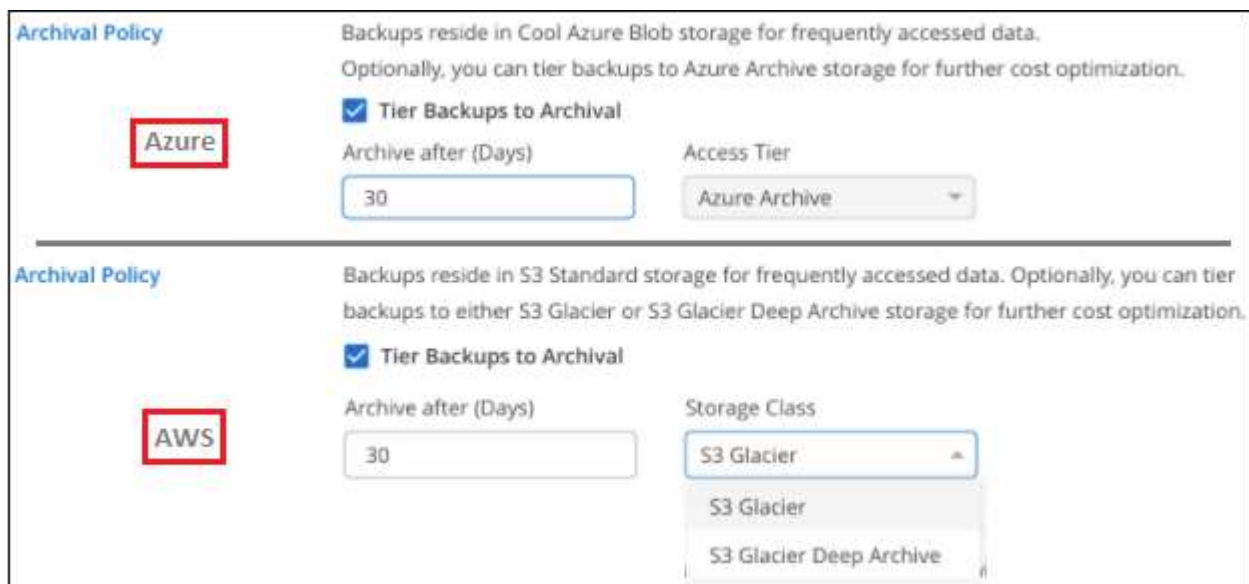


4. Edit Policy\_페이지에서 스케줄 및 백업 보존을 변경하고 \* Save \* 를 클릭합니다.



클러스터에서 ONTAP 9.10.1 이상이 실행 중이고 클라우드 스토리지에 AWS 또는 Azure를 사용하는 경우 일정 일 후에 아카이브 스토리지에 대한 백업 계층화를 활성화 또는 비활성화할 수도 있습니다.

"Azure 아카이브 스토리지 사용에 대해 자세히 알아보십시오". "AWS 아카이브 스토리지 사용에 대해 자세히 알아보십시오".



아카이브 스토리지로 계층화된 모든 백업 파일은 아카이빙에 대한 백업 계층화를 중지하는 경우 해당 계층에 남아 있습니다. 이러한 백업 파일은 표준 계층으로 자동으로 다시 이동되지 않습니다.

## 새 백업 정책 추가

작업 환경에 Cloud Backup을 활성화하면 처음에 선택한 모든 볼륨이 사용자가 정의한 기본 백업 정책을 사용하여 백업됩니다. RPO(복구 지점 목표)가 다른 특정 볼륨에 서로 다른 백업 정책을 할당하려면 해당 클러스터에 대한 추가 정책을 생성한 다음 해당 정책을 다른 볼륨에 할당할 수 있습니다.

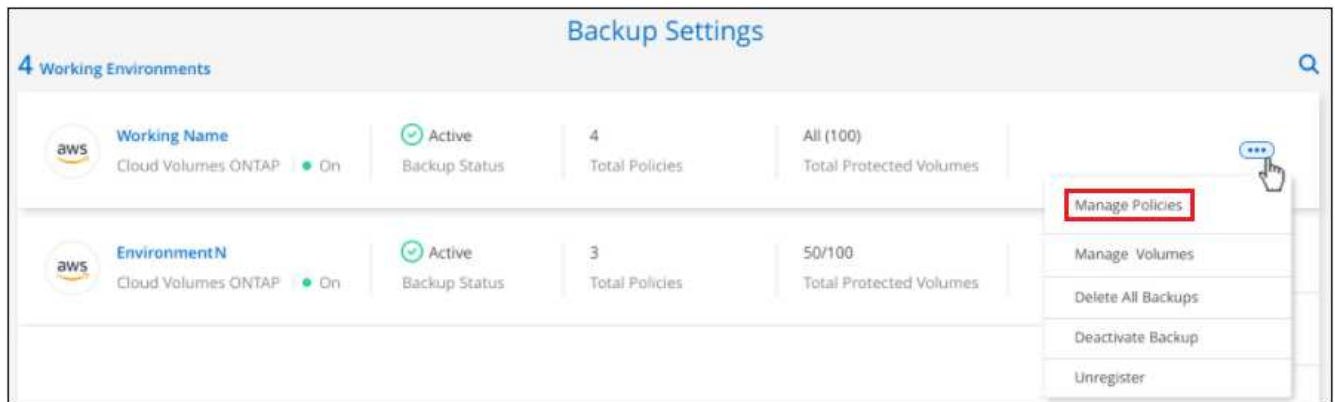
작업 환경의 특정 볼륨에 새 백업 정책을 적용하려면 먼저 작업 환경에 백업 정책을 추가해야 합니다. 그러면 됩니다  
[해당 작업 환경의 볼륨에 정책을 적용합니다.](#)

단계

1. 볼륨 \* 탭에서 \* 백업 설정 \* 을 선택합니다.



2. 백업 설정 페이지에서 을 클릭합니다 ... 새 정책을 추가할 작업 환경의 경우 \* 정책 관리 \* 를 선택합니다.



3. Manage Policies\_ 페이지에서 \* Add New Policy \* 를 클릭합니다.



4. Add New Policy\_페이지에서 스케줄 및 백업 보존을 정의하고 \* Save \* 를 클릭합니다.

### Add New Policy

Working Environment: Working Name

Policy - Retention & Schedule

☐ Hourly
 Number of backups to retain

☒ Daily
 Number of backups to retain

☐ Weekly
 Number of backups to retain

☐ Monthly
 Number of backups to retain

클러스터에서 ONTAP 9.10.1 이상이 실행 중이고 클라우드 스토리지에 AWS 또는 Azure를 사용하는 경우 일정 일 후에 아카이브 스토리지에 대한 백업 계층화를 활성화 또는 비활성화할 수도 있습니다.

"Azure 아카이브 스토리지 사용에 대해 자세히 알아보십시오". "AWS 아카이브 스토리지 사용에 대해 자세히 알아보십시오".

Archival Policy

Backups reside in Cool Azure Blob storage for frequently accessed data. Optionally, you can tier backups to Azure Archive storage for further cost optimization.

Azure

☒ Tier Backups to Archival

Archive after (Days)

Access Tier

---

Archival Policy

Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.

AWS

☒ Tier Backups to Archival

Archive after (Days)

Storage Class 

S3 Glacier
S3 Glacier Deep Archive

기존 볼륨에 할당된 정책을 변경합니다

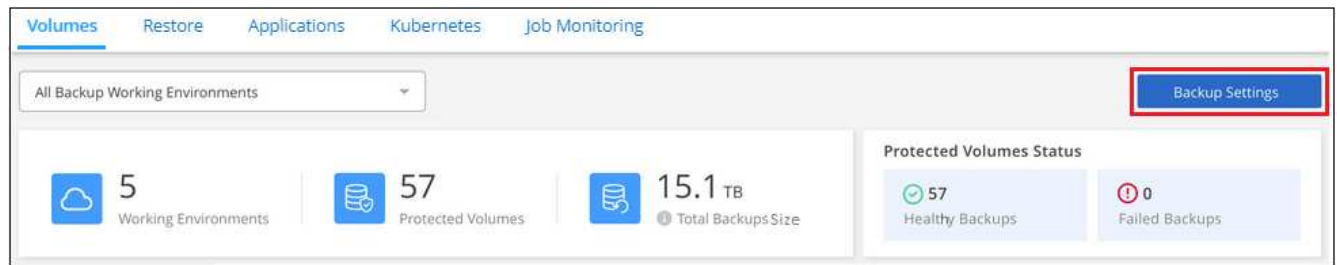
백업 빈도를 변경하거나 보존 값을 변경하려는 경우 기존 볼륨에 할당된 백업 정책을 변경할 수 있습니다.

볼륨에 적용할 정책이 이미 있어야 합니다. [작업 환경에 대한 새 백업 정책을 추가하는 방법에 대해 알아보십시오.](#)

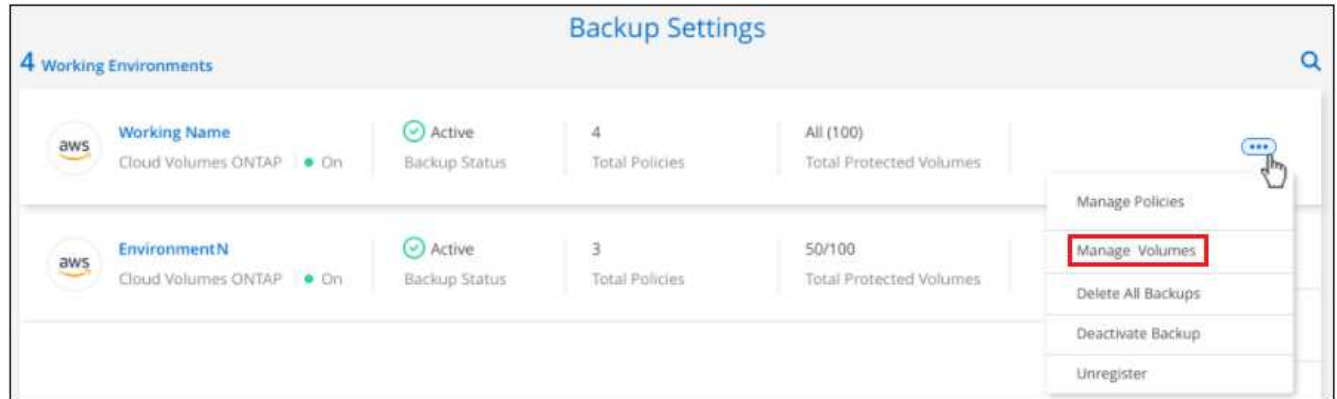
단계

1. 볼륨 \* 탭에서 \* 백업 설정 \* 을 선택합니다.

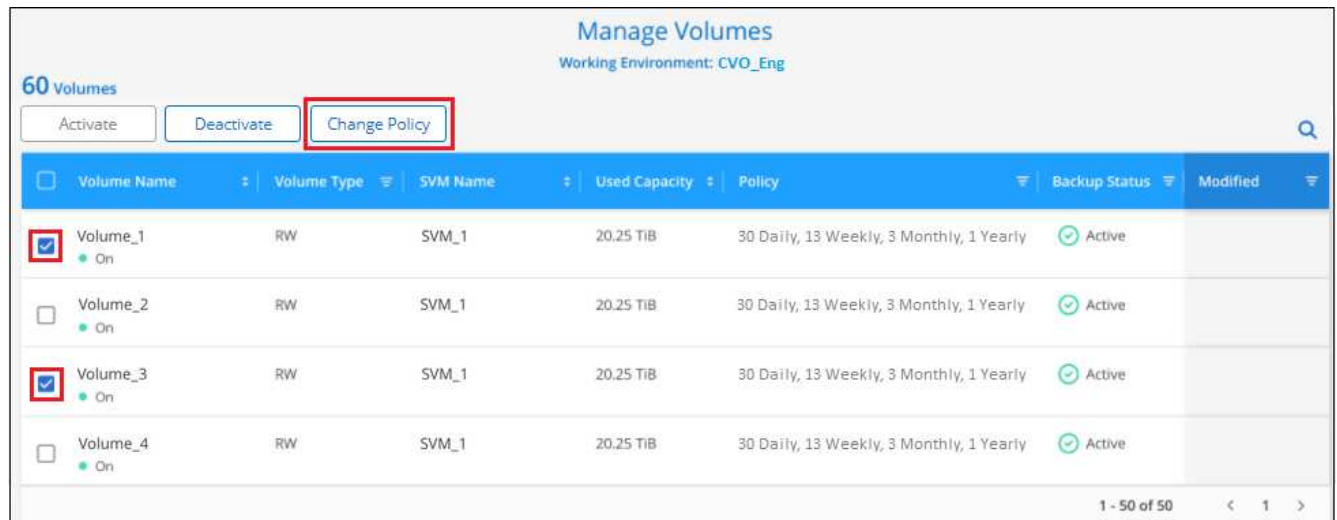




2. 백업 설정 페이지에서 \_을(를) 클릭합니다 ... 볼륨이 있는 작업 환경의 경우 \* 볼륨 관리 \* 를 선택합니다.

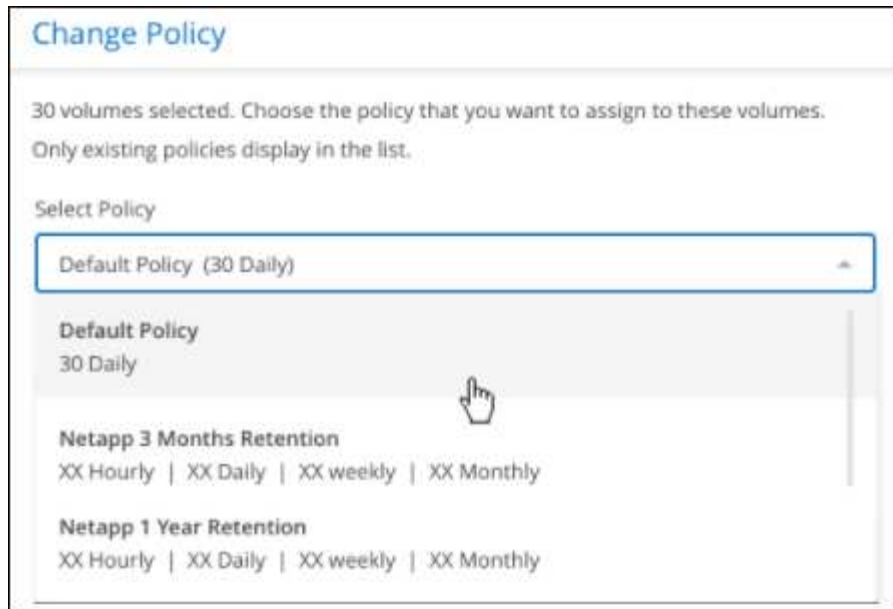


3. 정책을 변경할 볼륨 또는 볼륨의 확인란을 선택한 다음 \* 정책 변경 \* 을 클릭합니다.



4. Change Policy\_페이지에서 볼륨에 적용할 정책을 선택하고 \* Change Policy \* 를 클릭합니다.





5. 변경 사항을 적용하려면 \* 저장 \* 을 클릭합니다.

## 새 볼륨에 할당할 백업 정책 설정

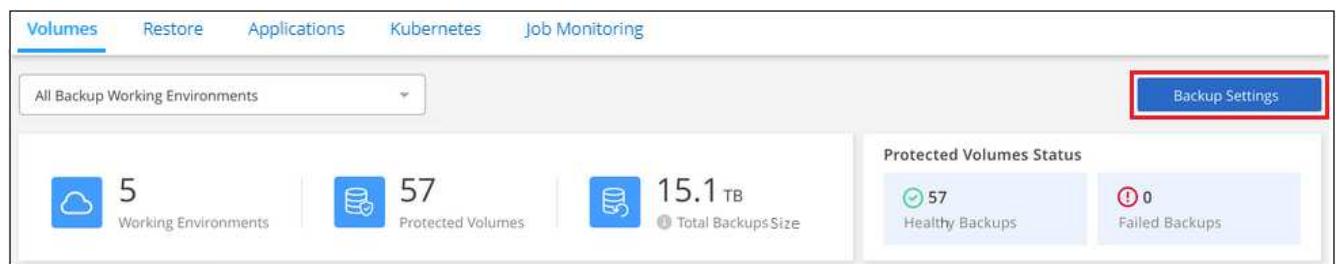
ONTAP 클러스터에서 클라우드 백업을 처음 활성화할 때 새로 생성된 볼륨에 백업 정책을 자동으로 할당하는 옵션을 선택하지 않은 경우 나중에 백업 설정 페이지에서 이 옵션을 선택할 수 있습니다. 새로 생성된 볼륨에 백업 정책을 할당하면 모든 데이터가 보호됩니다.

볼륨에 적용할 정책이 이미 있어야 합니다. [작업 환경에 대한 새 백업 정책을 추가하는 방법에 대해 알아봅니다.](#)

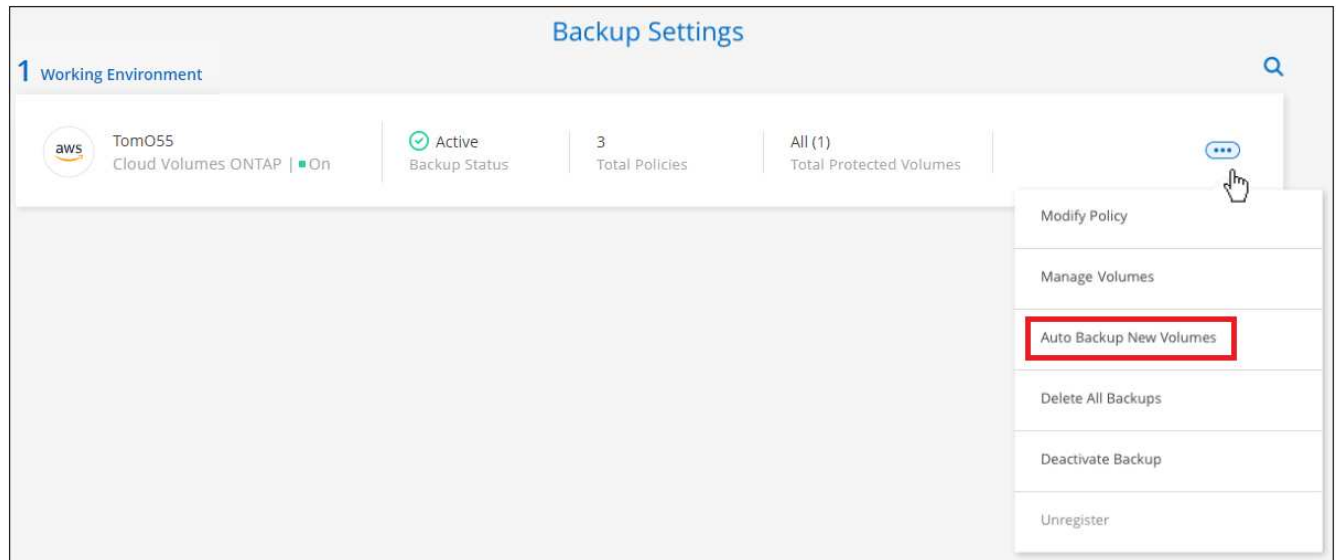
새로 생성된 볼륨이 자동으로 백업되지 않도록 이 설정을 비활성화할 수도 있습니다. 이 경우 나중에 백업하려는 특정 볼륨에 대해 백업을 수동으로 설정해야 합니다.

단계

1. 볼륨 \* 탭에서 \* 백업 설정 \* 을 선택합니다.



2. 백업 설정 페이지에서 \_ 을(를) 클릭합니다 ... 볼륨이 있는 작업 환경의 경우 \* Auto Backup New Volumes \* 를 선택합니다.



3. "새 볼륨 자동 백업..." 확인란을 선택하고 새 볼륨에 적용할 백업 정책을 선택한 다음 \* 저장 \* 을 클릭합니다.

### Auto Backup New Volumes

☒ Automatically back up new volumes on all SVMs for Working Environment TomO55

Choose the policy that will be assigned to new volumes. Only existing policies are shown in the list.

Select Backup Policy

CloudBackupService-1611307085985\_V2 (30 Daily)

Save

Cancel

이제 이 백업 정책은 Cloud Manager, System Manager 또는 ONTAP CLI를 사용하여 이 작업 환경에서 생성된 모든 새 볼륨에 적용됩니다.

## 언제든지 수동 볼륨 백업 생성

언제든지 주문형 백업을 생성하여 볼륨의 현재 상태를 캡처할 수 있습니다. 이 기능은 볼륨에 매우 중요한 변경 사항이 있어 해당 데이터를 보호하기 위해 다음 예약 백업을 기다리지 않으려는 경우 또는 볼륨이 현재 백업되고 있지 않아 현재 상태를 캡처하려는 경우에 유용합니다.

백업 이름에는 타임 스탬프가 포함되어 있어 다른 예약된 백업에서 필요 시 백업을 식별할 수 있습니다.

임시 백업을 생성할 때 소스 볼륨에 스냅샷이 생성됩니다. 이 스냅샷은 일반 스냅샷 스케줄의 일부가 아니므로 회전되지 않습니다. 백업이 완료되면 소스 볼륨에서 이 스냅샷을 수동으로 삭제할 수 있습니다. 이렇게 하면 이 스냅샷과 관련된 블록을 해제할 수 있습니다. 스냅샷의 이름은 CBS-SNSHOT-adhoc 으로 시작됩니다. ["ONTAP CLI를 사용하여"](#)

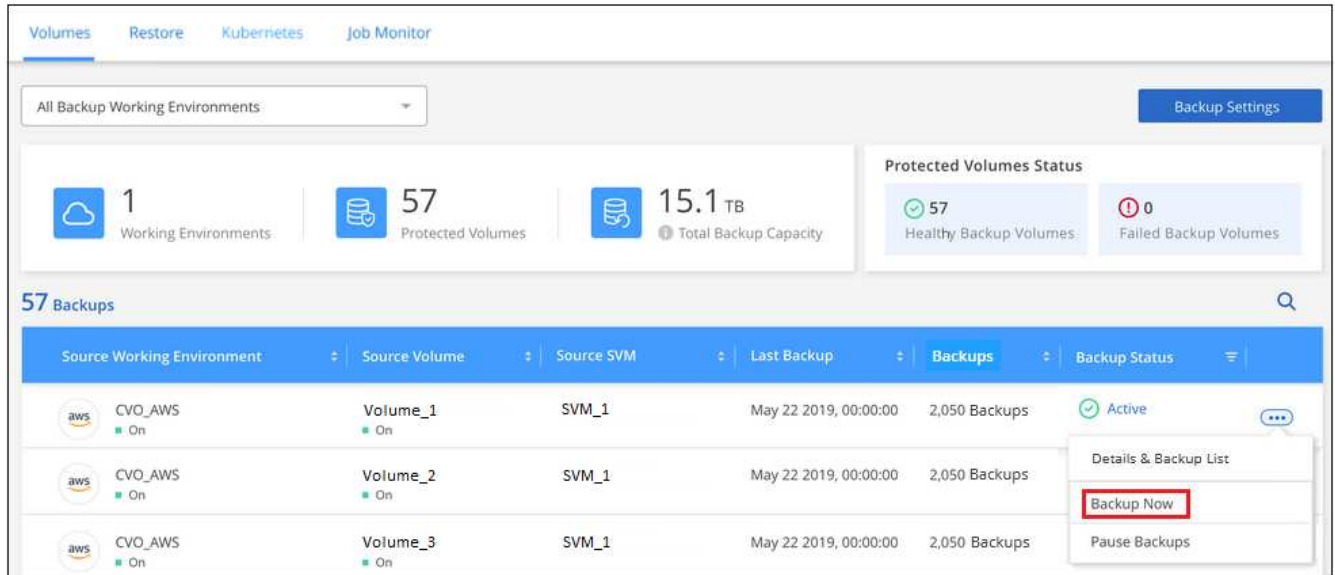
스냅샷을 삭제하는 방법을 알아봅니다".



데이터 보호 볼륨에서 필요 시 볼륨 백업을 지원하지 않습니다.

단계

1. 볼륨 \* 탭에서 을 클릭합니다 ... 볼륨에 대해 \* Backup Now \* 를 선택합니다.



백업이 생성될 때까지 해당 볼륨의 백업 상태 옆에 "진행 중"이 표시됩니다.

## 각 볼륨의 백업 목록 보기

각 볼륨에 있는 모든 백업 파일 목록을 볼 수 있습니다. 이 페이지에는 마지막으로 수행된 백업, 현재 백업 정책, 백업 파일 크기 등과 같은 소스 볼륨, 대상 위치 및 백업 세부 정보에 대한 세부 정보가 표시됩니다.

이 페이지에서는 다음 작업도 수행할 수 있습니다.

- 볼륨에 대한 모든 백업 파일을 삭제합니다
- 볼륨에 대한 개별 백업 파일을 삭제합니다
- 볼륨에 대한 백업 보고서를 다운로드합니다

단계

1. 볼륨 \* 탭에서 을 클릭합니다 ... 소스 볼륨에 대해 \* Details & Backup List \* 를 선택합니다.

The screenshot shows the Cloud Backup console interface. At the top, there are tabs for Volumes, Restore, Kubernetes, and Job Monitor. Below the tabs, a dropdown menu shows 'All Backup Working Environments'. The main dashboard displays three key metrics: 1 Working Environment, 57 Protected Volumes, and 15.1 TB Total Backup Capacity. To the right, a 'Protected Volumes Status' section shows 57 Healthy Backup Volumes and 0 Failed Backup Volumes. Below this, a '57 Backups' section contains a table with columns: Source Working Environment, Source Volume, Source SVM, Last Backup, Backups, and Backup Status. The table lists three backup entries for 'CVO\_AWS' volumes. A context menu is open for the first entry, showing options: 'Details & Backup List' (highlighted with a red box), 'Backup Now', and 'Pause Backups'.

모든 백업 파일 목록이 소스 볼륨, 대상 위치 및 백업 세부 정보에 대한 세부 정보와 함께 표시됩니다.

The screenshot shows the detailed backup information for a specific backup. The interface is divided into three main sections: Source, Destination, and Backup Information. The Source section shows 'Working Environment' as 'Working Environment N...', 'Type' as 'Cloud Volumes ONTAP (HA)', 'Provider' as 'AWS', 'Volume' as 'Volume Name', and 'SVM' as 'SVM Name'. The Destination section shows 'Cloud Provider' as 'AWS', 'Region' as 'us-east-1', 'Bucket' as 'netapp-backup', and 'Account ID' as '012345678901234567890'. The Backup Information section shows 'Relationship Status' as 'Active', 'Last Backup' as 'Oct 05 2021, 2:41:33 pm', 'Lag Duration' as '14 days 3 hours, 38 mi...', 'Backups' as '2,050', and 'Backup Policy' as 'Netapp7YearsRetention'. Below this, a '2,050 Backups' section contains a table with columns: Backup Name, Date, and Size. The table lists three backup entries: 'Backup\_2020\_Jan', 'Backup\_2020\_Mar', and 'Backup\_2020\_Apr'.

## 백업을 삭제하는 중입니다

Cloud Backup을 사용하면 작업 환경에서 단일 백업 파일을 삭제하거나, 볼륨의 모든 백업을 삭제하거나, 모든 볼륨 백업을 삭제할 수 있습니다. 백업이 더 이상 필요하지 않거나 소스 볼륨을 삭제하고 모든 백업을 제거하려는 경우 모든 백업을 삭제할 수 있습니다.



백업이 있는 작업 환경 또는 클러스터를 삭제하려면 \* 시스템을 삭제하기 전에 \* 백업을 삭제해야 합니다. Cloud Backup은 시스템을 삭제할 때 백업을 자동으로 삭제하지 않으며, 시스템이 삭제된 후 백업을 삭제할 수 있도록 UI에 현재 지원이 없습니다. 나머지 백업에 대한 오브젝트 스토리지 비용은 계속해서 청구됩니다.

작업 환경의 모든 백업 파일을 삭제하는 중입니다

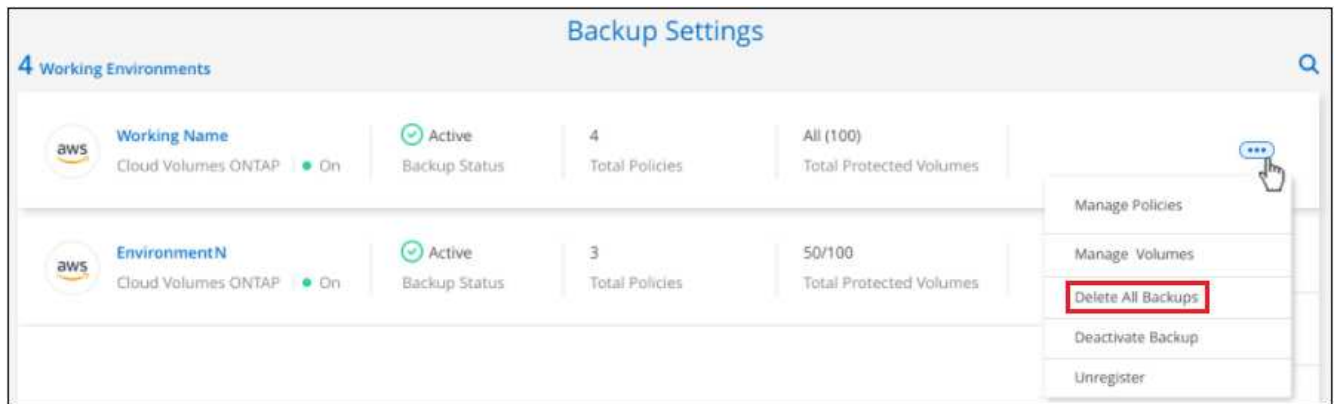
작업 환경의 모든 백업을 삭제해도 이 작업 환경의 볼륨에 대한 향후 백업이 비활성화되지는 않습니다. 작업 환경에서 모든 볼륨의 백업 생성을 중지하려면 백업을 비활성화할 수 있습니다 [참조하십시오](#).

단계

1. 볼륨 \* 탭에서 \* 백업 설정 \* 을 선택합니다.



2. 을 클릭합니다 ... 모든 백업을 삭제할 작업 환경의 경우 \* Delete all backups \* 를 선택합니다.



3. 확인 대화 상자에서 작업 환경의 이름을 입력하고 \* 삭제 \* 를 클릭합니다.

볼륨에 대한 모든 백업 파일을 삭제하는 중입니다

볼륨에 대한 모든 백업을 삭제하면 해당 볼륨에 대한 이후의 백업도 비활성화됩니다.

가능합니다 볼륨에 대한 백업을 다시 시작합니다 언제든지 백업 관리 페이지에서 수행할 수 있습니다.

단계

1. 볼륨 \* 탭에서 을 클릭합니다 ... 소스 볼륨에 대해 \* Details & Backup List \* 를 선택합니다.

The dashboard shows the following metrics:

- 1 Working Environments
- 57 Protected Volumes
- 15.1 TB Total Backup Capacity
- Protected Volumes Status: 57 Healthy Backup Volumes, 0 Failed Backup Volumes

Below the metrics, there is a section for 57 Backups. A table lists the backup details:

Source Working Environment	Source Volume	Source SVM	Last Backup	Backups	Backup Status
CVO_AWS (On)	Volume_1 (On)	SVM_1	May 22 2019, 00:00:00	2,050 Backups	Active
CVO_AWS (On)	Volume_2 (On)	SVM_1	May 22 2019, 00:00:00	2,050 Backups	
CVO_AWS (On)	Volume_3 (On)	SVM_1	May 22 2019, 00:00:00	2,050 Backups	

A dropdown menu for the first row shows options: Details & Backup List, Backup Now, and Pause Backups.

모든 백업 파일 목록이 표시됩니다.

The page displays backup configuration details in three columns:

- Source:** Working Environment (Working Environment N...), Type (Cloud Volumes ONTAP (HA)), Provider (AWS), Volume (Volume Name), SVM (SVM Name).
- Destination:** Cloud Provider (AWS), Region (us-east-1), Bucket (netapp-backup), Account ID (012345678901234567890).
- Backup Information:** Relationship Status (Active), Last Backup (Oct 05 2021, 2:41:33 pm), Lag Duration (14 days 3 hours, 38 mi...), Backups (2,050), Backup Policy (Netapp7YearsRetention).

Below the details, there is a section for 2,050 Backups. A table lists the backup details:

Backup Name	Date	Size
Backup_2020_Jan	May 22 2019, 00:00:00	19,001
Backup_2020_Mar	May 22 2019, 00:00:00	19,002
Backup_2020_Apr	May 22 2019, 00:00:00	19,009

2. Actions \* > \* Delete all backups \* 를 클릭합니다.

The page shows the 2,050 Backups table. The 'Actions' dropdown menu is open, showing the following options:

- Delete All Backups (highlighted with a red box)
- Download Backup Report

3. 확인 대화 상자에서 볼륨 이름을 입력하고 \* 삭제 \* 를 클릭합니다.

## 볼륨에 대한 단일 백업 파일 삭제

단일 백업 파일을 삭제할 수 있습니다. 이 기능은 ONTAP 9.8 이상의 시스템에서 볼륨 백업을 생성한 경우에만 사용할 수 있습니다.

단계

1. 볼륨 \* 탭에서 을 클릭합니다 ... 소스 볼륨에 대해 \* Details & Backup List \* 를 선택합니다.

Source Working Environment	Source Volume	Source SVM	Last Backup	Backups	Backup Status
CVO_AWS	Volume_1	SVM_1	May 22 2019, 00:00:00	2,050 Backups	Active
CVO_AWS	Volume_2	SVM_1	May 22 2019, 00:00:00	2,050 Backups	Active
CVO_AWS	Volume_3	SVM_1	May 22 2019, 00:00:00	2,050 Backups	Active

모든 백업 파일 목록이 표시됩니다.

Backup Name	Date	Size
Backup_2020_Jan	May 22 2019, 00:00:00	19,001
Backup_2020_Mar	May 22 2019, 00:00:00	19,002
Backup_2020_Apr	May 22 2019, 00:00:00	19,009

2. 을 클릭합니다 ... 삭제하려는 볼륨 백업 파일의 경우 \* 삭제 \* 를 클릭합니다.





3. 확인 대화 상자에서 \* 삭제 \* 를 클릭합니다.

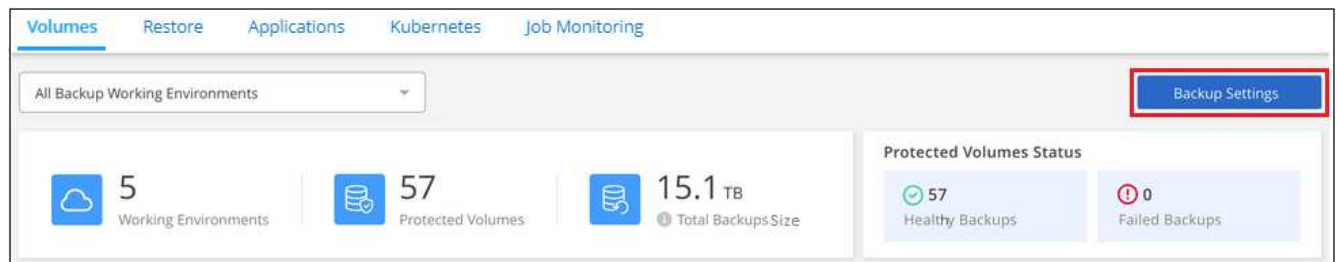
## 작업 환경에서 Cloud Backup을 해제합니다

작업 환경에서 Cloud Backup을 비활성화하면 시스템의 각 볼륨에 대한 백업이 비활성화되고 볼륨을 복구하는 기능도 비활성화됩니다. 기존 백업은 삭제되지 않습니다. 이 작업 환경에서 백업 서비스의 등록을 취소하지 않습니다. 기본적으로 모든 백업 및 복원 작업을 일정 기간 동안 일시 중지할 수 있습니다.

사용자가 비용을 부담하지 않는 한, 클라우드 공급자가 백업 용량에 대한 오브젝트 스토리지 비용에 대해 계속 청구한다는 점에 유의하십시오 **백업을 삭제합니다**.

단계

1. 볼륨 \* 탭에서 \* 백업 설정 \* 을 선택합니다.



2. 백업 설정 페이지에서 \_ 을(를) 클릭합니다 ... 백업을 비활성화하려는 작업 환경에서 \* 백업 비활성화 \* 를 선택합니다.



3. 확인 대화 상자에서 \* 비활성화 \* 를 클릭합니다.





백업이 비활성화된 동안 해당 작업 환경에 대해 \*백업 활성화\* 버튼이 나타납니다. 이 버튼을 클릭하면 해당 작업 환경에 대한 백업 기능을 다시 활성화할 수 있습니다.

## 작업 환경에 대한 클라우드 백업 등록을 취소하는 중입니다

백업 기능을 더 이상 사용하지 않고 해당 작업 환경의 백업에 대한 비용을 더 이상 부과하지 않으려는 경우 작업 환경에 대한 클라우드 백업 등록을 취소할 수 있습니다. 일반적으로 이 기능은 작업 환경을 삭제할 계획이고 백업 서비스를 취소할 때 사용됩니다.

클러스터 백업이 저장되는 대상 오브젝트 저장소를 변경하려는 경우에도 이 기능을 사용할 수 있습니다. 작업 환경에 대한 Cloud Backup의 등록을 취소한 후 새 클라우드 공급자 정보를 사용하여 해당 클러스터에 대한 Cloud Backup을 활성화할 수 있습니다.

클라우드 백업을 등록 취소하려면 먼저 다음 단계를 순서대로 수행해야 합니다.

- 작업 환경에서 Cloud Backup을 비활성화합니다
- 해당 작업 환경의 모든 백업을 삭제합니다

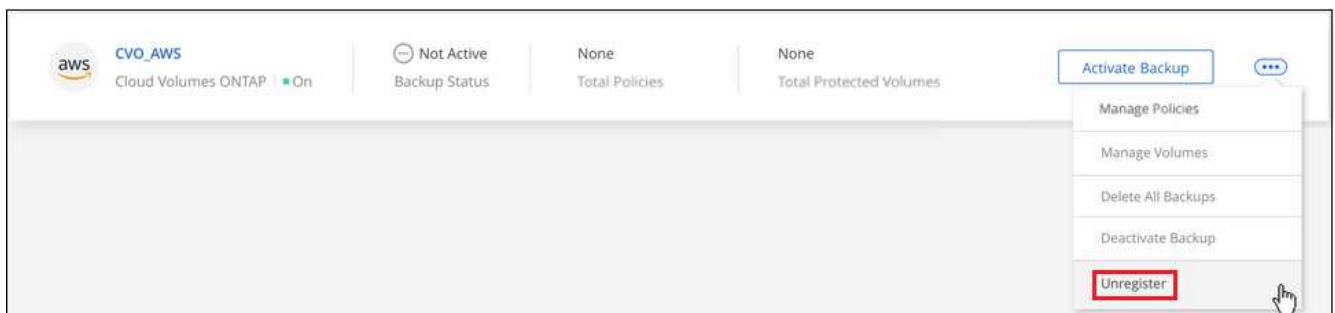
이 두 작업이 완료될 때까지 등록 취소 옵션을 사용할 수 없습니다.

단계

1. 볼륨 \* 탭에서 \* 백업 설정 \* 을 선택합니다.



2. 백업 설정 페이지에서 \_ 을(를) 클릭합니다 ... 백업 서비스의 등록을 취소하려는 작업 환경의 경우 \* 등록 취소 \* 를 선택합니다.



3. 확인 대화 상자에서 \* 등록 취소 \* 를 클릭합니다.

## 백업 파일에서 **ONTAP** 데이터를 복원하는 중입니다

백업은 클라우드 계정의 오브젝트 저장소에 저장되므로 특정 시점에서 데이터를 복원할 수

있습니다. 백업 파일에서 전체 ONTAP 볼륨을 복원하거나 몇 개의 파일만 복원해야 하는 경우 백업 파일에서 개별 파일을 복원할 수 있습니다.

볼륨 \* (새 볼륨으로)을 원래 작업 환경, 동일한 클라우드 계정을 사용하는 다른 작업 환경 또는 온프레미스 ONTAP 시스템으로 복원할 수 있습니다.

원래 작업 환경의 볼륨, 동일한 클라우드 계정을 사용하는 다른 작업 환경의 볼륨 또는 온프레미스 ONTAP 시스템의 볼륨으로 \* 파일 \* 을 복원할 수 있습니다.

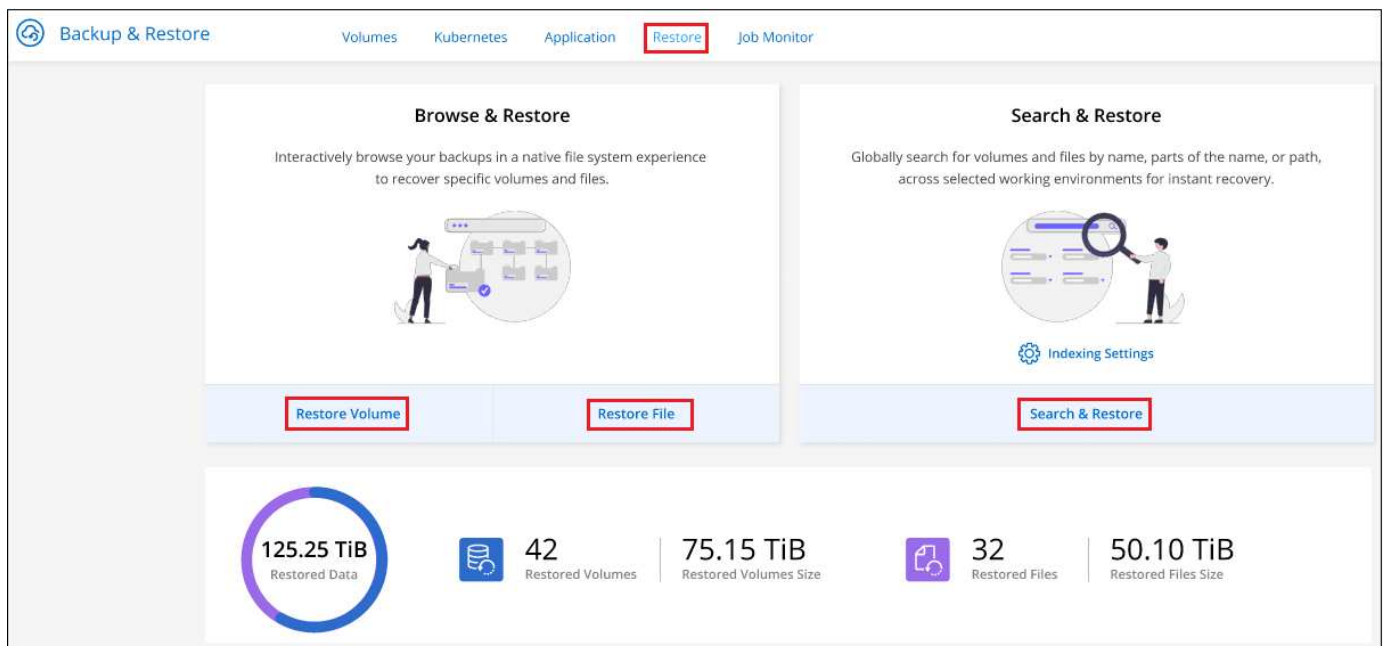
백업 파일에서 운영 시스템으로 데이터를 복원하려면 유효한 Cloud Backup 라이선스가 필요합니다.

## 복구 대시보드

복구 대시보드를 사용하여 볼륨 및 파일 복원 작업을 수행합니다. Cloud Manager 상단에 있는 \* Backup & Restore \* 를 클릭한 다음 \* Restore \* 탭을 클릭하여 Restore Dashboard에 액세스합니다. 을 클릭할 수도 있습니다 ⓘ > \* 서비스 패널의 백업 및 복원 서비스에서 복원 대시보드 보기 \* 를 선택합니다.



하나 이상의 작업 환경에 대해 Cloud Backup이 이미 활성화되어 있어야 하며 초기 백업 파일이 있어야 합니다.



보시다시피, 복원 대시보드는 백업 파일에서 데이터를 복원하는 두 가지 다른 방법을 제공합니다. \* 찾아보기 및 복원 \* 및 \* 검색 및 복원 \*.

## Browse & Restore와 Search & Restore 비교

일반적으로, 최근 주나 월로부터 특정 볼륨이나 파일을 복원해야 할 때 *Browse & Restore*가 더 낫습니다. 파일의 이름과 위치, 파일의 마지막 날짜를 알고 있어야 합니다. *Search & Restore*는 일반적으로 볼륨이나 파일을 복원해야 할 때 더 좋지만 정확한 이름, 해당 볼륨이 있는 볼륨 또는 마지막으로 양호한 상태의 날짜를 기억하지 못합니다.

이 표에서는 두 가지 방법을 비교합니다.

찾아보기 및 복원	검색 및 복원
폴더 스타일 구조를 탐색하여 단일 백업 파일 내에서 볼륨이나 파일을 찾습니다	일부 또는 전체 볼륨 이름, 일부 또는 전체 파일 이름, 크기 범위 및 추가 검색 필터를 사용하여 * 모든 백업 파일 * 에서 볼륨 또는 파일을 검색합니다
볼륨 복원은 Amazon S3, Azure Blob, Google Cloud 및 NetApp StorageGRID에 저장된 백업 파일과 함께 작동합니다. 파일 복원은 Amazon S3 및 Azure Blob에 저장된 백업 파일과 함께 작동합니다	볼륨 및 파일 복원은 Amazon S3 및 Google Cloud에 저장된 백업 파일과 함께 작동합니다
이름이 바뀌거나 삭제된 파일은 처리하지 않습니다	새로 생성/삭제/이름 변경된 디렉토리 및 새로 생성/삭제/이름 변경된 파일을 처리합니다
퍼블릭 및 프라이빗 클라우드 전체에서 결과 검색	퍼블릭 클라우드 및 로컬 스냅샷 복사본에서 결과를 찾습니다
파일 복원에 별도의 클라우드 복원 인스턴스가 필요합니다	클라우드 복원 인스턴스가 필요하지 않습니다
추가 클라우드 공급자 리소스가 필요하지 않습니다	계정당 필요한 추가 버킷 및 AWS 또는 Google 리소스
개별 파일의 백업을 탐색할 때 클라우드 복원 인스턴스와 관련된 비용입니다	검색 결과를 위해 백업 및 볼륨을 스캔할 때 AWS 또는 Google 리소스 관련 비용

두 복원 방법을 모두 사용하려면 먼저 고유한 리소스 요구 사항에 맞게 환경을 구성해야 합니다. 이러한 요구 사항은 아래 섹션에 설명되어 있습니다.

사용할 복원 작업 유형에 대한 요구 사항 및 복원 단계를 참조하십시오.

- [Browse & Restore](#)를 사용하여 볼륨을 복원합니다
- [Browse & Restore](#)를 사용하여 파일을 복원합니다
- [검색 및 Restore](#)를 사용하여 볼륨 및 파일을 복원합니다

## 찾아보기 및 복원을 사용하여 **ONTAP** 데이터를 복원합니다

볼륨 또는 파일 복원을 시작하기 전에 복원할 볼륨 또는 파일의 이름, 볼륨이 있는 작업 환경의 이름 및 복원할 백업 파일의 대략적인 날짜를 알아야 합니다.

- 참고: \* 복원하려는 볼륨의 백업 파일이 아카이브 스토리지(ONTAP 9.10.1부터 AWS 및 Azure에서 사용 가능)에 있는 경우 복원 작업에 더 많은 시간이 소요되고 비용이 발생합니다. 또한 대상 클러스터에서 ONTAP 9.10.1 이상이 실행되고 있어야 합니다.

["Azure 아카이브 스토리지에서 복원에 대해 자세히 알아보십시오."](#)["AWS 아카이브 스토리지에서 복원하는 방법에 대해 자세히 알아보십시오."](#)

### **Browse & Restore** 지원되는 작업 환경 및 객체 스토리지 공급자

ONTAP 백업 파일에서 다음 작업 환경으로 볼륨 또는 개별 파일을 복원할 수 있습니다.

백업 파일 위치	대상 작업 환경	
	* 볼륨 복원 *	* 파일 복원 *
Amazon S3	Cloud Volumes ONTAP를 사내의 AWS ONTAP 시스템에 설치하고	Cloud Volumes ONTAP를 사내의 AWS ONTAP 시스템에 설치하고

백업 파일 위치	대상 작업 환경	
Azure Blob	Azure 사내 ONTAP 시스템의 Cloud Volumes ONTAP	Azure 사내 ONTAP 시스템의 Cloud Volumes ONTAP
Google 클라우드 스토리지	Google 사내 ONTAP 시스템의 Cloud Volumes ONTAP	
NetApp StorageGRID를 참조하십시오	사내 ONTAP 시스템	

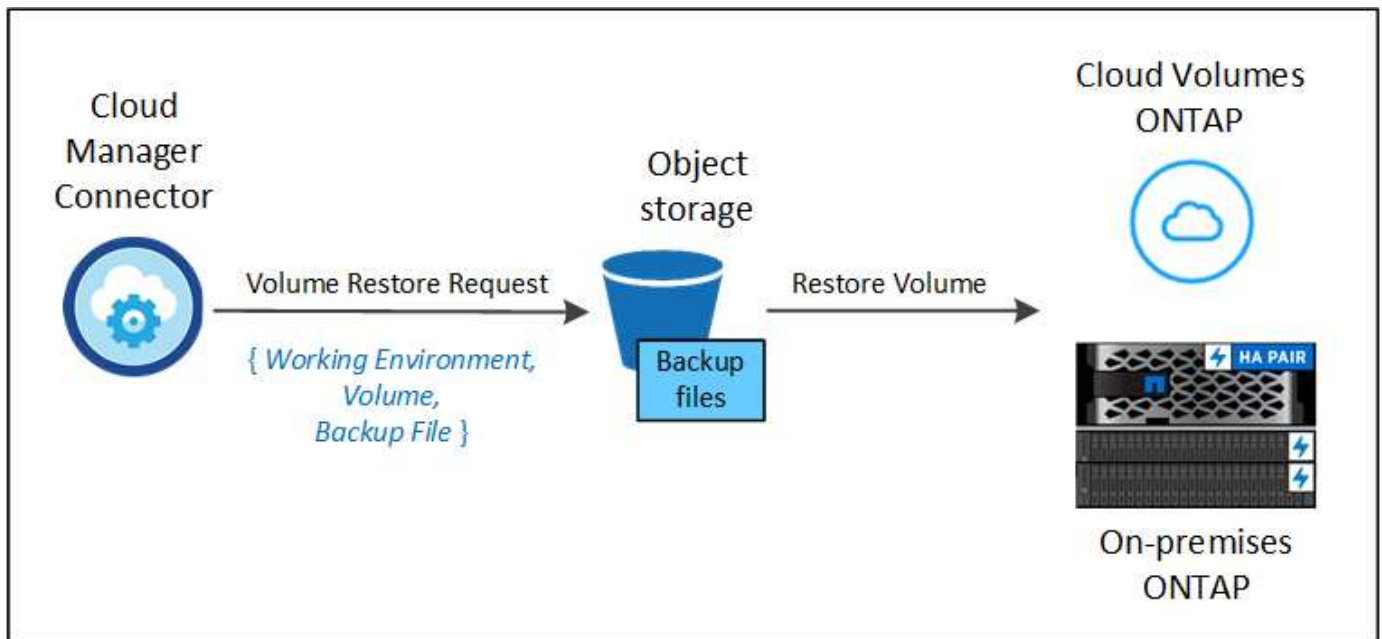
"사내 ONTAP 시스템"을 지칭할 때 FAS, AFF 및 ONTAP Select 시스템이 포함됩니다.



백업 파일이 아카이브 스토리지에 있는 경우 볼륨 복원만 지원됩니다. Browse & Restore를 사용하는 경우 현재 아카이브 스토리지에서 파일 복원이 지원되지 않습니다.

### Browse & Restore를 사용하여 볼륨을 복원합니다

백업 파일에서 볼륨을 복원하면 Cloud Backup은 백업의 데이터를 사용하여 `_new_volume`을 생성합니다. 원래 작업 환경의 볼륨이나 소스 작업 환경과 동일한 클라우드 계정에 있는 다른 작업 환경으로 데이터를 복원할 수 있습니다. 또한, 볼륨을 온프레미스 ONTAP 시스템으로 복원할 수 있습니다.



보시다시피 볼륨 복구를 수행하려면 작업 환경 이름, 볼륨 이름 및 백업 파일 날짜를 알아야 합니다.

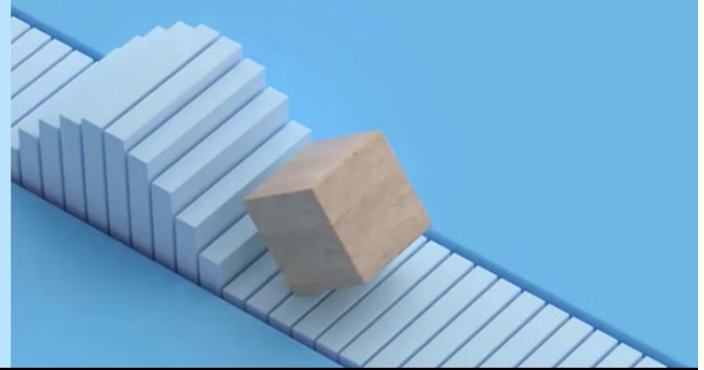
다음 비디오에서는 볼륨 복원에 대한 간단한 단계별 안내를 보여 줍니다.

# Cloud Backup Service: Restore Demo

Powered by Cloud Manager

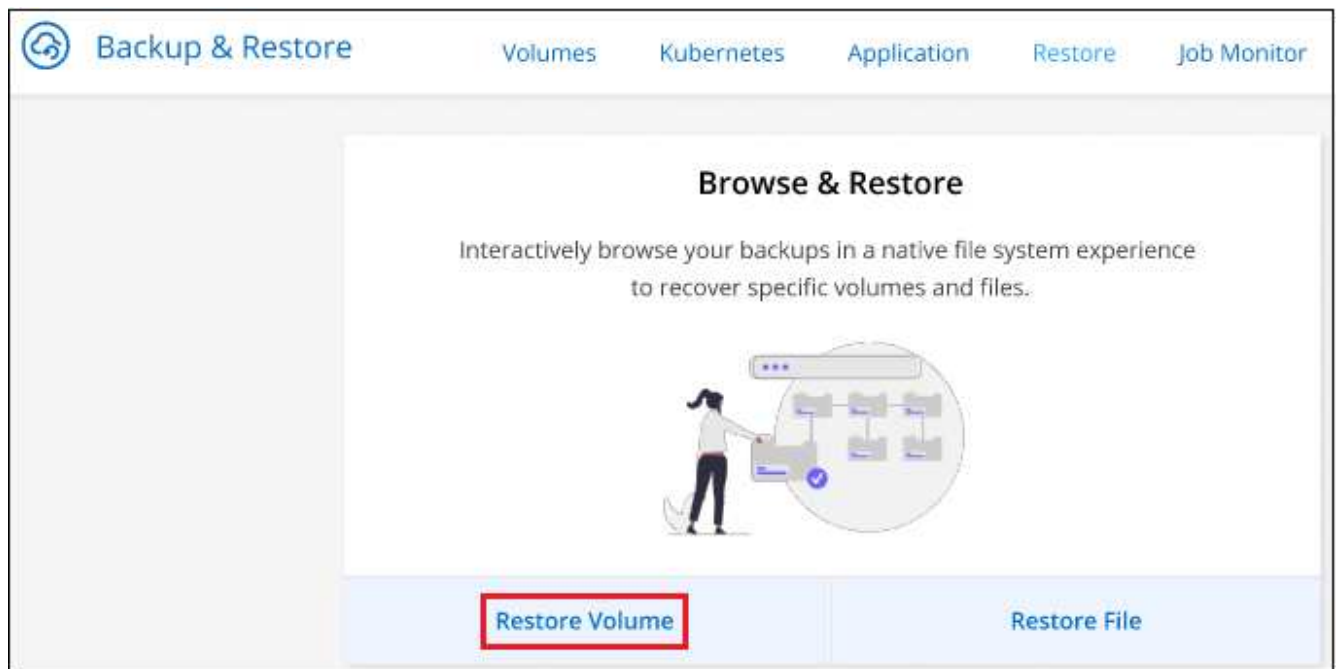
January 2022

 NetApp

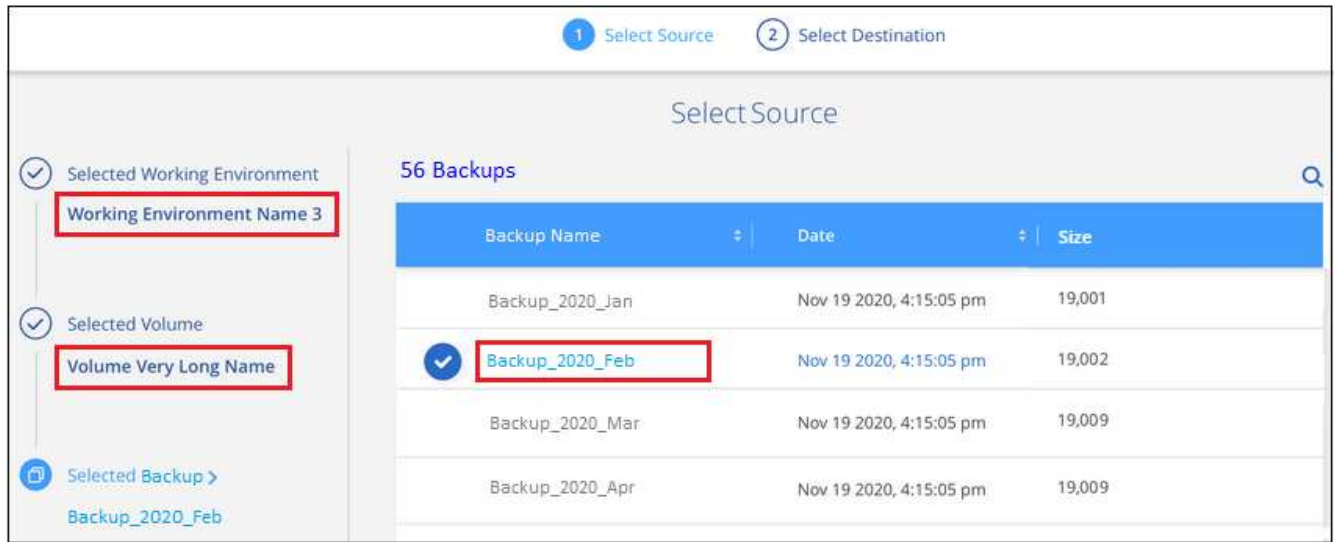


단계

1. 백업 및 복원 \* 서비스를 선택합니다.
2. Restore \* 탭을 클릭하면 Restore Dashboard가 표시됩니다.
3. Browse & Restore \_ 섹션에서 \* Restore Volume \* 을 클릭합니다.

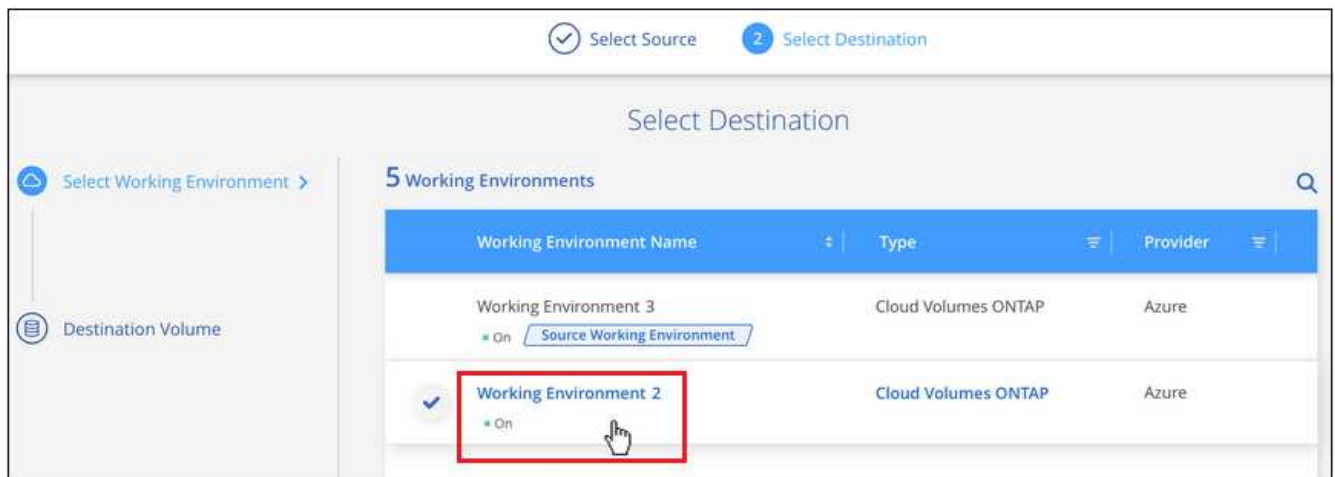


4. Select Source\_ 페이지에서 복원하려는 볼륨의 백업 파일로 이동합니다. 복원할 날짜/시간 스탬프가 있는 \* Working Environment \*, \* Volume \* 및 \* Backup \* 파일을 선택합니다.



5. 계속 \* 을 클릭합니다.

6. 대상 선택 페이지에서 볼륨을 복원할 \* 작업 환경 \* 을 선택합니다.



7. 사내 ONTAP 시스템을 선택하고 오브젝트 스토리지에 대한 클러스터 연결을 아직 구성하지 않은 경우 추가 정보를 묻는 메시지가 표시됩니다.

- Amazon S3에서 복원할 때 대상 볼륨이 상주할 ONTAP 클러스터에서 IPspace를 선택하고 ONTAP 클러스터에 S3 버킷에 대한 액세스 권한을 부여하기 위해 생성한 사용자의 액세스 키 및 암호 키를 입력합니다. 그리고 데이터 전송 보안을 위해 프라이빗 VPC 엔드포인트를 선택할 수도 있습니다.
- Azure Blob에서 복구할 경우 대상 볼륨이 상주할 ONTAP 클러스터에서 IPspace를 선택하고, 오브젝트 스토리지에 액세스할 Azure 구독을 선택한 다음 VNET 및 서브넷을 선택하여 보안 데이터 전송을 위한 프라이빗 끝점을 선택합니다.
- Google 클라우드 스토리지에서 복원할 때 Google 클라우드 프로젝트 및 액세스 키 및 비밀 키를 선택하여 오브젝트 스토리지, 백업이 저장되는 지역 및 대상 볼륨이 상주할 ONTAP 클러스터의 IPspace에 액세스합니다.
- StorageGRID에서 복구하는 경우 오브젝트 스토리지에 액세스하는 데 필요한 액세스 키 및 비밀 키를 선택하고 대상 볼륨이 상주할 ONTAP 클러스터에서 IPspace를 선택합니다.

8. 복원된 볼륨에 사용할 이름을 입력하고 볼륨이 상주하는 스토리지 VM을 선택합니다. 기본적으로 \* <source\_volume\_name>\_restore \* 가 볼륨 이름으로 사용됩니다.



볼륨을 온-프레미스 ONTAP 시스템으로 복원할 때만 볼륨의 '용량'에 사용할 Aggregate를 선택할 수 있습니다.

아카이브 스토리지 계층에 있는 백업 파일(ONTAP 9.10.1부터 사용 가능)에서 볼륨을 복원하는 경우 복원 우선 순위를 선택할 수 있습니다.

"Azure 아카이브 스토리지에서 복원에 대해 자세히 알아보십시오". "AWS 아카이브 스토리지에서 복원하는 방법에 대해 자세히 알아보십시오".

9. 복원 \* 을 클릭하면 복원 작업의 진행률을 검토할 수 있도록 복원 대시보드로 돌아갑니다.

Cloud Backup은 선택한 백업을 기반으로 새 볼륨을 생성합니다. 가능합니다 ["이 새 볼륨에 대한 백업 설정을 관리합니다"](#) 필요에 따라.

아카이브 스토리지에 있는 백업 파일에서 볼륨을 복원하는 데는 아카이브 계층 및 복원 우선 순위에 따라 몇 분 또는 몇 시간이 걸릴 수 있습니다. Job Monitor\* 탭을 클릭하여 복원 진행률을 확인할 수 있습니다.

찾아보기 및 복원을 사용하여 **ONTAP** 파일을 복원합니다

ONTAP 볼륨 백업에서 일부 파일만 복원해야 하는 경우 전체 볼륨을 복원하는 대신 개별 파일을 복원하도록 선택할 수 있습니다. 원래 작업 환경의 기존 볼륨이나 동일한 클라우드 계정을 사용하는 다른 작업 환경으로 파일을 복원할 수 있습니다. 또한 온프레미스 ONTAP 시스템의 볼륨에 파일을 복원할 수도 있습니다.

여러 파일을 선택하면 모든 파일이 선택한 동일한 대상 볼륨으로 복원됩니다. 따라서 파일을 다른 볼륨으로 복원하려면 복원 프로세스를 여러 번 실행해야 합니다.



백업 파일이 아카이브 스토리지에 있는 경우 개별 파일을 복원할 수 없습니다. 이 경우 보관되지 않은 최신 백업 파일에서 파일을 복원하거나, 아카이빙된 백업에서 전체 볼륨을 복원한 다음 필요한 파일에 액세스하거나, 검색 및 복원을 사용하여 파일을 복원할 수 있습니다.

필수 구성 요소

- 파일 복원 작업을 수행하려면 Cloud Volumes ONTAP 또는 온프레미스 ONTAP 시스템에서 ONTAP 버전이 9.6 이상이어야 합니다.
- 백업 파일에서 개별 파일을 복원하는 경우 별도의 복구 인스턴스/가상 시스템이 사용됩니다. 를 참조하십시오 ["파일 복원 작업에 배포될 인스턴스 유형입니다"](#) 또한 환경이 준비되어 있는지 확인합니다.
- Amazon S3의 백업에서 파일을 복원하려면 Cloud Manager에 사용 권한을 제공하는 사용자 역할에 특정 AWS EC2 권한을 추가해야 합니다. 또한 아웃바운드 인터넷 액세스를 허용하여 특정 엔드포인트에 연결해야 합니다.

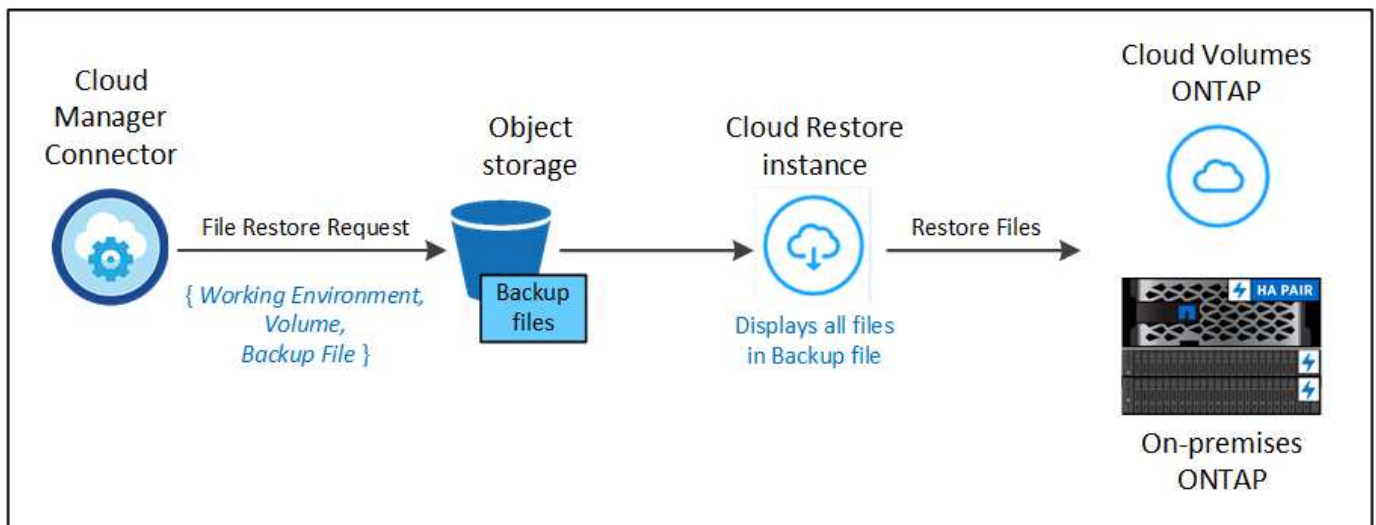
"구성이 파일을 복원할 준비가 되었는지 확인합니다".

- AWS 교차 계정 복원에는 AWS 콘솔에서 수동으로 수행해야 합니다. AWS 항목을 참조하십시오 ["교차 계정 버킷 권한 부여"](#) 를 참조하십시오.
- Azure Blob의 백업에서 파일을 복원하려면 특정 엔드포인트에 연결할 수 있는 아웃바운드 인터넷 액세스를 사용할 수 있어야 합니다. ["구성이 파일을 복원할 준비가 되었는지 확인합니다"](#).

#### 파일 복원 프로세스

프로세스는 다음과 같습니다.

1. 볼륨 백업에서 하나 이상의 파일을 복원하려면 \* 복원 \* 탭을 클릭하고, \_찾아보기 및 복원\_에서 \* 파일 복원 \* 을 클릭한 다음 파일(또는 파일)이 있는 백업 파일을 선택합니다.
2. 복구 인스턴스가 시작되고 선택한 백업 파일 내에 있는 폴더와 파일이 표시됩니다.
  - 참고: \* 복원 인스턴스는 파일을 처음 복원할 때 클라우드 공급자의 환경에 배포됩니다.
3. 해당 백업에서 복원할 파일(또는 파일)을 선택합니다.
4. 파일을 복원할 위치(작업 환경, 볼륨 및 폴더)를 선택하고 \* 복원 \* 을 클릭합니다.
5. 파일이 복원되고 일정 시간 동안 사용하지 않으면 복원 인스턴스가 종료되어 비용이 절감됩니다.



보시다시피 파일 복원을 수행하려면 작업 환경 이름, 볼륨 이름, 백업 파일 날짜 및 파일 이름을 알아야 합니다.

찾아보기 및 복원을 사용하여 파일을 복원합니다

다음 단계에 따라 ONTAP 볼륨 백업에서 볼륨에 파일을 복원합니다. 파일 또는 파일을 복원하는 데 사용할 백업 파일의 날짜와 볼륨의 이름을 알아야 합니다. 이 기능은 Live Browsing을 사용하여 각 백업 파일 내의 디렉터리 및 파일 목록을 볼 수 있습니다.

다음 비디오에서는 단일 파일 복원에 대한 간단한 단계별 안내를 보여 줍니다.

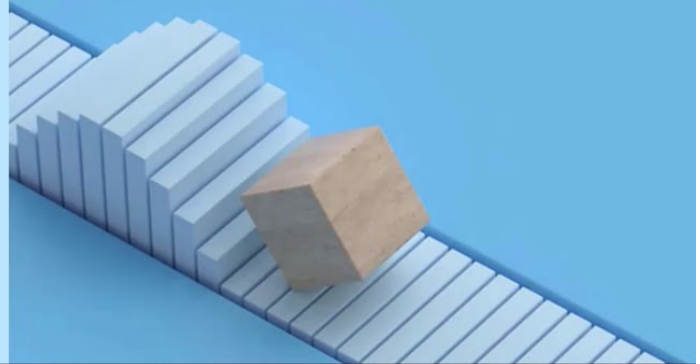


# Cloud Backup Service: Restore Demo

Powered by Cloud Manager

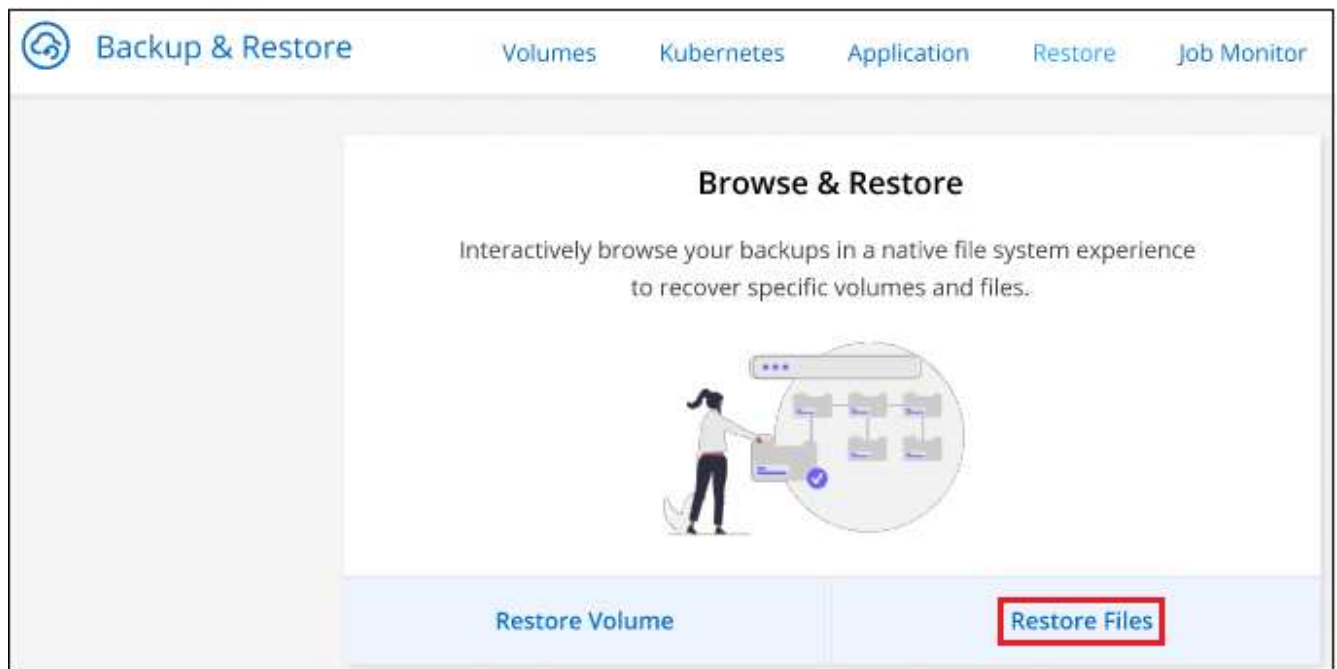
January 2022

 NetApp

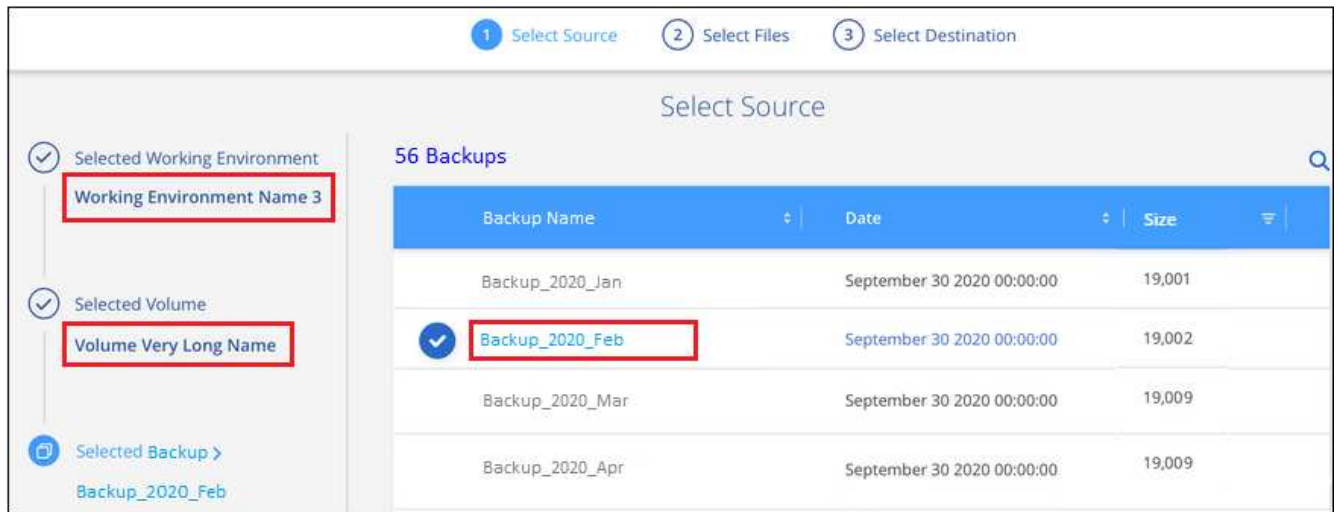


단계

1. 백업 및 복원 \* 서비스를 선택합니다.
2. Restore \* 탭을 클릭하면 Restore Dashboard가 표시됩니다.
3. Browse & Restore \_ 섹션에서 \* Restore Files \* 를 클릭합니다.

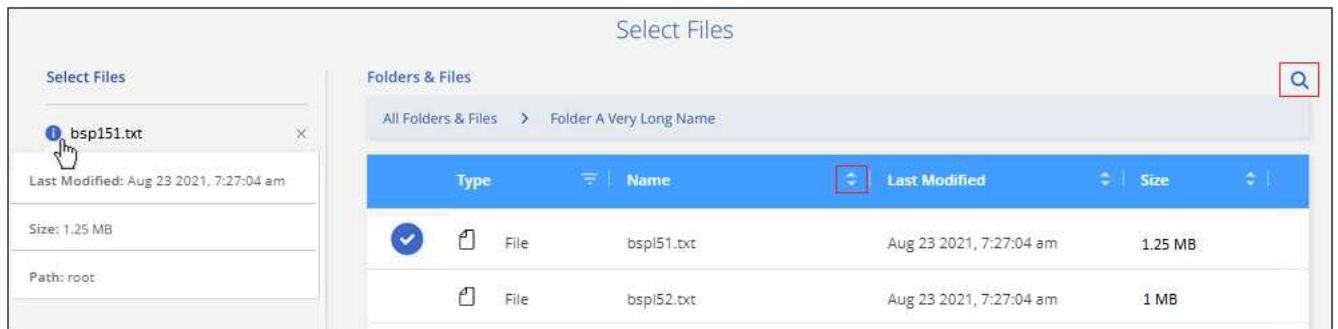


4. Select Source\_ 페이지에서 복원하려는 파일이 포함된 볼륨의 백업 파일을 찾습니다. 파일을 복원할 날짜/시간 스탬프가 있는 \* Working Environment \*, \* Volume \* 및 \* Backup \* 을 선택합니다.



5. Continue \* 를 클릭하면 Restore 인스턴스가 시작됩니다. 몇 분 후 볼륨 백업의 폴더 및 파일 목록이 표시됩니다.

- 참고: \* 파일을 처음 복원할 때 복원 인스턴스가 클라우드 공급자의 환경에 배포되므로 이 단계를 처음 수행할 때 몇 분 정도 더 걸릴 수 있습니다.

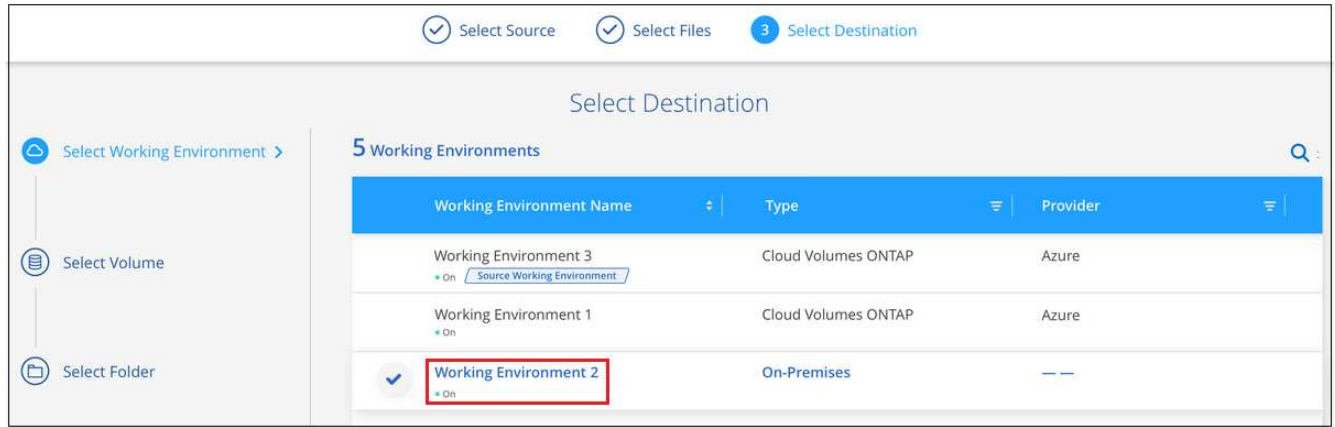


6. Select Files\_page(파일 선택 페이지)에서 복원하려는 파일을 선택하고 \* Continue \*(계속 \*)를 클릭합니다. 파일을 찾는 데 도움이 되는 방법은 다음과 같습니다.

- 파일 이름이 표시되면 해당 이름을 클릭할 수 있습니다.
- 검색 아이콘을 클릭하고 파일 이름을 입력하여 파일로 직접 이동할 수 있습니다.
- 를 사용하여 폴더의 하위 수준을 탐색할 수 있습니다 > 버튼을 클릭하여 파일을 찾습니다.

파일을 선택하면 이미 선택한 파일을 볼 수 있도록 페이지 왼쪽에 추가됩니다. 필요한 경우 파일 이름 옆의 \* x \* 를 클릭하여 이 목록에서 파일을 제거할 수 있습니다.

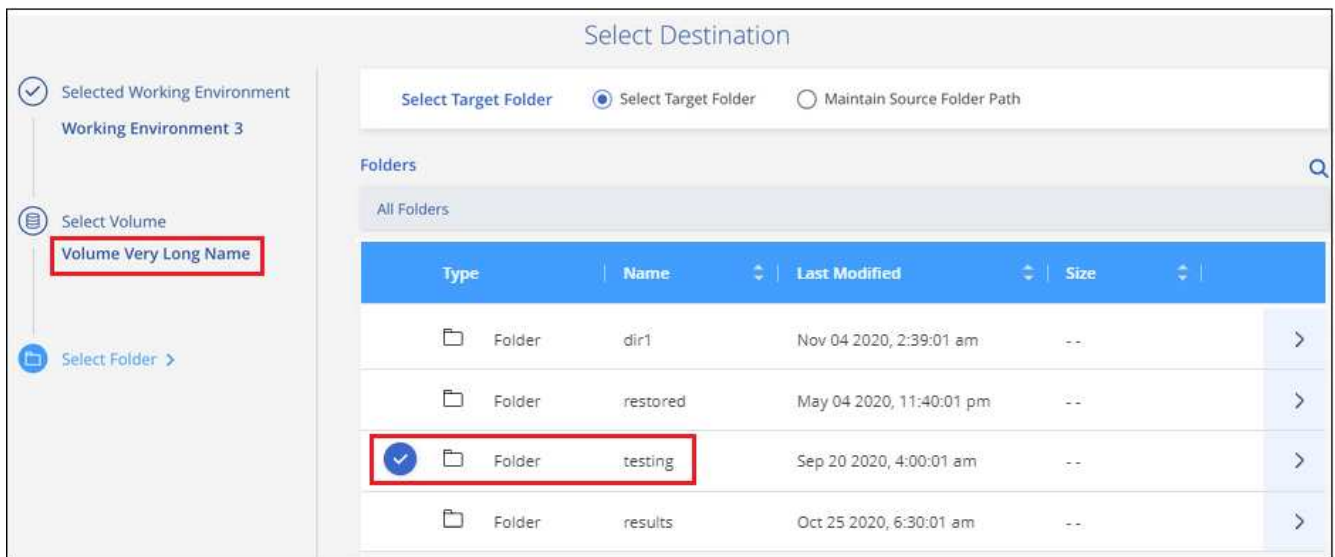
7. 대상 선택 페이지에서 파일을 복원할 \* 작업 환경 \* 을 선택합니다.



사내 클러스터를 선택하고 오브젝트 스토리지에 대한 클러스터 연결을 아직 구성하지 않은 경우 추가 정보를 묻는 메시지가 표시됩니다.

- Amazon S3에서 복원할 때 대상 볼륨이 있는 ONTAP 클러스터에 IPspace를 입력하고 오브젝트 스토리지에 액세스하는 데 필요한 AWS 액세스 키 및 비밀 키를 입력합니다.
- Azure Blob에서 복구할 경우 대상 볼륨이 있는 ONTAP 클러스터에 IPspace를 입력합니다.

8. 그런 다음 파일을 복원할 \* 볼륨 \* 과 \* 폴더 \* 를 선택합니다.



파일을 복원할 때 위치에 대한 몇 가지 옵션이 있습니다.

- 위와 같이 \* 대상 폴더 선택 \* 을 선택한 경우:
  - 폴더를 선택할 수 있습니다.
  - 폴더 위로 마우스를 가져가 을 클릭할 수 있습니다 ▶ 행 끝에서 하위 폴더로 드릴다운한 다음 폴더를 선택합니다.
- 소스 파일이 있는 위치와 동일한 대상 작업 환경 및 볼륨을 선택한 경우 \* 소스 폴더 경로 유지 \* 를 선택하여 파일 또는 모든 파일을 소스 구조에 있는 동일한 폴더로 복원할 수 있습니다. 모든 동일한 폴더와 하위 폴더가 이미 존재해야 하며 폴더가 생성되지 않습니다.

9. 복원 \* 을 클릭하면 복원 작업의 진행률을 검토할 수 있도록 복원 대시보드로 돌아갑니다. 또한 \* Job Monitor \* 탭을 클릭하여 복원 진행률을 확인할 수도 있습니다.

특정 기간 동안 사용하지 않으면 복원 인스턴스가 종료되므로 비용이 절약되므로 활성 상태일 때만 비용이 발생합니다.

## 검색 및 복원을 사용하여 **ONTAP** 데이터를 복원합니다

검색 및 복원을 사용하여 ONTAP 백업 파일에서 볼륨이나 개별 파일을 복원할 수 있습니다. 검색 및 복원을 사용하면 특정 공급자에 대해 클라우드 스토리지에 저장된 모든 백업에서 특정 볼륨이나 파일을 검색한 다음 복구를 수행할 수 있습니다. 정확한 작업 환경 이름 또는 볼륨 이름을 알 필요가 없습니다. 모든 볼륨 백업 파일을 검색합니다.

또한 검색 작업을 통해 ONTAP 볼륨에 대한 모든 로컬 스냅샷 복사본을 확인합니다. 로컬 스냅샷 복사본에서 데이터를 복원하는 것이 백업 파일에서 복원하는 것보다 빠르고 비용이 적게 들 수 있으므로 스냅샷에서 데이터를 복원할 수 있습니다. Canvas의 볼륨 세부 정보 페이지에서 스냅샷을 새 볼륨으로 복원할 수 있습니다.

백업 파일에서 볼륨을 복원하면 Cloud Backup은 백업의 데이터를 사용하여 `_new_volume`을 생성합니다. 원래 작업 환경에서 데이터를 볼륨으로 복원하거나 소스 작업 환경과 동일한 클라우드 계정에 있는 다른 작업 환경으로 복원할 수 있습니다. 또한, 볼륨을 온프레미스 ONTAP 시스템으로 복원할 수 있습니다.

파일을 원래 볼륨 위치, 동일한 작업 환경의 다른 볼륨 또는 동일한 클라우드 계정을 사용하는 다른 작업 환경으로 복원할 수 있습니다. 또한 온프레미스 ONTAP 시스템의 볼륨에 파일을 복원할 수도 있습니다.

복원하려는 볼륨의 백업 파일이 아카이브 스토리지(ONTAP 9.10.1부터 AWS에서 사용 가능)에 있는 경우 복원 작업에 더 많은 시간이 소요되고 추가 비용이 발생합니다. 대상 클러스터도 ONTAP 9.10.1 이상을 실행해야 하며 아카이브 스토리지에서 파일 복원은 현재 지원되지 않습니다.

["AWS 아카이브 스토리지에서 복원하는 방법에 대해 자세히 알아보십시오"](#).

시작하기 전에 복원하려는 볼륨이나 파일의 이름이나 위치를 알고 있어야 합니다.

다음 비디오에서는 단일 파일 복원에 대한 간단한 단계별 안내를 보여 줍니다.



검색 및 복원 지원되는 작업 환경 및 오브젝트 스토리지 공급자

ONTAP 백업 파일에서 다음 작업 환경으로 볼륨 또는 개별 파일을 복원할 수 있습니다.

백업 파일 위치	대상 작업 환경	
	* 볼륨 복원 *	* 파일 복원 *
Amazon S3	Cloud Volumes ONTAP를 사내의 AWS ONTAP 시스템에 설치하고	Cloud Volumes ONTAP를 사내의 AWS ONTAP 시스템에 설치하고
Google 클라우드 스토리지	Google 사내 ONTAP 시스템의 Cloud Volumes ONTAP	Google 사내 ONTAP 시스템의 Cloud Volumes ONTAP

"사내 ONTAP 시스템"을 지칭할 때 FAS, AFF 및 ONTAP Select 시스템이 포함됩니다.

#### 필수 구성 요소

- 클러스터 요구 사항:
  - ONTAP 버전은 9.8 이상이어야 합니다.
  - 볼륨이 상주하는 스토리지 VM(SVM)에는 데이터 LIF가 구성되어 있어야 합니다.
  - 볼륨에 NFS가 활성화되어 있어야 합니다.
  - SVM에서 SnapDiff RPC 서버를 활성화해야 합니다. 작업 환경에서 인덱싱을 활성화하면 Cloud Manager가 이 작업을 자동으로 수행합니다.

- AWS 요구사항:

- Cloud Manager에 권한을 제공하는 사용자 역할에 특정 Amazon Athena, AWS Glue 및 AWS S3 권한을 추가해야 합니다. ["모든 권한이 올바르게 구성되었는지 확인합니다"](#).

이전에 구성한 Connector와 함께 Cloud Backup을 이미 사용하고 있는 경우, 이제 Athena 및 Glue 권한을 Cloud Manager 사용자 역할에 추가해야 합니다. 새로운 항목이므로 검색 및 복원에 필요합니다.

- Google Cloud 요구사항:

- Cloud Manager에 권한을 제공하는 사용자 역할에 특정 Google BigQuery 권한을 추가해야 합니다. ["모든 권한이 올바르게 구성되었는지 확인합니다"](#).

이전에 구성한 Connector와 함께 Cloud Backup을 이미 사용하고 있는 경우 지금 BigQuery 권한을 Cloud Manager 사용자 역할에 추가해야 합니다. 새로운 항목이므로 검색 및 복원에 필요합니다.

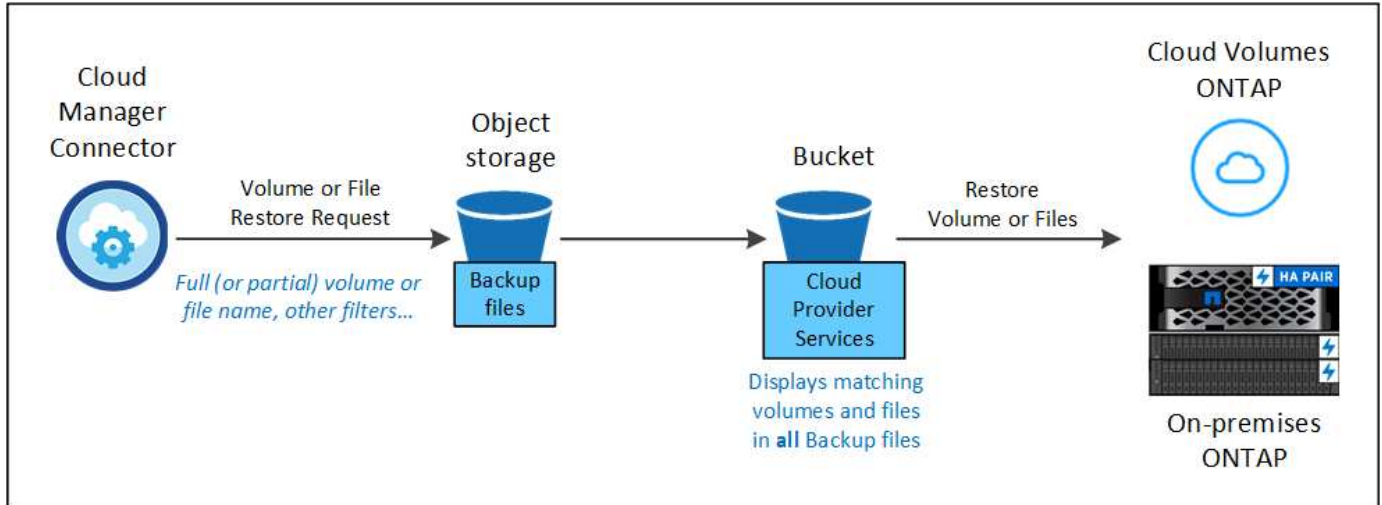
#### 검색 및 복원 프로세스

프로세스는 다음과 같습니다.

- 검색 및 복원을 사용하려면 볼륨이나 파일을 복원할 각 소스 작업 환경에서 "인덱싱"을 활성화해야 합니다. 따라서 인덱싱된 카탈로그를 통해 모든 볼륨의 백업 파일을 추적할 수 있습니다.
- 볼륨 백업에서 볼륨이나 파일을 복원하려면 *Search & Restore* 아래에서 \* 검색 및 복원 \* 을 클릭합니다.
- 볼륨 또는 파일의 검색 기준을 전체 또는 일부 볼륨 이름, 전체 파일 이름, 크기 범위, 생성 날짜 범위, 기타 검색 필터로 입력하고 \* 검색 \* 을 클릭합니다.

검색 결과 페이지에는 검색 기준과 일치하는 파일 또는 볼륨이 있는 모든 위치가 표시됩니다.

4. 볼륨 또는 파일을 복원하는 데 사용할 위치에 대한 모든 백업 보기 \* 를 클릭한 다음 사용할 실제 백업 파일에서 \* 복원 \* 을 클릭합니다.
5. 볼륨이나 파일을 복원할 위치를 선택하고 \* 복원 \* 을 클릭합니다.
6. 볼륨 또는 파일이 복원됩니다.



보시다시피, 부분 볼륨 또는 파일 이름만 알면 되며 Cloud Backup은 검색과 일치하는 모든 백업 파일을 검색합니다.

#### 각 작업 환경에 대해 인덱싱된 카탈로그 활성화

검색 및 복원을 사용하려면 볼륨 또는 파일을 복원할 각 소스 작업 환경에서 "인덱싱"을 활성화해야 합니다. 따라서 인덱싱된 카탈로그를 통해 모든 볼륨과 모든 백업 파일을 추적할 수 있어 검색이 매우 빠르고 효율적입니다.

이 기능을 활성화하면 Cloud Backup은 SVM에서 볼륨에 대해 SnapDiff v3를 활성화하고 다음 작업을 수행합니다.

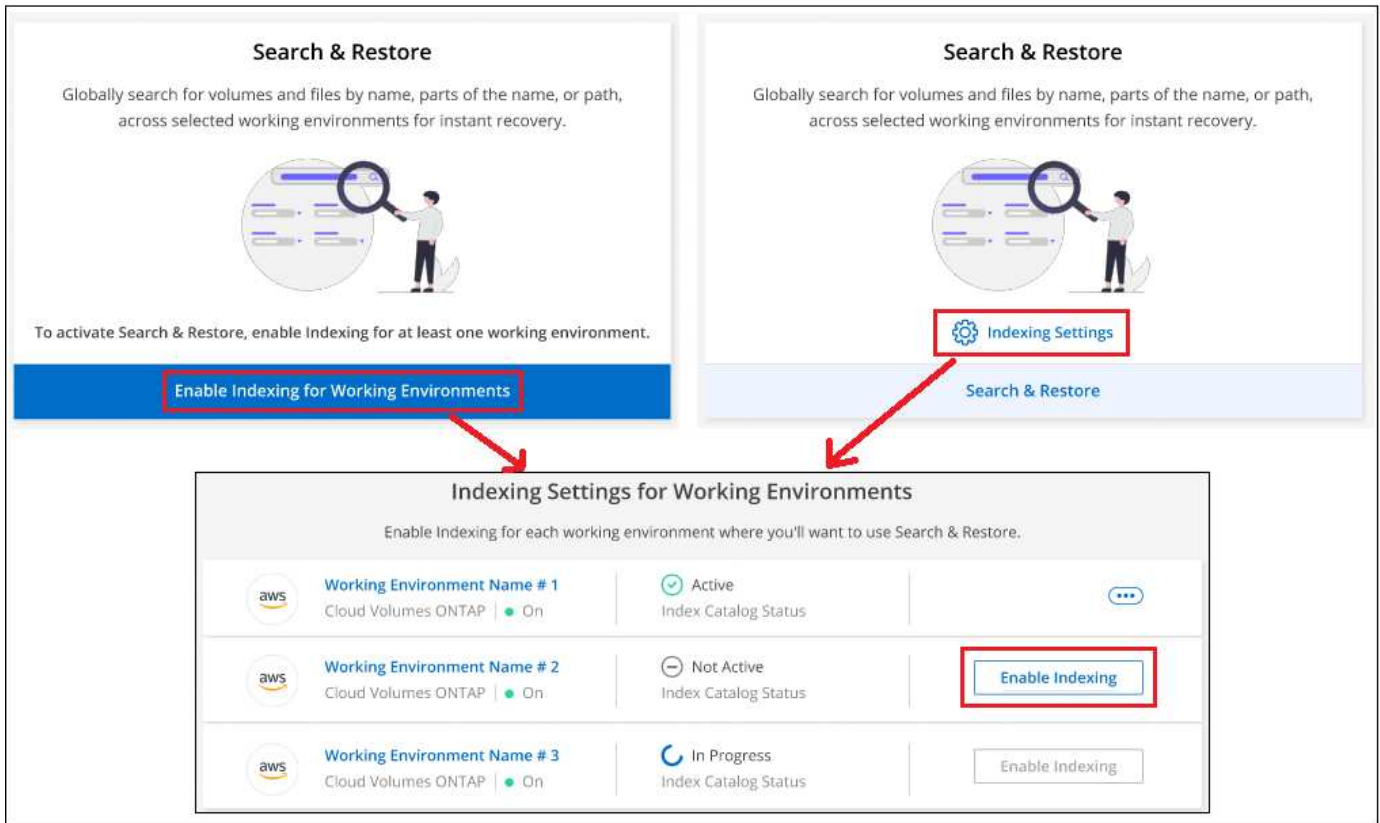
- AWS에 저장된 백업의 경우 새로운 S3 버킷과 을 프로비저닝합니다 ["아마존 Athena 대화형 쿼리 서비스"](#) 및 ["AWS Glue 서버리스 데이터 통합 서비스"](#).
- Google Cloud에 저장된 백업의 경우 IT 부서는 새로운 버킷과 을 프로비저닝합니다 ["Google Cloud BigQuery 서비스"](#) 계정/프로젝트 수준에서 프로비저닝됩니다. 작업 환경에 대해 인덱싱이 이미 활성화되어 있는 경우 다음 섹션으로 이동하여 데이터를 복원합니다.

#### 작업 환경의 인덱싱 활성화하기:

- 작업 환경이 인덱싱되지 않은 경우, 복구 대시보드의 **Search & Restore** 아래에서 \* 작업 환경에 대한 인덱싱 사용 \* 을 클릭하고 작업 환경에 대해 \* 인덱싱 사용 \* 을 클릭합니다.
- 하나 이상의 작업 환경이 이미 인덱싱된 경우, 복구 대시보드의 **Search & Restore** 아래에서 \* 인덱싱 설정 \* 을 클릭하고 작업 환경에 대해 \* 인덱싱 사용 \* 을 클릭합니다.

모든 서비스가 프로비저닝되고 인덱싱된 카탈로그가 활성화되면 작업 환경이 "활성"으로 표시됩니다.





작업 환경의 볼륨 크기와 클라우드의 백업 파일 수에 따라 초기 인덱싱 프로세스에 최대 1시간이 걸릴 수 있습니다. 그 이후에는 운영 환경에 영향을 미치지 않고 매시간 업데이트되며, 지속적으로 변경될 수 있습니다.

검색 및 복원을 사용하여 볼륨 및 파일을 복원합니다

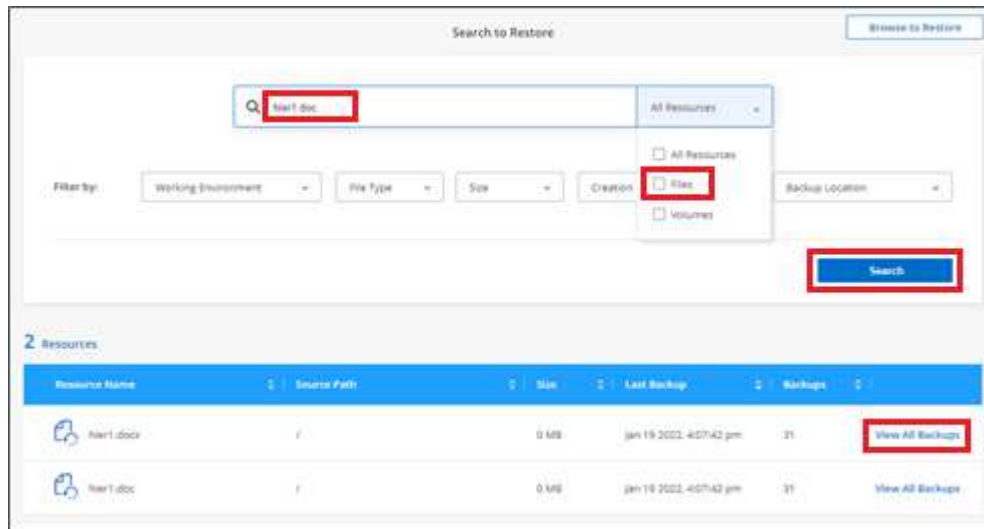
먼저 해 **작업 환경에 대한 인덱싱 기능을 활성화했습니다**, 검색 및 복원을 사용하여 볼륨이나 파일을 복원할 수 있습니다. 이를 통해 광범위한 필터를 사용하여 모든 백업 파일에서 복원하려는 정확한 파일 또는 볼륨을 찾을 수 있습니다.

단계

1. 백업 및 복원 \* 서비스를 선택합니다.
2. Restore \* 탭을 클릭하면 Restore Dashboard가 표시됩니다.
3. Search & Restore \_ 섹션에서 \* Search & Restore \* 를 클릭합니다.

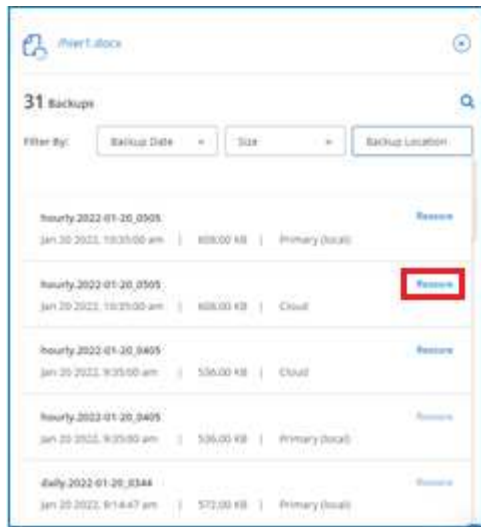


4. 검색 및 복원 페이지에서 다음을 수행합니다.
  - a. 검색 표시줄에 전체 또는 부분 볼륨 이름 또는 파일 이름을 입력합니다.
  - b. 필터 영역에서 필터 기준을 선택합니다. 예를 들어 데이터가 있는 작업 환경과 파일 형식(예: .doc 파일)을 선택할 수 있습니다.
5. 검색 \* 을 클릭하면 검색 결과 영역에 검색과 일치하는 파일 또는 볼륨이 있는 모든 위치가 표시됩니다.



6. 복원하려는 데이터가 있는 위치에 대해 \* 모든 백업 보기 \* 를 클릭하면 볼륨 또는 파일이 포함된 모든 백업 파일이 표시됩니다.





7. 클라우드에서 볼륨 또는 파일을 복원하는 데 사용할 백업 파일에 대해 \* 복원 \* 을 클릭합니다.

검색 결과에 파일이 포함된 로컬 볼륨 스냅샷 복사본도 포함됩니다. 현재 스냅샷에 대해 \* 복원 \* 버튼이 작동하지 않지만 백업 파일 대신 스냅샷 복사본에서 데이터를 복원하려면 볼륨의 이름과 위치를 적어 두고 Canvas에서 볼륨 세부 정보 페이지를 엽니다. 및 \* 스냅샷 복사본에서 복원 \* 옵션을 사용합니다.

8. 볼륨이나 파일을 복원할 위치를 선택하고 \* 복원 \* 을 클릭합니다.

- 파일의 경우 원래 위치로 복원하거나 대체 위치를 선택할 수 있습니다
- 볼륨의 경우 위치를 선택할 수 있습니다.

볼륨 또는 파일이 복원되고 복구 작업의 진행률을 검토할 수 있도록 복구 대시보드로 돌아갑니다. 또한 \* Job Monitor \* 탭을 클릭하여 복원 진행률을 확인할 수도 있습니다.

복원된 볼륨의 경우 를 사용할 수 있습니다 ["이 새 볼륨에 대한 백업 설정을 관리합니다"](#) 필요에 따라.

## Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.